International Standard

ISO/IEC 27011

Third edition
2024-03

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002

Reference number
ISO/IEC 27011:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T (as ITU-T Recommendation X.1051) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27011-1:2016), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 27011-1:2016/Cor 1:2018.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

INTERNATIONAL STANDARD ISO/IEC 27011
RECOMMENDATION ITU-T X.1051

Information security, cybersecurity and privacy protection – Information security controls based on ISO/IEC 27002 for telecommunications organizations

Summary

This Recommendation | International Standard:

a) establishes guidelines and general principles for initiating, implementing, maintaining and improving information security controls in telecommunications organizations based on ISO/IEC 27002;

b) provides an implementation baseline of information security controls within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.

As a result of implementing this Recommendation | International Standard, telecommunications organizations, both within and between jurisdictions, will:

a) be able to ensure the confidentiality, integrity and availability of global telecommunications facilities, services and the information handled, processed or stored within global facilities and services;

b) have adopted secure collaborative processes and controls ensuring the lowering of risks in the delivery of telecommunications services;

c) be able to deliver information security in an effective and efficient manner;

d) have adopted a consistent holistic approach to information security;

e) be able to improve the security culture of organizations, raise staff awareness and increase public trust.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1051	2004-07-29	17	11.1002/1000/7286
2.0	ITU-T X.1051	2008-02-13	17	11.1002/1000/9332
3.0	ITU-T X.1051	2016-04-29	17	11.1002/1000/12845
3.1	ITU-T X.1051 (2016) Cor. 1	2017-09-06	17	11.1002/1000/13407
4.0	ITU-T X.1051	2023-06-13	17	11.1002/1000/15559

Keywords

Information security controls and telecommunications extended controls, information security management, information security risk assessment, information security risk treatment, ISO/IEC 27002.

* To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

CONTENTS

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**。

国际标准

ISO/IEC 27011

信息安全、网络安全和隐私保护——基于 ISO/IEC 27002 的电信组织信息安全控制措施

信息安全、网络安全和隐私保护——基于 ISO/IEC 27002 的电信组织信息安全措施

2024 年 3月
第三版

Reference number ISO/IEC 27011:2024(en)

受版权保护的文件

前言

国际标准化组织（ISO）和国际电工委员会（IEC）构成了全球标准化的专业体系。作为 ISO 或 IEC 成员的各国机构通过各自组织为处理特定技术领域而设立的技术委员会参与国际标准的制定。ISO 和 IEC 的技术委员会在共同感兴趣的领域开展合作。其他国际组织，无论是政府的还是非政府的，通过与 ISO 和 IEC 的联络，也参与其中。

关于本文件的任何反馈或问题应提交给用户所在国家的标准机构。这些机构的完整列表可在 www.iso.org/members.html 和 www.iec.ch/national- 查阅。
委员会。

ISO/IEC 27011:2024（英文版）

国际标准 ISO/IEC 27011 推荐 ITU-T X.1051

信息安全、网络安全和隐私保护——基于 ISO/IEC 27002 的电信组织信息安全控制措施

摘要

本建议书 | 国际标准：

a) 根据 ISO/IEC 27002，为电信组织制定启动、实施、维护和改进信息安全控制措施的指导方针和一般原则；

b) 为电信组织的信息安全控制措施提供实施基准，以确保电信设施、服务以及由这些设施和服务处理、加工或存储的信息的保密性、完整性和可用性。

由于实施了本建议书 | 国际标准，电信组织无论是在同一司法管辖区内部还是在不同司法管辖区之间，都将：

a)能够确保全球电信设施、服务以及在这些设施和服务中处理、传输或存储的信息的保密性、完整性和可用性；

b) 已采用安全的协作流程和控制措施，确保降低电信服务交付过程中的风险；

c) 能够以有效且高效的方式提供信息安全；

d) 采取了一贯的整体方法来保障信息安全；

e) 能够提升组织的安全文化，提高员工的安全意识，并增强公众的信任。

历史

版本	推荐	批准	学习小组	唯一标识符
1.0	国际电信联盟电信标准化部门 X.1051 标准	2004-07-29	17	11.1002/1000/7286
2.0	国际电信联盟电信标准化部门 X.1051 标准	2008-02-13	17	11.1002/1000/9332
3.0	国际电信联盟电信标准化部门 X.1051 标准	2016-04-29	17	11.1002/1000/12845
3.1	国际电信联盟电信标准化部门 X.1051（2016 年）修订版	2017-01-06	17	11.1002/1000/13407
4.0	国际电信联盟电信标准化部门 X.1051 标准	2023-06-13	17	11.1002/1000/15559

关键词

信息安全控制和电信扩展控制、信息安全管理体系、信息安全风险评估、信息安全风险处理、ISO/IEC 27002。

* To access the Recommendation, type the URL https://handle. itu. int/ in the address field of your web browser, followed by the Recommendation's unique ID.

前言

国际电信联盟（ITU）是联合国负责电信、信息和通信技术（ICT）领域的专门机构。国际电联电信标准化部门（ITU-T）是国际电联的一个常设机构。ITU-T 负责研究技术、运营和资费问题，并就这些问题发布建议书，以期在全球范围内实现电信标准化。

世界电信标准化全会（WTSA）每四年举行一次，确定国际电联电信标准化部门（ITU-T）各研究组的研究课题，各研究组则就这些课题制定建议书。

国际电联电信标准化部门（ITU-T）建议书的批准程序依照世界电信标准化全会（WTSA）第 1 号决议的规定执行。
在国际电联电信标准化部门（ITU-T）职权范围内的某些信息技术领域，必要的标准是与国际标准化组织（ISO）和国际电工委员会（IEC）合作制定的。

注释

在本建议中，为简洁起见，“管理机构”一词用于表示电信管理机构和认可的经营机构。

本建议书的遵循是自愿的。然而，建议书中可能包含某些强制性规定（例如，为确保互操作性或适用性），只有满足所有这些强制性规定，才算遵循了本建议书。建议书中使用“应”或“必须”等具有义务性的词语以及其否定形式来表达要求。使用此类词语并不意味着任何一方必须遵循本建议书。

知识产权

国际电联提醒注意，采用或实施本建议书的做法可能涉及使用声称的知识产权。国际电联对在建议书制定过程中由国际电联成员或建议书制定过程之外的其他方提出的知识产权主张的证据、有效性和适用性不持任何立场。

截至本建议书批准之日，国际电联尚未收到有关可能需要实施本建议书的专利/软件版权保护的知识产权的通知。然而，实施者应谨慎行事，因为这可能不代表最新信息，因此强烈建议其通过国际电联网站 http://www.itu.int/ITU-T/ipr/ 查阅适当的国际电联电信标准化部门数据库。

目录

页面

介绍

本建议书 | 国际标准为电信组织基于 ISO/IEC 27002 实施和管理信息安全控制措施提供了指导方针。

电信组织通过其基础设施为客户提供通信服务。为了提供电信服务，电信组织需要相互连接和/或共享其服务和设施以及/或者使用其他电信组织的服务和设施。此外，诸如无线电站点、天线位置、地面电缆和公用设施供应（电力、水）等场地位置，不仅本组织的员工可以进入，外部承包商和供应商也可以进入。

因此，电信组织的信息安全管理十分复杂，可能：

- 依赖外部各方；

必须涵盖网络基础设施、服务应用及其他设施的所有领域；

包括一系列电信技术（例如，有线、无线或宽带）；

支持广泛的运营规模、服务区域和服务类型。

除了应用 ISO/IEC 27002 中所述的信息安全控制措施外，电信组织还可以实施额外的信息安全控制措施，以确保电信的保密性、完整性、可用性以及任何其他信息安全属性，从而充分管理信息安全风险。专门针对电信的信息安全属性可描述如下（不分优先顺序）。

1) *保密性*

保护与电信相关的信息不被未经授权的披露。这意味着不得披露通信的存在、内容、来源、目的地以及通信信息的日期和时间。

电信机构必须确保其处理的通信内容不被泄露。这包括确保电信机构的工作人员对其在工作职责中可能获悉的任何有关他人的信息予以保密。

请注意——在一些国家，“通信保密”这一术语是在“不披露通信内容”的语境下使用的。

2) *诚信*

保护电信信息的完整性包括控制电信设施的安装和使用，以确保通过有线、无线或任何其他方式传输、转接或接收的信息的真实性、准确性和完整性。

3) *可用性*

电信信息的可用性包括确保对用于提供通信服务的设施和媒介的访问是经过授权的，无论通信是通过有线、无线电还是任何其他方式提供的。通常，在紧急情况下，电信组织会优先处理重要通信，并按照法定和监管要求管理不太重要的通信的不可用情况。

观众

本建议书 | 国际标准的受众包括电信组织和负责信息安全的人员；以及安全供应商、审计员、电信终端供应商和应用内容提供商。本建议书 | 国际标准提供了一套基于 ISO/IEC 27002 的通用信息安全控制措施、电信行业特定的信息安全控制措施以及信息安全管理指南，以便选择和实施这些控制措施。

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**。