BS ISO/IEC 27017:2015

BSI Standards Publication

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC 27017:2015.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2015

ISBN 978 0 580 78159 9

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2015.

Amendments/corrigenda issued since publication

Date	Text affected

BS ISO/IEC 27017:2015

INTERNATIONAL STANDARD

ISO/IEC 27017

First edition
2015-12-15

Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Technologies de l'information — Techniques de sécurité — Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Reference number
ISO/IEC 27017:2015(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 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

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27017 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T. X.1631 (07/2015).

International Telecommunication Union

ITU-T X.1631

(07/2015)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cloud computing security – Cloud computing security design

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Recommendation ITU-T X.1631

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	**X.1602–X.1639**
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

INTERNATIONAL STANDARD ISO/IEC 27017
RECOMMENDATION ITU-T X.1631

Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Summary

Recommendation ITU-T X.1631 | ISO/IEC 27017 provides guidelines for information security controls applicable to the provision and use of cloud services by providing:

- additional implementation guidance for relevant controls specified in ISO/IEC 27002;
- additional controls with implementation guidance that specifically relate to cloud services.

This Recommendation | International Standard provides controls and implementation guidance for both cloud service providers and cloud service customers.

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1631	2015-07-14	17	11.1002/1000/12490

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

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)

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 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。

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。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：**17312273399@163.com**

2）也可通过客服电话咨询 **025-85307007**。