

## 关于认证依据标准的说明

本英文标准系我机构自中国标准服务网采购的正版授权文件，标准使用主体仅限北京三星九千认证中心有限公司。

标准所有者要求“未经事先书面许可，不得以任何形式或任何手段公开”。基于版权保护的相关要求，此处仅提供封面及目录等关键信息扫描件；如需要标准完整文本，请通过以下方式获取：

电话：010- 64429578（总机）

外联部：18518156209（王经理）

邮箱：[wanghy@sanxing9000.com](mailto:wanghy@sanxing9000.com)

---

---

**Security and resilience —  
Security management systems —  
Requirements**

使用方：北京三星九千认证中心有限公司  
订单号： 202609220855185993001  
购买日期： 2026-09-22  
销售机构： 中国标准化研究院  
联系电话： 010-58811360  
网址： <https://www.cssn.net.cn>



防伪查询：UTdc-fent-5kHD-JsIT-Wizp  
网址：https://www.cssn.net.cn  
销售机构：中国标准化研究院



扫描二维码查询标准授权信息

使用方：北京三星九千认证中心有限公司  
订单号：202609220855185993001  
购买日期：2026-09-22  
销售机构：中国标准化研究院  
联系电话：010-58811360  
网址：<https://www.cssn.net.cn>



版权声明

国家市场监督管理总局、国家标准化管理委员会负责ISO、IEC国际标准在中国境内推广发行工作的监督和管理，负责ISO、IEC国际标准在中国境内的版权管理与保护工作。国家标准技术审评中心具体承担ISO、IEC国际标准在中国境内推广发行工作，承担ISO、IEC国际标准在中国境内的版权管理与保护工作。

中国标准化研究院 为中国境内国际标准授权销售网站。  
正版授权销售网站及销售点名单，可在中国标准信息服务网（<https://www.sacinfo.cn/antifake>）查询。

未经授权，严禁对ISO、IEC标准出版物及相关技术文件进行复制、销售、传播和翻译出版，严禁将国际标准的任何部分通过电子信息网络或制作成标准数据库用于传播。

国家标准技术审评中心    电话：400 650 6190    网址：[www.sacinfo.cn](http://www.sacinfo.cn)

ISO 28000:2022(E)

北京三星九千认证中心有限公司专用

防伪查询：UTdc-fent-5kHD-JsIT-Wizp

网址：<https://www.cssn.net.cn>

销售机构：中国标准化研究院



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 2022

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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| Foreword.....                                                               | v         |
| Introduction.....                                                           | vi        |
| <b>1 Scope.....</b>                                                         | <b>1</b>  |
| <b>2 Normative references.....</b>                                          | <b>1</b>  |
| <b>3 Terms and definitions.....</b>                                         | <b>1</b>  |
| <b>4 Context of the organization.....</b>                                   | <b>4</b>  |
| 4.1 Understanding the organization and its context.....                     | 4         |
| 4.2 Understanding the needs and expectations of interested parties.....     | 4         |
| 4.2.1 General.....                                                          | 4         |
| 4.2.2 Legal, regulatory and other requirements.....                         | 4         |
| 4.2.3 Principles.....                                                       | 5         |
| 4.3 Determining the scope of the security management system.....            | 6         |
| 4.4 Security management system.....                                         | 6         |
| <b>5 Leadership.....</b>                                                    | <b>7</b>  |
| 5.1 Leadership and commitment.....                                          | 7         |
| 5.2 Security policy.....                                                    | 7         |
| 5.2.1 Establishing the security policy.....                                 | 7         |
| 5.2.2 Security policy requirements.....                                     | 8         |
| 5.3 Roles, responsibilities and authorities.....                            | 8         |
| <b>6 Planning.....</b>                                                      | <b>8</b>  |
| 6.1 Actions to address risks and opportunities.....                         | 8         |
| 6.1.1 General.....                                                          | 8         |
| 6.1.2 Determining security-related risks and identifying opportunities..... | 9         |
| 6.1.3 Addressing security-related risks and exploiting opportunities.....   | 9         |
| 6.2 Security objectives and planning to achieve them.....                   | 9         |
| 6.2.1 Establishing security objectives.....                                 | 9         |
| 6.2.2 Determining security objectives.....                                  | 10        |
| 6.3 Planning of changes.....                                                | 10        |
| <b>7 Support.....</b>                                                       | <b>10</b> |
| 7.1 Resources.....                                                          | 10        |
| 7.2 Competence.....                                                         | 10        |
| 7.3 Awareness.....                                                          | 11        |
| 7.4 Communication.....                                                      | 11        |
| 7.5 Documented information.....                                             | 11        |
| 7.5.1 General.....                                                          | 11        |
| 7.5.2 Creating and updating documented information.....                     | 11        |
| 7.5.3 Control of documented information.....                                | 12        |
| <b>8 Operation.....</b>                                                     | <b>12</b> |
| 8.1 Operational planning and control.....                                   | 12        |
| 8.2 Identification of processes and activities.....                         | 12        |
| 8.3 Risk assessment and treatment.....                                      | 13        |
| 8.4 Controls.....                                                           | 13        |
| 8.5 Security strategies, procedures, processes and treatments.....          | 14        |
| 8.5.1 Identification and selection of strategies and treatments.....        | 14        |
| 8.5.2 Resource requirements.....                                            | 14        |
| 8.5.3 Implementation of treatments.....                                     | 14        |
| 8.6 Security plans.....                                                     | 14        |
| 8.6.1 General.....                                                          | 14        |
| 8.6.2 Response structure.....                                               | 14        |
| 8.6.3 Warning and communication.....                                        | 15        |
| 8.6.4 Content of the security plans.....                                    | 15        |

**ISO 28000:2022(E)**

|           |                                                       |           |
|-----------|-------------------------------------------------------|-----------|
| 8.6.5     | Recovery .....                                        | 16        |
| <b>9</b>  | <b>Performance evaluation .....</b>                   | <b>16</b> |
| 9.1       | Monitoring, measurement, analysis and evaluation..... | 16        |
| 9.2       | Internal audit.....                                   | 17        |
| 9.2.1     | General.....                                          | 17        |
| 9.2.2     | Internal audit programme.....                         | 17        |
| 9.3       | Management review .....                               | 17        |
| 9.3.1     | General.....                                          | 17        |
| 9.3.2     | Management review inputs .....                        | 18        |
| 9.3.3     | Management review results.....                        | 18        |
| <b>10</b> | <b>Improvement.....</b>                               | <b>18</b> |
| 10.1      | Continual improvement.....                            | 18        |
| 10.2      | Nonconformity and corrective action.....              | 19        |
|           | <b>Bibliography.....</b>                              | <b>20</b> |

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see [www.iso.org/patents](http://www.iso.org/patents)).

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](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 28000:2007), which has been technically revised, but maintains existing requirements to provide continuity for organizations using the previous edition. The main changes are as follows:

- recommendations on principles have been added in [Clause 4](#) to give better coordination with ISO 31000;
- recommendations have been added in [Clause 8](#) for better consistency with ISO 22301, facilitating integration including:
  - security strategies, procedures, processes and treatments;
  - security plans.

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](http://www.iso.org/members.html).

## ISO 28000:2022(E)

### Introduction

Most organizations are experiencing an increasing uncertainty and volatility in the security environment. As a consequence, they face security issues that impact on their objectives, which they want to address systematically within their management system. A formal approach to security management can contribute directly to the business capability and credibility of the organization.

This document specifies requirements for a security management system, including those aspects critical to the security assurance of the supply chain. It requires the organization to:

- assess the security environment in which it operates including its supply chain (including dependencies and interdependencies);
- determine if adequate security measures are in place to effectively manage security-related risks;
- manage compliance with statutory, regulatory and voluntary obligations to which the organization subscribes;
- align security processes and controls, including the relevant upstream and downstream processes and controls of the supply chain to meet the organization's objectives.

Security management is linked to many aspects of business management. They include all activities controlled or influenced by organizations, including but not limited to those that impact on the supply chain. All activities, functions and operations should be considered that have an impact on the security management of the organization including (but not limited to) its supply chain.

With regard to the supply chain, it has to be considered that supply chains are dynamic in nature. Therefore, some organizations managing multiple supply chains may look to their providers to meet related security standards as a condition of being included in that supply chain in order to meet requirements for security management.

This document applies the Plan-Do-Check-Act (PDCA) model to planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of an organization's security management system, see [Table 1](#) and [Figure 1](#).

**Table 1 — Explanation of the PDCA model**

|                               |                                                                                                                                                                                                                             |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plan<br>(Establish)           | Establish security policy, objectives, targets, controls, processes and procedures relevant to improving security in order to deliver results that align with the organization's overall policies and objectives.           |
| Do<br>(Implement and operate) | Implement and operate the security policy, controls, processes and procedures.                                                                                                                                              |
| Check<br>(Monitor and review) | Monitor and review performance against security policy and objectives, report the results to management for review, and determine and authorize actions for remediation and improvement.                                    |
| Act<br>(Maintain and improve) | Maintain and improve the security management system by taking corrective action, based on the results of management review and reappraising the scope of the security management system and security policy and objectives. |

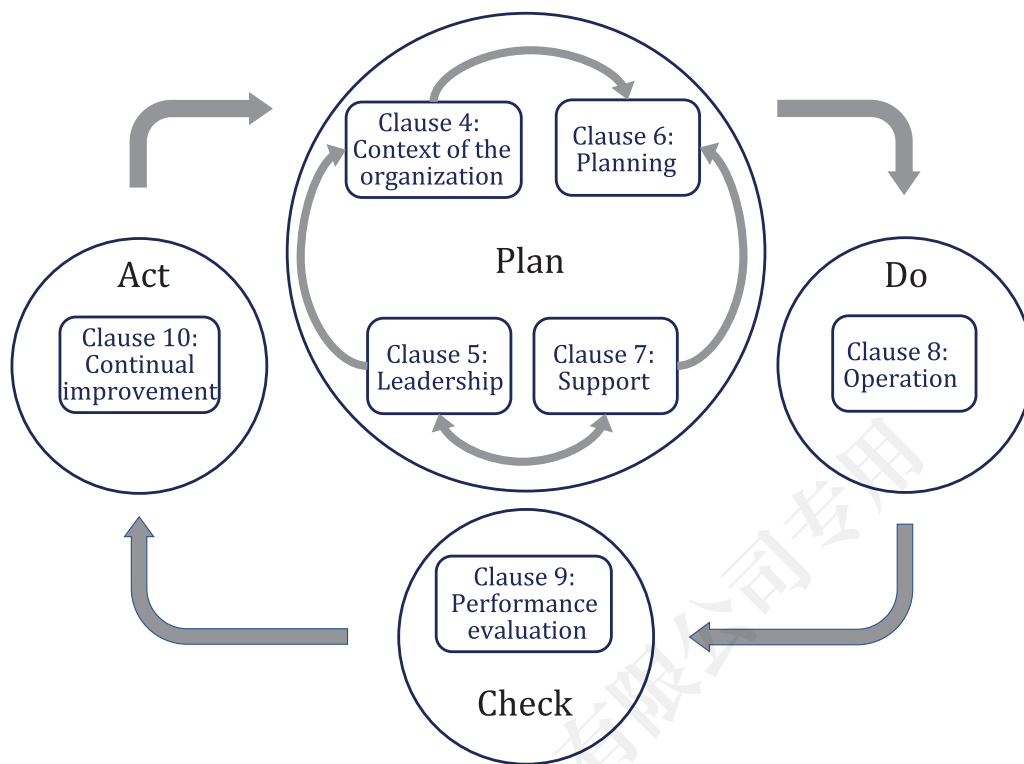


**Figure 1 — PDCA model applied to the security management system**

This ensures a degree of consistency with other management system standards, such as ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001, etc., thereby supporting consistent and integrated implementation and operation with related management systems.

For organizations that so wish, conformity of the security management system to this document may be verified by an external or internal auditing process.



# International Standard

**ISO 28000**

## **Security and resilience — Security management systems — Requirements**

**AMENDMENT 1: Climate action  
changes**

**Second edition  
2022-03**

**AMENDMENT 1  
2024-02**

使用方：北京三星九千认证中心有限公司

订单号：202609220855185993001

购买日期：2026-09-22

销售机构：中国标准化研究院

联系电话：010-58811360

网址：<https://www.cssn.net.cn>

防伪查询：UTdc-fent-5kHD-JsIT-Wizp  
网址：https://www.cssn.net.cn  
销售机构：中国标准化研究院



扫描二维码查询标准授权信息

使用方：北京三星九千认证中心有限公司  
订单号：202609220855185993001  
购买日期：2026-09-22  
销售机构：中国标准化研究院  
联系电话：010-58811360  
网址：<https://www.cssn.net.cn>



版权声明

国家市场监督管理总局、国家标准化管理委员会负责ISO、IEC国际标准在中国境内推广发行工作的监督和管理，负责ISO、IEC国际标准在中国境内的版权管理与保护工作。国家标准技术审评中心具体承担ISO、IEC国际标准在中国境内推广发行工作，承担ISO、IEC国际标准在中国境内的版权管理与保护工作。

中国标准化研究院 为中国境内国际标准授权销售网站。  
正版授权销售网站及销售点名单，可在中国标准信息服务网 (<https://www.sacinfo.cn/antifake>) 查询。

未经授权，严禁对ISO、IEC标准出版物及相关技术文件进行复制、销售、传播和翻译出版，严禁将国际标准的任何部分通过电子信息网络或制作成标准数据库用于传播。

国家标准技术审评中心    电话：400 650 6190    网址：[www.sacinfo.cn](http://www.sacinfo.cn)

**ISO 28000:2022/Amd.1:2024(en)**

北京三星九千认证中心有限公司专用

防伪查询：UTdc-fent-5kHD-JsIT-Wizp

网址：https://www.cssn.net.cn

销售机构：中国标准化研究院



**COPYRIGHT PROTECTED DOCUMENT**

© ISO 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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

© ISO 2024 – All rights reserved

## ISO 28000:2022/Amd.1:2024(en)

### Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives)).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes 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 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](http://www.iso.org/patents). ISO 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](http://www.iso.org/iso/foreword.html).

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*, in accordance with Technical Management Board Resolution 75/2023.

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](http://www.iso.org/members.html).