

云计算关键领域 安全指南 V3.0

导论

The guidance provided herein is the third version of the Cloud Security Alliance document, “**Security Guidance for Critical Areas of Focus in Cloud Computing**,” which was originally released in April 2009. The permanent archive locations for these documents are:

<http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf> (this document)

<http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf> (version 2 guidance)

<http://www.cloudsecurityalliance.org/guidance/csaguide.v1.0.pdf> (version 1 guidance)

In a departure from the second version of our guidance, each domain was assigned its own editor and peer reviewed by industry experts. The structure and numbering of the domains align with industry standards and best practices. We encourage the adoption of this guidance as a good operating practice in strategic management of cloud services. These white papers and their release schedule are located at:

<http://www.cloudsecurityalliance.org/guidance/>

In another change from the second version, there are some updated domain names. We have these changes: **Domain 3: Legal Issues: Contracts and Electronic Discovery** and **Domain 5: Information Management and Data Security**. We now have added another domain, which is **Domain 14: Security as a Service**.

© 2011 Cloud Security Alliance.

All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance Guidance at <http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf> subject to the following: (a) the Guidance may be used solely for your personal, informational, non-commercial use; (b) the Guidance may not be modified or altered in any way; (c) the Guidance may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Guidance as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Guidance Version 3.0 (2011).

目录

导论.....	1
目录.....	2
前言.....	3
V3.0 中文版 译者序.....	4
英文版致谢.....	6
编者寄语.....	8
关于风险的编者按.....	10
第一部分 云体系架构	
D1: 云计算体系架构.....	14
第二部分 云的治理	
D2: 治理与企业风险管理.....	31
D3: 法律问题：合同与电子发现.....	36
D4: 合规与审核.....	44
D5: 信息管理与数据安全.....	48
D6: 互操作性与可移植性.....	61
第三部分 云的运行	
D7: 传统安全、业务连续性和灾难恢复.....	70
D8: 数据中心运行.....	83
D9: 事故响应.....	87
D10: 应用安全.....	96
D11: 加密与密钥管理.....	119
D12: 身份，授权和访问管理.....	125
D13: 虚拟化.....	144
D14: 安全即服务 SecaaS.....	149

前言

Welcome to the third version of the Cloud Security Alliance’s “Security Guidance for Critical Areas of Focus in Cloud Computing.” As cloud computing begins to mature, managing the opportunities and security challenges becomes crucial to business development. We humbly hope to provide you with both guidance and inspiration to support your business needs while managing new risks.

The Cloud Security Alliance has delivered actionable, best practices based on previous versions of this guidance. As we continue to deliver tools to enable businesses to transition to cloud services while mitigating risk, this guidance will act as the compass for our future direction. In v3.0, you will find a collection of facts and opinions gathered from over seventy industry experts worldwide. We have compiled this information from a range of activities, including international chapters, partnerships, new research, and conference events geared towards furthering our mission. You can follow our activities at www.cloudsecurityalliance.org.

The path to secure cloud computing is surely a long one, requiring the participation of a broad set of stakeholders on a global basis. However, we should happily recognize the progress we are seeing: new cloud security solutions are regularly appearing, enterprises are using our guidance to engage with cloud providers, and a healthy public dialogue over compliance and trust issues has erupted around the world. The most important victory we have achieved is that security professionals are vigorously engaged in securing the future, rather than simply protecting the present.

Please stay engaged on this topic and continue to work with us to complete this important mission.

Best Regards,

Jerry Archer

Dave Cullinane

Nils Puhmann

Alan Boehme

Paul Kurtz

Jim Reavis

The Cloud Security Alliance Board of Directors

V3.0 中文版译者序

云计算已经成为行业中一个轰轰烈烈的“进行时”，云计算自身的安全防护、使用云计算变革网络安全都获得了迅速上升的关注和资源投入。云安全联盟以其大量的研究发布、迅速发展企业和个人会员成为国际范围内在云安全领域具备首屈一指影响力的组织。至本序写作之日，云安全联盟的企业会员达到 150 家，其中来自中国大陆的企业有 7 家，以 LinkedIn 为基准的个人会员达到 46500 多人。

《云安全指南》全称《云计算关键领域的安全指南》（Security Guidance for Critical Areas of Focus in Cloud Computing）。云安全指南第 1 版在 2009 年 4 月 1 日发布，也就是在 2009 年的 RSA 会议上 CSA 成立后的一个月。这个版本并没有引起特别大的关注。在 2009 年 12 月 17 日，CSA 发布了《云安全指南 v2.1》。在发布后的很长一段时间内，几乎是在世界范围内唯一的发布，非常引人注目，大量的下载和报道也帮助云安全联盟在行业内的被关注程度迅速上升。2010 年春节后，v2.1 的中文版发布。

2011 年 11 月 14 日 CSA 发布了《云安全指南 v3.0》，也就是在 v2.1 发布后的大约 2 年后。有必要说明的一点，从《云安全指南 v2.1》到《云安全指南 v3.0》的变化是非常大的，这从文档的页数从 76 页增加到 177 页足见一斑。对比来看，v3.0 除了新增第 14 域“安全即服务”一节之外，其他章节中之前许多概括性的描述在新版本中进行了丰富和细化。

v3 至今已有 1 年多时间，期间不少朋友专家同仁希望 CSA 能组织将其翻译成中文，以便于国内用户读者使用。在 2013 年春节前通过微博/邮件等方式发出中文版倡议后，得到了很多同仁的热烈响应，迅速组成了一个十多人的翻译小组。大家牺牲了春节很多和家人团聚休息的时间投入到翻译工作中，在 3 月份左右完成了每章节的翻译。随后又经过审校小组诸位同仁的认真校阅，到 5 月份终于告一段落。

在翻译工作中，D1 由臧铁军、林恒辉翻译，D2 由 Kelvin Gao、余晓光、潘吴斌翻译，D3 由杨帆、潘吴斌翻译，D4 由曹嘉、杨帆翻译，D5 由余晓光、龚习琴翻译，D6 由张荣典翻译，D7 由叶润国、曹嘉、臧铁军、林恒辉翻译，D8 由汪宏翻译，D9 由李本、王海涛、马蔚彦翻译，D10 由刘生权、马红伟翻译，D11 由徐甲甲翻译，D12 由田民、徐甲甲翻译，D13 由沈勇、杨勇涛翻译，D14 由刘弘利、王海涛、张荣典翻译。

潘柱廷审校了 D1/D2，沈勇审校了 D3/D4，Billy 审校了 D5/D6，Antony Ma 审校了 D7/D11，Otto Lee 审校了 D8，Frank Chow 审校了 D9，吴云坤审校了 D10/D14，Ricci leong 审校了 D12，Mike Lo 审校了 D13。

感谢卿思汉老师对翻译小组的指导和提出的宝贵意见。

另外，感谢王洋为最终稿排版付出了很多努力，他还帮助修正不少译稿中的小纰漏。

全文由赵粮负责组织和统稿。

当前翻译版本肯定还存在诸多问题，例如很多图表没有来得及制作中文版本，一些需要本地化的注解/注释等没有来得及添加，有些翻译不够精确，没有来得及和原作者/编辑小组沟通确认。欢迎读者批评指正。

另外，期间由于项目组织和个人方面的原因有诸多拖延，向大家致以歉意。

在 CSA 官方网址 <https://chapters.cloudsecurityalliance.org/china> 可以找到更多的研究项目和联系方式。另外，搜索新浪微群“云安全联盟”、在 LinkedIn 搜索“Cloud Security Alliance, Greater China Chapter”可以找到更多中国区的更新并与同仁互动。

希望中文版的翻译发布能够在云计算安全的研究、开发、推广、应用等活动中为行业、政府、标准机构和学术的同仁、同学提供帮助。

英文版致谢

Domain Authors/Contributors

Domain 1: Chris Hoff, Paul Simmonds

Domain 2: Marlin Pohlman, Becky Swain, Laura Posey, Bhavesh Bhagat

Domain 3: Francoise Gilbert, Pamela Jones Harbour, David Kessler, Sue Ross, Thomas Trappier

Domain 4: Marlin Pohlman, Said Tabet

Domain 5: Rich Mogull, Jesus Luna

Domain 6: Aradhna Chetal, Balaji Ramamoorthy, Jim Peterson, Joe Wallace, Michele Drgon, Tushar Bhavsar

Domain 7: Randolph Barr, Ram Kumar, Michael Machado, Marlin Pohlman

Domain 8: Liam Lynch

Domain 9: Michael Panico, Bernd Grobauer, Carlo Espiritu, Kathleen Moriarty, Lee Newcombe, Dominik Birk, Jeff Reed

Domain 10: Aradhna Chetal, Balaji Ramamoorthy, John Kinsella, Josey V. George, Sundararajan N., Devesh Bhatt, Tushar Bhavsar

Domain 11: Liam Lynch

Domain 12: Paul Simmonds, Andrew Yeomans, Ian Dobson, John Arnold, Adrian Secombe, Peter Johnson, Shane Tully, Balaji Ramamorthy, Subra Kumaraswamy, Rajiv Mishra, Ulrich Lang, Jens Laundrup, Yvonne Wilson

Domain 13: Dave Asprey, Richard Zhao, Kanchanna Ramasamy Balraj, Abhik Chaudhuri, Melvin M. Rodriguez

Domain 14: Jens Laundrup, Marlin Pohlman, Kevin Fielder

Peer Reviewers

Valmiki Mukherjee, Bernd Jaeger, Ulrich Lang, Hassan Takabi, Pw Carey, Xavier Guerin, Troy D. Casey, James Beadel, Anton Chuvakin, Tushar Jain, M S Prasad, Damir Savanovic, Eiji Sasahara, Chad Woolf, Stefan Pettersson, M S Prasad, Nrupak Shah, Kimberley Laris, Henry St. Andre, Jim Peterson, Ariel Litvin, Tatsuya Kamimura, George Ferguson, Andrew Hay, Danielito Vizcayno,

K.S. Abhiraj, Liam Lynch, Michael Marks, JP Morgenthal, Amol Godbole, Damu Kuttikrishnan, Rajiv Mishra, Dennis F. Poindexter, Neil Fryer, Andrea Bilobrk, Balaji Ramamoorthy, Damir Savanovic

Editorial Team

Archie Reed: Domains 3, 8, 9

Chris Rezek: Domains 2, 4, 5, 7, 13, 14

Paul Simmonds: Domains 1, 6, 10, 11, 12

CSA Staff

Technical Writer/Editor: Amy L. Van Antwerp

Graphic Designer: Kendall Scoboria

Research Director: J.R. Santos

编者寄语

Over the past three years, the Cloud Security Alliance has attracted around 120 corporate members and has a broad remit to address all aspects of cloud security, including compliance, global security-related legislation and regulation, identity management, and the challenge of monitoring and auditing security across a cloud-based IT supply chain. CSA is becoming the focal point for security standards globally, aligning multiple, disparate government policies on cloud security and putting forward standards for ratification by international standards bodies.

CSA sees itself as a cloud security standards incubator, so its research projects use rapid development techniques to produce fast results. To this end, the CSA Guidance editorial team is proud to present the third version of its flagship “Security Guidance for Critical Areas of Focus in Cloud Computing.” This work is a set of best security practices CSA has put together for 14 domains involved in governing or operating the cloud (Cloud Architecture, Governance and Enterprise Risk Management, Legal: Contracts and Electronic Discovery, Compliance and Audit, Information Management and Data Security, Portability and Interoperability, Traditional Security, Business Continuity and Disaster Recovery, Data Center Operations, Incident Response, Notification and Remediation, Application Security, Encryption and Key Management, Identity and Access Management, Virtualization, and Security as a Service).

CSA guidance in its third edition seeks to establish a stable, secure baseline for cloud operations. This effort provides a practical, actionable road map to managers wanting to adopt the cloud paradigm safely and securely. Domains have been rewritten to emphasize security, stability, and privacy, ensuring corporate privacy in a multi-tenant environment.

Over the past two years, version 2.1 of the guidance has served as the foundation for research in multiple areas of cloud security. Deliverables now in use from the TCI Architecture to the GRC Stack were inspired by previous versions of the guidance, and it is our hope that this version will be no different. The guidance serves as a high level primer for chief executives, consumers, and implementers wishing to adopt cloud services as an alternative or supplement to traditional infrastructure. However, the guidance is designed with innovation in mind. Those with an entrepreneurial mindset should read this work with an eye toward the inferred services and approaches many of the authors have included in the domain creation. Investors and corporate decision makers will also find this work of interest, as it serves as a roadmap for innovation and development already in place in companies throughout the world. Security practitioners and educators will find elements of this book both authoritative and thought provoking, and as the industry evolves, the value the authors have included should prove influential and timely.

In the third edition, the guidance assumes a structural maturity in parallel with multinational cloud standards development in both structure and content. Version 3.0 extends the content included in previous versions with practical recommendations and requirements that can be measured and audited. Please note that different interpretations of the term “requirements” exist, which we use throughout the document. Our guidance does not represent a statutory obligation, but “requirements” was chosen to represent guidance appropriate for virtually all use cases we could envision, and also aligns our guidance with similar well-accepted documents. CSA industry expert authors have endeavored to present a working product that is measured and balanced between the interests of cloud providers and tenants. Controls focus on the preservation of tenant data ownership integrity while embracing the concept of a shared physical infrastructure. Guidance Version 3.0 incorporates the highly dynamic nature of cloud computing, industry learning curve, and new developments within other research projects such as Cloud Controls Matrix, Consensus Assessments Initiative, Trusted Cloud Initiative, and GRC Stack Initiative and ties in the various CSA activities into one comprehensive C-level best practice. The Security Guidance v3.0 will serve as the gateway to emerging standards being

developed in the world's standards organization and is designed to serve as an executive-level primer to any organization seeking a secure, stable transition to hosting their business operations in the cloud.

On behalf of the Cloud Security Alliance, we would like to thank each and every volunteer for their time and effort in the development and editing of this new release of our flagship guidance document. While we believe this is our best, most widely reviewed work to date, the topic is still evolving and although our foremost intent is to guide, we also intend to inspire the readers to become involved in improving and commenting on the direction those composing the body of work have outlined. We humbly and respectfully submit this effort to the industry and await the most important component of any dialog, your opinion. We are eager to hear your feedback regarding this updated guidance. If you found this guidance helpful or would like to see it improved, please consider joining the Cloud Security Alliance as a member or contributor.

Best Regards,

Paul Simmonds

Chris Rezek

Archie Reed

Security Guidance v3.0 Editors

关于风险的编者按

Throughout this Guidance we make extensive recommendations on reducing your risk when adopting cloud computing, but not all the recommendations are necessary or even realistic for all cloud deployments. As we compiled information from the different working groups during the editorial process, we quickly realized there simply wasn't enough space to provide fully nuanced recommendations for all possible risk scenarios. Just as a critical application might be too important to move to a public cloud provider, there might be little or no reason to apply extensive security controls to low-value data migrating to cloud-based storage.

With so many different cloud deployment options — including the SPI service models (SPI refers to Software as a Service, Platform as a Service, or Infrastructure as a Service, explained in depth in Domain 1); public vs. private deployments, internal vs. external hosting, and various hybrid permutations — no list of security controls can cover all circumstances. As with any security area, organizations should adopt a risk-based approach to moving to the cloud and selecting security options. The following is a simple framework to help evaluate initial cloud risks and inform security decisions.

This process is not a full risk assessment framework, nor a methodology for determining all your security requirements. It's a quick method for evaluating your tolerance for moving an asset to various cloud computing models.

Identify the Asset for the Cloud Deployment

At the simplest, assets supported by the cloud fall into two general categories:

1. Data
2. Applications/Functions/Processes

We are either moving information into the cloud, or transactions/processing (from partial functions all the way up to full applications).

With cloud computing our data and applications don't need to reside in the same location, and we can choose to shift only parts of functions to the cloud. For example, we can host our application and data in our own data center, while still outsourcing a portion of its functionality to the cloud through a Platform as a Service.

The first step in evaluating risk for the cloud is to determine exactly what data or function is being considered for the cloud. This should include potential uses of the asset once it moves to the cloud to account for scope creep. Data and transaction volumes are often higher than expected.

Evaluate the Asset

The next step is to determine how important the data or function is to the organization. You don't need to perform a detailed valuation exercise unless your organization has a process for that, but you do need at least a rough assessment of how sensitive an asset is, and how important an application/function/process is.

For each asset, ask the following questions:

1. How would we be harmed if the asset became widely public and widely distributed?
2. How would we be harmed if an employee of our cloud provider accessed the asset?
3. How would we be harmed if the process or function were manipulated by an outsider?
4. How would we be harmed if the process or function failed to provide expected results?
5. How would we be harmed if the information/data were unexpectedly changed?
6. How would we be harmed if the asset were unavailable for a period of time?

Essentially we are assessing confidentiality, integrity, and availability requirements for the asset; and how the risk changes if all or part of the asset is handled in the cloud. It's very similar to assessing a potential outsourcing project, except that with cloud computing we have a wider array of deployment options, including internal models.

Map the Asset to Potential Cloud Deployment Models

Now we should have an understanding of the asset's importance. Our next step is to determine which deployment models we are comfortable with. Before we start looking at potential providers, we should know if we can accept the risks implicit to the various deployment models: private, public, community, or hybrid; and hosting scenarios: internal, external, or combined.

For the asset, determine if you are willing to accept the following options:

1. Public.
2. Private, internal/on-premises.
3. Private, external (including dedicated or shared infrastructure).
4. Community; taking into account the hosting location, potential service provider, and identification of other community members.
5. Hybrid. To effectively evaluate a potential hybrid deployment, you must have in mind at least a rough architecture of where components, functions, and data will reside.

At this stage you should have a good idea of your comfort level for transitioning to the cloud, and which deployment models and locations fit your security and risk requirements.

Evaluate Potential Cloud Service Models and Providers

In this step focus on the degree of control you'll have at each SPI tier to implement any required risk management. If you are evaluating a specific offering, at this point you might switch to a fuller risk assessment.

Your focus will be on the degree of control you have to implement risk mitigations in the different SPI tiers. If you already have specific requirements (e.g., for handling of regulated data) you can include them in the evaluation.

Map Out the Potential Data Flow

If you are evaluating a specific deployment option, map out the data flow between your organization, the cloud service, and any customers/other nodes. While most of these steps have been high-level, before making a final decision it's absolutely essential to understand whether, and how, data can move in and out of the cloud.

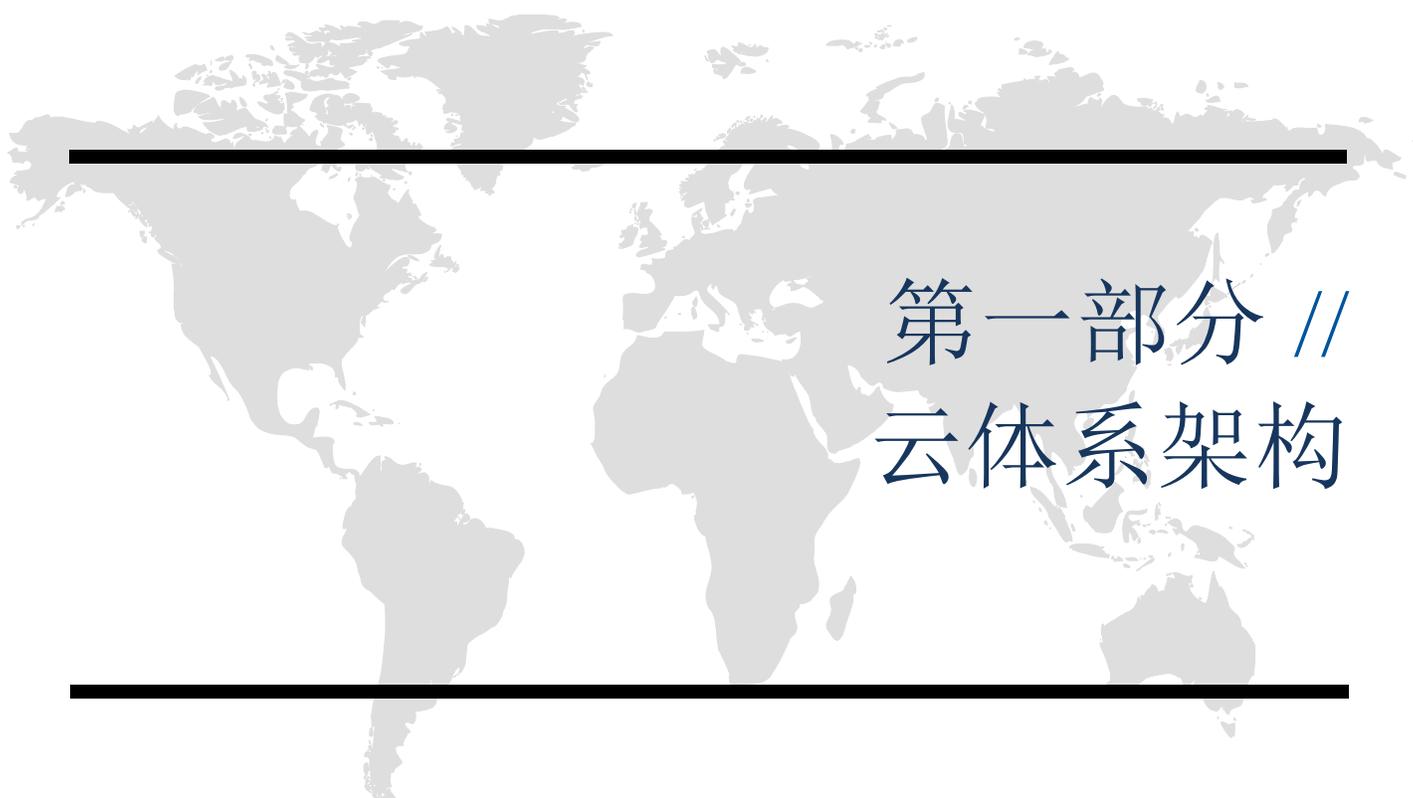
If you have yet to decide on a particular offering, you'll want to sketch out the rough data flow for any options on your acceptable list. This is to insure that as you make final decisions, you'll be able to identify risk exposure points.

Conclusions

You should now understand the importance of what you are considering moving to the cloud, your risk tolerance (at least at a high level), and which combinations of deployment and service models are acceptable. You should also have a good idea of potential exposure points for sensitive information and operations.

These together should give you sufficient context to evaluate any other security controls in this Guidance. For low-value assets you don't need the same level of security controls and can skip many of the recommendations — such as on-site inspections, discoverability, and complex encryption schemes. A high-value regulated asset might entail audit and data retention requirements. For another high-value asset not subject to regulatory restrictions, you might focus more on technical security controls.

Due to our limited space, as well as the depth and breadth of material to cover, this document contains extensive lists of security recommendations. Not all cloud deployments need every possible security and risk control. Spending a little time up front evaluating your risk tolerance and potential exposures will provide the context you need to pick and choose the best options for your organization and deployment.



第一部分 // 云体系架构

D1: 云计算体系架构

本域是云计算体系架构，为云计算安全指南的其它所有部分介绍一个概念性的框架。主要内容将集中在云计算的描述上，并按照 IT 网络和安全专业人士的视角进行了裁剪。

本域的最后一节简要介绍了本指南其它域的内容。

理解本域所描述的体系架构是理解云计算安全指南其它部分的重要一步，该框架定义了很多在其它域中广泛使用的概念和术语。

简介. 下面分三个部分分别来定义云计算体系架构

- 为保证词汇一致性而贯穿整个指南的术语。
- 为保护云应用和云服务安全的架构层要求和挑战。
- 一个描述云服务和体系架构分类的参考模型。

1.1 什么是云计算?

云计算是一个模式，它是一种无处不在的，便捷的，按需的，基于网络访问的，共享使用的，可配置的计算资源（如网络，服务器，存储，应用和服务）。云计算是一种颠覆性的技术，它可以增强协作，提高敏捷性、可扩展性以及可用性。还可以通过优化资源分配、提高计算效率来降低成本。云计算模式构想了一个全新的世界，组件可以迅速调配、置备、部署和回收，还可以迅速地扩充或缩减，以提供按需的、类似于效用计算的分配和消费模式。

从架构的角度来看，云和现有计算模式有什么相似和不同，以及这些相似和不同如何在网络和信息安全实践中对企业的组织、运行和技术路线构成影响，围绕着这些问题有很多令人困惑的地方。常规计算与云计算并不遥远。但是，云计算会在数据安全、网络安全和信息安全等领域对企业的组织、运营和技术路线产生深远的影响。

现在有许多定义尝试着从学术、架构师、工程师、开发人员、管理人员和消费者等不同的的角度来定义什么是云。本文档依照 IT 网络和安全专业人士的视角对云的定义进行了裁剪。

1.2 云计算的构成

这一版本的云安全指南对云计算所做出的定义，基于美国国家标准与技术研究院（NIST）的科学家所写的出版物以及他们围绕云计算定义所做出的努力。

NIST 出版物是被普遍接受的，所以，我们选择与 NIST Working Definition of Cloud Computing（写作本文时是 NIST 800-145）保持一致，这样我们能够集中精力到用例上，而不是细微的语法定义差别上，同时能保证一致性并获得广泛的共识。

值得注意的是，本指南的目的是使其具有广泛的易用性、适用于全球范围内的组织。虽然 NIST 是美国政府机构，选择此参考模型不应该被解释为是对其它观点或地域的排斥。

在 NIST 对云计算的定义中，包括了五个基本特征、三个云服务模式、以及四个云部署模型。图 1 对它们进行了形象的汇总，后面会有详细描述。

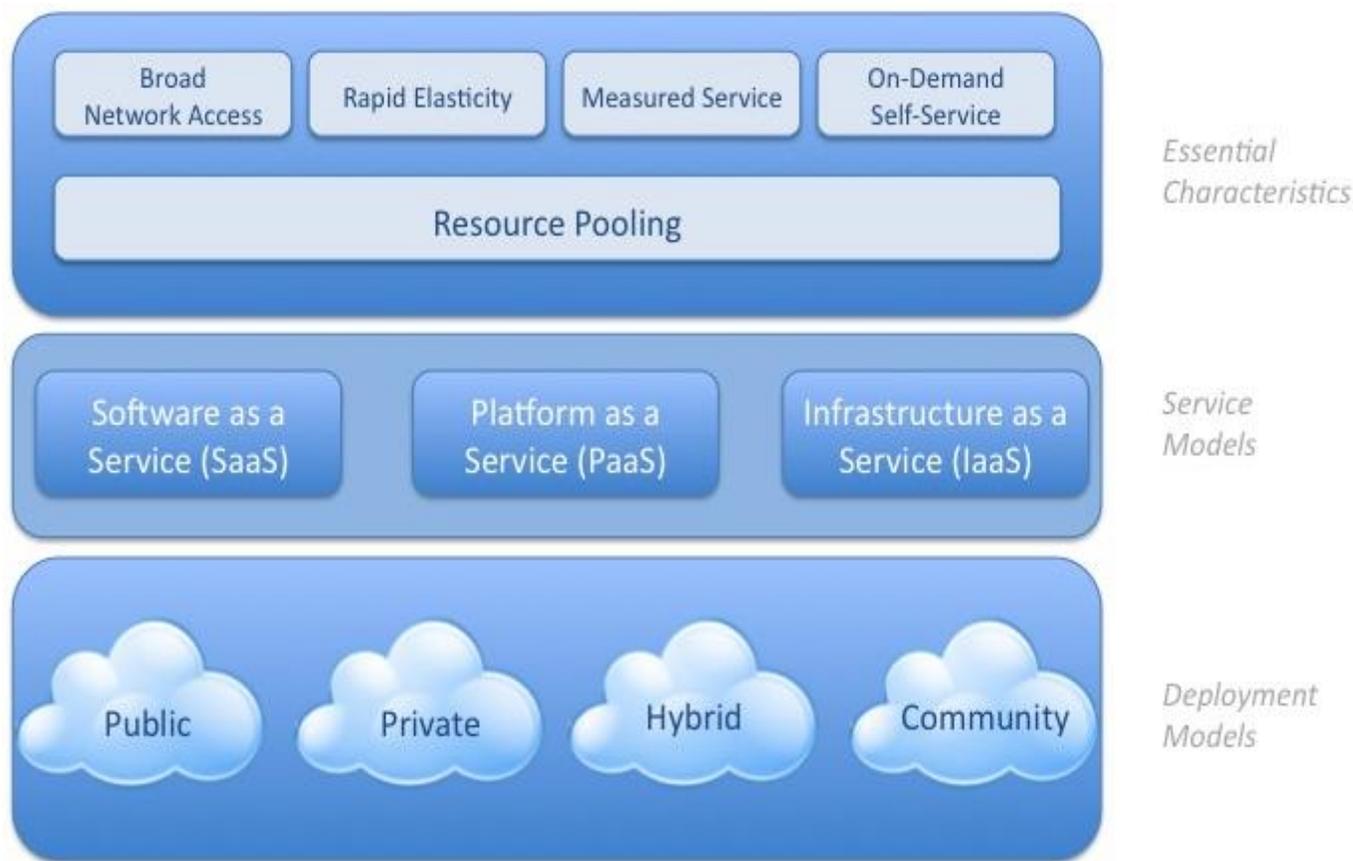


图 1：NIST 云计算定义的直观模型

1.3 云计算的特征

必须认识到的重要一点是虽然云服务经常和虚拟化技术一起使用，或者云服务基于虚拟化技术，但是并不必然。没有要求将资源抽象与虚拟化技术必须绑在一起。很多云服务产品并没有使用虚拟化层或操作系统容器。

还应该注意到，多租户并没有成为 NIST 云计算定义中的一个必备特征，但在讨论中确实经常这么认为。CSA 认为多租户是云的一个重要元素。

1.4 多租户

在本文中多租户被认为是一个重要元素，后续的章节将描述 CSA 对这个重要的云计算元素的理解和定义。

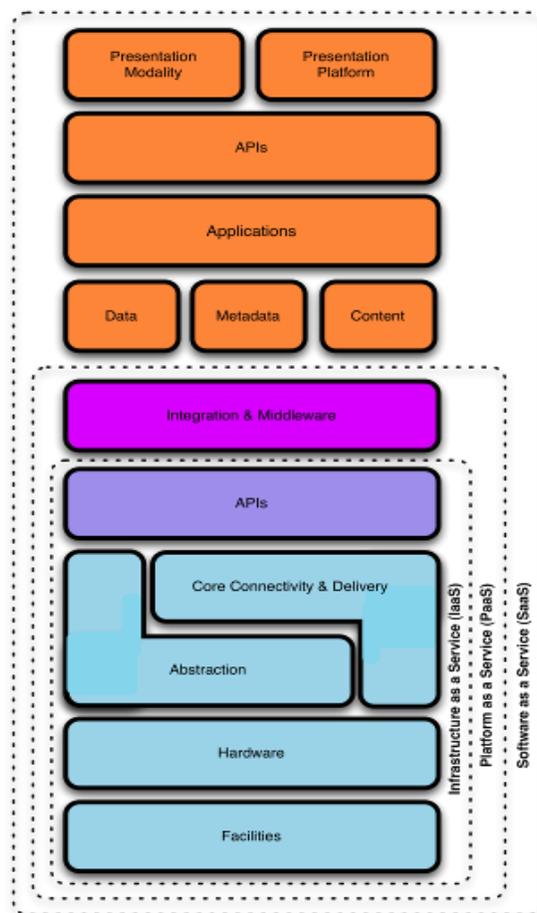
多租户的最简单形式就是多个消费者同时使用属于同一组织或不同组织的资源和应用。多租户的影响主要是残留数据可见性和对其它用户或租户操作的追踪。

云服务模式中的“多租户”意味着满足不同客户场景对策略驱动的安全增强、分段、隔离、监管、服务水平以及相应的计费/返款等模型的不同需求。

消费者可以以用户的身份使用公有云服务提供商的服务，或者是私有云服务中一个实例，一个组织可以将共享同一个公共基础的用户分隔为不同的业务单元 BU（business unit）。

从提供商的角度来看，多租户对架构和设计提出的要求是通过在很多不同消费者之间杠杆式地分享基础设施、数据、元数据、服务和应用等，来实现可扩展、可用性、管理、分区、隔离以及运行效率等方面的“经济性”。

依赖于服务商的云服务模式，“多租户”也可以有不同的定义，因为它可能在基础设施、数据库或应用等不同层面上实现。基础设施即服务（IaaS¹），软件即服务（SaaS²）和平台即服务（PaaS³）都是多租户的实现。



¹ IaaS: Infrastructure as a Service

² SaaS: Software as a Service

³ PaaS: Platform as a Service

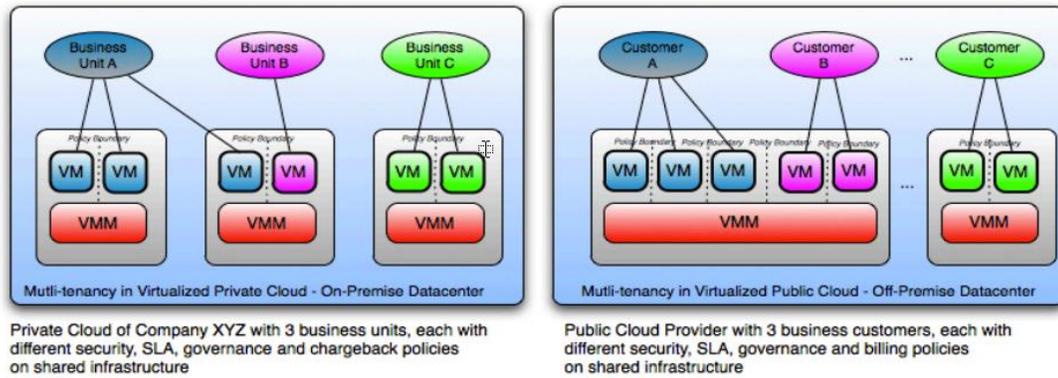


图 2：多租户

“多租户”在不同的云部署模型中的重要性也有所不同。然而，即使在私有云中，组织虽然是同一个，但是也存在来自各方的第三方顾问和临时合同人员，也存在对不同业务单元间高层逻辑分离的期望，因此，也需要考虑“多租户”。

1.5 云参考模型

理解云计算模式之间的关系和依赖性对于理解云计算的安全风险非常关键。IaaS 是所有云服务的基础，PaaS 建立在 IaaS 之上，而 SaaS 又建立在 PaaS 之上，它们之间的关系可参考云参考模型图示。沿着这个思路，如同云服务能力是继承的那样，信息安全风险和问题也是继承的。值得重点注意的是，商用云提供商可能并没有与这个模型的层次准确对应。然而，云参考模型对于将真实服务和某个架构框架联系在一起，进而理解需进行安全分析的资源和服务是非常重要的。

IaaS 涵盖了从机房设备到其中的硬件平台等所有的基础设施资源层面。它包括了将资源抽象化（或相反）的能力，并交付连接到这些资源的物理或逻辑网络连接，终极状态是 IaaS 提供商提供一组 API，允许消费者与基础设施进行管理和其它形式的交互。

PaaS 位于 IaaS 之上，又增加了一个层面用以与应用开发框架、中间件能力以及数据库、消息和队列等功能集成。PaaS 允许开发者在平台之上开发应用，开发的编程语言和工具由 PaaS 支持提供。

类似的，SaaS 又位于底层的 IaaS 和 PaaS 之上。SaaS 能够提供独立的运行环境，用以交付完整的用户体验，包括内容、展现、应用和管理能力。

因此，必须清楚，在三个模型中，在集成的功能特征、复杂性与开放性（可扩展性）和安全性等方面会有一些明显的权衡。一般来说，SaaS 会在产品中提供最为集成化的功能，最小的用户可扩展性以及相对来说较高的集成化的安全（至少提供商承担安全的职责）。

基础设施即服务（IaaS），将计算机基础设施（通常以虚拟化环境作为平台）与存储和网络资源一起作为服务交付。用户无需购买服务器，软件，数据中心空间或网络设备，而是将这些资源作为外包服务整体采购。

软件即服务（SaaS），有时也被称为“按需的软件”，是一种将软件和相关的数据集中存储（通常位于互联网上的公有云中）的软件交付形式。用户可以使用瘦客户机上的浏览器通过互联网来访问服务。

平台即服务（PaaS），将计算平台和解决方案包作为服务来交付。PaaS 提供部署应用所需的设施，消除了购买和管理底层硬件和软件以及部署这些主机所带来的成本和复杂度。所提供的能力需要在互联网上构建和发布 Web 应用以及服务提供完整的生命周期支持。

PaaS 提供的是开发者在平台之上开发自己应用的能力。因此，它倾向于提供比 SaaS 更多的可扩展性，其代价是没有了 SaaS 那些用户即买即用的功能。这种权衡也会延伸到安全特色和能力上，虽然内置安全能力变得不够完备，但是用户却拥有更多的灵活性去实现自己的强化安全。

IaaS 几乎不提供那些和应用类似的特色功能，但却有极大的“可扩展性”。这一般是指 IaaS 在除了基础设施自身的保护之外，提供更少的集成安全保护能力和功能。IaaS 模型要求云用户自己管理和保护操作系统、应用和内容。

云安全架构的一个关键特点是云服务提供商所在的等级越低，云服务用户自己所要承担的安全能力和管理职责就越多。

如果要向消费者承诺 SLA，则意味着需要在合同里需要对服务本身和提供商的服务水平、安全、管控、合规性以及责任期望等有明确要求。目前存在两种类型的 SLA，可协商的和不可协商的。缺少 SLA 时，消费者的管理员需要控制云的所有方面。如果采用不可协商的 SLA，则提供商的管理员需要根据协议负责这一部分。在 PaaS 或 IaaS 情况下，这些内容的管理责任是用户自己的系统管理员，提供商对于安全保护底层平台和基础设施组件以确保基本服务的可用性和安全，其具体要求可能会有一些相关的出入。必须清楚一点，用户可以指派/转移职责（responsibility）而不是责任（accountability）。

如果将每种云交付模型的范围或具体能力/功能，或它们相互交叉耦合的一些功能缩小一下，将会产生很多衍生的分类。例如存储作为服务（Storage as a Service）就是 IaaS 家族中的一个具体的子服务。

云计算的解决方案正在不断地演进，虽然讨论它的全景图超出了本文档的范围，但下面这张 OpenCrowd Cloud Solutions 分类图还是给出了一个非常不错的起点，它展示了当前风起云涌的由上述几种部署模型衍生而来的种种云解决方案。CSA 并不特别支持下图所列出的任何解决方案，而只是用来说明当前市场上提供的云解决方案的多样性。

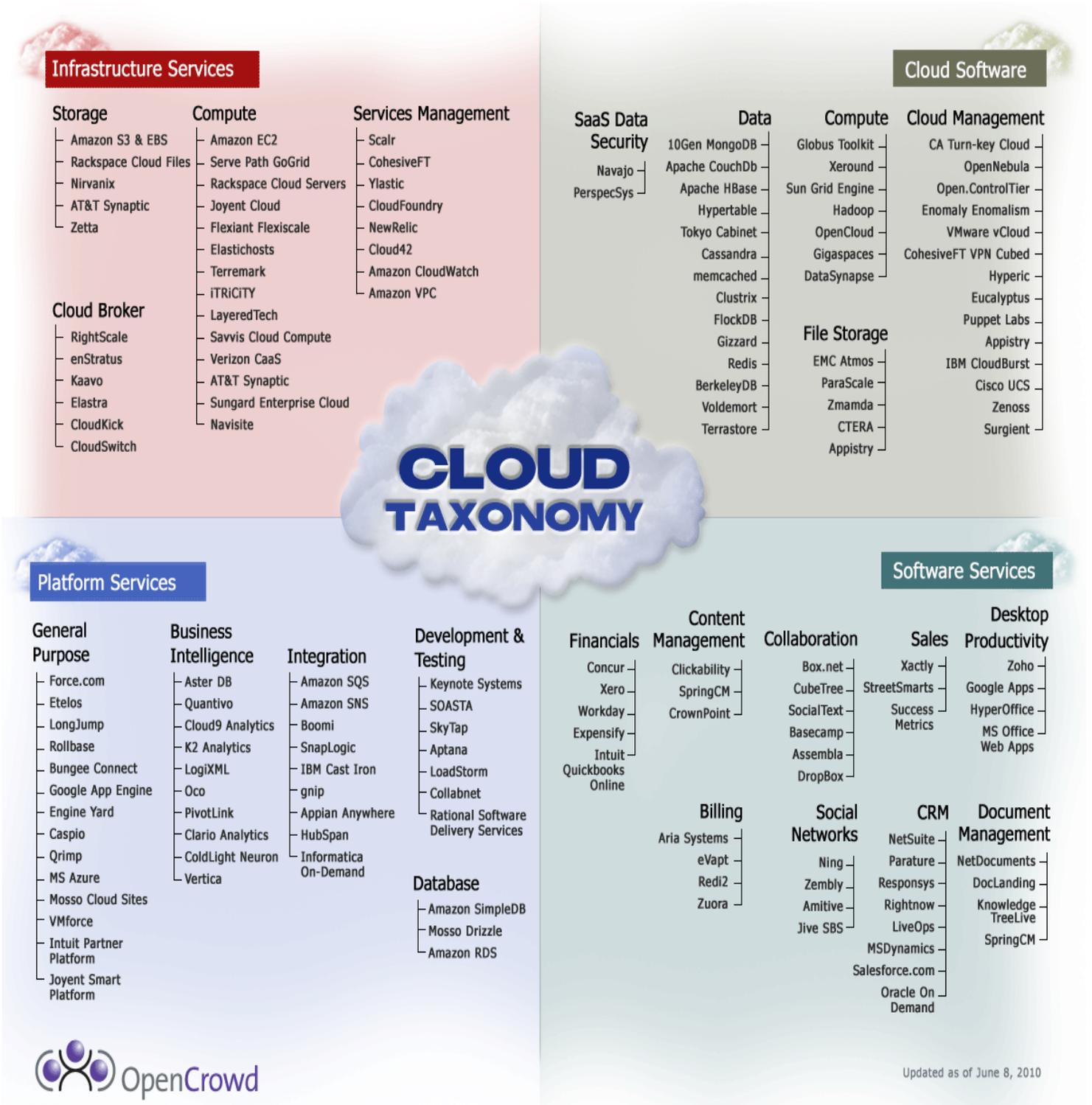


图3: OpenCrowd 的云分类

为了提供一个云计算用例的全面视图，Cloud Computing Use Case Group 开发了一个协同任务来描述和定义通用案例并展示云带来的好处，他们的目标设定为：“...让云用户和提供商一起来定义云计算的公共用例...强调云计算环境中需要标准化的能力和要求，以确保互操作性、更易集成、可移植性。”

⁴ http://www.opencrowd.com/assets/images/views/views_cloud-tax-lrg.png

1.5.1 云安全参考模型

云安全参考模型解决的是这些分类的关系，并把它们和与其相关的安全控制和顾虑放在一起考虑。对于初次接触云计算的组织和个人来说，注意到下面的问题以避免潜在的陷阱和困惑是很重要的：

- “云服务是如何部署的”与“云服务是在哪里提供的”这样的概念频繁混用所带来的困惑。例如，公共或私有可能被描述成外部或内部云，这种互换不是所有情况下都是准确的。
- 云服务的使用方式经常被描述成与组织的管理或安全边界位置有关（通常定义在某个防火墙上）。虽然了解云计算中安全边界在哪里很重要，但是，“界限清晰的边界”的这一概念对于大多数组织是一个时代性错误。
- 在企业中正在上演的对信任边界的重组（re-perimeterization）及侵蚀，被云计算放大并加速。无处不在的连接、各种形式的信息交换、无法解决云服务动态特性的传统静态安全控制，这些都要求针对云计算的新思维。针对企业网络的边界重整，Jericho Forum 开发了相当多的材料，包括很多案例分析。

云的部署和消费模式不能仅仅在“内部”还是“外部”概念上讨论，因为它们不仅与资产、资源和信息的物理位置有关，而且还要讨论由谁消费，由谁负责治理、安全、政策标准的合规性等。

这里不是在主张某个资产、资源和信息是在“场内”（on-premise）还是“场外”（off-premise）对组织的安全和风险状态没有影响，它们的的确确有影响。但是，这里更想强调的是风险还与下面这些有关：

- 所要管理的资产、资源和信息类型
- 谁管理？如何管理？
- 选择了哪些控制？如何集成？
- 合规性问题

例如，Amazon AWS EC2 里部署的 LAMP 套件应该归类为公共的、场外的、第三方管理的 IaaS 解决方案，即使其中的实例、应用、数据是由消费者或某个第三方负责管理。部署在 Eucalyptus 的为若干个业务单元服务某个常规应用，由同一个公司控制、管理并拥有，可以归类为私有的、场内的、自管理的 SaaS 解决方案。两个例子都使用了云的弹性架构和自服务能力。

下面的表格总结了这些要点：

表 1: 云计算部署模型

	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Organization Or Third Party Provider	Organization Or Third Party Provider	On-Premise Or Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

¹ Management includes: governance, operations, security, compliance, etc...

² Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment

³ Infrastructure Location is both physical and relative to an Organization's management umbrella and speaks to ownership versus control

⁴ Trusted consumers of service are those who are considered part of an organization's legal/contractual/policy umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.

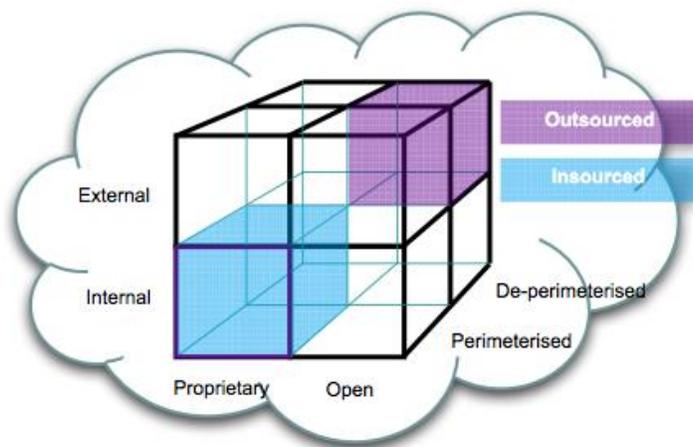
另外一个将云服务模型、部署模型、资源物理位置、管理和所有者属性等图形化展示的方法是 Jericho Forum (www.jerichoforum.org) 的云立方体模型 (Cloud Cube Model)，如下图所示：

云立方体模型很形象地阐述了市场上现有云产品的各种排列组合，提出了用以区分云从一种形态 (formation) 转换到另外一种形态的四种准则/维度，以及各种组成的供应配置方式以便理解云计算影响安全路线的方式。

云立方体模型还凸显了在理解云模型并将云模型映射到控制框架和标准上去时的挑战，这些控制框架和标准，像 ISO/IEC 27002，提供了“一系列指南和通用原则，用以在组织内部启动、部署、维护和提升信息安全管理”。

在 ISO/IEC 27002 的 6.2 节，“外方” (External Parties) 控制目标有：“……组织的信息和信息处理设施的安全不应该因为引入外方产品或服务而降低……”

因此，三种云服务模型的安全防护在方法和责任上有所不同，这意味着云服务的消费者面临很有挑战性的工作。除非云提供商愿意透露自己的安全控制以及为消费者部署的程度，同时消费者也知晓自己需要哪些控制以保持信息安全，否则，肯定会有极大可能误导风险管



The Cloud Cube Model

图 4: Jericho 的云立方体模型

理决策并损失惨重。

首先将一个云服务归类到云架构模型中。接下来对照其安全架构，以及业务、监管和其它合规要求做出差距分析。输出的结果决定了某个云服务的一般“安全”状态，以及它如何和某个资产的保障和保护要求关联到一起。

下图给出了一个很好的例子说明，如何通过对云服务组件和安全控制策略集的映射来确定哪些安全控制是存在或缺失的，这些安全控制分别由客户，云服务提供商或第三方提供。这也可以与合规框架或者强制要求（如 PCI DSS）来进行比较，同样如下图所示。

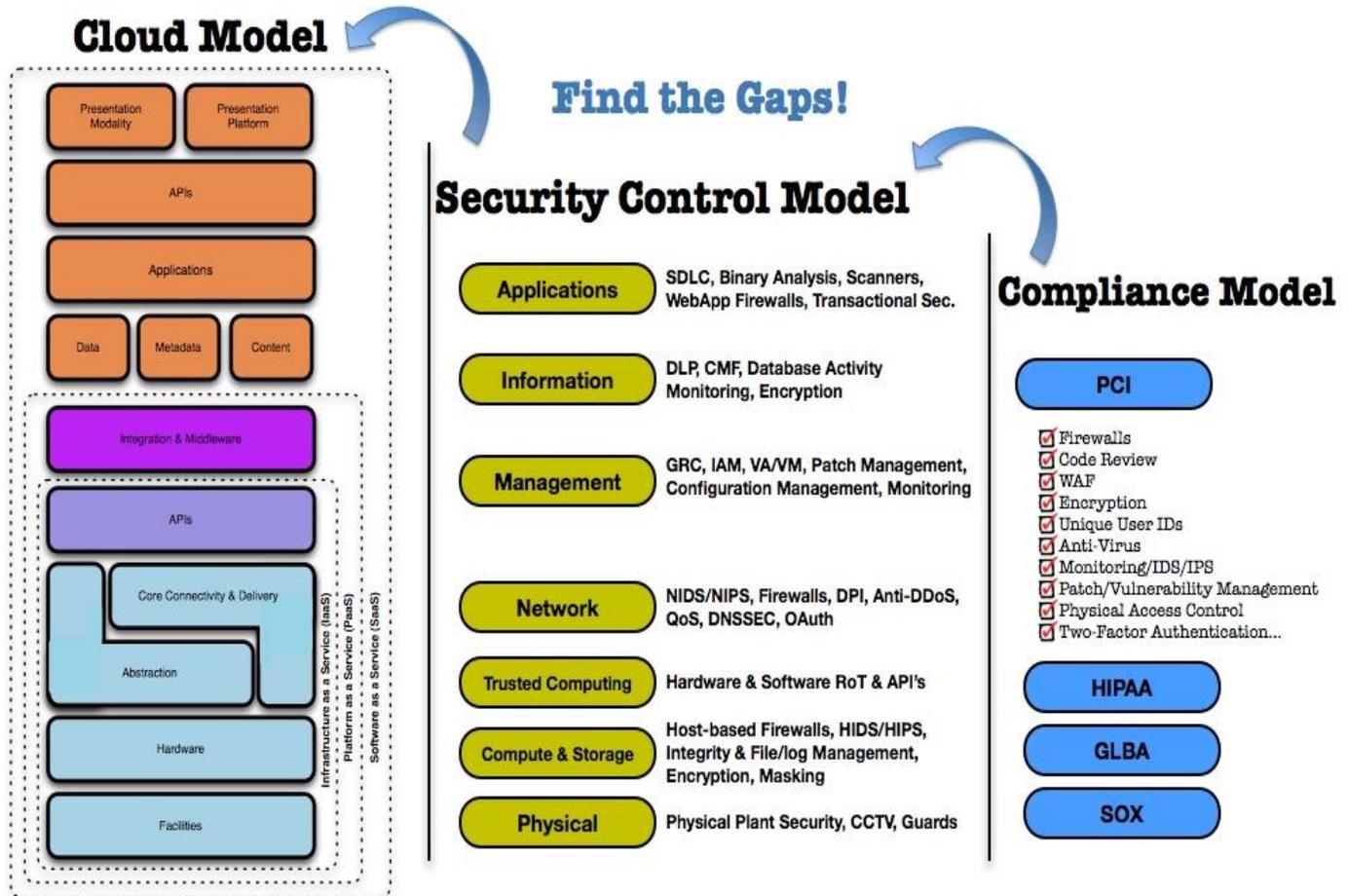


图5：将云模型与安全控制和合规性进行映射

完成差距分析后，按照监管方和合规方面的要求，就容易决定需要做哪些以反馈到风险评估框架了。相应地，这也可以帮助决定如何对待这些安全“差距”或最终的风险 - 接受、转移、或降低。

需要意识到的重要一点是，使用云计算作为一种运行模型并不会自然地提供或妨碍达成合规性。对于任何要求的合规是服务、所使用的部署模型、以及对范围内的资源的设计、部署、管理等的直接结果。

下面是几个对控制框架非常好的全面总结，它们提供了上面提及的通用控制框架的精彩阐述，包括开放安全架构小组（Open Security Architecture Group）的安全架构模式文档，还有最近刚刚更新的 NIST 800-53 修订版 3 - 联邦信息系统与组织安全控制建议（Recommended Security Controls for Federal Information Systems and Organizations）。

1.5.2 什么是云计算的安全性？

云计算中的安全控制，其中的大部分与其它 IT 环境中的安全控制并没有什么不同。然而，由于采用云服务模式、运行模式以及用于提供云服务的技术，与传统 IT 解决方案相比云计算使组织可能面临不同的风险。

一个组织的安全状况的态势（security posture）取决于风险调整后实施的安全控制的成熟度，有效性和完整性。这些安全控制可以在一层或多层上实现，包括设施（物理安全）、网络基础设施（网络安全）、IT 系统（系统安全），一直到信息和应用（应用安全）。此外，还包括人员和流程层面的安全控制，例如，职责分离和变更管理等。

如前文所述，在不同云服务模式中，提供商和用户的安全职责有很大的不同。例如，Amazon 的 AWS EC2 基础设施作为服务，供应商负责 Hypervisor 层以下层次的安全责任，这意味着它们只负责诸如物理安全，环境安全和虚拟化安全等这些安全控制。与之相应，用户则负责与 IT 系统（实例）相关的安全控制，包括操作系统、应用和数据。

Salesforce.com 的客户关系管理（CRM）SaaS 产品正好相反。由于 Salesforce.com 提供了整个服务，提供商不仅负责物理和环境安全控制，还必须解决基础设施、应用和数据相关的安全控制。这减轻了许多用户的直接运行责任。

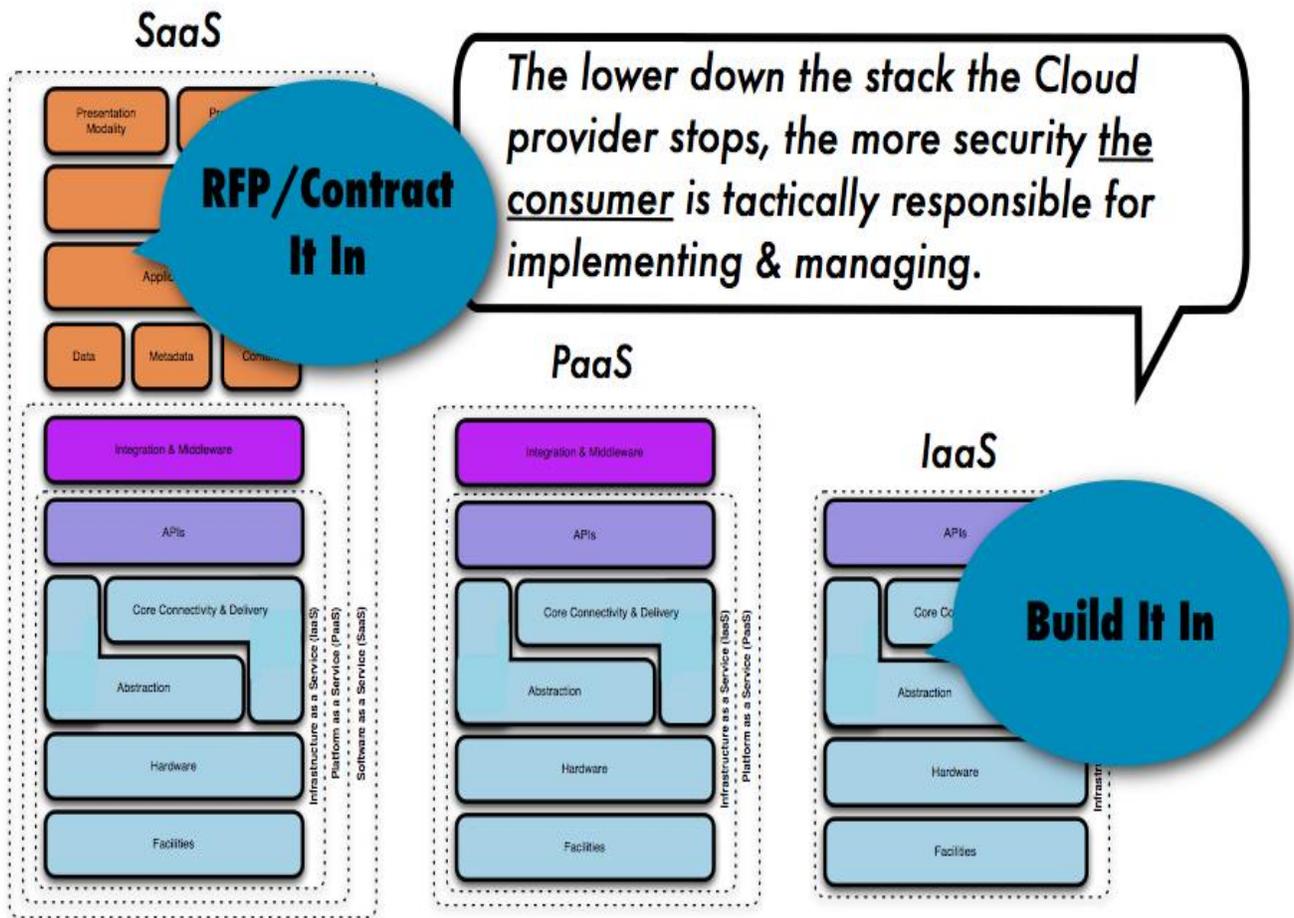
目前还没有一种方式，可以让一个没有经验的云服务用户简单地理解他/她的责任[虽然阅读本文将会提供帮助]，但 CSA 和其它组织正在努力进行与云审计相关的标准的制定。

云计算的吸引力之一在于由规模经济、重用和标准化带来的成本效益，为了支撑这种成本效益，云提供商提供的服务必须足够灵活，以服务最大可能的用户群、最大化他们的目标市场。不幸的是，将安全集成到这些服务方案中常会被认为使得方案变得僵化。

这种僵化往往体现在与传统 IT 相比，在云环境中无法获得同等的安全控制部署。主要原因是基础设施的抽象化、缺乏可视化和缺乏集成多种熟悉的安全控制手段的能力，特别是在网络层上。

下图说明了这些问题：在 SaaS 环境中，安全控制及其范围通过协商在服务合同中确认；服务等级、隐私和合规性等也都在合同中涉及。在 IaaS 环境中，底层基础设施和抽象层的安全防护属于提供商的职责，其它部分安全防护职责则属于客户。PaaS 介于两者之间提供了一个平衡，平台自身的安全防护转由提供商负责，而平台上应用的安全性及如何安全地开发这些应用则属于客户的职责。

图6：如何集成安全



理解这些服务模式间的差异造成的影响以及如何进行部署对于管理组织的风险状况是至关重要的。

1.5.3 架构之上: 关键关注领域

组成 CSA 指南的其它 13 个域着重介绍了云计算安全的关注领域，以解决云计算环境中战略和战术安全的“痛点”（pain points），从而可应用于各种云服务和部署模式的组合。

这些域分成了两大类：治理（governance）和运行（operations）。治理域范畴很广，解决云计算环境的战略和策略，而运行域则更关注于战术性的安全考虑以及在架构内的实现。

表 2a—治理域

域

指南涉及.....

治理和企业风险管理	<p>组织治理和度量云计算带来的企业风险的能力。</p> <p>例如违约的判决先例，用户组织充分评估云提供商风险的能力，当用户和提供商都有可能出现故障时保护敏感数据的责任，及国际边界对这些问题有何影响等都是关注点。</p>
法律问题：合同和电子举证	<p>使用云计算时潜在的法律问题。</p> <p>本节涉及的的问题包括信息和计算机系统的保护要求、安全漏洞信息披露的法律、监管要求，隐私要求和国际法等。</p>
合规性和审计	<p>保持和证明使用云计算的合规性。</p> <p>本节涉及评估云计算如何影响内部安全策略的合规性、以及不同的合规性要求（规章、法规等）。同时还提供在审计过程中证明合规性的一些指导。</p>
信息管理和数据安全	<p>管理云中的数据。</p> <p>本节涉及云中数据的识别和控制；以及可用于处理数据迁移到云中时失去物理控制这一问题的补偿控制。也提及其它项，如谁负责数据机密性、完整性和可用性等。</p>
可移植性和互操作性	<p>将数据或服务从一个提供商迁移到另一个提供商，或将它全部迁移回内部的能力。提供商间互操作性相关的问题也在这节讨论。</p>

表2b—运行域

域	指南涉及.....
传统安全、业务连续性和灾难恢复	云计算如何影响当前用于实现安全性、业务连续性和灾难恢复的操作流程和规程。关注点是讨论和检查云计算的潜在风险，希望增加针对企业风险管理模式巨大需求的对话和讨论。进而，本节还讨论了如何帮助人们识别云计算在哪些方面可以有助于减少安全风险，而在某些领域则增加了风险。
数据中心运行	如何评估提供商的数据中心架构和运行。主要关注帮助用户识别对持续服务不利的常见的数据中心特征，以及有助于长期稳定性的基础特征。
事件响应、通告和补救	适当的和充分的事件检测、响应、通告和补救。尝试说明为了启动适当的事件处理和取证，在用户和提供商两边都需要满足的一些条目。本域将会帮助您理解云给您现有的事件处理程序带来的复杂性。
应用安全	保护在云上运行或在云中开发的应用软件。包括将某个应用迁移到或设计在云中运行是否可行，如果可行，什么类型的云平台是最合适的（SaaS, PaaS, or IaaS）。
加密和密钥管理	识别恰当的加密使用方法以及可扩展的密钥管理。本节并不是什么规范，而是提供更多信息来探讨为什么需要这些方法，识别使用过程中出现的问题，包括保护对资源的访问以及保护数据。
身份和访问管理	管理身份和利用目录服务来提供访问控制。关注点是组织将身份管理扩展到云中遇到的问题。本节提供洞察评估一个组织准备就绪进行基于云的身份、授权和访问管理(IdEA)。
虚拟化	虚拟化技术在云计算中的应用。本节论述了与多租户、VM 隔离、VM 共居（co-residence）、Hypervisor 脆弱性相关联的风险。本域更关注系统和硬件虚拟化相关的安全问题，而不是对各种形式虚拟化的泛泛纵览。
安全即服务	提供第三方促进安全保障、事件管理、合规认证以及身份和访问监督。安全即服务是将安全基础设施的检测、修复和治理委托给一个具备恰当的工具和专业知识的可信第三方。这种服务的用户可以得益于在保护和加固敏感业务运作中获得专门的专业知识和前沿技术。

1.6 云部署模式

无论使用哪种服务模式（SaaS, PaaS, 或 IaaS），都有四种云服务部署模式并可以衍生变化以满足特定需求。

由于市场供给和客户需求的成熟，会衍生新兴的云部署模式，意识到这一点很重要。这方面的一个例子是“虚拟专用云” - 一种利用公共云基础设施中的私有或半私有的方式连接这些资源到用户数据中心的内部资源，通常是通过虚拟专用网络（VPN）连接。

设计“解决方案”时使用的架构思路，对将来方案的灵活性，安全性和流动性，以及协作能力都有明显的影响。依据经验，在四个领域中任意一个，其边界化(perimeterized)的解决方案效果都不如去边界化(de-perimeterized)的解决方案。

同样的道理，采取私有的还是开放的方案也需要仔细考量。

部署模式

- **公有云**: 云基础设施提供服务给一般公众或某个大型行业团体。并由销售云计算服务的组织所有。
- **私有云**: 云基础设施专为一个单一的组织运作。它可以由该组织或某个第三方管理并可以位于组织内部或外部。
- **社区云**: 云基础设施由若干个组织共享，支持某个特定的社区。社区是指有共同诉求和追求的团体（例如使命、安全要求、政策或合规性考虑等）。它可以由该组织或某个第三方管理并可以位于组织内部或外部。
- **混合云**: 云基础设施由两个或多个云（私有、社区、或公共）组成，以独立实体存在，但是通过标准的或私有的技术绑定在一起，这些技术促进了数据和应用的可移植性（例如，云间负载均衡的 cloud bursting 技术）。

1.7 建议

云服务的交付可以分为三种模式以及不同的衍生组合。这三种基本类型经常被称为“SPI”模型，其中 SPI 分别代表软件、平台和基础设施（作为服务）。

- **云软件即服务 (SaaS)**. 提供给用户的能力是使用服务商运行在云基础设施之上的应用软件。用户使用各种客户端设备通过“瘦”客户端接口，诸如浏览器等来访问应用（例如基于浏览器的电子邮件）。用户并不管理或控制底层的云基础设施，例如网络、服务器、操作系统、存储、甚至其中单个的应用功能，可能的例外是有限的用户特定的应用配置。
- **云平台即服务 (PaaS)**. 提供给用户的能力是在云基础设施之上部署用户创建或采购的应用，这些应用使用服务商支持的编程语言或工具开发。用户并不管理或控制底层的云基础设施，包括网络、服务器、操作系统、或存储等，但是可以控制部署的应用和应用程序托管的环境配置。
- **云基础设施即服务 (IaaS)**. 提供给用户的能力是云提供了处理、存储、网络及其它基础性的计算资源，以供用户部署和运行任意的软件，包括操作系统或应用软件。用户并不管理或控制底层的云基础设施，但是拥有对操作系统、存储和所部署的应用的控制，以及一些指定网络组件的有限控制（例如主机防火墙等）。

NIST 模型和本文并没有直接阐述新出现的云服务代理商相关的服务模式定义，这些提供商提供中介、监控、迁移/移植、治理、配置和集成服务，也提供用户和各云服务提供商之间关系的协调。

简而言之，由于创新会驱动快速的解决方案开发，用户和云服务提供商将会偏好诸如开发 API 和接口形式与云服务交互的各种方法。因此，云服务代理商将会成为整个云生态系统中重要的组成部分。

在通用、开放、标准化的长远解决方案出台之前，云服务代理商将各种不兼容的参数和接口进行抽象，为用户提供代理访问手段。所谓长远解决方案是指一种语义层面的功能，允许用户可以流畅和灵活地利用最能满足自己特定需求的模式。

同样重要的是要注意到出现了集中在开发开放和私有的 API 的许多努力，这些 API 用于云的管理、安全以及互操作。这些努力包括开放云计算接口工作组（Open Cloud Computing Interface Working Group），亚马逊公司的 EC2 API，Vmware 公司在 DMTF 提交的 vCloud API，Sun 公司的 Open Cloud API，Rackspace API 和 GoGrid API 等。开放的、标准的 API 会如同 DMTF 的开放虚拟化格式（OVF）这类通用容器格式一样，在云可移植性和互操作性方面将起到关键的作用。

目前有很多工作组、草案及已颁布的规范。在各种市场力量、用户需求和经济环境作用下会自然出现一个整合的过程，最终精简到更易于管理和互操作的状态。

1.8 要求

云服务呈现出的五个基本特征，表明了它们与传统计算方法的关系和区别：

- ✓ **按需自服务：**用户自己可以按需自动配置计算能力，例如服务器时间和网络存储，而无需与服务提供商的服务人员交互。
- ✓ **多种网络访问：**服务能力通过网络和标准的机制提供，促进瘦或胖客户端异构平台（例如移动电话、笔记本电脑和 PDA），以及其它传统的或基于云的软件服务的使用。
- ✓ **资源池化：**提供商的计算资源汇集到资源池中，采用多租户模式，按照用户需要，将不同的物理和虚拟资源动态地分配或重新分配给多个消费者使用。虽然存在某种程度上的位置无关性，也就是说通常用户无法控制或根本无法知道所使用资源的确切物理位置，但是原则上可以在更高抽象层面上来指定位置（例如国家、州、省、或者数据中心）。资源的例子包括存储、处理能力、内存、网络带宽以及虚拟机等。即使是私有的“云”，在同一组织内部不同部门往往也趋向将资源池化。
- ✓ **快速弹性扩展：**服务能力可以快速和弹性地供应，在某些情况下能自动地实现快速扩展、快速释放和回收。对于用户来说，可供应的服务能力近乎无限，可以随时按需购买。
- ✓ **服务可计量：**云系统通过利用计量参数在某种级别抽象恰当的服务类型（例如存储、处理、带宽或者活跃用户账号等）自动控制和优化资源的使用。资源的使用可以被监控、控制并生成报表，对提供商和用户双方都透明。

了解云架构对安全架构的影响的关键是通用和简洁的词汇，加上一致的产品分类，这样云服务和架构可以被解构，映射到补偿的安全和操作控制模型、风险评估框架和管理框架，反过来遵从标准。

在部署云计算服务时，了解架构、技术、流程和人力资本需求是如何变化或保持不变是至关重要的。如果对高层架构的影响没有一个清醒的认识，是不可能理性地解决那些细节问题。本节架构概述，以及 13 个其它关键领域，为读者评估、运作、管理和治理云计算环境的安全提供了坚实的基础。

参考资料

- [1] NIST 云计算定义
NIST 500-292 “NIST Cloud Computing Reference Architecture”
- [2] NIST 云计算定义和 API 主页
www.cloud-standards.org
- [3] Jericho Forum 云立方模型
www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf



第二部分 // 云的治理

D2: 治理与企业风险管理

云计算中的治理和企业风险管理的基本问题关系到识别和实施适当的组织架构、流程及控制来维持有效的信息安全治理、风险管理及合规性。组织还应确保在任何云部署模型中，都有适当的信息安全措施贯穿于信息供应链，包括云计算服务的供应商和用户，及其支持的第三方供应商。

一个有效的云计算治理和企业风险管理方案源于完善的信息安全治理流程，作为组织整体企业治理责任的一部分应给予足够的重视。完善的信息安全治理流程要求信息安全管理程序支持业务的可扩展性，在整个组织中可重复执行、可测量、可持续、可防御、可持续改进，并具有持续的成本效益。

在云计算部署中，治理都将是云服务提供者和客户之间协议的主要内容。在定制的情况下，每一条款都需进行详尽的斟酌和协商。对于较大规模的客户或供应商，需要在细节关注和可扩展性之间进行权衡。可视特定工作负载的重要程度或风险价值来排定优先顺序（例如，响应时间和可用性对于邮件系统比 HR 系统更加重要）。随着云计算的不断成熟，CloudAudit 或 STAR 会提供更加标准的治理方法，并更具有可扩展性。

概览 本控制域主要讲述：

- 治理
- 企业风险管理

本章节映射到云控制矩阵控制点 DG-01 、 IS-02 、 GRX-XML 和 CloudAudit 以建立补偿控制。

2.1 公司治理

公司治理包括一整套流程，技术，习惯，政策，法律和机构，影响企业的指引、管理或控制。公司治理同时还包括管理众多利益相关者与企业目标之间的关系。良好的公司治理的基础，是基于承认股东作为公司实际拥有者的权利，以及高管作为受托方的模式。公司治理的模型众多,但是都遵循以下五项基本原则：

- 供应链审计
- 董事会及管理层架构和流程
- 公司责任与合规（承诺）
- 财务透明和信息披露
- 股权结构和控制权的践行

客户决定选择某公司的一个关键因素是相信他们的期望可以在这里得到满足。对于云计算服务，多个服务的相互依赖关系使客户难以理清责任方。如果客户对某厂商信心不足，该厂商获得合同的可能性将会很小。如果这成为一个普遍性问题，对单个厂商失去信心会连累到其他厂商，市场不健康的发展会增加意外发生和厂商更迭的可能性。

利益相关者需要仔细考量监控机制对公司持续稳定和增长是适宜和必要的。

2.2 企业风险管理

企业风险管理（ERM）植根于每个组织向股东提供价值的承诺。所有的业务都存在不确定性，管理层的挑战之一是决定一个组织如何测量、管理和降低不确定性。不确定性既是机遇也是风险，可能增加或减少组织及其战略的价值。

信息风险管理是识别和理解风险暴露、风险管理能力以及数据所有者风险偏好和承受能力。因此，这是基本的决策支持工具，以便持续投入以保护信息资产的保密性、完整性和可用性。

公司业务风险管理包括组织管理风险和机遇所使用的方法和流程。在云计算环境中，管理者为识别和分析出来的具体风险选择某种风险处置策略，其中可能包括：

- 避免：退出引起风险的活动
- 减少：采取措施减少相关风险的可能性或影响
- 分担或保险：用财务方式来转移或分担一部分风险
- 接受-基于成本/收益的考虑不采取行动

风险管理本质是一个平衡过程，实现目标未必需要减少不确定性或波动，而是根据风险偏好和战略一致的前提下，实现价值最大化。

在任何云的选择或方案当中，存在许多的不确定性、收益和风险，这些都会影响到从风险或业务收益的角度决策是否应用云计算服务。每一家公司都必须权衡这些不确定性以决定是否采用云计算解决方案。

云计算为企业带来许多好处，包括：

- 优化资源利用率
- 为云计算租户节约成本
- 转换资本开销
- 资本开销（CAPEX）转化为运营成本（OPEX）
- 客户的 IT 动态扩展能力
- 缩短新应用程序开发或部署的生命周期
- 缩短了新业务实施的时间

**本章节映射到云控制矩阵控制点
DG-08 和 ISO31000 的使用，ISF 和
ISACA 指引以建立补偿控制。**

用户应该将云服务和安全视为供应链安全问题。这意味着需要最大程度地检查和评估服务提供商的供应链（服务提供商的关联和依赖关系）。这也意味着需对服务提供商自身的第三方管理进行审查。对第三方服务提供商的评估应具体指向服务提供商在事件管理、业务连续性和灾难恢复等方面的策略、流程和规程；还应包括对共用场地（co-location）和备份设施的审查。这应包括审查提供商是否遵从其自身策略和规程的内部评估，评估服务提供商在这些领域为其控制的绩效和有效性提供信息的指标体系。

事件信息可以在合同、服务等级协议（SLA）或其他共同协议中进行定义，能进行自动或定期的沟通,并直接进入报告系统或传递给关键人员。关注等级和监督程度与风险价值相关-如果第三方无法直接访问企业数据，风险水平会显著下降，反之亦然。

使用者应审阅风险管理流程和他们的服务提供者的治理并确保实践情况与之保持一致。

2.3 许可

Permissions

- 采用一个已建立的风险框架以便监控和度量公司风险。
- 采用风险管理效果衡量的指标（例如，SCAP⁵、CYBEX⁶或者 GRC-XML⁷）
- 确立以风险为核心的公司治理观点，高管层作为股东和利益相关人在供应链中的受信方角色。
- 从法律角度确立一个框架用来应对不同司法管辖区的差异。

2.4 建议

- 部分从云计算服务节省的费用须投资到提升服务提供商的安全能力、应用的安全控制和正在进行的详细评估和审计检查中，以确保能够持续满足需求。
- 用户组织应审查包括具体的信息安全治理架构和流程，及具体的信息安全控制，作为未来服务提供商组织的尽职调查（due diligence）的一部分。应根据用户信息安全管理流程的连续性、充足性、成熟度来评价服务提供商的安全治理流程和能力。服务提供商的信息安全控制应基于风险并明确地支持这些管理流程。
- 用户和服务提供商之间的协同治理架构和流程是很必要的，既是服务交付（services delivery）的设计和开发的一部分，也是风险评估和风险管理协议，最终作为服务协议的一部分。
- 在签订服务水平协议（SLA⁸）及合同契约义务时应包括安全部门，来确保安全需求在合同层面上是可强制执行的。

⁵ SCAP-安全内容自动化协议

⁶ CYBEX-网络安全信息交换框架

⁷ GRC-XML-实现并加强不同支持 GRC 功能技术之间信息共享的技术标准。

⁸ SLA: Service Level Agreement，服务水平协议

- 在迁移进云端前，衡量信息安全管理有效性和效果的指标体系和标准都应建立起来。至少，组织应理解并记录他们当前的指标，及运营迁移至云计算平台时，这些指标会如何变动，因为云计算服务提供商可能使用不同的（有可能不兼容）指标。
- 由于许多云计算部署中缺少对基础设施的物理控制，因此与传统的企业拥有基础设施相比，服务水平协议(SLA)、合同需求及提供商文档化在风险管理中会扮演更重要的角色。
- 由于云计算中的按需提供和多租户特点，传统形式的审计和评估可能并不适用，或需要更改。例如，一些服务提供商限制脆弱性评估和渗透测试，而其他的则限制提供审计日志和实时监控数据。如果这些在内部策略中都是要求的，那么就需要寻找替代的评估方法、某些具体的合同免责条款，或寻找与风险管理需求更一致的服务提供商来替代。
- 如果对组织的关键功能使用云服务，风险管理方法应该包括识别和评估资产，识别和分析威胁和脆弱性，及威胁和脆弱性对资产（风险和事件场景）的潜在影响，分析事件/场景的可能性，管理层批准的风险接受水平和标准以及多种风险处置（控制、避免、转移、接受）计划的开发。风险处置计划的结果应作为服务合约的一部分。
- 服务提供商和用户的风险评估方法中的影响分析标准和可能性定义需保持一致。用户和服务提供商应共同开发云服务的风险场景，这应该固化在服务提供商为用户服务的设计中和用户的云服务风险评估中。
- 由于云计算及其服务提供商不断变化的状况，应考虑服务提供商的风险，例如，服务提供商的商业生存能力，数据和应用程序的可移植性和互操作性。
- 资产清单应盘点支持云服务且在服务提供商控制下的资产。用户和服务提供商的资产分类和分级方案（valuation scheme）应一致。
- 服务提供商及其服务都应该是风险评估的重点。云服务的使用、采用的特定服务和部署模式，都应该与组织的风险管理目标及业务目标一致。
- 不论是什么服务或部署模式，云计算服务的用户和服务提供商都应参与构建健全的信息安全治理。信息安全治理应由用户和服务提供商协作来达到支持业务使命和信息安全的目标。服务模式可以调整协同信息安全治理和风险管理中定义的角色和职责（基于各自对用户和服务提供商的控制范围），部署模式可能定义责任和预期（基于风险评估）。
- 云服务的用户应询问管理层对云服务风险和可接受残余风险的容忍程度是否已经有所定义。
- 如果服务提供商不能证明其服务具备全面有效的风险管理流程，用户应详细评估该服务提供商，以及是否使用用户自身的能力来补偿潜在的风险管理差距。
- 组织应为服务提供商制定基于业务和技术风险的风险指标。这些风险指标应包括数据涵盖类型，不同用户类型的相关信息，以及厂商和其他对手的相关信息。

2.5 要求

- ✓ 向利益相关方和股东保持透明度，并证明财政偿付能力和组织透明。

- ✓ 正视在云计算供应链相互依存的风险并与供应链各方沟通企业的风险状况，随时准备向消费者和依赖方告知风险情况。
- ✓ 检查和统计从其他云计算供应链继承的风险，采取积极的措施来降低风险并通过运营控制风险。

D3: 法律问题：合同与电子发现

本域强调由云计算所引起的一些法律方面问题。本章提供将数据迁移到云上可能引起法律问题的一般背景、在云服务协议中要考虑的一些问题，以及在西方国家诉讼体系内电子发现（Electronic Discovery）所提出的特殊问题。

本域仅就所选择的问题提供概述，并不能替代您获得法律上的建议。

概述：本域将解决如下主题：

- 将数据迁移到云上所引起特殊法律问题的概述
- 云服务协议的考虑内容
- 电子发现引起的特殊问题

3.1 法律问题

纵观全球，众多国家有着不计其数的法律、法规以及其它的命令，它们要求公共组织和私营机构要保护个人数据的隐私性、信息和计算机系统的安全性。例如，在亚太地区、日本、澳大利亚、新西兰以及许多国家已经通过数据保护法律。这些法律要求数据的控制人依据经合组织（Organization for Economic Cooperation and Development，简称 **OECD**⁹）的隐私及安全指导意见，以及亚太经合组织（Asia Pacific Economic Cooperation，简称 **APEC**¹⁰）的隐私框架采用合理的技术、物理和管理措施来防范个人数据遭受丢失、滥用或是篡改。

在欧洲，欧洲经济区（**EEA**）¹¹成员国家已经制定数据保护法律，该法律延续了 1995 年的欧盟 European Union (EU) Data Protection Directive¹²数据保护指令、以及 2002 年的电子隐私指令（ePrivacy Directive，其在 2009 年得到修正）中阐述的准则。这些法律包含安全的组成部分，并必须将提供充分安全的职责传递给分包商。其它与欧洲经济区有紧密联系的国家，例如非洲的摩洛哥和突尼斯、中东的以色列和迪拜也已通过遵循同样准则的类似法律。

北美、中美以及南美国家也正在以快速的步伐通过数据保护法律。这些国家的法律都包括安全方面的要求，并且将确保个人数据防护和安全的重担放在了数据保管人身上。无论这些数据位于何处，特别是当向第三方传输时。譬如，除了加拿大、阿根廷以及哥伦比亚的数据保护法律已经出台多年外，最近墨西哥、乌拉圭和秘鲁也通过了数据保护法律。这些法律都主要受到欧洲模式的启发，并且也可能包括对亚太经合组织隐私框架的引用。

在日本，个人信息保护法案要求私营企业保护个人信息以及数据的安全。在医疗行业有行业特定的法律，如医疗从业者法案、公共健康护士法案、助产士和护士法案以及药剂师法案，这些法案要求注册的医疗职业人员对病人的信息进行保密。

⁹ **OECD** - Organization for Economic Cooperation and Development

¹⁰ **APEC** - Asia Pacific Economic Cooperation

¹¹ **EEA** - European Economic Area

¹² EU Directive 95/46/EC

在美国开展业务的组织可能受制于一个或多个数据保护法律。这些法律要求组织为他们分包商的行为负责。譬如，金融服务现代化法案（Gramm-Leach-Bliley Act (GLBA)¹³）或是 1996 年发布的医疗保险及责任法案（Health Insurance Portability and Accountability Act，简称 HIPAA）要求组织以书面合同的形式迫使他们的分包商采用合理的安全措施，并且遵守数据隐私条款。政府机构、例如联邦贸易委员会（Federal Trade Commission，简称 FTC）或是美国司法部长一致同意组织对他们分包商的行为负有法律责任。支付行业数据安全标准（Payment Card Industry PCI Data Security Standards，简称 PCI DSS）适用于世界上任何地方的信用卡数据，包括由分包商处理的数据也有类似的要求。

以下部分就个人数据被传输到云中、或是在云中处理时可能引发与之相关的法律问题提供一些例子。

表一 强制性要求

问题	描述
美国联邦法	美国众多的联邦法律以及相关的规定，例如 GLBA、HIPAA、1998 年的儿童在线隐私保护法案（Children's Online Privacy Protection Act，简称 COPPA），它们与由联邦贸易委员会发布的命令共同要求公司在处理数据时采取专门的隐私和安全措施，从而在他们与第三方服务提供商的合同中要求类似的预防措施。
美国州法	美国众多的州法也要求公司有义务为个人数据提供充分的安全保护，并要求他们的服务提供商做同样的事情。解决信息安全问题的州法通常至少要求公司与服务提供商的书面合同里有合理的安全措施条款。例如可参见马萨诸塞州的安全法规下的广泛要求。
标准	例如像 PCI DSS、或是 ISO 27001 这样的标准也引发类似联邦法以及州法那样的多米诺骨牌效应。受制于 PCI DSS、或是 ISO 27001 标准的公司必须遵守特定的标准，并同时将类似的义务传达给他们的分包商以便满足受制约的这些标准。
国际性规章	许多国家已经通过遵循欧盟模式、经合组织或亚太经合组织模式的数据保护法律。在这些法律下，数据的控制人（通常是与个人有主要关系的法律主体）对收集和处理的个人数据负有责任，即使是在第三方处理数据的情况下。数据的控制人被要求确保任何代表它处理个人数据的第三方采取充分的技术、组织架构上的安全措施来保护数据。
合同责任	<p>即使未被规定要采取具体的活动，公司合同上可能有责任保护他们的顾客、联系人或是雇员的个人信息，以确保这些数据未被挪作他用、以及未泄漏给第三方。譬如，这个责任可能来自公司在其 Web 站点上发布的条款和隐私声明。</p> <p>此外，公司可能与它的客户签订合同（例如服务协议），在合同中对数据保护（个人或公司的数据）、使用限制、确保安全性、使用加密等做出具体的承诺。</p> <p>组织必须确保当由其监管的数据位于云中时，它会具备持续的能力满足在隐私性通告、或其它合同内所做出的许诺和承诺。</p>

¹³ GLBA - Gramm-Leach-Bliley Act

	<p>例如，公司或许已经同意数据只能用于特定的用途。在云中的数据必须只能用于它们被收集的目的。</p> <p>如果隐私性通告允许这些个人数据的主体访问他们的个人数据、修改或是删除信息，云服务提供商也必须允许其与在非云服务关系下同程度地行使访问、修改和删除的权利。</p>
<p>针对跨国界数据传输的禁令</p>	<p>在全世界有许多法律禁止、或是限制信息传出该国。在大多数情况下，只有当接收信息的国家提供对个人信息、以及隐私权充分的保护时才允许信息传输。该充分保护要求的目的在于：确保那些跨国界被传输到别国数据的个人数据主体可以享有类似的、或是不低于数据传输前所在国家能够提供的隐私权利和隐私保护。</p> <p>因此对于云计算用户来说，知晓其雇员、客户以及其他人的个人数据将位于何处是重要的，以便能解决国外的数据保护法律可能施加给其的特定限制。</p> <p>依国家而定，确保该充分保护的要求可能是复杂的和严格的。在某些情况下，可能需要首先获得当地数据保护专员的许可。</p>

3.2 合同考虑

当数据被传输到云中后，保护数据以及确保其安全通常是数据收集人或保管人的职责，即使在某些情况下这个责任可能与他人共享。当数据的保管人依赖第三方来持有或是处理数据时其对于任何数据的丢失、损坏或滥用仍然承担责任。数据的保管人与云服务提供商签署一份书面的（法律）协议是慎重的，并且可能是法律上需要的。该协议清晰地定义双方的角色、彼此的期望，以及在双方之间分配与数据利害攸关的众多职责。

上述讨论的法律、法规、标准以及相关的最佳实践也要求数据保管人进行尽职调查（在执行合同前）或安全审计（在合同履行期间），以确保这些责任得到履行。

3.2.1 尽职调查

在签署云计算服务协议前公司应该评估自身的常规做法、需求以及限制条件，以便辨识与提议的云计算业务有关联的法律障碍和合规要求。譬如，它应该判断自身的业务模型是否允许使用云计算服务，以及在哪些情况下允许。业务的本质可能是任何放弃对公司数据的控制会受到法律的限制、或是导致公众产生严重的安全关切。

此外公司应该、并且在某些情况下可能是在法律上被要求对提议的云服务提供商进行尽职调查，以便判断是否其提供的服务能允许公司继续履行保护资产的职责。

3.2.2 合同

双方必须签署书面的合同。根据服务的性质，合同通常可能是以点击协议的方式（click-wrap agreement）。此类合同是不可协商的，或是双方为特定的情况量身定造、协商一份更为复杂的书面文档。如果点击协议是唯一可用的协议，云服务客户应该对比云服务提供商承诺的实际收益、财务的节省和易于使用这些因素来权衡放弃协

商的风险。如果双方能够协商合同，他们应该确保在合同期内、以及合同结束后该合同的条款解决双方的需要和职责。双方应该协商详尽的、全面的条款，解决那些在云环境下运作所带来的独有需求和风险。

如果这些问题没有在合同中得到解决，云服务客户应该考虑达成该目标的备选方法，如寻找备选厂商或是不把数据传送到云中。例如，如果云服务客户打算发送 HIPAA 法案涵盖的信息到云中，他们将需要寻找愿意签署 HIPAA 职责相关协议的云服务提供商、或是根本不将数据传送到云中。

以下是一些“云”具体问题的简要描述。此外，附加的检查列表提供了评审云服务合同时需要考虑的一份综合的(但不是包罗万象的)问题清单。

3.2.3 监控、测试和更新

云计算环境不是静态的。它在不断进化并且各方必须与之适应。建议对云服务进行定期的监控、测试和评估，以确保服务提供商采取了要求的隐私及安全措施，并且流程和策略得到遵循。此外，法律、法规以及技术的形势很可能以迅速的节奏发生变化。必须及时地解决新兴的安全威胁、新出现的法律和合规要求。各方必须与法律和其它要求齐头并进，并且确保运营保持在遵守可适用的法律之下；而且随着新的技术和法律浮现，要确保也有不断随之进化的到位的安全措施。

云审计以及云信任协议是自动监控和测试云供应链的两个机制。此外，国际电信联盟远程通信标准化组（ITU-T）正在致力于 X.1500 云审计规范，后者在被提及时通常被称作“网络安全信息交换框架”（Cybersecurity Information Exchange Framework，简称 CYBEX）。

3.3 电子证据发现引起的特殊问题

本节讨论的是美国诉讼的特殊要求。美国诉讼很大程度上依赖于文档为案件辩护。与其他大多数国家形成巨大反差的是，美国司法系统的特殊性是当事人必须提供给对手涉及到案件的所有文档。不仅必须提供有利于自己的文档，还必须提供有利于对方当事人的文档。

近年来，已经有不少诉讼当事人被指控自行删除、丢失、或修改不利于自己的重要证据的丑闻。因此，议事规则也已变更来明确当事人的义务，尤其针对数字信息(ESI)。

由于云计算将成为诉讼或调查中所需要的数字信息的仓库，云服务提供商和他们的客户必须仔细规划如何识别案件涉及的所有文档，为了能够满足联邦民事诉讼规则中电子证据发现条款的严格要求，各州也要与这些法律条款相吻合。

在这点上，云服务的客户和供应商需要考虑下列问题，当面对一个客户的发现请求，并且可能相关的数据存在于云服务提供商。

3.3.1 管有、保管与控制

在美国的大多数司法管辖区，各方生成相关信息的义务仅限于在其管有，保管或控制的文档和数据。相关的数据托管在第三方，即使是云服务提供商，一般也不免除一方当事人生成信息的义务，因为它可能有法律权利查阅或获得这些数据。然而，并非所有托管在云服务提供商的数据会在客户的控制下（例如，灾难恢复系统，云服

务提供商用于运行环境创建和维护的某些元数据)。区分哪些数据提供或不提供给客户可能牵涉到客户和供应商的利益。云服务提供商作为信息生成的云数据处理者,其法律程序方面的义务是每个司法管辖区亟待解决的遗留问题。

3.3.2 相关的云应用和云环境

在某些诉讼和调查中,实际的云应用程序或云环境本身可能与解决诉讼或调查的纠纷有关。在这种情况下,云应用程序和云环境可能超出客户的控制,用户直接对供应商发出传票或其他的电子证据发现过程。

3.3.3 可搜索性和电子证据发现工具

由于在云环境中客户可能无法和在自己的环境中一样申请或使用电子证据发现工具。此外,客户可能没有管理权限搜索或访问托管在云中的数据。例如,客户可以立即访问在自己服务器上的员工的电子邮件帐户,访问托管在云计算中的电子邮件帐户可能就不具备这种能力。因此,客户需要考虑导致受限访问潜在的额外的时间和费用。

3.3.4 保持 (Preservation)

一般来说,在美国一方有义务采取合理的措施防止在其管有、保管或控制的数据或信息被破坏或修改,它知道或理应知道保持数据或信息是有关于悬而未决或合理预期的诉讼或政府调查。根据客户使用的云服务和云部署模式,在云中保持与在其他 IT 基础设施中保持非常类似,也可以更复杂。

在欧盟,信息保持由欧洲议会和欧盟理事会 2006 年 3 月 15 日的指令 2006/24/EC 管辖,日本,韩国,新加坡也有类似的数据保护措施。在南美,巴西和阿根廷分别有阿泽雷多条例草案,阿根廷数据保留法 2004,以及 2004 年 2 月 6 号的 25.873 号法令。

3.3.4.1 成本和存储

保持可以要求延长大规模数据的保留。根据服务等级协议这样的后果是什么?如果保持要求超出服务等级协议的条款,会发生什么情况?如果客户继续保持数据,谁支付延时存储,以及以怎样的代价?客户是否有在服务等级协议下的存储容量?客户可以有效地以友好的方式下载数据,从而可以离线或近线保持数据?

3.3.4.2 保持范围

没有好的原由或具体需求,请求方仅有权访问托管在云中包含相关信息的数据,而不是所有在云中或应用程序中的数据。然而,如果客户没能以粒度方式保持相关信息或数据,可能需要过度保持 (over-preserve) 作为合理的保持,取决于诉讼或调查。

3.3.4.3 动态和共享存储

如果客户有空间来容纳数据,保持云中数据的责任可能相对适中的,数据是相对静态的,访问的人是有限的,而且知道保持数据。然而,在云环境中以编程方式修改或清除数据,或与没有意识到数据需要保持的人共享,保

持变得更加困难。当客户明确这些数据是相关的，而且需要保持的，客户可能需要与供应商合作，以确定合理的方式来保持这些数据。

3.3.5 收集

由于可能缺乏管理控制，客户收集来自云中的数据比收集防火墙后面的数据更困难，更耗时，更昂贵。特别是客户对其云中的数据可能不具有相同的能见度水平，和收集在云中的数据相比，可能有更多的困难来确定接口的完整性和准确性。

3.3.5.1 接入和带宽

在大多数情况下，客户访问其在云中的数据将取决于服务等级协议。这可能会限制其快速、以良好的方式（即所有合理相关的元数据保持）收集大量数据的能力。客户和云服务提供商尽早地考虑了这个问题，在诉讼和调查允许收集的情况下，为额外的访问建立协议（和成本）。如果没有这些协议，当请求方和法院交涉时，客户应考虑在云中收集带来的额外的时间和成本。

3.3.5.2 功能

关于接入和带宽是不同的。客户的访问权可以提供全方位的数据访问，但不提供在一个给定情况下更好地帮助他们的功能。例如，客户可访问三年的零售交易数据，但可能仅是由于功能限制，只能每 2 周下载一次数据。此外，客户可能无法看到所有实际存在的元数据的完整视图，而只是更有限度的元数据。

3.3.5.3 取证

“云”数据源的位逐位镜像通常是困难或不可能的。为了安全起见，供应商不愿允许访问他们的硬件，特别是在多租户环境中客户能访问到其他客户的数据。即使在私有云中，取证也非常困难，客户可能需要将这些限制通知对方律师或法院。幸运的是，取证在云计算中很少批准，而不是因为它是云计算，但由于它通常是一个结构化数据层次或虚拟化，本身不适合取证分析。

3.3.5.4 合理的完整性

客户面对请求发现应采取合理的措施以验证其从云供应商的收集是完整和准确的，尤其在日常业务流程不可用的情况和具体诉讼的措施被用来获取信息。这个过程除了验证都是独立的，存储在云中的数据是准确的，经过验证的，或可采纳的。

3.3.5.5 无法合理访问

由于客户存储的数据及客户的访问权限和特权存在差异，并非客户在云中的所有数据都可访问。客户（和供应商）应该分析信息的要求和相关数据结构的相关性，物质性，均衡性和可访问性。

3.3.6 直接访问

在云环境外，请求方对相应方的 IT 环境的直接访问是不支持的。在云环境中，更不被支持，可能和取证一样不现实。重要的是，客户可能无法提供直接访问是因为硬件和设施超出其管有、保管或控制，请求方需要传唤，或直接与供应商协商。

3.3.7 本地生成

云服务提供商通常把数据存储在中不受客户控制的高度专有的系统和应用程序中。原始格式的数据生成对请求方可能是无用的，因为他们将无法了解的信息生成。在这种情况下，可能最好的是要求所有有关方，包括生产方和供应商，相关信息的接口使用云计算环境中标准的报告或接口协议。

3.3.8 认证

认证在这种情况下是指对被接纳为证据的数据的取证鉴定。这不应该被混淆为用户认证，用户认证只是身份管理的一个组成部分。将数据存储在中不影响数据验证的认证分析，以确定数据是否应被接纳为证据。现在的问题是该文档是否是它所声称的。电子邮件不会因为它是存储在在公司防火墙后面或存储在云中而被认为更可信或更不可信。问题是它是否被完整的存储以及法院能否相信从它被发送或接收后没有被改变。

3.3.9 受理和信誉

如果没有其他证据，如篡改或黑客攻击，文件不应仅仅因为它们被创建或存储在云中就被认为更可信或者更不可信。

3.3.10 在电子证据发现方面供应商与客户之间的合作

供应商和客户最好从合作的一开始就考虑（电子）发现导致的复杂度并在服务等级协议中说明，这符合他们的共同利益。供应商可能要考虑设计包括发现服务的优秀云产品来吸引客户（“发现设计”）。无论如何，客户和供应商应该考虑包含一项协议，对任何发现请求事件合理的相互配合。

3.3.11 响应传票或搜索批准

云服务提供商可能被第三方以传票、搜查令或法院命令的形式要求其提供信息，获得对客户数据的访问请求。客户可能希望能对抗访问请求以实现数据的保密性和秘密性要求。为此，云服务协议应要求云服务提供商把收到传票的信息通知公司，并给公司时间来对抗访问请求。

云服务提供商可能受到诱惑答应开放其设施，并提供请求者访问请求中的任何信息。在这样做之前，云服务提供商应确保请求要求是在良好的秩序下，并采用适当的法律方法。云服务提供商在披露其保管的信息前应认真地分析要求。

复杂的法律适用取决于信息的具体性质，它的位置等。例如，访问电子邮件内容的请求适用不同的规则，这取决于电子邮件是否已经被打开，以及如何长期存储电子邮件。如果信息请求是电子邮件的内容，或只有交易数据的电子邮件适用不同的规则(例如，什么时候发送，发送给谁)。

参考文献

International Treaties and Agreements

- [1] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).
- [2] OECD Guidelines for the Security of Information Systems and Networks (2002).
- [3] OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy.

Publications

- [4] GILBERT, Françoise. © 2009-2011. Global Privacy & Security. Aspen Publishing / Wolters Kluwer (2 volumes).
- [5] GILBERT, Françoise. 2011. Cloud Service Providers Can Be Both Data Processors and Data Controllers (BNA Privacy & Security Law Report 10 PVLR 266 (2011). Journal of Internet Law, Volume 15, Number 2, page 3.
- [6] POWER, Michael E. AND TROPE, Roland L. 2005. Sailing in Dangerous Waters: A Director's Guide to Data Governance. American Bar Association.
- [7] SMEDINGHOFF, Thomas. 2008 Information Security Law: Emerging Standard for Corporate Compliance (ITGP).

Websites

- [8] Cloud computing definitions and business models:
http://p2pfoundation.net/Cloud_ComputingDefinition (technical aspects, business models)
- [9] Cloud Computing Incidents Database:
http://wiki.cloudcommunity.org/wiki/CloudComputing:Incidents_Database (Records and monitors verifiable, noteworthy events that affect cloud computing providers, such as outages, security issues, and breaches)

D4: 合规与审核

组织将其业务从传统数据中心迁移至云计算数据中心的选择将使其面临新的安全挑战，其中最重要的挑战之一即遵从众多监管条例对交付、度量和通信的合规约束。云计算服务用户和供应商需要理解和掌握当前合规和审核标准、过程和实践的区别和意义。云计算分布式和虚拟化的特性需要基于具体化的信息和过程实体进行重大的框架调整。

集中化和统一化的管理平台使云计算本身具备提升透明度和保障能力的潜力。此外，云服务供应商提供的外包方案降低了合规对规模的依赖程度。原本在云计算时代之前成本高昂的企业合规，将由于云服务供应商能够第一时间提供合规解决方案，使得企业（盈利性和非盈利性）能够获得市场准入开展业务。政府和其他原本抵触 IT 运维外包的组织考虑到安全性和合规性，将更积极采用云计算模型，其部分合规性需求将通过合约义务而满足。

此外对于云服务供应商和用户来说，其监管和审核机构也正在逐渐适应云计算这一新领域。仅有少量法律法规是面向虚拟化环境或者云部署模型的安全性证明而编写。云计算用户在向审核机构证明组织合规时将存在挑战。理解云计算与监管环境的相关性将是任何“云”战略的关键因素。云计算用户务必考虑并且理解以下几点：

- 针对特定的云服务或者服务提供商的监管含义，对适用跨境或者多管辖权的事例给予特别关注
- 云服务提供商和用户的合规责任分配，包括间接提供商（如你所采用云服务提供商的云服务提供商）
- 云服务提供商的合规呈现能力，包括及时的文档生成，证据产生以及过程合规
- 用户、服务提供商以及审核机构（用户和服务提供商双方）的关系，以确保按照需要的访问权（适当限制）并与治理要求相对应

概览 本章阐明如下主题：

- 合规
- 审核

4.1 合规

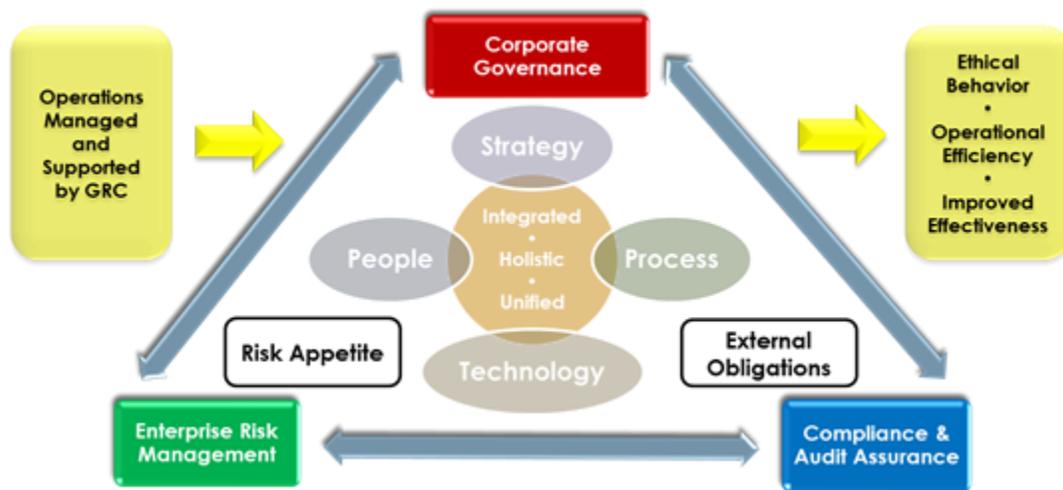


Figure 1—GRC Value Ecosystem

- **公司治理：**一个组织在股东，董事会和管理层之间达成控制平衡，能提供管理的一致性，方针、指南和控制项的结合应用，并支持有效地决策
- **企业风险管理：**组织采用方法和过程（框架）来确保作出平衡的决策，该决策基于对组织目标（风险和机遇）相关的特定事件和场景的识别，可能性和影响级别评估，响应策略的采取，进展监控，从而保护和创造股东价值
- **合规性和审核保证：**通过评估合规状态来对企业义务（企业社会责任、道德标准，适用法律，法律法规，合约，战略和方针）的感知和遵循，评估风险和违规成本以及达成合规的开销，从而对必要纠正措施进行排序、储备和发起。

“云”所使用的信息技术受到日益增多的方针和法律法规约束。所有的股东期望组织主动遵守多重的监管准则与要求。IT 治理对于满足相关要求是有必要的，同时，所有组织也需要采取战略来实现相关要求。

治理包括在外部环境约束下能够顺利达成组织目标的流程和方针。治理对合规活动提出要求，以确保运营完全满足上述流程和方针。从这层意义上说，合规的重点与外部要求相匹配（法律法规，工业标准），而治理则是与内部要求相匹配（董事会决定、企业方针）

合规可定义为对企业义务（企业社会责任、适用法律，道德指南）的感知和遵循，包括对适当和必要的纠正性措施的评估和排序。在某些高度监管的环境下，透明度可以对内部特定策略进行补充，成为组织效率的优势而非制约。

法律法规通常对信息技术和其治理来说意义重大，特别在监控、管理、防护和发布等方面。IT 治理是企业总体治理、企业风险管理、合规和审核/保障的支撑要素。

“云”成为治理和合规的辅助技术，通过管理平台尤其是内部管理云实现集中化控制和透明度。透过云服务的影响，一定规模以下的组织可以与规模更大，资源优势更明显的企业达成同等级别的合规。安全和保障服务成为第三方参与合规评估和通信的一种方法。

任何合规方法都将需要包括 IT 部门在内的整个组织参与。外部供应商所承担的角色需要仔细思考，承担将其直接或者间接纳入治理的责任，并在用户组织内清晰地实现分配。

此外，以下标准分别代表了 ISO/IEC 和 ITU-T 发布的云安全标准：

- ISO/IEC 27017: 云计算安全和隐私管理系统安全控制
- ISO/IEC27036-x:众多标准涉及供应商关系管理信息安全，后续计划将作为云供应链的一部分纳入。
- ITU-T X.ccsec:通信领域云计算安全指引
- ITU-T X.srfcts:基于云的通信服务环境安全要求和框架（X.srfcts）
- ITU-T X.sfcse :软件即服务（SaaS）应用环境安全功能要求

4.2 审计

适当的组织治理顺理成章地包含审计与保证。必须独立地实施审计，并且应该坚定地设计审计以便表现出最佳实践、恰当的资源，以及经过检验的协议及标准。

对于客户和服务提供商而言，内审和外审以及各种控制措施都是合情合理的、可为云计算效力的角色。在引入云计算的起步阶段，更多的透明度可能是增加利益相关者舒适度的最佳选择。审计是提供保证的方法之一，其保证运营风险管理活动得到彻底地检验和评审。

组织最高级别的治理要素（例如董事会和管理层）应该采纳并支持审计计划。对至关重要的系统及控制进行定期且独立的审计，包括伴随的审计记录和文档将会支持提升效率和可靠性。

许多组织使用成熟度模型（例如 CMM、PTQM）作为分析流程有效性的框架。在某些情况下更多采用的是统计性的风险管理方法（例如用于金融服务的巴塞尔协议和偿付能力标准）。并且随着该领域的成熟，可以采用适用于职能部门、或业务线的更具专业性的风险模型。

对于云计算而言，我们需要修订和加强这些实践。正如之前的信息技术模型一样，审计需要充分利用云计算的潜力，同时增大范围和规模来管理它诸多的新颖性。

4.3 建议

当接洽（云计算）提供商时会牵涉到客户所属组织内适当的法务、采购以及合同团队。服务的标准条款可能并未涉及合规需求，需要就此进行协商。

对于受到高度监管的行业（例如金融业、医疗行业）来说，当使用云服务时应该考虑专门的合规要求。理解自身当前要求的组织应该考虑分布式 IT 模型的影响，包括云服务提供商运营于不同的地理位置以及不同的法律管辖区所带来的影响。

为每项工作负荷（例如整套的应用和数据），确定使用云服务将会如何影响现有的合规要求，特别是当与信息安全有关时。尽管有许多外包服务解决方案，组织仍需理解他们哪个云服务合作伙伴正在处理并应当处理受监管的信息。受影响的策略以及流程的例子包括活动报告、日志、数据保持、事故响应、控制测试和隐私权策略。

各方都应该理解各自的合同职责。期望值的底线将会由于部署模型而有所不同，在 IaaS 模型中客户拥有更多的控制权和职责，对于 SaaS 解决方案而言服务提供商扮演着统治性的角色。特别重要的是彼此受约束的要求和责任——不仅只是限于客户与他们直接的云服务提供商，而且也是在最终用户与提供商的云服务提供商之间。

遵守法规以及行业规定和要求（例如法规、技术、法律、合规、风险和安全等方面）是关键的，并且必须在要求确认阶段就解决。任何被处理、传输、存储的信息，或是被看作是个人可识别信息（Personal Identifiable Information, 简称 PII）或私人信息都面临着世界范围内繁多的合规规定，这些合规可能随国家或州的不同而有差异。既然云计算被设计为是位于不同地区且可扩展的，解决方案中被存储、处理、传输或是检索的数据可能来自云服务提供商的众多场所或多个数据中心。一些法规明确规定的控制在某些云服务类型（例如地理上的要求可能与分布式的存储不一致）下很难、或是根本不可能实现。客户与提供商必须就如何收集、存储，以及共享合规证据（如审计日志、活动报告、系统配置）达成一致意见。

- 建议首选那些具有“云意识”的审计人员，他们熟悉保证虚拟化与云技术的挑战（以及优势）。
- 建议要求云服务提供商提供 SSAE 16 SOC2 或 ISAE 3402 类型 2 报告。这些报告将为审计人员和评估人员提供被承认的参考起点。
- 合同应该提供给第三方（例如由双方选择的中间方）来评审 SLA 的度量标准及合规性。

4.4 要求

- ✓ 有权审计的条款赋予客户审计云提供商的能力，这支持在频繁地变化的云计算环境与法规内的可追溯性和透明度。使用有权审计的标准化规范来确保对彼此期望值的理解。最终，这个权利应由第三方的认证（例如 ISO/IEC 27001 或 27017 认证）所取代。
- ✓ 使用指定访问权限的透明度条款提供那些身处受到高度监管行业的用户（包括那些可将不合规作为刑事诉讼依据的行业）所需要的信息。该协议应该与自动产生或可直接访问的信息（例如日志、报告），以及“推送的”信息（例如系统架构、审计报告）区分开来。
- ✓ 云提供商应该定期（或是按需）地评审、更新并且发布他们的信息安全文档和 GRC（Governance, Risk and Compliance, 简称 GRC）流程。这些资料应该包括漏洞分析以及相关的补救措施决策和活动。
- ✓ 第三方审计人员应由云提供商和客户事先共同披露或选择。
- ✓ 各方应就采用一个共同的 IT 治理和安全控制认证保证框架（例如 ISO 或 COBIT 标准）达成一致。

D5: 信息管理与数据安全

信息安全的主要目标是保护那些为系统及应用注入动力的基础数据。伴随着企业向云计算环境的迁移，保护数据的传统方法则面临基于云的架构所带来的全新挑战。高弹性的、多租户、全新的物理与逻辑架构，以及抽象控制均需要新的数据安全战略。在许多云部署方案中，用户往往将数据上传至外部，甚至上传到公共环境，而这一方式在数年前简直是不可想象的。

在云计算时代，管理信息对几乎所有组织来说都是所面临的一个严峻挑战，即使那些看上去并不热衷于云计算项目的组织也是如此。从管理内部数据开始，进而是云迁移，更进一步扩展至对广泛的、跨组织间的应用与服务所包含信息加以保护。因此，在云计算时代，信息管理和数据安全均要求新的战略与技术架构。幸运的是，不仅用户有所需的工具与技术，而且向云环境迁移数据也创造了在传统基础体系更好的保护数据的契机。

作者在推荐采用数据安全生命周期 Data Security Lifecycle（后面会详细介绍）来评估和定义云数据安全战略。这一安全战略应当基于明确的信息治理策略而分层细化，并通过诸如加密与特定监控工具等的关键技术实施而生效。

概览 本域包括三个小节：

- 第一节 提供云信息（存储）架构的背景资料
- 第二节 介绍包括数据安全生命周期 Data Security Lifecycle 在内的最佳实践
- 第三节 详述数据安全控制及适用场景。

5.1 云信息架构

云信息架构与云架构本体相比较而言，都具有多样性；本小节可能不会覆盖到所有潜在的排列组合，仅针对大多数云服务中具有共性架构而加以阐述。

5.1.1 基础设施即服务

无论是在公有云还是私有云环境下，IaaS(基础设施即服务)，通常均包括如下存储选项：

- **原始存储。**这包括用于存储数据的物理存储介质。原始存储在部分私有云的配置中可能会被映射为可直接访问。可能在某个私有云架构中被用于随机存取数据。
- **卷存储。**这包括在 IaaS 实例中所附加的卷，最为典型的莫过于虚拟硬盘。这些卷通常使用“数据离差（Data Dispersion）”来实现可复原性与安全性。

- **对象存储。**对象存储有时被当作文件存储来提及，较之虚拟硬盘，对象存储更像是一个通过 API¹⁴或 Web 界面加以访问的文件共享。
- **内容分发网络。**内容被保存在一个对象存储上，然后被分发到多个地理分布不同的节点以提高其网络消费速度。

5.1.2 平台即服务

平台服务（PaaS）不仅提供并依赖于一个非常广泛的存储选项。

PaaS 可提供：

- **数据库即服务。**一个多租户数据库架构可直接被视为一项可供直接消费的服务。用户可根据交付类型不同而通过 API 或直接 SQL¹⁵调用来使用该数据库。每一用户的数据则与其他租户的数据之间保持严格隔离及高度独立。，数据库本身则可能是关系型、平面型，或者任何其他通用架构。
- **Hadoop/Mapreduce/大数据即服务。**大数据是指具备大规模、广泛分布、异构性以及并发性/时间线等特性的数据，其必然要应用新的技术架构及分析机制。Hadoop 和其他类似大数据应用或可以云平台形态交付。数据则通常被存放在对象存储或其他分布式文件系统中。数据通常与处理环境密切相关，或会根据处理需要而临时移动。
- **应用存储。**应用存储包括任何内置在 PaaS 应用平台中且可通过不同于其它存储类别中的 API 来调用的存储选项。

PaaS 可消费：

- **数据库。**信息和内容可被直接存储在数据库中（如：文本或者二级制对象）或以数据库可引用的文件形式间接存放。。数据库本身则可能是多个共享后端存储的 IaaS 实例集合。
- **对象/文件存储。**文件或其他数据则存放在仅通过 PaaS API 接口可访问的对象存储中。
- **卷存储。**数据可以被存放在那些旨在于对外提供 PaaS 服务的实例所附加的 IaaS 卷中。
- **其它。**以上为绝大多数通用的存储模型，但这是一个不断更新的领域，因此仍会有新的选项可能出现。

5.1.3 软件即服务

类似于平台即服务（PaaS），软件即服务（SaaS）可采用非常广泛的存储模型和服务模型。SaaS 存储通常可通过一个 Web UI 接口或 C/S 应用方式而加以访问。如果存储可通过应用程序接口（API）来访问，那么软件服务（SaaS）也可视为是平台即服务（PaaS）。很多软件即服务（SaaS）供应商同时也提供此类平台即服务（PaaS）的应用程序接口 APIs。

SaaS 可提供：

¹⁴ API: 应用程序接口

¹⁵ SQL: 结构性查询语言，用以管理数据

- **信息存储与管理。**数据通过 Web 界面输入到系统，并存储在软件即服务 SaaS 类应用程序中（通常是一个后端数据库）。某些 SaaS 服务也可提供数据集上传选项，或者平台即服务（PaaS）的应用程序接口 API。
- **内容/文件存储。**基于文件的内容（如：报告、图片文件、文档等）可被存储在软件即服务 SaaS 应用中，并且提供基于 Web 的用户访问接口。

SaaS 可消费：

- **数据库。**与 PaaS 相类似，大量的 SaaS 服务依赖数据库后端于，即便是文件存储也不例外。
- **对象/文件存储。**文件或其他数据被存放在对象存储中，且仅能通过 SaaS 应用方式加以访问。
- **卷存储。**数据可以被存放在那些旨在于对外提供 SaaS 服务的实例所附加的 IaaS 卷中。

5.2 数据（信息）离差

数据（信息）离差是一种在无加密机制环境下广泛被用于提高数据安全性的技术。这些算法多（缩写为：IDA¹⁶：入侵检测算法）借助数据分段来对存储在云中的数据提供高可用性和安全保障，且被普遍应用于诸多云平台。在一个数据分段模式中，一个文件 f 被分成 n 个分段；所有这些分段都被签名并分发到 n 个远程服务器上。用户可任意选择 m 个分段来重构文件 f 。分段机制也适用于云中需高安全性且长期存储的数据。

当分段机制与加密机制同时使用时，数据安全得到增强：入侵者不得不访问 m 个云节点以找回文件 f 的 m 个分段，同时还得破解已有的加密机制。

5.3 信息管理

在讨论特定的数据安全控制项前，我们需要一个模型来理解和管理我们的信息，信息管理包括在理解信息如何应用及如何治理应用中所采用的过程和策略。在数据安全小节，我们会讨论用于监控和治理等需求的特定的技术控制措施和建议。

5.4 数据安全生命周期

尽管信息生命周期管理是一个相对成熟的领域，它也还不能完全满足安全专家的需求。数据安全生命周期则不同于信息生命周期管理，它应反映安全受众差异化需求。（生命周期概述和完整版本可参考 <http://www.secuosis.com/blog/data-security-lifecycle-2.0>）生命周期从创建到销毁共有六个阶段，六个阶段尽管是以线性过程显示，但一旦创建，数据可在任意两个阶段间切换，无需一定一定遍历所有阶段（例如，并不是所有的数据最终会被销毁）。

¹⁶ IDA: Intrusion Detection Algorithms 入侵检测算法

1. **创建。** 创建就是产生新的数字内容，也可能是对已有内容的替换/更新/修改。
2. **存储。** 存储是将数据提交到某种存储库中，该阶段通常在数据创建时并发产生。
3. **使用。** 数据被查看、处理以及不包括修改在内的其它各种使用方式。
4. **分享。** 信息本身就应可被诸如用户、客户、合作伙伴等所访问。
5. **归档。** 数据不再保持在可用状态而进入长期存储。
6. **销毁。** 使用物理或诸如密码粉碎之类的数字方式将数据永久销毁。



图一 数据生命周期

5.4.1 位置与访问

生命周期描述了信息的流转阶段，但并不涉及信息所在的位置及访问方式。

位置

可以用图解的方式来将生命周期视为一系列不同操作环境中更小的生命周期的集合，而非单一的、线性操作。几乎处于任何阶段的数据都能在这些环境里输入或者输出。

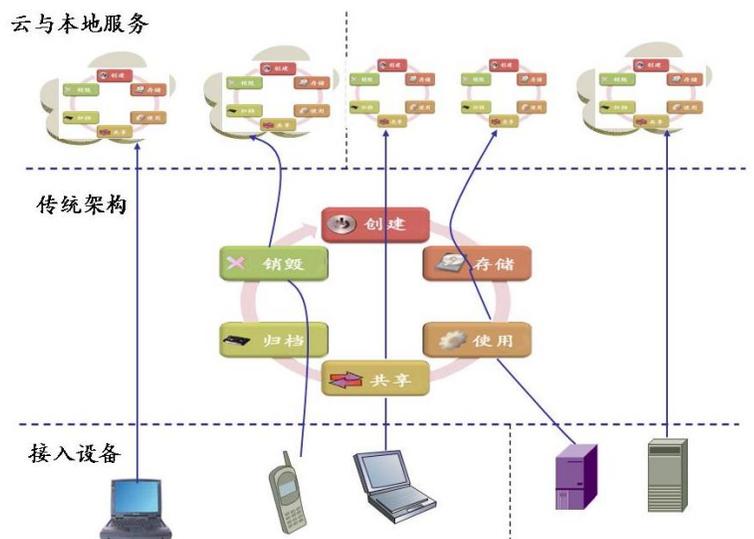
由于所有潜在的监管、合同以及其它相关法规的要求存在，因此理解数据的逻辑和物理位置就显得非常重要。

访问

当人们知道数据存放在哪里以及如何移动时，他们就需要知道谁在如何访问数据。这里有两个因素：

1. 谁在访问数据？
2. 是如何访问的（设备及通道）？

今天，访问数据可采用各种不同的设备，这些设备又有不同的安全特性，并且使用不同的应用程序或者客户端。



图一 云访问设备

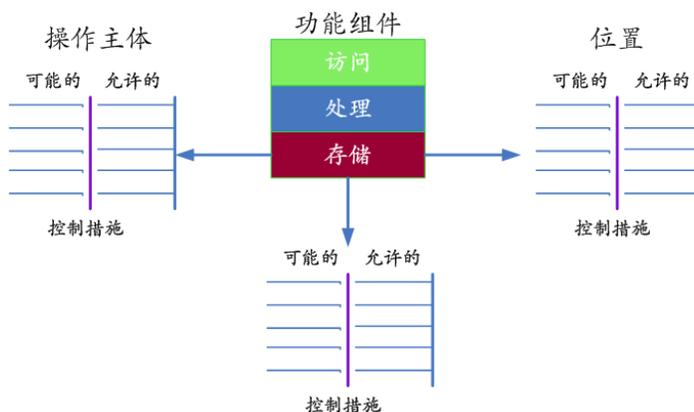
5.4.2 功能组件、操作主体和控制措施

功能组件是数据操作的功能模块，被主体执行（人或者系统），并有一个精确的位置。

功能组件

可使用三个组件来操作数据：

- **访问。** 浏览和访问数据，包括创建、复制、文件传输、分发，以及其它信息交换。
- **处理。** 执行数据的处理事务，如：更新数据，用来处理一个业务处理事务等。
- **存储。** 保存数据（在一个文件或数据库中）。



下表展现了各种功能组件与数据生命周期各阶段的矩阵关系：

表一 信息生命周期阶段

	创建	存储	使用	共享	存档	销毁
访问	X	X	X	X	X	X
处理	X		X			
存储		X			X	

一个操作主体（可以是人、应用程序或者系统/进程，而非访问设备）可在某个位置执行每个功能组件。

控制措施

一个控制措施限制了一系列可能发生的操作清单，直至之前已被允许的操作。下表是可能发生的操作清单的一种展现方式，用户可以使用该表来对照控制措施。

表二 可能的和允许的控制措施

功能组件		操作主体		位置	
可能的	允许的	可能的	允许的	可能的	允许的

5.5 信息治理

信息治理包括管理信息用途的策略和流程，有如下主要特征：

- **信息分类。**高阶描述重要信息的分类。与数据分类不同，其目标不是为组织的每一个信息打标签，而是定义高阶分类，如“受控的”和“商业秘密”等用于明确需要的安全措施。
- **信息管理策略。**策略用于定义各类信息被允许的操作。
- **位置及合规要求。**数据可被存放的地理区域，以及这个区域的重要法律法规等。
- **授权。**定义各类员工和用户允许访问的信息。
- **所有者。**谁最终应对信息负责。
- **保管职责。**在信息所有人所遗留下来的信息中，谁该为管理这些信息承担责任。

5.6 数据安全

数据安全是指因信息治理的要求而采取的特定控制措施和技术。可分解成三部分，涵盖检测和预防）数据在云架构中的迁移，保护数据进入云以及在不同提供者/环境之间的传输，保护已在云中的数据。

5.6.1 检测和预防数据在云架构内的迁移

组织所面临的云架构内的共同挑战就是管理数据本身。许多组织称，通常既没有得到许可，也没有作 IT 或安全通告，个人或业务单元就将敏感数据迁移到云设施上了。

除了传统的数据安全措施外（例如：访问控制或加密），还有两个步骤可帮助管理未经审批的数据向云服务设施的迁移：

1. 使用数据活动监测(**DAM**)¹⁷和文件活动监测(**FAM**)¹⁸来监控大量内部数据的迁移。
2. 使用 URL 过滤器和数据丢失保护 DLP 等技术监控数据向云中迁移的过程

内部数据迁移

在数据迁移到云之前，必须先将数据从所在的存储库中移出。数据库活动监控器可以监测到管理员或者其他用户在某个时刻将一个大数据集移出，或者做了一次数据库复制，而这可以表明有一次迁移正在发生。

文件活动监控器提供类似的文件库迁移保护，比如文件共享机制等

数据迁移到云

¹⁷ DAM - Database Activity Monitoring

¹⁸ FAM - File Activity Monitoring

通过一个 URL 过滤器（比如 web 内容安全网关）和数据丢失防护（DLP: Data Loss Prevention）的联合机制可检测到有数据从企业环境迁移到云架构中。

URL 过滤器可以监控（和阻止）用户连接到云服务上，因为云服务的管理控制台通常与用户消费端位于不同的地址，所以用户能够明确的分辩出究竟是未知的某人访问到管理控制台，抑或是真实用户访问了由供应商托管的应用程序。

与其寻找一个提供并持续更新的云服务清单的工具，还不如找到一个用于创建自定义类别及管理目标地址的用户工具。

对于更细粒度的数据迁移，需要使用数据丢失防护（DLP）。DLP 工具监测实际传输的数据/内容，而不是仅对目标地址进行检查。因此用户就可进行基于数据分级的告警（或拦截）。例如，用户可仅允许将企业内部数据迁移到一个获得许可的云服务中，而拦截将同样内容迁移到一个未经授权服务之上。

DLP 方案的一个介入点就是数据泄漏的检测成功与否。例如，当企业网络环境外外部的各种用户（例如，员工、供应商、最终客户）进入企业边界时，是否绕过了任何 DLP 解决方案，以此来确保云解决方案的可用性。

5.6.2 保护迁往云和在云内迁移的数据

在公共云和私有云部署方案中，无论什么服务模型，保护数据传输都是非常重要的。这数据传输过程包括：

- 数据从传统基础架构迁移到云供应商中，包括公有与私有之间转移，内部与外部之间转移，以及其他各种组合。
- 数据在云供应商之间的迁移。
- 数据在既定的云内实例间（或者其他组件之间）迁移。

有三种选项（或选择顺序）：

1. **客户端/应用程序加密。**数据在终端或服务器端先加密，然后再通过网络传输，或者在已经以恰当的加密格式存储。这既包括本地客户端（代理模式）加密机制（例如，针对存储文件）或者集成在应用程序之中的加密机制。
2. **链路/网络加密模式。**标准的网络加密技术包括 SSL、VPNs 和 SSH。既可以是硬件加密，也可以是软件加密。实现端到端加密当然是首选，但并不适用所有架构。
3. **基于代理的加密。**数据通过一个代理设备或服务器进行传输，数据在网络传输前完成加密。通常都是将代理加密机制整合到原有的应用程序中，但我们并不推荐采用这种方式。

5.6.3 保护云内数据的安全

云计算之中包括了非常广泛的技术与措施，就安全选项而言，也无法做到面面俱到。下面介绍一些更实用的技术与最佳实践，来保护各种云模型中的数全。

5.6.3.1 内容发现

内容发现指的是用于识别存储的敏感信息的工具和过程。它允许组织定义基于信息类型、结构或分类的策略，然后使用先进的内容分析技术扫描存储数据，来确定其存储位置及是否策略违规。

内容发现一般来说是数据丢失防护 DLP 工具的特性之一，有时也会内置在数据库活动监视类 DAM 产品中。扫描可通过文件共享的访问方式或操作系统上运行本地代理的访问方式进行。这种工具必须是“云感知”化的，而且能够具备在云环境中有效工作的能力（如：能够扫描对象存储）。内容发现也可以一种可管理服务的形式存在。

5.6.3.2 基础设施服务加密

5.6.3.2.1 卷存储加密

卷加密可抵御如下风险：

- 保护卷免除快照克隆或泄漏风险
- 保护卷免除被云供应商（和私有云管理员）而随意查看的风险
- 保护卷免除物理硬盘丢失（这更像是一个实际发生的安全事件，而不是仅仅满足合规性要求那么简单）而导致的信息泄漏风险

基础设施服务的数据卷可通过以下三种方式加密：

- **实例管理加密。**这种加密引擎是在实例中运行，密钥被存放在卷中，并采用密码或密钥对进行保护。
- **外部管理加密。**这种加密引擎同样在实例中运行，但密钥在外部管理，并响应实例请求而进行分配。
- **代理加密。**在这一模型里，先将卷连接到一个特定的实例或设备/软件中，然后将该实例再连接到加密实例上。，代理处理所有的加密操作，并将密钥保管在代理内部或外部之中。在线方式或外携方式保管密钥。

5.6.3.2.2 对象存储加密

对象存储加密用于抵御很多类似卷存储同样存在的风险。因为对象存储长期被暴露在公共网络上，并允许用户搭建虚拟私有存储（VPS）。就像 VPN 一样，VPS 在保护好数据的同时，可以使用公共共享的基础设施，即使这些数据被暴露，也只有那些有加密密钥的人才能查看。

- **文件/文件夹加密和企业数字版权管理 DRM。**在将数据放到对象存储前，先使用标准的文件/文件夹加密工具或者企业数字版权管理工具（EDRM）加密数据。
- **客户端/应用程序加密。**在一个应用程序（包括移动应用）里，对象存储通常被当作后端使用时，可以使用嵌入在应用程序内或客户端中的加密引擎加密数据。
- **代理加密。**在数据发送到对象存储前，使用加密代理进行数据加密。

5.6.3.3 平台服务加密

因为平台服务（PaaS）是多样化的，所以下面列表可能覆盖不了所有的选项：

- **客户端/应用加密。**数据在 PaaS 应用中加密，或者在访问平台的客户端程序中加密。
- **数据库加密。**数据通过数据库内置的加密机制加密并存储于数据库中，这需要数据库平台支持这种加密机制。
- **代理加密。**在数据发送到平台前，通过一个加密代理进行加密。
- **其它。**其它可选项还包括在平台中内置加密 API，外部加密服务和其它可选形式。

5.6.3.4 软件服务加密

软件服务（SaaS）供应商可以使用上述提到的任何一种选项，对于多租用式的隔离模型中，建议每个用户使用不同的密钥。以下选项可供软件服务用户使用：

- **服务提供方管理加密。**数据在 SaaS 应用中加密，并通常由服务提供方管理。
- **代理加密。**数据通过加密代理后再送到 SaaS 应用中。

使用共享密钥或公/私密钥对，以及额外的 **PKI/PKO**¹⁹架构等在内的哪种加密操作最为适合，此处可参阅域 11 了解更多关于加密和密钥管理信息。

5.6.4 数据防丢失保护

数据防丢失防护（DLP）可定义如下：

基于中心策略，通过深度内容分析识别、检测和保护数据的运转和使用及其它过程的产品。

DLP 能够发现是否违规操作数据并进行阻断操作（停止其 workflow），或采用诸如 DRM、ZIP 或 OpenPGP 等加密机制处理后允许其继续运行。

DLP 常通过如下机制进行内容发现，监测数据运行：

- **专用设备/服务器。**在云环境与其他网络/互联网边界，或云环境的两个子区域的抑制点部署标准的硬件。
- **虚拟设备**
- **终端代理**
- **Hypervisor 代理。**相对于在实例中运行，DLP 代理则内置在 Hypervisor 层，或可在 Hypervisor 层得以访问到。
- **DLP SaaS。**DLP 集成在一个云服务中（如：托管电子邮件），或者以一个独立标准的服务提供（一般是内容发现服务）。

¹⁹ PKI/PKO - Public Key Infrastructure/Operations

5.6.5 数据库和文件活动监测

数据库活动监测（DAM）工具定义为：

捕捉和记录细微的且实时或准实时发生的所有结构性查询语言（SQL）活动，包括数据库管理员跨多数据库平台的活动，并产生违规告警。

DAM 支持准实时的数据库活动监测并进行违规告警，如 SQL 注入攻击，或管理员未经授权的数据复制操作。云环境下的 DAM 工具常以代理的方式连接到一个集中的收集服务器（该服务器也常是虚拟出来的）。它常被用于单个客户的数据库实例，但未来亦可用于平台服务 PaaS。

文件活动监控（FAM）定义为：

检测和记录指定文件库在用户级的所有操作记录，并产生违规告警。

在云环境中的 FAM 需使用一个终端代理，或在云存储和云用户之间部署一个物理设备。

5.6.6 应用安全

较大比例的数据泄露是来自应用层攻击，特别是 Web 应用程序。可参考 D10 域了解更多应用安全信息。

5.6.7 隐私保护保护

几乎所有的云存储系统都需要访问者（云用户或内容供应商）通过某种身份认证方式来建立信任关系，无论是单向通讯还是双向通讯均需如此。尽管加密证书能够为多数应用场景很多提供足够的安全性保障，但其因为与真人（云用户）而严格绑定而不适用于隐私信息。因为证书的任何一次应用均可能将证书持有者的身份泄漏给发起认证请求的团体。有很多场景（如：电子病历存储）就是因为采用了证书认证方式而不必要的暴露了证书持有者的身份。

在过去的十到十五年里，大量技术（如密码证书等）涌现，并且被用于使系统在值得信任的同时还能保护持有者的隐私信息（例如：隐藏真实持有者的身份信息等）。基于属性的证书就像普通加密证书（如 x.509 证书）一样都使用数字（或加密的）签名密钥。然而，基于属性的证书（attribute-based credentials, ABCs）允许持有者将其作为一个仅包含源证书内所含属性的子集封装在新的证书里。这些封装后的新证书能够被当作普通加密证书（使用公有密钥）来校验，以提供同样强度的安全保证。

5.6.8 数字版权管理（DRM）

DRM 的核心就是用其加密内容，并应用一系列版权要求。版权要求既可以简单如防拷贝，也可以复杂如限定某组或基于用户的诸多活动集合，诸如剪切、粘贴、发送邮件、改变内容等。任何使用 DRM 进行数据保护的应用或系统必须能够解释和执行权限，这常常意味着系统需整合密钥管理系统。

这里有两种主要的数字版权管理分类：

- **消费者 DRM** 多用于保护广泛分发的媒体内容，如：提供给广大受众的音频、视频和电子书。这一 DRM 可使用各种不同的技术与标准，但重点是都基于单向分发方式。
- **企业 DRM** 是用于保护组织内部的信息和合作伙伴之间的信息。重点在于有很多复杂的权限、策略，以及与业务环境，尤其是企业目录服务 DS 的整合。

企业 DRM 能够很好地保护存储在云中的信息，但需要深度的基础架构整合。这对基于内容管理的文件和分发是非常有用的。消费者 DRM 能够为分发给消费者的内容有较好的保护，但是却因为大多数技术在单点上易被破解而无法保持很好的跟踪记录。

5.7 建议

- 理解所采用的云存储架构，有助于确定安全风险和可用的控制措施。
- 如果可能的话，选择支持数据离差技术的云存储。
- 使用数据安全生命周期 DSL 来识别易受攻击的安全，以确定最合适的控制措施。
- 使用 DAM 和 FAM 监测内部核心数据库和文件库，识别能够表明数据向云中转移的的大数据迁移。
- 使用 URL 过滤和（或）DLP 工具监测员工的互联网访问，来识别是否敏感数据迁移。选择可对云服务作预分类的工具，并通过过滤规则阻断非授权行为。
- 所有敏感信息移入云或在云内传输时，应在网络传输前的网络层或者节点侧进行数据加密。这一建议适用于所有的云服务和部署模型。
- 使用任何数据加密机制时，应特别注意密钥管理（详见第 11 章）。
- 使用内容发现机制来扫描云存储，并识别已泄漏的敏感数据。
- 加密 IaaS 中的敏感卷，来限制因为快照或未授权管理员访问导致的信息泄露。至于采用何种技术依赖于具体的操作需要。
- 采用文件/文件夹或客户端/代理加密机制加密对象存储中的敏感数据。
- 加密平台服务 PaaS 应用和存储中的敏感数据。通常情况下应用层加密机制为首选，因为几乎没有云数据库支持原生加密机制。
- 当使用应用加密时，密钥无论如何必须存放在应用系统外面。
- 若软件服务（SaaS）需使用加密，应尽可能使用可提供原生加密机制的供应商；若无该工具或必须到规定信任等级，则可使用代理加密机制。
- 使用 DLP 来识别云部署的敏感数据泄漏，这种情况仅对基础设施服务（IaaS）适用，这对其他公共云供应商均不适用。
- 使用数据库活动监测工具（DAM）来监控敏感数据库，并对违反安全策略的行为进行告警。

- 当交付的基础设施或应用在正常访问敏感用户信息时，应考虑对可能的泄漏采取私有存储保护机制。
- 谨记绝大多数数据安全缺陷都源自于应用程序极为脆弱的安全性。
- 云供应商不仅应当遵循这些实践，并且为用户发布数据安全工具和配置选项。
- 无论是合同到期或其他原因，应在 SLA 中详细说明如何从云供应商供应商中转移数据，必须包括用户账号删除，从主/冗余存储中迁移或删除数据，迁移密钥等。

5.8 要求

- ✓ 使用数据安全生命周期来识别安全易受攻击点，从而确定最合适的控制措施。
- ✓ 考虑到潜在合规的、合约方面的以及其他法律方面的问题，应充分理解逻辑和物理数据。
- ✓ 使用 URL 过滤器和/或 DLP 工具监测员工的互联网访问，来识别敏感信息的传输。
- ✓ 在网络层或传输前在节点加密所有传输的敏感信息。
- ✓ 加密基础实施中的敏感卷，限制因快照或非授权访问的信息泄露。
- ✓ 在平台服务应用和存储中加密敏感信息。

参考文献

- [1] RABIN, M. O. 1989. Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance. J. ACM, 36(2), 335–348.
- [2] SECUROSIS. 2011. The Data Security Lifecycle. <http://www.securosis.com/blog/data-security-lifecycle-2.0>
- [3] SECUROSIS. 2011. Understanding and Selecting a Data Loss Prevention Solution. <http://www.securosis.com/research/publication/report-data-loss-prevention-whitepaper>
- [4] SECUROSIS. 2008. Understanding and Selecting a Database Activity Monitoring solution. <http://www.securosis.com/research/publication/report-selecting-a-database-activity-monitoring-solution/>
- [5] CHAUM, D. L. Feb. 1981. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 24 (2), 84-90.

D6: 互操作性与可移植性

云计算的出现为每个组织机构的 IT 配置和管理带来了前所未有的不同于“传统”内部基础架构的可扩展性。组织机构得以响应动态变化中的处理需求，接近实时地添加、移动或者删除额外的容量。为满足增长的业务需求，一个新的应用支撑系统可以在数小时内而不是数周内启动起来；而当业务需求回落时，额外的容量可以同样快速地关停而不是让过剩的硬件设备在那里空转。从 IaaS 到 SaaS，任何基于云实施的系统都需要将互操作性和可移植性定为设计目标才能获得这种更加弹性环境的收益回报。

一方面，互操作性和可移植性允许你在全球范围内横跨多个独立的服务供应商来扩展一个服务，而且整个系统的运转就像是同一个系统。另一方面，互操作性和可移植性允许你轻松地将数据和应用从一个平台迁移到另一个平台，或者从一个服务供应商迁移到另一个服务供应商。

可移植性与互操作性其实并不是云环境所特有的考虑因素，并且与其相关的安全性问题也不是云计算所带来的新概念。然而，云计算中所存在的开放和往往是共享的处理环境带来了比传统处理模型中更加需要提前预防和准备的需求。多租户就意味着你的数据和应用与其它公司的数据和应用是共存的，而这种通过共享的平台、共享的存储和共享的网络访问到你的机密数据（不管是有意还是无意的）是可能的。

本章定义了在设计互操作性和可移植性时需要重点考虑的因素。

概览 后续小节采用以下条目来定义互操作性和可移植性：

- 互操作性介绍
- 保障互操作性的建议
- 可移植性介绍
- 可移植性的建议

6.1 互操作性介绍

互操作性是对一个云生态系统中的各个组成构件的需求，以确保它们可以协同工作从而获得所期望的结果。在一个云计算的生态系统中，各个组成构件很可能来自于不同的地方，例如云和传统 IT 环境、公有云和私有云实现（所谓的混合云）。互操作性确保这些组成构件可以被不同供应商的不同的或者新的组成构件所替换并且继续工作，同样也将确保系统之间数据的交换。

随着时间的推移，商业企业一定会作出需要更换供应商的决策，需要更换的原因包括：

- 合同续约时无法接受成本的增加
- 可以以更低的价格获得同样的服务

- 供应商终止业务运营
- 供应商突然停止一个或者多个正在使用的服务并且没有可以接受的迁移计划
- 无法接受的服务质量下降，例如无法满足关键性能需求或者达成服务水平协议(SLA's)²⁰
- 云消费者与云供应商之间的业务纠纷争议

缺乏互操作性（可移植性同理）将导致云消费者被特定的云供应商锁定。

在考虑一个云项目的时候，互操作性所能达到或维持的程度依赖于云供应商使用开放或已公布的架构、标准协议以及标准 API's²¹的程度。虽然很多声称“开放”和“基于标准”的云供应商会推出正常合理的挂接(hook)、扩展和增强(例如 Eucalyptus)，但这些也会影响阻碍互操作性和可移植性。

6.2 可移植性介绍

可移植性决定了应用程序组成构件无需担心供应商、平台、操作系统、基础架构、地理位置、存储、数据格式或 API，就可以被迁移和重用到别的地方的难易程度。

无论云迁移是向公有云、私有云还是混合云部署解决方案迁移，可移植性和互操作性都是必须要考虑的。无论迁移战略是向软件即服务(SaaS)，平台即服务(PaaS)还是基础架构即服务(IaaS)迁移，它们也都是服务模式选择的重要考虑要素。

可移植性是选择云供应商时一个关键考虑方面，它既可以帮助防止厂商锁定，也可以允许你在不同的云供应商解决方案之上部署相同的云以实现容灾目的或者实现分布式单一解决方案的全球部署，从而交付更多的商业价值与回报。

获得云服务的可移植性通常依赖于 D1 域所定义的云立方中采用相同架构象限的两种服务，服务是运行在不同的象限中，所以迁移一个服务往往意味着在将该服务重新外包到一个可选的云服务之前需要先将该服务迁回到“内部”。

在云迁移项目中如果不能很好地处理可移植性和互操作性有可能导致无法获得迁移到云的收益和回报，而且会因为以下本来应该避免的因素导致成本问题或者项目延误：

- 应用软件、厂商或服务供应商的锁定 — 选择某个特定的云解决方案可能会限制迁移到另一个云服务或者云供应商的能力
- 处理导致服务中断的不兼容性和冲突 — 供应商、平台或者应用的差异性可能会引发不兼容并导致应用程序在不同云基础架构中运行时发生故障
- 预期之外的应用程序返工或者业务流程变更 — 迁移到一个新的云供应商时，为保留应用程序原有的行为状态会产生重新制定流程运作的要求或者代码变更的需求

²⁰ SLA - Service Level Agreement

²¹ API - Application Program Interface

- 额外成本的数据迁移或数据转换 — 缺乏可互操作和可移植的数据格式可能会在迁移到新的供应商时产生计划外的数据改变
- 新应用程序或管理软件的重新培训或者工具改造
- 数据或者应用的安全缺失 — 迁移到新的供应商或者平台时可能会因为供应商之间不同的安全策略或者控制点、不同的密钥管理或者数据保护措施产生无法察觉的安全缺陷

将服务迁移到云也是一种外包方式；外包的黄金原则是“预先了解并为如何退出合约作准备”。可移植性（和一定程度上的互操作性）应该成为任何迁移到云服务的组织战略的关键评判标准，以便制定可靠的退出策略。

6.3 建议

6.3.1 互操作性建议

硬件—物理计算机硬件

硬件设备会随着时间的推移和供应商的更换无法避免地发生变化和改变，所以如果需要直接访问硬件设备就难免产生互操作性差异。

- 任何时候在可能的情况下，尽可能采用虚拟化以消除硬件层的关联，需要记住的是虚拟化并不会消除所有硬件设备的考虑，尤其是在现有的系统中。
- 如果一定要直接访问硬件设备，重要的是要确保在从一个供应商向另一个供应商迁移时具有同等或者更好的物理和管理安全控制点。

物理网络设备

不同服务供应商其包括安全设备在内的网络设备和设备的 API 以及配置流程都会有所不同。

- 为确保互操作性，在虚拟域中应采用网络物理硬件和网络及安全的抽象。尽可能 API 应该具备相同的操作功能。

虚拟化

虽然虚拟化有助于消除物理硬件设备的顾虑，但是要区分出常见 Hypervisor 之间存在的差异（例如 XEN, VMware 以及其它的 Hypervisor）。

- 采用象 OVF 这样的开放虚拟化格式有助于保障互操作性。
- 不管采用哪种格式都需要记录并了解使用了哪种特定的虚拟化挂接（hooks）。每种格式都仍有可能在其它的 Hypervisor 上无法工作

框架

不同的平台供应商会提供不同的云应用框架，而它们之间必然存在的差异性会影响互操作性。

- 通过调查研究 API 以确定差异性所在，并且为迁移到新的供应商时任何必要的应用程序处理变更作好准备。
- 采用开放的和已公布的 API 以确保最广泛地支持组成构件间的互操作性和便于必须要更换服务供应商时应用和数据的迁移。
- 云中的应用程序往往是通过互联网来交互的，而断路也是意料中会发生的事情。所以需要确定当一个组成构件发生故障（或者响应缓滞）时如何影响其它的组成构件，避免当远端组成构件发生故障时会造成系统数据完整性风险的状态依赖性。

存储

不同类型的数据对于存储的需求不尽相同。结构化数据多数情况下会需要数据库系统或者需要应用程序特定的格式。非结构化数据通常会遵从字处理、表格处理和幻灯片管理程序所使用的一系列常用应用格式中的某一种。这里我们需要考虑的是如何无缝地将一个服务所存储的数据迁移到另一个服务。

- 将非结构化数据存储为已经确立的可迁移的格式。
- 评估数据传送中加密的需求。
- 检查可兼容的数据库系统，需要的情况下评估转换需求。

安全

云中的应用程序和数据所处的系统不是用户所有，并且用户往往只能进行有限的控制。关于可互操作安全性需要考虑的一些要点包括：

- 认证采用 SAML 或者 WS-Security 以便控制点可以与其它采用标准的系统进行交互。参见域 12 了解更多细节。
- 在数据存放到云上之前对其进行加密可以保障其在云环境中不会被不恰当地访问。参见域 11 了解更多关于加密的细节。
- 如果已经使用了加密密钥，需要研究密钥是存在哪里和如何存放的以确保对于加密数据的访问可控。参见域 11 了解更多关于密钥管理的细节。
- 了解由于服务供应商未曾预料的保护措施“缺陷”而产生安全损害时你所拥有的责任和权利。
- 日志文件信息需要与迁移到云上的所有其它数据一样采用相同安全级别处理。确保日志文件可以互操作以确保迁移前与迁移后日志分析的连贯性以及无论使用何种日志管理系统的兼容性。
- 完全迁移后应确保所有的数据、日志和其它信息从原有系统中删除。

6.3.2 可移植性建议

向云上迁移的途中会存在各种各样的问题，会影响到向云上迁移的可移植性考虑因素和建议包括：

- **服务水平。**不同的供应商服务水平协议(SLA)会有所差异，所以需要了解这种差异将会如何影响你更换云供应商的能力。
- **架构的差异。**云中的系统可能会存在于不同的平台架构之上。了解服务和平台的依赖性以认识这种差异将会如何限制可移植性是非常重要的，服务和平台的依赖性可能会包括 API、Hypervisor、应用逻辑以及其它的约束条件。
- **安全集成。**云系统引入了为保障安全性所特有的可移植性考虑因素，包括：
 - 用户或者进程访问系统的认证和身份管理机制现在必须贯穿一个云系统的所有组成构件运作。采用类似 SAML 这样的开放标准对身份进行管理有助于保障可移植性。开发内部的支持 SAML 声明的 IAM 系统和可以接受 SAML 的内部系统有助于未来系统到云上的可移植性。
 - 加密密钥应该在本地由第三方保管，如果可能的话也在本地维护。
 - 元数据是数字信息的一个方面，由于（通常）在文件和文档上工作时元数据并不直接可见所以元数据经常被轻易忽视。由于元数据随着文档而移动，所以在云中元数据就变成了重要的考虑因素。将文件和其元数据迁移到新的云环境时，需要确保文件元数据的拷贝安全地清除以防止此类信息被遗留并产生可能的安全泄露。

6.3.3 不同云模式的建议

以下为一些对所有云模式均适用的通常的风险和建议。

- 更换云供应商时遇到原有云供应商的抵触是很正常的。所以必须参照域 3 中描述的在合同流程中、域 7 中描述的在业务连续性计划中、域 2 中描述的作为完整的管控组成部分对此进行计划。
- 了解托管在一个云供应商的数据集合的大小。大量的数据可能会导致转换过程中服务的中断或者超出预期的转换窗口。很多客户发现对于较大的数据集采用硬盘快递要比采用电子传输快得多。
- 记录安全架构和每一个组成构件安全控制点的配置以便用于支持内部审计，同时还有助于向新供应商的迁移以及新环境的验证。

基础架构即服务 (IaaS)

云供应商的职责是提供基本的计算资源例如存储、计算等等，而云消费者则需要对涉及互操作性的大部分应用设计任务负责。云供应商应该提供可以以最小代价与各种完全迥异的系统进行交互的标准化的硬件和计算资源。云供应商应该严格地遵循行业标准以确保互操作性。云供应商应该可以支持诸如云中介、云爆发 (Cloud Bursting)、混合云、多云联邦(Multi-cloud federation)等等复杂应用场景。

- 了解虚拟机镜像如何被获取并被迁移到新的云供应商和谁可能会采用了不同的虚拟化技术。示例：DMTF(Distributed Management Task Force)的开放虚拟化格式 (OVF)。
- 识别并消除（或者至少记录）任何厂商特有的虚拟机环境扩展。
- 了解一个应用从云供应商迁出后有哪些可以确保恰当移除虚拟机镜像的实践可用。

- 了解可以使用的废弃磁盘和存储设备的实践。
- 应用/数据迁移前了解需要识别出来的硬件设备/平台的依赖性。
- 向原有云供应商要求访问系统日志、使用痕迹、访问记录和计费记录。
- 识别与原有的云供应商部分或全部恢复及至扩展服务的选项如果新的服务被证明更差。
- 确定是否存在任何新供应商不兼容或者未实现的在用的管理层功能、界面或者 API。
- 了解数据在云供应商之间迁移时可能会涉及到的费用。
- 确定哪些手段可以用来支持类似于数据压缩这样的可以尽可能高效地将数据往云上迁移的标准能力。
- 了解提供了哪些安全措施以及谁来维护加密密钥的访问。

平台即服务 (PaaS)

云供应商负责提供云消费者可以在其上构建自己系统的平台。他们提供运行环境和预集成的程序堆栈。开发人员可以快速地在所提供的平台之上开发和部署定制应用而无需自行构建基础架构。云供应商为云消费者提供完整的基础架构和维护管理。

- 在可能的情况下，尽可能使用采用了标准语法、开放 API 和开放标准的平台组成构件，例如(OCCI)²²。
- 了解哪些工具可以用来实现安全数据传输、备份和恢复。
- 了解并记录 PaaS 供应商特有的应用组件和模块，开发具有抽象层的应用架构以最小化对专有模块的直接访问。
- 了解类似于监控、日志和审计这类的基础服务如何转移到一个新的供应商。
- 了解为放置在云上与在云上产生和维护的数据提供了哪些保护措施。
- 了解原有云供应商所提供的控制功能以及如何将其对应转换到新的云供应商。
- 迁移到新的平台时，了解迁移后对应用的性能和可用性的影响以及这些影响如何度量。
- 了解迁移前与迁移后如何完成测试以验证应用或者服务正常运行。确保供应商和用户在教学中的职责是明确的并且记录下来。

软件即服务 (SaaS)

云供应商在云上提供应用软件能力，云消费者只需要管理自己的操作和信息在系统中的流入和流出。客户只需要一个浏览器，而所有层面的主要的管理维护工作是由云供应商来负责。

- 定期将数据抽取和备份成没有 SaaS 供应商也可以使用的格式。
- 了解元数据是否可以被保存和迁移。

²² OCCI - Open Cloud Computing Interface

- 如果需要可以采用第三方数据保管服务。
- 理解任何定制工具都可能需要重新开发，或者新的供应商必须提供这些工具或者承诺迁移（与支持）这些工具。
- 检视和审计以确保新旧服务供应商的控制点有效性是一致的。
- 确保法务和合规原因所需的日志、访问记录和任何其它相关信息的备份和其它拷贝可以迁移。
- 了解管理、监控和报表接口以及它们在不同环境间的集成。
- 迁移之前测试和评估所有的应用程序，如果可行的话在切换之前采用双系统并行

私有云

私有云是云消费者在企业内部运行云环境/服务，或者采用云供应商所提供的私有云服务（通常是将企业内部网络延伸到供应商的托管中心）。

- 确保常见 Hypervisor,例如 KVM、VMware、Xen 之间的互操作性。
- 确保管理功能采用标准的 API 例如：用户和权限管理、虚拟机镜像管理、虚拟机管理、虚拟网络管理、服务管理、存储管理、基础架构管理、信息管理等等。

公有云

公有云的互操作性意味着开放出最通用的云接口。它们可能是厂商特定的或者象 OCCI、Libcloud 等等这样的开放的规范和接口。

- 确保云供应商开放出可以访问其服务所有云功能的通用的与/或开放的接口。

混合云

在混合云场景下云消费者的本地私有基础架构需要具备与外部云供应商协同工作的能力。一个常见的场景是“云爆发”(Cloud Bursting)，在这个场景下企业借用外部云供应商来分担高峰需求时的负载。

- 确保云供应商开放可以访问其服务中所有云功能的通用的与/或开放的接口。
- 确保可以与不同云供应商进行联邦的能力以实现更高水平的可扩展性

参考资料

- [1] <http://msdn.microsoft.com/en-us/library/cc836393.aspx>
- [2] <http://blogs.msdn.com/b/eugenio/archive/2010/01/12/adfs-wif-on-amazon-ec2.aspx>
- [3] <http://download.microsoft.com/download/6/C/2/6C2DBA25-C4D3-474B-8977-E7D296FBFE71/EC2-Windows%20SSO%20v1%20--Chappell.pdf>
- [4] <http://www.zimbio.com/SC+Magazine/articles/6P3njtcljmR/Federation+2+0+identity+ecosystem>
- [5] <http://www.datacenterknowledge.com/archives/2009/07/27/cloud-brokers-the-next-big-opportunity/>
- [6] http://blogs.oracle.com/identity/entry/cloud_computing_identity_and_access
- [7] http://www.opengroup.org/jericho/cloud_cube_model_v1.0.pdf
- [8] <http://www.burtongroup.com>
- [9] <http://www.pkware.com/appnote>
- [10] <http://www.apps.ietf.org/rfc/rfc4880.html>



第三部分 // 云的运行

D7: 传统安全、业务连续性和灾难恢复

云计算作为一种广受欢迎的 IT 运营外包技术出现以来，云计算这种托管模式所带来的安全问题正受到批判，云计算安全变得越来越重要。云计算概念的内在风险是如何确保储存在第三方或纯粹云计算服务提供商(CSP)²³处私密和敏感数据的安全。

云计算服务模式已经演变到企业实体只需要付出较少的成本就可以做更多的事情：也就是说，提供较少的资源，但能得到更好的运营效率。这对于企业经营来说则能够获得很多实实在在的好处。但是，云计算存在很多内在安全风险，在企业具有足够的信心决定把他们的 IT 需求外包给云计算服务提供商之前，不得不去评估和试图解决这些安全风险。

本安全域的一个目标是帮助云用户去形成一个对云计算服务相关的传统安全（物理安全）共识。传统物理安全被定义为采取一些安全措施来确保数据和人员的安全和物质存在，防止被盗窃、间谍活动和蓄意破坏。在云计算信息安全上下文中，这些资产指的是信息、产品和人员。

*本节于云控制矩阵的IS-01 和IS-02
以及ISO/IEC 27002 的第9 条款对应。*

正确的信息安全方案一般是采取多层安全机制来达到其安全目标，也就是通常所说的多层安全或深度防御。当实施安全措施时，管理员应该认识到，没有哪个安全措施是百分之百安全的。信息安全必须采取深度和多层防御的方法来达到一个综合安全水平。这些安全层中的任何一个脆弱点都可能导致安全被破坏。物理保护只是多层安全防御战略以确保云计算信息安全中的一个最初步骤。如果针对云计算的物理保护不存在、没有正确实施、保护力度较弱、安全执行不一致、或者只是作为一个项目对待（做完了事），则最安全的逻辑层面措施也无法弥补物理安全上的弱点，后果是，可能导致安全防护整体失败。

一种有效的传统安全流程是，首先需要一系列完好设计的风险评估、脆弱性分析，以及对业务连续性计划和灾难恢复（BCP/DR）策略、过程和流程的经常审查和测试。一个设计完好的物理安全程序应该是，物理安全可随着业务扩展，在组织内部可重复、可测量、可持续和站得住脚，整个过程能够在一个经常性的基础上进行持续改进，并且经济有效。

概览：一些和云计算相关的安全风险是云计算所特有的，在这种情形下，一个云计算服务提供商的业务连续性、灾难恢复和传统安全环境都需要全面评估（比如，采用标准的工业指南如 TOGAF²⁴、SABSA²⁵、ITIL²⁶、COSO²⁷或 COBIT²⁸）。本安全域解决一下安全问题：

- 建立一个物理安全机能

*本节对应云控制矩阵 FS-01, FS-02,
FS-03, 和 FS-04, 以及 ISO/IEC 27002
第9 条款。*

²³ CSP - Cloud Service Provider

²⁴ TOGAF: (The Open Group Architecture Framework, 开放组体系架构)

²⁵ SABSA: (Sherwood Applied Business Security Architecture, 舍伍德可执行业务安全体系)

²⁶ ITIL - Information Technology Infrastructure Library

²⁷ COSO - Committee of Sponsoring Organizations

²⁸ COBIT - Control Objectives for Information and Related Technology

- 人力资源物理安全
- 业务连续性
- 灾难恢复

7.1 建立一个传统安全机能

很多组织经常忽略那些 IT 设备、网络技术和通讯网络上过时的物理安全措施。这将导致很多组织在楼宇里安装计算机设备、网络和网关时，都没有采取正确的、可确保资产安全或维护方便的物理设施。

要为云计算环境中的 IT 设备、网络技术和通讯资产建立恰当的物理安全，将责任落实到云计算服务提供商组织中具体的人员是至关重要的。在云服务提供商组织内部，一个承担具体管理职责的个体有责任对相关的规划和程序进行有效的管理、规划、实施和维护。负责物理安全的员工需要接受培训，并且需要评估其工作能力。为了建立适合云计算环境的物理安全机能，必须考虑以下问题：

- 各受保护设备和服务的安全需求
- 被安排来负责物理安全的人力资源情况
- 将遗留应用迁移到云之前，对其物理安全是如何管理和分工的
- 可投入到安全方面的资金情况

物理安全可以是如增加一扇带锁门一样简单，也可以像实施一个包括障碍物和武装安全保卫人员的多层安全防御方案一样复杂。一个正确的物理安全实施方案应该使用多层防御概念，采用恰当的组合，通过阻止和延迟物理安全威胁来对风险进行管理。对基础设施、人员和系统构成物理安全威胁的攻击不只是局限在入侵行为。为了抵御这些风险，必须组合部署各种主动和被动防御措施，这些措施包括：

- 用来阻止和延迟事件、事故和攻击的障碍
- 用来监控安全和系统环境状态的检测系统
- 用来击退、拘押或劝阻攻击者的安全响应措施

物理安全在设计和实施时通常采用如下几种形式之一：

- 环境设计
- 机械的、电子的、程序控制
- 检测、响应和恢复过程
- 人员识别、认证、授权和访问控制
- 安全策略和过程，包括对人员的培训

7.1.1 安全物理安全评估

当评估一个云服务提供商的传统物理安全时，云用户需要 IaaS 多个方面的信息，或者基础数据中心提供商的物理存在相关的信息，这包括物理设施的物理位置，以及对关键风险和恢复要素的文档记载等等。

7.1.1.1 CSP 设施的物理位置

云用户应该对数据中心的物理位置进行一个关键评估。如果它们依赖于一个云供应链，清楚地知道云基础设施的哪些部分存在依赖性是非常重要的。

以下是在评估设施物理位置时的一些建议：

- 检查这些设施的位置是否位于任何地震活跃地带，以及地震活动可能造成的风险。
- 这些设施不应该位于存在以下风险的地理区域：洪水、滑坡或者其它自然灾害
- 这些设施不应该位于那些高犯罪率、政治或社会动荡的区域
- 检查对这些设施的位置的可达性（以及不可达可能发生的频率）

7.1.1.2 文档审查

那些支持业务恢复操作的文档对于评估托管企业能在发生灾难性事件时及时响应的能力是至关重要的。当我们准备和一个物理数据中心提供商签约前，以下的文档集合应该被审查：

- 风险分析
- 风险评估
- 脆弱性评估
- 业务连续性计划
- 灾难恢复计划
- 物理和环境安全计划
- 用户账户终止流程
- 意外事件计划，包括测试计划
- 事故报告和响应计划，包括测试协议
- 应急响应计划
- 设施结构图—应急出口、CCTV 监控头位置、安全入口等
- 消防疏散示意图和消防指令程序
- 紧急情况转移计划和流程

- 危机通讯流程
- 紧急情况联系电话号码
- 用户设施访问审查/审计日志
- 安全意识培训文档、报告和传单等
- 安全意识出席记录
- 关键主管的连续性计划
- 技术文档—走线图、BMS、UPS 和 AHU 细节
- 电力、发电机和 CCTV 监控头的维护规划
- 紧急情况燃料服务供应商合同
- 可以进入设施内部的授权人员名单
- 安全人员档案-生物和背景信息
- 安全人员的背景检查报告（必须每年执行一次）
- 对关键设备和设施的每年维护合同（主要关注 SLA²⁹中的设备/设施的停机和恢复时间）

当审查这些文档的时候，有一些需要云服务购买者重点关注的地方以确保可以减低他们使用云服务的风险。当云用户将他们的业务迁移到云计算平台中，需要确保他们的业务和利益，以下的建议也许证明是非常关键的：

- 检查是否所有的文档都是最新的。这些文档必须被 CSP 每年至少审查一次。文档中必须包含维护时间和维护者签名，以便可以验证这些文档确实在内部被审查过。
- 此外，策略和流程文档（从雇员视角看）必须是可以通过公共的 Intranet 网络可以获取的，CSP 中被授权的雇员可以在任何时间访问这些文档。安全团队必须足够小心，以确保这些被更新的文档是最新版本并且被管理员及时确认过。
- 所有的策略和流程只有当雇员有意识遵照执行时才是有效的。最后，我们需要检查一个 CSP 是否有到位的安全意识程序计划。至少，CSP 应该确保雇员接受了足够的安全意识培训，至少每年一次，并签字保证。此外，新加入组织的雇员应该接受一个安全谈话作为新员工就职程序的一部分，对这些关键的策略和流程必须维护正式的签到记录，并且是在任何时候都是可以审查的。为了使得这个程序更有效，必须请安全团队老员工来执行安全谈话。

7.1.1.3 国际/工业标准安全合规

确保云服务提供商实现诸如全球安全标注 ISO 27001 信息安全管理体或者其他工业标准，诸如 TOGAF、SABSA、ITIL、COSO 或者 COBIT 的合规。合规活动将被证明为云服务提供商的安全级别和成熟度评估提供了价值。

²⁹ SLA - Service Level Agreement

- 验证合规性证书以及其有效性。
- 寻找资源分配的可验证的证据，例如为了维持合规性项目的预算和人力资源。
- 验证内审报告和审核发现补救措施的证据。

7.1.1.4 实地考察 CSP 设施

覆盖区域

数据中心边界安全评估时，应确定哪些方面需要物理覆盖。以下为应确保安全的高风险区域：

- 管理区
- 前台
- 停车区
- 储物区
- 火灾出口
- 有线电视指令室
- 空气处理机房
- 更衣室
- 不间断电源室
- 发电室
- 燃料存储罐

标志

检查下列标志应在适当的地点显著展示：

- 火灾逃生路线图和紧急出口
- 火灾指令须知
- 消防安全标志
- 安全海报和指示
- 制止尾随海报
- 温度/湿度相关信息
- 警告和指导标志

- 紧急联系号码
- 事故升级流程图

7.1.2 安全基础设施

边界安全作为阻止入侵者和不必要访问者的第一道防线非常重要，随着技术进步，边界安全的原则已经发生了翻天覆地的变化。边界安全针对有意访问设施的入侵者，可以用威慑（Deter）、检测(Detect)、延缓(Delay)和拒绝(Deny)等 4 个 D 来概括。

选择物理基础设施提供商上，以下特质应优先考虑。根据不同的云服务供应商的设计和功能，应严格按照过程遵循下表。应当关注以确保物理基础设施具有适当的大小、性质和经营规模。安全控制应战略性地部署和符合可接受的质量标准，并与普遍准则和最佳实践保持一致。

- 安全入口点 - 访问控制系统（感应卡/生物识别门禁）
- 访问控制系统相关联的火灾紧急释放控制面板
- 动作传感警报系统，热跟踪设备，玻璃破损检测
- 火灾安全设备 - 湿喉，消防栓，软管，烟雾探测器和水喷头
- 灭火器
- 火灾出口（务必不上锁或者阻塞）
- 安全出口紧急门闸
- 警报器和警报灯
- 有线电视摄像机和数字视频记录服务器在（包括备份时间轴）
- 门关闭和延时报警器
- 数据中心内气体灭火器
- 打印机旁的碎纸机
- 消磁设备和磁盘粉碎机
- 紧急响应小组工具包(ERT Kit)
- 保安人员双向无线设备（头戴对讲机）
- 保安桌下和隐蔽有利位置的胁迫告警
- 入口处门框式金属探测器和手持金属探测器（如需要）
- 保管重要文件和媒体的防火保险箱

7.2 人力资源物理安全

人力资源物理控制的目的是最小化接近数据的相关人员，干扰运行和危及云服务的风险。一个能够接触到控制台的有经验入侵者能够通过重启系统或者访问当前已经是 root 或者管理员权限的系统绕过大多数逻辑保护措施。配线间可能被用来隐蔽访问或者破坏现有网络。应考虑如下手段：

本节对应云控制矩阵 IS-15, FS-05, FS-06, FS-07 和 FS-08 以及 ISO/IEC 27002 第9 条款。

- 角色和职责（通过类似 RACI: Responsible, Accountable, Consulted, and Informed）方式的控制矩阵）
- 背景调查和审查协议
- 雇佣协议（保密协议）
- 公司策略的认知和培训（代码和商业行为）

角色和职责是云计算环境的一部分，通过角色和职责，人、流程以及技术集成一起，形成了支撑租户安全的统一基础。职责分离（SOD），即要求完成端到端交易或者处理过程至少需要两名人员具备分离的工作职责。避免利益冲突对于保护云计算用户是必要的，应该通过建立监控手段以规避该风险。职责分离起源于财务和会计管理，职责分离的好处已被扩展至满足其他风险消除需要，如物理安全、可用性和系统保护。职责分离通过消除高风险组合来实现，例如，不允许相同的人员担任批准订单采购和有能力和进行支付的角色。这一原则被应用于云的开发和运行的职责划分上，同样也应用于软件开发生命周期。常见情况下，云的软件开发即为分离状态，确保在最终交付物内不含有未授权的后门留存，确保不同人员管理不同的关键基础设施组件。此外，给予员工履行其职责所需的最小访问特权将进一步减少但并不是消除风险。职责分离和最小特权/访问是支持云服务提供商达成保护和影响组织信息资产目标的原则。云安全管理程序要求关键角色和职责的分配将由特定个体或者组织完成。这些角色和职责必须被组织信息安全策略框架正式定义，并被高级管理人员参照 GRC（治理、风险和合规）义务和责任正式审核和批准。

此外，开发有效的人力资源安全必须包括雇佣和保密协议，背景调查（在法律允许范围内）以及合法的雇佣和终止手段。作为额外措施可考虑是否适用于所有领域的组织，包括正式的工作描述、适当的培训、安全许可、工作轮换以及敏感或者高风险角色员工强制休假。

7.3 评估 CSP 安全性

一些与云计算相关的安全风险是特有的，部分原因是存在一个扩展的以数据为中心的产销监管链，在这种背景下，需要参照行业标准，对云服务提供商的业务连续性、灾难恢复和传统的安全环境进行彻底评估。

云计算服务提供商的基础设施的传统或物理安全很重要，需要按照各种参数进行彻底的评估。这是一个具有高度相似性的领域 - 云和非云计算数据中心的安全性要求是非常相似的。

对 CSP 的“人员、流程、技术”模式或理念有一个全面的观点和理解，将极大地有助于评估 CSP 的成熟度，标记还未解决的问题，并提出实现安全的解决方法。在继续之前，这些问题必须得到解决、批准和关闭。

组织的成熟度和经验对有效处理物理安全的程序和任何可能出现的突发事件有很大贡献。总是有很强人为因素参与有效管理物理安全程序。管理层的支持程度和安全领导的能力水平是保护公司资产的关键因素，而管理层的支持至关重要。

物理安全通常是第一道防线，防御未经授权以及经授权访问一个组织的实物资产，防御物理窃取档案资料、商业秘密、工业间谍活动和欺诈。

7.3.1 程序

云服务提供商应确保可以应用户要求提供下列文件用于审查：

- 第三方提供的背景调查（每年一次）
- 保密协议（NDA）
- 实现“需要知道”和“需要具备”的政策，用于信息共享
- 职责分离
- 用户访问管理
- 定义职位描述(角色和责任)
- 基于角色的访问控制系统
- 用户访问评审

7.3.2 安保人员

人工监测和干预是必要的，由警卫、监管人员和管理职员组成的物理安保人员应该部署(基于 24×7 的基础)在 CSP 的基础设施处。

除其他事项外，站点和岗位指导应包括以下内容：

- 检查员工、合同员工和访客的凭证并使用登记日志
- 发放和回收访客证件
- 遏制尾随员工
- 管理访客和在设施内的行动
- 处理安全相关的电话呼叫
- 监测入侵、火灾报警系统和调度人员响应警报
- 对材料进出建筑进行控制并强制执行物业进入规定

- 强制执行建筑物相关的规章制度
- 在设施内巡逻
- 闭路电视监控
- 钥匙控制和管理
- 执行应急响应程序
- 升级安全相关的问题到安全经理
- 接收和分发邮件
- 在办公室内陪同无人随行的商务访客

7.3.4 环境安全

安全服务提供商的设施需要通过实施控制来保护人员和资产，以保护环境免遭危害。这些控件包括但不限于：温度和湿度控制器，烟雾探测器和自动灭火系统。

7.3.4.1 环境控制

- 数据中心应根据公布的内部标准，本地和/或地区的法规或法律，配备支持特定环境的设备，包括紧急/不间断电源。
- 必须保护环境控制所需的设备，来减少来自环境的威胁和危害的风险，及降低对信息未经授权访问的风险。

7.3.4.2 设备的位置和保护

被列为包含限制或机密信息的系统，必须考虑以下控制：

- 设备放置在一个物理上安全的位置，以尽量减少不必要的访问。
- 环境条件，如湿度，会对计算机系统运行产生不利影响，需要受到监控。
- 安保人员应考虑在附近的楼宇发生灾难的潜在影响，例如，邻近建筑物发生火灾，从屋顶或地面以下楼层发生的漏水，或街上的爆炸等。
- 彻底销毁和处置废弃媒质的方法（例如，磁盘驱动器）。

7.3.4.3 设备维护

为了确保设备持续的可用性和完整性，需要按照设备维护控制进行恰当的维护，包括：

- 按照供应商推荐的维修间隔和规范维护设备。
- 仅允许授权的维修人员进行设备的维修和服务。

- 维护所有可疑的或实际故障和预防性及矫正性维护的记录。
- 当发送设备离开场所进行维护时，使用适当的控制。适当的控制措施的例子包括适当的包装和密封容器，存储在安全可靠的地方和清晰完整的运输和追踪指导。
- 维护适当的资产控制政策和程序，包括保留所有硬件、固件和软件及追溯性、责任制和所有权的记录。

全面评估 CSP 的设施将使未来的用户理解和评估安全程序的成熟度和经验。一般情况下，专注于 IT 安全，物理安全仅获得有限的关注。然而，威胁场景盛行的今天，当务之急是物理安全应受到应有的关注。尤其是在一个客户的数据可能与许多其他共同托管的客户（包括竞争对手）共存环境中，物理安全承担更大的意义。物理安全是防御入侵者和恶意访问 CSP 设施的企业破坏者的防线之一。

7.4 业务连续性

传统意义上，信息安全的三大宗旨是保密性、完整性和可用性。业务连续性则涉及上述三方面需求的持续性部分。向云服务提供商的过渡将包括对供应商合约承诺的正常运行时间进行评估。然而仅通过服务水平协议（SLA）可能还无法满足客户，应充分考虑典型业务中断造成的潜在影响。鉴于近期受人关注的第三方服务中断，作者建议业务连续性维护应作为维持业务运营的关键保障。

应参考下文所述的指南进行特定服务的连续性维护。尽管与第三方提供服务（例如云）相比，大量指南更倾向被内部提供服务所采用，但这些指南的编写也可以成为定义第三方服务责任的依据。

7.5 灾难恢复

对于 IT 而言，云存储最有趣的一方面是如何利用它来完成备份与灾难恢复（DR）。云备份与灾难恢复服务的目标是降低基础架构、应用以及总体业务流程的成本。云备份与灾难恢复应该是一种可靠，相对廉价且容易管理的服务。云存储、云备份与灾难恢复所面临的挑战主要包括可移动性，可用性，可扩展性，信息如何传入传出云，保障最佳的业务连续性以及计量计费。云灾难恢复构建于以下三个基础要素：一个完全虚拟化的存储基础架构，一个可扩展的文件系统以及一个可以应对客户紧急业务需求的自服务灾难恢复程序。

客户将灾难恢复迁移到云之前应该先确认服务提供商的灾难恢复项目中包含下述组织或团队：

- 应急响应团队（ERT）
- 危机管理团队
- 事件响应团队

要按照危机处理流程仔细核查上述团队的构成。

7.5.1 恢复优先级

核查服务提供商的恢复计划文档：计划应该包括优先级（决定恢复顺序）的细节信息，其内容应该与合约中承诺的 SLA（决定于客户所购买的服务以及服务的关键程度）相符合，RPO（恢复点目标）和 RTO（恢复时间目标）是两个重要的服务指标，应该包含在恢复计划之中。

在恢复过程中也需要认真设计和实现信息安全控制，这一部分需要考虑的细节信息如下例：

- 明确需要介入恢复过程的员工
- 备用站点的物理安全控制如何实现
- 与恢复过程相关的特定的依赖关系（供应商和外包服务合作伙伴）
- 当主站点不可用时，备用站点的地理位置要尽可能集中

7.6 权限

- 确保配备了必要的设施。
- 采用彼此相互强化的，集成式的物理与逻辑安全系统。
- 建立服务等级协议，要遵循对供应链后端所负有的安全职责和义务。

7.7 建议

7.7.1 策略建议

- 云服务提供商应该为那些在安全方面要求严格的客户建立一个安全基线（内容可包括系统，设施和流程等）。这些安全指南不应给客户体验带来负面的影响，严格的安全指南应该是经济的，并且可以有效地降低企业人员、公司收入、声誉和股东价值等方面所面对的风险。
- 另外，云服务提供商也要为低安全需求的用户建立安全基线，或者为所有用户提供一个基线，在此基础上为那些有需求的用户提供更多的附加服务选项。对于后一种情况，提供商应该意识到有些客户只对那些仅提供高安全等级服务的服务商有兴趣。服务商必须在系统，设施和流程等方面就安全等级进行权衡。
- 云服务提供商应该严格划分工作职责，实行背景调查，要求并强制员工签署保密协议，并基于最小权限原则限制员工获取客户的信息。

7.7.2 透明性建议

- 为了表明在安全方面的态度，云服务提供商需要提高服务的透明度。现场参观云服务提供商的设施和数据中心可以帮助用户更好地评估服务水平，清楚地理解各种安全标准。但是，云计算具有按需置备和多租户等特性，传统形式的审计和评估可能不适用，或者需要修改（如共享式访问与第三方检查）。

- 为了增加现场评估的效力，应该在没有事先通知的情况下（如果需要事先通知，指定一个较宽泛的时间窗口而不是一个特定的时间）拜访云服务提供商的设施或数据中心。这样可以保障用户在一个平常的工作日里进行一次真实的评估，而不是由云服务提供商在客户或第三方访问时装装门面。
- 如果需要直接检查，评估团队应该由两名或更多来自 IT、信息安全、业务连续性、物理安全和管理部门（如部门首脑或数据所有者）的专家组成。
- 在访问之前，客户应该索取业务连续性计划和灾难恢复文档，包括相关的证书（基于 ISO，ITIL 等标准），审计报告和测试协议。

7.7.3 人力资源建议

- 客户应该检查云服务提供商是否为保障物理安全而部署了能胜任工作的安全人员。建议配置一名负责领导和推动物理安全项目的专职安全经理。业界顶尖的认证可以帮助你验证工作人员在物理安全方面的知识和技能，例如 **CISA**³⁰，**CISSP**³¹，**CISM**³²，**ITIL**³³，or **CPP**³⁴ (from **ASIS**³⁵)。下面是一些具有代表性的认证：
- 客户应该索取一份全面介绍安全经理及其组织的报告。它可以帮助你判断该位置上是否安排了尽职尽责的人员。安全经理应该向部门主管或 GRC 委员会报告，而不是向物业或 IT 人员报告。为了保证这一职位的独立与客观，最好可以通过其它途径（如通过 CRO 或公司高管）向 CEO 报告。

7.7.4 业务连续性建议

- 已部署服务的连续性通常由第三方在合约中做出承诺，客户只需要审查合约，但实际上客户才是实际的数据管理者，因此有必要对服务商的能力做深入的分析。对于个人数据，通常要遵循特定的法规要求，采取相应的控制手段。即使采用第三方数据处理服务也是如此。
- 客户应该审查第三方的业务连续性流程和特定的认证。例如，云服务提供商可能取得了 **BS25999**，即业务连续性管理英国标准。客户可以审查这一认证的范围和评估细节记录。
- 客户应该对云服务提供商的设施进行现场评估，以确认和验证服务商为保证服务的连续性所采取的控制手段。如果要检验特定业务连续性计划的实现，一般不应采取这种不事先通告的服务商设施评估，因为这一类实现只有在灾难或事件发生时才会被启用。
- 客户要保证自己在云服务提供商执行完任何的业务连续性计划或灾难恢复计划测试之后都能收到确认。要特别关注的是，服务商确实是通过模拟重大事件发生来进行测试的，并通过文档承诺服务的可用性将得到保障。这在许多的建议中都曾经提到过。客户应该对业务连续性和灾难恢复测试的正式报告给予特别重视，要清楚地了解测试是否满足合约中所承诺的服务级别。不要等待灾难真的发生时才重视。

³⁰ **CISA** - Certified Information Security Auditor，认证的信息安全审计员

³¹ **CISSP** - Certified Information System Security Professional，认证的信息系统安全专家

³² **CISM** - Certified Information Security Manager，认证的信息安全经理

³³ **ITIL** - Information Technology Infrastructure Library，信息技术基础架构库

³⁴ **CPP** - Certified Privacy Professional，认证的隐私保护专家

³⁵ **ASIS** - American Society for Industrial Security，美国工业安全学会

7.7.5 灾难恢复建议

- 使用云服务的客户不应依赖单一服务商的服务，应该制定一个灾难恢复计划，明确当前服务商失去服务能力时，如何对业务系统进行迁移或故障切换。
- 基础架构云服务商应该在合约中约定，采用多种平台来提供服务，且必须拥有在服务受损之后可用于快速恢复系统的工具。
- 数据验证应该是一个自动化的，或者基于可由用户启动的验证协议，以便客户可以随时检查他们的数据，从而确保数据的完整性。
- 增量备份可以按照系统用户所设定的间隔为所有受保护系统或快照更新副本。消费者可以根据恢复点目标来决定设置。
- 可以通过一个用户驱动的，自助服务的门户来访问全站、系统、磁盘和文件恢复服务，这样用户就可以灵活地选择他们想要恢复哪个文件、磁盘或者系统。
- 云服务提供商应该提供快速的，符合服务等级协议的数据恢复服务。
- 服务等级协议应该预先协商好，客户只需要购买他们所需要的服务。所有的数据、文件或系统都应该在30分钟以内恢复。
- 客户与物理站点之间的应该采用广域网优化技术，在确保数据可移动性的同时还可以减少带宽和存储设备的利用率，从而节省成本。

7.8 要求

- ✓ 所有相关方面都必须确保基础架构的设计是满足物理安全要求的。
- ✓ 所有供应链的参与方应该顾及到威慑、侦查以及验证解决方案的相关性。
- ✓ 最终用户必须检查、记录和修正来自云供应链中其它成员的人为风险。必须通过正确的责任分工和最小权限访问原则设计和实现一种主动发现和消除人为风险的方法。

D8: 数据中心运行

为了云计算的发展，提供商不仅仅是利用简单应用虚拟化技术来管理服务器资产，更必须升级企业的数据中心。为了实现业务敏捷性，绿色技术，提供商开放性，鼓励电力和数据中心的建设与管理中涌现的越来越多的创新理念，数据中心应该寻求向云计算上的长期成功而转变。

“下一代数据中心”，一个已经被提出好几年的术语，现在已经发展成为数据中心的运行，包括数据中心内的商业智能适应，对数据中心的运行的应用程序的了解，以及大规模分析集群的托管。数据中心不再是一个独立的实体，而是和应用一样灵活并且与其他数据中心连接的实体，因此延迟以及安全都要管理。

概览 本单元将讨论以下主题：

- CCM 相关的物理安全方面的考虑
- 自动化数据中心使用案例
- 新型数据中心？家庭云计算（Cloud computing at home）
- 云基础设施分散部署和数据中心

*CCM 的注意事项以及云数据中心的
新思路如何互相影响*

8.1 数据中心运行

本节中的新概念：

- **云应用任务** 安置在数据中心内的行业或应用任务。例如，一个医疗保健或电子商务应用任务。
- **数据中心分散部署** 协同运行的但是分布在独立物理区域中的云基础设施。

基于服务的自动化和以预测分析，使服务为基础的自动化在很长一段时间内被信息技术服务管理（Information Technology Service Management³⁶，ITSM）所代表，ITSM 使用信息技术基础设施库（Information Technology Infrastructure Library³⁷，ITIL）标准指导数据中心的发展。

安置在数据中心内的不同类型的应用程序需要自动化。当理解了数据中心中正在运行什么以及数据中心需要如何作为一个整体来应对不同的使用时，数据中心的经营者将大大受益。

云安全联盟撰写的“云控制矩阵”根据不同的标准和管理需求制定了相应的一些物理要求。数据中心的专业人员应阅读本版指南中的“物理安全”单元和“云控制矩阵”以理解数据中心内部和外部的需求。为方便读者参考，下表举例说明了数据中心中的不同应用程序的任务所需的控制。该列表并不详尽但提供了一些交叉引用“云控制矩阵”和规范的应用类型或任务的示例。

³⁶ ITSM - Information Technology Service Management

³⁷ ITIL - Information Technology Infrastructure Library

表1——应用任务控制

应用任务	控制	规范
医疗保健（HIPAA） ³⁸	设施安全-安全政策	应建立政策和规程以保持办公室，房间，设施和安安全区域中的安全工作环境
卡处理/支付（PCI） ³⁹	设施安全-用户访问	应限制对信息资产的物理访问以及用户和保障人员的权限功能
发电（NERC CIP） ⁴⁰	设施安全-受控的访问点	应实施物理边界安全（围栏，围墙，栅栏，守卫，门，电子监控，物理验证机制，接待处，安保巡逻）来保护敏感数据和信息系统

上表不再在本章赘述。读者可以参考“云控制矩阵”并根据相关组织希望遵守的标准或必须遵从的规范。

数据中心中运行的包含管控信息的应用程序（受信息安全或应用程序安全标准管辖）将被审核。数据中心运营商进行的物理审计结果可以公布给数据中心运营商的客户或由应用程序查询基础设施如云审计提供的基础设施来发布。

在以往版本的“指南”中，读者被指示建立自己的审计。对于很多数据中心运营商或云提供商来说，该做法可能不可行。在多租户的环境中，运营商或提供商通常不能满足对每个用户的访问进行审计。用户应该要求运营商或提供商提供独立的审计结果。

这个想法带来了服务自动化。通过基于应用任务的自动化的报告，日志，以及审计结果的发布，数据中心运营商能够使它们的用户确信，数据中心的具体管制措施是到位并令人满意的。云审计，云信任协议和 CYBEX（X.1500）能通过一个通用的访问接口自动发布审计结果。

数据中心的更进一步的自动化依赖于包含数据中心资产的库。通过理解库中的资产如何使用数据中心中的资源，运营管理中心可以预测哪些租户正在使用资源。如果数据中心使用如 PoD⁴¹和虚拟数据中心 VMDC⁴²的理念，那么数据中心就能足够灵活使其可以迅速促进云或虚拟化业务。

8.1.1 新型和新兴模型

最近（2011年夏天）出现了更多关于家庭（home-based）云平台的新闻。在这些类似 SETI@home⁴³模型的基础设计类型中，云是基于志愿者提供其家中或办公室中的电脑的计算资产来支持其他的应用。这些情况下数据

³⁸ HIPAA-医疗保健信息转移和保护行为

³⁹ PCI-支付卡行业。具体来说，PCI-DSS 是数据安全标准

⁴⁰ NERC CIP-北美电子可靠性公司关键基础设施保护（North American Electric Reliability Corporation Critical Infrastructure Protection）

⁴¹ PoD-交付点。一个机架化的聚合了电源，计算，存储访问和网络组件的单元。

⁴² VMDC-虚拟多租户数据中心。与 PoD 类似，使用模块化的，容易机架化的组件来快速扩展数据中心。

中心由每个志愿者的家组成。这些类型的云在以社区为基础的应用托管环境中将可以良好运行，但这种环境不是标准中可审核的规范环境。例如，如果一个云建立在 100,000 个家中的计算机之上，可能就没有办法来审计这样一个被有效分割成 100,000 个部分并且分散在一大片地理区域的数据中心。这种类型的基础设施可以托管基于兴趣（如读书俱乐部）或住宅信息网站的基于社区的应用。

云正越来越多地被视为一种商品或一个工具。因为一些其他的原因，行业内正努力在为身份识别，互操作性和业务连续性而建立 SecaaS 或建设代理基础设施。这些应用将被分离并运行在特定的物理环境中，以满足组织或组织运行的应用程序的特殊需求。

数据中心分散部署将应用程序放置在需要满足特定管理需求的多个其他的专门数据中心中。通过将应用分散跨越多个物理边界，应用程序在云中的负担变轻了，但是更难于控制和管理。

8.2 权限

- 数据中心合作分散部署。跨越多个物理上没有关联的数据中心的自动化需要软件精心协调数据中心的请求来在审计中记录和报告生成日志。
- 数据中心属于个人的家庭共享云。标准和规范的审计在家庭共享云中几乎不可能实现。合规的环境和合乎标准的环境的控制要求也将在家庭共享云中遇到困难。可能在某些情况下应用程序的某些部分可以被分散部署到以家庭为基础设施中。

8.3 建议

- 建设云数据中心的组织应纳入管理过程，实践和软件来了解运行在数据中心中的技术并对它们做出反应。
- 购买云服务的组织应该确保提供商已通过服务管理流程和实践运行其数据中心，并且使用了机架化技术来保证数据中心中资源的灵活和高可用性。
- 了解在数据中心中正在运行哪些任务。在建或购买的数据中心必须满足“云控制矩阵”中的物理和资产控制要求。
- 数据中心的位置是重要的。如果技术和应用组件跨越多个数据中心，那么数据中心之间会存在延迟。
- 购买云服务的组织必须清楚地了解当遇到合规性要求时哪个部门应该为其负责，以及当进行合规性评估时他们和他们的云提供商所扮演的角色，并将它们记录成文件。

8.4 要求

云安全联盟拥有多种信息来源来帮助服务于云的数据中心的建设或改建。控制矩阵强调在一个非常广泛范围的安全标准和法规上的需求。云安全联盟的云审计和其他项目同样可以为数据中心的建设和管理以及其中运行的技术提供帮助。

⁴³ SETI@home - <http://setiathome.berkeley.edu/>

- ✓ 通过了解数据中心的运行方式来全面理解控制矩阵要求。使用其共同点以满足大部分应用程序的任务。
- ✓ 使用 IT 服务管理技术来确保可靠性，安全性，以及资产交付和管理。
- ✓ 如果数据中心为提供商所拥有，应通过一个规章制度和安全标准模板进行审计并将结果发布给用户。

D9: 事故响应

事故响应（IR - incident Response，下同）是信息安全管理的基础之一，即使最周详的计划、实施并执行了相关的预防性安全措施，也无法完全避免信息资产遭到攻击。因此，当机构转向云的时候，面临的核心问题之一就是：怎样才能有效处理关于云资源的安全事故。

云计算不需要一个新的事故响应概念框架，只需将原有的 IR 程序、处理机制和工具与云计算相关的环境对应起来。这一观点贯穿了本指南文档，通常情况下，需要首先进行对组织内 IR 功能的控制进行差距分析。

本部分（Domain）力图明确这些与云计算独有特性相关的 IR 差距项，供安全专家作为参考，用于 IR 生命周期中的准备阶段制定响应计划和指导相关活动。为了理解云计算对事故处理带来的挑战，我们必须明确云计算及变化的部署和服务方式给事故处理带来了什么特殊性。

本部分（domain）按照“事故响应生命周期”来编制，这是由美国国家标准技研究院的计算机安全事故处理指南(NIST800-61)定义的，并已经被业界广泛接受。首先确定云计算对 IR 最直接特征影响，然后将这些特征对应到生命周期的每个阶段，并探讨响应者应该考虑的问题。

概览 本部分将讨论如下题目：

- 云计算对事故响应的影响
- 事故响应生命周期
- 取证责任

9.1 影响事故响应的云计算特征

尽管云计算在很多层面带来了变化，但其中某些云计算的特性相比其他特性对 IR 活动更具有直接的挑战。

首先，由于云计算的按需自服务性质，客户在处理安全事故的时候很可能会发现很难甚至不可能从云服务商 (CSP)⁴⁴那里获得协助。服务和部署模式不同，客户与 CSP 的 IR 互动方式就会不同。关于安全事故的检测、分析、遏制（containment）和恢复能力通常已经被工程化到服务承诺中，这是 CSP 和客户需要重点关注的问题。

第二，云服务的资源池化，除了使云基础设施可提供快速弹性的交付外，可能还会导致 IR 过程复杂化，特别是作为事故分析的取证（forensic）活动部分，必须在高度动态的环境下实现，这对基本的取证工作带来了挑战，例如界定事故的范围、数据的收集和归属性、保留数据的语义完整性、维护全部证据不变性。这些问题当取证活动时会被强化，这是由于是在一个对他们不透明的环境下进行（取证）操作（就像前面提到的，这是云服务商必须提供的支持）。

⁴⁴ CSP - Cloud Service Provider

第三，在合租（co-tenants）场景下，如果没有关于隐私信息处理的妥协（compromising），资源池化的云服务方式，对于收集和分析事故的非直接数据和原始数据（telemetry and artifacts）（例如：日志、netflow 数据、内存、设备映像、存储等）可能会带来对隐私性问题的担忧。这是云提供商必须首要解决的技术挑战。同时，也取决于云服务消费者来确保他们的云服务提供商具备了适当的数据收集和分离流程、能提供所要求的事故处理支持。

第四，尽管没有被描述成云的基本特性，云计算可能导致数据跨越地理区域和司法管辖边界，对这种状况，客户可能并没有这方面的明确知识，后续的法律和监管的介入（implications）可能会对事故处理过程有不利影响，法律和监管的介入会在事故生命周期的各个阶段限制什么可以做/什么不可以做或者规定什么必须做/什么一定不能做。法律部门应该为机构或代表处的事故响应团队制订处理类似问题的指南。

云计算也给事故响应者带来了新的机会，对于云的持续监控机制，可以减少承担事故处理练习所需的时间或者事故响应。

虚拟化技术和云计算平台固有的弹性特质，会允许更有效率和效果的遏制（containment）和恢复。通常会比传统数据中心技术减少服务中断时间。并且在某些方面使得事故调查变得更容易，因为虚拟机可以很容易地被移动到试验环境中，在那里可以管理运行环境、取得鉴定映像并进行检查。

9.2 云结构安全参考模型

很大程度上，当涉及到云生态系统中的 IR，部署和服务模式决定了分工，参考 D1 中（Figure 1.5.2a 的云参考模型）提出的结构性框架和安全控制，将有助于标示出那个技术或过程单元，应该由那个机构负责并负责到什么层面。

云服务模式（IaaS,PaaS,SaaS）明确区分了客户对于基础 IT 系统和其它提供计算环境的基础架构的可见程度和控制程度，该模式适用于事故响应的各个阶段，本指南的其它域也是依据这个模式来处理的。

例如：对于 SaaS 解决方案，事故响应责任很可能几乎完全属于云服务商（CSP）。而对于 IaaS，很大程度上事故检测和响应的责任和能力主要属于客户。但是，即使是 IaaS，对云服务商也有明显的依赖性，源于主机、网络设备、共享服务、像防火墙等安全设备、及后端的管理系统的数据必须由 CSP 提供。有些供应商已经准备好了为他们的用户提供这种数据，某些管理安全服务商也正在大力推广处理云的这些数据的解决方案。

考虑到问题的复杂性，在 D1(图 1.5.1c)中描述的安全控制模式,及组织执行的与企业云部署相关联的具体安全控制活动，应该关联到 IR 规划，反之亦然。通常情况下，IR 控制关注更窄和更高层的机构需求，但是，安全专家必须保持更全面的视角，以确保 IR 的有效性，安全专家也有责任和权利介入到可能直接和间接影响（事故）响应的任何安全技术（手段）的选择、购买和部署过程中去。这最起码有助于划分 IR 生命周期各个阶段的角色和责任。

在审查云环境下的 IR 能力的时候，应该考虑云部署模式（公有，私有，混合，社区）。对于每一种部署模式，获取 IR 数据的难易程度会不同，模式不同所需的控制和责任也不同。在这部分（domain）中，主要关注的是公共端的问题。作者认为，云（应用）越私有，越需要开发适当的安全控制手段或者由服务商提供给客户更多安全控制手段，以提高客户满意度。

9.3 事故响应生命周期研究

NIST 800-61 定义了如下的事故响应生命周期的主要阶段：准备，检测&分析，抑制，根除&恢复。下面章节分析云计算对这些阶段带来的挑战，并为如何应对这些挑战提出了建议。

9.3.1 准备

当信息资产部署在云中时，准备可能是事故响应生命周期中最重要的阶段。识别事故响应的挑战（和机会）是信息安全专家在客户迁移到云之前应该提前进行的一项正式工作。如果机构这方面经验不足，可聘请外部专家进行咨询，并应该在每一次企业更新事故响应计划时进行。

下面讨论的每个生命周期阶段，将提出问题并给出解决建议，这可以用于指导给客户的规划过程。将结论记录到正式文档中，将有助于驱动利用任何机会对差距进行矫正。

准备（阶段）是从清晰了解和全面核查对客户的流动和驻留数据，考虑到客户的信息资产会分散在机构内，并可能跨地理边界，这会导致需要从物理和逻辑两个层面去进行威胁建模。采用对应到物理资产、组织机构、网络、管辖边界的数据流图，可以用于明确在响应时的依赖关系。

由于涉及到多个机构，服务水平承诺和多方合同变成了在事故响应生命周期各个阶段中沟通和实现对责任预期的主要依据。建议与各方共享事故响应计划，并且精确定义和澄清术语是明智选择，如果可能，任何模糊之处应该在事故发生前明确下来。

期望 CSP 为每个客户都建立一个特别的事故响应计划，但是，在合同或者(SLA)⁴⁵协议中给出的如下要点，能够说明 CSP 已经事先做出了事故响应计划，这样会提升客户（关于事故响应）的信心。

- 联系人，沟通渠道，可用的事故响应团队
- 服务商提供给客户和其他外部团体的事故定义和通知标准
- 云服务商为客户提供的检测事件的支持（例如：可用的事件数据，关于可疑事件的通知，等。）
- 定义安全事故处理的角色/责任，明确 CSP 提供的事故处理支持（例如：通过事故数据/处理过的中间数据的采集实现的取证支持，参与/支持事故分析等）
- 定义根据合同进行的常规事故响应测试责任方规范以及结果是否会被公开
- 定义事后分析活动的范围（例如：根源分析，事故响应报告，通过经验教训改进安全管理等）
- 在 SLA 中清晰定义 IR 中的供应商及客户的责任

一旦角色和任务确定，客户可以有效地培训事故响应团队，来处理那些他们有直接责任的事故。例如。例如，如果在 PaaS 环境下由客户负责应用，且云服务商承诺提供（或允许检索）平台的日志，客户自然需要具备技术/工具和人员对这些日志进行接收，处理和分析。对于 IaaS 和 PaaS，与虚拟化相关的能力及对虚拟机调查取证的

⁴⁵ SLA - Service Level Agreements

办法将影响响应效果。关于需要客户组织自身的特定技能的自行解决还是外包给第三方，要在准备阶段确认下来。请注意，外包需要由另外的一套合同/**NDA's**⁴⁶ (保密协议)来管理的。

必须准备好连接各介入方的沟通渠道。应考虑传输的那些信息是敏感的，用加密手段确保信息的完整性和真实性。最好参照现有标准进行应急响应过程中的沟通，以便于方便其他各方参与到调查中。例如，由(IETF)⁴⁷编制的事件描述和交换格式(IODEF)⁴⁸及相关实时网间防御(RID)⁴⁹ 标准，这些标准也被国际电联(ITU)⁵⁰包括在网络安全交换 Cybersecurity Exchange (CYBEX)⁵¹项目中。IODEF 定义了一个标准的 XML 语言模式，用于描述事故，RID 描述了一种标准方法来实现实体间关于事故信息的通信，至少是租户和云服务商之间的通信。

关于事故（响应）准备阶段最重要的事是对计划进行测试，测试应该是全面的并且组织全部可能参与到真实事故响应的各方参加。云服务商不一定有资源参与所有客户的测试；客户可以用角色扮演的方式确定哪些任务或信息需求是属于运营商的，这些信息将用于以后与运营商进行准备阶段的讨论。另一种可能是客户自愿参加云服务商可能已经计划的任何测试。

9.3.2 检测与分析

及时发现安全事故，和成功的进行事后事故分析（回答发生了什么，如何发生的，涉及到哪些资源等问题），依赖于相关数据的可用性，和对数据进行正确解析的能力。如上文所述，云计算同时带来了这双方面的挑战。第一，数据的可用性在很大程度上取决于云服务商提供给客户的资源，并可能被云计算的高度动态特性所限制。第二，分析工作涉及的基础设施，至少部分是由运营商所持有的，非透明化的。这使得分析作业变得复杂。由于客户只掌握有限的基础设施信息，加上云计算的动态特性，数据的解读变得困难，甚至成为不可能的任务。

暂不论事故分析面临的技术挑战，关于应如何在云环境中进行数字化调查，争取在书写记录时，最大化所持证据的证明力的这一问题上，也并不存在令人满意的答案。因此，在与云技术事故相关的司法案件变得更为普遍，和在被广泛接受的最佳实践性指导方案存在之前，云计算的安全事故分析结果存在无法被司法部门视为有效证据的风险。

在用于检测与分析安全事故的相关标准、方法和工具能够赶上云计算所带来的技术革新之前，事故的检测与分析将会一直是云环境中的重要挑战。云客户必须迎接这一挑战，确定己方掌握获取如下两项资源的途径：（1）与事故检测及分析相关的数据源及信息，（2）在所使用的云环境中进行事故分析的相关取证支持。

9.3.3 数据源

与任何 IT 集成托管服务（hosted IT service integration）中一样，应急响应团队需要确定适当的事件记录方法，以求能够有效的检测并识别那些影响其资产的异常事件与恶意行为。客户必须对三个问题进行评估，即哪些记录（以及其他数据）是可用的，如何收集并处理数据，数据会在何时，以何种方法由云服务供应商交付。

⁴⁶ **NDA** - Non-Disclosure Agreement

⁴⁷ **IETF** - Internet Engineering Task Force 互联网工程组

⁴⁸ **IODEF** - Incident Object Description Exchange Format 事件描述和交换格式

⁴⁹ **RID** - Real-time Inter-network Defense 实时网间防御

⁵⁰ **ITU** - International Telecommunication Union's

⁵¹ **CYBEX** - Cybersecurity Exchange

在客户侧，用于事故检测和随后分析的主要数据源是日志信息。以下几个有关的日志信息的问题必须被纳入考量。

- **应记录哪些信息？** 相关日志类型示例有：审计日志（例如网络活动日志，系统活动日志，应用程序活动日志，云管理角色及其访问活动日志，备份和恢复活动日志，维护和变更管理活动日志），错误日志（例如 Hypervisor 的核心消息报错日志，操作系统报错日志，应用程序报错日志等），安全性日志（例如，入侵检测系统日志，防火墙记录日志等），性能日志等。在现有日志信息中存在不足之处，须进行协商，并添加额外的日志源。
- **信息记录是否一致和完整？** 导致信息记录不一致的一个典型原因是信息源间的时钟同步处理失败。同样，缺少时区记录的不完整的信息记录，会导致在分析过程中，收集到的数据无法被准确地解读。
- **记录的信息是否充分反映出云服务的动态性质？** 云服务环境的动态行为也是一个导致信息记录不一致或不完整的常见原因。例如，在新的云资源（如虚拟机等）被添加加入网络环境以满足需要时，需要将新资源产生的相关日志信息添加到日志数据流之中。未能在日志信息中明确环境中发生的动态变化是另外一个可能存在的问题。例如，web 服务请求一定的 PaaS 组件这一事件被记录，但也可以是由这项服务的各种实例之一动态提供。信息不完整的问题，例如服务的请求，可能导致难于或无法进行正确的分析，例如，如果一个事件的根本原因是一个单一的不完全的事件。
- **与法规是否存在冲突？** 一些因素可能会限制日志数据的收集，储存、使用。它们包括使用同云空间的租户间的隐私问题，一般性日志数据的规定，和特定的个人识别信息的规定等。在不同司法管辖区中，数据处理或存储中所涉及的相关规定会存在差异。客户必须理解并重视这些规定。
- **日志应以何种方式保存？** 法律及合规要求会直接明确日志留存方式。云客户应理解并定义任何扩充的日志保存方式，以满足他们不断更新的对事故分析和取证的需求。
- **如何防止信息记录日志是防篡改的吗？** 为了进行准确的取证分析，确保储存的日志是防篡改的是至关重要的。可以考虑使用一次性记录设备，区分用于储存日志的服务器和应用的服务器，加强储存日志用服务器的访问控制，作为这一需求的关键因素。
- **信息记录应采用何种格式进行通信？** 日志数据格式的标准化是一个很大的挑战。运用通用格式（如一般事件表达法）可简化客户对数据的处理。

云供应商只能检测到一部分的事故。原因是这些事故发生在云供应商所拥有的基础设施的内部。需要特别注意的是，服务级别协议必须包含有关云供应商应及时，准确地通知云客户，以执行达成共识的事故响应。至于其他一些客户都有能力检测到的事故，云供应商进行检测可能更佳。云客户应该选择那些通过关联与过滤日志数据提供最佳的事件检测协助的云供应商。

云部署所产生的数据可能相当大的。也许需要去研究云服务供应商提供的有关日志过滤手段的可选方案，用于在交给客户之前减轻网络压力与客户内部处理的影响。其他一些应考虑的因素有，云服务供应商或云租户进行的分析与关联的水平以在取证（forensics）之前识别可能的事故。如果是由云服务供应商进行分析，那么事故调查的关键点（升级点和切换点）必须提前确定。

9.3.4 用于事件分析的电子取证与其它调查性支持

尽管还不成熟，在法律调查取证的社区中已经在尝试开发一些工具和协议，用以采集和检查特别是从虚拟环境中获得的与法律取证相关的产出物。同时 PaaS 和 SaaS 环境中所需要的电子取证支持也正在进行研究中。

客户要了解在进行事件分析时的电子取证需求，并要调研云服务供应商满足这些需求的程度，而且选择相应合适的供应商，并解决与自身需求间剩余的差距，这是非常重要的。不同的云服务和部署模式下，能够提供给客户的潜在证据的数量是有非常大差异的。

对于 IaaS 服务，客户可以在他们自己的虚拟机实例内进行调查取证，但无法调查云服务供应商控制的网络组件。此外，标准的电子取证活动，如通常的对于网络流量的调查，对于内存快照的访问，或是硬盘镜像的创建，都需要供应商提供支持。由于虚拟化而成为可能的高级电子取证技术，如在活动系统上生成虚拟机状态的镜像或者进行 VM 的自我测试，均需要云服务供应商提供取证支持。

对于问题根源发生在底层基础设施的 PaaS 和 SaaS 安全事件，云的客户几乎完全依赖于云服务供应商提供的分析支持，并且如之前提及的，必须对事件响应（IR）中的角色和职责在 SLA 中进行约定。对于 PaaS，客户的组织要对部署在云中的任何应用层代码负责。对于问题根源存在应用中（如应用代码中的缺陷）这类场景下的事件分析，需要进行充分的应用日志记录。这种情况下，云服务供应商的支持可以采取为应用日志的产生、安全存储以及通过只读 API 的安全访问提供便利的形式来提供。SaaS 供应商生成更广泛的客户特定应用的日志、提供安全的存储以及附加的分析功能，可以减轻客户一方的事件响应负担。这可能能够减少相当多的应用级安全事件。

那些使用他们自己的管理平面/系统来确定调查安全事件范围，识别系统中已经或正在遭受攻击的部分，并将这些数据提供给自己云的客户的供应商，将大大地增强所有服务模式下的响应能力。

为在特定云环境中进行事件分析做准备，客户的事件响应团队应使自己熟悉云供应商提供给客户的用以辅助操作和事件响应流程的信息工具。知识库文章、FAQ、事件诊断矩阵等，可以帮助云的客户弥补其在云基础设施和云操作规范方面存在的经验上的欠缺。例如，这些信息可以辅助事件响应团队将操作性问题与真正的安全事态和事件区别开来。

9.3.5 遏制、根除和恢复

如同事件响应的其它阶段一样，为确保所定义的事件遏制、根除和恢复策略是可用的、高效率的，并且考虑了所有涉及的法律和隐私相关要求，需要所有的利益相关方密切协作。所定义的这些策略必须与业务目标一致，并且力图将对服务所造成的中断最小化。在事件响应涉及多个组织时，如云计算情形下，这是相当具有挑战性的。

部署和服务模式以及攻击目标所处层次的不同，这一阶段可选择的选项也不同。在这里可以有多种策略，可能由具备不同技术解决方案的不同实体来采用。如果有可能的话，应在准备阶段进行思考以对这些场景进行预测，确定一个冲突解决流程。客户除了考虑那些直接以他们自己的组织为目标的事件之外，也应考虑他们的供应商如何处理影响到供应商自身或者共享平台上其他租户的事件。

IaaS 情况下，服务使用者对于事件的遏制、根除和恢复负主要责任。云的部署方式可能会为此带来一些好处。例如，可以通过暂停虚拟机镜像达到在不破坏证据的情况下将受影响的镜像隔离起来的目的。如之前讨论过的，当要部署更新代码时，节点可以相对容易的关闭，新的实例可以相对容易的建立，这可以将对服务所造成的中断最小化。如果某个特定的 IaaS 云有问题，那么客户可以选择将服务迁移到另一个云，特别是如果他们已经实施了 meta-cloud 解决方案的情况下。

SaaS 和 PaaS 部署方式下情况更为复杂。服务使用者除了关闭用户访问和在重新开放前检视/清理托管在服务内的数据之外，可能很少有技术能力来遏制 SaaS 或 PaaS 事件。尤其是 SaaS 情景下，即使是这些基本的措施，

在缺少云服务供应商的足够支持下，如服务商细粒度的访问控制机制以及服务商允许客户对其数据的直接访问（而不是通过 WEB 界面），也难以或不可能执行。

在所有服务模式中，供应商可能对某些种类的攻击能够提供帮助，如拒绝服务攻击（DOS）。例如，较小的企业可以受益于云的规模效益，能将运营商部署的较昂贵的风险缓解技术，如对于 DoS 的防护，延伸到他们的站点。同之前的阶段一样，供应商的设施，在帮助应对攻击时，能够向客户提供到什么程度，应该在准备阶段就确定。此外，在什么情况下供应商有义务为应对攻击提供帮助，也应加以合同性的定义。

SLA 和事件响应计划应具有灵活度，为事件恢复后进行的教训总结活动留有空间。应编写一份基于事件响应活动的详尽的事件报告，并在受影响的各方之间共享，如云的客户、云服务供应商、以及其他受影响/涉及的组织。事件报告中应包含事件的时间跨度、对于事件根本原因或弱点的分析、消除问题和恢复服务所采取的措施、以及对于长期性纠正措施的建议。

纠正性措施可能会是客户特定措施和供应商支持措施的混合，供应商的事件响应团队应提供一节文字用以说明他们对于事件的看法以及所建议的解决方法。在客户和云服务供应商完成对于事件报告的初步回顾后，应组织进行共同讨论，以开发和批准补救计划。

9.4 建议

- 云的客户必须理解云服务供应商如何区别感兴趣的事态的定义与安全事件的定义、以及供应商以哪种方式向客户报告哪些事件/事态。以公开格式提供的事态信息能够方便于在客户方一侧进行这些报告的处理工作。
- 云的客户必须建立起与云服务供应商的正规之沟通渠道、在事故发生时可以应用。使用现有的公开标准能够方便于事件的沟通。
- 云的客户必须了解云服务供应商对于事件分析所提供的支持，特别是供应商所提供的用于分析目的之数据的性质（内容和格式）以及与供应商事件响应团队的互动水平。特别是，必须对可获得的用以进行事件分析的数据进行评估，判断其是否能够满足可能涉及到云服务客户的电子取证调查的法律需求。
- 云的客户应当倾向于选择利用了虚拟化为电子取证分析和事件恢复所带来机会（如对于虚拟环境的快照的访问和回滚、虚拟机的自我测试等）的那些云服务供应商，尤其是在 IaaS 的情况下。
- 云的客户应当倾向于选择利用了硬件辅助的虚拟化和具备电子取证分析能力的加固的 Hypervisor 的那些云服务供应商。
- 对于每一项云服务，云的客户应当识别与自身最为相关的事件类别，并为事件的遏制、根除和恢复准备好策略；必须确保每一云服务供应商能够提供执行这些策略所必需的协助。
- 云的客户应当获取到云服务供应商在事件响应方面的历史记录并进行考察。供应商可以提供来自其现有客户的对于其 IRP 的业内推荐。

9.5 要求

- ✓ 在企业的事件响应计划中，针对所用到的每个云服务供应商，必须对托管在该供应商的资源的事件检测和处理方法加以计划和描述。
- ✓ 对于所用到的每一个服务供应商，在与其约定的 SLA 中，必须保证对于企业事件响应所需要的事件处理支持，确保企业事件处理流程中检测、分析、遏制、根除和恢复每一阶段所对应企业事件响应计划的有效执行。
- ✓ 至少每年进行一次事件响应的测试。客户应尽最大可能寻求将自己的测试过程与其供应商（及其他合作伙伴）的测试过程集成到一起。理想情况下，应有一个团队（由客户和云服务供应商的成员共同组成）来针对一份事件响应计划执行各种健康检查，并相应的将改进建议应用于新一版的事故响应计划。

参考文献

- [1] GRANCE, T., KENT, K., and KIM, B. Computer Security Incident Handling Guide. NIST Special Publication 800-61.
- [2] MELL, P. and GRANCE, T. The NIST Definition of Cloud Computing, NIST Special Publication 800-145.
- [3] GROBAUER, B. and SCHRECK, T. October 2010. Towards Incident Handling in the Cloud: Challenges and Approaches. In Proceedings of the Third ACM Cloud Computing Security Workshop (CCSW), Chicago, Illinois.
- [4] WOLTHUSEN, S. 2009. Overcast: Forensic Discovery in Cloud Environments. In Proceedings of the Fifth International Conference on IT Security Incident Management and IT Forensics.
- [5] REED, J. 2011. Following Incidents into the Cloud. SANS Reading Room
- [6] DANYLIW, R., et al. 2007. The Incident Object Description Exchange Format, IETF Internet Draft RFC 5070.
- [7] MORIARTY, K. 2010. Real-time Inter-network Defense, IETF Internet Draft RFC 6045.
- [8] MORIARTY, K., and TRAMMELL, B. 2010. Transport of Real-time Inter-network Defense (RID) Messages, IETF Internet Draft RFC 6046.
- [9] FITZGERALD, E., et al. 2010. Common Event Expression (CEE) Overview. Report of the CEE Editorial Board.
- [10] BIRK, D. and WEGENER, C. 2011. Technical Issues of Forensic Investigations in Cloud Computing Environments In Proceedings of 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (IEEE/SADFE), Oakland, CA, USA.

D10: 应用安全

云环境，尤其是公有云环境，以其灵活性和开放性的优势颠覆了许多有关应用安全的基本假设。这些假设中一部分很好理解，但大部分并非如此。本文期望提供一份关于云计算如何影响一个应用的一生（从设计到运营到最后下线）的指南。这个指南可以指导所有的干系人（包括应用设计者、安全专家、运营人员以及技术管理者）如何在设计云计算应用时降低风险，确保过程可管理。

对于那些跨软件即服务（SaaS）、平台即服务（PaaS）和基础设施即服务（IaaS）多个层面的应用来说，云计算是一个特别的挑战。基于云的软件应用要求设计严密，这类似于一个连接到原始网络的应用 - 应用必须提供安全性，不能有任何有关外部环境的假设。但是暴露在云环境中的应用要面对的威胁要远超过在传统数据中心中经历的威胁。这就需要制定严格的实践，在云中开发或迁移至云中时，必须严格遵循这些实践。

概览 应用安全领域有以下焦点领域：

- 安全开发生命周期 **SDLC**⁵²（用于确保 SDLC 安全的一般实践及特定云的细微差别）
- 认证、授权、合规 - 云中的应用安全架构
- 身份验证，以及与云计算应用安全相关的身份验证的使用。授权流程和基于风险的访问管理以及与之相关的云计算应用中的云加密
- 应用授权管理（策略制定/更新，执行）
- 针对云的应用渗透测试（一般实践与云应用下的细微差别）
- 云计算应用的监控
- 应用认证、合规、风险管理及其在多租户及共享基础设施下的影响
- 规避恶意软件和提供应用安全的区别

⁵² SDLC - Software Development Life Cycle

10.1 安全软件开发生命周期（SDLC）

安全软件开发生命周期（SSDLC）（也有些人称为安全开发生命周期 SDLC⁵³），在向云中迁移和部署应用时其重要性日益凸显。组织应该确保其开发过程和整个应用的生命周期中贯彻应用安全、身份管理、数据管理和隐私权的最佳实践。

云环境下的开发与传统托管环境在如下几个方面有所不同：

- 在公有云环境中，对物理安全的控制大幅度减少。
- 当服务（例如存储）从一个厂商迁移到另一个厂商时，可能不兼容。
- 必须考虑整个生命周期中对数据的保护，包括传输、处理和存储。
- 在云环境中，Web 服务的聚合导致的安全脆弱性开始显现。
- 访问日志的能力变得更加困难，尤其是在共享的公有云中，应该将其指定为服务水平承诺的一部分。
- 云中的数据故障转移和数据安全必须比传统环境更详细、分层更明确。
- 在云环境中，保障（并提供证据）合乎相关行业和政府的规则通常会更加困难。

在执行一个 SSDLC 时，企业必须采用开发的最佳实践。为此，要么企业自己拥有一套自主的流程、工具和技术，要么就采用一个成熟度模型，比如：

- 利用成熟度模型构建安全（BSIMM2）（最新的标准是 BSIMM4）
- 软件保障成熟度模型（SAMM）
- 系统安全工程能力成熟度模型

10.1.1 应用安全保证程序

企业应该有一个应用安全保障程序，确保在向云环境中迁移、开发或维护应用时能达到以下几点要求：

- 在足够的高层支持下，目标和指标被定义、实现以及追踪。
- 已针对云中应用建立起安全策略和隐私策略，用来满足法律和监管合规性需求，这些需求符合组织的业务需要和监管义务。
- 通过及时的聘用新员工或者培训合适的员工，来保证组织在架构、设计、开发、测试以及部署安全的应用时拥有充足的资源和安全保障的能力。
- 在所有应用上执行安全及隐私评估，来确保需求定义恰当。
- 定义并实施一系列流程，使云中的开发和维护过程达到确保安全和隐私要求。

⁵³ SDLC: Security Development Life Cycle, 安全开发生命周期

- 配置及变更管理必须是可审计和可验证的。
- 执行针对应用和数据的物理安全风险评估，且所有云基础设置部件的访问都足以满足这些需求。
- 在开发阶段需要遵循规范化的编码最佳实践，要考虑到所使用语言的优势和劣势。
- 隐私和安全评估必须是可审计且可验证的。

10.1.2 验证及鉴权（V&V）

10.1.2.1 设计复核

有些功能的安全敏感性远高于其他功能，运行在云环境中可能不是一个可行的候选方案，这个时候，需要考虑特殊的设计或者特定的需求。

在执行应用程序的安全设计时，应遵循以下原则。如果云计算架构无法满足这些原则，应该通过适当的技术和/或补偿控制予以修复。否则，将会对云计算的部署可行性带来问题。

- **最小特权**。该原则主张个人、程序或其它类型的实体都应只在完成一项任务所需的最少时间内、持有最小特权和资源。在很多情况下，最小特权只能使用精细的、前后关联的应用程序授权管理与安全政策自动化机制得以有效实施。
- **职责分离 SOD**。这是一项控制策略，根据这项策略，每个人的职责或者访问权限被控制住对应的范围内，不能对超越范围的部分拥有职责或者访问权限。
- **深度防御（Defense in depth）**。这是一个多层次防护的应用，在这种应用中，如果前面的层被攻破，后面会提供保护。
- **失效安全（Fail safe）**。如果云系统崩溃了，它应该处于系统的安全性以及数据不被危及的状态。例如，为了确保失效安全，系统默认进入这样一种状态，该系统会拒绝用户或程序的访问。
- **机制经济（Economy of mechanism）**。该原则推崇简单、可理解的设计和实施保护机制，因此非计划的访问路径不存在或者很容易识别并拒绝。
- **完备仲裁（Complete mediation）**。这种原则下，计算机系统中的实体⁵⁴对某一个对象的所有访问请求都必须得到授权。
- **开放设计**。指通过专家社区来评估和同行评审的开放访问的云系统设计，从而使设计更加安全。
- **最少公用机制（Least common mechanism）**。指最小化跨多个应用程序的共用机制（尤其是保护机制）的数量，最大限度的减少一个应用程序出问题导致其它应用程序破坏或颠覆的能力。
- **最薄弱环节（Weakest link）**。最重要的是识别安全链和防护层次中的最薄弱机制，并进行提升，从而将系统的风险降低到可接受的水平。

10.1.3 构造

10.1.3.1 代码审查

⁵⁴ 一个实体可以是用户、代码、设备、组织或代理

建议在企业级别定义并且遵从安全软件开发。可以遵从 SAFECODE⁵⁵、CERT (SEI)⁵⁶ 或 ISO 标准等的基础实践部分描述的安全软件开发指南。

动态代码分析当代码在运行的云应用中执行时检查该代码，测试器跟踪源代码中的外部接口与执行代码的相互作用，因此任何出现在执行接口中的漏洞或异常现象也同时在源代码中被定位，从而可以在源代码中修复。

和静态分析不同，动态分析启用测试器来不断执行软件，以暴露用户交互、配置变更或环境组件的行为等方式引入的漏洞。

下面列举了一些编写安全代码和审查的最佳实践：

- 云服务器代码中应该包含最少的必要信息。注释应该从运行代码中剥离，并且避免带有姓名和其它个人信息。
- 利用源代码分析工具来检查典型的编程错误，比如缓存溢出、格式化字符串攻击、条件竞争（Race Conditions）等。
- 验证并确认所有输入、用户、计算机和交互系统。当云基础架构接受任意输入并将该输入的内容应用到命令或 SQL 语句时，可能发生内容注入和一些其它攻击。
- 使用目标代码（二进制）时，例如，正在使用第三方库，在目标代码上使用能够测试静态漏洞的测试服务。

10.1.3.2 安全测试

渗透测试是一种安全测试方法，它通过模拟恶意来源的攻击让测试者掌握目标网络的安全强度。该过程包含寻找任意潜在漏洞的云系统主动分析，这些漏洞可能由于系统配置不足或不当、已知或未知的软硬件缺陷、或者操作规程或技术措施的缺陷而导致。该分析以潜在攻击者的角度执行，可能会包含安全漏洞的主动利用。

云模型的类别极大地影响了渗透测试或者决定渗透测试是否可行。一般来说，平台即服务（PaaS）和基础设施及服务（IaaS）可能允许渗透测试。然而，软件即服务（SaaS）提供商不太可能允许客户对其应用和基础设施进行渗透测试，除了云提供商自己为了合规或安全最佳实践而让第三方执行的渗透测试。

渗透测试通常在“黑盒”场景中执行，也就是说，预先不了解将要测试的基础设施。在其最简单的级别，渗透测试包括三个阶段：

1. **准备。**这个阶段执行正式合同，合同包含对客户数据保密以及对测试者的法律保护。至少，合同需列出要测试的 IP 地址。
2. **执行。**这个阶段中执行渗透测试，测试者寻找潜在的漏洞。
3. **交付。**评估结果交付给测试者在企业中的联络人，并且会提供纠正措施。

不管渗透测试是全了解（白盒）测试、部分了解（灰盒）测试还是零了解（黑盒）测试，得到报告和结果后，必须应用缓解技术来将泄漏风险降低到可接受水平。该测试应在尽可能大的范围来确定某些领域的漏洞和相应的风险，如应用、远程访问系统和其它相关 IT 资产。

⁵⁵ <http://www.safecode.org/>

⁵⁶ <https://www.cert.org/secure-coding/>

10.1.3.3 互通性测试

互通性测试评估一个云应用是否能与其它组件或应用交换数据（互通）。互通性测试活动确定应用在使用通用交换格式交换数据、读写相同文件格式、以及使用相同协议通讯等方面的能力。

互通性测试的主要目标是在云软件应用投入运行之前发现它们之间的互通性问题。互通性测试需要大多数应用在测试进行前已经完工。

和互通性测试一样，这些测试应该确认所用的数据交换、协议和接口都正在使用安全的信息传输。

互通性测试通常选用以下三种方法之一：

1. **全配对测试。**这种方法常由第三方独立测试组织引导，这些测试者了解多个软件产品和软件厂商间的互通性特点。
2. **测试一些组合。**这种方法只测试部分组合并且假设没有测试的组合也互通。
3. **测试针对的参考实现。**该方法需要搭建一个参考实现，比如使用可接受的标准，并测试针对此参考的所有产品。

10.1.4 量化改进

10.1.4.1 指标

任何应用安全保障程序都应该收集度量指标，这些指标可以分析或用来定期报告安全开发的状态。随着应用安全程序逐渐成熟，指标收集和报告也会增强。

下面推荐一些指标：

- 过去一季或一年中，被评估带有风险等级的云应用和数据资产的占比。
- 一季或一年中，对一个基于云的应用项目或程序，用于应用安全保障程序的成本。
- 在云中开发或部署的应用程序由于安全问题（如果有的话）导致的损失的估计。

10.1.4.2 使用自动的 SDLC 安全技术工具和特性

以人为核心的 SDLC 活动（流程、培训和测试）是有必要的，但是对于较高要求的应用安全，这常常是不充分或不可靠的。只要可行，应使用一些自动化工具来构造安全应用，自动地将安全性生成到应用中。

这些自动生成技术安全特性的工具常常与开发和集成/编排（*integration/orchestration*）工具绑定。例如，技术授权策略规则可通过分析应用及其交互⁵⁷的工具按照安全需求规格自动生成（在开发/集成/混搭（*mash-up*）时）。

类似地，一些自动化的测试也可以在开发/集成阶段完成，并且可以生成信息保障证据。

⁵⁷ 这个科学领域被称为“模型驱动的安全”，更多信息见 www.modeldrivensecurity.org

对于云而言，这可以在订户端在开发或混搭期间（尤其是用于 IaaS 时）完成，或者是云提供商提供这项技术（订户在需要时可以自己配置），尤其是对于 PaaS 云应用平台。

对于 SaaS，大部分安全自动化一般都是由云提供者内置、配置和运行。

10.2 认证、授权和合规 - 云中的应用安全架构

10.2.1 云服务/应用的开发和业务挑战

访问敏感数据和系统时有一些新的潜在风险。清楚地理解应用和业务环境中的以下安全风险对于解决云服务/应用全领域的安全和隐私问题十分重要：

- **缺乏控制。**是指云订户通常缺少对云安全策略和控制的控制。
- **缺乏可见性（visibility）。**是指云订户通常缺少云安全策略执行和控制的有效性的可见性。
- **缺乏可管理性。**是指云订户常常没有足够的管理能力来管理云计算应用的安全，尤其是访问和审计策略。
- **治理丧失。**是指组织可能不能直接控制基础设施，只能信任提供者（有时是盲目信任）以及提供者自身的能力来提供适当的安全。
- **合规风险。**是指云提供商冲击了组织合规（符合法规，隐私评估，工业标准）的能力，因为数据和系统可能存在于组织的直接控制之外。
- **隔离失效。**多租户和资源共享是云计算的本质特征。因此，彼此竞争的公司完全有可能使用相同的云服务，实际上，他们的工作负载肩并肩运行着。保持内存、存储和网络访问的隔离是至关重要的。
- **数据保护。**组织放弃数据的直接控制。它依赖提供者来保证数据安全，当数据被删除时，提供者应该确保（或能够证明）数据的确被永久删除了。
- **管理接口和访问的配置。**云应用通过互联网访问和管理，有可能涉及到复杂的和控制方面的需求。这样就增加了安全入侵相关的风险，因此必须仔细考虑适当的访问授权。

10.2.2 技术风险和解决方案

多数云服务提供商在云服务设计中包含了所谓身份、授权和访问管理 (IdEA)⁵⁸。通常采用联邦标准 (Federation Standard) 将用户认证和授权委托给客户的用户管理系统。

对身份、授权和访问管理的支持会影响到客户，因为整合受限于认证传递机制。依赖于身份管理的基础设施如计费 and 计量，产生了集成和迁移风险。

⁵⁸ IdEA - Identity, Entitlement, and Access Management

对身份、授权和访问管理的支持对客户带来集成方面的影响。这些影响包括安全的传输凭证和标签、为额外用户提供服务等。云计算服务提供商内部的业务运营也会受到影响，这些运营包括收费和财务资源效用。因此将身份、授权和访问管理的整合作为设计的主要部分很重要。

应用的 **IdEA** 能力（或缺乏它），如应用接受 **SAML**（安全声明标记语言）声明的能力，会影响云计算服务的治理、集成以及用户体验，所以理解云计算应用下的特定的 **IdEA** 需求是需求定义的关键部分。

云计算应用设计中特定的 **IdEA** 需求包括：

- 理解云应用将如何为用户、高级用户和管理员提供帐号- 这些触发器可以链接到内部的人力资源系统或基于云的人力资源平台。
- 为服务到服务的集成的提供云服务，例如，内部应用和基于云计算的服务之间的集成。
- 从多种资源和基于联邦标准（例如 **SAML**、**WS FED** 等）的实体处接受声明和断言（身份和标签）的能力。
- 基于链中所有实体（用户、设备、代码、企业、代理）的身份和属性能够针对到云计算应用（或者在云计算应用中）的访问做出基于风险的授权决策。
- 一个丰富的基于风险的授权语言，来引导受保护资源（例如，每个资源的哪些访问是被允许的）的访问管理（编写/分配/升级等）。
- 支持内部安全和管理政策的合规需求，如基于声明的认证，或者最小限度的角色访问控制。
- 根据内部政策和法规的合规性要求（如萨班斯法案 **SOX**、**PCI** 标准和 **HIPAA** 法案）进行的用户行为监控、记录和报告。

各种身份提供商或服务提供商会生成令牌，比如用 **SAML**、**OpenID**⁵⁹ 或者 **OAuth**⁶⁰ 令牌，这些令牌通过会话缓存允许直通登录。部署在云中的应用应该具有集成这些申明/断言服务的能力，应用/服务的设计应支持联邦身份验证的开放标准，如 **SAML**、**OAuth**、**OpenID** 等。

授权管理过程将要求能通过集中的界面来定义、管理和访问云计算应用的访问控制规则。这样的界面或服务可以自己托管在云上，也可以在内部，可以利用的标准有 **XACML**⁶¹ 等。主要挑战是可管理性：随着安全策略和合规的复杂性、IT 复杂性和 IT 敏捷性的增加，对最终用户组织来说，将安全策略转化为安全实施变得更费时、重复性更高、更昂贵、更容易出错，且更容易达到安全成本限制。因为传统的用户管理是基于角色的访问控制，要通过访问控制列表对访问是否在列表内进行管理，因此需要昂贵的（规则）引擎来处理这些列表以保证职责分离的原则不被打破。

取而代之的，为授权层定义一系列的规则，在事务中为实体提供声明（断言）和标签，将会显著地简化和增强组织对其应用的控制，进一步导致最终用户组织（和云计算提供商）减少成本并改善策略实施的精确性。

⁵⁹ **OpenID** - an open standard permitting users to be authenticated in a decentralized manner

⁶⁰ **OAuth** - Open Authorization, an open standard for authorization, allowing users to share their private resources with tokens instead of credentials

⁶¹ **XACML**- eXtensible Access Control Markup Language, an OASIS standard

表 1 - 云计算 HR 应用的简单授权矩阵示例

声明/属性	企业 HR 经理访问	用户在企业内访问	企业 HR, 经理家庭, 访问 (公司笔记本)
ID: 组织 Id	有效	有效	有效
ID: 用户标识	有效	有效	有效
ID: 设备	有效	有效	有效
属性: 设备是安全的	有效	有效	有效
属性: 设备打了补丁	有效	有效	有效
属性: 设备 IP (在企业网络中?)	有效	有效	无
属性: 用户是 HR 经理	有效	不是	有效
访问结果	读/写访问 -> 所有 HR 帐户	读/写访问 -> 仅用户 HR 帐户	读/写访问 -> 仅用户 HR 帐户

为了整合应用安全控制、数据安全和隐私保护，服务应该使用可审计的行业标准，例如 ISAE 3402/SSAE（取代 SAS 70）、PCI、HIPAA 和 ISO 27002。每个标准都有多个类别的控制，来管理云计算提供商的数据中心以及部署在这类环境中的应用的运营。

重要的是评估不同的安全声明，并为部署在云计算环境中的应用/服务采用何种标准作出一个合理的决定。有必要进行基于需求的深入分析以识别服务水平目标，这样可以在用户和云计算提供商两方面避免应用代码、部署和支持工具等的主要代码变更。

10.2.3 合规构建模块

不论使用何种标准，要使运行云中的应用实现合规要有一些基本的构建模块，所有标准的基础都依赖于云提供商的基础物理设施。基础设施控制包括诸如自然灾害下的保护设施、保证发生断电时的可靠电力供应、以及硬件故障时的数据备份。这些控制还包括监管云计算供应商的程序和策略，如系统管理审计、访问数据中心和对数据中心访问的认证、用于内部安全审查的方法，以及这些方法是如何执行和汇报的。

基础设施控制顶部的上一层是一系列的应用控制。这要求多个等级的安全，比如传输层必须是安全的，当数据离开数据中心时，数据必须使用企业控制下的密钥进行加密。为了合规某些存储标准或在传输个人信息时为了满足隐私需求，某些应用可能需要信息层安全、数字签名和其它附加安全功能。对于将迁移至云中的服务/应用，所有的这些应用控制都应该在设计阶段确定出来，以便它们可以很好的被整合到架构设计中，并且依照这些需求进行开发。著名的标准有 PCI-DSS、SOX、ISAE 3402/SSAE 16、HIPAA 和其它隐私标准。

10.3 用于云应用安全的身份、授权和访问管理

传统的企业内部应用可以通过传统的边界安全控制予以保护，比如防火墙、代理服务器等。这可以很好地满足企业的风险等级和安全需求，因为应用都运行在可信硬件和可信网络上。企业还可以利用其企业目录基础设施来验证其应用用户，并在保持所有应用中的访问决策。在这种情况下企业的安全边界被很好的定义了。

当用户将这些应用迁移入云时，所有传统的控制都不足以保护它们，因为这些应用运行在不受信任的网络上（非参数化⁶²）。来自相同服务提供商（资源池）不同租户的应用程序可能放在一起，并且可以通过任意设备从任意地点进行访问。根据 www.rationalsurvivability.com 所说，云构造参考如下：



图1-云构造

根据以上参考架构，用户现在可以添加他/她访问这些应用的方式。该构造如下所示：



图2 云交付组成

根据上方的构造图能清晰地看到，您的应用是通向数据的窗口，新的边界线是内容（数据）和用户用以访问数据的上下文。这使得在云应用上实施安全控制变得至关重要。访问该数据的上下文变得很重要，需要附带一系

⁶² 译者注：原文是 de-parameterization，怀疑应为 de-perimeterization，去边界化

列丰富的标识符和属性来制定访问决策。随着 IT 的消费化⁶³，企业现在正面临"用户自带设备 (BYOD⁶⁴)"的现实。因此设备身份和设备属性也变成确定访问控制的重要因素。

身份不应只被视为认证实体时参考，还应该收集更多关于用户的信息来帮助进行访问决策。身份还包括运行应用的设备的身份信息 (VM Image 的标识)、管理该 VM Image 的特权用户 (可能是企业用户也可能是服务提供商用户)、该应用需要与其交互的其它应用或服务的身份信息，该应用的系统管理员用户身份信息，以及企业之外的需要访问该应用的外部 (应用或服务的，比如 B2B, B2C 等) 身份信息。值得注意的是，访问决策还将基于身份无关的属性，策略授权/管理工具需要支持这类的非身份属性 (可见后面的"授权管理和策略自动化")。

在本节中，我们将研究认证、授权和访问管理如何影响云计算应用的安全。IdEA 可广泛地分为以下五大部分：

1. 认证
2. 授权
3. 管理
4. 审计与合规
5. 策略

10.3.1 认证

认证指的是在应用中创建或者断言身份。这通常分为两个阶段。第一阶段是澄清身份，第二阶段是验证已经提供给用户的凭证。云应用认证的几大驱动因素是设备独立性、普通且简单的用户界面 (UI) 以及设备通用的单一协议。很多服务提供商还以 API 形式推出其服务，这些 API 在设计上接受标识符而不是密码。

在常规企业应用中，认证的完成依赖于企业的用户存储 (AD⁶⁵ 或 LDAP)，而认证凭证通常是用户 ID 和密码。对于基于云的应用，使用企业凭证的认证更复杂。某些企业在服务提供商到企业网站间建立了 VPN 通道，使得它们可以通过企业用户目录进行认证。尽管该方案可能可行，但企业应该考虑延迟、连通性和 BCP/DR 规划等方面的问题，并且该方案也不一定在新的云应用中使用到或设计上支持。企业应该规划采用开放标准，如 SAML 和 WS-Federation。

企业合作伙伴和客户对企业应用的使用也有所增加。对云计算应用也是如此。这些用户不想为其第三方访问维护独立的身份 (但是现在常常别无选择)。所以企业应该规划采用"自带身份 (BYOI⁶⁶)"机制，并且该云计算应用需要设计为支持多个机构的身份和属性。

由于云计算应用可通过多种设备进行访问，使用简单用户 ID 和密码的简单认证方法应该降级为一个解决方案。企业应该规划更强大的认证。消费者应该考虑用于原始身份确认的强大认证并确定能满足其风险需求的凭证

⁶³ Consumerization, 消费化

⁶⁴ BYOD: Bring Your Own Device, 用户自带设备

⁶⁵ AD 指的是微软公司的 Active Directory

⁶⁶ BYOI: Bring Your Own Identity, 用户自带身份

类型（RSA Token、经由短信或手机的 OTP⁶⁷、智能卡/PKI、生物特性认证等）。它随后将通过高水平认证将认证者和属性传递给云应用，以便授权层可以对访问管理作出更好的风险决策。

企业应该为其云计算应用规划使用基于云的验证。此类验证基于设备标识码、地理位置、ISP、启发式信息等。云应用不该只在初始连接时执行认证，还在应用内部发生交易时执行基于风险的认证。

云计算应用还应该充分利用可应用的标准，比如 SAML 和 OAuth。正如本节前面所提到的，云服务 API 专门设计用来接受标识而不是密码，因此，当用户试图通过他们的移动设备访问云计算服务的时候，必须先通过身份提供商的认证（今天，可能是他们的企业），身份提供商会生成一份 SAML 声明并递交给云计算服务提供商。SAML 声明成功批准后，会生成一个 OAuth 令牌并发送到移动设备上。然后移动设备会传递这些令牌到要访问的基于 REST⁶⁸的云计算服务 API。

10.3.2 授权和访问控制

授权广义上是指强制执行基于资源授权的访问规则。授权过程实现了业务策略，进而转化成对企业资源的访问。对于基于云计算的应用，授权不应只基于内容执行，还应该参考上下文环境。

对于以用户为中心的授权模型而言，用户是策略决策点（PDP⁶⁹）。用户决定对资源的访问，而服务提供商充当策略执行点（PEP⁷⁰）。OAuth 广泛地用于该模型，用户管理访问（UMA）也是该领域的一个新兴标准。

对于以企业为中心的授权模型，企业就是 PDP 或者策略访问点（PAP⁷¹），而服务提供商充当 PEP。在某些情况下，企业为 PEP 实施云计算安全网关。企业客户应该考虑使用 XACML 和集中的策略管理。

云应用可以利用多种类型的服务。某些服务可能是传统的应用使用中间件技术展现出来的 Web Service，或者 Web 服务也可能是本地的云计算 Web 服务。尽管 Web 服务接口已经进行了抽象，但是交付供应链的多样性还是可能让治理流程复杂化。在设计时，治理包括定义服务、开发服务、注册服务并为访问这些服务执行策略需求。运行时间的治理包括发现服务、为调用服务实施安全限制、为访问服务强制执行安全限制，以及审核所有访问。运用开放的标准，比如 W3C 的 WS⁷²-policy 来定义安全和管理策略申明，使用 WS-security 来强制执行访问限制，使用 WS-trust 实现安全令牌服务（STS⁷³）来验证并颁发令牌、交换令牌格式等等。

还有一些不同类型的授权模型，如基于角色的、基于规则的、基于属性的访问、基于声明的，以及基于授权的访问控制（如 ZBAC⁷⁴）。已经拥有 Web 访问管理（WAM⁷⁵）解决方案的企业应该利用这些解决方案来无缝地保护其云计算应用。大部分 WAM 产品都支持基于规则和角色的访问控制。

Application architects and designers should plan to migrate to Rule-based using claims and attributes as the source for those rules via the Entitlement process described above, and depreciate other legacy solutions.

⁶⁷ OTP: One Time Password, 一次性口令

⁶⁸ REST: Representational state transfer, 表示层状态转移, <http://zh.wikipedia.org/wiki/REST>

⁶⁹ PDP - Policy Decision Point

⁷⁰ PEP - Policy Enforcement Point

⁷¹ PAP - Policy Access Point

⁷² WS: Web Service

⁷³ STS: Secure Token Service, 安全 Token 服务

⁷⁴ Described in publications by Alan Karp, HP Labs

⁷⁵ WAM - Web Access Management

应用架构师或者设计师应该有计划的迁移到基于规则的解决方案，通过如上的所述的授权过程采用申明和标签作为规则的资源，而逐渐摒弃其他传统的解决方案。

当使用基于属性的访问控制时，身份提供者（IdP⁷⁶）将属性传递给云服务提供商用于强制执行。身份提供商应该保证：

- 身份附带的属性不需要严格地指向用户身份，如姓、名、邮件地址等。它也可以包括 IP 地址、地理信息、隶属组织、电话号码等等。
- 共享可直接识别用户的属性时应该注意，因为它会引起隐私方面的问题。
- 企业还需对访问控制决策过程中属性的复杂性制定计划。它们应该了解针对某个特定属性的权威性应该与哪个属性提供者联系。企业可以利用属性的聚合者，这有可能复杂化也有可能简化这种信任关系。企业应该考虑到冲突解决的复杂性、处理不完整数据等。
- 企业还应考虑到属性的可扩展性，如确认（validation）、可验证性（verifiability）、使用条款、数据等。
- 企业应该考虑隐私、属性发布策略和许可（consent）。例如，包括 EU 隐私条例、国家及地方法律等。IdP、CSP 和用户的地理位置（管辖权问题）也应该纳入决策因素。
- 访问控制要求使用最少量的信息，用后及时释放。
- 企业确保非身份为中心的属性也应得到支持。
- 企业应确保访问策略和授权策略都是可管理的且技术上是可以实现。使用策略自动化技术（可能与 PaaS 应用混搭工具⁷⁷捆绑）是潜在的解决方案之一。

基于声明的访问控制主要目的是受控制的信息共享。声明以交易的上下文为基础。企业如果计划采用基于声明的认证，应该考虑如下几点：

- 使用有意义的声明（用验证过的邮箱而非只是邮箱地址）。
- 声明的类型、担保人、新鲜度和质量（如果声明不在声明提供者的缓存范围内，那么该声明就失去了新鲜度）。
- 声明的权威方和其上下文有关，例如，电信公司在验证手机号码方面有权威性，邮件提供商在验证邮箱地址方面有权威性。
- 尽可能的使用声明代理（claim broker），因为他们可以作为不同的声明提供商的抽象，例如，他们可以在要求的信任级别创建一个声明包，或者为用户许可创建一个集中点。
- 根据交易需求发布最少的声明。

⁷⁶ IdP - Identity Provider

⁷⁷ 混搭工具的英文原文是 Mash up tool

云计算应用还可以同其它相同或不同服务提供商提供的云计算应用进行混合。企业应该准备用户如何在所有这些云应用无缝地获得认证，相关群组、授权、角色等用户资料如何跨这些云应用共享来得到精细的访问控制。建议企业针对该使用案例使用开放标准（SAML、OAuth、XACML 等）。

10.3.3 管理

在企业中身份管理（IDM⁷⁸）主要关注管理用户（开通）和管理访问策略（针对企业应用）。IDM 是 IdEA 的一个重要组成部分，它不但可用来给用户及时的访问，还可以在用户离职时及时撤销访问或在用户切换到其它角色时及时管理访问。在企业内部，身份管理通常与数据存储（用户、策略等）高度集成，并直接连接。在大多数部署中，身份管理会很高程度的定制化。由于云的分布式本质，可能没有办法使用相同的部署方法，因为 IDM 可能不能直接访问服务提供者的数据存储。此外，也没有标准的 API 可用于开通。很多服务提供商还未采用服务开通标记语言（SPML⁷⁹）。

云计算环境中的 IDM 不应只管理用户身份。它还应该扩展到管理云计算应用/服务的身份、这些云计算应用/服务的访问控制策略、用于这些应用/服务的特权身份等。

现有的联合权限分配由服务提供商推出的专用 API 实现。企业 IDM 遵循的 PUSH 模型不会应用在云计算应用中，因为该模型可能会让服务提供商超载。

简单云身份管理（SCIM⁸⁰）是一种新兴标准，其主要目的是通过更简易更快速的实现，以达到更省钱的身份管理。另一个目的是简化用户身份进出云的迁移。SCIM 因为使用了定义良好的核心模式而简单，同时因为它使用了 REST API（众多云服务提供商支持）而云端友好，另外因为兼容很多现有协议（比如 SAML、OpenID 连接等）而支持身份管理。基于这些事实（在撰写本文的时候），SCIM 可能被采纳为身份权限管理的一个行业标准。

企业在身份管理方面要考虑到的一些挑战：

- 如何在企业到云、云到云和云到企业间同步身份/访问的变更。
- 如何跨企业和云取消⁸¹身份和访问授权。
- 如何以可管理、可扩展、易维护、低成本的方式撰写/更新/管理访问策略。

很多企业现在的解决方案是采用混合 IDM 方案，它在企业和云中都能使用。

访问策略管理是应用安全的主要挑战，它常需要最大化的安全自动化作为解决方案：安全策略自动化对云计算尤其重要，因为云用户会要求云提供商给予监管合规支持，但同时他们又会以以评判云计算相同的测量标准来评判财务上的投资回报率，比如他们减少了多少前期资本支出，以及减少了多少内部的人工维护成本。

⁷⁸ IDM - Identity Management，身份管理

⁷⁹ SPML: Service Provisioning Mark-up Language，服务开通标记语言

⁸⁰ SCIM: Simple Cloud Identity Management，简单云身份管理

⁸¹ 取消的英文原文是 de-provision

10.3.4 审计/合规

使用云服务的企业应回答以下三个基本问题：

1. 用户可以访问哪些云资源？
2. 用户实际访问了哪些云资源？
3. 运用何种访问策略规则作为决策的基础？

在现在的云部署下，企业客户获得的云服务提供商的可见性有限，难以支持数据审计。企业需要访问这些数据，不只是为了满足业务驱动的合规，还是为了满足行业法规和欺诈纠纷的处理。

现有的 IDM 市场正在转向身份和访问治理（IAG⁸²）市场。企业还应考虑使用 SIEM（安全事故和事件管理⁸³）工具把云应用访问日志数据和策略数据进行关联生成策略合规报告，也可以使用可审计的行业标准，如 ISAE 3402/SSAE 16、HIPPA、DSS PCI、ISO27002 等。

有关云应用安全的通用 IdEA 考虑有：

- 身份、授权和访问管理不应是事后追加的内容，它应该一体化到应用的软件开发生命周期，从收集需求时就开始。
- 在设计阶段，尽可能地使用基于声明的访问来控制到应用的访问。
- 考虑使用 SAPM（共享帐户密码管理）之类的工具来管理应用内部的高特权帐户。这应该考虑到职责分离（SOD）和最小特权。
- 如果企业已经有 Web 访问管理工具，应确保这些工具可以扩展到云环境中，比如通过添加 SAML 支持能力。
- 云应用也许会需要利用服务提供商提供的服务，如日志、数据库连通性等。大多服务提供商将服务作为 Web 服务或 API 来发布。访问这些服务应由 OAuth 令牌控制。因此，云应用应该考虑支持多种令牌类型，如 OAuth、API Keys 等。
- 应确保遵循敏捷开发过程，并且应用应由模块化组件构建而成。这样应用可以在未来使用新兴标准，如 Mozilla 的浏览器 ID、Microsoft 的 U-Prove 和 Kantara Initiative 的 UMA（用户管理访问）。

要意识到如下的云应用安全威胁：

- **身份诈骗（Spoofing）**。伪装另一用户的身份。
- **篡改（Tampering）**。修改传输中的数据。
- **抵赖（Repudiation）**。否认交易处理（请求或响应）的来源。

⁸² IAG: Identity and Access Governance，身份和访问治理

⁸³ 译者注：通常 SIEM 指 Security Information and Event Management，但原文中使用了 Security Incident & Event Management

- **信息泄漏 (Information disclosure)**。未授权下泄漏数据。
- **拒绝服务 (Denial of Service)**。影响可用性。
- **权限提升 (Elevation of Privilege)**。假扮角色或授权。

如下威胁可以通过 IdEA 加以解决：

- **身份诈骗 - 认证 (强验证)**。
- **篡改 - 数字签名或哈希 (和在 SAML 声明中使用方法一样)**。
- **抵赖 - 数字签名 (和在 SAML 声明中使用方法一样)、审计日志**。
- **信息泄漏 - SSL、加密 (不是 IdEA 特有的特性)**。
- **拒绝服务 - 安全网关 (Web 服务安全网关)**。
- **权限提升 - 授权 (OAuth)**。

10.3.5 策略管理

访问策略管理（当以授权为主时常被称为“授权管理”）是访问策略中指定并维护对资源访问的过程，它基于的属性包括调用者相关的身份和相关的属性（如调用者认证）、上下文属性（如环境/业务/IT 相关）及目标相关的属性（如限制或 QoS 访问策略）。

授权管理是组成授权和访问管理的一部分，它还包括为非身份相关但必需的属性（除身份和其属性之外）编制和维护策略，以制定有意义的访问决策。

授权也考虑那些与身份无关的属性，如：

- IT 状况的一般状态、业务/业务流程、IT 系统或业务流程的互连性，或者环境（如危机等级、紧急情况）等。
- 其他实体做出的其它决策（如批准、事前决策）。
- 保护目标资源的相关属性（如 QoS 或节流策略）。

一般来说，授权管理、决策和实施过程在下面的三种情况下执行：

1. 使用集中/外部的策略实施点/策略服务器/策略即服务 (Policy-as-a-Service)
2. 作为云应用的组成部分嵌入
3. 使用身份即服务或角色即服务（一个实体角色是它的身份再加上选定的属性）。

10.3.5.1 云问题 vs. 政策管理

云的认证/授权管理面临几个问题⁸⁴。

首先，面向云的授权管理（entitlement management）有特定问题，在云设施中，云用户通常对技术准入策略、决策制定和执行没有足够的控制权。目前，大部分云提供商不提供用户可配置的管理策略实施点（例如，基于 OASIS XACML 标准），且云提供商不能针对用户（因为他们是具体用户）来预先配置用户特定的策略。

其次，用于相互连结的云（混搭式⁸⁵）授权管理的复杂性在于，访问控制是针对互联云混搭的需求，而不只针对每一个独立的云节点。这意味着该策略的制定需要出于跨互联云混搭的服务链和委托（delegation）方面考虑。

10.3.5.2 授权（authorization）管理最佳实践

- 确定是否是一个以身份为中心或以权限（entitlement）为中心的视角是企业制定并维护管理策略的最佳方式。很多情况下，以受保护资源为中心的视角也许更易于制定和维护，因为目标常是受保护资源，同时为了自动的策略实施，策略常分布到受保护的终端系统（如在授权和权限管理系统中）。在这种情况下，身份仅仅是访问策略中的一个属性，应考虑到该策略与实施目标在受保护终端系统一起写入。
- 确保策略采用可管理的表单明确提出。这包括描述的策略是通用的，在足够高的抽象层面描述，并且表述能够接近于相关企业/业务/人的认知。通过这些可管理的表单，可采用机械装置和工具生成详细的技术访问策略规则（如使用模型驱动的安全策略自动化）。

10.3.5.3 与访问策略提供者对接的架构

使用标准协议（如 XACML）或专有协议（直接的 Web 服务或其它中间件调用）的策略决策/实施点（PEP/PDP）可以访问策略服务器（它包含用于互联云混搭的法规）。如果该策略涵盖了一个单一信任域（如企业内网），该架构通常是一（服务器）对多（PDP/PEP）的。但是在大型部署中，可能有很多联合的策略服务器服务于很多不同的 PDP/PEP。某些访问管理产品现在支持授权管理规则（如在 XACML 中），这可用来展现身份的权限（entitlement）。另外，某些授权管理产品可用来从更以目标资源为中心的角度来授权策略。

10.3.5.4 访问策略的开通

在身份+属性的开通之外，访问策略也需要开通（参照 10.3.5.3 与访问策略提供者对接的架构）。此外，非身份属性需要基于目录服务或其它属性源开通⁸⁶。两者都需要对 PDP/PEP 开通⁸⁷，时效性和正确性扮演重要角色。

10.3.5.5 管理云的访问策略

让创建和维护访问策略可管理是一项重大的挑战。通常有太多简单的技术规则需要管理，使用的策略语言和属性与人类管理员的理解不匹配，有些技术规则需要频繁的更新，以保证在每次系统更新后保持正确（如用于敏捷云混搭）。在技术策略执行上要建立与人类管理员意图相匹配的信心/保障级别很困难。因此，关键是要仔细规划工具和流程，通过它们让这个访问策略制作/更新过程自动化，以达到可管理。

⁸⁴ Details: Lang U, Schreiner R, Analysis of recommended cloud security controls to validate OpenPMF, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.001

⁸⁵ 混搭式的原文是 mash-up

⁸⁶ Provision from

⁸⁷ Provision to

现有解决方案包括将高级别的安全策略转为（低级别）技术访问规则的自动化方法，包括：

- 模型驱动安全⁸⁸，以有工具支持的流程对安全需求在更高抽象层次上建模，使用该系统的其它可用信息来源（由其他利益相关者产生）。这些输入都以域特定语言（DSL⁸⁹）描述，随后它们会在尽可能少的人类干预下转换成可执行的安全法规。它还包括运行时安全管理（如权限/授权），例如，运行时执行针对受保护 IT 系统的策略、动态的策略更新、以及监控策略违规行为。
- 将技术访问规则聚类到相似的群组以便减少复杂性。
- 通过视觉化使技术策略更易于理解。

10.3.5.6 云中授权的最佳实践

- 仔细考虑相对以身份为中心的角度而言，从受保护资源为中心角度来创建访问策略是否更适合您的环境。
- 确保访问策略的可管理性，尤其是面向动态变更的云混搭应用时。这包括策略制定、策略分发、实施和更新的一致性。考虑使用自动化工具和方法（如模型驱动的安全）来生成策略执行所需的技术访问规则。
- 为策略管理和策略审计指定明确的责任。
- 确保你的云提供者提供授权管理 PEP/PDP，可以通过特定用户的授权策略进行配置，并且你的策略服务器可以与所选的策略正确对接。
- 如果你需要为云混搭应用打造一个集中的策略服务器，应考虑使用“策略即服务”作为策略服务器。

选择授权服务的现有最佳实践如下：

- 授权管理服务最重要的特征是云用户策略的可管理性，因为管理访问策略是授权面临的最大挑战。
- 服务应该考虑到尽可能的自动化的生成（和更新）技术策略（排除人类直觉），以及通用的安全策略需求。
- 如果对企业而言在政策上是可行的，并且于你而言也是可用的，那么可以考虑把“策略即服务”当作外包策略制定和更新的一个选择。这最可能在社区云内得到认可，这种情况下“策略即服务”提供给封闭的社区。
- 确保服务有到 OASIS XACML 等标准的导入/导出功能。
- 确保服务能连接安装在云基础设施中的 PEP/PDP，还能连接用于事件监控/审计的策略监控点。

10.4 云中的应用渗透测试

⁸⁸ 参见 NIST IR 7628

⁸⁹ DSL: Domain Specific Language

渗透测试包含评估应用或系统层出现残余漏洞的过程，外部或内部黑客可能恶意地利用这些漏洞。该测试一般会包括对“黑盒”应用或系统表面的主动分析，并且试图识别可能普遍存在的由不良编程或安全加固实践导致的典型漏洞。

开放 Web 应用安全计划 (OWASP)⁹⁰ 在其 OWASP 测试指南 V3.0 中推荐了以下的 9 个类别的主动安全测试：

1. 配置管理测试
2. 业务逻辑测试
3. 认证测试
4. 授权测试
5. 会话管理测试
6. 数据验证测试
7. 拒绝服务测试
8. Web 服务测试
9. Ajax 测试（RIA 安全测试）

上面的安全测试类别同样可应用到即将在云中部署的应用，因为从技术角度来看，应用漏洞的本质不会改变。但是根据云部署模型的类别来看，可能还包含额外的威胁向量（这在非云中部署没有）。

在 SaaS 部署中，这样一个威胁向量的例子由多租户引起，它发生在相同的应用运行时间用来服务多个租户及其隔离数据的时候。

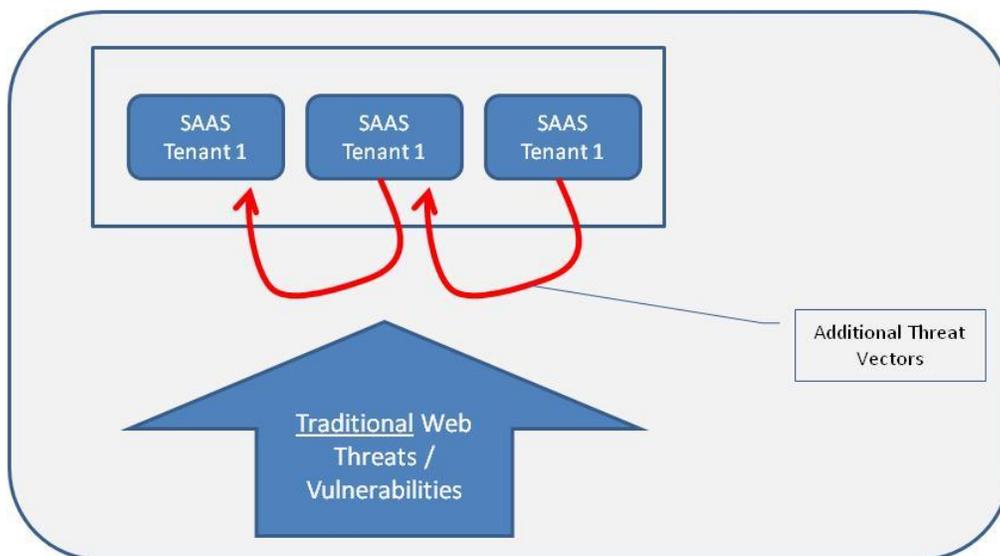


图3-威胁向量继承

⁹⁰ OWASP - Open Web Application Security Project, www.owasp.org

为应对因云计算应用部署模式而导致的新生威胁，需要开发和囊括额外的其他类别的测试。下表对此详细说明。

表 2-威胁向量继承

部署应用上的云模型	额外的威胁诱导	威胁示例	相关的传统安全测试类别	额外的测试类别
SAAS	应用级别的多租户	使用相同 SaaS 基础设施一名租户通过 Web 层漏洞（权限提升）获得另一名租户的数据	<ul style="list-style-type: none"> ▪ 配置管理测试 ▪ 业务逻辑测试 ▪ 认证测试 ▪ 授权测试 ▪ 会话管理测试 ▪ 数据有效性测试 ▪ 拒绝服务测试 ▪ Web 服务测试 Ajax 测试（RIA 安全测试）	<ul style="list-style-type: none"> ▪ 多租户测试（权限提升）特权的扩展
PAAS	平台级别上的多租户	同上	同上	同上
IAAS	基础设施级别上的多租户	虚拟化安全的不足（VM 分区、隔离的不当执行导致跨多个 IaaS 租户的 VM 间攻击。）	传统的基础设施漏洞评估（需要“定义”它）	VM 间安全/漏洞测试

10.5 云中的应用监控

和云安全的其它方面一样，在基于云的系统中监控什么和如何监控会因云类型的变化而有所不同。这对监控云应用意味着什么？如何监控不同类型的云应用？下面将对此进行详细阐述。

10.5.1 云中的应用监控: 平等交换

在本文中，我们限定“监控”专注于应用安全监控。特别的，下列各项指标应该得到解决：

1. **日志监控。**它不仅仅是出于合规目的而归档日志。了解可能这些日志的潜在产出，并监控可操作的事件。除非存在流程来发现并响应应用错误的日志，否则应用错误的日志就什么用也没有。

2. **性能监控。**它是共享云计算的一个重要因素。一个应用性能的显著变化可能源于一名客户对受限资源（如 CPU、内存、SAN 存储）的使用超过了公平分配的资源限制，或者源于受监控的应用或者是在共享基础设施中的其它应用中存在恶意行为。
3. **监控恶意使用。**其成功要求结合审计和监控。当恶意用户企图访问或使用他们没有的权限时，企业必须了解发生了什么。审计日志必须记录失败（和成功）的登录尝试。数据验证功能会记录所有事情吗？如果一个应用经历了流量负载的大幅度增长，是否会在什么地方创建一个警告呢？
4. **监控违规。**这里的关键在于企业如何快速、高效地响应违规。根据应用的复杂性，决定违规也许相对容易些（例如“用户 A 登录了两次”），也可能需要更多的努力（例如，开发启发式算法来监控数据的使用）。这是一个很好的例证，在 SDLC 中越早的阶段解决，其管理就会越简单。
5. **监控违反策略（尤其是访问控制）行为。**监控和审计一个策略决策点如何做出决策很重要，例如，应用了哪些策略规则来做出特定的访问决策。这符合通用的策略驱动的监控方法，该方法能避免误报及事件超负荷等一般监控问题。

这些是日志监控背后的关键概念 - 平等交换等式中的“获取”部分。同等重要的是，应用的开发者负责相应的“给予”部分，他的应用必须提供可靠的记录子系统来让监控系统高效地进行工作：

1. **易解析的。**日志应该写成可以很容易的被异构系统进行解析的格式。一个好的示例是使用 XML 之类的知名且被普遍接受的格式。一个不好的示例是采用无描述的、多行文本输出格式写日志条目。
2. **易读取的。**除非以人类无法直接读取的二进制格式编写，否则毫无疑问，对于有技术背景且熟悉应用的人来说，日志条目应该是能看明白的。
3. **良好的文档。**仅仅编写文件日志是不够的。错误代码需要被文档化，并且应该是唯一的。如果特定日志条目有已知的解决方案，对该解决方案建立文档，或提供指向它的参考。

10.5.2 监控不同云类型中的应用

对于基于 IaaS 的应用，相比于部署在非共享环境中的“遗留”应用，监控该类应用几乎是“正常的”。客户需要监控共享基础设施的事件或恶意合租户（co-tenant）对应用的无授权访问尝试。

监控部署在平台云的应用需要额外的工作。除非平台提供商还提供能够监控已部署应用的监控方案，否则客户只有两个选择：要么编写另外的应用逻辑来执行平台内的监控任务，要么把日志发送到一个远程监控系统，这个系统可以是客户的内部监控系统，也可以是一个第三方服务。

由于 SaaS 应用提供最少的灵活性，监控这类应用的安全性是最困难的，这是在意料之中的。在使用 SaaS 产品之前，客户必须对以下问题有个通透的了解：

- 提供商如何监控其应用？
- 提供商会给客户发送什么类型的审计、日志或警告信息？客户能选择他们将接收什么信息吗？
- 提供商用何种方式向客户传递信息？（Twitter？邮件？定制的 API？）

云中应用安全监测要考虑的最后一点：虽然提供商（或第三方云监控服务）搭建了一个监控系统来监控客户的应用，但这些监控系统正监控着几百甚至几千个客户。提供商作为一个企业，当然希望这个监控系统能够工作得“足够好”。如果客户有资源，运行只监控自己应用的自主监控系统通常会比云提供商的系统响应更快，信息量更多。

10.6 建议

10.6.1 安全保证建议

- 定义功能和监管的安全及隐私需求来满足云开发及部署的需要。
- 云环境中攻击向量和风险的详细评估是可以理解的，且应对策略也要整合到需求中去。
- 执行并记录对所有风险和攻击向量的影响评估，连同每种情况下造成潜在的损失和损害。
- 安全和隐私需求及努力应优先于可能性和影响。

10.6.2 风险分析建议

- 对应用的安全和隐私的进行风险分析（机密性、完整性和可用性），并且应创建并维护威胁模型。
- 应该从云中的开发和部署角度来分析风险并维护相关风险模型。
- 应该分类并维护云架构特定的攻击向量和影响分析。
- 应该维护安全保障功能和所有已确认的风险/威胁之间的可跟踪性。

10.6.3 架构建议

- 应该开发并维护安全的软件架构框架。
- 应该使用能明确降低威胁的云计算架构模型（例如，来自“开放安全架构”或 TOGAF/SABSA）。
- 应用架构中可复用的构建模块可用于降低众所周知的安全及违规的情况。
- 应使用云特定的安全数据架构来增强已选择的安全架构框架，这将解决如下云特定的问题和威胁：
 - 动态数据库服务器的监控
 - 在任意时间能确切了解数据库托管位置
 - 集中记录所有活动，跨越不同（可能是全局的）系统行为的日志，来提供应用的整体视图，标记可疑事件。
 - 规定必须使用加密的地方（见 D12）
 - 由第三方提供系统、数据和所有特权行为范围内的充分的职责分离，数据所有者企业的员工能监控它们。

10.6.3 云上渗透测试建议

- 执行常规的 Web 应用渗透测试来检查十大 OWASP 漏洞。
- 基于危急程度/影响对漏洞进行分类并且有修复流程。
- 从多租户角度执行手动测试来验证没有提升权限漏洞，并在缺乏会话执行下验证数据隔离。
- 对于迁移到 IaaS 或 PaaS 环境的应用来说，需要执行安全评估来确保 VM 分区和隔离、虚拟化安全等潜在的安全控制已经有效实施且不会给应用生态系统造成太大的风险。

参考文献

- [1] The Building Security In Maturity Model. <http://bsimm.com/>
- [2] OpenSAMM – Software Assurance Maturity Model. <http://www.opensamm.org/>
- [3] DAVIS, NOOPUR. Secure Software Development Life Cycle Processes. Software Engineering Institute
- [4] SP-011: Cloud Computing Pattern. <http://www.opensecurityarchitecture.org/cms/en/library/patternlandscape/251-pattern-cloud-computing>
- [5] KRUTZ, RONALD L. and VINES, RUSSEL DEAN. 2010. Cloud Security- A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing, Inc., Indianapolis, IN.
- [6] SARNA, DAVID E.Y. 2010. Implementing and Developing Cloud Computing Applications. Auerbach Publications.
- [7] BELK, MARK, COLES, MATT, et al. 2011. Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices in Use Today, 2nd EDITION. Software Assurance Forum for Excellence in Code. http://www.safecode.org/publications/SAFECode_Dev_Practices0211.pdf
- [8] RITTINGHOUSE, JOHN W. and RANSOME, JAMES F. 2009. “Cloud Security Challenges” in Cloud Computing: Implementation, Management, and Security. Auerbach Publications.
http://www.infosectoday.com/Articles/Cloud_Security_Challenges.htm
- [9] Guidelines on Security and Privacy in Public Cloud Computing. Computer Security Division Information Technology Laboratory. 2011. National Institute of Standards and Technology - Gaithersburg, MD 20899-8930
http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
- [10] Homomorphic Encryption. Making Cloud Computing More Secure.
<http://www.technologyreview.in/computing/37197/>
- [11] Cloud Data Protection. Best Practices. <http://www.ciphercloud.com/blog/?cat=10>

D11: 加密与密钥管理

对于一个安全专业人士而言，如果一个组织需要存储数据，但又不确定谁能访问或使用这些数据，很显然这些数据必须要加密。在本地数据中心内，组织能够控制所有的数据资产，只有在采用一些明确要求的加密的规范（如 PCI DSS）时才会对数据加密。

在云计算环境中，由于有多于一个的租户，以及为别人工作的管理员，需要加密的数据将急剧增加。如果是这种情况，这些过程如何工作？这些组织如何管理他们的密钥？加密所有的东西将会增加复杂度。甚至于，加密带来的处理上的复杂度是否会使得弊大于利？是否存在其他的方式减少加密的需要及管理密钥？本章将关注这些问题。

概览 本章将讲述以下主题：

- 介绍加密
- 可供选择的加密方法
- 云部署中密码编码
- 云数据库中加密
- 云中密钥管理
- 密钥的存储和防护

加密还是不加密？这是个问题。如果加，怎么管理密钥？如果不加，风险会太高吗？

11.1 加密介绍

出于合规或公司隐私的需求，机密的数据必须要保护。随着由系统内部管理的机密信息不断的迁移到云中，与之相应，需要花同样的力气去保护这些机密信息。将数据迁移到云中对提高机密性和数据保护没有任何帮助。与之相反，由于失去了对处于公司安全边界外的数据的控制，将会增加数据保护的复杂度，欺诈的风险也会上升。

有很多因素促使我们考虑云中数据加密，包括：

- 在将数据迁移到云中时通过加密来保护数据，所需要做的多于仅仅确保使用安全转移通道（如 TLS）。在数据传输过程中加密不能确保数据在云中能得到保护。一旦数据达到云中，这些数据无论在云中还是在使用仍然需要保护；
- 对于在云中存储或共享时必须保护的无结构文件。这些文件可能通过以数据为中心的加密进行保护，或者在能够直接对文件进行保护时将加密嵌入到文件格式之中。
- 理解在数据的整个生存周期中，如何管理加密或解密的密钥。只要有可能，都应避免依赖云服务提供商去保护，并且应该适当地使用密钥去保护你的关键信息；

- 加密可以避免因为雇员失误造成的损失，或者区域法律造成的麻烦。除非需要委托别人访问你的加密文件。如果只有你自己有密钥，那么只有你资格访问你的文件；
- 不要忘记保护那些经常被忽略的文件，因为它们经常包含敏感信息。登录文件和元数据可能是数据泄露的途径；
- 使用足够耐用的加密强度（如 AES-256）的加密技术，遵守同一公司规定批准的方式去机密维护的文件。使用公开有效的格式，只要有可能的地方应避免使用专用加密格式。

11.2 可供选择的加密方法

在云计算里，有充分的因素促使用户去寻找可供选择的方法去加密数据。因为很多组织将数据发送到云中就相当于转移了保管关系。

对于这些组织将不安全的数据发送到组织外部是有一些问题的：

- **令牌化**：私有云可以整合成为公有云服务以存储敏感数据，发往公有云的数据已作改变，且包含残留在私有云里的数据的参考；
- **数据匿名**：在处理之前去除个人可识别信息(PII)⁹¹和敏感个人信息(SPI)⁹²
- **利用云数据库控制**：访问控制植入数据库可视为提供了合适的等级隔离

作为规则，在将数据迁移至云中之前好的数据管理措施是至关重要的，不管所有或者仅是一部分数据加密，或用其他的方法保护，或根本就一点都不保护。

当评估通过加密或者其他方法保护哪些东西时，数据共享⁹³的风险可分解为两个基本的类别：泄露（公开）、滥用，包括以下方面：

- **意外公开泄露**，使得信息或数据可被一般的公众通过公共网站获取
- **意外或恶意泄露**，由于不恰当的数据保护使信息或数据被第三方利用的行为
- **强迫公开给第三方**，有义务回应以诉讼的形式要求数据公开行为
- **政府公开**，依据法律或法院命令将数据对政府公开
- **滥用用户或网络档案资料**，通过分析和数据挖掘去从看似为交通数据中提取出敏感信息，以揭露用户行为、关系、偏好或兴趣
- **滥用推理**，能够合成一阶或二阶识别器去描绘推理关于个人的行为或身份
- **滥用重鉴定和去匿名**，通过访问足够的匿名信息以推测原始主题

⁹¹ PII - Personally Identifiable Information

⁹² SPI - Sensitive Personal Information

⁹³ <http://www.caida.org/data/sharing/>

11.3 云部署中的密码编码

在加密部分常用两个互补的概念，它们是：

- **内容感知加密：**在数据防泄露中使用，内容感知软件理解数据或格式，并基于策略设置加密。例如在使用 email 将一个信用卡卡号发送给执法部门时会自动加密；
- **保格式加密：**加密一个消息后产生的结果仍像一个输入的消息。例如一个 16 位信用卡卡号加密后仍是一个 16 位的数字，一个电话号码加密后仍像一个电话号码，一个英文单词加密后仍像一个英语单词；

从企业内部到云上时，加密过程可以不需要用户干预是保障数据安全的首选方式。如果软件能配置协议感知，内容感知软件能够促进公有云加密的改善，加密的领域可从 REST⁹⁴ http 事务扩展到公有云应用等领域；现今的数据防泄露(DLP)⁹⁵应用案例满足产品的需求，能增强对将要离开企业的数据（通常以 email 形式）的保护，并在数据离开企业之前加密。这种原理可用于云数据保护，不过数据防泄漏产品或许产生警告。一个内容感知服务需要探测、加密和记录而不是警告。

保格式加密比内容感知更进一步，通过检测数据的敏感程度来决定加密及维持数据格式和类型。例如使用传统的加密，一个信用卡的卡号被加密后的结构是一个密文，再也不是一个 16 位的数字。保格式加密将会产生加密后的 16 位的密文⁹⁶数字。

通过保持数据类型和格式，这一服务能在众多的协议上有秩序地轻易改变很多数值。保格式加密的关键挑战是加密大规模的明文数值，如存储在云中的 email。大规模加密通常地是使用块加密⁹⁷算法，对文本数据进行。在保格式的应用中，需要花费一定的时间将每一个单词加密成相同长度的字符串。不过，加密后的密文结果能像原始明文一样存储在相同数据类型的文件中。

云应用中加密为商业应用提出一些问题，应用架构需要解决，具体如下：

- 如果需要查询记录或者对象，加密过的主键（**primary key**⁹⁸）将使查询过程很复杂；（译者注：密文域的信息检索要比明文的检索复杂的多）
- 如果云应用集包含一批工作或其他涉及敏感数据的处理过程，尤其是 PII 和 SPI 数据，这些处理过程迁移到云中时，云环境将会使密钥管理变得复杂；

一个应用需要在数据库中找到记录或对象时，可能采用另外一种方式去存储唯一的值，例如令牌化。令牌常被用在信用卡环境中，以确保信用卡卡号在应用中最低程度的被访问。从数值中产生的唯一的令牌能被用于产生新的主键，这些主键可以在公有云上的应用中使用，而不会暴露敏感数据。

正如在下面 11.4 中将要讨论的，在可能的情况下，密钥不应存储在云中，而必须被企业本身或一个可信的密钥管理服务提供商所维护。

⁹⁴ REST: Representational State Transfer, 表述性状态转移

⁹⁵ Data Leak Prevention (DLP) products have an enforcement mode that detects data leaving a secured device or the enterprise and encrypts it.

⁹⁶ Cipher text - The result of an encryption operation. The input is known as clear text.

⁹⁷ Ciphers - Algorithm based software/hardware that perform encryption/decryption and signing/verifying

⁹⁸ Primary key - A database column/field/attribute that is used to uniquely identify records in a database

在云上，与其他应用程序和数据一同工作的过程，如果需要操作明文数据，为实现其功能，必须能访问密钥或服务。更多详细内容参见 11.4 云中的密钥管理。

11.3.1 云数据库加密

第一件事需要考虑加密数据的必要性。所有的数据库都具有限制访问的功能。某些合适的实现已经足以保护数据机密性。

其他需要通过加密来保护存储在数据库中的数据因素有：

- 对数据库的特权用户（如数据库管理员）隐藏数据
- 为了遵守法律法规（如加利福尼亚州法律识别 1386）
- 数据拥有者不能通过帐户来控制对数据的访问（如使用共享账户）

当使用云数据库，特别是用到了数据库的 SaaS 解决方案时，数据库的正常功能将会降低，迫使数据库或云应用能访问密钥，除非能在密文上操作。

数据加密会带来复杂度和性能上的成本。除了加密之外，还有一些别的有效方法：

- **使用对象安全。**使用 SQL 准许及废除声明去约束账户访问这些数据。这些账户中哪些准许访问的必须严格控制，以确保只有授权的用户才能访问。
- **存储安全哈希值。**存储这些数据的哈希值而不是直接存储这些数据，这能允许你的程序能证明持有者有正确的值而不必实际存储它。

11.4 密钥管理

在公有云计算中一个很困难的过程就是密钥管理，公有云中的多租户模型造成其上运行的过程需要考虑密钥管理问题。

最简单的应用案例是在公有云中有应用程序运行，加密数据的从企业内部流到公有云中，密钥仅供企业内部使用。正如在第一部分中所述的，有的加密引擎能够在数据流出时加密，在数据流入时解密。当公有云上的其他处理过程，例如批处理，需要访问密钥去解密数据时，一个使用密钥的应用程序将变得复杂。

企业中使用者需要拥有他们自己的密钥，而不是一个能用于访问整个企业的单独的共享密钥。最简单的解决方法是采用一个加密引擎，基于实体身份信息为每一个用户或实体⁹⁹分配（或管理）一个密钥。以这种方式，为一个实体特别加密的任何信息将为那一实体所维护。如果一个群体内的实体需要共享数据，那么可以为管理群体访问的应用程序分配一个群体级别密钥，并在群体内的实体间共享密钥。密钥在企业内部应该像这一部分前面讨论的那样进行管理。

⁹⁹ Entity - For the purpose of identity, could be a user, code, a device, an organization or agent

当数据存储在有云环境中，在停用这一环境时，证明所有数据（尤其是 PII 或 SPI 数据或隶属于法律法规的数据）已经从公有云环境中删去，包括其他媒体如复制盘等，将存在着问题；维护当地密钥管理能够从密钥管理系统中废除（或删除或丢失）密钥，以确保任何数据残留在公有云的数据不能被解密，来提供这一保证。

11.4.1 密钥的存储和安全防护

如果云服务提供商和用户没有一个有效的密钥管理过程，加密数据就没有多大价值。

在服务提供方，需要关注的因素包括，服务器拥有加密的数据，同时访问密钥服务器缺少职责划分¹⁰⁰；数据库管理员能访问个人密钥；或数据库服务架构依赖于单一密钥。

使用密钥加密密钥¹⁰¹，在内存中产生加密密钥，以及只存储密钥服务器的加密密钥，都是能控制和保护密钥本身的有效的架构解决方案。构建任何解决方案时都应该考虑这些。

客户端密钥管理，在本身并不安全的设备（如移动终端）上保护密钥，或者这一设备没有得到同等级别的控制，都是需要考虑的因素。

11.5 建议

总体建议

- 当使用任何形式的加密或解密产品时，应用最好的密钥管理措施。
- 如有可能，应该使用可信源中现成的技术，以得到最佳实践。
- 使用最好的密钥管理实践，获取技术和产品用于加密、解密、签署，并从可信源中核实。
- 尤其建议组织要维护他们自己的密钥或使用已经运营这种服务的可信密码服务。
- 如果一个组织需要使用存在云中的数据运行分析或其他处理，这个组织应该基于一个平台如 Hadoop 开发，从云中的数据源中导出数据；这种开发平台，包括 Hadoop，会有它们自己的安全问题，但这并非本章的内容。
- 密钥的管辖范围能在个人或集体级别维护。
- 集体访问的管理可以使用现成的技术，如 DRM 系统，或者其他运行在桌面或笔记本上，用以加密硬盘、文件和 email 消息的软件。

数据库加密建议

- 使用标准算法。不要使用专用的不规范的技术，专用加密算法没有被证明且容易被攻破。
- 避免使用旧的不安全的加密标准如数据加密标准（DES）。
- 使用对象安全。即使在加密的情况下，也应该坚持使用基本对象安全（SQL 准许及废除声明）去阻止对数据的访问。
- 不要加密主键或者索引列。如果加密主键，将必须加密所有的参考外部键。如果你加密索引列，当你曾是使用加密数值时，查询数据将会很慢。
- 使用柱状的方法去加密（因为大数据系统使用这种方式）。

¹⁰⁰ SOD - Segregation of Duties

¹⁰¹ KEK - Key Encrypting Keys

11.6 要求

- ✓ 为了维护最好的实践措施和通过审计，企业应该自己管理他们的密钥，或者使用来自于加密软件提供商那里的可信服务；
- ✓ 现有加密技术中使用的密钥如 DRM 和硬盘加密产品应该在企业内部，使用密钥存储技术来集中管理；硬件安全调制应该用于存储密钥，以及处理加密操作如加解密、签名和修改等；
- ✓ 企业使用者应该通过注册步骤去启用企业中的加密操作和其他处理，如能根据需要来访问加/解密密钥的内容感知或保格式加密系统
- ✓ 基于身份认证的所有组件，将技术部署整合进公司系统，在处理流程中做授权决定
- ✓ 使用捆绑加密操作来管理加解密过程的密钥
- ✓ 如有可能，使用现有的系统如 E-DRM¹⁰²或数据防泄露（DLP）
- ✓ 将加密操作和密钥管理捆绑到公司的身份认证系统上，为组织提供最大灵活度的整合，以及使用组织已经了解、审计过的或检验过的技术。

¹⁰² E-DRM - Enterprise Digital Rights Management. A process that protects content such as internal corporate communications or copyrighted material.

D12: 身份，授权和访问管理

云环境下对身份，授权和访问管理概念的理解较传统计算环境需要根本的改变，可以分成三个相对独立的部分：身份，授权以及授权访问管理（IdEA）。

对于大多数机构来说，部署一个传统应用意味着在 DMZ¹⁰³区部署一台服务器，以及在大多数情况下关联一个目录服务（DS¹⁰⁴）（比如 Microsoft Active Directory，Novell eDirectory，或 Open LDAP）用于用户认证。在某些情况下，意味着部署一个应用或采用独立认证系统的基于 WEB 的服务，需要用户必须记住一系列的凭证（甚至更糟，复用其他可能具有更高信任度的域的证书）。

相反，一个部署完善的基于云的服务或身份应用需要向各种外部来源提供服务并关联不同的属性（身份不仅应用于用户（Users¹⁰⁵），同时设备、代码（Codes¹⁰⁶）、机构和代理都拥有身份和属性）。在一项事务中，全面考虑身份和属性，使得云系统能够提供更好、更全面的基于风险的，以及对系统、进程和数据细粒度访问的决策（在授权过程¹⁰⁷中确定，并被授权和访问管理组件执行）。

在这个过程中采用多种身份来源及其相关属性是十分重要的，特别是当云应用有可能会面向互联网，同时有可能是该机构希望采用“真实”的云服务以及在其 DMZ 中采用虚拟化技术来连接自有的内部目录服务时，需要克服的主要障碍。

这个去边界化¹⁰⁸的防护思路为身份、授权以及访问管理去边界提供了一个更为灵活和安全的手段，同时也可以在企业内部部署实施。

概述 接下来各节包括云环境下身份、授权和访问管理的主要内容：

- 云环境下的身份介绍
- 云身份架构
- 身份联邦(Identity Federation)
- 身份和属性的提供和治理
- 授权和访问管理
- 与身份和属性提供商对接的架构

¹⁰³ DMZ- DeMilitarized Zone，非军事区

¹⁰⁴ Directory Service : DS 或目录服务，本节中作为通用企业目录服务使用，用于用户名和密码登录

¹⁰⁵ Typically humans; for a wider definition and expansion refer to www.opengroup.org/jericho/Jericho%20Forum%20Identity%20Commandments%20v1.0.pdf

¹⁰⁶ Code includes all forms of code, up to including applications and self-protecting data.

¹⁰⁷ Entitlement：“授权”是一个对身份及其相关属性授予权力的过程（例如对一个应用或其数据的访问）

¹⁰⁸ De-perimeterization：“去边界化”是在 Jericho Forum 中使用的名词

- 身份和属性的信任等级
- 云系统账号的提供
- 身份应用设计
- 身份和数据保护

12.1 术语

不同语言中围绕身份的说法容易使人混淆，一些词语对于不同的人有着恰恰相反的意思。在阅读本章的过程中为了避免混淆的出现，在本章中使用的部分身份词语，其定义如下：

- **身份 Identity**。可以一致和全面地确定一个实体的唯一性的方法。
- **标识 Identifier**。可以加密地断言一个身份，通常使用公钥技术。
- **实体 Entity**。不同类型（用户，设备，机构和代理）所对应的身份。
- **权限 Entitlement**。将权力（例如对一个应用或其数据的访问）映射给身份及相关属性的过程
- **简化登录 Reduced Sign-on (RSO)**。通过账号及凭证同步工具减少用户需要记住的凭证数量（如用户名和密码），大部分情况下是一种折中的安全方案。
- **单点登录 Single Sign On(SSO)**。使用类似 SAML¹⁰⁹和 OAuth¹¹⁰这样的安全标准，通过云服务安全地交付身份和属性。
- **联邦 Federation**。一个身份知识库到另一个身份知识库的连接。
- **角色 Persona**。由身份附加特定的属性提供环境供实体操作。角色可以是个体身份与机构身份及机构属性的叠加（例如，一个名叫 Fred Smith 的企业角色，可以是 ACME 公司的 CEO，也可以是属于 ACME 公司的个人计算机）。
- **属性 Attributes**。从不同方面描述身份。

12.2 云环境下的身份介绍

一个身份的生态系统面临扩展性的挑战（可以想象从一个小镇搬家到一个大镇子或城市）。随着业界身份系统从单独的计算机到全球企业再到云部署模式的迁移中，能够在业务处理中标识所有的实体变得越来越困难。

然而，云计算下，在业务处理的价值链中，对于所有的实体使用身份并采用基于风险的决策，不仅可以缓解风险，同时可以潜在地提高安全性。

¹⁰⁹ SAML: Security Assertion Markup Language, 安全断言标记语言

¹¹⁰ OAuth: Open Authorization, 开放授权

当部署采用身份信息的云方案时，需要考虑如下要点：

- 与某身份关联进行风险计算，作为输入的该身份的强度定义。（例如，包括匿名者，自我主张，由具有知名度和信誉度机构给予机构身份的强断言认可）
- 角色的属性，例如身份，在与某角色关联进行风险计算时，作为输入的该属性的强度定义。断言强度从自我主张到来自具有知名度和信誉度机构给予的认可。
- 由于身份和属性需要为多个来源提供服务，因此云方案/云体系需要具备向多个互不相关来源提供身份和属性服务的能力。
- 充足的身份保证临时性的需求（足够的信息来标识实体的唯一性）。
- 满足对匿名身份的需求（例如投票）。

12.3 云身份架构

在传统的基于边界的机构体系下，在内部数据中心基于传统服务器的应用无法为该机构机构提供足够的灵活性。然而，不管是部署在机构边界的内部（私有云）还是外部的公共云（SaaS，PaaS，IaaS），基于云的体系架构可以提供更多的灵活性。

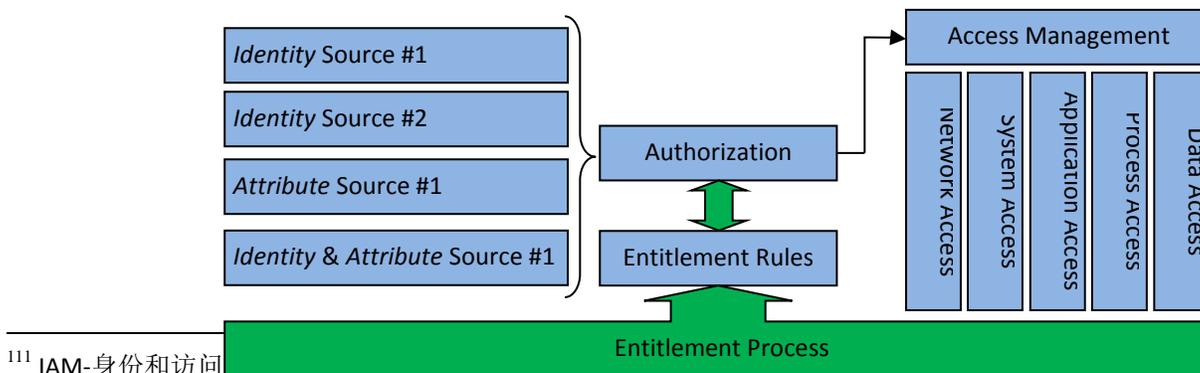
接下来的表格体现了传统部署和不同云体系下部署模式对身份的需求：

表1 - 身份体系断言

体系类型	传统体系	云体系
内部/边界化	连接内部的目录服务，应用需要调用的身份其维护必须在内部目录服务中，潜在的使用 RSO 方案。	可以从多个来源获得身份和属性
内部/去边界化	需要严格控制，在连接企业服务时需要在对端采用 VPN 隧道。不是一个建议采用的体系。	使用断言提供身份和属性来访问云服务
外部/边界化	外部主机托管意味着边界延伸到提供主机服务的供应商。身份扩展到企业无法管理的外部，往往需要复制部署一个目录服务以保证基本的性能。	使用断言提供身份和属性来访问云服务
外部/去边界化	外部主机托管意味着通过对端专线或 VPN，将内部身份扩展到外部环境中。身份扩展到不属于使用者并无法管理的外部环境，往往需要复制目录服务到外部环境中，以保证性能。	使用断言提供身份和属性来访问云服务

在传统的“IAM”¹¹¹体系中，所有的组件往往作为一台单独服务器的一部分独立存在。云体系下则较复杂，身份和属性的来源很多，而授权/访问管理的决策通过一套由授权过程定义的授权规则来决定。

如图 1 所示，身份和属性（潜在地）来自多个来源，同时作为授权/访问管理层的输入，将授权规则转换成访问管理。



¹¹¹ IAM-身份和访问

图1 通用身份、授权和访问管理系统

访问管理必须（依据业务/安全需求，以及 IaaS, PaaS 或 SaaS 的云部署模式）监管如下访问：

- **网络层。**不满足授权规则，则可能无法“发现”（例如 Ping 或 route）云系统。此外，授权规则可以直接访问特定的接口。
- **系统层。**授权规则定义允许访问和修改系统的协议，例如终端服务器或网站服务器。
- **应用层。**授权规则将身份及属性通过特定应用的功能体现出来，展现为精简的菜单或选项。
- **处理层。**授权规则可以用来定义一个应用内部运行的进程（或功能）。授权也定义了需要额外认证（可以直接获取或从背景中引导出来）的增强功能（例如从生态系统中提取出资金）。
- **数据层。**授权规则可能限制访问不同区域的数据和文件体系，或单独文件及文件里的字段（例如数据库）。在更高级的层面，授权可以被用来自动化地编辑文档，例如两个用户同时访问相同的文档看到的却是不同的内容（例如建立特定的动态的数据库表）。

授权过程始于客户对业务和安全的需求，最终转化为授权规则。这个过程将对用来评估授权规则的身份和属性进行定义，而规则反过来驱动授权/访问系统。

12.4 身份联邦

概念上来讲，联邦是指建立在完全不同的目录服务间的关系。某些机构采用联邦网关（“桥”或“联邦 Hub”）来实现外部联邦的部署。联邦及其一系列对联邦网关中身份管理的规则，通常来说是一个正式的合同，允许其他合作伙伴在这座桥梁上采用一致的和明确的信用等级定义，而不是自行发布。

从技术上来讲，联邦采用 SAML 来提供分离和相对独立的安全域的可移植性，一些机构使用处理 SAML 断言的网关产品来扩充目录服务环境。另一些机构则采用来自身份服务的本地 SAML 断言。

在上述联邦架构中，有必要了解身份和属性断言的出处。

联邦标准被广泛应用于 SaaS 部署模式下的身份联邦和访问控制。在 PaaS 或 IaaS 中没有类似的标准。云消费者权衡 IaaS 部署模式时需要考虑如何进行身份生命周期的管理（共享账号、指定账号、特权账号等）。企业需要做将特权身份管理（PIM）工具进行超级用户管理（SUPM）和共享用户密码管理（SAPM）操作扩展到云部署模式下的调查。必须为企业或云使用者制定一个完善的高特权访问（HPA）策略。

12.5 身份和属性的开通（Provisioning）和治理

谈到开通，我们一般会想到用户的开通，但这还不够。从基于风险的决策上来说，云系统/应用需要参与交易的全部实体的身份和属性，以及潜在的来自其他系统/进程的其他实体。

下面是一些身份和属性的例子（并不是全部）：

- 用户断言：用户标识（公共/私有密钥中公共的部分）

- 用户名（用户名为另一个身份属性）
- 凭证强度/信任
- 位置断言；IP 地址，地理位置，GPS，蜂窝服务位置
- 机构身份（标识-密码）以及机构断言
- 设备身份（标识-密码）和设备断言；功能需求；功能提供；沙盘能力，安全容器，清洗设备
- 代码身份（标识-密码）和代码断言
- 培训记录/合规等

身份和身份属性的主来源（可能存在多个来源）需要在授权过程的设计中明确出来。

作为规则，尽可能避免将云服务或云应用本身作为身份的主来源（除非基于云的 HR 服务，或提供 Identity-as-a-Service 的云服务）。然而，在向云服务迁移中（这并非最佳实践），云服务/应用可能需要持有身份或采取混合的操作模式。

全部的属性需要和一个身份关联，如果不关联标识及其标识的信任等级，属性就无从谈起。这可能与直觉相违背，授权过程处理的强度在于定义这些属性以满足业务对规则得以有效使用的条件，以及确定提供这些属性（相关实体标识）的授权来源（或越接近越好）。举例来说，包括：

- 安全威胁等级：机构，治理或外包供应者身份
- 其他实体的认可或原有决策：实体身份
- 与一个被防护目标源相关的 QoS 或节流策略：系统身份

12.6 权限过程

权限（entitlement¹¹²）过程始于将业务需求和安全需求转化为可以对云系统不同方面进行授权和访问治理的一系列的规则。接下来，这个过程将定义可以满足正确评估授权规则的身份和属性。授权过程和导出的规则不仅仅需要驱动对云系统的授权和访问管理，同时它们可以确定对于云体系全部层面的协商/授权的程度，例如，允许的网络和/或系统层的协议和接口。

权限过程需要嵌入到所有业务需求文档和技术需求文档中。同时，需要作为来自云厂商提供或“上线（customer on-boarding）”流程的一个组成部分。

云服务一旦启动和运行后，权限过程就不会停止，但是必须对支撑授权和访问的授权规则及其后续规则进行定期的检查评审。授权过程必须依据业务需求由业务的“系统所有者”进行审计。任何的审计必须包括威胁和风险评估以及法律方面的要求。

¹¹² 译者注：翻译中我们将 entitlement 翻译为权限，authorization 翻译为授权，即 authorization 是为为某个 entity 授予手中 entitlement 的过程

当前，自动化地将高级安全策略转化为（低级）技术访问规则的手段包括：

- **模式驱动的安全**¹¹⁸，工具支撑的将安全需求模型化，需要高层次的抽象和使用系统可获得的其他信息源（由其他利益相关者提供）
- 将技术访问规则聚合为同类型的分组来降低复杂性
- 使得技术策略更容易被理解的可视化尝试

权限过程需要对使得授权和访问决策具有意义的实体、身份和属性下定义。同时，需要对要么作为过程中固化的一部分，要么具有临时特点的属性下定义，为此，要么经过一定的时间间隔后重新获得，或通过强制触发获得。

如果权限过程中所定义的身份和属性来自业务控制之外，那么身份提供者（实体）的机构身份（标识）也必须上线，并（在之后的某个时候）下线。

通常，权限规则会在如下三个其中之一地方解释：

1. 使用内部/外部策略执行点/策略服务器/策略即服务
2. 作为云应用的一部分嵌入
3. 使用身份即服务（IDaaS） Using a central/external Policy Enforcement point / Policy Server / Policy-as-a-Service

12.7 授权与访问管理

授权与访问管理是将权限规则（通过授权层）转换为访问管理规则的过程。

在大部分基于云的系统，授权层可能是一个“策略决策点（PDP）¹¹⁹”或评估和发布授权策略的点，同时访问管理层是执行 PDP 决策的点，即，“策略执法点”（PEP）¹²⁰。

PDP 和 PEP 是使用 XACML¹²¹（eXtensible Access Control Markup Language）授权生态系统的一部分，作为 XML 中执行的公开的访问控制策略语言。

PEP 在云应用中可以像 IF（条件）语句一样的简单，也可以很高级复杂，就像运行在一个应用服务器或在一个 XML 网关过滤器之中用来解释访问请求的代理，收集必要的属性（属性）以至于可以评价授权规则，并制定和执行这些决策。

这不是要求在云环境下必须使用 XACML，PDP 和 PEP 进行授权，其功能也可以通过其他方法（可能在一个封闭或私有的生态环境中）来实现。

¹¹⁸ www.modeldrivensecurity.org

¹¹⁹ PDP-Policy Decision Point

¹²⁰ PEP-Policy Enforcement Point

¹²¹ XACML- eXtensible Access Control Markup Language

PDP 可以在云环境之外的客户环境中执行。其潜在好处是与内部目录服务对接以及将围绕认证授权所做决策直接集成到内部日志系统中。

12.8 与身份和属性提供者对接的架构

有三种与身份和属性提供者对接的基本框架：

1. 集中的身份和属性管理并与其它云服务或云应用互动的轴辐模型；
2. 可以配置云服务及云应用支持从多个来源接受身份和属性的自由态模型；
3. 潜在使用其它云服务组件的分布式的混合方案。

每个模型各有其好处，通过如下因素来选择：

- 服务的客户有其对应的身份
- 云服务的选择能力
- 企业提供基于断言的身份和属性能力

12.8.1 轴辐模型

轴辐模式通常允许云服务，以基于标准的断言协议的形式，如 OAuth & SAML，直接就身份和属性与相应机构接口。

机构的内部系统负责跟踪用户、其他实体和属性。这更像一个传统的 IAM 系统，因此对于机构来说，也是最容易的向云方案迁移的方法，因为大多数目录服务或 LDAP 系统具备支持 SAML 的能力。

在这个模型中，授权过程可以在机构内通过一个策略执行点和策略服务器来处理并通过 XACML 进行通信（尽管这样使用 XACML 并不常见）。如图 2 所示。

这个方法的好处之一在于，在机构内部维护一个策略执行点允许在机构内部维护整合的审计日志，甚至可以与其他不相关的审计记录（云环境之外或来自其他云环境）关联从而获得所需要的完整描述。例子包括对职责分离 SOD 的分析和监管要求的符合程度。

当多角度的轴辐模型可以用于通过集中注册的过程对全部用户采用高级控制。还可以用于在机构内贯彻严格的管理。由于属性常常在中心处储存（复制），轴辐模型也可以减少对身份/属性提供者的依赖。

这模型也是一个机构向一个“桥”或“身份中心”注册时可以采用的模型

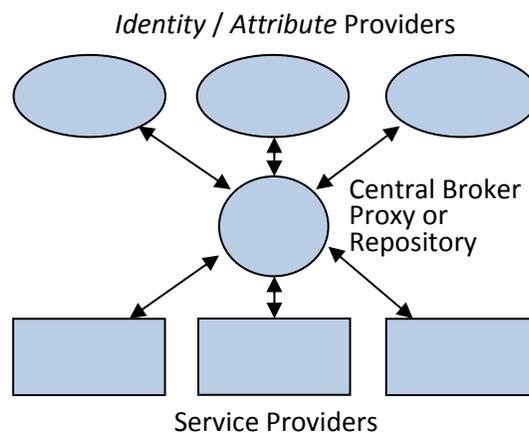


Figure 2— "Hub & Spoke" Model

12.8.2 自由态模型

在自由形态模型中，云服务/应用负责维护身份/属性的来源。这个方案更适合作为一个面向公共的方案或一个存在大量互不相关合作者的方案。

至少在现有的联邦协议（例如 SAML）下，自由形态的好处在于创建简单，但是依赖于是否可以很好地实施授权模型以允许扩展到大量用户。

一个方法是在服务和属性/身份提供者之间建立点对点的联合信任关系（采用诸如 SAML 和 OAuth 协议），但是这个方法需要对这些提供者上线和下线的高效处理。

自由形态模型提供了对“用户”供应的挑战，在新实体环境下，连接更类似 Ad-Hoc 的形式。对授权过程的细致设计有助于缓解这个问题。点对点的模式如图 3 所示。

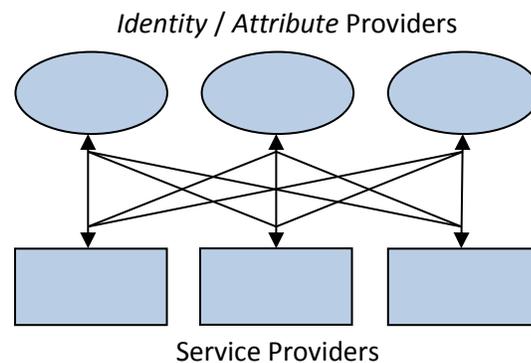


Figure 3—“Free Form” Model

12.8.3 混合式模型

混合模型顾名思义即混合了辐射型和自由形态两种模型。举例来说，授权规则可以掌握在机构内部并向一个提供 PDP 的云服务推送。接下来，这些决策提交给作为不同云服务组成部分的多个不相关的 PEP。在更大规模的部署中，可以存在多个联邦策略服务器服务于很多不同的 PDP/PEP。混合模型还可以存在于机构内，实现云环境（公共或私有）与传统和/或遗留计算并存。

混合模型可以提供对一个分布式资源的有效使用，但是安全漏洞范围的变化会使得风险变得更为复杂。它还会导致长期维护面临很多问题（即便所有的实施人员都离开很久，简单规则背后的原理仍旧容易被理解。）

混合模型还会存在日志决策，以及将所有日志以共同的格式收集到一起进行统一审计这一潜在需求的处理问题。

混合模型潜在的复杂性强调通过可视化工具来开发、维护以及对将身份规则转化为实际访问控制过程审计的需求。

12.9 身份和属性的信任等级

身份和属性来自不同等级的信任，取决于用于交易的不同身份以及赋予这些身份的属性。传统上讲，信任的缺乏导致机构必须要维护所有需要访问其系统的人的身份，可能涉及成千上万的非雇员或无法直接管理的人。

某些机构（军队/航空，制药等）需要采用“桥”或“联邦枢纽”（参见 12.4 节）与一个事先商定好的信任等级关联，同时，获得信任的身份也需要具有相对应的获得信任的属性。

在授权过程中，一个基本的认识是不仅需要属性，同时也需要这些属性的来源，提供它们的机构，以及可以断言它们的（信任等级）强度。

从一个具有任何信任等级的外部机构获取属性，需要一个对该组织的上线过程，同时机构的身份（标识）将被用来进行属性的断言。

作为规则，目的是要求身份和属性从主来源或这些属性的权威来源获得，并且所有的属性具有已知的身份来进行断言。置于属性中的信任等级不可以超过置于身份中对于属性断言的信任等级。

当属性在云系统中被独一无二地创建出来，治理过程就必须到位以保证所有的属性是准确的以及具有恰当的生命周期管理。

12.10 云系统中账号的开通

为云系统提供一个“账号”是必要的（通常是为用户，但是可能为任何的实体类型），当提供（和取消）这些账号时会面临挑战。通常来说，在机构内部使用的常规的“推送”模式对于云部署来说并不是一个可行的方案。

迄今为止，尚无广泛使用或事实上的标准；SPML¹²²（Service Provisioning Markup Language）还没有被云供应商广泛采纳，同时，SCIM¹²³（Simple Cloud Identity Management）也只是作为潜在的标准刚刚出现。

在云系统上提供身份的关键，从涉及到全部系统账号和属性的提供和使用来看，在于对账号全部生命周期的理解，包括创建，管理和最后的消除（包括删除以及存档）。

关于提供身份和属性的来源，需要关注的关键问题在于：

- 人力资源（或人-用户信息的授权来源）存在问题，体现在人力资源往往就是日常工资单上员工的主来源。
- 常常没有合作伙伴及其设备的授权信息来源。
- 在大多数机构中，尚无提供其他实体（特别是机构和设备）的能力。
- 公开的身份服务经常只提供身份自断言并只涉及人，而不能扩展到其他实体类型。
- 取消提供需要扩展到全部实体，然而当合同结束，或发现在系统中存在问题代码或已过期的代码并需要删除代码时，大多数机构并不具备下线其他机构的能力。

上述问题再加上可不成熟的标准，为在云生态环境里做出一个完善的规划并实现身份，属性，账号和全部实体类型的生命周期管理的操作增加了压力。

12.11 身份认证即服务

云身份认证即服务（IDaaS¹¹³）是一个广义的术语其含义包括云服务中的身份、权限及授权或访问管理中的任何一部分的管理工作。

¹²² SPML- Service Provisioning Markup Language

¹²³ SCIM- Simple Cloud Identity Management

¹¹³ IDaaS - Cloud Identity as a Service

此项服务包括了软件服务、平台服务及基础设施服务，同时涵盖公有及私有云。在组织内部通过身份认证依然能够实现内部管理（混合解决方案也是有可能的），与此同时其他的组件例如认证则需要通过面向服务的体系结构加以扩展。这样实际上就创建一个平台即服务层以使基于云的身份认证与接入管理方案更加便利。

更多信息请参考 D14 “SecaaS” 中的身份认证即服务部分。

12.12 合规与审计

考虑合规或安全因素，授权规则的输出则需要通过授权/认证过程所作出的决定一起记录。合规和审计已与身份认证整体捆绑。如果没有合适的身份认证管理，就无法去保证监管合规。审计也需要合适的身份认证管理，如果没有一个能工作的身份认证系统，使用记录文件的价值就很小。

12.13 身份认证的应用设计

本部分致力于将应用设计运用到身份认证中，应该与 D10(应用安全)连起来一起阅读。

由于云服务和应用会用到认证及属性信息，在设计基于云的系统或应用时，需要改变涉及身份认证的观念，并至少保持于交易过程中，其中部分方面可能需要维持更长的时间。但由于云环境很可能不是一个组织的物理组成或逻辑管辖权的一部分，甚至是在不同的法规监管区，那么一个组织对隔离区占有、管理服务及应用设计，需要与传统客户服务有本质的区别。

设计的目标应该是对身份认证与属性的需求最小。从原理上看，如果能理解阈值作用就是将一个动态账号切换到一个确定的账号时，身份认证就是非必要的了。例子如下：

- 使用其他属性来建立唯一的会话，例如连接设备的 IP 地址（考虑 IP 地址可能是虚假的）或唯一的会话 Cookie
- 在很多情况基于属性的授权就已足够，不需要用户信息或实际身份认证；不能假设个人(Persona)需要与会话或账号绑定。
- 当第一次遇到一个新实体（经过安全声明标记语言认证），然后创建一个基本动态账户。（注意这种方法需要通过取消配置）
- 当可能的时候要使用属性推导（如不需要问生日，相反可以询问“是否大于 18”）

当产生任何唯一账户时，需要判断系统是否能销毁一个实体外部唯一标识符或者系统需要产生它自身唯一的标识符（如消费者参考编号）。

必须仔细考虑迁移云系统维护用户的账户；必须要认真设计考虑如何将云用户账号与用户现有的其他系统（内部或者其他云系统）账号同步，尤其是围绕着整合“加入者和离开者”的过程，及当用户在内部移动时对接入访问的需求变化。设计云系统满足可伸缩(scale)的需要，避免强制制通过公共帮助过程，包括手动或半自动同步脚本、密码增强有效性过程、密码重置过程、密码泄密后重置等，这些都归咎于缺少对消费外部身份认证的最初设计思考。

避免尝试扩展内部 DS 到云服务中和/或复制组织 DS 到网络上（通常非常不安全）或者通过秘密通道（专用线或虚拟专用网），因为这样将把组织的整体 DS 暴露在组织无法控制的环境中。同时也担心简化登录（RSO¹¹⁴）产品的保证，因为 RSO 通常以损失登录后的内部安全为代价而工作的，当将 RSO 拓展到云环境下会更加严重。

云服务和云应用作为一个规则应该接受兼容标准单点登录 SSO 联邦格式，如安全断言标记语言(SAML)和 OAUTH 协议（或者甚至更小范围内接受的网络服务联邦规范(WS-Federation)）

当给消费者身份认证和属性设计一个应用时，要记得身份认证包含实体和应用安全，安全是全套方案中的组成部分，贯穿所有层：网络层、系统层、应用层、处理层及数据层（详见 12.3）。云应用可以使用被授权规则（在授权过程中有定义）所允许的两种连接类型作为接入方法，使用 Web/AJAX/Java 或者 Citrix “Screen-Scrape” 模式。

12.14 身份认证和数据保护

如何控制身份认证的各个组成部分，包括个人可识别信息（PII¹¹⁵）以及归类为敏感个人信息（SPI¹¹⁶）的特殊信息，是所有组织面临的共同问题。在组织外部运行或管理的云服务需要专家的建议，来确保其符合所有使用的法律法规。

在考虑适用的法律法规时，可以参考但不限于下述列表：

- 涉及数据主体的所有国家
- 组织运营所在国家
- 组织拥有合法实体的国家
- 组织及所属机构股票交易或已发行股票的国家
- 云服务物理所在地的国家
- 相关法律法规、规章制度和类规章制度（如 PCI-DSS：支付卡行业数据安全标准）

12.15 消费及身份认证挑战

在基于云的服务和应用中，与用户或终端交互过程中带来了一些挑战和机遇。用户和终端直接与面向互联网的云服务交互的能力跳过了复杂网络层，但是带来了一系列的安全挑战，这些挑战未来可以利用身份认证去缓解。

但是在用户空间，终端和用户身份认证的标准是不完整的，很少有一致性和标准化水平相同，这些在公司的环境中能够做到。

不幸的是，大部分用户终端和用户自身不容易或不按标准步骤在要求严格的认证系统中去注册他们的终端或自身信息，因此没有充分身份认证的授权是很困难的。甚至当用户的一个账户已经具备充分的认证方式时（如银行信息），也几乎无法被另一个账户重新使用。这将导致用户的身份认证超过可扩展的极限。资料表明，超过

¹¹⁴ RSO: Reduced- Sign- On，简化登录点

¹¹⁵ PII: Personal Identifiable Information，个人可识别信息

¹¹⁶ SPI: Sensitive Personal Information，敏感个人信息

61%的用户在可能的情况下都会设置相同的密码¹¹⁷，这意味着每一个附加的注册或认证都可能会造成一部分潜在用户的丢失。

解决此问题可通过无缝接入应用，这将使商业便利化，清晰的分拆了身份认证和授权将带来额外的使用便利，比如允许一个人授权使用第三方的个人身份（persona）连接到某一具体的信用卡，代表第三方交易。

12.16 身份认证服务的供应商

利用外部服务进行认证的相关消费信息会带来其自身的一些问题。供应商的可信级别和属性的有效性是其中的两个典型。大多数现有的提案或者实际案例中使用的全面持续身份认证框架是由个人或集团成员的需要演变而来，而很少或者不考虑其他社区的需要。

几乎所有公开可使用的身份认证服务只处理用户的验证，通过使用自我核实或来自于非权威源的属性来提供个人信息（属性及身份认证）。

身份认证和属性的来源举例如下：

- 国家政府
 - 美国，NSTIC（海军科技信息）
 - 德国“电子身份卡(EID card)”、澳大利亚“城市居民卡”、爱沙尼亚“身份证”、芬兰“城市居民证书”、香港“智能身份卡”、马来西亚“居民卡”
- 通过 API 公共集成
 - Facebook 脸谱
 - Amazon 亚马逊
 - Google 谷歌
 - Twitter 推特
 - Windows Live ID 微软通行证
 - OpenID 提供商
- 桥¹¹⁸ 或者枢纽
 - 服务于美国高等教育机构的教学研究桥接¹¹⁹
 - 服务于所有美国联邦机构的联邦公钥基础设施架构

¹¹⁷ <http://www.guardian.co.uk/technology/2008/jan/17/security.banks>

¹¹⁸ www.the4bf.com

¹¹⁹ REBCA: Research / Education Bridge, www.hebca.org

- 服务于航空和国防工业的环球国际安全合作计划¹²⁰
- 服务于生物医药与卫生机构的 生物制药协会¹²¹
- 身份认证服务(Identity Service offering)
- 检查确认自己邮政编码和地址
- Experian、美国征信所 (Equifax)
- 3D 卡证明 (Visa/Mastercard)
- eBay / PayPal / X.Commerce .

12.17 建议

12.17.1 联邦建议

- 云计算使用者(consumer)、云计算实施者 (implementer)、云计算提供者 (providers) 应该在内容和“联邦”的定义上达成一致；
- 实施者应该理解什么是信任关系、已有的信任传递和双向信任关系的需求
- 可能的情况下，实施者应该基于开源的标准如安全断言标记语言(SAML)和 OAuth 协议
- 如果使用“桥接”或“联邦枢纽”，实施者应当理解已经存在于枢纽内不同成员之间的信任的本质与关系。当新成员接入云或与其他桥结盟时，要理解其对自身授权规则的影响。
- 实施者应该明白公开身份认证提供商如 Facebook、Yahoo 或 Google 提供了没有担保的身份认证资源，这些认证低等级、通常自我断言 (self-asserted)，而且将来他们不会联邦其他的提供商。
- 实施者应该反对不好的方案设计，诸如从与云方案访问管理连接的数据集抽取身份信息等。这样的例子如内网中虚拟专用网和网外专业线路。

12.17.2 开通和治理建议

- 所有的属性应该来源于尽可能权威或优异的资源
- 作为一条规则，云服务或应用自身应该避免成为优质认证资源
- 云服务或应用自身应该只是优质的属性直接控制资源
- 所有属性的消费应该有一个已知的信任等级

¹²⁰ CertiPath/Transglobal Secure Collaboration Program: www.certipath.com / www.tscp.org

¹²¹ SAFE-BioPharma Association: www.safe-biopharma.org/

- 所有属性的消费应该与身份认证衔接
- 一个确定实体的识别器应该标记所有的属性消费
- 任何一个属性应该有一个符合目标生命周期
- 任何一个身份（及相关识别器）应该有一个符合目标的生命周期。

12.17.3 权限（entitlement）建议

- 权限过程中的各部分应该清晰定义
- 应该为同意与认可权限规则清晰地指派责任
- 审计权限规则的频率应该清晰的定义
- 权限过程应该聚焦在使用最小特权原则设计产生简单最小化的权限规则
- 权限过程应该聚焦在设计暴露最少的身份信息或者避免一起消费身份信息的权限规则
- 短暂的属性（如位置定位）需要通过交易的有效期重新使得授权规则生效而实现实时属性检查
- 权限规则应该由某个过程进行触发（或者某个初始化意图，例如针对环境外的钱财转移）。在某些环境中，最优的权限规则需要采取屏蔽这些功能的措施。在其他的环境，最好的措施需要额外的身份或属性信息，期望确保实体在某点有权执行这个过程
- 实施者（implementer）应该确保双向的信任关系以确定交易中最优的安全关系，这需要在权限过程中进行定义。
- 权限规则的设计应该包括经过委托（Delegation）¹²² 才能被间接实体访问的部分（不是所有的）信息，而直接实体能访问所有信息的规则。
- 尽管权限规则的设计者需要考虑系统、组织和涉及实体的司法管辖，权限的设计应该包括访问的没收（包括司法占有）。在实现任何访问没收之前，应该听取法务方面的意见。
- 在实际的接口管理、工具或其他可视化技术方面，需要使用它们帮助权限管理，帮助确保互操作满足商业需求或规范（如 SOX 的职责分离）。

12.17.4 授权（authorization）和访问建议

- 实施者应该确保服务有一个入口或出口功能符合标准如可扩展访问控制标记语言(OASIS XACML: eXtensible Access Control Markup Language)
- 当在云计算环境中使用策略决策点(PDP)，为把握访问的整体状况实施者应该知道如何将授权决定日志抽取或整合到一个组织日志中

¹²² XACML 3.0 中已支持委托（Delegation）

- 实施者应该确保现有（遗留）服务能够使用策略决策点(PDP) 和策略执行点(PEP) 进行交互
- 实施者应该确保任何策略决策点(PDP)能恰当的解释在授权过程中定义的授权规则
- 如果需要中心策略服务器时，实施者应该考虑使用策略即服务（policy-as-a-service）作为策略服务器（例如，云混搭 cloud mashups).

12.17.5 架构建议

- 实施者应该确定任何云服务提供商能够提供授权 (Authorization)管理 PEP /PDP，这些可通过权限 (Entitlement)规则来配置
- 实施者应该确定身份、权限 (Entitlement)、授权 (Authorization) 及访问管理 (IdEA¹²³) 的所有组件能够正确的协同工作
- 实施者应该确定策略决策点 (PDP) 和策略执行点 (PEP) 是使用的标准协议（如可 XACML¹²⁴），而避免使用专用的协议（如直接网络服务或者中间件呼叫）
- 实施者应该确定任何强认证服务都是遵从 OATH ¹²⁵的。使用与符合 OATH 规定的解决方案，组织能够避免被锁在一家认证服务上的凭证里面
- 云服务和应用应该具有支持来自使用 SAML 的权威资源的消费认证的能力
- 实施者应该确保服务有一个导入或导出功能符合标准如 XACML
- 实施者应该确定服务能够通过安装在云基础设施上的 PEP /PDP 和用于实践检测或审计的策略检测点交互
- 实施者应该确定关于授权决定和接入的记录能够被允许以一种常见的格式使用标准安全协议登陆。

12.17.6 权限 (entitlement) 建议

- 实施者应该确定权限过程中定义的每一个身份和属性匹配相应的信任级别，这些不仅身份/属性自身需要，而且要与所提供的资源相匹配
- 实施者应该确定所有的身份/属性提供组织的身份信息
- 实施者应该确定无论何时尽可能充分高效的利用属性信息
- 实施者应该确定属性的使用能够正确地推导出正确的结论（你的上下文可能和提供属性的源不一样）
- 实施者应该确定身份/属性源既要在数据质量的标准上，又要在治理机制上满足你的需求

¹²³ IdEA: Identity, Entitlement, and Authorization / Access Management

¹²⁴ XACML: eXtensible Access Control Markup Language, 可扩展访问控制标记语言, OASIS 制定

¹²⁵ OATH- Open Authentication Reference Architecture, <http://www.openauthentication.org/>

- 消费者应该明白信誉是信任机制的重要资源。通过权限定义，消费者应意识到细小的价值转变也会引起交易信任度的增加，这可能会使得随后的大规模交易出现欺诈。

12.17.7 开通（provision）建议

- 提供商应该理解无论 SPML 或 SCIM 可能会是规定中的切实可行选项
- 当准备账户时，实施者应该遵循最小特权（least privilege）的规则，在像计算机设备的实体案例中，到组织机构资产注册表的链接（link）是不错的做法
- 大多数系统和应用在用户和接入上有一对一的关系，没有代表的概念
- 实施者应该确定开通（provisioning）和取消（de-provisioning）对于用户身份而言没有限制，架构必须包括所有实体类型的授权
- 实施者应该确定 provisioning 和 de-provisioning 应该实时操作
- 如果要求权限必须很精确，那么提供商对身份和属性的维护工作非常关键

12.17.8 身份合规与审计建议

- 实施者应该确定来自权限规则或授权过程的可用日志可被利用
- 实施者应该确定日志能被整合进一个更为广泛系统，已确保日志的可用、及时、格式和传输安全是合适的
- 当记录登录决定时，实施者应该将属性与在作决定时的授权逻辑一起组合，结果也应该记录
- 所有云参与者应该记住，在会话的整个生命周期中，那些具有临时组件的属性需要重新确认（revalidated）和重新记录重登录得
- 当记录 PII 或 SPI 时，只要有可能，实施者在记录时应该使用属性变形（derivation）以最小化 PII 或 SPI 的暴露
- 消费者应该意识到包含 PII 或 SPI 的记录也将适用于数据保护法规。

12.17.9 应用设计建议

- 实施者应该使用 ITU X.805 关于用户、系统和管理层的三层定义以确保隔离
- 在应用设计时，实施者应该使得对身份和属性的需要最小化
- 可能的情况下，设计云系统时尽量使用外部资源的身份和属性
- 实施者应该确保云系统支持标准 SSO 联邦格式，如 SAML 和 OAuth

- 实施者应该采取整体策略解决安全，将身份和属性的使用贯穿系统全层
- 实施者应当了解，互认证在所有的层次都很关键，在云环境中甚至更重要。正如云环境需要实体和其他系统去验证一样，云系统也同样需要反向的验证。

12.17.10 数据保护建议

- 实施者应该最小化使用和存储 PII 或 SPI，在授权过程的设计阶段应该这样做，确保在只在身份和属性的关键过程才使用
- 实施者应该考虑下述技术，以最小化 PII 或 SPI 的暴露的程度
 - 加密
 - 令牌
 - 同态加密¹²⁶

更多的信息参见 D11 “加密和密钥管理”

- 实施者应该考虑使用最佳的方法去保护 SPI，如使用双密钥方法，一个被主体拥有（或密钥反抗其他人登录），另外一个供系统处理过程使用
- 实施者应该理解如何约束或停止管理者访问 PII 和 SPI
- 实施者应该理解在被委托的合法时间期限内如何处理“主体访问请求¹²⁷”，尤其是当数据被云系统保有（held），而不被已收到请求的组织拥有（owned）或管理（managed）
- 如果需要分享 PII 或 SPI，消费者需要理解如何获得 PII/SPI 的主体的同意
- 实施者应该减少存储 PII/SPI，尤其是非权威的资源，只参考那些来自于权威资源，而不是存储它们
- 实施者应该理解 PII/SPI（不管是身份或是属性）在维护工作中及时处理的流程

12.17.11 身份认证实现建议

- 实施者应该从身份重用的原则开始，而不是新用户或设备唯一注册
- 消费者应该理解现有的身份资源能提供足够的信任级别和重用
- 提供商应该理解什么样的用户和设备的属性可被断言（asserted）为足够信任级别以用于进行交易
- 在适当的时候，消费者应该允许低级别认证下做低风险交易。只在交易价值/风险的增加时，逐步升级（escalate）所需的身份

¹²⁶ 同态加密（Homomorphic Encryption）当前还处于产品化的早期阶段，尚不够成熟

¹²⁷ 主体访问请求（Subject Access Request），在某些国家，请求关于自己的任何 PII 或 SPI 是合法权利

- 当考虑用户和用户设备时，在授权（entitlement）过程中，提供商应该提供所需身份和属性的关键评估
- 提供商应该理解能够用于用户设备以增加保障水平的技术，尤其是可后台运行的技术
- 消费者应该理解用户设备管理可能不被执行的地方，及其提供的保障级别，保障级别有可能从根本无保障到有很好的保障
- 消费者应该理解在某种保障级别和法律责任存在时，用户设备交易是否会导致问题（issue）出现

12.18 要求

- ✓ 实施者必须设计一个可独立运行的公共服务层，从而在不违反现有信息安全政策和程序的前提下，顺利地删除应用程序。
- ✓ 所有的云参与者必须要尊重供应链的完整性，尊重现有的身份和访问管理（IAM）措施。必须遵守诸如隐私、完整性和审计能力等要素。当将数据迁移至线下和/或将解决方案的核心植入网络服务架构时，必须保持身份认证的完整性和审计。

D13: 虚拟化

虚拟化是基础设施即服务(IaaS) 云和私有云中的关键因素之一，而且越来越多地被应用在平台即服务(PaaS)和软件即服务(SaaS)提供商的后台中。虚拟化也是由公有云或私有云交付的虚拟桌面的一项关键技术。

虚拟化的优点已是众所周知，包括多租户、最佳的服务器利用率和数据中心整合等。云服务提供商可（用虚拟化）实现更高的密度，由此转化更好的利润；企业可用虚拟化来压缩在服务器硬件上的资本支出，同时提升营运效率。

然而虚拟化也同时带来所有以客居方式运行操作系统的安全问题，Hypervisor 层引入的新安全考虑；以及新的虚拟化特有的安全威胁，例如，虚拟机(Virtue Machine)间的攻击和盲点，安全功能消耗 CPU 和内存导致的性能问题，虚拟机蔓延（VM Sprawl）导致的运作复杂度。新的问题如防护间隙（Instant-On Gap），数据混杂（Data Comingling），加密虚拟机（Virtue Machine）镜像的难度，及残余数据清除等正成为焦点。

概览 虚拟化技术有许多形式。当前操作系统虚拟化最常用，也是本章重点关注的。本章包含以下虚拟化相关的安全问题，如果云服务的基础设施采用了虚拟机（VM）技术，这些 VM 系统间的隔离加固是必须要考虑的。

- 虚拟机客居加固
- Hypervisor 安全
- 虚拟机间攻击和盲点
- 性能关注
- 虚拟机蔓延（VM Sprawl）导致的运作复杂度
- 防护间隙（Instant-On Gap）
- 虚拟机加密
- 数据混杂（Data Comingling）
- 虚拟机数据清除
- 虚拟机镜像篡改
- 迁移中虚拟机（In-Motion VM）Hypervisor security

虚拟化带来所有以客居方式运行操作系统的安全问题，以及虚拟化特有的安全威胁。

13.1 Hypervisor 架构问题

13.1.1 虚拟机加固

对虚拟机个体实施适当的加固和保护包括防火墙（入站/出站），主机入侵防御系统（HIPS），网站应用层保护，防病毒，文件完整性监控和日志监控等都可透过软件向每个虚拟机客户提供，或利用内嵌的虚拟机与基于 HypervisorAPI¹²⁸协同提供。

13.1.2 Hypervisor 安全

Hypervisor 需被锁定并参照最佳实践进行加固。使用虚拟化的企业和用户主要关心的是 Hypervisor 所运行物理主机是否有恰当的配置管理、操作和物理安全。

13.1.3 虚拟机间攻击和盲点

虚拟化对网络安全带来偌大的威胁，虚拟机间可能通过硬件背板而不是网络，进行通讯，因此这些通讯流量对标准的网络安全控制来说是不可见的，无法对它们进行监控或内嵌封堵。内嵌虚拟设备可以帮助解决这个问题；另一个解决途径是硬件辅助虚拟化（Hardware Assisted Virtualization），它需要与 Hypervisor 和虚拟化管理框架进行 API 级别的整合。虚拟机的迁移也是令人担心的地方。一个可能的攻击场景是一个可疑的虚拟机迁移进信任区域，在传统以网络为基础的安全控制措施下，将无法检测到它的不当行为（misbehavior）。在每个虚拟机上安装全套的安全工具，是加添保护层的另一途径。

13.1.4 性能问题

将为物理服务器设计的安全软件安装在虚拟的服务器上可导致严重的性能下降，因为一些安全任务，比如病毒扫描就是非常占用 CPU 资源的。虚拟化服务器上的共享环境导致了资源竞争。特别是在虚拟桌面或高密度环境中，安全软件需具备虚拟环境识别能力或它需要能够在一台虚拟机上执行安全功能来支持其他虚拟机。

13.1.5 虚拟机蔓延（VM Sprawl）导致的运作复杂度

在典型的企业中，虚拟机可提供的便捷性，导致虚拟机需求的增加。这缔造了更大的攻击面，错误配置或操作失误导致安全漏洞的几率也随之上升。实施基于策略的管理和虚拟化管理架构的使用是必需的。

13.1.6 防护间隙（Instant-On Gap）

虚拟机关闭/启动便捷，再结合威胁变化的速度，产生了一种情况：当虚拟机被关闭时配置是安全的；但是当它被再次启动时，威胁已经演化了，结果该虚拟机就可能存在漏洞风险了。最佳实践包括基于网络的安全控制和“虚拟补丁”，他们在网络流量到达新部署或新启动的虚拟机前，对已知攻击行为进行检查。也可能采取类似网络访问控制(NAC¹²⁹)的措施，以隔离尚未更新的虚拟机，直至规则和模式库更新到最新并执行完成扫描任务。

13.1.7 虚拟机加密

¹²⁸ API - Application Program Interface

¹²⁹ NAC - Network Access Control

虚拟机镜像无论在静止还是运行状态都有被窃取或篡改脆弱漏洞。对应解决方案是在任何时刻对虚拟机镜像（image）进行加密，但这又会导致性能问题。在安全性要求高或有法规要求的环境下，（加密的）性能成本是值得的。加密必须与管理性措施、数据泄露保护（DLP）和审计踪迹配合以防止运行中虚拟机的快照（Snapshot）“逃到野外”，从而给攻击者获取快照中数据的机会。

13.1.8 数据混杂（Data Comingling）

另一个问题是不同等级的数据（或虚拟机储存着不同等级的数据）可能交错混杂在同一台物理机器中。在 PCI¹³⁰条款中，我们称之为混合实施模式（Mixed-mode deployment）。我们建议组合使用虚拟局域网（VLAN），防火墙，入侵检测/入侵防护系统（IDS/IPS）来保证虚拟机隔离以支持混合实施模式。我们还推荐使用数据分类和基于策略的管理（例如，DLP 数据泄露保护）来预防数据混杂。在云计算环境中，某一最低安全保护的租户，其安全性可能成为多租户虚拟环境中所有租户共有的安全性。

13.1.9 虚拟机数据清除

当虚拟机从一个物理服务器间迁移至另一物理服务器时，企业需要确保没有任何一个比特数据遗留在磁盘上，有关数据可能被其他用户恢复或当磁盘被回收时恢复。对内存/存储清零或者对全部数据加密是此问题的解决方案。加密密钥应当存储在虚拟环境以外的一个基于策略的密钥服务器上。此外，如果没有使用加密或恰当的数据擦洗，虚拟机在运行的状态下迁移，自身可能面临风险。

13.1.10 虚拟机镜像篡改

预先配置的虚拟设备和镜像，在你启动之前可能配置不当或被篡改过。

13.1.11 可迁移的虚拟机

虚拟机可以从一个物理服务器迁移到另外一个物理服务器的独特能力为审计和安全监测增加了复杂度。在很多情况下，虚拟机可以在不产生告警或者审计跟踪（audit trail）的情况下被重新安置于另一个物理服务器（与地理位置无关）。

13.2 建议

- 如果有的话，用户应该确认云平台供应商使用的虚拟化类型
- 实施者应该考虑通过分区的方式将生产环境与测试/开发以及高度敏感数据/业务分离
- 由于性能差异很大，实施者在测试和安装虚拟机安全工具时应该考虑性能问题。考虑具有虚拟化感知能力的服务器和网络安全工具也同样重要

¹³⁰ PCI: Payment Card Industry，这里指 PCI-DSS，支付卡行业数据安全标准

- 在虚拟化的环境中用户应该与主要的供应商评估、协商并且完善许可协议
- 通过在每个访客实例中采用硬化软件或者具有基于 Hypervisor 的 API 的内嵌虚拟机，实施者应该保障每个虚拟化的操作系统的安全
- 虚拟化的操作系统应该附加内置的安全措施，充分利用第三方安全技术实现分层的安全控制，减少对平台供应商的单纯依赖
- 实施者应该确保在默认配置下安全措施达到或者超过现行业界基准水平
- 实施者应该对不在使用中的虚拟机镜像进行加密
- 通过在分离的物理硬件诸如服务器，存储等设备上标识数据的应用（比如桌面 vs.服务器），生产阶段（比如研发，生产，以及测试）和敏感度，实施者应该探寻对虚拟机的隔离和建立安全区的效果和可行性
- 实施者应该确保安全漏洞评估工具和服务能覆盖到所采用的虚拟化技术
- 实施者应该考虑在整个组织内采用数据自动发现和标签方案（比如 DLP 数据泄露保护），以此增加虚拟机和环境间的数据分类和控制
- 实施者应该考虑对非工作状态的虚拟机镜像进行补丁操作或者对刚刚运行的虚拟机采取其它保护措施，直到他们被打上补丁
- 实施者应该明白在虚拟机的外部采用何种合适的安全控制来保护面向用户的管理接口（例如基于 web 或 API 的）

13.3 要求

- ✓ 必须采用内嵌于 Hypervisor API 的虚拟机特定安全机制对虚拟机背板间的流量进行细粒度监控，（这些流量）对于传统的网络安全控制是不可见的。
- ✓ 为了应对虚拟化带来的新的安全挑战，实施者必须更新安全策略。
- ✓ 实施者必须通过基于策略的密钥服务器对虚拟机访问的数据进行加密，存储密钥的服务器与虚拟机和数据隔离。
- ✓ 用户必须意识到虚拟机处于多租户环境下，监管可能要求保证虚拟机的隔离。
- ✓ 用户必须验证来自任意第三方的虚拟机镜像或者模板的来源和完整性，或者更好的话建立自己的虚拟机实例。
- ✓ 虚拟化的操作系统必须包含防火墙（入口/出口）、主机入侵防御系统（HIPS）、网络入侵防御系统（NIPS）、web 应用保护、防病毒、文件完整性检测以及日志检测等。安全对策可以通过每个访客虚拟机实例或者具有基于 Hypervisor 的 API 的内嵌虚拟机中的软件来传递。
- ✓ 提供商删除虚拟机镜像时必须清空所有的备份和失效备援（failover）系统

- ✓ 提供商必须具备报告机制。如果有隔离被突破时，报告机制可以提供隔离的证据并发出告警。

D14: 安全即服务 SecaaS

云计算是行业所经历过的信息技术最为重大的变化之一。将计算做到像一种公用设施一样提供功能，这具有巨大的潜力和前途广阔的创新意义。其中一项创新就是安全资源的集中化。安全行业已经意识到一个标准化的安全框架可以为服务提供者 and 使用者带来的好处。在提供者与使用者之间所定义的云的 SLA 中，标准化的安全框架以一份说明提供哪些、以及如何并在何处提供安全服务的文档的形式体现。随着基于标准框架的安全服务产品的成熟，云服务使用者已经认识到提供者和使用者将计算资源加以集中的需要。云作为业务运营平台的成熟度的里程碑之一就是在全世界范围内安全即服务(SecaaS)的应用以及对于安全如何能够由此得到增强的认知。在世界范围内将安全作为一种外包的商品加以实现，将最终使得不同差异和安全缺失最小化。

SecaaS 是从云的角度出发来考虑企业安全，这使之有别于大多数其它有关云安全的工作和研究。云安全的讨论主要集中在如何迁移到云平台，如何在使用云时维持机密性、完整性、可用性和地理位置。SecaaS 则从另一角度着眼，通过基于云的服务来保护云中的、传统企业网络中的、以及两者混合环境中的系统和数据。这些 SecaaS 的系统可能在云中、也可能以传统的方式托管在客户的场所内。托管的垃圾邮件和病毒过滤就是 SecaaS 的一个例子。

概述 本领域将讨论以下主题：

- 市场上 SecaaS 的普遍性
- 实现 SecaaS 时的顾虑
- 实现 SecaaS 的优势
- 可归类为 SecaaS 的多种服务

该文档对应于 SecaaS(安全即服务)以及 CSA CCM(云安全控制矩阵) 相关发布

14.1 SecaaS 的普遍性

客户对于云计算的前景既兴奋又不安。使他们兴奋的是云计算将带来降低资本支出的机遇、带来摆脱基础设施管理而专注于核心竞争力的机会。尤其是为计算资源的按需供应所带来的敏捷性、以及可获得的更快速的将信息技术与业务战略和需求对齐的能力而感到兴奋。然而客户同时也为云计算的安全风险以及失去对他们所负责系统的安全的直接控制而感到非常担心。供应商已经尝试通过在云平台中提供安全服务来满足这一对于安全的需求，但是因为这些服务采取了太多样的形式，并且就已部署的安全控制而言缺乏透明度，因此导致了市场的混乱，并使选择过程也变得复杂。这些因素使得迄今为止基于云的安全服务仅获得了有限的采用。SecaaS 正在经历一次指数式的增长，Gartner 预测到 2013 年在很多细分市场中，基于云的安全服务的使用将增长三倍以上。

为数众多的安全供应商正在利用云的模式来交付安全解决方案。这一变化的发生有多种原因，包括更大的规模效益、流水线化的交付机制。使用者越来越多的面临着对那些未运行在自身场所内的安全解决方案进行评估的情况。使用者需要理解基于云交付的安全产品所具有的独特的、多样的、普遍的特性，从而可以对产品进行评价，并了解它们是否能够满足自己的需求。

14.2 实现 SecaaS 的顾虑

尽管云安全服务带来了诸如动态扩展能力、虚拟化的无限资源、以及与较低或零拥有成本同时存在的更大的规模效益等让人印象深刻的大量好处，人们对于云计算环境的安全仍有很多顾虑。一些安全顾虑与合规、多租户、以及被供应商锁定相关。尽管这些都被引用为将安全迁移到云中的阻碍因素，其实相同的顾虑在传统数据中心中同样存在。

对于云环境的安全考虑通常基于两种顾虑，一种顾虑是缺乏对已经实施了的安全控制的可见性意味着系统不能像在传统数据中心中那样封闭，以及人员缺少足够的可信度和背景调查。SecaaS 供应商意识到了关系的脆弱性，并往往在确保他们的环境尽可能封闭这一点上无所不用其极。他们经常对他们的人员进行背景调查，这些调查甚至可以与最为严格的政府人员背景审查相匹敌，而且他们频繁进行。物理和人员安全是 SecaaS 供应商的首要事项之一。

考虑到全球的监管环境，法律合规也成为用户的顾虑之一。SecaaS 的供应商也意识到了这一点，并且已经做了非常大的努力，来证明他们的能力不仅能够满足而且能够超出这些合规的需求，或者是确保能够集成到客户的网络中去。SecaaS 供应商应能够认识到能影响其服务和消费者的那些地理和区域性的法律规定，并能将之内置到产品和服务实现中。最为审慎的 SecaaS 供应商经常借助仲裁和法律服务的帮助，先发制人的以某一司法管辖权内的区域性法律规定要求来解决使用者的监管需求。当在一个受到严格监管的行业或环境中部署 SecaaS 时，用以定义达成监管目标所需服务水平的度量指标体系的有关协议，应与定义服务的 SLA 文档同时进行协商。

就任何云服务而言，多租户模式引出了有关虚拟实例间数据泄漏的顾虑。当客户为此而担心的时候，SecaaS 的供应商也鉴于现代商业所具有的诉讼性质而对此高度关切。由此而带来的结果是一个成熟产品可能会采取大量的预防措施来确保数据高度隔离，确保任何共享的数据是匿名化的以保护用户身份和数据源。这一切同样适用于由 SecaaS 供应商所监控的数据，以及由他们所保留的来自于其所监控的客户系统（包含云和非云部分）的数据，譬如日志和审计数据。

另一应对多租户环境诉讼特性的办法是增强与语义处理（semantic processing）相结合的分析。资源描述符、应用法学（legal reasoning）、将法律推理解释为高层级概念并以机器可读格式表示的过程，可以主动的加以应用以消除与共享资源相关的任何法律上的歧义性。

当一个企业使用了 SecaaS 的供应商时，会将若干、很多或者全部安全日志记录、合规和报表置于某个供应商的监护之下，而后者有时可能会使用自己专用的标准。如果该企业寻求新的供应商，他们必定关心如何进行有序转换，并设法找到能够以一种保持法律有效性的方式将现有数据和日志文件进行正确翻译的方法。

需要注意的一点是，除了多租户这一项之外，上面所提到的这些顾虑都不是云所独有的，而是内部模式和外包模式下都同样面临的问题。因此，需要非专有性的、统一的安全控制，如云安全联盟云控制矩阵（Cloud Control Matrix）所提出的控制，来帮助企业和供应商从 SecaaS 的环境中受益。

14.3 实现 SecaaS 的优势

那些见证到日常效率增加的技术专家能够更好的认识到利用集中的安全服务在战略层面所具有的潜在优势。正如云计算同时为提供者和使用者提供了诸多好处一样，云 SecaaS 也带来了许多显著的收益，这些收益源自若干因素。举几个来说，如知识的聚集、广泛的可用的智能情报、以及随时可供使用的一整套安全专业人员。积极

参与到安全最佳实践集中化和标准化的那些公司，通常都会因为效益的提高而获得显著的中长期的成本节省，以及超越市场中其他对手的竞争优势。安全以服务形式交付使得安全服务的用户能够以单一的标准来度量每一供应商，从而更好的了解他们所获得的究竟是什么。

14.3.1 竞争优势

使用第三方安全服务供应商的公司会比他们的同行更具竞争优势，因为他们可以更早的获取到信息来帮助他们认识到给定 IT 战略下的风险对策。此外，通过使用集中的安全基础设施，服务消费者可以更好地阻止不良内容的进入。公司利用第三方来报告法规合规状况、度量义务断言（继承下来的与身份和数据相联系的法律和合同义务），可能使其能够避免他们的竞争者所易于遭受的那些代价高昂的诉讼和处罚。一旦整体的安全服务得以采用和实现，供应商将因为能够保证他们的客户满足安全最佳实践而获得竞争上的优势。使用这些服务的客户则可以将其合规框架的一部分指向安全供应商，并通过指向第三方保证服务供应商来提供证明其自身达成 SLA 义务的证据。

14.3.2 改善供应商客户关系

SecaaS 能带来很多明显的好处。第三方保证的服务所具有的透明度使得客户能够确切地理解他们所获得的是什么，并易于对供应商服务进行比较，同时使供应商遵守清晰、一致的服务标准。迁移服务使企业能够将数据和服务从一家供应商迁移到另一家。利用迁移服务，服务使用者和提供者都能够更好的对他们的第三级供应商施加市场压力，增加使用这些服务的企业自身的价值，并保护其供应链的安全。

14.4 现有 SecaaS 产品的多样性

SecaaS 不仅仅只是安全管理的一种外包模式，它还是保护业务弹性和连续性的一个基本组件。作为业务弹性的一种控制，SecaaS 提供了很多好处。由于通过云所交付服务的可灵活伸缩模式，客户只需按需付费，例如按照受保护的工作站数目来付费，而非为支撑各种安全服务的支持性基础设施和人员付费。一个专注于安全的服务提供商在安全专业技能方面，通常也比一个组织内部能找到的资源更具专业性。最后，将日志管理等管理性任务外包，能够节省时间和金钱，可以让企业在自己的核心竞争力上投入更多资源。

Gartner 预测，针对消息通信类应用的基于云的安全控制，例如恶意软件防护和垃圾邮件防护，到 2013 年将产生该行业领域中 60% 的销售收入。

用户和安全专业人员最有可能感兴趣的基于云的 SecaaS 的领域有：

- 身份服务和访问管理服务
- 数据泄漏保护(DLP)
- Web 安全
- Email 安全
- 安全评估
- 入侵管理、检测和防护(IDS/IPS)
- 安全信息和事件管理

- 加密
- 业务连续性和灾难恢复
- 网络安全

14.4.1 身份、授权和访问管理服务

身份管理即服务（Identity-as-a-service）是一个通用的名称，包含一个或者多个组成身份管理生态系统的服务，例如策略执行点即服务（PEP-as-a-service）、策略决策点即服务（PDP-as-a-service）、策略访问点即服务（PAP-as-a-service）、向实体提供身份的服务、提供身份属性的服务、以及提供身份信誉的服务。

所有这些身份服务可以作为一个单一的独立服务来提供，也可以以多个供应商服务的一种混合搭配来提供，或者，在如今，更有可能是以一个由公有云、私有云、传统的 IAM 和基于云的服务混合构成的方案来提供。

这些身份服务应该提供对于身份、访问和权限管理的控制。身份服务需要包含用来管理企业资源访问的人员、流程和系统等要素，它们帮助确保每一实体的身份都经过核实、并且对这些有保证的身份授予正确的访问级别。对于访问行为的审计日志，比如成功或者失败的验证、访问尝试等，应由应用/解决方案本身或者 SIEM 服务进行管理。身份、授权和访问管理服务属于保护和预防类（Protective and Preventative）技术控制。

14.4.2 数据泄漏防护

数据泄漏保护（DLP）服务通常在桌面/服务器上以客户端形式运行，执行对特定数据内容操作授权的策略，对云中和本地系统中静态的数据、传输中的数据以及使用中的数据进行监控、保护以及所受保护的展示。有别于诸如“不能 FTP”或者“不能上传到网站”这样宽泛的规则，数据泄漏防护能够理解数据，例如用户可以定义“包含类似信用卡号码的文档不能邮件外发”、“任何存储到 USB 介质的数据自动进行加密并且只能由其他正确安装 DLP 客户端的办公机器解密”、“只有安装了 DLP 软件且工作正常的机器可以打开来自文件服务器的文件”。在云中，DLP 服务可以作为标准 Build 的一个组成部分来提供，这样所有为某一客户构造的服务器都可以预先安装 DLP 软件并预置一套已约定的规则。另外，DLP 可以利用集中的 ID 或者云的中介来增强使用场景的控制。利用一项服务来监控和控制数据从企业流向云服务供应链不同层级的能力，可以作为对监管数据（如 PII¹³¹）跨平台传输、后续损失的一种预防类控制。DLP 属于预防类技术控制。

14.4.3 Web 安全

Web 安全是指某种实时保护，或者通过本地安装的软件/应用提供，或者通过使用代理或重定向技术将流量导向云提供商而通过云提供。这在其他的保护措施之上（例如防恶意程序软件）提供了一层额外保护，可以防止恶意程序随着诸如 Web 浏览之类的活动进入到企业内部。通过这种技术还可以执行那些围绕 Web 访问类型和允许访问时间窗口的策略规则。应用授权管理可以用来为 Web 应用提供更进一步的细粒度和感知上下文的安全控制。Web 安全属于保护类、检测类（detective）和响应类（reactive）的技术控制。

14.4.4 Email 安全

¹³¹ PII-Personally Identifiable Information, 个人可识别信息

Email 安全应该提供对于进站和出站邮件的控制，保护企业免受钓鱼链接、恶意附件的威胁，执行企业策略，比如合理使用规则、垃圾邮件防护，并且提供业务连续性方面的可选项。另外，**Email** 安全方案应该提供基于策略的邮件加密功能，并能与各种邮件服务器整合。数字签名提供的身份识别和不可抵赖也是许多邮件安全方案提供的功能。**Email** 安全属于保护类、检测类和响应类的技术控制。

14.4.5 安全评估

安全评估是指对于云服务的第三方或客户驱动的审计，或是通过云提供的基于业界标准的方案对客户本地系统的评估。对于基础设施、应用的传统安全评估以及合规审计，业界已有完备的定义和多个标准的支持，如 NIST¹³²、ISO¹³³、CIS¹³⁴。安全评估具备相对成熟的工具集，一些工具已通过 SecaaS 的交付模式实现。在 SecaaS 交付模式下，服务订户可以获得云计算变体的典型好处 - 弹性扩展、几乎忽略不计的安装部署时间、较低的管理开销、按使用付费以及较少的初始投资。

使用这些工具审计云计算环境带来了额外的挑战，虽然这不是这些工具原本关注的焦点。包括 CSA 在内的多个组织，已经在致力于一些指南定义方面的工作来帮助组织理解这些额外的挑战：

- 工具的虚拟化感知能力，IaaS 平台审计常常需要
- 对于 PaaS 应用中常见 Web 框架的支持
- 对 IaaS、PaaS 和 SaaS 平台的合规控制
- 自动化的事件和违规通知工具，以此来维护云供应链的整体性
- 为 XaaS 环境提供标准化的调查问卷，用以帮助了解：
 - 云环境中应该测试什么？
 - 多租户环境中如何确保数据隔离？
 - 在典型的基础设施漏洞报告中哪些需要呈现？
 - 能否接受使用云服务商提供的结果？

14.4.6 入侵检测 / 防护 (IDS/IPS)

IDS/IPS 使用基于规则的、或启发式的、或者行为模型来监控网络行为模式，检测对企业存在风险的异常活动。由于网络 IDS/IPS 能够提供企业网络内所发生事件的细粒度视图，因此在过去十年得到了广泛使用。IDS/IPS 监控网络流量，通过基于规则的引擎或者统计分析将行为与基线进行比较。IDS 一般部署为被动模式，对客户的敏感网段进行被动的检测；IPS 则扮演主动的角色来保护客户的网络。在传统的基础架构中，这些网段可以包括由防火墙或者路由器分隔的、放置公司 Web 服务器的 DMZ 区（非军事区），或者监控到内部数据库服务器的连接。在云环境中，IDS 通常专注于虚拟基础设施和跨越 Hypervisor 的活动，因为在这里构造的攻击能够影响多个租户并导致系统混乱。IDS 是检测类的技术控制，而 IPS 则是检测类、保护类和响应类的技术控制。

¹³² NIST: National Institute of Standards and Technology, 美国标准技术研究所, 官方网址在 www.nist.gov

¹³³ ISO: International Organization for Standardization, 国际标准组织, 官方网址在 www.iso.org

¹³⁴ CIS: Center for Internet Security, 互联网安全中心, 官方网址在 www.cisecurity.org

14.4.7 安全信息和事件管理 (SIEM)

安全信息和事件管理 (SIEM) 系统归集 (通过推动或拉引机制) 日志和事件数据, 这些数据来自于虚拟或者物理的网络、应用和系统。通过对这些信息进行关联和分析, 来对需要进行干预或作出其它类型响应的信息或事件提供实时的报告和告警。这些日志通常以防篡改的方式进行收集和归档, 以在事后调查时作为证据使用或者用以生成历史报告。SIEM SecaaS 产品属于检测类的技术控制, 但是也可通过配置而成为防护类和响应类技术控制。

14.4.8 加密

加密是使用加密算法对数据进行模糊处理 / 编码的过程, 输出的是加密数据 (称为密文)。只有预期的接收者或系统才拥有正确的密钥, 能够对密文进行解码 (解密)。模糊处理系统的加密功能通常包含在计算上难以 (或不能) 被破解的一个或多个算法、一个或多个密钥、以及管理加密、解密和密钥的系统、流程和程序 (processes and procedures)。每一部分都缺一不可, 如果流程不严谨导致攻击者可以得到密钥, 即使最好的加密算法也能轻易破解。

在单向加密的情况下, 生成的是摘要或哈希值。单向加密包括哈希散列、数字签名、证书生成和更新、以及密钥交换。这些系统通常由一个或多个容易复制但很难伪造的算法、以及相关的管理流程和程序构成。由 SaaS 提供者提供的加密服务归入保护和检测类技术控制。

14.4.9 业务连续性和灾难恢复

业务连续性和灾难恢复是为了确保在任何服务中断发生时保证运营弹性而设计和实施的措施。无论是自然的还是人为的服务中断事件, 这些措施都提供了灵活可靠的故障转移 (failover) 和灾难恢复方案。例如, 在一个地点发生了灾难, 在另外一个地点的主机可以保护前述地点中应用的运行。这种类型的 SecaaS 产品是一种响应类、保护类和检测类的技术控制。

14.4.10 网络安全

网络安全包含限制或者分配访问的安全服务, 以及分发、监控、记录和保护底层资源服务的安全服务。

从架构上来讲, 网络安全提供的服务致力于集中的网络上的安全控制, 或者每一底层资源单个网络的特别的安全控制。在云 / 虚拟环境或者混合环境中, 网络安全可能由虚拟设备和传统的物理设备一起提供。与 Hypervisor (虚拟机管理程序) 紧密集成, 确保虚拟网络层流量的可视化, 这是网络安全服务的关键。网络 SecaaS 产品是检测类、保护类和响应类的技术控制。

14.5 许可

- 实施者可以采用用户行为模式识别技术。
- 实施者可以为进行 SLA¹³⁵期望值管理而对安全度量体系采用法律仲裁。

¹³⁵ SLA-Service Level Agreement

- 实施者可以为进行渗透测试而使用可信通道。

14.6 建议

- 实施方应该确保租户与服务使用者之间安全的通信通道。
- 提供者应该在须知原则基础之上，在整个供应链上提供自动化的、安全和持续的通知功能。
- 提供这应该为 SLA 合规提供内部操作的可靠的日志记录。
- 服务使用者应该要求附加第三方审计和 SLA 仲裁服务。
- 各方应通过标准化的安全接口，如 SCAP(NIST)、CYBEX(ITU-T)或者 RDI&IODEF(IETF)，来对所有接口启用持续监控。

14.7 要求

14.7.1 身份管理即服务需求

- ✓ 身份管理即服务提供者必须向客户提供帐户的开通/取消（云上的与内部的应用和资源）。
- ✓ 身份管理即服务提供者必须向客户提供认证服务（多种形式和多因子）。
- ✓ 身份管理即服务提供者必须向客户提供身份生命周期管理。
- ✓ 身份管理即服务提供者必须向客户提供目录服务。
- ✓ 身份管理即服务提供者必须向客户提供目录同步服务（需要的情况下提供多边同步）。
- ✓ 身份管理即服务提供者必须向客户提供联邦的单点登录(SSO)。
- ✓ 身份管理即服务提供者必须向客户提供 Web 单点登录(SSO)（细粒度的访问控制执行和会话管理 - 区别于 SSO 联邦）。
- ✓ 身份管理即服务提供者必须提供保密会话的监控。
- ✓ 身份管理即服务提供者必须提供细粒度的访问管理。
- ✓ 身份管理即服务提供者必须提供防篡改的审计纪录存储（包括不可否认性的选项）。
- ✓ 身份管理即服务提供者必须提供策略管理（包括授权管理、角色管理、合规策略管理）。
- ✓ 身份管理即服务提供者必须向客户提供授权管理（用户和应用/系统）。
- ✓ 身份管理即服务提供者必须向客户提供授权令牌管理和开通服务。
- ✓ 身份管理即服务提供者必须向客户提供用户配置和权限管理（用户和应用/系统）。

- ✓ 身份管理即服务提供者必须向客户提供策略和法规遵从监控与/或汇总报告支持。
- ✓ 身份管理即服务提供者必须向客户提供云应用的联邦开通服务（federated provisioning）。
- ✓ 身份管理即服务提供者必须提供权限用户和口令的管理（包括管理的、共享的、系统的和应用的帐户）。
- ✓ 身份管理即服务提供者必须向客户提供基于角色的访问控制(RBAC)(同时其下的系统/服务需要支持)。
- ✓ 身份管理即服务提供者必须向客户提供可选的数据泄露保护（DLP）集成支持。
- ✓ 身份管理即服务提供者必须向客户提供可选的细粒度分解到个体行为审计的支持。
- ✓ 身份管理即服务提供者必须向客户提供基于身份权限的责任划分。
- ✓ 身份管理即服务提供者必须向客户提供围绕合规的汇总报告。
- ✓ 身份管理即服务提供者必须向客户提供集中的策略管理。
- ✓ 身份管理即服务提供者必须向客户提供可用的管理界面。
- ✓ 身份管理即服务提供者必须向客户提供统一的访问控制和审计。
- ✓ 身份管理即服务提供者必须向客户提供不同提供者之间的互操作性和异构兼容性。
- ✓ 身份管理即服务提供者必须向客户提供可扩展性。

14.7.2 数据泄露保护（DLP）SecaaS 需求

- ✓ “DLP 即服务”提供者必须向客户提供数据分级和标记。
- ✓ “DLP 即服务”提供者必须向客户提供敏感数据识别。
- ✓ “DLP 即服务”提供者必须向客户提供重要法规遵从预定义的策略。
- ✓ “DLP 即服务”提供者必须向客户提供情景检测启发功能。
- ✓ “DLP 即服务”提供者必须向客户提供结构化数据的匹配功能（静态数据）。
- ✓ “DLP 即服务”提供者必须向客户提供 SQL 正则表达式的检测。
- ✓ “DLP 即服务”提供者必须向客户提供流量跨度（动态传输中的数据）检测。
- ✓ “DLP 即服务”提供者必须向客户提供实时用户感知功能（Real Time User Awareness）。
- ✓ “DLP 即服务”提供者必须向客户提供安全级别指派。
- ✓ “DLP 即服务”提供者必须向客户提供自定义属性查询。
- ✓ “DLP 即服务”提供者必须向客户提供自动化的事件响应。

- ✓ “DLP 即服务”提供者必须向客户提供数据签名。
- ✓ “DLP 即服务”提供者必须向客户提供加密数据保护和访问控制。
- ✓ “DLP 即服务”提供者必须向客户提供机器可读的策略定义语言。

14.7.3 Web 服务 SecaaS 需求

- ✓ Web 服务 SecaaS 提供者必须向客户提供 Web 监控和过滤。
- ✓ Web 服务 SecaaS 提供者必须向客户提供恶意软件、间谍软件和僵尸网络的分析和屏蔽。
- ✓ Web 服务 SecaaS 提供者必须向客户提供钓鱼网站屏蔽。
- ✓ Web 服务 SecaaS 提供者必须向客户提供即时通信扫描。
- ✓ Web 服务 SecaaS 提供者必须向客户提供邮件安全。
- ✓ Web 服务 SecaaS 提供者必须向客户提供带宽管理和流量控制。
- ✓ Web 服务 SecaaS 提供者必须向客户提供 DLP。
- ✓ Web 服务 SecaaS 提供者必须向客户提供防欺诈功能。
- ✓ Web 服务 SecaaS 提供者必须向客户提供 Web 访问控制。
- ✓ Web 服务 SecaaS 提供者必须向客户提供备份服务。
- ✓ Web 服务 SecaaS 提供者必须向客户提供 SSL（解密/交接(hand off)）。
- ✓ Web 服务 SecaaS 提供者必须向客户提供使用策略强制执行。
- ✓ Web 服务 SecaaS 提供者必须向客户提供安全漏洞管理。
- ✓ Web 服务 SecaaS 提供者必须向客户提供 Web 智能报表服务。

14.7.4 Email SecaaS 需求

- ✓ Email SecaaS 提供者必须向客户提供精准的用以屏蔽垃圾和钓鱼邮件的过滤功能。
- ✓ Email SecaaS 提供者必须向客户提供病毒和间谍软件的深度防护以阻止其进入企业边界。
- ✓ Email SecaaS 提供者必须向客户提供灵活的策略以制定细粒度的邮件流转和加密。
- ✓ Email SecaaS 提供者必须向客户提供丰富的交互式的报告和实时关联性报告。
- ✓ Email SecaaS 提供者必须向客户提供深度内容扫描以实施策略。
- ✓ Email SecaaS 提供者必须向客户提供基于策略部分或者全部加密邮件的选项。

- ✓ Email SecaaS 提供者必须向客户提供与不同邮件服务器解决方案集成的能力。

14.7.5 安全评估 SecaaS 需求

- ✓ 安全评估 SecaaS 的提供者必须向客户提供详尽的治理流程和度量说明（实施者应定义并以文档记录设定策略和执行决策的流程）。
- ✓ 安全评估与治理产品的提供者应实现一套自动化的解决方案，以在发生破坏或安全事件时能够通知其直接供应链的成员。
- ✓ 安全评估 SecaaS 的提供者必须向客户提供适当的风险管理（实施者应定义并以文档记录流程，以确保重要的业务流程和行为保持在相关策略和决策的容许度内）。
- ✓ 安全评估 SecaaS 的提供者必须向客户提供合规的细节（实施者应定义并以文档记录对策略和决策的遵从流程）。
- ✓ 安全评估 SecaaS 的提供者必须向客户提供可从内部的指引、程序、需求或者外部的法律、法规、标准和协议中推论出的策略。
- ✓ 安全评估 SecaaS 的提供者必须向客户提供技术上的合规审计（对设备、操作系统、数据库和应用的配置设置进行自动化的审计）。
- ✓ 安全评估 SecaaS 的提供者必须向客户提供应用安全评估服务（对于客户化应用自动化的审计）。
- ✓ 安全评估与治理服务产品的提供者必须向云的客户提供脆弱性评估服务-通过对网络设备、计算机和应用进行自动化的检测来发现已知脆弱点和配置问题。
- ✓ 安全评估 SecaaS 的提供者必须向客户提供渗透测试服务（利用弱点和配置问题获得对于某一环境、网络或计算机的访问，通常需要人工辅助）
- ✓ 安全评估 SecaaS 的提供者必须向客户提供安全评级。

14.7.6 入侵检测 SecaaS 需求

- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于入侵和策略违规的识别。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于入侵的自动化或手工的补救。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于负载和虚拟层管理平面（VMM/Hypervisor）的覆盖。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供基于统计分析、行为分析、特征字、启发式中一项或多项技术的深度包检测（DPI）。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于系统调用的监控。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供系统/应用日志的检测。

- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于操作系统完整性的监控（文件、注册项、端口、进程、已安装软件等）。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于 VMM/Hypervisor 完整性的监控。
- ✓ 入侵检测 SecaaS 的提供者必须向客户提供对于 VM 镜像库的监控。
- ✓ Providers of Intrusion Detection SecaaS must provide cloud customers with VM Image Repository Monitoring.

14.7.7 SIEM SecaaS 需求

- ✓ SIEM SecaaS 提供者必须向客户提供实时的日志/事件收集、去重、规范化、归集与可视化。
- ✓ SIEM SecaaS 提供者必须向客户提供电子取证支持。
- ✓ SIEM SecaaS 提供者必须向客户提供合规报告和支持。
- ✓ SIEM SecaaS 提供者必须向客户提供 IR（事件响应）支持。
- ✓ SIEM SecaaS 提供者必须向客户提供不限于电子邮件的异常检测。
- ✓ SIEM SecaaS 提供者必须向客户提供详细的报告。
- ✓ SIEM SecaaS 提供者必须向客户提供灵活的策略管理和数据保留时间设置。

14.7.8 加密 SecaaS 需求

- ✓ 加密 SecaaS 提供者必须向客户提供对于传输中数据的保护。
- ✓ 加密 SecaaS 提供者必须向客户提供对于静态数据的保护。
- ✓ 加密 SecaaS 提供者必须向客户提供加密密钥与策略管理。
- ✓ 网络安全 SecaaS 提供者必须向客户提供对于缓存数据的保护。

14.7.9 业务连续性与灾难恢复 SecaaS 需求

- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供灵活的基础设施。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供安全的备份。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供受监控的操作。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供与第三方服务的互联性（connectivity）。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供复制的基础设施组件。

- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供复制的数据（核心/关键系统）。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供对于数据和/或应用的恢复。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供操作的备用地点。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供测试过的标准的流程和操作以确保操作的弹性。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供地理上分布开的数据中心/基础设施。
- ✓ 业务连续性与灾难恢复 SecaaS 提供者必须向客户提供网络的可存活性。

14.7.10 网络安全 SecaaS 需求

- ✓ 网络安全 SecaaS 提供者必须向客户提供数据所面临威胁的细节。
- ✓ 网络安全 SecaaS 提供者必须向客户提供访问控制所面临威胁的细节。
- ✓ 网络安全 SecaaS 提供者必须向客户提供访问和认证控制。
- ✓ 网络安全 SecaaS 提供者必须向客户提供安全网关（防火墙、WAF、SOA/API）。
- ✓ 网络安全 SecaaS 提供者必须向客户提供安全产品（IDS/IPS、服务器层防火墙、文件完整性监控、DLP、防病毒、防垃圾邮件）。
- ✓ 网络安全 SecaaS 提供者必须向客户提供安全监控和事件响应。
- ✓ 网络安全 SecaaS 提供者必须向客户提供 DoS 防护/缓解。
- ✓ 网络安全 SecaaS 提供者必须向客户提供安全的基础服务，如 DNSSEC、NTP、OAuth、SNMP、管理网络分区和安全。
- ✓ 网络安全 SecaaS 提供者必须向客户提供流量监控。
- ✓ 网络安全 SecaaS 提供者必须向客户提供与 Hypervisor 层的集成。

参考文献

- [1] Security and Economic Benefits of Standardization for Security as a Service. September 2011 Proceedings. United Nations ITU-T.
- [2] Gartner. Gartner Says Security Delivered as a Cloud-Based Service Will More Than Triple in Many Segments by 2013. July 15, 2008. <http://www.gartner.com/it/page.jsp?id=722307>
- [3] Cloud Security Alliance. Defined Categories of Service 2011. https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf