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).

我在这里的意思是说，我在这里的意思是说，我在这里的意思是说，我在这里的意思是说，我在这里的意思是说，我在这里的意思是说，我在这里的意思是说

ITU-T

X.1631

(07/2015)

国际电信联盟的电信标准化部门

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。