

ICS 33.040

M 10

YD

中华人民共和国通信行业标准

YD/T 3148-2016

云计算安全框架

Security framework for cloud computing

(ITU-T X.1601, Security framework for cloud computing, IDT)

2016-07-11 发布

2016-10-01 实施

中华人民共和国工业和信息化部 发布



目 次

前 言.....II

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

4 概述.....5

5 云计算的安全威胁.....5

6 云计算的安全挑战.....7

7 云计算的安全能力.....10

8 框架方法.....14

附录A（资料性附录）与云计算安全威胁和挑战相对应的安全能力.....16

参考文献.....20

前 言

本标准使用翻译法等同采用ITU-T X.1601《云计算的安全框架》。

本标准按照GB/T 1.1-2009给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中国信息通信研究院。

本标准主要起草人：张彦超、谢 玮、魏 薇。

云计算安全框架

1 范围

本标准分析云计算环境中，云服务客户、云服务提供商、云服务伙伴面临的安全威胁和挑战，并阐明可减缓这些风险和应对安全挑战的安全能力。本标准提供的框架方法适用于在减缓云计算安全威胁和应对安全挑战时，应对安全能力做出的具体规范。

2 规范性引用文件

无。

3 术语、定义和缩略语

3.1 本标准定义的术语

下列术语和定义适用于本文件。

3.1.1

云计算 Cloud Computing

有助于网络以按需自助方式调配和管理获取一系列可伸缩和富有弹性的、可共享的物理或虚拟资源的范式。

3.1.2

云服务 Cloud Service

通过云计算实现的一种或多种能力，通过使用声明接口启动。

3.1.3

云服务客户 Cloud Service Customer

使用云服务的具体业务关系的一方。

3.1.4

云服务伙伴 Cloud Service Partner

支持或辅助云服务提供商或云服务客户活动的合作伙伴。

3.1.5

云服务提供商 Cloud Service Provider

提供云服务的一方。

3.1.6

云服务用户 Cloud Service User

与使用云服务的云服务客户相关联的人。

3.1.7

通信即服务 Communications as a Service (CaaS)

一种类别的云服务，其中为云服务客户提供的能力是实时通信和协作。

注：CaaS既可提供平台能力类型，也可提供应用能力类型。

3.1.8

社区云 Community Cloud

专门支持并由一系列特定云服务客户共享的云部署模式，资源至少由上述客户中的一人控制。

注：共享要求包括但不限于任务、信息安全要求、政策和合规性方面的考虑。

3.1.9

基础设施即服务 Infrastructure as a Service (IaaS)

一种类别云服务，其中向云服务客户提供的云能力类型是一种基础设施能力类型。

注：云服务客户不管理也不控制下层物理和虚拟资源，但控制操作系统、存储和使用物理及虚拟资源得到部署的应用。云服务客户也可拥有控制特定网络成份（如主机防火墙）的有限能力。

3.1.10

多租户 Multi-Tenancy

物理和虚拟资源的分配方法能够使多租户及其计算和数据相互隔离并无法实现互访。

3.1.11

网络即服务 Network as a Service (NaaS)

一种类别云服务，其中向云服务客户提供的能力为传送连接和相关网络能力。

注：NaaS可提供三种云能力类型中的任何一种。

3.1.12

相关方 Party

自然人或组织。

3.1.13

平台即服务 Platform as a Service (PaaS)

一种类别云服务，其中向云服务客户提供的能力为传送连接和相关网络能力。

注：NaaS可提供三种云能力类型中的任何一种。

3.1.14

私有云 Private Cloud

专门由一个单一云服务客户享用的云部署模式，资源由云服务客户控制。

3.1.15

公共云 Public Cloud

可潜在地向任何云服务客户提供的云部署模式，资源由云服务提供商控制。

3.1.16

安全挑战 Security Challenge

一种源自自然或云服务操作环境的安全“困难”（包括“间接”威胁），而非直接安全威胁。

3.1.17

软件即服务 Software as a Service (SaaS)

一种类别云服务，其中向云服务客户提供的云能力类型为应用能力类型。

3.1.18

租户 Tenant

共享一套物理和虚拟资源接入的一组云服务用户。

注：通常且在多租户的环境中，形成一个租户的一组云服务用户将全部属于同一个云服务客户组织。有些情况下可能一组云服务用户涉及来自多个不同消费者的用户，特别是社区云的部署，但这属于特殊例外情况。然而，特定云服务客户组织可在单一云服务提供商那里拥有多个不同租户（或许代表组织中不同的业务部门（如销售与财务）），因为从业务和商业角度出发，可能有充分理由需要将属于这些不同部门的数据和活动保持分离。

3.2 他处定义的术语

本标准使用了下列他处定义的术语。

3.2.1

认证 Authentication

核实用户、程序或装置的身份，这常常是允许获取信息系统资源的前提条件[NIST-SP-800-53]。

3.2.2

能力 Capability

有能力从事特定活动的品质。[ISO/IEC 19440]

3.2.3

数据控制方 Data Controller

确定个人数据的使用目的和处理方法的人（自己或联合他人或与其他人一道进行）[key definition]。

3.2.4

数据处理方 Data Processor

在个人数据方面，这意味着代表数据控制方处理数据的任何人（而非数据控制方的雇员）[key definition]。

3.2.5

管理程序 Hypervisor

管理主机客户操作系统并控制客户操作系统与物理硬件之间指令流动的虚拟化部分[NIST-SP-800-125]。

3.2.6

个人可识别信息 Personally Identifiable Information

（a）可被用于识别相关信息与之关联的PII（个人可识别信息）主体，或（b）能被或可能被直接或间接与PII主体联系起来的任何信息[ISO/IEC 29100]。

3.2.7

安全域 Security Domain

指一套元素、安全政策、安全管理机构和一组与安全相关的活动，其中有关元素须符合相关活动的安全政策，而安全政策则受到有关安全域中安全管理机构的管理[ITU-T X.810]。

3.2.8

安全事件 Security Incident

指使安全的某个方面受到威胁的有害事件[ITU-T E.409]。

3.2.9

服务水平协议 Service Level Agreement (SLA)

服务提供商与客户之间书面记录的、明确服务和服务目标的协议。

注1：也可在服务提供商与供应商、内部集团或作为供应商行事的客户之间签定服务水平协议。

注2：可将服务水平协议纳入合同或另一种文件记录协议之中[ISO/IEC 20000-1]。

3.2.10

威胁 Threat

可能对系统或机构造成伤害的有害事件的潜在起因[ISO/IEC 27000]。

3.2.11

虚拟机器 Virtual Machine (VM)

对真实机器的高效、隔离和逻辑复制[NIST-SP-800-145]。

3.2.12

漏洞 Vulnerability

可由威胁来源加以利用的信息系统、系统安全程序、内部控制或实施中存在的弱点[NIST-SP-800-30]。

3.3 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用程序编程接口
BCP	Business Continuity Planning	业务连续性计划
CaaS	Communications as a Service	通信即服务
CPU	Central Processing Unit	中央处理器
CSC	Cloud Service Customer	云服务客户
CSN	Cloud Service Partner	云服务伙伴
CSP	Cloud Service Provider	云服务提供商
CSU	Cloud Service User	云服务用户
DNS	Domain Name System	域名系统
IaaS	Infrastructure as a Service	基础设施即服务
IAM	Identity and Access Management	身份和接入管理
ICT	Information and Communication Technology	信息通信技术
IP	Internet Protocol	互联网协议
IT	Information Technology	信息技术
NaaS	Network as a Service	网络即服务
OS	Operating System	操作系统
PaaS	Platform as a Service	平台即服务
PII	Personally Identifiable Information	个人可识别信息
PKI	Public Key Infrastructure	公钥基础设施
SaaS	Software as a Service	软件即服务
SIM	Subscriber Identity Module	用户身份模块

SLA	Service Level Agreement	服务水平协议
VM	Virtual Machine	虚拟机

4 概述

云计算是一种有助于网络方便和按需获取一系列可调配资源（如网络、服务器、存储、应用和服务）的服务，这些资源可被服务提供商管理，并迅速得到调配和释放。云计算客户可使用这些资源在任何装置、任何时间和地点以灵活和按需方式开发、托管和运行服务和应用。云计算服务通常以特定服务类别提供，如，基础设施即服务（IaaS）、平台即服务（PaaS）、软件即服务（SaaS）、网络即服务（NaaS）等。这些服务有助于云计算客户在无需建立新的信息通信技术（ICT）基础设施和系统的前提下快速和方便地出台或改变其业务，并获得了按照需要弹性调配资源的机会。例如，某些云服务提供商（CSP）可提供抽象硬件和软件资源服务（如 IaaS 或 NaaS），某些云服务提供商能提供平台服务（PaaS）或应用服务（SaaS），以方便客户和伙伴快速开发和部署并能远程配置和使用应用。

在采用云服务方面亦存在着安全威胁和挑战，且不同云计算服务部署模式和服务类别的安全要求也不同。由于云计算具有分布式和多租户性质，远程获取云计算服务司空见惯，且每一程序所涉实体众多，因此，云计算比其他范式更易受到内部和外部安全威胁的影响。可采用传统安全程序和机制缓解诸多安全威胁。安全涉及和影响到云计算服务的诸多方面，因此，对云计算服务相关的资源进行安全管理是云计算的一个至关重要的方面。

在将 ICT 系统过渡到云计算之前，潜在的云服务客户（CSC）应确定其安全威胁（见以下第 5 章）和安全挑战（见以下第 6 章）。

根据这些威胁和挑战，应明确一系列安全能力（见以下第 7 章）。有关这些能力的具体要求不属于本标准的范围，需要根据对已明确的威胁和挑战做出风险评估，提出实施具体云计算服务的相关能力要求。

在风险评估基础上，CSC 可确定是否采用云计算，并就服务提供商和架构做出知情决定。应通过采用信息安全风险管理框架（如[ISO/IEC 27005]确定的风险管理框架）进行上述风险评估。有关推荐使用的框架方法亦见以下第 8 章。

本标准对安全威胁和安全挑战做出区分。安全威胁与攻击（主动和被动）相关联，但也与环境故障或灾难有关。安全挑战是由自然或云服务操作环境产生的困难。如果安全挑战不能得到正确应对，则可能为威胁的产生打开方便之门。

本标准在这些得到确定的安全威胁和挑战基础上，描述一系列旨在减缓云计算安全威胁和应对安全挑战的安全能力。

5 云计算的安全威胁

威胁会对诸如信息、程序和系统等资产带来潜在危害，因此也会对组织造成潜在危害。威胁可源于自然，或由人为造成，可以是意外性质，也可以是故意所为。威胁可来自组织内部或外部，威胁也可被归类为意外威胁或有意威胁，以及主动或被动威胁。

所遇到的具体威胁在很大程度上取决于选定的特定云服务。例如，对于公共云而言，威胁可源自 CSC 和 CSP 之间的职责分工：对数据和程序的责任权方面的规定、数据保护的一致性和充分性以及隐私的保护等。然而，对于私有云而言，威胁则更易于解决，因为 CSC 控制着由 CSP 托管的所有租户。尽管本标准确定的一些威胁已由一些行业现有文件涵盖（如 ITU-T X.800 建议书），但所有威胁均与云计算相关。

本章阐述云计算环境中可能出现的多种不同安全威胁。

5.1 云服务客户（CSC）的安全威胁

下述威胁直接影响到CSC。这些威胁可能影响CSC的个人或企业利益、隐私、合法性或安全。并非所有CSC都将受到所有威胁的影响，CSC的性质不同以及所使用云服务的不同决定了风险不是等同的。例如，针对商业视频文档代码转换（trans-coding）的云服务并不要求保护个人可识别信息（PII），但却强烈要求保护数字资产。

5.1.1 数据丢失和泄漏

由于云服务环境通常为多租户环境，因此，数据丢失或泄漏对CSC是一项严重威胁。不能恰如其分地管理加密信息（如加密密钥）、认证代码和接入特权，可能会带来诸如数据丢失和向外界意外泄露数据的极大损害。例如，造成这一威胁的主要原因可能是认证、授权和审计控制不足、加密和/或认证密钥的使用不统一、操作失败、处理不当、数据中心的可靠性以及数据恢复情况，且这些与本标准6.1.2、6.1.3和6.1.4所述的挑战相关联。

5.1.2 不安全的服务获取

身份证书（包括CSC管理员的身份证书）在云计算环境中易于被未经授权的用户加以利用，这是因为云计算不同于传统电信环境，常常难以依赖地点（如有线网络）或特定硬件元素的存在（如，移动签约用户身份模块（SIM））来强化身份认证。由于多数服务为远程提供服务，因此，未得到保护的连接存在潜在漏洞。即使连接得到保护或为局部连接，其他攻击方式（如网上钓鱼、欺诈、社交工程和软件漏洞的利用）也可能获得成功。如果攻击方获得用户或管理员的证书，则他们可以对活动和交易进行偷听、操纵数据、返回虚假信息，并将CSC的客户机指向非法网站。密码常常被重复用于多个网站和服务，这就加大了此类攻击的影响，因为任何一种单一破坏都会使诸多服务面临风险。云计算解决方案还在此之上增加了一种新的威胁：CSC的账户或服务实例可能变成攻击者的新基地。攻击者可以此为起点，充分利用CSC的声誉和资源发起后续攻击。

5.1.3 内部威胁

只要涉及到人，就总是存在个人以与服务安全不一致的方式行事的风险。CSC雇员共用“管理员”密码、不能安全保管证书（如，将证书写在贴在屏幕上的便签上）、用户（或消费者群体中的成员）粗心大意或训练无素、心怀不满的雇员的恶意行为等始终会带来重大威胁。

5.2 云服务提供商（CSP）的安全威胁

本节明确直接影响CSP的威胁。这类威胁可能影响到CSP提供服务、开展业务、保留客户的能力。对特定CSP的威胁也取决于其提供的服务和环境。

5.2.1 未经授权的管理获取

云计算服务包括CSC员工管理由CSC掌控的云服务部分的接口和软件成份，如，增加或消除CSC雇员账户、与CSC的自身服务器进行连接，改变服务能力、更新域名系统（DNS）条目和网站等。这种管理接口可成为攻击者选定的目标，攻击者可假冒CSC管理员对CSP发起攻击。由于此类云服务必须由CSC自身员工获取，因此，保护这些服务就成了云计算安全的主要关切。

5.2.2 内部威胁

只要涉及到人，就永远存在个人以恶意或粗心大意方式行事的风险，使服务安全受到威胁。

CSP雇员共用“管理员”密码、不能安全保管证书（如将证书写在贴在屏幕上的便签上）、粗心大意或训练无素的用户、或心存不满的雇员的恶意行为始终会对任何企业都造成重大威胁。

CSP特别需要认真考虑其自身雇员的可信任性。即使对雇员进行过很好的鉴别，也总是会有技能娴熟的入侵者成功获得CSP数据中心员工的位置。这种入侵者可能企图破坏CSP本身，或打算渗透目前得到支持的特定CSC系统，尤其当CSC是高度知名的公司或管理机构时。

6 云计算的安全挑战

安全挑战包含产生于自然或云服务操作环境的困难，而非安全威胁，挑战包括“间接”威胁。间接威胁是指云服务参与者面临的可能对其他方带来有害后果的威胁。

本标准确定的挑战如不能得到适当应对，则可能为威胁打开方便之门。在考虑云计算服务时，应对这些挑战做出考虑。

6.1 云服务客户（CSC）的安全挑战

本节阐述与环境困难相关的安全挑战或间接威胁，这些可能会直接威胁CSC的利益。

6.1.1 职责分工不明确

云服务客户通过不同类别服务和部署模式消费所提供的资源，因此，客户自建的信息通信系统依赖于这些服务。在CSC与CSP之间缺乏明确职责分工可能会带来理念和操作方面的冲突。如果所提供服务的合同相互矛盾，则会导致异常现象或事件的发生。例如，在国际范围内，哪个实体是数据控制方，哪个实体是数据处理方可能并不明确。

6.1.2 丧失信任

由于云计算服务具有黑盒（black-box）特点，因此，CSC难以确定对其CSP的信任程度。如果无法以正式方式获得并认可提供商的安全水平，则CSC无法评估提供商所实施的安全水平。这种有关CSP安全水平认可的缺乏可能成为一些CSC在使用云服务方面的一项严重安全威胁。

6.1.3 丧失管理

云服务客户决定将其部分ICT系统过渡到云计算基础实施上意味着由CSP部分掌控其自身系统，这可能会对CSC的数据造成严重威胁，特别在涉及到提供商的作用和所获得的特权时。如果与此同时还不明确了解云计算提供商的做法的话，则可能会出现配置失当、甚至方便不怀好意的内部人员发起攻击的情况。

一些CSC在采用云计算服务时，可能担心失去自身对由CSP托管的信息和资产、数据存储、对数据备份的依赖（数据保留问题）、业务连续性计划（BCP）措施和灾难恢复等的控制。

例如：

- 云服务客户希望删除某一文件，但CSP却保留了CSC并不知情的副本。
- 云服务提供商赋予CSC管理员超出后者允许的特权。
- 一些CSC可能担心CSP向外国政府透露其数据。

6.1.4 丧失隐私

当CSP处理私密信息时，可能对隐私造成侵犯，从而违反了相关隐私规则或法律，其中包括泄露私密信息，或处理私密信息的目的并非为CSC和/或数据主体所授权的目的。

6.1.5 服务的不可用性

可用性并非为云计算环境独有，但由于云计算设计原理是面向服务的，因此，如果上游云计算服务不能完全得到提供，则服务提供可能受到影响。此外，由于云计算的依赖性动态变化的，因此为攻击者带来了更多的可能性。例如，对一个上游服务发起的拒绝服务攻击可能影响同一个云计算系统中的多个下游服务。

6.1.6 锁定一家云服务提供商

高度依赖单一一家CSP会使由另一家CSP取而代之更加困难。如果CSP依靠非标准功能或格式、且不提供互操作性的话，即会出现这一情况。倘若被锁定使用的CSP不能解决安全漏洞，则上述情况会变成一种安全威胁，从而使CSC在面临风险时无法迁移至另一家CSP。

6.1.7 盗用知识产权

当CSC的代码由CSP运行或其他资产由后者存储时，则存在该资料被泄露给第三方或被盗用（用于未经授权的用途）的挑战。这其中可包括侵犯版权或暴露商业秘密。

6.1.8 丧失软件完整性

一旦CSC的代码由CSP运行，则该代码可能被修改或感染，而CSC却无法对此直接掌控，从而使其软件在某种程度上行为异常。尽管这种可能性无法由CSC控制，但它却可严重影响到云服务客户的声誉和业务。

6.2 云服务提供商（CSP）的安全挑战

本节阐述可能会使CSP利益受到更多直接威胁的与环境困难相关的安全挑战或间接威胁。

6.2.1 职责分工不明确

可在云计算系统中确定不同作用（CSP、CSC以及云服务伙伴（CSN））。职责分工不明确涉及到诸如数据拥有、接入控制或基础设施维护等问题，这些会影响到业务或带来法律争端（特别是在涉及到第三方或CSP同时也是CSC或CSN时）。当CSP跨多个管辖区开展工作和/或提供服务（合同和协议可能以不同语言拟就或属于不同法律框架）时，这种职责分工不明确的风险进一步加大。亦见以下有关“管辖冲突”的6.2.4。

6.2.2 共享环境

云计算在很大范围内实现大量数据共享，因此可节约成本，但这种情况也使诸多接口面临潜在风险。例如，不同CSC同时消费同一个云的服务，由此，CSC可在未得到授权时接入租户的虚拟机、网络流量、实际/剩余数据等。这种对另一家CSC资产的未经授权或恶意接入可能使完整性、可用性和保密性受到危害。

例如，多个共同托管在一个物理服务器上的虚拟机器既共享中央处理单元（CPU），也共享由管理程序（hypervisor）予以虚拟化的内存资源，由此产生的挑战涉及到管理程序隔离机制的失效，从而方便了对其他虚拟机的内存或存储器进行未经授权的访问。

6.2.3 保护机制之间的相互矛盾和冲突

由于云计算基础设施呈非集中架构，因此，其分布式安全模块之间的保护机制可能相互矛盾。例如，由一个安全模块拒绝的接入可能获得另一个模块的许可，这种相互矛盾可能为得到授权的用户带来问题，或可能由攻击者利用，从而使保密性、完整性和可用性受到危害。

6.2.4 管辖冲突

云中的数据可在数据中心之间、甚或跨国境移动。在不同托管国，数据可能受不同适用管辖区的规管，管辖冲突可能带来法律方面的复杂性。

6.2.5 演进风险

云计算的一个优点是可从系统设计阶段到实施阶段推迟某些选择，这意味着，只有当要求采用系统相关依赖软件组件的功能得到实现后才选择和实施这些成份。然而，传统的风险评估方法不再适应这种动态演进系统的需求。在设计阶段已通过安全评估的系统在其后期可能出现新的漏洞，因为软件成份发生了变化。

6.2.6 不良的过渡和集成

向云系统进行过渡往往意味着需要移动大量数据并对配置做出重大修改（如网络寻址）。将一部分ICT系统过渡到外部CSP可能要求在系统设计方面做出重大改变（如网络和安全政策）。互不兼容的接口或相互矛盾的政策执行所引起的不良集成可能会带来功能性和非功能性方面的影响。例如，在专用数据中心防火墙后运行的虚拟机器可能在CSP的云中被意外暴露给开放的互联网。

6.2.7 业务中断

云计算对资源进行分配并将其作为服务予以提供。整个云计算生态系统由多个相互依赖的部分组成，任何一个部分的中断（如断电、拒绝服务或延误）都可能影响到与6.1.5—服务的不可用性—相关的云计算的可用性，并随后导致业务中断。

6.2.8 云服务伙伴的锁定

云服务提供商的平台是利用来自多家不同供应商的软件和硬件成份构建的，一些成份可能包含对CSP有用的专用功能特性或扩展。然而，依赖这些专用功能特性限制了CSP采用另一家部件供应商服务的能力。

虽然锁定是一个业务问题，本身并非安全威胁，然而，该问题有时会带来安全方面的担忧。例如，如果提供关键部件的CSN停业，则可能无法进一步提供安全补丁。如果部件出现漏洞，则减缓该风险会异常困难或代价高昂。

6.2.9 供应链漏洞

如果通过CSP供应链提供的平台硬件或软件威胁到CSC或CSP的安全，则前者会面临风险（如意外或有意引入恶意软件或可被利用的漏洞）。

一个有说服力的例子便是CSN的不良代码。如果CSN的代码由CSP运行，如客户界面、虚拟机器（VM）、客户操作系统（OS）、应用、平台部件或审计/监测软件（如伙伴提供服务审计），则存在这一安全挑战。

另一个示例是CSP运行由伙伴提供的代码。如果伙伴不能及时提供必要的安全更新，则CSP面临风险。

6.2.10 软件依赖

如发现漏洞，可能无法立即应用更新，因为如此行事会破坏其他软件成份（尽管这些成份可能并不要求更新）。如果由一家或多家CSN而非CSP本身提供的成份之间相互依赖，则这种情况会更为明显。

6.3 云服务伙伴（CSN）的安全挑战

本节说明直接影响CSN的挑战。这类挑战可能影响到CSN开展业务、获得付款、保护其知识产权的能力。特定CSN面临的安全挑战取决于其具体的业务和环境，如开发、集成、审计或其他方面。

6.3.1 职责分工不明确

如果服务中混合运行CSP和CSN代码，则CSC不能明确了解由谁负责减缓风险和处理安全事件。通过技术分析可能难以确定应负责的实体，这会使CSP和CSN就责任问题相互指责，且如果不能找出根源则使情况进一步恶化。

6.3.2 盗用知识产权

当伙伴提交代码或其他资产由CSP执行时，则存在该材料被泄露给第三方或被盗用（用于未经授权的用途）的安全挑战，其中可能包括侵犯版权或泄露商业秘密。

6.3.3 丧失软件完整性

一旦伙伴的代码由CSP运行，则该代码可能被修改或感染，而CSN却无法对其直接掌控，从而使其软件在某种程度上行为异常。尽管这种可能性无法由CSN控制，但它却可严重影响到其声誉和业务。

7 云计算的安全能力

本标准针对已明确的云计算安全威胁和挑战确定下列安全能力。可在安全服务水平协议（SLA）中明确规定与这些安全能力相关的参数，如事件响应时间。

7.1 信任模式

对于任何多个提供商通过合作提供值得信任服务的任何系统而言，一个共同的信任模式是必不可少的。

由于云计算具有高度分布和多利益攸关方性质，因此，云计算环境需要纳入一个总体信任模式。该信任模式将便于创建受信任实体的联盟，从而使系统中不相干的成份能够对其他实体和成份的身份和授权权利进行认证。每一个信任联盟都将以一个或多个受信任的管理机构（如，公共密钥基础实施（PKI）证书管理机构）为基础。

当前，云计算和非云计算环境中都存在多信任模式，具体信任模式的采用不属于本标准的范围。

7.2 身份和接入管理（IAM）、认证、授权和交易审计

云计算服务涉及到多个管理员和用户，且这些云计算服务既由内部（CSP）也由外部（CSC）获取和使用。身份管理不仅对保护身份是必要的，而且有助于在这种动态和开放的云计算基础设施中进行接入管理、认证、授权和交易审计。

为了通过IAM进行身份认证，所以需要一或多个共同信任模式（7.1），同时开发商、管理程序和其他系统成份也需要利用这些模式来认证系统成份，如已下载的软件模块、应用或数据集。

身份和接入管理有助于实现服务和资源的保密性、完整性和可用性，因此在云计算中必不可少。

此外，IAM通过使用不同认证机制或在不同安全域中得到分布促成实现云的单一登录和身份联盟的实施。

交易审计可保护交易不受否认的影响，便于在出现安全事件后进行取证分析（forensic analysis），并阻止攻击（入侵者和内部作案人员）。交易审计不仅仅是简单的记录，而且包括主动监测，以便对可疑活动做出标记。

7.3 物理安全

有必要实现物理安全。应将包含CSP设备地点的出入限于得到授权的人员，并要求相关人员只能在其履行工作职责直接相关的地点活动，这是IAM程序的组成部分。然而，物理安全的程度取决于数据的价值以及多个客户被允许接入的程度。

7.4 接口安全

该能力可确保向CSC和/或其他定有合同的CSP开放的接口的安全（多种不同云计算服务通过上述方面提供），并确保基于这些接口的通信的安全。现有的可保障接口安全的机制包括但不限于：单边/相互认证、完整性校验和、端到端加密、数字签名等。

7.5 计算虚拟化的安全

虚拟化安全指整个虚拟化环境的安全，它保护管理程序免受攻击、保护托管平台免受源自计算虚拟化环境的威胁，并保持VM在整个生命周期期间的安全。特别应当指出，该能力有助于实现VM隔离，并在存储和迁移过程中保护VM。

对于CSP而言，管理程序往往对被托管VM形成保护（例如通过在管理程序内提供反病毒和反垃圾信息处理功能实现），从而使VM无需单独实施这些功能。通常，用尽可能少的一套服务对管理程序进行配置，不必要的接口和应用程序接口（API）被关闭，无关的服务成份也通常被禁用。

该能力涵盖的VM既包括由CSC在SaaS中创建的VM，也包括SaaS和PaaS创建的任何VM。通常，在共享内存、中央处理单元（CPU）和存储容量时会对虚拟机进行严格隔离。一般情况下，虚拟机都拥有固有的安全能力和策略意识（如，在客户操作系统中）。

7.6 网络安全

在云计算环境中，网络安全既能实现物理和虚拟网络的隔离，也能确保所有参与方之间通信的安全。它能促成实现网络安全域分割、网络边界接入控制（防火墙）、入侵发现和预防、在安全策略基础上分离网络流量，并保护网络免受物理和虚拟环境的攻击。

7.7 数据隔离、保护和隐私保护

该能力旨在解决一般性数据保护问题，这些问题往往具有法律影响。

• 数据隔离

在云计算环境中，租户不能接入属于另一租户的数据，即便数据得到加密也是如此，但明确得到授权的情况除外。根据所要求的隔离梯度和云计算软件及硬件的具体部署情况，可以逻辑或物理方式实现数据隔离。

注1：在云计算中，隔离出现在租户层面。例如，在云中，一个特定CSC可能拥有多个租户，目的是为了将不同下属机构、处室或业务单位相互分开。

• 数据保护

数据保护确保云计算环境中保存的CSC数据和衍生数据得到适当保护，使其只能按照CSC的授权（或按照适用法律）得到访问或修改。这种保护包括采用访问控制清单、完整性核实、误码纠正/数据恢复、加密和其他适当机制。

当CSP为CSC提供存储加密时，该加密可以是客户机一侧加密（如，在CSP应用内）或服务器一侧加密。

• 隐私保护

私密信息可包括PII和公司保密数据，对私密信息的收集、使用、传送、处理、存储和销毁须遵守有关隐私的规则和法律，这一限制既适用于CSP，也适用于CSC。如，CSC必须有能力永久删除包含私密信息的数据表，即便CSP并不知晓该表的内容。CSP可能还需要以经过改造或加密的形式支持CSC数据的处理，如，搜索CSC数据。

隐私保护还包括觉察到的或由CSC活动衍生的私密信息，如业务趋势、与其他各方的关系或通信、活动程度等。

隐私保护还能够确保所有私密信息（包括觉察到的或衍生的数据）都仅用于CSC与CSP之间一致认可的目的。

对私密信息进行风险评估（称作“隐私风险评估”）可帮助CSP明确在预见到的工作中可能产生的破坏隐私的具体风险。CSP应确定并实施相关能力，以解决通过风险评估确定的隐私风险，并处理私密信息。

注2：在一些管辖区，作为自然人的个人（即个人用户）独立于其雇主而得到单独对待，目的是保护隐私。在这种情况下，除保护云服务客户（CSC）或云服务租户的隐私外，云服务用户（CSU）的隐私也将得到适当保护。

7.8 安全协调

由于不同云服务意味着需要实施不同的安全控制手段，因此，这种安全能力可以对安全机制做出统一的协调，以避免出现保护方面的冲突。

在云计算生态环境中发挥不同作用的各方，如CSP、CSC、CSN，对物理或虚拟资源和服务（包括对安全的控制）拥有不同程度的控制权。

对于以上各方而言，可采用繁复多样的安全机制，包括管理程序隔离、LAM、网络保护等。

云计算的目的之一是方便这些不同方面共同协作，对多种不同物理和虚拟资源进行设计、建造、部署和运营。因此，CSP需要有能力和各不同方的不同安全机制进行协调。安全协调取决于多种不同安全机制的互操作性和统一性。

7.9 操作安全

该能力可为云计算服务和基础设施的日常操作和维护提供安全保护。

这一操作安全能力包括：

- 确定一套安全策略和安全活动，如配置管理、补丁升级、安全评估、事件响应（亦见关于“事件管理”第7.10），并确保这些安全措施得到正确落实，以满足适用法律和合同（包括任何安全SLA）的要求。
- 监督CSP的安全措施及其效果，并向受到影响的CSC和相关第三方审计者（作为CSN行事）提出报告，这将有助于CSC衡量CSP是否在履行其有关SLA的安全承诺。

如果CSP的安全措施或其效果发生变化，应向所有下游CSP和CSC发出有关变化的提示。

这些报告和提示将有助于得到授权的CSC看出相关事件、审计信息和与其云计算服务有关的配置数据。

7.10 事件管理

事件管理旨在对事件进行监督、做出预测、发出警告并做出响应。为了解云服务是否在整个基础设施上按照预期进行运行，需要连续不断进行检测（如，检测虚拟化平台和虚拟化机器的实时性能）。这将使系统能够捕获服务的安全状况、确定不正常情况并早期发出有关安全系统过载、受到破坏、服务中断等警告。出现安全事件后，要明确问题，并很快自动或通过管理员的干预迅速对事件做出响应。非公开事件得到记录和分析，以了解其可能潜在的规律，从而便于积极主动对其加以研究解决。

7.11 灾害恢复

灾害恢复能力是对毁灭性灾害做出响应，以恢复安全状态，并尽快重启正常操作。该能力可以在最小程度地中断所提供服务的条件下保持服务的连续性。

7.12 服务安全评估和审计

该能力有助于对云计算服务做出安全评估，它有助于得到授权的方面核实某种云服务是否符合适用的安全要求。安全评估或安全审计可由CSC、CSP或第三方（CSN）进行，安全认证可由得到授权的第三方（CSN）进行。

应实施相关安全标准，以使CSC和CSP之间就安全水平达成相互谅解。

每一个CSP及其所有服务都可具有有关CSP安全控制及其效果的安全水平。明确宣布的CSP及其服务的安全水平将有助于对相关CSP和云计算服务做出比较和选择。可利用受信任的独立第三方提供可靠、独立和中立的安全水平评估。

为避免CSP对每一个CSC都单独进行安全审计，可重复使用统一的服务审计结果。如果CSP的云计算服务范围广泛，则可对每一项云计算服务都进行安全审计。CSP可向经授权的CSC（如潜在客户）和某些其他CSP及CSN（如第三方审计者）提供所有和部分云计算服务的审计结果。

对于云计算服务链而言，下游服务提供商的安全审计结果将综合上游服务提供商的相关安全审计结果。

7.13 互操作性、可移植性和可反转性

该能力有助于异质成份实现共存和合作（互操作性），并方便CSC酌情以另一家CSP替换现有CSP（可移植性），同时有助于CSC将其ICT系统由云计算环境转回至非云计算ICT基础实施（可反转性）。这种可反转性还促进实现“被遗忘权”（如果当地法律或规则要求的话）。

注1：该能力仅涉及云计算安全功能的可互操作和可移植性，不涉及实际数据、元数据或信息格式，后者属于云计算平台的其他功能。例如，该能力可提供过渡性加密、密钥管理和身份信息，以便于数据和其他内容能在两个不同加密系统之间移动（在传送过程中，两个系统或数据都不会被暴露）。

注2：“被遗忘权”尚未得到明确定义，在一些情况下，可能受到有关将特定数据保存最低一段时间的监管要求限制，如呼叫记录或连接信息。因此，可能需要在同一时间段内保留相关密钥或其他安全信息。

7.14 供应链安全

云服务提供商使用若干供应商来建造其服务，其中一些可能来自云计算行业，如CSN，而其他供应商可能是传统信息技术（IT）设备或服务提供商，如，与云计算没有直接关系的硬件制造商。这一能力有助于通过安全活动在CSP与所有参与供应链的各方之间建立起信任关系。这种供应链安全活动包括明确并收集有关CSP所购得成份和服务（用以提供云计算服务）的信息，并实施供应链安全政策。

例如，CSP开展的典型供应链安全活动可包括：

- 确认供应链中各方的背景信息；
- 验证CSP使用的硬件、软件和服务；
- 检查CSP购买的硬件和软件，以确保在传送过程中不会被破坏；
- 提供有关核实云服务软件来源的机制，如由CSN提供的代码。适当时，CSN及其托管CSP还应提供验证CSN软件成份完整性的程序，以确保供货完全符合要求，未被改动或破坏。一些CSN可能要求提供由其直接对之进行验证的手段。

该能力是持续不断的，以满足系统的持续演进和更新需求。

8 框架方法

如第5和6章所述，确定云计算的安全框架意味着要了解威胁和挑战何在，同时须了解选定的特定云服务及业务、技术和监管要求，以确定特定云服务所需的安全控制、政策和程序。随后，可采用第7章所述的旨在减缓和解决这些威胁和挑战的能力来制定针对选定的特定云计算服务的安全控制、政策和程序。本标准的重点是云计算环境中的安全需求、云环境中存在的传统计算环境的威胁和挑战，因此，除本标准外，还应遵守业界确定的下列标准和最佳做法。

应采用在此描述的方法创建相关框架，以明确特定云计算服务需要哪些安全控制、政策和程序。不可能为所有云计算服务提供一种单一的规范性框架，因为云计算服务的业务模式、所提供的服务和实施选择大相径庭：

- 步骤1：通过第5和6章的内容确定云计算服务面临的安全威胁以及挑战带来的安全影响。
- 步骤2：在已确定的威胁和挑战基础上，利用第7节的内容确定所需的安全能力，以减缓安全威胁并应对安全挑战。
- 步骤3：由此制定相关安全控制、策略和程序，确定提供所需的安全能力。

注：云服务客户和CSP需通过利用相关标准，确定一套有关安全能力的要求。这一工作应以风险评估为基础。
为明确哪些安全威胁和挑战涉及云服务，应对每一种威胁和挑战都做出审议。其中一个简单的方法是在一表格中以“Y”标出威胁和挑战。

现举例说明如何使用这一方法。当CSP向个人用户提供作为服务的文档存储时，该CSP可能需要了解用户主要担心哪些安全威胁和挑战，并对CSP应对的安全威胁和挑战做出分析。表1具体说明该方式。

表1 安全框架分析法步骤1示例（作为服务的文档存储）

分析领域	具体威胁或挑战	是否适用于该服务
5.1 - 云服务客户（CSC）的安全威胁	5.1.1 - 数据丢失和泄露	Y
	5.1.2 - 不安全的服务获取	Y
	5.1.3 - 内部威胁	
5.2 - 云服务提供商（CSP）的安全威胁	5.2.1 - 未经授权的管理获取	Y
	5.2.2 - 内部威胁	Y
6.1 - 云服务客户（CSC）的安全挑战	6.1.1 - 职责分工不明确	Y
	6.1.2 - 丧失信任	Y
	6.1.3 - 丧失管理	Y
	6.1.4 - 丧失隐私	Y
	6.1.5 - 服务的不可用性	Y
	6.1.6 - 锁定一家云服务提供商	Y
	6.1.7 - 盗用知识产权	
	6.1.8 - 丧失软件完整性	
6.2 - 云服务提供商（CSP）的安全挑战	6.2.1 - 职责分工不明确	
	6.2.2 - 共享环境	Y
	6.2.3 - 保护机制之间的相互矛盾和冲突	Y
	6.2.4 - 管辖冲突	Y
	6.2.5 - 演进风险	

表1（续）

分析领域	具体威胁或挑战	是否适用于该服务
6.2 - 云服务提供商（CSP）的安全挑战	6.2.6 - 不良的过渡和集成	Y
	6.2.7 - 业务中断	Y
	6.2.8 - 云服务伙伴的锁定	
	6.2.9 - 供应链漏洞	Y
	6.2.10 - 软件依赖	
6.3 - 云服务伙伴（CSN）的安全挑战	6.3.1 - 职责分工不明确	
	6.3.2 - 盗用知识产权	
	6.3.3 - 丧失软件完整性	

一旦明确了安全威胁和挑战，则可明确能够减缓这些威胁并应对这些挑战的安全能力。表 I.1 以示例将云安全威胁和挑战与安全能力相对应。该表中纵向栏和横向行形成的交叉框中的字母“Y”表明可由相应安全能力应对特定安全威胁和挑战。该表列出了所有威胁和挑战及相应安全能力。

一旦所需能力得到明确，则可确定所需的安全控制、政策和程序。可得到使用的控制为“操作安全”（[ISO/IEC 27002]第12章）和“信息安全事件管理”（[ISO/IEC 27002]第16章），可分别通过第7章和第8章所确定的能力得出上述控制。

云服务可拥有由多家CSP构成的供应链。参与该供应链的公司在供应链安全方面可参阅国际电联和业界标准（如[ISO/IEC 28000]）。每一个CSP都需要明确界定其在云服务链中的职责，并根据上述分三步走的方式得出的安全能力制定其安全控制、策略和程序。为向CSC提供连贯一致的安全性，上游CSP可能需要按照其安全职责与其下游CSP就这些安全能力进行谈判。必要时，CSC也应遵守这一分三步走的程序。

此外，必要时应定期实施上述分三步走的程序（如，当出现破坏安全的情况，或CSP更改了其上游CSP时）。

附录 A
(资料性附录)

与云计算安全威胁和挑战相对应的安全能力

表 A.1 所示为与云计算安全威胁和挑战相对应的安全能力。由表中纵向栏和横向行形成的方格中的字母“Y”表示由相应安全能力应对特定安全威胁和挑战。

表 A.1 与云计算安全威胁和挑战相对应的安全能力

第7章 云计算的安全能力															
	7.1	7.2	7.3	7.4	7.5	7.6	7.7	7.8	7.9	7.10	7.11	7.12	7.13	7.14	
	信任模式	身份和接入管理(IAM)、认证、授权和交易审计		接口安全	计算虚拟化安全	网络安全	数据隔离、保护和隐私保护	安全协调	操作安全	事件管理	灾难恢复	服务安全评估和审计	互操作性、可移植性和可反转性	供应链安全	
第5章 云计算的安全威胁	5.1.1 数据丢失和泄漏	Y	Y				Y				Y				
	5.1.2 云计算客户(CSC)的不安全的服务获取	Y	Y	Y	Y	Y									
	5.1.3 内部威胁		Y	Y								Y			
	5.2.1 未经授权云服务提供商(CSP)的取	Y	Y	Y											
	5.2.2 内部威胁		Y	Y								Y			

表 A.1 (续)

第7章 云计算的安全能力													
	7.1 信任模式	7.2 身份和接入管理(物理安全、认证、授权和交易审计)	7.3 接口安全	7.4 计算虚拟化安全	7.5 网络安全	7.6 数据隔离、保护和隐私保护	7.7 操作安全	7.8 事件管理	7.9 灾难恢复	7.10 评估和审计	7.11 互操作性、可移植性和可反转性	7.12 供应链安全	7.13 供应链安全
第6章 云计算的安全挑战	6.1.1 职责分工不明确	Y					Y						
	6.1.2 丧失信任								Y				
	6.1.3 丧失管理	Y	Y			Y	Y	Y	Y				
	6.1.4 丧失隐私	Y				Y			Y				
	6.1.5 服务的不可用性						Y	Y	Y				Y
	6.1.6 锁定一家云服务提供商										Y		
	6.1.7 盗用知识产权	Y	Y			Y			Y				

表 A.1 (续)

第7章 云计算的安全能力															
		7.1 信任模式	7.2 身份和接入管理(IAM)、认证、授权和交易审计	7.3 物理安全	7.4 接口安全	7.5 计算虚拟化安全	7.6 网络安全	7.7 数据隔离、保护和隐私保护	7.8 安全协调	7.9 操作安全	7.10 事件管理	7.11 灾害恢复	7.12 服务安全评估和审计	7.13 互操作性、可移植性和可反转性	7.14 供应链安全
第6章 云计算的安全挑战	6.1 云服务客户(CSC)的安全挑战		Y			Y		Y							
	6.1.8 丧失软件完整性														
	6.2.1 职责分工不明确		Y							Y					
	6.2.2 共享环境					Y	Y	Y							
	6.2.3 保护机制之间的矛盾和冲突								Y					Y	
	6.2 云服务提供商(CSP)的安全挑战														
	6.2.4 管辖冲突							Y		Y					
	6.2.5 演进风险									Y				Y	Y
	6.2.6 不良的过渡和集成				Y	Y	Y	Y	Y	Y					

表 A.1 (续)

第7章 云计算的安全能力															
	7.1 信任模式	7.2 身份和接入管理(IAM)、认证、授权和交易审计	7.3 物理安全	7.4 接口安全	7.5 计算虚拟化的安全	7.6 网络安全	7.7 数据隔离、保护和隐私保护	7.8 安全协调	7.9 操作安全	7.10 事件管理	7.11 灾害恢复	7.12 服务安全评估和审计	7.13 互操作性、可移植性和可反转性	7.14 供应链安全	
第6章 云计算的安全挑战	6.2 云服务提供商(CSP)的安全挑战	6.2.7 业务中断								Y					
		6.2.8 云服务伙伴的锁定												Y	
		6.2.9 供应链漏洞												Y	
	6.3 云服务伙伴(CSN)的安全挑战	6.2.10 软件依赖												Y	
		6.3.1 职责分工不明确	Y							Y					
		6.3.2 盗用知识产权	Y	Y				Y		Y					
	6.3.3 丢失软件完整性		Y												
						Y		Y							

参 考 文 献

- [1] [ITU-T E.409] Recommendation ITU-T E.409 (2004), *Incident organization and security incident handling: Guidelines for telecommunication organizations*.
- [2] [ITU-T X.810] Recommendation ITU-T X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- [3] [ISO/IEC 19440] ISO/IEC 19440:2007, *Enterprise integration – Constructs for enterprise modelling*.
- [4] [ISO/IEC 20000-1] ISO/IEC 20000-1:2011, *Information technology – Service management – Part 1: Service management system requirements*.
- [5] [ISO/IEC 27000] ISO/IEC 27000:2012, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
- [6] [ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.
- [7] [ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management*.
- [8] [ISO/IEC 28000] ISO/IEC 28000:2007, *Specification for security management systems for the supply chain*.
- [9] [ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology – Security techniques – Privacy framework*.
- [10] [NIST-SP-800-30] NIST Special Publication 800-30 (2012), *Guide for Conducting Risk Assessments*.
- [11] [NIST-SP-800-53] NIST Special Publication 800-53 Rev.3 (2009), *Recommended Security Controls for Federal Information Systems and Organizations*.
- [12] [NIST-SP-800-125] NIST Special Publication 800-125 (2011), *Guide to Security for Full Virtualization Technologies*.
- [13] [NIST-SP-800-145] NIST Special Publication 800-145 (2011), *The NIST Definition of Cloud Computing*.
- [14] [CSA Matrix] CSA (2013), *Cloud Controls Matrix*, Cloud Security Alliance.
- [15] [key definition] Key definitions of the Data Protection Act, Information Commissioners Office
<http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx>
-

