云计算合规教程

云计算合规教程

对于合规性的关注是阻碍众多公司使用云服务的主要原因之一。价格低廉、计算灵活，可根据需求创建、拆开、重配置、扩张和收缩，这些都是其吸引人的特点，但是它是否包括了必要的监管要求？

企业在盲目部署云服务前，必须考虑到云计算的合规问题。本技术手册将带你一起讨论云合规问题，帮助企业全面的看待云计算所带来的影响。

认识云计算合规性问题

说起云计算，你可能滔滔不绝地讲出它的概念，理念，基本模式，好处及风险等等。那么，什么是云计算合规问题？对此，你不是很清楚？没关系，我们首先就来了解一下云计算合规性问题，即云合规问题。

- ❖ 了解并解决云计算合规性问题
- ❖ 云计算 PCI 合规：这可能吗？
- ❖ 云计算的战略要点——成本控制与合规审查

云合规问题中的几个主要方面

了解了什么是云合规问题，我们就要着手解决这个问题了，在解决过程中，有哪些思路可供企业参考？众多问题中，什么是关键问题和主要问题？这部分中，我们将介绍云合规问题中的几个重要方面。

- 关于云计算合规性的四条建议
- 云归档：合规数据的安全很重要
- 云计算规则遵从：可视性是关键
- 在云计算合同中遵循合规性需求

促进云计算合规的解决方案

知道了云计算合规的几个重要方面，下一步就是考虑部署促进云合规的方案了，目前有什么措施可供企业选择，未来又会出现哪些解决方案呢？这一部分，我们就来获取促进云计算合规的解决方案。

- 补偿控制有助于促进云合规
- 云成熟度模型帮助中小企业判断云服务提供商的安全

了解并解决云计算合规性问题

本文是云安全应用指南系列中的第八篇，我们将讨论云的合规性问题。对于合规性的关注是阻碍众多公司使用云服务的主要原因之一。价格低廉、计算灵活，可根据需求创建、拆开、重配置、扩张和收缩，这些都是其吸引人的特点，但是它是否包括了必要的监管要求？

诸如 Massachusetts 隐私法（201 CMR17）、PCI-DSS、SOX、Nevada SB-227 和 HIPAA 之类的标准与法规都要求众多组织对他们的数据保护措施进行安全评估。将数据和应用迁移至云将影响该组织遵守这些法规和标准的能力。在本文中，我们将主要探讨云计算对企业保持合规性能力产生负面影响的两个特点。

关于合规性问题，每个法规都需要各组织充分保护他们的实体资产和信息资产。要达到这个目的，需要对整个系统有一个很好的控制，并且确定：

- 系统中存储什么信息？
- 存储的信息位于何处？
- 谁能够访问系统？
- 他们可以访问什么？
- 访问是否合适？

所有这些问题意味着一个资产所有权的级别问题，也就是云合规性问题的核心所在。在公共云环境中，您可以肯定地回答第一个问题，但是剩余四个问题在合规性方面就有一定的麻烦，我们来分别对其进行分析。

存储的信息位于何处？

在一个典型企业数据中心或托管中心中，大家都知道磁盘和服务器实际的物理位置所在，这一事实可在审核过程中得到证实。通常而言，即使是一个共享服务供应商也能告诉你，你所使用系统的是哪一个物理系统，并根据审核的目的来辨识数据的位置。即使对于虚拟化和灾难恢复，你也可以想办法来确定信息资源所在的物理位置。根据其定义，这并不符合公共云的情况，这便是我们所谈到的第一个云合规性问题。

在云中，我们并不期望供应商方能够提供信息实际位置的相关信息。但这并不是说供应商不能这么做，然而市场并未要求他们提供该项服务。同时，说句公道话，要求了解数据位置的需求与云计算的本质目的是相矛盾的。

那么，你可以做什么？确保你的供应商也愿意与你合作，提供并检测你可能遇到的数据位置限制。

谁将访问系统、访问系统的哪些信息以及为什么访问系统？

公共云中第二个合规性问题如下因素相关：

- 谁能够访问你的信息存储系统？
- 他们可以访问哪些信息？
- 服务是否合适（也就是说为什么要提供这种服务）？

关于访问权限问题，除了你所控制的一方，供应商工作人员也可以访问系统。在供应商方，我们所关注的主要人员是系统管理员和应用管理员。我们需要了解系统管理员和应用管理员是的身份。当考虑他们能够访问什么信息时，我们主要关注供应商访问我们底层信息存储基础设施或应用的能力。了解他们是通过管理程序（如基础设施即服务，IaaS）还是在应用层（如平台即服务，PaaS）访问？

最后的一个问题是他们“为什么”需要访问系统？这也是 Security 101 所规定的：必须基于工作角色来确定访问权限，必须对访问等级提供明确的说明。

事实上，这也是一个共享主机设备中出现的问题。其主要区别在于许多云供应商并不能满足众多合规性文件中规定的要求，而共享主机设备已足够成熟具备该能力。

那么，你需要做的就是确保合作供应商能够并愿意证明他们提供的管理功能能够实现职责分离，而且他们有能力“证明”谁有机会访问系统和信息，并提供访问的时间信息。请注意，还有最后一个要求，你需要部署健全的、与最新安全等级相关的日志解决方案。

作为附带说明，我认为整个行业需要对公共云供应商进行认证，而那些认证对于用户合规性而言是可以接受的。

总结

大部分合规性要求是为了对有机会访问资产的人员、他们所访的问等级以及那些等级的维护进行适当的控制。通常的方法是对我们的进程进行审核。公共云环境的相对不成熟性将使得审核过程变得非常困难，有时甚至是不可能实现。改变这一状况要从以下两方面入手：

- 公共云产品必须成熟，更加遵守标准。
- 公共云供应商必须与用户签署相关合同协议，这有助于客户满足云合规性的需求。

（作者：Phil Cox　译者：滕晓龙　来源：TechTarget 中国）

云计算 PCI 合规：这可能吗？

问：一些厂商和服务提供商声称他们提供符合 PCI DSS 的基于云的服务，抛开厂商的自我宣传，这是真的吗？

答：这是可能的，但要记住，在作出这样一个大胆的、绝对的和明确的声明前，各个领域的 PCI 合规都需要深入研究。

首先，“云计算”一词可以有任何多种不同的含义，每个都以它们自己的方式显著。确保你了解关于云服务提供的确切性质。

也就是说，如果典型的云计算服务可以被定义为“目标用户池在虚拟环境中共享计算资源”，那么如果厂商和服务提供商计划实现 PCI 合规的话，他们还有很多工作要做。具体来说，这些组织必须提供真实可信的证据满足 PCI DSS 所有的 12 条要求，更加强调确保客户 A 端的数据到客户 B 的端数据的逻辑分离及保护。此外，这些组织也将提供证据，满足经常被忽视的 PCI DSS 的附录 A 部分，其中有明确要求，确保共享宿主环境中的数据分离，比如云计算。

云计算 PCI 合规最困难的一个方面是，获得可验证和可靠的审计证据，从而通过合格的安全评估（质量体系评审）签署。许多传统厂商和服务提供商实际上是提供基于云的服务，但他们多次通过亚马逊或微软的云基础设施，而这一点，是很难取得审计证据的。但是，如果实际的供应商或服务提供商通过自己专有搭建的云平台来提供这些服务，验证将不再是一个挑战。

即使考虑到这一点，每个 PCI DSS 要求也必须得到验证，一个质量体系评审（QSA）或其他主管审计师必须验证以下两点，（1）12 个 PCI DSS 要求做到位；（2）在 12 个 PCI DSS 要求中，并在适用情况下，要真正实现数据在客户端 A 到客户端 B 间的分离。不管一个企业是否在其持卡人数据环境中采用云计算服务，验证都是必须的。这不是个简单的任务，但如果云提供商和质量体系评审愿意以有效的方式共同努力，验证是可以做到的。因此，许多领域将需要通过实际上属于附录 A 范围的检查，附录 A 中说明了分离和隔离的要求。

（作者：Charles Denyer 译者：Ping 来源：TechTarget 中国）

云计算的战略要点——成本控制与合规审查

我是个老 IT 人了，经历了很多的风吹雨打。很多老家伙看不惯自持才高的年轻人，说他们“傲慢无知”，我不会。但和激进的年轻人不同，我更多时候是冷静，因为在 IT 这行，我看到过太多的分合交替，盛衰兴旺。多年前，在 Al Gore 发明互联网之后不久，无数的应用服务供应商（ASP）和管理服务供应商（MSP）便一涌而出，妄图争夺这块潜在的大蛋糕。时光流逝，绝大部分供应商从市场上永远地消失了，历经磨难留存下来的只有极少一部分。因为，那时候的市场（无数的像我这样的企业）还全然接受不了将自己的应用服务托管在第三方的基础设施上。

目前的市场宠儿当属云计算，业内业外一片喧嚣嘈杂，像极了当年 ASP/MSP 热潮的初期。当然了，我不会无端偏见-如果云计算名副其实，我一定不想错过。因此，我想客观地评估一下“云”模式并确定其能否助我创造商业价值。

我评估“云”模式的方法与我解决其他 IT 难题相同：向我熟知的一群精英求教。多年来，因为工作关系我结交了约 200 位 CIO 同仁，一旦遇到任何超越个人理解/控制范畴的困难我便向他们求助，屡试不爽。

我这次是给他们发电邮，请他们回答几个问题，以助我理解“云”的实际价值：1、已迁移到“云”的 IT 服务有哪些；2、正考虑向“云”进行迁移的 IT 服务有哪些；3、什么是云计算的真正核心价值；4、如果不考虑云计算，理由是什么。

不久我便收到了他们的回复。对云计算持积极态度的总结如下：1、不少 CIO 将其垃圾邮件过滤系统迁到了“云”上，以释放更多带宽给正常的邮件处理使用；2、几位勇敢果断的同行将其整个电邮系统迁到了“云”上；3、一小部分更积极的在往“云”上转移他们的存储、备份及数据恢复系统。所有采取实际行动的 CIO 都已体会到了云计算的好处-显著降低了采购/运营成本，大大提高了 IT 服务水平，同时前所未有地感受到了 IT 服务完全按需分配的便捷。

一部分不看好云计算的主要担心“云”的安全隐患：自己的核心数据交由第三方托管，数据的安全及完整怎能得到保证？

剩下的一部分，包括我在内，对云计算持观望态度：“云”的成本模式仍不清晰。例如，当初我们对电邮系统进行了大量投入，如果现在全盘转移到“云”下显然又得重新投入-开销又多大，比我们运维现有系统的成本大多少？一旦知道相差无几，我会立即开始规划迁移。

另外不得而知的是，引入云计算是否令公司每年的合规审查更加复杂。例如，为了应付噩梦一般的萨班斯法案合规内审，我不得不仔细研读并答复常规服务供应商们提供的大量 SAS70 审计报告。如果“云”带给我更多 SAS70 报告，我只有暂对其敬而远之。

总而言之，我们接受新事物的观念越来越强，市场对技术的要求也越来越高。虚拟化的成功，意味着我们开始承认，具体服务不必再与物理服务器联系起来，远程系统的完全控制也并非不可能。因此云计算的出现，我相信不是昙花一现，而是能实实在在改变 IT 现状。

如今，云计算的先行者正在进一步开拓能适应“云”的 IT 服务范畴，“云”供应商也在抓紧攻克和云计算相关的安全、数据管理及定价模型等难关。与此同时，我自己正在尝试将非核心数据的存档转移到“云”存储中，然后我还会考虑用“云”实现远程办公。这些都是能让我们更实际地理解云计算，并在未来更恰当的时机用“云“一步步地实现更多的 IT 服务。

谈了一些对云计算的战略认识，相信自己还是能接受新鲜事物，毕竟还没有那么老。

（作者：Niel Nickolaisen　译者：秦明焓　来源：TechTarget 中国）

关于云计算合规性的四条建议

从理论上看云计算似乎很简单，云部署和许可才是最吸引人的资产。但是，当行动起来问题也接踵而来。你会发现要遵从“云”其实没那么简单，有很多问题需要思考。云规则可谓无处不在，大到政府法规，例如，Sarbanes-Oxley、欧盟数据保护法；小到行业法规，例如，支付卡行业数据安全标准(PCI DSS)和美国健康保险携带以及责任法案(HIPAA)。你可能已经实现了内部掌控，但在公有云基础设施平台或基于云的应用套件迁移的过程中，你不得不放弃对供应商的一些掌控。

这正是今天许多审计员、CIO 和 CEO 面临的一大困扰。他们迫切想知道：怎样在大力发展“云”的同时遵守云规则，避免声誉受损。以下是来自分析师、供应商和顾问的四条建议：

1、注意云对 IT 工作负载的新挑战

当对云供应商进行评估时，寻找鉴定用户身份和访问管理策略;数据保护和应急响应方面提供良好策略的供应商。这些都是最基本的合规要求。然后，一旦你给未来的供应商制定具体的合规要求，就很可能会面临具体的云挑战。

数据定位是其中之一。以欧盟数据保护法为例，这一法案禁止欧盟居民的个人信息外流。为符合法规要求，你的云供应商应该把欧盟客户的信息放在欧洲的服务器上。

多租户和清楚配置同样构成了挑战。公有云供应商使用多租户以便优化服务器工作负载和降低成本。但是，这就意味着你需要和其他企业共享服务器空间。因此，你应该了解你的云供应商提供的保护措施防止向任何妥协。根据数据的关键程度来决定是否加密。以美国健康保险携带和责任法案(HIPPA)为例，要求所有的用户数据设置密码，不管数据是否正在使用。

随着密码身份认证技术越发复杂，为用户清除配置也愈发具有挑战性。不可否认，联合身份管理计划帮助用户更方便地登陆至多个“云”，但也导致配置的清除更为棘手。

“当雇员离开公司，你希望按一下按钮，就可以自动关闭他们的 Windows 帐户和所有企业内部应用程序。同时，你希望雇员的移动电话无权获取企业信息，雇员无权接触企业 SaaS 应用。”身份管理及合规工具提供商 Centrify 总裁 Tom Kemp 表示，目前看来，自动清除配置尚未实现基于云平台和内部部署系统的同时应用。

2、追踪瞬息万变的云标准

不论你喜欢与否，你都是云的早期的使用者。你决定把那些应用程序迁移到云中以及何时迁移它们都会受益于对现在云计算演变的了解。

现在，你可以参照 SAS 70 Type II 和 ISO 27001 两大标准，遵守金融和信息安全方面的政府以及行业法规，但不能担保，这些法规是适合公司发展的。

“ISO 27001 和 SAS 70 的标准是很有帮助的，但可能已经落伍了”美国福雷斯特研究公司的副总裁兼首席分析师 Jonathan Penn 表示，“它们没有对数据安全、身份鉴定、管理员控制等诸如此类事情做出详细的规定。我们必须让用户清楚即将发生的一切。现在它基本上是一个“黑箱”。”

提高对用户的透明的是云安全联盟的重要目标，CSA 公司创办三年来快速在用户、审计师、服务供应商中深受欢迎。云安全联盟的一个重要目标是标准化审计框架和促进用户和云供应商间的沟通。

以现在遵守的法规为例，GRC(监控、风险和合规)标准套件进展顺利，它包含 4 大要素：云信托协议、云审计、共识评估倡议、云控制矩阵。其中，云控制矩阵以电子表格的形式罗列了企业遵守其 IT 控制领域标准须达到的基本要求，例如“人力资源-终止雇佣关系”。而共识评估倡议就用户和审计师对供应商在控制领域的具体期望，提供了一份详尽问卷调查。

在 CSA 等联盟、行业团体、政府机构的共同努力，未来几年内，新标准会层出不穷。CSA 已经与国际标准化组织(ISO)、国际电信联盟(ITU)、美国国家标准和技术协会(NIST)实现正式联盟，以帮助这些组织进一步完善标准。据 Forrester Research 公司报道，截至 2010 年底，已有 48 个行业团体致力于云安全相关标准的研究。

3、认真对待 SLA

不管你的企业规模和状态如何，都不要轻信云供应商的合同条款满足你的要求。一切要从认真尽职检查供应商的合同开始。

这是 Hogan Lovells 律师事务所的一名律师——Michael Larnei 提供的建议。Hogan Lovells 是一家在云合规性及安全问题上具有丰富经验的国际律师事务所。Larner 经常帮助客户就服务水平协议(service level agreements，SLA)与云供应商进行谈判，他表示首先从风险效益分析开始，了解云供应商的标准合同条款是否满足您对合规性的需求。如果不满足合规性要求，就要决定需要与云供应商进行谈判以增加舒适度。

公司的规模能够为谈判增加砝码，但小型公司也能够找到谈判的砝码，那就要小型的公司是云供应商试图拓展新行业。总而言之，在任何情况下都不要害怕和云供应商进行谈判。

Larner 表示“很多公司认为一个大的云供应商不会和他们进行谈判。事实上，你可以提升你的舒适度来让云供应商乐意为你破例的。”

如果你对云不是很了解，不妨以非关键性数据开始，你就会发现这是一个很好的办法。Larner 补充道。

但是严格的评估不应该仅仅以全面的 SLA 结束。RSA 公司的云计算战略总监 Nirav Mehta 表示你应该继续密切关注云供应商。“你可能有一个很好的 SLA，但是如果供应商的云服务中断，业务连续性会发生什么?”

Mehta 认为最好的战略是使用多个云作为备份。

4、优先考虑安全性问题

为了更好的理解企业的潜在风险以及利益，你应该尽可能早地与云安全小组进行讨论，Forrester 公司的 Penn 认为。

“在适当的环境中安全及合规性问题才能提上日程。” Penn 说，“重要的是：企业主管能够理解安全问题而且能够在风险级别与提供的降低某些风险的预算之间进行权衡。”

在向云迁移的过程中，通过安全委员会正式的风险评估功能，为企业提供一个以更持久的方式实现企业安全和企业目标联盟的机会。安全委员会能够帮助评估风险并做出符合企业战略目标的预算建议。

你应该注意众多安全服务及云供应商合作伙伴提供的安全创新。Dome9 是 Amazon 的合作伙伴，它解决云相关的技术问题—当不使用云服务器的 SSH 以及其他端口时，Dome9 就关闭这些端口，这样已经获得访问权限的攻击者就不能登录到云服务器中了。

Dome9 的销售副总裁 Dave Meizlik 说：“在企业中，这些端口默认是打开的。但是当你的云服务器不需要工作时，你希望能够关闭它们。而你不能每次关闭服务器都要求云提供者帮你关闭相应的端口”。

云计算可能带来了某些风险，但是当安全创新迎头赶上后，这些风险自然会减少。即使在今天，根据 Forrester 公司的 Penn 所说，“云服务的安全问题不会像其他 IT 趋势比如智能手机或者社交媒体的蔓延那样，令大多数企业对安全问题感到担忧。从根本上说，对于云应用，安全问题将逐渐减少而不会引起越来越多的关注。”

（来源：TechTarget 中国）

云归档：合规数据的安全很重要

对于存储合规相关的数据而言，云技术显然非常合适。软件即服务（Saas）供应商也将其服务定义为一种更经济的方式，来将很少访问而要求很高安全性和访问控制的数据从主站点存储上分离出来。不过专家提醒，在没有仔细检查第三方服务的情况下，将合规数据通过云归档的方式存放可能会带来风险。

目前有很多不同类型的基于云的服务供应商提供数据归档服务，从公有云存储站点，比如亚马逊的 Simple Storage Service（S3）到专业提供合规数据归档的供应商。

提供合规数据归档的云服务供应商一直在努力平息在数据安全性、可控性和业务稳定性方面的问题。“做这行的人都有一段时间的业务经验，他们知道他们在做什么，”ESG 资深咨询分析师 Brian Baineau 如是说。

不过并不是所有人都深信所有问题都解决了。以下是一份纲要，列出供应商如何缓解应用基于云的合规数据归档时通常会有的顾虑，以及仍然遗留的问题。

云技术中的安全性

许多知名的业务和服务供应商（包括微软在内，其在 2010 年 12 月表示有未经授权的用户从起 BPOS 上下载了数据）都尴尬地对外透露过信息泄露事件，这使得管理员对于云供应商中高度敏感的合规相关数据的物理和虚拟安全性颇具质疑。

“我们正在谈论的是获取这些团体内最为关键的部分数据”George Tziahanas 是法律和合规解决方案的 Autonomy 公司的全球总裁，“这着实是这些公司的命脉，是高度机密的。”

一些供应商定位其符合第 70 号审计标准（SAS70），Type I 或 Type II，作为安全性衡量的标准证明。Gartner 公司的研究副总裁 Jay Heiser 解释了这两者的不同。“SAS70 Type I 由审计从业人员发布，用以证明相应的控制流程足以处理合同中的服务级别要求，”他说。根据 Heiser 的说法，SAS 70 Type II 审计要求审计员到现场检查服务供应商是否遵从了相应的流程。

不过 Heiser 警告表示，SAS 70 审计“并非是一项认证，而是一项证明”其中问题在于审计并非基于任何最佳实践或工业标准；SAS 70 仅仅是审计报告的一种形式。根据 Heiser 的观

点，一项成功的 SAS 70 Type I 审计只意味着服务供应商的过程可以满足其在合约上的承诺。“它不会承诺任何实际服务的质量，”他说道。

Heiser 同时表示，他建议企业在云服务供应商的选取时，在候选公司中至少进行以下四部的调查：

1.准备并通过调查问卷的方式服务供应商的基本服务信息、设备信息和安全措施。Heiser 提到 SharedAssessments.org 和 Cloud Security Alliance (CSA)已经提供了相应的调查问卷供管理员参考使用。

2.检查每家云服务供应商的上游供应商信息。

3.检查所有第三方的证明信息，比如 SAS 70 或 ISO/IEC 27001:2005。

4.到现场去。Heiser 提到服务供应商通常会根据你的业务价值让你访问他们的现场情况。

三家提供基于云服务的服务供应商——Autonomy，Mimecast 和 Symantec 公司——通过高级数据保护技术和加密技术解决用户在安全性方面的顾虑。

Autonomy 管理超过 17PB 的合规相关数据，并且同步地将数据写入多块独立的物理设备中，并可能位于不同位置，采用不同格式。

根据 Mimecast 技术讲师 Orlando Scott-Cowley 的说法，Mimecast 同样将其数据存储在不同的设备上并位于不同的位置，因此即便偷取整块磁盘驱动器或机架也无法取得任何有用的信息。该公司同样采用加密技术保护所有用户数据并未每位用户分配一个 256 位的高级加密标准（AES）密钥。作为进一步的安全措施，Scott-Cowley 说，Mimecast 还为每位用户分配一个用户号，并且为相应的数据标记上该用户号。用户只能查看有一致客户号的数据。

Symantec 则在用户数据传输至数据中心过程中对其加密，并在存放过程中使用一个 256 位的 AES 密钥。

你知道你的数据存放在哪里么？

有一些政府条例对数据可以存放的地点有区域限制。欧盟资料保护纲领（95/46/EC）要求其成员区域在向第三方国家传输数据时，必须确保这些国家可以对个人数据提供“充足的保护级别”。

管理员同样也不喜欢云服务供应商将数据分割在不同的数据中心中，甚至不同国家的数据中心中。Autonomy 的 Tziahanas 说，“这些受到规范约束的公司想到的第一件事情就是必须明确他们的数据到底存放在哪里。”

“通常的云供应商，比如亚马逊和 Google 云和 Autonomy 最大的不同在于，你在特定的一段时间可以明确你的数据到底在哪里，”他补充说道。

Autonomy 和 Symantec 允许潜在用户对其自己进行审计，以确保数据存放在公司宣称的那些地方。Symantec 允许公司制定数据存放的数据中心，并且和该公司关联的邮件账户等也会指向到该数据中心。

从云中检索数据

此外，管理员对于云服务供应商还有的一项顾虑就是快速检索数据的能力。

“从合规或法律的角度讲，任何时候你存放的信息，你都要可以将其取回，”Phil Favaro 是 Symantec 公司一位电子发现方面的律师，他说道。其实受合规约束的公司不仅要求在特定时间段内存储制定的数据，并且当需要内部或政府审计以及电子发现方面需求时，有义务到法庭、合规主题和管理层来快速取回数据和原始数据。

“你是否能够快速浏览你的虚拟文件柜，并在七天之内根据法庭要求找出与之想顺应的资料？”Favaro 问道，“我有这样的一个问题，这非常重要，云供应商是否能够提供这样一种结构，如果没有这样一种结构的话，公司会和法院或监管机构惹上麻烦。”

Ponemon 学院 LLC 安全调查中心近期的一项研究发现合规以及存储非结构化的信息每年平均花费了企业约 210 万元，却无法进行企业智能化的资本管理。

该学院的成立者兼主席，Larry Ponemon 说道，这项研究关注大约 100 家公司的至少 1,000 的 IT 席位，这些人私下都认为云是一项降低合规成本的途径。不过，他提醒将记录放在云端并非是完美的答案。

“我和近 20 家企业谈过，几乎每家企业都提到使用云或管理服务可能会在很大程度上改善这些问题，”Ponemon 说道，“我想云确实是提供这样一种服务，不过，正因为是云，它无法解决这样的问题，谁访问了什么数据，以及为什么。他们只是简单地访问它。”

Ponemon 说很重要的一点是，任何合规应用，云或者内部的，将记录视作文件级别。“其必须是文件级别而非卷级别的，”他说道，“很可能你只需要 1,000 条记录中的一条。”

服务水平协议的重要性

Autonomy 和 Mimecast 通过严格的服务水平协议解决这方面的问题。“当有人听到‘云’这个词时，他们想到了亚马逊和 Google，当他们独到这些恐怖的故事，并且理解他们的数据可能会被从这样一个基础架构上偷走，这完全是他们无法控制的，没有任何服务水平协议保证，”Mimecast 的 Scott-Cowley 说。他说 Mimecast 确保 100%的服务可用性，包括任何时间、地点通过网络界面访问归档后的邮件。

Autonomy 所提供的服务水平协议涵盖了访问，数据多快可以被写入磁盘和目录，多快可以被调取供调查所用，数据可以多快通过政策过滤，以及用户可以多快地通过政策过滤推送出的信息中找到所需资料。“你可以存储每一天的数据，不过假设你没有一个很好的机制来对其进行访问，这些就是完全不相干的信息。”公司的 Tziahanas 说道。

通过严格的服务水平协议，本地化的服务，以及严格的安全性衡量，云数据归档服务市场正在日渐成熟。不过这并不非意味着每家服务供应商会使用相同的工具。“从风险管理角度看，你无法在‘云’前止步不前，”Gartner 的 Heiser 说，“你必须深挖并发现供应商所谓的‘云’究竟是什么。”

这意味着挖掘得更深入一些，在所谓的工业标准安全性审计上更深入一些，可能的话实地考察服务供应商的设备。这一系列的防御措施可以使你在应对法院和监管机构时更为从容不迫。

（作者：Todd Erickson　译者：张瀚文　来源：TechTarget 中国）

云计算规则遵从：可视性是关键

在2011年度RSA会议上，小组成员告诉会议出席者，云提供商的基础设施和安全控制可视性及透明性可能并不清晰，但是对解决云计算的规则遵从问题至关重要。

Dennis Morreau是RSA CTO办公室的高级战略分析师，隶属于EMC公司的安全事业部，他表示："首先需要解决的就是可视性，这可以让你决定在什么情况下应该避免或者缓解云计算的问题。"

Terremark Worldwide公司的首席安全架构师Christopher Day表示，在硬件、管理程序和应用程序级上添加可视性，是供应商和客户应该采取的最重要的一步，"如果你看不到问题，你就无法修复或消灭它。"

然而，思科安全技术事业部云和虚拟化解决方案总监Chris Hoff表示，现有云提供商环境中的可见性和透明性还是不够的，"我们只是被告知不要担心是由什么东西在进行工作。"

例如，当问题涉及到基础设施即服务(IaaS)提供商管理程序上的多租户(multitenant)环境时，Hoff说："我应该怎么信任管理程序？我们总是被告知，只要信任它就可以了。"

英特尔安全解决方案总监Steve Orrin表示，公司需要确定自己的需要，并做好为加强安全而给向云提供商付费的准备。他说："截止到今天，云计算依然必须通过使用案例来推动。"Hoff同意这一观点，并指出："并不是所有的云都相同。"且补充说，检查供应商可以提供的控制很重要。

Day表示，Terremark公司推出了混合云模型，使得用户不必在共享的多租户架构上进行部署。他说："人们认为，IT所包含的全部东西都应该是云。然而云只是提供了交付IT服务的另一种方式。"

在另一个公共云计算规则遵从专门小组中，Rackspace Hosting公司的首席技术官John Engates表示，混合云模型已经帮助很多用户缓解了他们对规则遵从的担心。例如，一个客户在专用机器上保持大型数据库服务器管理数据，并把部分不太敏感的应用程序移动到公共云上。他说，他的公司已经有一个安全小组在与客户进行交流，以确定"适合开展这个任务的工具。"

Engates 补充道：“透明性是关键，我们愿意同你坐下来，讨论清楚我们将要为解决安全性和规则遵从而做的事情。然而这依然取决于用户自己的选择。”

动态云环境引起了安全性和规则遵从的挑战，需要对审计和安全功能进行自动化。Hoff 说：“我们还有很长的路要走……很难指出我们将要如何应对那种灵活性。”

Terremark 公司的 Day 也指出，意识云环境中的威胁是很重要的。他表示：“攻击者已经在云中的某处研究云的复杂性，因为云确实的确非常复杂。”

（作者：Marcia Savage　译者：Sean　来源：TechTarget 中国）

在云计算合同中遵循合规性需求

希望把云计算基础设施用于数据备份和存储的公司，在签订合同之前，需要考虑合规性需求。

据两位市场专家讲，在某些情况下，云供应商能够满足合规性需求——但往往需要付出昂贵的代价。甚至价格谈判开始之前，CIO 们就必须明白云中的数据备份和存储没有取消该公司附加在这些信息上的法律、法规和审计义务等的责任。

CIO 们应该为云供应商准备一份合规性问题清单。但是，不要指望他们的回答满足你的需求。事实上，在上个月，Gartner 公司发表了一份报告。该报告指出，直到 2012 年，安全、隐私和合规性将阻止在受管制性行业和全球性公司采用云计算。

以下是来自 Gartner 企业内容管理分析师 Debra Logan 和 CA 的 GRC 管理套件的产品管理副总裁 Tom McHale 的一些指导方针和建议。

谁有权访问云中的敏感数据？

云中心往往提供 SAS 70 认证和一些审计功能。在云数据中心的安全性（尤其是边界安全）大部分时间是好的。但还需要回答很多人的问题。

McHale 说：“虽然你购买了基础设施，但你仍需要负责：谁有权访问这些应用、谁管理这些应用以及处理这些数据的人员的职责划分。”

公司通常做定期的背景检查，以确保其雇员合格并值得信赖，他们需要看到云供应商遵循什么类型的人事过程。但是，McHale 警告说，除非你是一个非常大的客户，否则，在规定人事政策上，你不会有很多运气：例如，要求每 3 个月做一次药物测试。他说：“你的公司可能有很好的策略。该策略对于处理敏感数据的人是一种很好限制，在这种情况下，这可能是一个挑战。”

数据备份：频率、多久、多好？

CIO 们应该明确他们的系统将被备份的频率，以及当系统不可用时，供应商定期维护的窗口。McHale 说：“备份可能需要五到六个小时。”

一旦确定备份和维护计划，就应该考虑隐私和安全问题：当管理员开始做备份时，他们究竟可以看到什么？难道管理员必须有数据的访问权限？用什么工具确保备份（或副本）并没有备份到CD或拇指驱动（thumb drive）上，而仅仅备份到被认可的系统中？

Gartner的Debra Logan推荐，你要求对基础设施的描述、数据保存的格式、备份磁带会发生什么变化以及您是否可以将特定的保留过程应用到你的数据上。

您将如何管理电子发现（E-discovery）请求并满足不同的保留法规？

公司都受到无数法律或法规的制约，规定他们以何种方式以及必须保存数据多长时间。许多国家——例如，德国和英国——具有电子邮件相关的具体规定。Logan指出，在民事案件中，美国律师必须遵循的民事诉讼法联邦规则（FRCP）要求在案件的早期阶段披露电子存储信息。这些都是供应商必须解决的问题。

Logan建议：“为发现和保护需求的过程、成本以及职责，需要预先进行谈判，并且为维护律师和委托人特权相应的协议也应在一开始就规定。”

Logan列出了协商云计算条款的几个问题：

- 如果我需要保存数据会怎样？
- 如果我需要产生数据，如何做数据收集工作？
- 谁来做呢？
- 假定在得到传票后，可以立即开始“保存”操作，且只允许90至120天用于生产数据，SLA是什么？
- 您的数据中心在哪些管辖区域，以及在这些管辖区域中，如何保护隐私？
- 您如何回应有关您的数据信息的政府要求呢？
- 从托管服务导出数据，可能是什么格式的？
- 你怎么保证满足数据存储的跨境法律限制？

如果贵公司属于一个受到严格监管的行业，Logan认为在未来几年，在云中，你将做许多IT业务。Logan说，如果法律部门正关注公司何时采用云服务，他们将快速刹车。

她说：“早期云服务的采用将极大地受到云提供商未能充分解决安全、隐私和风险担忧的抑制，尤其是在高度管制的产业。”

（作者：Linda Tucci　译者：陈德彦　来源：TechTarget中国）

补偿控制有助于促进云合规

在当前的经济形势下，许多组织面临着成本削减和效率压力，这迫使它们去考虑云资源。虽然云服务有许多特性，如灵活性、低入门成本以及快的市场进入率，这些特性能很好的支持各种业务，但是在考虑转向云时，合规将会是一个难题。因此，云带来的好处与保持合规之间就存在着分歧。

导致这种冲突的一个原因是“云”的定义，即“云”是无处不在，随时随地可接入的。但需要注意的是，即使云服务能在任何地方被访问，但是它并不是无处不在的。事实上，Forrester Research 公司最近发现许多基础设施即服务（IaaS）云仍在使用传统的 IT 外包模式：它们从位于特定地域的特定数据中心提供服务。虽然确实存在真正的全球云（如 Google），但在软件即服务（SaaS）方面，许多供应商最终仍选择使用本地云来提供全球化服务。

那么，为什么云服务的提供方式这么重要呢？有几个原因，首先规章制度会影响云的运作，使用本地化云服务的用户会发现他们的目标与当地的法律法规相冲突。此外，也只有全球云才能提供真正的地理多样性和高可用性。这意味着如果云操作被限制在一个或几个地点，地域多样性和高可用性都将不复存在。

最重要的是，位置很重要；如果你不知道云服务供应商的数据中心在哪里，或者说你的数据在哪里，那你将无法去评估你的数据是否受当地法律法规的约束，而且这些法律法规很有可能与你的数据隐私合规目标相冲突。除了 HIPAA 方面的新 HITECH 法案，美国境内已经很少有法律法规提到对服务提供商的要求。这意味着如果违反了法律法规，那么上法庭的将不是服务提供商。所以，如果你不知道你的数据在哪里存放，那么是时候去找出来了。

在云计算的经济学当中数据和应用是与基础设施相分离的。也正是这样一种概念使得企业在获得巨大的运营和业务效率的同时，出现了安全和合规性的问题。与其坐等云计算行业对法律合规性提供支持，安全专家们不如把眼光放的比他们的供应商更远些，通过寻找补偿控制措施来帮助云合规。下面有一些补偿控制措施供参考：

- **尽可能频繁地清理或匿名化私有数据**：并非所有的数据都需要以明文的形式存储在云中。清理或匿名化私有数据也许是实现隐私控制最经济的方式；因此请把这个方法作为第一选择。

- **使用独立于云的加密手段**：在实施基于 IaaS 的 HIPAA 时，加密技术可以用于保护云之外的数据和应用程序。客户对密钥妥善保管，使用可以对虚拟机或数据进行云内加密的新兴技术可以大大增强数据保护力度。

- **为更高机密数据支付更多费用**：如果供应商当前并没有提供特殊的控制措施来满足法律法规方面的要求，那么我们需要与他们共同努力来尽可能的获得这些控制措施。有时仅仅需要多支付一些费用就可以满足这些需要。可以向供应商指出实施这些附加的控制措施可以使他们从其他客户手中获得额外的收入，以及增加他们在市场中的竞争力。

- **使用托管的私有云**：托管的私有云是一套专用的云基础设施；换句话说，它是一种实用定价模式，通过标准的 Internet 协议来访问，并且能自动分配由第三方托管的工作负载。由于基础设施是专供你的组织使用，所以你可以选择推行严格的安全和私密政策，甚至可以让审核人员对其进行合规审查。托管的私有云在建设前期的投入会比公共云大很多，但随之而来的是低的运营成本以及更好的控制。

无论通过何种方法去控制，安全专家们最终应当承担起对云合规的责任。从长远来看，合规性和高效性将成为云服务行业的评判标准，并且很有可能成为企业采用的推动力。为什么？因为云服务可以将合规支持的成本平摊给多个客户，同时可以利用这部分额外的投入来提供更高效的服务。

（作者：Chenxi Wang 译者：Rick Lee 来源：TechTarget 中国）

云成熟度模型帮助中小企业判断云服务提供商的安全

几乎在每个关于云计算的调查中，公司对采用基于云的技术犹豫不决的众多原因中，安全都排名靠前。并且确实如此，如果无法确定你的数据会被如何对待，以及是否得到充分地保护，那么盲目地采用云服务就只是有勇无谋的行为，即使云服务在经济上的利益看起来十分诱人。

那么，企业怎样才能证实云服务提供商是否达标准？大型公司和政府部门或许有影响力来要求对云提供商的场所和流程进行详细的考察。然而，小公司们可能就不太受欢迎了。

最值得人注意的是来自于云安全联盟（Cloud Security Alliance，CSA）的几个倡议，已经在设法帮助企业至少商定出正确的问题来询问预期的服务提供商，但这可能仍是一项缓慢且艰巨的任务。并且正如我们已经注意到的，小型企业向大型的云服务提供商提交问卷只能期望很少的合作，更别提得到回答了。

但希望可能就在眼前。一个用于给云服务公司评分的新的云成熟度模型承诺为企业提供简单的指导，针对云服务公司提供的安全水平，给预期的买方及卖方都带来了好处，后者现在只需要经历一次审计过程，而用为每个顾客都进行一次。

所谓的通用保障成熟度模型（Common Assurance Maturity Model，CAMM）是 Raj Samani 的思想结晶，他是安全界的一名老手，曾经作为顾问在公共部门工作，现在是 McAfee 公司的欧洲 CTO。

CAMM 的形成

Samani 已经从一家大型企业早期的项目中了解到，要和大量的供应商打交道是多么的困难。他恰好没有资源或财力来执行必须的检查，以确保他们正在照看着这些信息，这些是数据保护法案背景下他所要负责的信息。

然而，在和他的父亲、伦敦中心的一家旅馆拥有人的谈话中他找到了解决方案："我的父亲正在抱怨那些想对旅馆进行详细检查的令人棘手的顾客，他说这会引起很大的麻烦"，

Samani 说道。“他的回答是这是一家一星级的旅馆，意味着它不是豪华而是廉价的。这就是所有那些顾客们需要知道的”。

这个事件孕育了类似的五星评分系统，后者可能应用在云计算服务上。Samani 意识到如果该系统被广泛采用的话，不仅会让云计算服务的顾客们更容易找到恰当的安全级别及服务，同时也缓解了提供商们所经历的无尽的顾客审计。

这是两年前的事情，并且从那以后来自各种支持组织的志愿者们组成的团队一直在努力着，但如果 CAMM 有一些全职的工作人员帮助时，这种状况会很快得到改变。Samani 表示，他将在二月的旧金山 CSA 峰会上宣布关于招聘计划的完整细节。

CAMM 组件

Samani 说，CAMM 模型目的在于涵盖关于安全的基线控制，但已被设计和其它标准如 ISO27001、COBIT 及 PCI DSS 进行交叉映射，因为顾客们对这些标准有特定的需要。

“CAMM 模型提供控制的基线级别，然后你可以在上面添加不同的模块”，Samani 说道。“这意味着人们能为他们要求的安全级别进行支付。所以如果现在你需要在德国找到一家带有 PCI 模块的级别为 3 的提供商，CAMM 让找到这家公司变得更容易了”。

Samani 表示，CAMM 模型的重要方面之一，是用于执行审计的工具和知识产权框架对任何人都是免费的。“它是爱心的劳动成果”，他补充道。

公司开始使用 CAMM 模型时唯一需要付费的组件是第三方保障中心（Third Party Assurance Centre，TPAC）。TPAC 是关于服务提供商的信息仓库，列出他们根据一系列衡量标准得到的安全级别。TPAC 将作为一个市场，旨在为顾客和提供商提供交流。顾客们会上传他们的要求，列出 CAMM 级别加上任他们需要的何其它模块，TPAC 将立刻呈现符合他们要求的供应商的简短列表。

Samani 补充道，CAMM 模型会有助于安全经理们根据他们的老板能理解的东西来量化残余风险。“你走到 CEO 面前并且说，‘我们打算寻找一家级别为 3 级的公司但是那会留下一些风险’”，Samani 说道。“CEO 接着会询问找一家 4 或 5 级的公司要花费多少钱，然后在理解风险后做出判断。因为这种时候，你不能有同业务主管谈论安全的那种谈话”。

最近 CAMM 模型经历了有四个试用用户的 alpha 测试，一旦来自这些测试的反馈结果在二月份得到"消化"，在年底大规模启动前会进行一系列 beta 测试。

该项目得到 150 个组织的支持包括大型云服务提供商、政府团体以及行业团体诸如 CSA 和 ISACA（信息系统审计与控制协会）。

对 CAMM 模型的反应

CAMM 方法被普遍视为一个有价值和有前途的方法。Paul Simmonds 谈到 CAMM 发挥了极具价值的作用，他是国际组织 Jericho Forum 的董事会成员、CSA 的安全指导 V3 版本的合著者。

"CAMM 模型已非常深思熟虑，我对此印象十分深刻"，Simmonds 说道。"该模型在它的领域内是模块化的，因此作为云服务的用户，你能明确要求在不同的区域需要什么级别的安全。CAMM 使得更容易找到潜在供应商的简短列表，并且它会继续发展为大多数公司可以自我管理的更为完善和彻底的审计方法"。

该倡议还得到了来自欧洲的有力支持，其中包括欧洲网络及信息安全机构（ENISA）的督导委员会。"我们坚信 CAMM 模型是帮助云计算起飞的关键所在"，ENISA 在希腊 Crete 岛的安全服务项目经理 Giles Hogben 谈道。

不过 Hogben 提醒注意，任何新的标准应该避免给公司增加额外的费用。他补充道，按照 1 到 5 的范围来衡量成熟度"可能导致过度简化"，因此必须小心处理。

（作者：Ron Condon　译者：Odyssey　来源：TechTarget 中国）