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的云服务信息安全控制实践准则

信息技术 - 安全技术 - 守则
以ISO/IEC
27002为基础的信息安全性控制的实用性，适用于新的服务。

参考号 ISO/IEC
27017:2015(E)

受版权保护的文件

ISO版权局
Case postale 56 CH-1211 Geneva 20
电话。+ 41 22 749 01 11
传真：+41 22 749 09 47
电子邮件 copyright@iso.org
网站 www.iso.org

发表于瑞士

前言

ISO（国际标准化组织）和IEC（国际电工委员会）构成了全世界标准化的专门体系。作为ISO或IEC成员的国家机构通过各自组织建立的技术委员会参与国际标准的制定，以处理特定的技术活动领域。ISO和IEC技术委员会在共同感兴趣的领域进行合作。其他国际组织，政府和非政府组织，与ISO和IEC联络，也参与了工作。在信息技术领域，ISO和IEC建立了一个联合技术委员会，即ISO/IEC JTC 1。

国际标准是根据ISO/IEC指令第2部分中给出的规则起草的。

联合技术委员会的主要任务是编制国际标准。联合技术委员会通过的国际标准草案将分发给国家机构进行表决。作为国际标准的出版需要至少75%的国家机构投票批准。

请注意，本文件中的某些内容可能是专利权的对象。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合作编写。相同的文本以ITU-T.X.1631 (07/2015).

ITU-T

国际电信联盟的电信标准化部门

X.1631

(07/2015)

X系列。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的云服务信息安全控制实践准则

建议 ITU-T X.1631

ITU-T

International Telecommunication Union

ITU-T X系列建议

数据网络、开放系统通信和安全

公共数据网络	X.1-X.199
开放系统互连	X.200-X.299
网络之间的互通性	X.300-X.399
信息处理系统	X.400-X.499
目录	X.500-X.599
OSI网络和系统方面	X.600-X.699
OSI管理	X.700-X.799
安全性	X.800-X.849
OSI应用	X.850-X.899
开放式分布处理	X.900-X.999
信息和网络安全	
一般安全问题	X.1000-X.1029
网络安全	X.1030-X.1049
安全管理	X.1050-X.1069
远程生物计量学	X.1080-X.1099
安全的应用和服务	
多播安全	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
点对点的安全	X.1160-X.1169
联网的ID安全	X.1170-X.1179
IPTV安全	X.1180-X.1199
网络空间安全	
网络安全	X.1200-X.1229
反击垃圾邮件	X.1230-X.1249
身份管理	X.1250-X.1279
安全的应用和服务	
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
网络安全信息交流	
网络安全概述	X.1500-X.1519
脆弱性/状态交换	X.1520-X.1539
事件/事故/启发式交流	X.1540-X.1549
交流政策	X.1550-X.1559
启发式方法和信息请求	X.1560-X.1569
识别和发现	X.1570-X.1579
有保证的交换	X.1580-X.1589
云计算安全	
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准则	X.1640-X.1659
云计算安全实施	X.1660-X.1679
其他云计算安全	X.1680-X.1699

更多细节，请参考ITU-T建议列表。

国际标准 ISO/IEC 27017 建议 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准则

摘要

建议ITU-T X.1631 | ISO/IEC 27017提供了适用于提供和使用云服务的信息安全控制准则，提供。

- 为ISO/IEC 27002中规定的相关控制提供额外的实施指导。
- 额外的控制措施与实施指南，特别是与云服务有关的。

该建议-国际标准为云服务提供商和云服务客户提供控制和实施指导。

历史

版本	建议	审批	研究小组	独特的ID*
1.0	ITU-T X.1631	2015-07-14	17	11.1002/1000/12490

* 要访问该建议，请在您的网络浏览器地址栏中输入URL http://handle.itu.int/，然后再输入该建议的唯一ID。例如，http://handle.itu.int/11.1002/1000/11830-en。

序言

国际电信联盟（ITU）是联合国在电信、信息和通信技术（ICTs）领域的专门机构。ITU电信标准化部门（ITU-T）是ITU的一个常设机构。ITU-T负责研究技术、操作和关税问题，并就这些问题发布建议，以便在全球范围内实现电信标准化。

世界电信标准化大会（WTSA）每四年召开一次，确定ITU-T研究小组的研究主题，而这些研究小组又会就这些主题提出建议。

ITU-T建议的批准由WTSA第1号决议规定的程序涵盖。

在属于ITU-T职权范围的某些信息技术领域，必要的标准是在与ISO和IEC合作的基础上制定的。

注意事项

在本建议中，为简洁起见，使用了 "行政部门 "这一表述，以表示电信行政部门和公认的运营机构。

对本建议的遵守是自愿的。然而，本建议书可能包含某些强制性条款（以确保，例如，互操作性或适用性），当所有这些强制性条款得到满足时，就实现了对本建议书的遵守。词语 "应 "或其他一些强制性语言，如 "必须 "和否定的等价物，被用来表达要求。使用这些词语并不意味着要求任何一方遵守本建议书。

知识产权

国际电联提请注意，本建议的实施或执行可能涉及使用所主张的知识产权。国际电联对所声称的知识产权的证据、有效性或适用性不采取任何立场，无论这些知识产权是由国际电联成员还是建议制定过程之外的其他人所主张的。

截至本建议批准之日，国际电联尚未收到关于实施本建议可能需要的受专利保护的知识产权的通知。但是，实施者要注意，这可能不代表最新的信息，因此强烈要求查阅TSB专利数据库（http://www.itu.int/ITU-T/ipr/）。

目 录

简介

本建议-国际标准中包含的准则是对ISO/IEC 27002中给出的准则的补充和完善。

具体而言，本建议-
国际标准提供了支持云服务客户和云服务提供商实施信息安全控制的指南。有些指南是针对实施控制措施的云服务客户的，有些则是针对支持实施这些控制措施的云服务提供者的。选择适当的信息安全控制措施和应用所提供的实施指南，将取决于风险评估和任何法律、合同、监管或其他云行业特定的信息安全要求。

国际标准ITU-T建议

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准则

1 范围

本建议--国际标准为适用于提供和使用云服务的信息安全控制提供了指导方针。

- 为ISO/IEC 27002中规定的相关控制提供额外的实施指导。
- 额外的控制措施与实施指南，特别是与云服务有关的。

该建议-国际标准为云服务提供商和云服务客户提供控制和实施指导。

2 规范性参考资料

以下建议和国际标准所包含的条款，通过在本文本中的引用，构成了本建议和国际标准的条款。在出版时，所指明的版本是有效的。所有建议和标准都会被修订，鼓励基于本建议和国际标准达成协议的各方调查适用下列建议和标准的最新版本的可能性。IEC和ISO的成员保持着目前有效的国际标准的登记册。国际电联的电信标准化局有一份目前有效的国际电联建议的清单。

2.1 相同的建议 - 国际标准

- 建议ITU-T Y.3500（生效）| ISO/IEC 17788。(生效), *信息技术-云计算-概述和词汇。*
- 建议ITU-T Y.3502（生效）| ISO/IEC 17789：（生效），*信息技术-云计算-参考架构。*

2.2 其他参考资料

- ISO/IEC 27000：（生效），*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--信息安全控制的实践准则。*

3 定义和缩略语

3.1 其他地方定义的术语

在本建议中，ISO/IEC 27000、Rec.ISO/IEC 27000、Rec.ITU-T Y.3500|ISO/IEC 17788、Rec.ISO/IEC 17789和以下定义适用。

3.1.1 以下术语在ISO 19440中被定义。

- **能力**。能够进行特定活动的质量。

3.1.2 以下术语在ISO/IEC 27040中得到了定义。

- **数据泄露**。导致意外或非法破坏、丢失、更改、未经授权披露或访问传输、存储或以其他方式处理的受保护数据的安全妥协。
- **安全多租户**。多租户的类型，采用安全控制，明确防范数据泄露，并为适当的治理提供这些控制的验证。

  注1 - 当单个租户的风险状况不高于专用的单租户环境时，就存在安全多租户。

  注2 - 在非常安全的环境中，甚至租户的身份也是保密的。

3.1.3 以下术语在ISO/IEC 17203中被定义。

– **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、虚拟磁盘和与之相关的元数据的完全封装。虚拟机允许通过一个称为管理程序的软件层对底层物理机进行复用。

3.2 缩略语

在本建议-国际标准中，适用以下缩写。Iaa基础设施即服务

PaaSPlatformas a Service

PIIP个人可识别信息

SaaSS软件即服务

SLAS服务水平协议

VM虚拟机

4 云计算部门的具体概念

4.1 概述

由于计算资源的技术设计、运营和管理方式发生了重大变化，云计算的使用已经改变了组织应如何评估和减轻信息安全风险。本建议--国际标准在ISO/IEC
27002的基础上提供了额外的针对云计算的实施指导，并提供了额外的控制措施来解决针对云计算的信息安全威胁和风险考虑。

本建议-国际标准的用户应参考ISO/IEC
27002中的第5至18条，以了解控制、实施指导和其他信息。由于ISO/IEC
27002的普遍适用性，许多控制措施、实施指导和其他信息都适用于企业的一般情况和云计算背景。例如，ISO /IEC 27002的 "6.1.2 职责分离 "提供了一个控制，无论该组织是否作为云服务提供商，都可以应用。此外，云服务客户可以从同一控制中得出云环境中的职责分离要求，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 的延伸，本建议 -
国际标准进一步提供了云服务的具体控制措施、实施指南和其他信息（见第 4.5 条），旨在降低伴随云服务的技术和运营特点的风险（见附件 B）。云服务客户和云服务提供商可以参考 ISO/IEC 27002 和本建议-
国际标准，选择具有实施指南的控制措施，并在必要时添加其他控制措施。这一过程可以通过在使用或提供云服务的组织和业务背景下进行信息安全风险评估和风险处理来完成（见 4.4 条）。

4.2 云服务中的供应商关系

ISO/IEC 27002第15条 "供应商关系 "为管理供应商关系中的信息安全提供了控制、实施指导和其他信息。云服务的提供和使用是一种供应商关系，其中云服务客户是收购方，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者。

云服务客户和云服务提供者也可以形成一个供应链。假设一个云服务提供商提供一个基础设施能力类型的服务。此外，另一个云服务提供商可以提供一个应用能力类型的服务。在这种情况下，第二家云服务提供商相对于第一家而言是云服务客户，相对于使用其服务的云服务客户而言是云服务提供商。这个例子说明了本建议-
国际标准适用于作为云服务客户和云服务提供商的机构的情况。由于云服务客户和云服务提供商通过设计和实施云服务形成一个供应链，ISO/IEC 27002 的 "15.1.3 信息和通信技术供应链 "条款适用。

由多部分组成的国际标准ISO/IEC 27036 "*供应商关系的信息安全* "为产品和服务的获取者和供应商提供了关于供应商关系信息安全的详细指导。

ISO/IEC
27036第4部分直接处理供应商关系中的云服务安全问题。该标准也适用于作为收购方的云服务客户和作为供应商的云服务提供商。

4.3 云服务客户和云服务提供商之间的关系

在云计算环境中，云服务客户的数据是由云服务存储、传输和处理的。因此，云服务客户的业务流程可能取决于云服务的信息安全。如果没有对云服务的充分控制，云服务客户可能需要对其信息安全做法采取额外的预防措施。

在建立供应商关系之前，云服务客户需要选择云服务，同时考虑到云服务客户的信息安全要求和服务所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来管理云服务的使用。在这种关系中，云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要求。当云服务提供商提供的信息安全控制是预设的，且云服务客户无法更改时，云服务客户可能需要自己实施额外的控制来降低风险。

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备信息安全风险管理流程。建议他们参考ISO/IEC
27001，了解在其信息安全管理系统中进行风险管理的要求，并参考ISO/IEC
27005，了解关于信息安全风险管理本身的进一步指导。ISO/IEC 27001和ISO/IEC 27005所遵循的ISO 31000也有助于对风险管理的一般理解。

与信息安全风险管理流程的普遍适用性相比，云计算有其自身的风险源类型，包括威胁和漏洞，这些风险源来自其特点，例如，网络、系统的可扩展性和弹性、资源共享、自助式供应、按需管理、跨管辖区的服务供应，以及对控制措施实施的有限可见性。附件 B
提供了有关这些风险源以及提供和使用云服务的相关风险的参考信息。

本建议-国际标准的第 5 至 18 条和附件 A 中给出的控制和实施指导涉及云计算的具体风险源和风险。

4.5 本标准的结构

本建议书-国际标准的结构与ISO/IEC 27002相似。本建议书
| 国际标准包括ISO/IEC 27002的第5至18条，在每个条款和段落中说明其文本的适用性。

当ISO/IEC 27002中规定的目标和控制是适用的，不需要任何额外的信息时，只提供对ISO/IEC 27002的参考。

除 ISO/IEC 27002 中的目标外，如果还需要带有控制的目标或 ISO/IEC 27002 中的目标下的控制，它们将在规范性附件 A 中给出：云服务扩展控制集。当 ISO/IEC 27002 或本建议附件 A 的某项控制需要与该控制相关的额外云服务具体实施指导时，将在 **"云服务实施指导"**副标题下给出。该指导是以下列两种类型之一提供的。

当对云服务客户和云服务提供商有单独的指导时使用类型

1。当对云服务客户和云服务提供者的指导相同时，使用类型 2。**类型1**

云服务客户	云服务提供者

类型2

云服务客户	云服务提供者

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 信息安全政策

5.1 信息安全的管理方向

ISO/IEC 27002第5.1条中规定的目标适用。

5.1.1 信息安全的政策

ISO/IEC 27002中规定的控制5.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云计算的信息安全政策应被定义为云服务客户的特定主题政策。云服务客户的云计算信息安全政策应符合组织对其信息和其它资产的可接受的信息安全风险水平。 在确定云计算的信息安全政策时，云服务客户应考虑到以下因素。 – 存储在云计算环境中的信息可以被云服务提供商访问和管理。 – 资产可以在云计算环境中维护，例如，应用程序。 – 流程可以在多租户、虚拟化的云服务上运行。 – 云服务用户和他们使用云服务的背景。 – 拥有特权访问权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存储云服务客户数据的国家（即使是临时的）。	云服务提供商应加强其信息安全政策，以解决其云服务的提供和使用问题，并考虑到以下因素。 – 适用于云服务设计和实施的基线信息安全要求。 – 来自授权内部人员的风险。 – 多租户和云服务客户的隔离（包括虚拟化）。 – 云服务提供者的工作人员对云服务客户资产的访问。 – 访问控制程序，例如，对云服务的管理访问的强认证。 – 在变更管理期间与云服务客户的沟通。 – 虚拟化安全。 – 对云服务客户数据的访问和保护。 – 云服务客户账户的生命周期管理。 – 违规行为的沟通和信息共享准则，以帮助调查和取证。

云服务的其他信息

云服务客户的云计算信息安全政策是ISO/IEC 27002 5.1.1中描述的特定主题政策之一。一个组织的信息安全政策涉及其信息和业务流程。当一个组织使用云服务时，它可以作为云服务客户拥有云计算的政策。一个组织的信息可以在云计算环境中存储和维护，而业务流程可以在云计算环境中运行。在最高级别的信息安全政策中规定的一般信息安全要求，在云计算的政策中得到遵循。

与此相反，提供云服务的信息安全政策涉及云服务客户的信息和业务流程，而不是云服务提供者的信息和业务流程。提供云服务的信息安全要求应满足潜在的云服务客户的要求。因此，它们可能与云服务提供者的信息和业务流程的信息安全要求不一致。信息安全政策的范围通常是根据服务来定义的，但并不完全由组织结构或物理位置来定义。

云计算有几个虚拟化安全方面，包括虚拟实例的生命周期管理、虚拟化图像的存储和访问控制、休眠或离线虚拟实例的处理、快照、管理程序的保护以及管理自助服务门户使用的安全控制。

5.1.2 对信息安全政策的审查

ISO/IEC 27002中规定的控制5.1.2和相关实施指南及其他信息适用。

6 信息安全的组织

6.1 内部组织

ISO/IEC 27002第6.1条中规定的目标适用。

6.1.1 信息安全角色和责任

ISO/IEC 27002中规定的控制6.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应与云服务提供商就信息安全角色和责任的适当分配达成一致，并确认其能够履行 所分配的角色和责任。双方的信息安全角色和责任应在协议中说明。 云服务客户应确定并管理其与云服务提供商的客户支持和护理功能的关系。	云服务提供商应与其云服务客户、其云服务提供商和供应商商定并记录适当的信息安全角色和责任分配。

云服务的其他信息

即使在各方内部和之间确定了责任，云服务客户也要对使用服务的决定负责。该决定应根据云服务客户的组织内确定的角色和责任作出。云服务提供商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根据云服务提供商组织内确定的角色和责任进行。

角色以及与数据所有权、访问控制和基础设施维护等问题相关的责任界定和分配上的模糊不清，可能会引起商业或法律纠纷，特别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，对服务的安全运行、恢复和连续性可能至关重要。所有资产的所有权，以及对与这些资产相关的操作（如备份和恢复操作）负有责任的各方，都应加以定义和记录。否则，就会出现云服务提供商认为云服务客户执行这些重要任务的风险（反之亦然），并可能发生数据丢失。

6.1.2 职责分离

ISO/IEC 27002中规定的控制6.1.2和相关实施指南及其他信息适用。

6.1.3 与当局联系

ISO/IEC 27002中规定的控制6.1.3和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应确定与云服务客户和云服务提供商的联合运营有关的机构。	云服务提供商应告知云服务客户云服务提供商机构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。

云服务的其他信息

有关可存储、处理或传输云服务客户数据的地理位置的信息可帮助云服务客户确定监管机构和管辖区。

6.1.4 与特殊利益集团的联系

ISO/IEC 27002中规定的控制6.1.4和相关实施指南及其他信息适用。

6.1.5 项目管理中的信息安全

ISO/IEC 27002中规定的控制6.1.5和相关实施指南及其他信息适用。

6.2 移动设备和远程办公

ISO/IEC 27002第6.2条中规定的目标适用。

6.2.1 移动设备政策

ISO/IEC 27002中规定的控制6.2.1和相关实施指南及其他信息适用。

6.2.2 远程办公

ISO/IEC 27002中规定的控制6.2.2和相关实施指南及其他信息适用。

7 人力资源安全

7.1 就业前

ISO/IEC 27002第7.1条中规定的目标适用。

7.1.1 筛选

ISO/IEC 27002中规定的控制7.1.1和相关实施指南及其他信息适用。

7.1.2 就业条款和条件

ISO/IEC 27002中规定的控制7.1.2和相关实施指南及其他信息适用。

7.2 就业期间

ISO/IEC 27002第7.2条中规定的目标适用。

7.2.1 管理责任

ISO/IEC 27002中规定的控制7.2.1和相关实施指南及其他信息适用。

7.2.2 信息安全意识、教育和培训

ISO/IEC 27002中规定的控制7.2.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
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）的宣传、教育和培训计划中增加以下项目。 – 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。 – 使用云服务的系统和网络环境风险。 – 适用的法律和法规考虑。	云服务提供商应向员工提供有关适当处理云服务客户数据和云服务衍生数据的认识、教育和培训，并要求承包商也这样做。这种数据可能包含对云服务客户保密的信息，或者受到云服务提供商访问和使用的特定限制，包括监管限制。

云服务客户	云服务提供者
应向管理层和监督管理人员（包括业务部门的管理人员）提供有关云服务的信息安全意识、教育和培训计划。这些努力支持信息安全活动的有效协调。	

7.2.3 纪律处分程序

ISO/IEC 27002中规定的控制7.2.3和相关实施指南及其他信息适用。

7.3 终止和改变就业

ISO/IEC 27002第7.3条中规定的目标适用。

7.3.1 终止或改变就业责任

ISO/IEC 27002中规定的控制7.3.1和相关实施指南及其他信息适用。

8 资产管理

8.1 对资产的责任

ISO/IEC 27002第8.1条中规定的目标适用。

8.1.1 资产盘点

ISO/IEC 27002中规定的控制8.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户的资产清单应说明存储在云计算环境中的信息和相关资产。清单的记录应说明资产的维护地点，例如，云服务的标识。	云服务提供者的资产清单应明确指出。 – 云服务客户数据。 – 云服务衍生的数据。

云服务的其他信息

有一些云服务应用通过向云服务客户数据添加云服务衍生数据，提供管理信息的功能。将这种云服务衍生数据识别为资产并在资产清单中维护它们，有助于提高信息安全。

8.1.2 资产的所有权

ISO/IEC 27002中规定的控制8.1.2和相关实施指南及其他信息适用。

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）或基础设施即服务（IaaS）服务时，应用软件将属于云服务客户，而对于软件即服务（SaaS）服务，应用软件将属于云服务提供者。

8.1.3 可接受的资产使用

ISO/IEC 27002中规定的控制8.1.3和相关实施指南及其他信息适用。

8.1.4 资产的回报

ISO/IEC 27002中规定的控制8.1.4和相关实施指南及其他信息适用。

8.2 信息分类

ISO/IEC 27002第8.2条中规定的目标适用。

8.2.1 信息的分类

ISO/IEC 27002中规定的控制8.2.1和相关实施指南及其他信息适用。

8.2.2 信息的标示

ISO/IEC 27002中规定的控制8.2.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应根据云服务客户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。如果适用，可采用云服务提供商提供的支持贴标的功能。	云服务提供商应记录并披露其提供的任何服务功能，允许云服务客户对其信息和相关资产进行分类和标记。

8.2.3 资产的处理

ISO/IEC 27002中规定的8.2.3控制和相关实施指南及其他信息适用。

8.3 媒体处理

ISO/IEC 27002第8.3条中规定的目标适用。

8.3.1 对可移动媒体的管理

ISO/IEC 27002中规定的控制8.3.1和相关实施指南及其他信息适用。

8.3.2 媒介的处置

ISO/IEC 27002中规定的控制8.3.2和相关实施指南及其他信息适用。

8.3.3 物理介质传输

ISO/IEC 27002中规定的8.3.3控制和相关实施指南及其他信息适用。

9 访问控制

9.1 访问控制的业务要求

ISO/IEC 27002第9.1条中规定的目标适用。

9.1.1 访问控制政策

ISO/IEC 27002中规定的控制9.1.1和相关实施指南及其他信息适用。

9.1.2 访问网络和网络服务

ISO/IEC 27002中规定的控制9.1.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户使用网络服务的访问控制政策应规定用户对所使用的每个单独的云服务的访问要求。	(没有额外的实施指导)

9.2 用户访问管理

ISO/IEC 27002第9.2条中规定的目标适用。

9.2.1 用户注册和取消注册

ISO/IEC 27002中规定的控制9.2.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
(没有额外的实施指导)	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取消注册的功能，以及使用这些功能的规范。

9.2.2 用户访问规定

ISO/IEC 27002中规定的控制9.2.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
(没有额外的实施指导)	云服务提供商应提供管理云服务客户的云服务用户访问权限的功能，以及这些功能的使用规范。

云服务的其他信息

云服务提供商应支持其云服务和相关管理界面的第三方身份和访问管理技术。这些技术可以使云服务客户的系统与云服务之间更容易整合，更容易进行用户身份管理，并且可以方便使用多种云服务，支持单点登录等功能。

9.2.3 特权访问权限的管理

ISO/IEC 27002中规定的控制9.2.3和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应使用足够的认证技术（例如，多因素认证），根据已识别的风险对云服务客户的云服务管理员进行认证，以获得云服务的管理能力。	云服务提供商应根据确定的风险提供足够的认证技术，以验证云服务客户的云服务管理员对云服务的管理能力。例如，云服务提供商可以提供多因素认证功能，或支持使用第三方多因素认证机制。

9.2.4 管理用户的秘密认证信息

ISO/IEC 27002中规定的控制9.2.4和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应验证云服务提供商分配秘密认证信息（如密码）的管理程序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认证信息的程序信息，包括分配此类信息和用户认证的程序。

云服务的其他信息

云服务客户应通过使用其自身或第三方身份和访问管理技术控制秘密认证信息的管理。

9.2.5 对用户访问权限的审查

ISO/IEC 27002中规定的控制9.2.5和相关实施指南及其他信息适用。

9.2.6 撤销或调整访问权

ISO/IEC 27002中规定的控制9.2.6和相关实施指南及其他信息适用。

9.3 用户责任

ISO/IEC 27002第9.3条中规定的目标适用。

9.3.1 使用秘密认证信息

ISO/IEC 27002中规定的控制9.3.1和相关实施指南及其他信息适用。

9.4 系统和应用访问控制

ISO/IEC 27002第9.4条中规定的目标适用。

9.4.1 信息访问限制

ISO/IEC 27002中规定的控制9.4.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应确保可根据其访问控制政策限制对云服务中信息的访问，并确保此类限制得以实现。这包括限制对云服务、云服务功能和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，使云服务客户能够限制对其云服务、其云服务功能和服务中保存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额外领域。作为云服务或云服务功能的一部分，对功能和服务的访问，如管理程序管理功能和管理控制台，可能需要额外的访问控制。

9.4.2 安全登录程序

ISO/IEC 27002中规定的控制9.4.2和相关实施指南及其他信息适用。

9.4.3 密码管理系统

ISO/IEC 27002中规定的控制9.4.3和相关实施指南及其他信息适用。

9.4.4 使用有特权的实用程序

ISO/IEC 27002中规定的控制9.4.4和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
在允许使用实用程序的情况下，云服务客户应确定将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。	云服务提供商应确定对云服务中使用的任何实用程序的要求。 云服务提供商应确保任何能够绕过正常操作或安全程序的实用程序的使用都严格限于授权人员，并且定期审查和审计此类程序的使用。

9.4.5 对程序源代码的访问控制

ISO/IEC 27002中规定的控制9.4.5和相关实施指南及其他信息适用。

10 密码学

10.1 加密控制

ISO/IEC 27002第10.1条中规定的目标适用。

10.1.1 关于使用加密控制的政策

ISO/IEC 27002中规定的控制10.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
如果风险分析认为合理，云服务客户应针对其对云服务的使用实施加密控制。这些控制措施应具有足够的强度，以减轻已确定的风险，无论这些控制措施是由云服务客户还是由云服务提供商提供。 当云服务提供商提供加密技术时，云服务客户应审查云服务提供商提供的任何信息，以确认加密能力是否。 – 满足云服务客户的政策要求。 – 与云服务客户使用的任何其他加密保护兼容。 – 适用于静止的数据和在云服务中传输的数据，以及从云服务中传输的数据。	云服务提供商应向云服务客户提供有关其使用加密技术保护所处理信息的情况的信息。云服务提供商还应向云服务客户提供信息，介绍其提供的可协助云服务客户应用其自身加密保护的任何功能。

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种类的信息，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 关键管理

ISO/IEC 27002中规定的控制10.1.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应确定每个云服务的加密密钥，并实施密钥管理程序。 如果云服务提供密钥管理功能供云服务客户使用，云服务客户应要求提供以下信息，说明用于管理与云服务相关的密钥的程序。 – 键的类型。 – 钥匙管理系统的规格，包括钥匙生命周期的每个阶段的程序，即生成、改变或更新、储存、退役、检索、保留和销毁。 – 建议云服务客户使用的密钥管理程序。 当云服务客户采用自己的密钥管理或单独的、不同的密钥管理服务时，云服务客户不应允许云服务提供者存储和管理用于加密操作的加密密钥。	(没有额外的实施指导)

11 物理和环境安全

11.1 安全区域

ISO/IEC 27002第11.1条中规定的目标适用。

11.1.1 物理安全边界

ISO/IEC 27002中规定的控制11.1.1和相关实施指南及其他信息适用。

11.1.2 实际进入控制

ISO/IEC 27002中规定的控制11.1.2和相关实施指南及其他信息适用。

11.1.3 确保办公室、房间和设施的安全

ISO/IEC 27002中规定的控制11.1.3和相关实施指南及其他信息适用。

11.1.4 防范外部和环境威胁

ISO/IEC 27002中规定的控制11.1.4和相关实施指南及其他信息适用。

11.1.5 在安全区域工作

ISO/IEC 27002中规定的控制11.1.5和相关实施指南及其他信息适用。

11.1.6 交付和装载区域

ISO/IEC 27002中规定的控制11.1.6和相关实施指南及其他信息适用。

11.2 装备

ISO/IEC 27002第11.2条中规定的目标适用。

11.2.1 设备选址和保护

ISO/IEC 27002中规定的控制11.2.1和相关实施指南及其他信息适用。

11.2.2 支持公用事业

ISO/IEC 27002中规定的控制11.2.2和相关实施指南及其他信息适用。

11.2.3 布线的安全性

ISO/IEC 27002中规定的控制11.2.3和相关实施指南及其他信息适用。

11.2.4 设备维护

ISO/IEC 27002中规定的控制11.2.4和相关实施指南及其他信息适用。

11.2.5 移除资产

ISO/IEC 27002中规定的控制11.2.5和相关实施指南及其他信息适用。

11.2.6 院外设备和资产的安全

ISO/IEC 27002中规定的控制11.2.6和相关实施指南及其他信息适用。

11.2.7 安全处置或重新使用设备

ISO/IEC 27002中规定的控制11.2.7和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求确认云服务提供商拥有安全处置或重新使用资源的政策和程序。	云服务提供商应确保为及时安全地处置或重新使用资源（例如，设备、数据存储、文件、内存）做出安排。

云服务的其他信息

关于安全处置的其他信息可以在ISO/IEC 27040中找到。

11.2.8 无人看管的用户设备

ISO/IEC 27002中规定的控制11.2.8和相关实施指南及其他信息适用。

11.2.9 清理桌面和清理屏幕政策

ISO/IEC 27002中规定的控制11.2.9和相关实施指南及其他信息适用。

12 业务安全

12.1 业务程序和责任

ISO/IEC 27002第12.1条中规定的目标适用。

12.1.1 文件化的操作程序

ISO/IEC 27002中规定的控制12.1.1和相关实施指南及其他信息适用。

12.1.2 变革管理

ISO/IEC 27002中规定的控制12.1.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户的变更管理流程应考虑到云服务提供商做出的任何变更的影响。	云服务提供商应向云服务客户提供有关可能对云服务产生不利影响的云服务变更的信息。以下内容将帮助云服务客户确定变更对信息安全可能产生的影响。 – 变化的类别。 – 变化的计划日期和时间。 – 对云服务和基础系统变化的技术描述。 – 变化的开始和完成的通知。 当云服务提供商提供的云服务依赖于对等云服务提供商时，那么云服务提供商可能需要通知云服务客户由对等云服务提供商引起的变化。

云服务的其他信息

通知中应包括的项目清单可以在协议中确定，例如，主服务协议或服务水平协议（SLA）。

12.1.3 能力管理

ISO/IEC 27002中规定的控制12.1.3和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应确保云服务所提供的商定容量符合云服务客户的要求。 云服务客户应监测云服务的使用情况，并预测其容量需求，以确保云服务在一段时间内的性能。	云服务提供商应监测总的资源容量，以防止因资源短缺造成的信息安全事件。

云服务的其他信息

云服务涉及由云服务提供商控制的资源，并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、可扩展和按需分配通常会增加服务的总容量。然而，云服务客户应该意识到，所提供的资源可能有容量限制。容量限制的例子包括一个应用程序的处理器核心数量、可用的存储量或可用的网络带宽。

这些约束条件可根据云服务客户购买的特定云服务或特定订阅而有所不同。如果云服务客户的要求超过限制条件，云服务客户可能需要改变云服务或改变订阅。

为了让云服务客户对云服务进行容量管理，云服务客户应能获得有关资源使用的相关统计数据，如：。

- 特定时间段的统计数据。
- 资源使用的最大水平。

12.1.4 开发、测试和运行环境的分离

ISO/IEC 27002中规定的控制12.1.4和相关实施指南及其他信息适用。

12.2 防范恶意软件

ISO/IEC 27002第12.2条中规定的目标适用。

12.2.1 对恶意软件的控制

ISO/IEC 27002中规定的控制12.2.1和相关实施指南及其他信息适用。

12.3 备份

ISO/IEC 27002第12.3条中规定的目标适用。

12.3.1 信息备份

ISO/IEC 27002中规定的控制12.3.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
如果云服务提供商将备份功能作为云服务的一部分，云服务客户应向云服务提供商索取备份功能的规格。云服务客户还应该验证它们是否符合其备份要求。 当云服务提供商不提供备份功能时，云服务客户应负责实施备份功能。	云服务提供商应向云服务客户提供其备份能力的规格。该规格应酌情包括以下信息。 – 备份的范围和时间表。 – 备份方法和数据格式，包括加密，如果相关的话。 – 备份数据的保留期。 – 核实备份数据完整性的程序。 – 从备份中恢复数据所涉及的程序和时间尺度。 – 程序来测试备份能力。 – 备份的存储位置。 如果向云服务客户提供虚拟快照等备份服务，云服务提供商应提供安全和隔离的访问。

云服务的其他信息

在云计算环境中进行备份的责任分配通常并不明确。在IaaS的情况下，进行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它有责任对云计算系统中产生的所有云服务客户数据进行备份，例如使用PaaS服务的开发功能产生的可执行文件。

注意
不同级别的备份和恢复可能作为一项服务提供，需要额外的费用，在这种情况下，云服务客户可以选择备份的内容和时间。

12.4 记录和监测

ISO/IEC 27002第12.4条中规定的目标适用。

12.4.1 事件记录

ISO/IEC 27002中规定的控制12.4.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应定义其对事件记录的要求，并验证云服务是否满足这些要求。	云服务提供商应向云服务客户提供日志记录功能。

云服务的其他信息

云服务客户和云服务提供商对事件记录的责任因所使用的云服务类型而异。例如，对于IaaS，云服务提供商的记录责任可能仅限于云计算基础设施组件的记录，而云服务客户可能负责记录其自己的虚拟机和应用程序的事件。

12.4.2 保护日志信息

ISO/IEC 27002中规定的控制12.4.2和相关实施指南及其他信息适用。

12.4.3 管理员和操作员日志

ISO/IEC 27002中规定的控制12.4.3和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
如果特权操作被委托给云服务客户，应记录这些操作的操作和性能。云服务客户应确定云服务提供商提供的日志记录功能是否合适，或者云服务客户是否应实施额外的日志记录功能。	(没有额外的实施指导)

云服务的其他信息

云服务客户和云服务提供商之间的责任分配（见 6.1.1 条）应涵盖与云服务相关的特权操作。监测和记录特权操作的使用是必要的，以支持针对不正确使用这些操作的预防和纠正措施。

12.4.4 时钟同步

ISO/IEC 27002中规定的控制12.4.4和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求提供有关云服务提供商的系统所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有关云服务提供商系统使用的时钟的信息，以及有关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云服务提供商的系统的时钟同步，后者运行云服务客户使用的云服务。如果没有这种同步，就很难将云服务客户的系统上的事件与云服务提供商的系统上的事件进行协调。

12.5 操作软件的控制

ISO/IEC 27002第12.5条中规定的目标适用。

12.5.1 在业务系统上安装软件

ISO/IEC 27002中规定的控制12.5.1和相关实施指南及其他信息适用。

12.6 技术漏洞管理

ISO/IEC 27002第12.6条中规定的目标适用。

12.6.1 技术漏洞的管理

ISO/IEC 27002中规定的控制12.6.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求云服务提供商提供有关管理可能影响所提供云服务的技术漏洞的信息。云服务客户应确定其将负责管理的技术漏洞，并明确规定管理这些漏洞的流程。	云服务提供商应向云服务客户提供有关管理可能影响所提供的云服务的技术漏洞的信息。

12.6.2 对软件安装的限制

ISO/IEC 27002中规定的控制12.6.2和相关实施指南及其他信息适用。

12.7 信息系统审计的考虑

ISO/IEC 27002第12.7条中规定的目标适用。

12.7.1 信息系统审计控制

ISO/IEC 27002中规定的控制12.7.1和相关实施指南及其他信息适用。

13 通信安全

13.1 网络安全管理

ISO/IEC 27002第13.1条中规定的目标适用。

13.1.1 网络控制

ISO/IEC 27002中规定的控制13.1.1和相关实施指南及其他信息适用。

13.1.2 网络服务的安全性

ISO/IEC 27002中规定的控制13.1.2和相关实施指南及其他信息适用。

13.1.3 网络中的隔离

ISO/IEC 27002中规定的控制13.1.3和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
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。	云服务提供商应在以下情况下执行网络访问隔离。 – 在一个多租户环境中，租户之间的隔离。 – 云服务提供者的内部管理环境和云服务客户的云计算环境之间的隔离。 在适当情况下，云服务提供商应帮助云服务客户验证云服务提供商实施的隔离措施。

云服务的其他信息

法律和法规可以要求对网络进行隔离或对网络流量进行隔离。

13.2 信息传输

ISO/IEC 27002第13.2条中规定的目标适用。

13.2.1 信息传输政策和程序

ISO/IEC 27002中规定的控制13.2.1和相关实施指南及其他信息适用。

13.2.2 关于信息传输的协议

ISO/IEC 27002中规定的控制13.2.2和相关实施指南及其他信息适用。

13.2.3 电子信息传递

ISO/IEC 27002中规定的控制13.2.3和相关实施指南及其他信息适用。

13.2.4 保密或不披露协议

ISO/IEC 27002中规定的控制13.2.4和相关实施指南及其他信息适用。

14 系统获取、开发和维护

14.1 信息系统的安全要求

ISO/IEC 27002第14.1条中规定的目标适用。

14.1.1 信息安全要求分析和规范

ISO/IEC 27002中规定的控制14.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应确定其对云服务的信息安全要求，然后评估云服务提供商提供的服务是否能满足这些要求。 为了进行这种评估，云服务客户应要求云服务提供商提供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其使用的信息安全能力的信息。这种信息应该是信息性的，而不披露可能对有恶意的人有用的信息。

云服务的其他信息

应注意限制披露有关安全控制的实施细节，因为它们与正在提供的云服务有关，而这些云服务客户或潜在的云服务客户已签订保密协议。

14.1.2 确保公共网络上的应用服务安全

ISO/IEC 27002中规定的控制14.1.2和相关实施指南及其他信息适用。

14.1.3 保护应用服务交易

ISO/IEC 27002中规定的控制14.1.3和相关实施指南及其他信息适用。

14.2 开发和支持过程中的安全问题

ISO/IEC 27002第14.2条中规定的目标适用。

14.2.1 安全的发展政策

ISO/IEC 27002中规定的控制14.2.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求云服务提供商提供有关云服务提供商使用安全开发程序和做法的信息。	云服务提供商应在符合其披露政策的范围内提供有关其使用安全开发程序和实践的信息。

云服务的其他信息

云服务提供商的安全开发程序和实践对SaaS来说可能是至关重要的。

14.2.2 系统变更控制程序

ISO/IEC 27002中规定的控制14.2.2和相关实施指南及其他信息适用。

14.2.3 操作平台改变后的应用程序的技术审查

ISO/IEC 27002中规定的控制14.2.3和相关实施指南及其他信息适用。

14.2.4 对软件包更改的限制

ISO/IEC 27002中规定的控制14.2.4和相关实施指南及其他信息适用。

14.2.5 安全系统工程原则

ISO/IEC 27002中规定的控制14.2.5和相关实施指南及其他信息适用。

14.2.6 安全的开发环境

ISO/IEC 27002中规定的控制14.2.6和相关实施指南及其他信息适用。

14.2.7 外包开发

ISO/IEC 27002中规定的控制14.2.7和相关实施指南及其他信息适用。

14.2.8 系统安全测试

ISO/IEC 27002中规定的控制14.2.8和相关实施指南及其他信息适用。

14.2.9 系统验收测试

ISO/IEC 27002中规定的控制14.2.9和相关实施指南及其他信息适用。

云服务的其他信息

在云计算中，系统验收测试的指导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条中规定的目标适用。

14.3.1 测试数据的保护

ISO/IEC 27002中规定的控制14.3.1和相关实施指南及其他信息适用。

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条中规定的目标适用。

15.1.1 供应商关系的信息安全政策

ISO/IEC 27002中规定的控制15.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应在其供应商关系的信息安全政策中将云服务提供商作为一种类型的供应商。这将有助于降低与云服务提供商对云服务客户数据的访问和管理有关的风险。	(没有额外的实施指导)

15.1.2 解决供应商协议中的安全问题

ISO/IEC 27002中规定的控制15.1.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应确认与云服务有关的信息安全角色和责任，如服务协议中所述。这些可以包括以下流程。 – 恶意软件保护。 – 备份。 – 加密控制。 – 脆弱性管理。 – 事件管理。 – 技术合规性检查。 – 安全测试。 – 审计。 – 收集、维护和保护证据，包括日志和审计跟踪。 – 服务协议终止时的信息保护。 – 认证和访问控制。 – 身份和访问管理。	作为协议的一部分，云服务提供商应明确规定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措施可根据云服务客户使用的云服务类型而有所不同。

15.1.3 信息和通信技术供应链

ISO/IEC 27002中规定的控制15.1.3和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
(没有额外的实施指导)	如果云服务提供商使用同行云服务提供商的云服务，云服务提供商应确保对自己的云服务客户的信息安全水平得到保持或超过。 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实现该目标。

15.2 供应商服务交付管理

ISO/IEC 27002第15.2条中规定的目标适用。

15.2.1 对供应商服务的监测和审查

ISO/IEC 27002中规定的控制15.2.1和相关实施指南及其他信息适用。

15.2.2 管理供应商服务的变化

ISO/IEC 27002中规定的控制15.2.2和相关实施指南及其他信息适用。

16 信息安全事件管理

16.1 信息安全事件的管理和改进

ISO/IEC 27002第16.1条中规定的目标适用。

16.1.1 责任和程序

ISO/IEC 27002中规定的控制16.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应核实信息安全事件管理的责任分配，并应确保其符合云服务客户的要求。	作为服务规范的一部分，云服务提供商应定义云服务客户和云服务提供商之间的信息安全事故管理责任和程序的分配。 云服务提供商应向云服务客户提供涵盖以下内容的文件。 – 云服务提供商将向云服务客户报告的信息安全事件的范围。 – 信息安全事件的检测和相关反应的披露程度。 – 信息安全事件通知的目标时间框架。 – 信息安全事件的通知程序。 – 处理与信息安全事件有关的问题的联系信息。 – 如果发生某些信息安全事件，可适用的任何补救措施。

16.1.2 报告信息安全事件

ISO/IEC 27002中规定的控制16.1.2和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求云服务提供商提供关于以下机制的信息。 – 云服务客户向云服务提供者报告其检测到的信息安全事件。 – 云服务提供者接收关于云服务提供者检测到的信息安全事件的报告。 – 云服务客户跟踪报告的信息安全事件的状态。	云服务提供者应提供以下机制。 – 云服务客户向云服务提供商报告一个信息安全事件。 – 云服务提供商向云服务客户报告一个信息安全事件。 – 云服务客户跟踪报告的信息安全事件的状态。

云服务的其他信息

这些机制不仅要定义程序，还要给出云服务客户和云服务提供者的联系电话、电子邮件地址和服务时间等基本信息。

信息安全事件可由云服务客户或云服务提供商检测到。因此，与云计算有关的主要额外责任是，检测事件的一方应该有程序立即向另一方报告该事件。

16.1.3 报告信息安全的弱点

ISO/IEC 27002中规定的控制16.1.3和相关实施指南及其他信息适用。

16.1.4 对信息安全事件的评估和决定

ISO/IEC 27002中规定的控制16.1.4和相关实施指南及其他信息适用。

16.1.5 对信息安全事件的反应

ISO/IEC 27002中规定的控制16.1.5和相关实施指南及其他信息适用。

16.1.6 从信息安全事件中学习

ISO/IEC 27002中规定的控制16.1.6和相关实施指南及其他信息适用。

16.1.7 收集证据

ISO/IEC 27002中规定的控制16.1.7和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户和云服务提供商应商定程序，对来自云计算环境内的潜在数字证据或其他信息的请求作出回应。	

17 业务连续性管理的信息安全问题

17.1 信息安全的连续性

ISO/IEC 27002第17.1条中规定的目标适用。

17.1.1 规划信息安全的连续性

ISO/IEC 27002中规定的控制17.1.1和相关实施指南及其他信息适用。

17.1.2 实施信息安全的连续性

ISO/IEC 27002中规定的控制17.1.2和相关实施指南及其他信息适用。

17.1.3 核实、审查和评估信息安全的连续性

ISO/IEC 27002中规定的控制17.1.3和相关实施指南及其他信息适用。

17.2 裁员

ISO/IEC 27002第17.2条中规定的目标适用。

17.2.1 信息处理设施的可用性

ISO/IEC 27002中规定的控制17.2.1和相关实施指南及其他信息适用。

18 遵守规定

18.1 遵守法律和合同的要求

ISO/IEC 27002第18.1条中规定的目标适用。

18.1.1 确定适用的立法和合同要求

ISO/IEC 27002中规定的控制18.1.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应考虑的问题是，除了管辖云服务客户的法律和法规外，相关法律和法规也可能是管辖云服务提供者的法律和法规。 云服务客户应要求提供云服务提供商符合云服务客户的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计师出具的证明。	云服务提供商应告知云服务客户有关管理云服务的法律管辖区。 云服务提供商应确定其自身的相关法律要求（例如，关于加密以保护个人身份信息（PII））。该信息也应根据要求提供给云服务客户。 云服务提供商应向云服务客户提供其目前遵守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监管要求，特别是在处理、存储和通信能力在地理上分布以及可能涉及多个司法管辖区的情况下。

必须注意的是，合规性要求，无论是法律还是合同，仍然是云服务客户的责任。合规责任不能转移到云服务提供者身上。

18.1.2 知识产权

ISO/IEC 27002中规定的控制18.1.2和相关的实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
在云服务中安装商业许可的软件可能会导致违反该软件的许可条款。在允许在云服务中安装任何授权软件之前，云服务客户应该有一个程序来确定云的具体许可要求。应特别注意以下情况：云服务具有弹性和可扩展性，软件可在超过许可条款所允许的系统或处理器核心上运行。	云服务提供商应建立一个响应知识产权投诉的流程。

18.1.3 记录的保护

ISO/IEC 27002中规定的控制18.1.3和相关的实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求云服务提供商提供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 个人身份信息的隐私和保护

ISO/IEC 27002中规定的控制18.1.4和相关实施指南及其他信息适用。

云服务的其他信息

ISO/IEC 27018，作为PII处理者的公共云中的PII保护实践守则，提供了关于这个主题的额外信息。

18.1.5 加密控制的监管

ISO/IEC 27002中规定的控制18.1.5和相关的实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应核实适用于使用云服务的一套加密控制措施符合相关协议、立法和法规。	云服务提供商应向云服务客户提供关于云服务提供商实施的加密控制的描述，以审查是否符合适用的协议、立法和法规。

18.2 信息安全审查

ISO/IEC 27002第18.2条中规定的目标适用。

18.2.1 信息安全的独立审查

ISO/IEC 27002中规定的控制18.2.1和相关实施指南及其他信息适用。以下特定部门的指南也适用。

云服务的实施指南

云服务客户	云服务提供者
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和准则的实施符合云服务提供商的任何声明。此类证据可包括根据相关标准进行的认证。	云服务提供商应向云服务客户提供书面证据，以证实其实施信息安全控制的说法。 如果对单个云服务客户的审计不切实际或会增加信息安全的风险，云服务提供商应提供独立证据，证明信息安全是按照云服务提供商的政策和程序实施和运行的。这应在签订合同前提供给潜在的云服务客户。由云服务提供商选择的相关独立审计通常应是一种可接受的方法，以满足云服务客户对审查云服务提供商运营情况的兴趣，前提是提供足够的透明度。当独立审计不可行时，云服务提供商应进行自我评估，并向云服务客户披露其过程和结果。

18.2.2 遵守安全政策和标准

ISO/IEC 27002中规定的控制18.2.2和相关实施指南及其他信息适用。

18.2.3 技术合规性审查

ISO/IEC 27002中规定的控制18.2.3和相关实施指南及其他信息适用。

附件A

云服务扩展控制集

(本附件构成本建议-国际标准的一个组成部分)。

本附件提供额外的控制目标、控制和实施指导，作为云服务的扩展控制集。与这些控制措施相关的 ISO/IEC 27002 控制目标不再重复。

一个打算在符合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，应通过包括本附件中所述的控制措施来扩展其适用性声明（SOA）。

CLD.6.3 云服务客户与云服务提供者之间的关系

目标。澄清云服务客户和云服务提供商之间在信息安全管理方面的共同角色和责任关系。

CLD.6.3.1 云计算环境中的共享角色和责任

控制

在使用云服务的过程中，共享信息安全角色的责任应分配给已确定的各方，并由云服务客户和云服务提供商进行记录、沟通和实施。

云服务的实施指南

云服务客户	云服务提供者
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政策和程序，并使云服务用户了解他们在使用云服务中的角色和责任。	云服务提供商应记录并交流其使用云服务的信息安全能力、角色和责任，以及云服务客户在使用云服务时需要实施和管理的信息安全角色和责任。

云服务的其他信息

在云计算中，角色和责任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。角色和责任的分配应考虑到云服务客户的数据和云服务客户的应用，因为云服务提供商是其监护人。

CLD.8.1 对资产的责任

ISO/IEC 27002 第 8.1 条中规定的目标适用。

CLD.8.1.5 云服务客户资产控制

云服务客户在云服务提供商处所的资产应被移除，并在以下情况下归还
必要时，在云服务协议终止时及时进行。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求提供关于终止服务流程的书面说明，包括归还和移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，并记录终止服务的时间表，这应及时发生。	云服务提供商应提供信息，说明在使用云服务的协议终止后，归还和移除任何云服务客户的资产的安排。 资产归还和移除安排应在协议中记录下来，并应及时执行。这些安排应明确规定要归还和移除的资产。

CLD.9.5 共享虚拟环境中的云服务客户数据的访问控制

目标。在使用云计算的共享虚拟环境时减轻信息安全风险。

CLD.9.5.1虚拟计算环境中的 隔离

控制

云服务客户在云服务上运行的虚拟环境应受到保护，免受其他云服务的影响。
导致客户和未经授权的人的损失。

云服务的实施指南

云服务客户	云服务提供者
(没有额外的实施指导)	云服务提供商应该对云服务客户数据、虚拟化应用、操作系统、存储和网络进行适当的逻辑隔离。 – 云服务客户在多租户环境中使用的资源的分离。 – 将云服务提供商的内部管理与云服务客户使用的资源分开。 如果云服务涉及多租户，云服务提供商应实施信息安全控制，以确保不同租户使用的资源得到适当隔离。 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带来的风险。

云服务的其他信息

逻辑隔离的实施取决于应用于虚拟化的技术。

– 当软件虚拟化功能提供一个虚拟环境（例如，虚拟操作系统）时，网络和存储配置可以被虚拟化。此外，软件虚拟化环境中的云服务客户的隔离可以使用软件的隔离功能来设计和实现。

– 当云服务客户的信息与云服务的 "元数据表 "存储在一个物理上共享的存储区域时，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* "中给出的相关指导可以适用于云计算环境。

CLD.9.5.2虚拟机加固控制

云计算环境中的虚拟机应该被加固以满足业务需求。

云服务的实施指南

云服务客户	云服务提供者
在配置虚拟机时，云服务客户和云服务提供商应确保适当的方面得到加固（例如，只有那些需要的端口、协议和服务），并确保对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）。	

CLD.12.1操作程序和责任

ISO/IEC 27002第12.1条中规定的目标适用。

CLD.12.1.5 管理员的操作安全控制

云计算环境的行政运作程序应该被定义、记录和保存。
监视。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应记录关键操作的程序，在这些操作中，故障会对云计算环境中的资产造成无法恢复的损害。 关键业务的例子有：。 – 安装、更改和删除虚拟化设备，如服务器、网络和存储。 – 使用云服务的终止程序。 – 备份和恢复。 该文件应规定，主管应监督这些业务。	云服务提供商应向有需要的云服务客户提供有关关键操作和程序的文件。

云服务的其他信息

云计算具有快速配置和管理，以及按需自助服务的优点。这些操作通常由来自云服务客户和云服务提供者的管理员执行。由于对这些关键操作的人为干预可能导致严重的信息安全事件，因此应考虑保障操作的机制，并在需要时定义和实施。严重事件的例子包括删除或关闭大量的虚拟服务器或破坏虚拟资产。

CLD.12.4 记录和监测

ISO/IEC 27002第12.4条中规定的目标适用。

CLD.12.4.5监控云服务的控

制

云服务客户应该有能力监测云服务运行的特定方面
云服务客户所使用的。

云服务的实施指南

云服务客户	云服务提供者
云服务客户应要求云服务提供商提供关于每个云服务可用的服务监控能力的信息。	云服务提供商应提供能力，使云服务客户能够监控与云服务客户相关的云服务运行的特定方面。例如，监测和检测云服务是否被用作攻击他人的平台，或敏感数据是否从云服务中被泄露出来。 适当的访问控制应确保对监控功能的使用。这些功能应仅提供对云服务客户自身云服务实例信息的访问。 云服务提供商应向云服务客户提供有关服务监控能力的文件。 监测应提供与条款12.4.1中描述的事件日志一致的数据，并协助实现SLA条款。

CLD.13.1网络安全管理

ISO/IEC 27002第13.1条中规定的目标适用。

CLD.13.1.4调整虚拟和物理网络的安全管理 控制

在配置虚拟网络时，应保证虚拟和物理网络之间配置的一致性。
根据云服务提供商的网络安全政策进行验证。

云服务的实施指南

云服务客户	云服务提供者
(没有额外的实施指导)	云服务提供商应根据物理网络的信息安全政策，为虚拟网络的配置定义并记录信息安全政策。云服务提供商应确保虚拟网络配置与信息安全政策相匹配，而不考虑用于创建配置的手段。

云服务的其他信息

在建立在虚拟化技术上的云计算环境中，虚拟网络被配置在物理网络的虚拟基础设施上。在这种环境中，网络策略的不一致会导致系统中断或访问控制的缺陷。

注意 - 根据云服务的类型，配置虚拟网络的责任在云服务客户和云服务提供者之间可能有所不同。

附件B

与云计算相关的信息安全风险参考文献

(本附件不构成本建议书和国际标准的组成部分)。

正确使用本建议-
国际标准所提供的信息安全控制措施，有赖于组织的信息安全风险评估和处理。尽管这些都是重要的主题，但本建议的重点不是信息安全风险评估和处理的方法。以下是包含对提供和使用云服务中的风险源和风险描述的参考文献列表。应当注意的是，风险源和风险因服务的类型和性质以及云计算的新兴技术而有所不同。建议本建议-国际标准的用户在必要时参考这些文件的最新版本。

建议ITU-T X.1601（2014），*云计算的安全框架*。

澳大利亚政府信息管理办公室2013年，《澳大利亚政府机构的隐私和云计算》中的*检查点摘要，更好的实践指南，1.1版，2月，第8页。澳大利亚政府机构的隐私和云计算，更好的实践指南*，1.1版，二月，*第*8页 。
http://www.finance.gov.au/files/2013/02/privacy-and-cloud-computing-for-australian-government-agencies-v1.1.pdf。

澳大利亚政府网络安全中心2015年，*租户的云计算安全* - 4月。
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，*云服务提供商的云计算安全* - 4月。
http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Cloud_Service_Providers.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OGCIO 2013，*云服务提供商在云平台上处理个人身份信息的安全和隐私检查表* - 4月。

香港OGCIO 2013, *云服务消费者的安全检查表* - 1月。ISACA 2012,

云计算的安全考虑 - 七月。

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。

SPRING新加坡2012，*附件A：*新加坡*虚拟化安全风险评估*技术参考30：2012服务器虚拟化安全技术参考-3月。

2012年新加坡标准协会，*附件A：*新加坡技术参考31：2012年公共云计算服务使用安全和服务水平指南的技术参考--3月，*审查SaaS时的安全和服务水平考虑清单。*

新加坡标准SPRING 2013，*附件A：云服务提供商披露*新加坡标准SS 584:2013多层次云计算安全规范--8月。

2012年新加坡标准协会，*附件B：*新加坡技术参考31：2012年公共云计算服务使用安全和服务水平指南的技术参考，3月，*审查IaaS时的安全和*服务水平*考虑清单。*

2013年新加坡标准协会，新加坡标准SS 584:2013*多层次云计算安全规范*-8月。

SPRING新加坡2012，新加坡技术参考30:2012*服务器虚拟化安全技术参考*--三月。

SPRING新加坡2012，新加坡技术参考31:2012*公共云计算服务使用安全和服务水平指南的技术参考*--3月。

美国政府FedRAMP PMO 2014，*FedRAMP安全控制基线2.0版*--6月。

书目

- 建议ITU-T X.805（2003），*提供端到端通信的系统的安全架构。*
- 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-信息安全管理系统-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--保护作为PII处理者的公共云中的个人身份信息（PII）的实践守则。*
- 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-第二部分：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-第三部分：信息和通信技术供应链安全指南。*
- ISO/IEC CD 27036-4, *信息技术-安全技术-供应商关系的信息安全-第4部分：云服务的安全准则-*（正在开发）。
- ISO/IEC 27040:2015，*信息技术-安全技术-存储安全。*
- ISO 19440:2007，*企业整合--企业建模的结构。*
- ISO 31000:2009, *风险管理-原则和指南。*
- NIST，SP 800-145 2011，*NIST对云计算的定义。*
- NIST 2009, *有效和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，*《云计算关键重点领域安全指导》V3.0。*
- 云安全联盟，*云计算的顶级威胁V1.0。*
- 云安全联盟，*领域12：身份和访问管理指南V2.1。*
- ISACA, *云计算。从安全、治理和保证的角度看商业利益。*
- ISACA, *云计算管理审计/保证计划。*