



International
Standard

ISO/IEC 27011

**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*

**Third edition
2024-03**



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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.

**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/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	<i>Page</i>
1 Scope	1
2 Normative references	1
3 Definitions and abbreviations.....	1
3.1 Definitions.....	1
3.2 Abbreviations	2
4 Overview	2
4.1 Structure of this Recommendation International Standard.....	2
4.2 Information security management systems in telecommunications organizations.....	3
5 Organizational controls	5
5.1 Policies for information security	5
5.2 Information security roles and responsibilities.....	5
5.3 Segregation of duties.....	6
5.4 Management responsibilities.....	6
5.5 Contact with authorities	6
5.6 Contact with special interest groups.....	6
5.7 Threat intelligence.....	6
5.8 Information security in project management.....	6
5.9 Inventory of information and other associated assets.....	6
5.10 Acceptable use of information and other associated assets	6
5.11 Return of assets	6
5.12 Classification of information.....	7
5.13 Labelling of information	7
5.14 Information transfer.....	7
5.15 Access control	7
5.16 Identity management	7
5.17 Authentication information	7
5.18 Access rights	7
5.19 Information security in supplier relationships.....	7
5.20 Addressing information security within supplier agreements	8
5.21 Managing information security in the ICT supply chain.....	8
5.22 Monitoring, review and change management of supplier services.....	8
5.23 Information security for use of cloud services	8
5.24 Information security incident management planning and preparation	8
5.25 Assessment and decision on information security events.....	9
5.26 Response to information security incidents.....	9
5.27 Learning from information security incidents.....	9
5.28 Collection of evidence.....	9
5.29 Information security during disruption.....	9
5.30 ICT readiness for business continuity	10
5.31 Legal, statutory, regulatory and contractual requirements	10
5.32 Intellectual property rights	10
5.33 Protection of records	10
5.34 Privacy and protection of PII.....	10
5.35 Independent review of information security.....	10

5.36	Compliance with policies, rules and standards for information security.....	10
5.37	Documented operating procedures.....	10
5.38	TEL – Interconnected telecommunications services.....	10
5.39	TEL – Security management of telecommunications services delivery.....	11
5.40	TEL – Response to spam.....	12
5.41	TEL – Response to DoS/DDoS attacks.....	12
5.42	TEL – Non-disclosure of communications.....	13
5.43	TEL – Essential communications.....	14
5.44	TEL – Legality of emergency actions.....	15
5.45	TEL – Coordination for information security incident management.....	15
6	People controls.....	16
6.1	Screening.....	16
6.2	Terms and conditions of employment.....	16
6.3	Information security awareness, education and training.....	16
6.4	Disciplinary process.....	16
6.5	Responsibilities after termination or change of employment.....	16
6.6	Confidentiality or non-disclosure agreements.....	16
6.7	Remote working.....	17
6.8	Information security event reporting.....	17
7	Physical controls.....	17
7.1	Physical security perimeter.....	17
7.2	Physical entry.....	17
7.3	Securing offices, rooms and facilities.....	17
7.4	Physical security monitoring.....	17
7.5	Protecting against physical and environmental threats.....	17
7.6	Working in secure areas.....	17
7.7	Clear desk and clear screen.....	17
7.8	Equipment siting and protection.....	18
7.9	Security of assets off-premises.....	18
7.10	Storage media.....	18
7.11	Supporting utilities.....	18
7.12	Cabling security.....	18
7.13	Equipment maintenance.....	18
7.14	Secure disposal or re-use of equipment.....	18
7.15	TEL – Securing communication centres.....	18
7.16	TEL – Securing telecommunications equipment room.....	19
7.17	TEL – Securing physically isolated operation areas.....	20
7.18	TEL – Equipment sited in other carriers' premises.....	21
7.19	TEL – Equipment sited in user premises.....	21
8	Technological controls.....	22
8.1	User endpoint devices.....	22
8.2	Privileged access rights.....	22
8.3	Information access restriction.....	22
8.4	Access to source code.....	22
8.5	Secure authentication.....	22

8.6	Capacity management	22
8.7	Protection against malware	22
8.8	Management of technical vulnerabilities.....	22
8.9	Configuration management.....	22
8.10	Information deletion.....	22
8.11	Data masking.....	22
8.12	Data leakage prevention.....	22
8.13	Information backup	22
8.14	Redundancy of information processing facilities	22
8.15	Logging	23
8.16	Monitoring activities	23
8.17	Clock synchronization.....	23
8.18	Use of privileged utility programs.....	23
8.19	Installation of software on operational systems	23
8.20	Network security	23
8.21	Security of network services	23
8.22	Segregation of networks.....	24
8.23	Web filtering	24
8.24	Use of cryptography	24
8.25	Secure development lifecycle.....	24
8.26	Application security requirements.....	24
8.27	Secure system architecture and engineering principles.....	24
8.28	Secure coding	24
8.29	Security testing in development and acceptance	24
8.30	Outsourced development.....	24
8.31	Separation of development, test and production environments.....	24
8.32	Change management	24
8.33	Test information.....	25
8.34	Protection of information systems during audit testing.....	25
8.35	TEL – Telecommunications carrier identification and authentication by users	25
Annex A	Additional guidance for network security	26
A.1	Security measures against network attacks	26
A.2	Network security measures for network congestion.....	27
Bibliography		28

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

奥邦检验认证集团有限公司翻译
内部资料

奥邦检验认证集团

奥邦检验认证集团公示用途

奥邦检验认证集团公示用途



受版权保护的文件

©ISO/IEC 2024

版权所有。除非另有规定或在实施过程中有此需要，否则未经事先书面许可，不得以任何形式或通过任何手段（包括电子或机械手段，如影印、在互联网或内联网上发布）复制或以其他方式使用本出版物的任何部分。可向以下地址的

国际标准化组织（ISO）成员机构提出。国际标准化组织版权办公室

CP 401 · 布兰东内街 8 号

瑞士日内瓦韦尔涅 1214 号

电话 41 22 746 9111 电子邮件 copyright@iso.org

出版于瑞士 网站: www.iso.org

www.iso.org



©ISO/IEC 2024 - 保留所有权利

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-06	2017-06-06	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。

©国际电信联盟 2024

目录

页面

1	范围	1
2	规范性引用文件	1
3	定义和缩略语	1
3.1	定义	1
3.2	缩略语	2
4	概述	2
4.1	本建议书的结构 国际标准	2
4.2	电信组织的信息安全管理体系	3
5	组织控制	5
5.1	信息安全政策	5
5.2	信息安全角色与职责	5
5.3	职责分离	6
5.4	管理职责	6
5.5	与当局联系	6
5.6	与特殊利益集团接触	6
5.7	威胁情报	6
5.8	项目管理中的信息安全	6
5.9	信息及其他相关资产清单	6
5.10	信息及其他相关资产的可接受使用方式	6
5.11	资产回报	6
5.12	信息分类	7
5.13	信息标注	7
5.14	信息传递	7
5.15	访问控制	7
5.16	身份管理	7
5.17	认证信息	7
5.18	访问权限	7
5.19	供应商关系中的信息安全	7
5.20	在供应商协议中处理信息安全问题	8
5.21	在信息通信技术供应链中管理信息安全	8
5.22	供应商服务的监控、审查和变更管理	8
5.23	云服务使用的信息安全	8
5.24	信息安全事件管理规划与准备	8
5.25	信息安全事件的评估与决策	9
5.26	信息安全事件响应	9
5.27	从信息安全事件中学习	9
5.28	证据收集	9
5.29	中断期间的信息安全	9
5.30	企业业务连续性的信息通信技术准备情况	10
5.31	法律、法规、规章及合同要求	10
5.32	知识产权	10
5.33	记录保护	10
5.34	隐私与个人身份信息保护	10
5.35	信息安全独立审查	10

5.36	遵守信息安全政策、规则 and 标准	10
5.37	已记录的操作程序	10
5.38	TEL - 相互连接的电信服务	10
5.39	电信服务交付的安全管理	11
5.40	TEL - 对垃圾邮件的回应	12
5.41	TEL - 对拒绝服务/分布式拒绝服务攻击的响应	12
5.42	电信 - 通信内容保密	13
5.43	TEL - 基本通信	14
5.44	紧急行动的合法性	15
5.45	信息安全事件管理的协调工作电话	15
6	人员管控	16
6.1	筛选	16
6.2	雇用条款和条件	16
6.3	信息安全意识、教育与培训	16
6.4	纪律处分程序	16
6.5	终止或变更雇佣关系后的责任	16
6.6	保密协议或不披露协议	16
6.7	远程办公	17
6.8	信息安全事件报告	17
7	物理控制	17
7.1	物理安全边界	17
7.2	实体进入	17
7.3	保障办公室、房间和设施的安全	17
7.4	物理安全监控	17
7.5	防范物理和环境威胁	17
7.6	在安全区域工作	17
7.7	整洁桌面, 清晰屏幕	17
7.8	设备选址与防护	18
7.9	离场所资产的安全	18
7.10	存储介质	18
7.11	支持工具	18
7.12	布线安全	18
7.13	设备维护	18
7.14	设备的安全处置或再利用	18
7.15	TEL - 保障通信中心安全	18
7.16	电信设备机房安全措施	19
7.17	TEL - 物理隔离操作区域的安全保障	20
7.18	位于其他运营场所的设备	21
7.19	用户场所安装的终端设备	21
8	技术控制	22
8.1	用户终端设备	22
8.2	特权访问权限	22
8.3	信息访问限制	22
8.4	源代码访问权限	22
8.5	安全认证	22

8.6	容量管理	22
8.7	防范恶意软件	22
8.8	技术漏洞管理	22
8.9	配置管理	22
8.10	信息删除	22
8.11	数据屏蔽	22
8.12	数据泄露防护	22
8.13	信息备份	22
8.14	信息处理设施的冗余	22
8.15	日志记录	23
8.16	监测活动	23
8.17	时钟同步	23
8.18	特权实用程序的使用	23
8.19	在操作系统上安装软件	23
8.20	网络安全	23
8.21	网络服务的安全性	23
8.22	网络隔离	24
8.23	网络过滤	24
8.24	密码学的使用	24
8.25	安全开发生命周期	24
8.26	应用程序安全要求	24
8.27	安全系统架构与工程原则	24
8.28	安全编码	24
8.29	开发和验收中的安全测试	24
8.30	外包开发	24
8.31	开发、测试和生产环境的分离	24
8.32	变更管理	24
8.33	测试信息	25
8.34	审计测试期间的信息系统保护	25
8.35	TEL - 用户对电信运营商的识别与认证	25
附件 A	网络安全的补充指南	26
A.1	防范网络攻击的安全措施	26
A.2	网络拥塞的网络安全措施	27
参考文献		28

ISO/IEC 27011:2024 (英文版)

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**。