云经纪师培训教程

中级云经纪师

韩景倜　何　杰　主　编
刘　涛　于长锐　梁贺君　陈逸群　副主编

上海财经大学出版社

云经纪师培训教程

中级云经纪师

韩景倜　何　杰　主　编

刘　涛　于长锐
梁贺君　陈逸群　副主编

上海财经大学出版社

图书在版编目(CIP)数据

中级云经纪师/韩景倜，何杰主编．—上海：上海财经大学出版社，2015.1
（云经纪师培训教程）
ISBN 978-7-5642-2083-9/F·2083

Ⅰ.①中… Ⅱ.①韩… ②何… Ⅲ.①信息服务业-经纪人-培训-教材
Ⅳ.①F719

中国版本图书馆 CIP 数据核字(2014)第 300155 号

□ 责任编辑　汝　涛
□ 封面设计　张克瑶
□ 责任校对　林佳依　卓　妍

ZHONGJI YUN JINGJISHI

中级云经纪师

韩景倜　何　杰　主　编
刘　涛　于长锐　梁贺君　陈逸群　副主编

上海财经大学出版社出版发行
（上海市武东路 321 号乙　邮编 200434）
网　　址：http://www.sufep.com
电子邮箱：webmaster @ sufep.com
全国新华书店经销
上海华教印务有限公司印刷装订
2015 年 1 月第 1 版　2015 年 1 月第 1 次印刷

787mm×1092mm　1/16　19.5 印张　474 千字
印数：0 001—3 500　定价：46.00 元

云经纪师培训教程
编写委员会

主　编　　韩景倜　何　杰

副主编　　刘　涛　于长锐
梁贺君　陈逸群

编写组成员
（按姓氏笔画排序）

石　云　付佳蕊
边　珅　关　欣
华　斌　刘　蕾
李馨楠　张　盛
张馨月　陈　群
陈宇中　陈虹宇
严伟江　罗晓兰
杨夏燕　曹　宇
管俞洁

总　序

随着计算机技术与通信技术的发展与融合，计算机互联网方兴未艾，给现代社会带来了巨大的变化。特别是进入21世纪以来，互联网已经成为人类社会生活不可或缺的基础设施。这种数字化、网络化的发展趋势在催生各种计算机应用新技术的同时，也发展和丰富了各行业的业务形态，并对相关经营模式具有颠覆之势。

互联网领域活跃的创造力，吸引着人们的关注。在这里，技术的竞争和淘汰非常激烈，极大地缩短了技术概念的生命周期，一些技术风行几年甚至几个月后就不知所踪，被新的技术概念与模式所替代；而有一些技术在市场的检验下因其具有良好的基因与发展空间而存活，云计算就是其中的佼佼者。云计算非但没有消失，反而有越来越多的软硬件公司加入云计算产业中。

考察计算机网络的发展史，我们会发现，生存下来的一些主流的技术标准，一开始是为了特定的目的而以极为简化的技术来实现的，如以太网、TCP/IP协议。虽然在技术上它们存在一些缺陷，之后推出了不少的网络技术和标准化的OSI协议，希望以此来完善或者取代它们，不过因为技术方面的复杂性而使得推行的范围始终有限。云计算属于市场先行的技术，在技术规范还没有制定出来之前，各大公司已经在推出自己的云计算商用产品了。从这个意义上看，云计算也会与IP技术一样，先占有市场，然后获得学术界的承认。

在这个背景下，云计算已经成为各行业认真对待的互联网的下一个关键应用，纷纷积极投入财力、物力和人力来跟上这个潮流。云经纪师应运而生，其作为第三方咨询服务商为用户进行IT应用现状、组织结构和业务流程等方面的信息化需求分析，例如，帮助用户在中亚云交易平台或线下选择合适的云计算提供商。

就云计算市场现状来看，尽管云计算产业发展迅猛，但在云计算提供商和用户之间，由于缺少有效的对接，市场需求“瓶颈”仍未被有效突破。按照一般的市场原则，用户潜在的计算和存储需求需通过专业的从业人员去挖掘，这就需要云经纪师，云经纪师是云产业的“润滑剂”，在行业中肩负着促进买方和卖方沟通的职能。

在本系列丛书的编写过程中，我们参阅了国内外大量的文献和资料，其中信息明确的已列于参考文献中，而信息不全、无法详细查证其出处的，未能一一列出，在此，向所有在本系列丛书编写过程中所帮助的国内外专家和学者致以真诚的谢意！

本系列丛书为云经纪从业人员提供了一套完整的云经纪师培训教材，包括《云经纪基础知识》、《助理云经纪师》、《中级云经纪师》、《高级云经纪师》。本系列丛书是国内第一套系统的云经纪师培训教材，但由于编者水平所限，加上时间仓促，书中一定存有不足之处，恳请读者批评、指正。

编　者

2014 年 11 月于上海财经大学

目　录

第一章
云的商业价值

学习要点

1.了解云计算的商业推手

2.了解云的商业影响

第一节　云计算的商业推手

现今，云计算(Cloud Computing)已不仅是国际IT业界热炒的概念，而且已经开始在中国落地生根。通过长期对中国服务器市场的跟踪研究，以及对云计算的密切关注，综合各方面因素考虑，我们认为云计算在中国具有广阔的市场空间，但前提是需要有更多的市场参与者投入云计算的运营中。

与其说云计算是一项新技术，倒不如说它是一项在业务模式方面的创新。从技术角度来讲，云计算由一系列新技术组合而成。它由分布式计算、网格计算等技术发展而来，并融合了近年来的热点技术(如虚拟化、Web 2.0等)。从本质上来讲，云计算实际上是服务器虚拟化技术和基础架构(即服务)(Infrastructure as a Service，IaaS)两者的结合，并辅以其他技术。其核心是将某一或某几个数据中心的计算资源虚拟化之后，向用户提供以租用计算资源(Computing Resource)为形式的服务。而这种提供计算资源的服务实际上并不是新技术，而是业务模式上的创新。云计算业务在中国市场具有巨大的发展潜力，越来越多的IT供应商将中国作为云计算业务发展的热点区域。目前，云计算业务的发展也印证了这一点。

通过对云计算产业链的深入分析，对云计算产生影响的主要环节包括最终用户、供应商(包括硬件设备厂商和云计算解决方案提供商)以及云计算业务的运营机构。

在最终用户方面，中国拥有世界上数量最多的中小企业，这些企业的业务正随着中国经济的高速增长而快速发展。对于正处于成长期的中小企业而言，自己投资建立计算中心的投资回报率较低，并且很难与业务的快速成长相匹配。而云计算的租用模式刚好为这些中小企业提供了合适的解决方案。同时，中国未来将承办的亚运会等一系列大型活动，也可以借用云计算模式来提供伸缩性的IT基础架构，并进一步节省成本。云计算对于计算资源更有效率的利用，也使其在节省能耗方面成为“绿色IT”技术的代表之一，这又与中国政府“节能、减排”的政策相符。因此，中国市场上最终用户对于云计算的需求将成为其在未来几年中高速发展的基石。

从IT供应商角度来说，众多的服务器、存储硬件厂商以及平台软件厂商都希望通过云计算平台将自己的产品推广到发展中的中小企业中，并将其IT环境锁定在自己的平台上，以便在这些企业发展到一定规模后能够获得更多的市场机会。因此，IT供应商对于云计算市场，尤其是中国的云计算市场也表现得异常热心。

云计算运营商是目前国内云计算产业链中最薄弱的一环。政府及其下属的企事业单位是国内云计算运营的主体，主要面对公共计算领域。这种由政府机构主导的运营模式将在云计算业务发展的初期成为主要模式，但是未来还将会有更多的企业投入到该业务的运营中去。国内更多类型的云计算运营商的发展，将会成为推动中国云计算市场发展的决定性因素。电信运营商和大型互联网公司都具有成为云计算运营商的潜力。这些企业都拥有大型的数据中心，但这些数据中心并不都是7×24小时满负荷运转。这些数据中心的计算资源可以在空闲时打包成云计算虚拟机，为用户提供服务。这种对计算资源的进一步开发将成为这些企业新的盈利点。当前迅速发展的IT环境与20世纪初迅速崛起的商业环境有着很多联系，许多业务原来是通过维护自己的封闭系统完成的，这样既需要设备又需要专人来操纵，效率很低。解决方案就是让当地的电信公司或者其他的服务供应商来管理远程通信，提高资源的利用率。

如今云计算的商业推手也正是把IT技术引入商业领域的推手，云计算在众多方面给组织带来了核心的竞争力，如成本、效率、组织灵活性等。关于云计算的商业价值，企业界和IT业众说纷纭，但可以肯定的是，云计算正在改变我们的商业社会图谱。云计算让大企业变成“快公司”和“轻公司”，让小企业可以轻松实现“国际化”，可以尝试以前只有大企业才能问津的超级计算力和数以百万美元计的企业级应用。云计算让企业能够更快对市场环境变化作出反应，实现前所未有的业务灵活性，这一切都拜强大而富有弹性的云计算所赐。

一、降低开支和提高效率

为什么云计算可以节约成本呢？总的来说，这是因为经济的规模性(scalability)。经济的规模性指的是存在这样一种关系：每增加一单位成本投入带来的产量增加的量。产品的规模经济递增促使扩张固定成本的数量会带来单位成本的递减。在云计算中，通过资源的共享实现了经济的规模性。一个云服务的提供商把成本分摊到整个客户群中，使得每个客户相对于自己付同样的成本而言，都可以得到相对更丰富的IT功能。

通过云计算，最初购买新硬件用来建立IT项目或扩展容量的费用就节省下来了，组织只需要付它们用在软件商上的使用费，这些软件在组织使用前服务的供应商就已经购买好了，同样地，当它们不再需要或者要整个放弃某些服务时，也不用担心沉没成本的问题。

组织使用公用的云服务可以把IT费用从资本费用转向了操作费用，这可以带来更多的税收优惠。组织使用内部私有的云可以减少资本费用的根本原因在于基础设施的使用效率得到了提高。如表1—1所示。

表 1—1　　资本费用与操作费用

	资本费用	操作费用
定义	资本费用是与固定资产相关的费用，既包括原始的购买设施的费用，也包括近期用以改善设施的费用。如用于计算的实际设备和软件等的费用。	操作费用指的是与商业总体运营相关的成本。如技术工人的薪酬、网络成本、软件使用权的购买成本等费用。
差异	资本费用的价值要延续到税收年，而操作费用在税收年限是被完全用掉的，整个的价值也要被减去。	

经济的规模性也称为弹力(flexibility)或弹性(elasticity)，它是云计算中的一个关键特征。它可以使客户提高或者降低计算资源，如存储、计算能力、网络动态的带宽和其他基于用户需求并愿意购买的数量。规模性既可以是垂直的也可以是水平的。垂直的也即纵向的，包括给一个节点增加资源，如存储卡、处理器或者多余的组件；水平的也即横向的，包括对分布的系统增加更多的节点，这个概念如图 1—1 所示，垂直规模性(vertical scaling)和水平规模性(horizontal scaling)都可以用来判断性能问题和可用性问题，这个还被称为对角线的规模性。

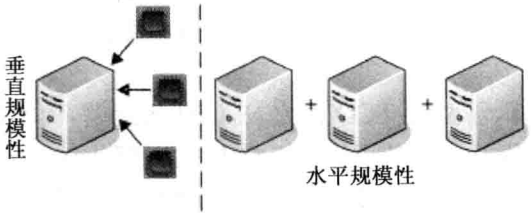

图 1—1　垂直规模性和水平规模性

这种能力可以通过不连续的资源需求显著减少组织的成本，例如，那些线上的零售商在节假日前看到网站的“交通拥堵”情况严重，又或者软件开发公司需要定期提供大规模的测试环境。

现在存在这样一个问题：为什么花费数亿美元购买资产，不但承担运营这些资产的责任，还要部署相应的人力资源(技术评估、供应商关系、容量规划等)，会被认为比直接享受外部供应商(负责所有运营职责)提供的资产更具吸引力呢？另一个可能出现的噩梦就是基础设施和运营团队将不再参与云计算运营，转而由应用程序团队负责直接与外部供应商沟通，基础设施和运营团队将继续负责不断被云计算“吞噬”的企业内部所需的固有资产。

关于云计算的成本问题有各种激烈的讨论，主要围绕资本开支和运营开支方面。然而，围绕这个主题的大多数讨论没有完全理解不同资金模式的深远含义，以及其对 IT 应用程序未来的影响。

实际上，这些讨论都是为了确定运营应用程序的最佳办法，因为应用程序是 IT 创造所有价值的所在。以下是目前关于资本开支和运营开支的讨论未能理解的对资金模式的思考和影响。

(一)运营开支应该比资本开支更昂贵

运营开支模式的好处之一就是不存在长期的约束。用户一旦用完资源，就可以将资源

归还给供应商，供应商拥有对资源的所有权，也就是说，供应商需要想办法如何充分有效地利用资源保证其经济利益。

没有长期约束当然是有经济效益的，因为用户不需要进行巨额的长期投资。所以这也是很合理的，也就是说，从每计量单位来看，运营开支应该比资本开支更昂贵。我们可以看看汽车租赁的价格，其实我们只是为短期使用资源而支付了额外的费用。既然是短期使用，租一辆汽车肯定比花大价钱买一辆汽车更划算。

（二）如何计算

因此，真正的问题并不是哪个选择为每计量单位支付费用更多，而是哪个选择对于资源的总用量更便宜（或者说，运营应用程序所使用的所有资源的总用量），这种计算比每单位的费用计算更加棘手。

首先，这种计算需要预测某段时间（通常是一个月）的总使用情况。换句话说，这个应用程序每个月会运营多少个小时？它会使用多少存储量？会有多少网络流量？

其次，这种计算可能要考虑根据使用层来改变租赁费率。如果总存储使用的是 10 千兆，千兆存储属于某个费率水平，而如果总存储使用的是 10 万兆将会更加便宜。

最后，这种计算还需要考虑不同的使用模式，如某些时期的低使用率和其他时候的高使用率。例如，金融服务公司的应用程序可能会有每月高峰期、每季度高峰期和每年高峰期，更别提受非周期性事件影响的不可预测的高峰期，例如修改法律——改变某些种类金融产品对消费者的吸引力。

对于这种棘手的计算，需要与 TCO 作比较，O 代表运营，而不是所有权。对于很多使用模式，有可能租赁模式要比累计使用模式更具吸引力，即使每计量单位更昂贵。再拿汽车租赁来举例，即使每天租车的价格要比购买汽车的价格高，如果一个月只有五天要使用汽车，那么租车肯定更加便宜。

那么，也就是说，考虑到不同使用情况以及与资产租赁模式相关的不同成本，经济评估应该会更加复杂。当然，无论使用模式如何不同，资产所有权模式的成本都是一样，无论是每天使用还是每月使用都不超过一小时。

（三）影响运营开支和资本开支的其他阻力因素

当然，还存在影响这个计算的其他因素。租用一辆车会根据时间及里程来收费，并且你需要走租赁流程、听取对额外保险的讲解、检查汽车状况。如果一个人一个月有八天需要使用汽车，那么租车还算划算。不过有时候，人们反复听到这样的话后可能还是会选择买车，“你打算如何处理这辆车的保险问题？我们的顶级服务可以让你不必支付这些费用”等。

换句话说，这些阻力因素可能会让你改变你的选择。诺贝尔经济学奖获得者 Ronald Coase 将汽车租赁所表示的开销描述为“交易成本”：与经济交易相关的费用，增加了这个选择的额外负担。

在 IT 应用程序方面，通常会存在更多这样的因素使企业启动应用程序后，尽量避免触碰它们。对于租赁模式而言，“简单设置后就放下不管”的方法从经济角度来看并不是好办法。

在租赁模式中，当用户想要评估资产使用时，很明显应该尽可能减少使用。Forrester 研究所云分析师 James Staten 将这个方法描述为“满足最低使用需求”：人们应该尽可能减少应用程序的资源，只要其功能和性能要求得到满足即可。如果没有使用需求，应用程序应

该关闭，当重新需要时再次开启。

然而，涉及资源管理的这些阻力因素太多了，大多数 IT 团队在进行运营开支和资本开支的讨论时，都会假设应用程序高峰负载时需要的最高量资源的完全使用，然后以这个作为基础来评估资产租赁模式和资产所有权模式。这样计算根本不合理。事实上，大部分企业通常甚至没有考虑其他选择，因为选择不同的运作模式并不会消除这些摩擦因素。

（四）资本开支和运营开支的未来发展

在适当管理的云环境中，这种阻力因素正在减少。我们可以使用工具来推动自动化资源的实例化及终止，甚至应用程序本身可以进行自动化管理这个过程，并不需要人工干预。在这种环境中，“交易成本”要比“满足最低使用需求”更加可行。

总体而言，降低运营交易成本意味着应用程序运营模式需要随着时间的推移而进行转变。反过来说，这意味着随着 IT 企业开始重新评估应用程序资源消费模式，财务分析将需要改变。很多应用程序设计将转向资源的一定基础水平的连续运营，以及改变使用模式而增加和减少额外的资源。最终的结果可能会让这个临界点计算转向资产运营模式，而不是资产所有权模式。

至少，这将避免假设全时间高峰负载资源运营的计算，从而避免错误地确定资产所有权模式是最可行的办法。

二、通过经济规模性来提高安全

在这一部分，我们首先要理解安全与风险、私有性、合规性等概念，再把这些具体应用于云计算中。

（一）理解安全与风险

讨论云计算的安全与风险之前，我们要对安全与风险的概念有所了解。尽管在商业中有很多种类型的风险，本章中所提到的主要指的是信息风险。

（二）信息安全的主要原则

1. 保密性

保密性指数据的敏感性。机密数据需要避免受到未授权的读取、使用或泄露。机密信息的例子包括人事档案、个人健康信息、财务记录和商业机密等。

2. 完整性

完整性指数据的可靠性。要有完整性，数据需要被保护不受未授权的修改。

3. 可得性

可得性指数据的可获得性。要拥有可得性，数据需要被保护，不受服务中断影响。

（三）安全控制

通过应用安全控制措施，可以达到保护组织数据的保密性、完整性和可得性的目的。这些措施被设计用来防止、探测和最小化安全事故的影响。安全控制可以被分为管理、技术或操作三类。要实施成功的信息安全管理系统（ISMS），这三类都不可缺少。本章稍后将详细讨论 ISMS。安全控制的三种类别如下：

1. 管理控制

管理控制包括方针、标准和措施。它们与组织的目的和监管要求保持一致，且提供了操作流程的框架。

2. 技术控制

技术控制是指那些直接应用于信息技术资源或直接由其实施的控制。例如，包括接口管理、身份验证、防火墙和加密措施。

3. 操作控制

操作控制一般包括个人实施的过程或步骤。它们基于管理控制之上，且包含了技术控制。例如，包括灾后恢复计划、配置管理、事故响应和实体安全。

此外，同样必需的(甚至是关键的)是上级管理的支持。技术控制可以由 IT 人员实施、监管人员可以实行操作控制，但管理控制必须来自组织的高级管理层。他们有责任制定有利于实现商业目标的制度，并据此分配资源。

(四)纵深防御

安全的另一个关键概念是纵深防御。这是指使用分层框架来实施对计算机设备、网络边界、主机(服务器、工作站、笔记本电脑等)、应用和数据的安全控制。纵深防御经常被用于实体安全，如银行的安保。正如银行不能通过简单锁上门来保护它的资产，敏感或关键数据不能只用一个网络防火墙或一个密码来保护。

(五)风险管理基础

风险是概率(可能性)和冲击(损失)的要素，具体来讲，是指一个特定事件发生的概率，以及当它发生时对业务的影响。事件包括但不限于：设备的盗窃或丢失、未授权的数据读取、拒绝服务以及未授权的数据操作。本书将不对风险管理做深入的讨论，但对这一过程的简要概述如下：

第一步：识别资产并将其归类。这是从实体或逻辑上识别资产，包括硬件、软件、数据、虚拟主机和其他任何信息资源。在库存过程中，所有者和托管者应该被分辨出来，信息系统和数据应该按照敏感性和重要性等级归类。这一步也可能牵涉到根据监管和安全政策确定合适的控制措施。

第二步：识别威胁和弱点。威胁指任何有潜在可能对信息系统造成负面影响，并因此影响其支持的商业过程的事物。威胁可能是人、环境、或是电子的威胁。人的威胁包含黑客，以及有相同登录凭证的员工。环境威胁包含火灾、水灾、停电或极端天气。电子威胁包含病毒、软件故障或自动式攻击。

对于每个识别的威胁，都有与之相关的系统弱点。有些弱点，如软件的漏洞，能够被很快发现。其他的一些弱点可能是行业或组织所特有的，甚至是主机或数据集所特有的。

第三步：评估风险。要评估风险，需要评估威胁变成真的安全事件的概率，以及如果发生的话所带来的冲击。估算概率的一种方法是看是否有合适的安全控制措施。例如，如果所有主机都安装了防病毒软件、及时更新、定期扫描，病毒爆发的概率就被显著降低了。冲击大小，如名誉、资金、销售、雇员工作效率或设备的损失，应由管理层决定。

接下来，概率和冲击都被分配为高、中、低三个等级，并可以通过矩阵得到一个风险评级。

第四步：应对风险。风险通常依重要性高低处理。组织可能选择承担风险不做任何事、终止风险行为以规避风险、应用安全控制措施减轻风险、通过保险或外包转移风险。这些决定基于商业需要和组织的风险偏好，即组织愿意承担的风险数量。

尽管通过外包可以转移一些风险，但不可能转移所有风险，也不可能转移法律责任。例

如，一个组织可以选择通过承包给第三方数据中心来转移计算设备遭到盗窃的风险。如果设备从数据中心被窃，组织可以成功地规避了这个风险。另外，如果设备遭窃导致了数据破坏，违反了组织的合同或法律监管要求，组织将承担这个责任。

第五步：监控风险。监控是为了确保缓和措施（或其他风险管理决定）是有效的。

受法律或行业监管的组织一般会被要求进行某种形式的风险管理活动。即使是那些没有要求的，也能从中受益匪浅。通过阅读被广泛认可的风险管理标准（如下面这些），可以获得关于风险管理的更多信息。这些广泛认可的风险管理标准包括：ISO/IEC 31000——风险管理标准；NIST 特别出版 800-37，将风险管理框架应用于联邦信息系统指南；COSO 企业风险管理综合框架。

（六）回顾安全标准

标准是指订立好的规则、原则和要求的集合——一个被认可的模型。有许多被广泛认可的信息安全标准，有些是免费可得的，有些是商业化的。组织选择采用哪一种信息安全标准，取决于组织的行业、部门或商业需要。在选择云服务提供商时，组织应该使自己熟悉多种标准，以确保提供商遵循的标准与组织的一致。

1. 审计准则公告第 70 条（SAS70）

SAS70 是一个审计准则，包含信息技术控制和安保。需要说明的是，通过 SAS70 的审计并不能保证提供商提供的云服务是安全的，只能说明它可确认的控制措施是否符合规定。

2. 较为熟知的信息安全标准

（1）信息安全 COBIT5。COBIT 是 ISACA 维护的一个 IT 管理框架。其第五版包含了来自其他 ISACA 框架（如 Val IT、Risk IT、IT Assurance）的企业信息安全的指导。

（2）ISO/IEC 27000 系列。这是一个信息安全管理标准的集合，由国际标准化组织（ISO）和国际电工委员会（IEC）发布。

（3）NIST 特殊发布 800 系列。NIST 在它的特殊发布 800 系列中发布了很多健全的信息与计算机安全相关的标准。尽管主要是为美国政府机构制定的，但是这些标准（有一些例外）基本上可以适用于有类似安全要求的组织，在有些情况下直接对应 ISO/IEC 的标准。另外，NIST 有三个与云计算相关的特殊发布：SP 800-144：公有云计算安全和隐私指导。SP 800-145：NIST 对云计算的定义。SP 800-146：云计算提要和推荐。

3. 开放安全架构（OSA）

OSA 是一个开源项目，以图案形式（图形和解释性文字）提供安全标准。它吸取了其他被认可的标准，如 NIST 特殊发布 800-53 对联邦信息系统和组织的推荐安全控制。它的云计算图案（SP-011）指出了云计算的关键控制领域和活动。

4. 支付卡行业数据安全标准（PCI-DSS）

PCI-DSS 是一个由 PCI 安全标准委员会维护的安全框架，用来保护卡片持有人的数据。其包含网络、数据保护、脆弱性管理、访问控制、监测和政策方面的安全要求，还包含了对云计算使用的共享主机的特殊要求：数据和过程分离、日志和审计跟踪、及时的法律调查。

一个相关的标准如支付应用数据安全标准（PA-DSS）适用于开发支付应用的软件提供商。寻求使用云端支付应用的组织应确保这些应用遵循上述标准。

信息安全的良好实践标准由信息安全论坛（ISF）维护，与本章讨论的其他信息安全标准非常一致。它每年更新，最新版本包含了对云计算的覆盖。

5. 常见的安全风险和规避方法

传统计算的基础风险也会发生在云计算中，但云计算有其自身的特定风险，这与部署模式无关。无论是公有和私有，云都需要某种类型的跨边界安全，不管它是公有云中顾客间的边界，还是公有云中组织各个部门的边界。另外，云计算在一个共享责任模型上操作，组织和提供商都有各自的安全责任。

(1)CSA 安全、信任和保证登记。云安全联盟(CSA)是一个推广使用安全最优实践的非营利组织。CSA 安全、信任和保证登记(STAR)是一个云计算提供商提供的安全控制的登记，用来协助云服务使用者对现有或潜在的提供商进行安全评估。

(2)外围防卫。在研究特定的风险和规避方法前，有一些外围防卫可以在实施时应用于云计算：

①防火墙。防火墙是一个装置或应用，基于一个参数化规则的集合来检测和监管网络流量，例如，允许或阻断特定网络接口或流向/来自特定主机的流量。它通过检查数据包来识别其来源、目的地和(有些时候)装载内容，然后将这些信息与规则比较。云计算环境使用的防火墙设备有能力根据顾客需要进行调整，非常可靠，拥有充分的网络连接和电源，一般比传统防火墙更加稳健。

②状态包过滤。防火墙根据现有的规则去分析流入和流出的流量。它也记录访问状态，以能确保流入的数据包是网络内部所要求的。

③无状态数据包过滤。防火墙分析数据包，根据现有规则允许或拒绝其访问系统。访问状态没有像状态包过滤那样被维持，这使无状态数据包过滤可以用来控制对系统的访问，常见例子包括在 80 接口(HTTP)或 21 接口(FTP)阻止流入流量。

④虚拟防火墙。虚拟防火墙被设计用来保护虚拟主机，运行模式取决于部署方式。在桥接模型中，虚拟防火墙部署在网络设施内部，扮演传统防火墙的角色。在 hypervisor 模型中，虚拟防火墙不在网络内，而是在 hypervisor 环境中，以直接监控虚拟机流量。

⑤虚拟私有网络。虚拟私有网络(VPN)是使用一个公共网络(也就是互联网)或者另一个中介网络的安全私有网络。VPN 通信通过 IP 通道被孤立于网络其他部分之外，通过加密和认证确保其安全。在云计算中，这允许终端用户安全地访问云资源，无论他们的位置在哪里，只要他们有合适的凭证，并且使用一台支持 VPN 客户端的设备就可以访问。当调查 VPN 解决方案时，组织应该识别在使用的设备以确保兼容。

⑥应用界面。客户通过软件来与云服务提供商进行交互，这些软件被称为应用程序编程接口(API)。如果 API 没有被妥善保护，它可能会影响 CIA 的全部三要素：数据可能被泄露或修改，服务和账户可能被关闭或劫持。API 可能因为编程缺陷、数据(包含登录凭证)明文传输或者无效的检测能力导致的弱点而变得不安全。

⑦规避方法。针对 API 的弱点的解决方法一般是提供商的责任，包含安全的应用开发测试。当 API 互相交互时，足够的测试特别重要。一些责任是共享的，如认证和访问管理(后文有详细讨论)以及信号的加密。如果你的组织有这些需求，它们应该被包含在 SLA 中。

⑧共享科技。云计算的一个主要好处是来自共享资源和多租户架构的规模经济。不幸的是，共享科技也会导致安全风险。迁移到云并非没有风险，企业领导者需要周全考虑多种因素，以确保其解决方案正确有效：

➢ 失去控制和角色转变。在过去，一切事务都由你亲自完成，而现在你将会对很多环节失去控制，你的企业组织对此能否适应？数据和基础设施都被托管在了其他地方，你将无法控制。你的角色也将转变——从过去自己来运营基础设施到现在与你的供应商打交道。

➢ 信息安全。你的企业组织风险承受能力和安全要求如何？你会用什么样的安全指标来选择供应商？数据的传输从封闭的内部网络变成了共有网络，这显然会让数据保护变得脆弱。多个用户共享基础设施，数据的安全也都全部掌握在供应商手里。因此，企业应该考虑信息的敏感性以及服务提供商的位置是否适当，能否确保数据安全。

➢ 隐私。在隐私方面，相比本地存储，重要的私人信息存储在云上可能会泄露。你需要考虑将敏感数据放置在公有云上的潜在后果，比如可能受制于一些未知的法规，特别是你想与之交易的提供商不告知其数据中心的位置。

➢ 可靠性和业务的连续性。业务连续性至关重要，所以需要了解云服务提供商的地理覆盖范围以及可能给你的业务造成的影响。此外，云服务提供商的业务连续性计划、灾难恢复能力以及操作能力都将完全影响到你，因此要慎重考虑。

大多数组织会受到有关数据收集、存储、处理和共享等方面法律的约束。组织考虑采用云服务时应确定适用的法律要求，并考虑云服务的合规性。

（七）识别法律风险

一个组织不能简单地依赖于云服务提供商以确保遵守法律法规。虽然供应商作为数据控制者或托管商（取决于数据提供者的角色）可能有一定的责任，但最终其法律责任仍在于拥有数据的组织或个人。

采用云服务的组织应当考虑以下法律风险：

1. 数据位置和管辖权

数据在云服务器中可以由任何地方的数据中心进行存储或处理。虽然存储在多个服务器上具有明显的数据恢复能力，但也存在一些显著的法律问题。例如，有些数据可能会受到出口限制以及一些法规的约束。

因为法律一般未能随着技术进步而调整，因此法律在某种程度上也成了一种风险。在云服务器中，存储的数据会受到以下位置法律的约束：

➢ 物理服务器的位置。

➢ 服务供应商的总部所在地。

➢ 数据拥有者的位置。

➢ 服务提供商的服务器之间的中间地带。

该风险可通过与服务提供商达成约定以使数据保持在适当的地理位置来降低。

2. 数据隔离

某些数据安全方面的规定可能会对数据隔离提出要求。在传统的计算中，数据可以进行物理隔离（如在一个单独的服务器上）或逻辑隔离（如一个单独的虚拟服务器、文件或数据库）。在云计算中，多用户是很常见的，确保数据隔离就更加困难了。在多用户云计算环境中，数据隔离是逻辑上的。它可以通过隔离虚拟机发生在虚拟机管理程序层面上，或者在数据库层面上，可能涉及以下内容：

➢ 隔离在一个共享的数据库行级别，并由唯一的用户标识来实现。

➢ 隔离在架构层面是通过使用一个共享的数据库，为每个用户使用单独的表来实现。

➢ 最大限度的数据隔离，为每个用户提供独立的数据库来实现，虽然这会导致成本的增加。

3. 数据销毁

考虑组织和云服务供应商之间的合同终止后会发生什么是很重要的，该组织必须保证（通过合同或服务条款）它的所有数据包括档案会被删除，并无法恢复。

4. 破产

如果云服务提供商破产了，数据可能会在资产处置过程中暴露出来。事实上，数据甚至可能被认为是一种企业资产，并可以出售，这取决于服务提供商的条款。

5. 服务条款

云服务供应商并不总是单独与客户签订合同。他们可能已经发布了适用于所有客户的服务和隐私条款。这些条款和政策必须在选择供应商之前被仔细审查。即使条款似乎是与数据拥有者的需求相适应的，但总是存在服务条款可能会未经通知被改变的风险，这可能会给数据所有者带来民事甚至刑事责任。

（八）特殊的法律规定

某些类别的信息有一些特殊的法律规定，有可能会影响云服务的用户，以下是一些例子。

1. 健康信息

在美国，隐私和健康记录的安全性是由健康保险流通与责任法案（HIPAA）所管辖。HIPAA 主要影响医疗服务提供者和健康计划（包括实体），但是，合规还需要包括有机会获得电子保护的健康信息（EPHI）的商业组织。这将包括云服务提供商。受管制的实体和云服务运营商都需要进入一个商业协议去规定每一方的履约义务。

2. 特权信息

某些专业人士，如医生和律师有法律义务保留客户的私密信息，尽管不同国家和地区的法律有所不同。服务提供商的服务协议必须经过仔细审查，以避免破坏法律的特权。

3. 个人身份识别信息（PII）

这种类型的信息可以被用于唯一地识别个体。PII 的分类以及其安全性和限制取决于管辖权。有价证券例子包括联系信息、金融信息、在线账户用户名、政府颁发的身份证明文件（如身份证和密码端口），以及生物特征数据。

（九）记录管理

记录管理（records management）指的是公共和私营机构可以承受的记录保留要求。在决定使用云服务之前，组织应首先确定自己的记录保存要求是基于业务、法律和相关政策的；确保其与内部政策是一致的，然后确保云服务符合组织的合规性。

与记录管理和保留相关的以下条件可能会导致风险：原来的元数据与存档的记录相关联、基于提供者的记录留存期限比该组织要求的更短、保留期满后记录才能销毁。

云计算可以通过经济的规模性对安全起到积极的作用。云服务的供应商可能比依靠自身能力在它的客户之间分摊成本的单个组织，以提供更高的潜在的安全水平。以下的例子在某种程度上说明云计算对安全起到积极的作用：增加可用性，通过大量的其他地点改善意外恢复能力；安全专家；24/7 基础设施的员工与管理运营人员比例。