国际标准 ISO/IEC 27017

第一版 2015-12-15

信息技术-安全技术-基于ISO/IEC 27002的云服务的信息安全控制实践规范

参考编号 ISO/IEC 27017:2015

ISO版权局
案例邮政 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org
发布于瑞士

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全球标准化的专业系统。作为ISO或IEC成员的国家机构通过技术委员会参与国际标准的制定，这些技术委员会是由各自组织建立用于处理特定领域的技术活动。ISO和IEC技术委员会在共同感兴趣的领域开展合作。与ISO和IEC联络的其他国际组织、政府和非政府组织也参与了这项工作。在信息领域技术、ISO和IEC成立了联合技术委员会，ISO/IEC JTC 1。

国际标准的制定遵循ISO/IEC导则第2部分的规则。

联合技术委员会的主要任务是制定国际标准。联合技术委员会通过的标准草案会分发给国家机构进行表决。要作为国际标准出版至少需要75%的国家机构投票通过。

需要注意的是，本文件的某些要素可能是专利权的主体。ISO和IEC不负责识别任何或所有此类专利权。

ISO/IEC 27017 是由联合技术委员会ISO/IEC JTC 1-信息技术、小组委员会SC 27-IT安全技术，与ITU-T合作。相同的文本发布为ITU-T.X.1631（07/2015）。

国际电信联盟

国际电联**-T** X.1631

国际电联电信标准化分部 （07/2015）

系列 X：数据网络，开放系统
通信和安全
云计算安全--云计算安全设计

信息技术-安全技术-基于ISO/IEC 27002的云服务控制实用规则

推荐 ITU-T X.1631

ITU-T X-系列推荐文档

数据网络、开放系统通信和安全

公共数据网络	X.1-X.199
开放式系统互连	X.200-X.299
网络间的互通	X.300-X.399
消息处理系统	X.400-X.499
目录	X.500-X.599
OSI 网络与系统方面	X.600-X.699
OSI 管理	X.700-X.799
安全	X.800-X.849
OSI 应用	X.850-X.899
打开分布式处理	X.900-X.999
信息和网络安全	
一般安全方面	X.1000-X.1029
网络安全	X.1030-X.1049
安全管理	X.1050-X.1069
远程生物识别	X.1080-X.1099
安全的应用程序和服务	
多播安全性	X.1100-X.1109
家庭网络安全	X.1110-X.1119
移动安全	X.1120-X.1139
网络安全	X.1140-X.1149
安全协议	X.1150-X.1159
点对点安全性	X.1160-X.1169
网络 ID 安全性	X.1170-X.1179
IPTV 安全性	X.1180-X.1199
网络空间安全	
网络安全	X.1200-X.1229
打击垃圾邮件	X.1230-X.1249
身份管理	X.1250-X.1279
安全的应用程序和服务	
紧急通信	X.1300-X.1309
无处不在的传感器网络安全	X.1310-X.1339
PKI 相关建议	X.1340-X.1349
网络安全信息交换	
网络安全概述	X.1500-X.1519
漏洞/状态交换	X.1520-X.1539
结果/事件/启发式交换	X.1540-X.1549
政策交换	X.1550-X.1559
启发式和信息请求	X.1560-X.1569
识别和发现	X.1570-X.1579
保证交换	X.1580-X.1589
云计算安全性	
云计算安全概述	X.1600-X.1601
云计算安全设计	X.1602-X.1639
云计算安全最佳实践和指南	X.1640-X.1659
云计算安全实施	X.1660-X.1679
其他云计算安全性	X.1680-X.1699

更多详细资料，请参见ITU-T推荐文档列表

国际标准 ISO/IEC 27017
推荐 ITU-T X.1631

信息技术--安全技术--
基于 ISO/IEC 27002 的云服务信息安全控制实践规则

概述

推荐ITU-T X.1631 | ISO/IEC 27017为适用于提供和使用云服务的信息安全控制措施提供了以下指南:

----ISO/IEC 27002 中相关控制措施的附加实施指南
-----和云服务特别相关的附加控制措施和实施指南

本推荐 | 国际标准既为云服务提供商也为云服务客户提供控制措施和实施指南。

历史

版本	推荐号	审批	研究小组	唯一识别号
1.0	ITU-T X.1631	2015-07-14	17	11.1002/1000/12490

要访问推荐文档，请在网络浏览器的地址字段中输入URL http://handle.itu.int/，然后输入推荐文档的唯一识别号。例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是联合国在电信、信息和通信技术（ICTs）领域的专门代表机构。国际电信联盟电信标准化分部(ITU-T)是国际电联的常设机构。ITU-T负责技术研究，运营和关税问题，并就这些问题颁布推荐标准，以在全世界范围内使电信标准化。

每四年举行一次的世界电信标准化大会(WTSA)为ITU-T研究小组确定研究主题，这些研究小组又就这些主题研究出推荐文档

ITU-T推荐文档的批准包括在WTSA1号决议规定的程序中。

在ITU-T职权范围内的一些信息技术领域，必要的标准是与ISO和IEC共同开发的。

注释

在本推荐文档中，为简洁起见，“管理”一词既可用于表示电信管理，也可用于表示公认的经营组织。

遵守本推荐文档是自愿的。但是，本推荐文档中可能包含一些强制性规定(以确保例如互操作性或适用性)，当所有这些强制性规定都得到满足时，就实现了对本推荐文档的符合性。“应该”或其他一些强制性语言如“必须”以及一些对等的否定性词语被用来表达要求。使用这类词语并不意味着任何一方必须遵守本推荐文档。

知识产权

国际电联提请注意，本推荐文档的实践或实施可能涉及使用已声明的知识产权。国际电联对主张的知识产权的证据，有效性或适用性不抱任何立场，无论是国际电联成员或本推荐文档制定程序之外的其他组织所主张的。截至本推荐文档批准之日，国际电联尚未收到知识产权通知实施本建议书可能需要专利的保护。但是，执行者请注意，这可能不代表最新信息，因此强烈建议您访问TSB专利数据库，网址为http://www.itu.int/ITU-T/ipr/。

目录

引言

本推荐文档|国际标准中所载的指南，是对ISO/IEC 27002中给出的指南的附加和补充。

具体来说，本推荐|国际标准，为云服务客户和云服务提供商提供了在实施信息安全控制的指南。一些准则适用于云执行控制的服务客户，以及支持云服务提供商实现的其他客户这些控件。选择适当的信息安全控制并应用它们所提供的指导将接受风险评估，以及任何法律、合同、监管或其他特定于云领域的指导信息安全需求。

国际标准

ITU-T 推荐文档

信息技术**------**安全技术**-----**基于**ISO/IEC 27002** 的云服务的信息安全控制实用规则

1 范围

本推荐文档| 国际标准为适用于提供和使用云服务的信息安全控制措施提供了以下指南:

----ISO/IEC 27002 中相关控制措施的附加实施指南
-----和云服务特别相关的附加控制措施和实施指南

本推荐文档| 国际标准既为云服务提供商也为云服务客户提供控制措施和实施指南。

2 规范性引用文件

下列推荐和国际标准载有本推荐| 国际标准的规定，通过案文的引用。在出版时，所指出的版本是有效的。所有建议和标准均须修订，并鼓励根据本建议订立的《协定》缔约国调查采用下列建议和标准的最新版本的可能性。IEC和ISO的成员维护当前有效的国际标准的登记册。国际电联电信标准化局备有一份目前有效的国际电联-T建议清单。

下列推荐和国际标准所包含的规定，通过在本文中引用而构成本推荐/国际标准的规定。在出版时，所指示的版本有效。所有推荐文档和标准都可能会进行修订，并且鼓励基于此推荐文档/国际标准的协议的各方研究应用下列推荐文档和标准最新版本的可能性。IEC和ISO的成员维护着当前有效的国际标准的登记表。ITU电信标准化局保留一份当前有效的ITU-T推荐文档清单。

2.1 相同的推荐文档|国际标准

----推荐文档ITU-T Y. 3500(现行) |ISO/IEC 17788(现行)，信息技术--云计算—概述和术语。

----推荐文档ITU-T Y.3502(现行) |ISO/IEC 17789(现行)，信息技术--云计算--参考架构。

2.2 其他参考

----ISO/IEC 27000:(现行)，信息技术--安全技术--信息安全管理系统--概述和词汇。

----ISO/IEC 27002:2013，信息技术--安全技术—信息安全控制实用规则。

3. 定义和缩写

3.1 术语定义

在ISO/IEC 27000、推荐文档ITU-T Y.3500| ISO/IEC 17788、推荐文档ITU-T Y.3502| ISO/IEC 17789中给出的术语和定义以及下列定义适用于本推荐文档| 国际标准：

3.1.1 ISO 19440 定义了以下术语：

----**能力**：能够执行给定活动的质量。

3.1.2 ISO/IEC 27040 定义了以下术语：

----**数据泄漏**：安全性受损，导致意外或非法的破坏、丢失、更改、未经授权的披露或访问已被传输、存储或以其他方式处理的受保护数据

----**安全多租户**：一种多租户类型，它使用安全控制措施明确地防范数据泄露，并为适当的治理提供这些控制措施的确认。

注1：当单个租户的风险水平不大于专用单租户环境中的风险水平时，存在安全的多租户关系。
注2：在非常安全的环境中，即使是租户的身份也是要保密。

3.1.3 ISO/IEC 17203 定义了以下术语：

----- 虚拟机：支持客户软件执行的完整环境
注意：虚拟机是对虚拟硬件、虚拟磁盘和与其关联的元数据的完整封装。
虚拟机允许底层物理机器通过一个称为管理程序的软件层进行多路复用。

3.2 缩写

以下缩写适用于本推荐文档| 国际标准：

IaaS 基础架构即服务
PaaS 平台即服务
PII 个人身份信息
SaaS 软件即服务
SLA 服务级别协议
VM 虚拟机

4 云行业特定概念

4.1 概述

云计算的使用由于在计算资源的技术设计、运行和管理方式的重大变化，改变了组织评估和降低信息安全风险的方式。本推荐|国际标准提供了基于ISO/IEC 27002的特定于云的附加实施指南，并提供针对特定于云的信息安全威胁和风险考虑的附加控制措施。

本推荐| 国际标准的使用者请参阅ISO/IEC 27002中的第5至18章，以获得控制措施、实施指南和其他信息。由于ISO/IEC 27002的普遍适用性，许多控制措施、实施指南和其他信息都适用于组织的一般环境和云计算环境。例如，ISO/IEC 27002的“6.1.2职责分离”提供了一个无论组织是否充当云服务提供商都可以应用的控制措施。此外，云服务客户可以从同样的控制措施中派生出对云环境中职责分离的需求，例如，将云服务客户的云服务管理员和云服务用户分离。

作为ISO/IEC 27002的扩展，本推荐| 国际标准进一步提供特定于云服务的控制措施、实施指南和其他信息（请参阅4.5），旨在减轻与云服务的技术和运营功能相关的风险（请参阅附录B）。
云服务客户和云服务提供商可以参考ISO/IEC 27002和本推荐| 国际标准来选择控制措施和

实施指南，并在必要时添加其他控制措施。通过在使用或提供云服务的组织和业务环境中执行信息安全风险评估和风险处置，可以完成此过程（请参阅4.4）。

4.2 云服务中的供应商关系

ISO/IEC 27002第15章“供应商关系”为管理供应商关系中的信息安全提供了控制措施、实施指南和其他信息。云服务的提供和使用是一种供应商关系，其中云服务的客户是获取者，而云服务提供商是供应商。因此，该条款适用于云服务客户和云服务提供商。

云服务客户和云服务提供商也可以形成供应链。假设云服务提供商提供了基础设施功能类型的服务。另外，另一个云服务提供商可以提供应用程序能力类型服务。在这种情况下，第二个云服务提供商相对于第一个云服务提供商是云服务客户，并且相对于使用其服务的云服务客户而言是云服务提供商。本示例说明了本推荐| 国际标准适用于一个组织同时作为云服务客户和云服务提供商的情况。因为云服务客户和云服务提供商通过云服务的设计和实施形成了供应链，因此ISO/IEC 27002的“15.1.3信息和通信技术供应链”条款适用。

国际标准ISO/IEC 27036“供应商关系的信息安全性”里的多个部分，为产品和服务的获取者与供应商提供了有关供应商关系中信息安全性的详细指南。

ISO / IEC 27036第4部分直接涉及供应商关系中云服务的安全性。该标准也适用于作为获取方的云服务客户和作为供应商的云服务提供商。

4. 3 云服务客户与云服务提供商之间的关系

在云计算环境中，云服务客户数据由云服务存储、传输和处理。因此，云服务客户的业务流程可能依赖于云服务的信息安全。如果对云服务没有足够的控制措施，云服务客户可能需要对其信息安全实践采取附加预防措施。

在建立供应商关系之前，云服务客户需要选择一个云服务，选择时考虑的因素是云服务客户的信息安全要求与该服务实际提供的信息安全能力之间可能存在的差距。一旦选择了云服务，云服务客户应以满足其信息安全要求的方式管理云服务的使用。在这种关系中，云服务服务提供商应提供必要的信息和技术支持，以满足云服务客户的信息安全需求。当云服务提供商提供的信息安全控制是预置的并且云服务客户无法更改时，云服务客户可能需要实施自己的附加控制措施以减轻风险。

4. 4 管理云服务中的信息安全风险

云服务客户和云服务提供商都应具有适当的信息安全风险管理流程。建议其参考ISO/IEC 27001，了解在其信息安全管理体系中进行风险管理的要求，并参考ISO/IEC 27005，了解有关信息安全风险管理本身的进一步指导。ISO/IEC27001和ISO/IEC 27005都符合的ISO31000，也可以帮助组织全面了解风险管理。

与信息安全风险管理流程的普遍适用性相反，云计算具有自己特有的风险来源类型，包括威胁和漏洞，这些风险和漏洞源于其功能，例如网络，系统的可伸缩性和弹性，资源共享，自助服务提供，按需管理，跨辖区服务提供以及对控制实施的可见性有限。附录B提供了一些参考资料，提供了有关在提供和使用云服务时的风险源和相关风险的信息。

本推荐| 国际标准第5至18章和附录A中给出的控制措施和实施指南用于处理云计算特定的风险来源和风险。

4.5 本标准的结构

本推荐| 国际标准的结构类似于ISO/IEC 27002。本推荐| 国际标准包括ISO/IEC 27002第5至18章，并在每个条款和段落中陈述了其文本的适用性。

当ISO/IEC 27002中规定的目标和控制措施适用而不需要增加任何额外信息时，只提供对ISO/IEC 27002的引用。

当需要增加ISO/IEC 27002内容之外的目标及控制措施，或当目标采用ISO 27002中的内容，但还需要增加该目标之下的其他控制措施时，这些内容描述在规范性附录A：云服务扩展控制措施集合中。当ISO/IEC 27002标准中的控制措施或本推荐| 国际标准的附录A中的控制措施需要与云服务特定相关的附加实施指南时，在副标题“云服务的实施指南”下给出。指南分为以下两种类型：

类型1适用于单独的指南分别提供给云服务客户和云服务提供商。

类型2适用于提供给云服务客户和云服务提供商的指南相同时。

类型1

云服务的客户	云服务提供商

类型2

云服务的客户	云服务提供商

可能需要考虑的其他信息在副标题“云服务的其他信息”下提供。

5 信息安全策略

5.1 信息安全管理方向

ISO/IEC 27002 第5.1条规定的目标适用。

5.1. 1 信息安全策略

ISO/IEC 27002中的控制措施5.1.1控制措施及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云计算的信息安全策略应定义为云服务客户的特定主题策略。云服务客户的云计算信息安全策略应与组织对其信息和其他资产的信息安全风险的可接受水平相一致。 在定义用于云计算的信息安全策略时，云服务客户应考虑以下因素： - 存储在云计算环境中的信息可以由云服务提供商进行访问和管理； - 资产可以在云计算环境中维护，例如应用程序；	云服务提供商应增强其信息安全策略，以解决其云服务的提供和使用，并考虑以下因素： - 适用于云服务设计和实施的基准信息安全要求； - 来自内部授权人员的风险； - 多租户和云服务客户隔离（包括虚拟化）； - 云服务提供商的员工访问云服务客户资产； - 访问控制程序，例如用于对云服务进行管理访问的强身份验证； - 在变更管理期间与云服务客户的沟通；

- 流程可以在多租户虚拟化云服务上运行； - 云服务用户及其使用云服务的环境； - 具有特权访问权限的云服务客户的云服务管理员； - 云服务提供商组织的地理位置以及云服务提供商可以（即使是临时）存储云服务客户数据的国家/地区。	- 虚拟化安全性 - 访问和保护云服务客户数据； - 云服务客户账户的生命周期管理 - 沟通违规行为和信息共享指南，以协助调查和取证。

云服务的其他信息

云服务客户用于云计算的信息安全策略是ISO/IEC 27002 5.1.1中描述的特定主题策略的一项，组织的信息安全策略涉及其信息和业务流程。当组织使用云服务时，作为云服务客户它可以拥有针对云计算的策略。组织的信息可以在云计算环境中存储和维护，并且可以在云计算环境中运行业务流程。通用的信息安全需求在顶层的信息安全方针中声明，然后是云计算策略。

与此相反，为提供云服务而制定的信息安全策略处理的是云服务客户的信息和业务流程，而不是云服务提供商的信息和业务流程。提供云服务的信息安全需求应满足潜在的云服务客户的安全需求。因此，它们可能与云服务提供商的信息和业务流程的信息安全要求不一致。信息安全策略的范围通常是根据服务来定义的，而并不仅仅由组织结构或物理位置来定义。

云计算有多个虚拟化安全方面，包括虚拟实例存储的生命周期管理、虚拟映像的访问控制、休眠或离线虚拟实例的处理、快照、虚拟机监控程序保护和控制使用自助服务端口的安全控制。

5. 1. 2 信息安全策略的评审

ISO/IEC 27002中的控制措施5.1.2及其相关的实施指南和其他信息适用。

6 信息安全组织

6.1 内部组织

ISO/IEC 27002第6.1条规定的目标适用。

6. 1. 1 信息安全的角色和职责

ISO/IEC 27002中的控制措施6.1.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应该与云服务提供商就信息安全角色和职责的适当分配达成一致，并确认它能够履行其分配的角色和职责。双方的信息安全角色和职责应在协议中阐明。 云服务客户应识别并管理其与云服务提供商的客户支持和关怀功能的关系。	云服务提供商应该与其云服务客户、云服务提供商和供应商就信息安全角色和职责的适当分配达成一致并编制文档。

云服务的其他信息

即使在各方内部和之间确定了职责，云服务客户也要对使用该服务的决定负责。该决定应该根据云服务客户的组织内部确定的角色和职责做出。云服务提供商要对作为云服务协议一部分的信息安全负责。信息安全的实施和供应应该根据云服务提供商组织内确定的角色和职责来进行。

与数据所有权，访问控制和基础架构维护等问题相关的角色以及职责的定义和分配中的歧义会引起业务或法律纠纷，尤其是在与第三方打交道时。

在使用云服务期间创建或修改的云服务提供商系统上的数据和文件对于服务的安全操作，恢复和连续性至关重要。应定义并记录所有资产的所有权以及与这些资产相关的操作（如备份和恢复操作）的责任方。否则，云服务提供商可能会认为云服务客户执行了这些重要任务（反之亦然），从而导致数据丢失。

6. 1. 2　职责分离

ISO/IEC 27002中的控制措施6.1.2及其相关的实施指南和其他信息适用。

6. 1. 3 与职能机构的联系

ISO/IEC 27002中的控制措施6.1.3及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应识别与云服务客户和云服务提供商的联合运营相关的权限。	云服务提供商应将云服务提供商组织的地理位置以及云服务提供商可以存储云服务客户数据的国家/地区告知云服务客户。

云服务的其他信息

有关可以存储，处理或传输云服务客户数据的地理位置的信息可以帮助云服务客户确定监管机构和辖区。

6.1. 4　与特定相关方的联系

ISO/IEC 27002中的控制措施6.1.4及其相关的实施指南和其他信息适用。

6.1.5　项目管理中的信息安全

ISO/IEC 27002中的控制措施6.1.5及其相关的实施指南和其他信息适用。

6.2　移动设备和远程工作

ISO/IEC 27002 第6.2条规定的目标适用。

6.2. 1　移动设备政策

ISO/IEC 27002中的控制措施6.2.1及其相关的实施指南和其他信息适用。

6.2. 2　远程工作

ISO/IEC 27002中的控制措施6.2.2及其相关的实施指南和其他信息适用。

7　人力资源安全

7.1　任用前

ISO/IEC 27002 第7.1条规定的目标适用。

7.1. 1　审查

ISO/IEC 27002中的控制措施7.1.1及其相关的实施指南和其他信息适用。

7.1. 2 任用条款和条件

ISO/IEC 27002中的控制措施7.1.2及其相关的实施指南和其他信息适用。

7.2 任用中

ISO/IEC 27002 第7.2条规定的目标适用。

7.2.1 管理职责

ISO/IEC 27002中的控制措施7.2.1及其相关的实施指南和其他信息适用。

7.2.2 信息安全意识、教育和培训

ISO/IEC 27002中的控制措施7.2.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应在针对云服务业务经理、云服务管理员、云服务集成商和云服务用户(包括相关员工和承包商)的意识、教育和培训计划中添加以下内容： ---使用云服务的标准和程序; ---与云服务有关的信息安全风险，以及如何管理这些风险; ---使用云服务带来的系统和网络环境风险 ---适用的法律法规考虑因素。 信息安全意识、教育培训应向管理人员和监督管理人员，包括业务单位。这些努力支持协调信息安全活动。 有关云服务的信息安全意识，教育和培训计划应提供给管理层和一线经理们，包括各业务单元的管理人员和一线经理。这些努力能够为信息安全活动有效协调地开展提供支持。	考虑到对云服务客户数据和云服务派生数据的适当处理，云服务提供商应该为员工提供意识、教育和培训，并要求其承包商也这样做。这些数据可能包含云服务客户的保密信息，或者对云服务提供商的访问和使用有特定的限制，包括法规性限制。

7.2.3 违规处理过程

ISO/IEC 27002中的控制措施7.2.3及其相关的实施指南和其他信息适用。

7.3 终止和变更雇佣关系

ISO/IEC 27002 第7.3条规定的目标适用。

7.3.1. 任用终止或变更的责任

ISO/IEC 27002中的控制措施7.2.2及其相关的实施指南和其他信息适用。

8 资产管理

8.1 资产责任

ISO/IEC 27002 第8.1条规定的目标适用。

8.1.1 资产清单

ISO/IEC 27002中的控制措施8.1.1及其相关的实施指南和其他信息适用。以下特定领域指南

也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户的资产清单应该考虑存储在云计算环境中的信息和相关资产。资产的记录应表明资产的维护地点，例如：云服务的标识。	云服务提供商的资产清单应该明确标识： ---云服务客户数据 ---云服务派生数据

云服务的其他信息

有些云服务应用程序通过提供将云服务派生数据添加到云服务客户数据中的功能来管理信息。将此类云服务衍生的数据标识为资产并将其维护在资产清单中可以有助于提高信息安全性。

8.1.2 资产的所属关系

ISO/IEC 27002中的控制措施8.1.2及其相关的实施指南和其他信息适用。

云服务的其他信息

资产的所有权可能会根据所使用的云服务的类别而有所不同。当使用平台即服务(PaaS)或基础架构即服务(IaaS)这样的服务时，应用软件属于云服务客户，而当使用软件即服务(SaaS)这样的服务时，应用软件又属于云服务提供商。

8.1.3 资产的可接受使用

ISO/IEC 27002中的控制措施8.1.3及其相关的实施指南和其他信息适用。

8.1.4 资产归还

ISO/IEC 27002中的控制措施8.1.4及其相关的实施指南和其他信息适用。

8.2 信息分级

ISO/IEC 27002 第7.2条规定的目标适用。

8.2.1 信息的分级

ISO/IEC 27002中的控制措施8.2.1及其相关的实施指南和其他信息适用。

8.2.2 信息的标记

ISO/IEC 27002中的控制措施8.2.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应按照云服务客户所采用的标签程序，对云计算环境中维护的信息和相关资产进行标签记。在适用的情况下，可以采用云服务提供商提供的支持标记的功能。	云服务提供商应记录并披露其提供的任何服务功能，以使云服务客户可以对其信息和相关资产进行分类和标记。

8.2.3 资产处理

ISO/IEC 27002中的控制措施8.2.3及其相关的实施指南和其他信息适用。

8.3 介质处理

ISO/IEC 27002 第8.3条规定的目标适用。

8.3.1 移动介质的管理

ISO/IEC 27002中的控制措施8.3.1及其相关的实施指南和其他信息适用。

8.3.2 介质的处置

ISO/IEC 27002中的控制措施8.3.2及其相关的实施指南和其他信息适用。

8.3.3 物理介质的转移

ISO/IEC 27002中的控制措施8.3.3及其相关的实施指南和其他信息适用。

9 访问控制

9.1 访问控制的业务要求

ISO/IEC 27002 第9.1条规定的目标适用。

9.1.1 访问控制策略

ISO/IEC 27002中的控制措施9.1.1及其相关的实施指南和其他信息适用。

9.1.2 网络和网络服务的访问

ISO/IEC 27002中的控制措施9.1.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户使用网络服务的访问控制策略应规定用户对使用的每个单独云服务的访问要求	（没有附加的实施指南）

9.2 用户访问管理

ISO/IEC 27002 第9.2条规定的目标适用。

9.2.1 用户注册及注销

ISO/IEC 27002中的控制措施9.2.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
（没有附加的实施指南）	为了管理云服务客户的云服务用户对云服务的访问，云服务提供商应向云服务客户提供用户注册和注销功能，以及使用这些功能的规范。

9.2.2 用户访问供给

ISO/IEC 27002中的控制措施9.2.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
（没有附加的实施指南）	云服务提供商应提供用于管理云服务客户的云服务用户的访问权限的功能，以及使用这些功能的规范。

云服务的其他信息

云服务提供商应为其云服务和关联的管理接口提供支持第三方身份和访问管理的技术。这些技术可以使云服务之间的集成更容易，用户身份管理更容易，并且可以简化对多个云客户系统和服务的使用，从而支持诸如单点登录之类的功能。

9.2.3 特权访问权管理

ISO/IEC 27002中的控制措施9.2.3及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应该使用足够的身份验证技术(例如:多因素认证)，根据识别出的风险，对云服务客户的云服务管理员对云服务的管理能力进行认证。	云服务提供商应该提供足够的身份验证技术，以便根据识别的风险对云服务的管理功能对云服务客户的云服务管理员进行身份验证。例如，云服务提供商可以提供多因素身份验证功能，或者启用第三方多因素身份验证机制。

9.2.4 用户的秘密鉴别信息管理

ISO/IEC 27002中的控制措施9.2.4及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应验证云服务提供商分配如密码等秘密身份验证信息的管理流程是否符合云服务客户的要求。	云服务提供商应提供有关管理云服务客户的秘密鉴别信息的过程的信息，包括分配此类（秘密鉴别）信息和进行用户身份验证的过程。

云服务的其他信息

云服务客户应该使用自己的或第三方的身份和访问管理技术来控制秘密身份验证信息的管理。

9.2.5 户访问权的评审

ISO/IEC 27002中的控制措施9.2.5及其相关的实施指南和其他信息适用。

9.2.6 访问权的移除或调整

ISO/IEC 27002中的控制措施9.2.6及其相关的实施指南和其他信息适用。

9.3 用户的责任

ISO/IEC 27002 第9.3条规定的目标适用。

9.3.1 秘密鉴别信息的使用

ISO/IEC 27002中的控制措施9.3.1及其相关的实施指南和其他信息适用。

9.4 系统和应用访问控制

ISO/IEC 27002 第9.4条规定的目标适用。

9.4.1 信息访问限制

ISO/IEC 27002中的控制措施9.4.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应确保可以根据其访问控制策略来限制对云服务中信息的访问，并确保实现这些限制。这包括限制对云服务，云服务功能以及服务中维护的云服务客户数据的访问。	云服务提供商应提供访问控制，以允许云服务客户限制对其云服务，其云服务功能以及服务中维护的云服务客户数据的访问。

云服务的其他信息

云计算环境包括需要访问控制的其他区域。作为云服务或云服务功能的一部分，对功能和服务的访问，例如虚拟机监控程序管理功能和管理控制台，可能需要附加访问控制。

9.4.2 安全登录规程

ISO/IEC 27002中的控制措施9.4.2及其相关的实施指南和其他信息适用。

9.4.3 口令管理系统

ISO/IEC 27002中的控制措施9.4.3及其相关的实施指南和其他信息适用。

9.4.4 特权实用程序的使用

ISO/IEC 27002中的控制措施9.4.4及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
在允许使用实用程序的情况下，云服务客户应确定要在其云计算环境中使用的实用程序，并确保它们不会干扰云服务的控制。	云服务提供商应该识别云服务内部使用的任何实用程序的需求。云服务提供商应确保任何能够绕过常规操作或安全程序的实用程序的使用都严格限于授权人员，并定期对此类程序的使用进行评审和审计。

9.4.5 程序源代码的访问控制

ISO/IEC 27002中的控制措施9.4.5及其相关的实施指南和其他信息适用。

10 密码

10.1 密码控制

ISO/IEC 27002 第10.1条规定的目标适用。

10.1.1 密码控制的使用策略

ISO/IEC 27002中的控制措施10.1.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商

如果风险分析证明需要，则云服务客户应对其使用云服务实施加密控制。这些控制措施应具有足够的强度，以减轻已识别的风险，无论这些控制措施是由云服务客户提供还是由云服务提供商提供。 当云服务提供商提供加密时，云服务客户应查看云服务提供商提供的任何信息，以确认加密功能是否： - 满足云服务客户策略要求； - 与云服务客户使用的任何其他密码保护兼容； - 适用于静态数据以及往返于云服务以及从云服务内部传输的数据	云服务提供商应该向云服务客户提供关于它使用密码技术来保护其处理的信息的情况的信息。云服务提供商还应向云服务客户提供有关其提供的任何可协助云服务客户应用其自身的密码保护功能的信息。

云服务的其他信息

在一些司法管辖区，可能需要应用加密技术来保护特定类型的信息，如健康数据、居民登记号码、护照号码和驾驶执照号码。

10.1.2 密钥管理

ISO/IEC 27002中的控制措施10.1.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应该识别每个云服务的加密密钥，并实施密钥管理过程。 如果云服务提供供云服务客户使用的密钥管理功能，则云服务客户应要求提供有关用于管理与云服务相关的密钥的过程的信息： ——密钥的类型； ——密钥管理系统的规范，包括密钥生命周期的各个阶段的程序，即生成、更改或更新、存储、退休、检索、保留和销毁 ——推荐云服务客户使用的密钥管理流程。 当云服务客户使用自己的密钥管理或单独的、不同的密钥管理服务时，云服务客户不应该允许云服务提供商存储和管理用于加密操作的加密密钥。	(没有附加的实施指南)

11 物理和环境安全

11.1 安全领域

ISO/IEC 27002 第11.1条规定的目标适用。

11.1.1 物理安全边界

ISO/IEC 27002中的控制措施11.1.1及其相关的实施指南和其他信息适用。

11.1.2 物理入口控制

ISO/IEC 27002中的控制措施11.1.2及其相关的实施指南和其他信息适用。

11.1.3 办公室、房间和设施的安全保护

ISO/IEC 27002中的控制措施11.1.3及其相关的实施指南和其他信息适用。

11.1.4 外部和环境威胁的安全防护

ISO/IEC 27002中的控制措施11.1.4及其相关的实施指南和其他信息适用。

11.1.5 在安全区域工作

ISO/IEC 27002中的控制措施11.1.5及其相关的实施指南和其他信息适用。

11.1.6 交接区

ISO/IEC 27002中的控制措施11.1.6及其相关的实施指南和其他信息适用。

11.2 设备

ISO/IEC 27002 第11.2条规定的目标适用。

11.2.1 设备的安置和保护

ISO/IEC 27002中的控制措施11.2.1及其相关的实施指南和其他信息适用。

11.2.2 支持性设施

ISO/IEC 27002中的控制措施11.2.2及其相关的实施指南和其他信息适用。

11.2.3 布缆安全

ISO/IEC 27002中的控制措施11.2.3及其相关的实施指南和其他信息适用。

11.2.4 设备维护

ISO/IEC 27002中的控制措施11.2.4及其相关的实施指南和其他信息适用。

11.2.5 资产移动

ISO/IEC 27002中的控制措施11.2.5及其相关的实施指南和其他信息适用。

11.2.6 组织场所外的设备与资产安全

ISO/IEC 27002中的控制措施11.2.6及其相关的实施指南和其他信息适用。

11.2.7 设备的安全处置或再利用

ISO/IEC 27002中的控制措施11.2.7及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应请求确认云服务提供商具有用于安全处置或重新使用资源的策略和规程。	云服务提供商应确保对资源进行安全处置或再利用 (例如:如设备、数据存储、文件、内存等) 的安排是及时的。

云服务的其他信息

有关安全处置的其他信息可以在ISO/IEC 27040中找到。

11.2.8 无人值守的用户设备

ISO/IEC 27002中的控制措施11.2.8及其相关的实施指南和其他信息适用。

11.2.9 清理桌面和屏幕策略

ISO/IEC 27002中的控制措施11.2.9及其相关的实施指南和其他信息适用。

12 运行安全

12.1. 运行规程和责任

ISO/IEC 27002 第12.1条规定的目标适用。

12.1.1 文件化的操作规程

ISO/IEC 27002中的控制措施12.1.1及其相关的实施指南和其他信息适用。

12.1.2 变更管理

ISO/IEC 27002中的12.1.2控制措施及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户的变更管理流程应考虑到云服务提供商所做的任何变更的影响。	当云服务提供商提供依赖于对等云服务提供者的云服务时，云服务提供商可能需要将对等云服务提供商引起的更改通知云服务客户。 云服务提供商应向云服务客户提供有关可能会对云服务产生不利影响的有关云服务变更的信息。以下内容将帮助云服务客户确定变更可能对信息安全产生的影响： - 变更的类别； - 计划的变更日期和时间； - 对云服务和底层系统的变更的技术描述； - 变更开始和完成的通知。 当云服务提供商提供依赖于伙伴云服务提供商的云服务时，则云服务提供商可能需要将对伙伴服务提供商引起的变更通知云服务客户。

云服务的其他信息

可以在协议中标识应包含在通知中的项目列表，例如主服务协议或服务级别协议（SLA）。

12.1.3 容量管理

ISO/IEC 27002中的控制措施12.1.3及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应确保云服务提供的协议容量满足云服务客户的要求。 云服务客户应监视云服务的使用情况，并预测其容量需求，以确保云服务的性能随时间推移（依然能够满足）。	云服务提供商应该监控总资源容量，以防止资源短缺导致的信息安全事件。

云服务的其他信息

云服务涉及云服务提供商控制下的资源，这些资源根据主服务协议和相关SLA的条款提供给云服务客户。这些资源包括软件、处理硬件、数据存储和网络连接。

云服务中资源的弹性、可伸缩性和按需分配性通常会提高服务的总容量。然而，云服务客户应该清楚所提供的资源可能存在容量限制。容量限制的示例包括应用程序的处理器内核数量、可用的存储量或可用的网络带宽。

这些限制可能取决于云服务客户购买的特定云服务或特定订阅。如果云服务客户的需求超出

了限制，云服务客户可能需要更改云服务或更改订阅。

约束条件可以根据特定的云服务或云服务客户购买的特定订阅而有所不同。如果云服务客户的要求超出了限制，则云服务客户可能需要更改云服务或更改订阅。

为了使云服务客户能够执行云服务的容量管理，云服务客户应该能够访问有关资源使用情况的相关统计信息，例如：
- 特定时间段的统计数据；
- 资源使用的最大级别。

12.1.4 开发、测试和运行环境的分离

ISO/IEC 27002中的控制措施12.1.4及其相关的实施指南和其他信息适用。

12.2 恶意软件的控制

ISO/IEC 27002 第12.2条规定的目标适用。

12.2.1 对恶意软件的控制

ISO/IEC 27002中的控制措施12.2.1及其相关的实施指南和其他信息适用。

12.3 备份

ISO/IEC 27002第12.3条规定的目标适用。

12.3.1 信息备份

ISO/IEC 27002中的控制措施12.3.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
如果云服务提供商将备份功能作为云服务的一部分提供，则云服务客户应向云服务提供商索要备份功能的规格参数。 云服务客户还应验证这些规格参数是否满足备份要求。 当云服务提供商不提供备份功能时，云服务客户负责实施备份功能。	云服务提供商应该向云服务客户提供其备份功能的规范。规范应适当包括以下信息: ---备份的范围和时间表； ---备份方法和数据格式，包括相关的加密； ---备份数据的保留期限； ---验证备份数据完整性的程序； ---从备份中恢复数据所涉及的过程和时间表； ---测试备份功能的程序； ---备份的存储位置； 云服务提供商应提供安全和如果将此类服务提供给云服务客户，则对备份(如虚拟快照)的访问将被隔离。 如果将备份的云服务提供给云服务客户，则云服务提供商应提供对备份（例如虚拟快照）的安全且隔离的访问。

云服务的其他信息

在云计算环境中，进行备份的职责分配通常是不太清楚的。对于IaaS，备份的责任通常由云服务客户承担。然而，云服务客户可能不知道自己有责任备份云计算系统中生成的所有云服务客户数据，例如使用PaaS服务的开发功能生成的可执行文件。

注意——不同级别的备份和和恢复可能作为额外的服务进行收费，在这种情况下，云服务客户可以选择对什么进行备份以及何时备份。

12.4 日志和监视

ISO/IEC 27002第12.4条规定的目标适用。

12.4.1 事态日志

ISO/IEC 27002中的控制措施12.4.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该定义其事件日志的需求，并验证云服务是否满足这些需求。	云服务提供商应该为云服务客户提供日志功能。

云服务的其他信息

云服务客户和云服务提供商对事件日志的职责因使用的云服务类型而异。例如，使用IaaS，云服务提供商的日志记录职责可以局限于云计算基础设施组件的日志记录职责，云服务客户可以负责记录自己的虚拟机和应用程序的事件。

12.4.2 日志信息的保护

ISO/IEC 27002中的控制措施12.4.2及其相关的实施指南和其他信息适用。

12.4.3 管理员和操作员日志

ISO/IEC 27002中的控制措施12.4.3及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
如果将特权操作委托给云服务客户，则应该记录这些操作的操作和性能。云服务客户应该确定云服务提供商提供的日志功能是否合适，或者云服务客户是否应该实施额外的日志功能。	(没有附加的实施指南)

云服务的其他信息

云服务客户和云服务提供商之间的职责分配(参见第6.1.1条)应涵盖与云服务相关的特权操作。监视和记录特权操作的使用对于支持针对错误使用这些操作的预防和纠正措施是必要的。

12.4.4 时钟同步

ISO/IEC 27002中的控制措施12.4.4及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应请求关于云服务提供商的系统使用的时钟同步的信息。	云服务提供商应向云服务客户提供云服务提供商系统使用的时钟信息，以及云服务客户如何将本地时钟与云服务时钟同步的信息。

云服务的其他信息

有必要考虑云服务客户的系统与运行云服务客户所使用的云服务的云服务提供商的系统的时钟同步。如果没有这样的同步，就很难协调云服务客户系统上的事件和云服务提供商系统

上的事件。

12.5 运行软件的控制

ISO/IEC 27002第12.5条规定的目标适用。

12.5.1 运行系统的软件安装软

ISO/IEC 27002中的控制措施12.5.1及其相关的实施指南和其他信息适用。

12.6 技术方面的脆弱性管理

ISO/IEC 27002第12.6条规定的目标适用。

12.6.1 技术方面脆弱性的管理

ISO/IEC 27002中的控制措施12.6.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该向云服务提供商请求关于能够影响所提供的云服务的技术脆弱性管理的信息。云服务客户应识别它将负责管理的技术脆弱性，并明确定义管理这些脆弱性的流程。	云服务提供商应该向云服务客户提供关于能够影响所提供的云服务的技术漏洞管理的信息。

12.6.2 软件安装限制

ISO/IEC 27002中的控制措施12.6.2及其相关的实施指南和其他信息适用。

12.7 信息系统审计的考虑

ISO/IEC 27002第12.7条规定的目标适用。

12.7.1 信息系统审计的控制

ISO/IEC 27002中的控制措施12.7.1及其相关的实施指南和其他信息适用。

13 通信安全

13.1 网络安全管理

ISO/IEC 27002第13.1条规定的目标适用。

13.1.1 网络控制

ISO/IEC 27002中的控制措施13.1.1及其相关的实施指南和其他信息适用。

13.1.2 网络服务的安全

ISO/IEC 27002中的控制措施13.1.2及其相关的实施指南和其他信息适用。

13.1.3 网络中的隔离

ISO/IEC 27002中的控制措施13.1.3及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商

云服务客户应定义其对隔离网络的要求，以便在云服务的共享环境中实现租户隔离，并验证云服务提供商是否满足这些要求。	对于以下情况，云服务提供商应强制实施网络访问隔离： - 在多租户环境中租户之间的隔离； - 云服务提供商的内部管理环境与云服务客户的云计算环境之间的隔离。 在适当的地方，云服务提供商应帮助云服务客户验证由云服务提供商实施的隔离。

云服务的其他信息

法律法规可能要求隔离网络或隔离网络流量。

13.2 信息传输

ISO/IEC 27002第13.2条规定的目标适用。

13.2.1 信息传输策略和规程

ISO/IEC 27002中的控制措施13.2.1及其相关的实施指南和其他信息适用。

13.2.2 信息传输协议

ISO/IEC 27002中的控制措施13.2.2及其相关的实施指南和其他信息适用。

13.2.3 电子消息发送

ISO/IEC 27002中的控制措施13.2.3及其相关的实施指南和其他信息适用。

13.2.4 保密或不披露协议

ISO/IEC 27002中的控制措施13.2.4及其相关的实施指南和其他信息适用。

14 系统的获取、开发和维护

14.1 信息系统的安全要求

ISO/IEC 27002第14.1条规定的目标适用。

14.1.1 信息安全需求分析和说明

ISO/IEC 27002中的控制措施14.1.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该确定其对云服务的信息安全需求，然后评估云服务提供商提供的服务是否能够满足这些需求。 为了进行此评估，云服务客户应向云服务提供商请求有关信息安全能力的信息。	云服务提供商应向云服务客户提供有关他们使用的信息安全功能的信息。这些信息应具有参考价值，而不会透露可能对具有恶意意图的人有用的信息

云服务的其他信息

应注意限制有关安全控制措施的实施细节的披露，因为它们与提供给已签署保密协议的那些云服务客户或潜在云服务客户的云服务有关。

14.1.2 公共网络上的应用程序的安全保护

ISO/IEC 27002中的控制措施14.1.2及其相关的实施指南和其他信息适用。

14.1.3 应用程序服务事务的保护

ISO/IEC 27002中的控制措施14.1.3及其相关的实施指南和其他信息适用。

14.2 开发和支持过程中的安全

ISO/IEC 27002第14.2条规定的目标适用。

14.2.1 安全的开发策略

ISO/IEC 27002中的控制措施14.2.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该向云服务提供商索取关于云服务提供商使用的安全开发规程和实践的信息。	云服务提供商应在符合其公开策略的范围内提供关于其使用安全开发规程和实践的信息。

云服务的其他信息

云服务提供商的安全开发规程和实践对SaaS非常重要。

14.2.2 系统变更控制程序

ISO/IEC 27002中的控制措施14.2.2及其相关的实施指南和其他信息适用。

14.2.3 操作平台变更后对应用的技术评审

ISO/IEC 27002中的控制措施14.2.3及其相关的实施指南和其他信息适用。

14.2.4 软件包变更的限制

ISO/IEC 27002中的控制措施14.2.4及其相关的实施指南和其他信息适用。

14.2.5 系统安全工程原则

ISO/IEC 27002中的控制措施14.2.5及其相关的实施指南和其他信息适用。

14.2.6 安全的开发环境

ISO/IEC 27002中的控制措施14.2.6及其相关的实施指南和其他信息适用。

14.2.7 外包开发

ISO/IEC 27002中的控制措施14.2.7及其相关的实施指南和其他信息适用。

14.2.8 系统安全测试

ISO/IEC 27002中的控制措施14.2.8及其相关的实施指南和其他信息适用。

14.2.9 系统验收测试

ISO/IEC 27002中的控制措施14.2.9及其相关的实施指南和其他信息适用。

云服务的其他信息

在云计算中，系统验收测试指南适用于云服务客户对云服务的使用。

14.3 测试数据

ISO/IEC 27002第14.3条规定的目标适用。

14.3.1 测试数据的保护

ISO/IEC 27002中的控制措施14.3.1及其相关的实施指南和其他信息适用。

15 供应商关系

15.1 供应商关系中的信息安全

ISO/IEC 27002第15.1条规定的目标适用。

15.1.1 供应商关系的信息安全策略

ISO/IEC 27002中的控制措施15.1.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应在其针对供应商关系的信息安全策略中将云服务提供商作为一种供应商看待。这将有助于降低云服务提供商访问和管理云服务客户数据相关的风险。	(没有附加的实施指南)

15.1.2 在供应商协议中强调安全

ISO/IEC 27002中的控制措施15.1.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应按照服务协议中的描述，承担与云服务相关的信息安全角色和职责。这些包括以下流程： ——恶意软件保护 ——备份 ——加密控制 ——脆弱性管理 ——事件管理 ——技术符合性检查 ——安全性测试 ——审计 ——收集、维护和保护证据，包括日志和审计跟踪 ——服务协议终止后的信息保护 ——身份验证和访问控制 ——身份和访问管理	云服务提供商应在协议中明确云服务提供商将实施的相关信息安全措施，以确保云服务提供商和云服务客户之间没有误解。 云服务提供商将实施的相关信息安全性措施可能会根据客户使用的云服务的类型而有所不同。

15.1.3 信息与通信技术供应链

ISO/IEC 27002中的控制措施15.1.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商

(没有附加的实施指南)	如果云服务提供商使用伙伴云服务提供商的云服务，则云服务提供商应确保其自身云服务客户的信息安全级别得到维持或超越。 当云服务提供商基于供应链提供云服务时，云服务提供商应向供应商提供信息安全目标，并要求每个供应商执行风险管理活动以达到目标。

15.2 供应商服务交付管理

ISO/IEC 27002第15.2条规定的目标适用。

15.2.1 供应商服务的监控和评审

ISO/IEC 27002中的控制措施15.2.1及其相关的实施指南和其他信息适用。

15.2.2 供应商服务的变更管理

ISO/IEC 27002中的控制措施15.2.2及其相关的实施指南和其他信息适用。

16 信息安全事件管理

16.1 信息安全事件的管理及改进

ISO/IEC 27002第16.1条规定的目标适用。

16.1.1 职责和规程

ISO/IEC 27002中的控制措施16.1.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应验证信息安全事件管理的责任分配，并确保其满足云服务客户的要求。	作为服务规范的一部分，云服务提供商应定义在云服务客户和云服务提供商之间信息安全事件管理职责和流程的分配。 云服务提供商应该提供向云服务客户提供的文件包括以下内容： ——云服务提供商向云服务客户报告的信息安全事件的范围 ——信息安全事件检测及响应的披露水平 ——信息安全事件通知产生的目标时间范围 ——信息安全事件通报程序 ——处理信息安全事件相关事宜的联系方式 ——如果发生某些信息安全事件，可以采取的任何补救措施。

16.1.2 报告信息安全事态

ISO/IEC 27002中的控制措施16.1.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商

云服务客户应向云服务提供商请求有关以下机制的信息： -云服务客户将其检测到的信息安全事态报告给云服务提供商； -云服务提供商接收关于由云服务提供商检测到的信息安全事态的报告； -云服务客户跟踪报告的信息安全事态的状态。	云服务提供商应该提供以下机制： ——云服务客户向云服务提供商报告信息安全事态； ——云服务提供商向云服务客户报告信息安全事态； ——云服务客户跟踪报告的信息安全事态的状态

云服务的其他信息

该机制不仅应该定义流程，还应该为云服务客户和云服务提供商提供基本信息，如联系电话、电子邮件地址和服务时间。

信息安全事态可能由云服务客户或云服务提供商检测到。因此，与云计算相关的主要额外职责是，检测到事态的一方应该拥有立即报告事态给另一方的程序。

16.1.3 报告信息安全弱点

ISO/IEC 27002中的控制措施16.1.3及其相关的实施指南和其他信息适用。

16.1.4 信息安全事件的评估和决策

ISO/IEC 27002中的控制措施16.1.4及其相关的实施指南和其他信息适用。

16.1.5 信息安全事件的响应

ISO/IEC 27002中的控制措施16.1.5及其相关的实施指南和其他信息适用。

16.1.6 从信息安全事件中学习

ISO/IEC 27002中的控制措施16.1.6及其相关的实施指南和其他信息适用。

16.1.7 证据的收集

ISO/IEC 27002中的控制措施16.1.7及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户和云服务提供商应该就在云计算环境中响应潜在的数字证据或其他信息的请求的流程达成一致。	

17. 业务连续性管理的信息安全方面

17.1 信息安全的连续性

ISO/IEC 27002第17.1条规定的目标适用。

17.1.1 规划信息安全连续性

ISO/IEC 27002中的控制措施17.1.1及其相关的实施指南和其他信息适用。

17.1.2 实施信息安全连续性

ISO/IEC 27002中的控制措施17.1.2及其相关的实施指南和其他信息适用。

17.1.3 验证、评审和评价信息安全连续性

ISO/IEC 27002中的控制措施17.1.3及其相关的实施指南和其他信息适用。

17.2 冗余

ISO/IEC 27002第17.2条规定的目标适用。

17.2.1 信息处理设施的可用性

ISO/IEC 27002中的控制措施17.2.1及其相关的实施指南和其他信息适用。

18 符合性

18.1 符合法律和合同要求

ISO/IEC 27002第18.1条规定的目标适用。

18.1.1 适用的法律和合同要求的识别

ISO/IEC 27002中的控制措施18.1.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应该考虑的问题是，除了云服务客户适用的相关法律法规之外，还需考虑适用于云服务提供商的管理辖区的相关法律法规。 云服务客户应要求提供云服务提供商遵守云服务客户业务所需的相关法规和标准的证据。此类证据可以是第三方审核员出具的证明。	云服务提供商应将管理云服务的法律管辖权告知云服务客户。云服务提供商应该识别自己的相关法律要求（例如，有关保护个人身份信息（PII）的加密）。还应在云服务客户要求时向其提供此信息。 云服务提供商应向云服务客户提供其当前符合适用法律和合同要求的证据。

云服务的其他信息

应确定适用于提供和使用云服务的法律和法规要求，特别是当处理、存储和通信功能在地理上是分布式的，并且涉及多个司法管辖区时。

重要的是要注意，合规性要求（无论是法律要求还是合同要求）仍然是云服务客户的责任。合规性责任不能转移给云服务提供商。

18.1.2 知识产权

ISO/IEC 27002中的控制措施18.1.2及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
在云服务中安装商业许可软件可能会违反软件的许可条款。云服务客户在编写任何要安装在云服务中的许可软件之前，应该有一个程序来识别特定于云的许可要求。特定的应该注意云服务所在的情况弹性和可扩展性，软件可以运行在更多系统或处理器核心超出许可条款。 在云服务中安装商业许可的软件可能会违反该软件的许可条款。云服务客户应具有一个规程，在允许将任何获得许可的软件安装到云服务之前，应识别其特定于云的许可要求。应特别注意云服务具有可碎性和可扩展性，并且软件可能会在许可条款允许的范围之外的更多系统或处理器内核上运行的情况。	云服务提供商应该建立一个处理知识产权投诉的流程。

18.1.3 记录的保护

ISO/IEC 27002中的控制措施18.1.3及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务的客户	云服务提供商
云服务客户应向云服务提供商请求有关保护云服务提供商收集和存储的与云服务客户使用云服务有关的记录的信息。	云服务提供商应向云服务客户提供关于保护云服务提供商收集和存储的与云服务客户使用云服务有关的记录的信息。

18.1.4 隐私和个人可识别信息保护

ISO/IEC 27002中的控制措施18.1.4及其相关的实施指南和其他信息适用。

云服务的其他信息

ISO/IEC27018，作为PII处理者的公有云中保护PII的实用规则，提供了有关此主题的其他信息。

18.1.5 密码控制规则

ISO/IEC 27002中的控制措施18.1.5及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该验证应用于云服务使用的一套密码控制是否符合相关协议、法规和法规。	云服务提供商应向云服务客户提供云服务提供商实施的密码控制措施的描述，以评审是否符合适用的协议、法规和法规。

18.2 信息安全评审

ISO/IEC 27002第18.2条规定的目标适用。

18.2.1 信息安全的独立评审

ISO/IEC 27002中的控制措施18.2.1及其相关的实施指南和其他信息适用。以下特定领域指南也适用。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应要求提供书面证据，证明云服务的信息安全控制措施和指南的实施符合云服务提供商的任何声明。此类证据可以包括针对相关标准的认证。	云服务提供商应该向云服务客户提供书面证据，以证实其实施了信息安全控制措施的声明。 如果单个云服务客户审核是不切实际的或可能增加信息安全风险，则云服务提供商应提供独立的证据，证明信息安全是按照云服务提供商的策略和规程实施和运行的。在签订合同之前，应将证据提供给潜在的云服务客户。如果提供了足够的透明度，由云服务提供商选择的相关独立审核通常是一种可接受的方法，可以满足云服务客户对云服务提供商的运行进行评审的兴趣。当独立审计不切实际时，云服务提供商应进行自我评估，并将其过程和结果披露给云服务客户。

18.2.2 符合安全策略和标准

ISO/IEC 27002中的控制措施18.2.2及其相关的实施指南和其他信息适用。

18.2.3 技术符合性评审

ISO/IEC 27002中的控制措施18.2.3及其相关的实施指南和其他信息适用。

附录 A

云服务扩展控制措施集合
(本附录为本推荐文档|国际标准的组成部分。)

本附录作为云服务的扩展控制措施集合，提供了附加的控制目标、控制措施和实施指南。与这些控制措施有关的ISO/IEC 27002控制目标不再重复。

拟在符合ISO/IEC 27001的信息安全管理体系(ISMS)中实施这些控制措施的组织，应将本附录中所述的控制措施包含进其适用性声明（SOA）中。

CLD.6. 3云服务客户与云服务提供商的关系

目的:明确云服务客户和云服务提供商在信息安全管理中的角色和职责的共享关系。

CLD.6. 3.1在云计算环境中角色和职责的共享

控制措施
在使用云服务时，共享信息安全角色的职责应分配给已识别的各方，并由云服务客户和云服务提供商共同记录，传达和实施。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应根据其对云服务的使用情况,定义或扩展其现有的策略和规程,并使云服务用户了解其在使用云服务时的角色和职责。	云服务提供商应记录并沟通其使用云服务的信息安全功能、角色和职责，以及作为云服务使用的一部分，云服务客户需要实施和管理的信息安全角色和职责。

云服务的其他信息
在云计算中，角色和职责通常在云服务客户的员工和云服务提供商的员工之间划分。角色和职责的分配应考虑云服务提供商托管的云服务客户数据和云服务客户应用程序。

CLD.8.1 资产责任
ISO/IEC 27002 第8.1条规定的目标适用。

CLD.8.1.5 移除云服务客户资产

控制措施
云服务客户在云服务提供商场所内的资产，应在云服务服务协议终止后及时移除，必要时返还。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应要求提供关于终止服务流程的书面说明，其中包括返还和删除云服务客户的资产，然后从云服务提供商的系统中删除这些资产的所有副本。该说明应列出所有资产并记录服务终止时间表，该过程应及时进行。	云服务提供商应提供关于在云服务使用协议终止后返还和移除任何云服务客户资产的安排的信息。资产的返还和移除安排应在协议中记录,并应及时执行。这些安排应具体说明要退还和移除的资产。

CLD.9.5 共享虚拟环境下云服务客户数据的访问控制

目的：降低使用云计算共享虚拟环境时的信息安全风险。

CLD.9.5.1 在虚拟计算环境中的隔离

控制措施
运行在云服务上的云服务客户的虚拟环境应防止其他云服务客户及未经授权人士的访问。

云服务的实施指南

云服务客户	云服务提供商
(没有附加实施指南)	云服务提供商应针对以下方面对云服务客户数据、虚拟化、应用程序、操作系统、存储和网络实施适当的逻辑隔离： - 在多租户环境中将云服务客户使用的资源分离； - 将云服务提供商的内部管理与云服务客户使用的资源分离。 如果云服务涉及多租户，则云服务提供商应实施信息安全控制措施，以确保适当隔离不同租户使用的资源。 云服务提供商应考虑在云服务提供商提供的云服务中运行云服务客户提供的软件所引起的相关风险。

云服务的其他信息

逻辑隔离的实现取决于应用于虚拟化的技术：

- 当软件虚拟化功能提供虚拟环境（例如虚拟操作系统）时，可以虚拟化网络和存储配置。此外，可以使用软件的隔离功能来设计和实现软件虚拟化环境中的云服务客户隔离。
- 当云服务客户的信息与云服务的“元数据表”存储在物理共享的存储区域中时，可以通过对“元数据表”的访问控制来实现与其他云服务客户的信息隔离 。

安全多租户和“ISO/IEC 27040，信息技术-安全技术-存储安全”中给出的相关指南可以应用于云计算环境。

CLD.9.5.2 虚拟机强化

控制措施
云计算环境中的虚拟机应被强化以适应业务需求

云服务的实施指南

云服务客户	云服务提供商
在配置虚拟机时，云服务客户和云服务提供商应确保强化适当的方面（例如，只有那些需要的端口，协议和服务），并为每个使用的虚拟机采取适当的技术措施（例如，反恶意软件，日志记录）。	

CLD.12.1 运行规程和职责
ISO/IEC 27002第12.1条规定的目标适用。

CLD.12.1.5 管理员操作安全

控制措施
应该定义，记录和监视云计算环境的管理操作过程。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该记录关键操作的过程，在这些操作中，故障可能对云计算环境中的资产造成不可恢复的损害。关键操作的示例如下： --病毒化设备的安装、更改和删除例如服务器、网络和存储 --云服务使用终止程序 --备份和恢复 该文件应规定由一个主管来监视这些操作。	云服务提供商应该向提出需要的云服务客户提供关于关键操作和过程的文档。

云服务的其他信息

云计算具有快速供应和管理以及按需自助服务。这些操作通常由云服务客户和云服务提供商的管理员执行。因为人类对这些关键操作的关注会导致严重的信息安全。事件、机制的保障应该考虑操作，如果需要，应该定义和实现操作。严重事件的例子包括擦除或关闭大量虚拟服务器或破坏虚拟资产。

由于在这些关键操作中的人为干预可能会导致严重的信息安全事件，因此应考虑保护操作的机制，并在需要时定义和实施这些机制。严重事件的示例包括删除或关闭大量虚拟服务器或破坏虚拟资产。

CLD.12.4 日志记录和监视

ISO/IEC 27002第12.4条规定的目标适用。

CLD.12.4.5云服务监控

控制措施

云服务客户应具有监视云服务客户使用的云服务的特定方面操作的能力。

云服务的实施指南

云服务客户	云服务提供商
云服务客户应该向云服务提供商请求每个云服务可用的服务监视功能的信息。	云服务提供商应该提供一些功能，使云服务客户能够监视与云服务客户相关的云服务操作的特定方面。例如，监视和检测云服务是否被用作攻击他人的平台，或者是否敏感数据正在从云服务中泄露。 适当的访问控制应确保监视功能的使用。该功能应仅提供对有关云服务客户自己的云服务实例的信息的访问。 云服务提供商应向云服务客户提供服务监视功能的文档。 监视应提供与第12.4.1条中描述的事件日志一致的数据，并有助于SLA条款。

CLD.13.1网络安全管理

ISO/IEC 27002第13.1条规定的目标适用。

CLD.13.1.4虚拟和物理网络安全管理的一致性

控制措施

在配置虚拟网络时，应基于云服务提供商的网络安全策略来验证虚拟网络与物理网络之间的配置一致性。

云服务的实施指南

云服务客户	云服务提供商

(没有附加的实施指南)	云服务提供商应该定义并记录一个配置虚拟的信息安全策略符合网络信息安全政策的物理网络。云服务提供商应该确保无论采用何种方式创建虚拟网络，虚拟网络连接都与信息安全策略相匹配配置。 云服务提供商应为虚拟网络的配置定义并记录一个与物理网络的信息安全策略一致的信息安全策略。云服务提供商应确保，无论用于创建配置的方式如何，虚拟网络配置与信息安全策略相匹配。

云服务的其他信息

在基于虚拟化技术构建的云计算环境中，虚拟网络是在物理网络的虚拟基础架构上配置的。在这样的环境中，网络策略的不一致会导致系统中断或访问控制缺陷。

注–根据云服务的类型，配置虚拟网络的职责在云服务客户和云服务提供商之间可能有所不同。

附录 B

关于云计算相关信息安全风险的参考文献
(本附录不构成本推荐文档|国际标准的组成部分。**)**

正确使用本推荐文档|国际标准提供的信息安全控制措施，取决于组织的信息安全风险评估和处理方法。尽管信息安全风险评估和处理的方法是重要的主题，但本推荐文档|国际标准的重点不是他们。以下是参考文献列表，其中包括对云服务的提供和使用中的风险来源和风险的描述。 需要注意的是，风险来源和风险会根据服务的类型和性质以及云计算的新兴技术而变化。建议该推荐/国际标准的用户根据需要参考文档的当前版本。

ITU-T X. 1601(2014)，云计算安全框架
澳大利亚政府信息管理办公室2013年，为澳大利亚政府机构的隐私和云计算检查点总结，更好的实践指南，1.1版，2月，第8页。
http://www.finance.gov.aufiles/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf
2015年4月，澳大利亚政府网络安全中心，租户云计算安全。
http://www.asd.gov.au/publications/protect/Cloud Computing Security for Tenants.pdf
澳大利亚政府网络安全中心2015年- 4月云服务提供商的云计算安全。
http://www.asd.gov.au/publications/protectCloud Computing Security for Cloud Service provider.pdf
云安全联盟2014，云控制矩阵- 1月。
ENISA 2009。云计算安全风险评估- 11月。
ENISA 2009，云计算信息保障框架- 11月。
《香港政府资讯科技总监办公室2013年云服务供应商处理云端个人识别资料保安及私隐核对表》- 4月。
香港政府资讯科技总监办公室2013年云服务消费者安全检查清单-1月。
ISACA 2012，云计算安全考虑-7月。
NIST。SP 800 - 144 2011。公共云计算的安全和隐私指南- 12月。
NIST, SP 800-146 2012，云计算概要和建议- 5月。
2012年春季新加坡，附录A:新加坡虚拟化安全风险评估技术参考文献30:2012服务器虚拟化安全技术参考文献- 3月。
2012年春季新加坡，附录A:审查新加坡SaaS技术参考31:2012《公共云计算服务使用安全与服务水平指南技术参考》安全与服务水平注意事项清单- 3月。
2013年春季新加坡，附录A:《新加坡标准s584:2013多层次云计算安全规范》云服务提供商披露- 8月。
2012年新加坡春天。附录B:审查新加坡技术参考31:2012《公共云计算服务使用的安全和服务水平指南技术参考》时的安全性和服务水平考虑事项清单- 3月。
2013年春，新加坡标准SS 584:2013多层云计算安全规范。
2012年春，新加坡技术参考30:2012服务器虚拟化安全技术参考- 3月。
2012年春，新加坡技术参考31:2012《公共云计算服务使用的安全性和服务水平指南技术参考》- 3月。
美国政府FedRAMP PMO 2014，FedRAMP安全控制基线版本2.0- 6月。

参考文献

--推荐ITU-T X.805(2003)，端到端通信系统的安全体系结构。
--ISO / IEC 17203:2011,信息技术开放虚拟化格式(OVF)规范。
--ISO / IEC 27001:2013,信息技术---安全技术---信息安全管理体系---要求
--ISO / IEC 27005:2011,信息技术---安全技术---信息安全风险管理
--ISO / IEC 27018:2014,信息技术---安全技术---作为PII处理者的公共云中保护个人身份信息(PII)的实用规则
--ISO / IEC 27036 - 1:2014,信息技术---安全技术---供应商关系的信息安全---第1部分:概述和概念
--ISO / IEC 27036 - 2:2014,信息技术---安全技术---供应商关系的信息安全---第2部分:要求
--ISO / IEC 27036 - 3:2013,信息技术---安全技术---供应商关系的信息安全---第3部分:信息和通信技术供应链安全指南
--CD ISO / IEC 27036 - 4,信息技术---安全技术---供应商关系的信息安全---第4部分:云服务安全指南。(正在开发中)
——ISO / IEC 27040:2015。信息技术---安全技术---存储安全。
——ISO 1940:2007，企业集成---企业建模的构造。
——ISO 31000:2009。风险管理---原则和指南。
——NIST, SP 800-145 2011云计算的NIST定义。
——NIST 2009，有效且安全地使用云计算范式。
——ENISA 2009，云计算的好处、风险和信息安全建议。
——云安全联盟，云计算V3.0重点领域安全指南。
——云安全联盟，云计算的最大威胁V1.0。
——云安全联盟，领域12:身份与访问管理指南V2.1。
——ISACA，云计算:从安全、治理和保证的角度获得业务利益。
——ISACA。云计算管理审计/保证程序。