

ICS 35.030



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 29246-2023

**Information security technology - Information security
management systems - Overview and vocabulary**

信息安全技术 信息安全管理体系统 概述和词汇

(English Translation)

Issued on: December 28, 2023

Implemented on: July 1, 2024

Issued by: State Administration for Market Regulation

Table of Contents

Foreword...	3
1 Scope...	5
2 Normative references...	5
3 Terms and definitions...	5
4 Information security management systems (ISMS)...	18
4.1 General...	18
4.2 Concept of ISMS...	19
4.3 Process approach...	21
4.4 Why an ISMS is important...	22
4.5 Establishing, monitoring, maintaining and improving an ISMS...	23
4.6 ISMS critical success factors...	27
4.7 Benefits of the ISMS family of standards...	28
5 ISMS family of standards...	29
5.1 General information...	29
5.2 Standard describing an overview and terminology. ISO/IEC 27000 (GB/T 29246).....	30
5.3 Standards specifying requirements...	31
5.4 Standards describing general guidelines...	32
5.5 Standards describing sector-specific guidelines...	36
References...	40
Indexes...	43

Foreword

This document was drafted in accordance with the provisions of GB/T 1.1-2020 Directives for standardization - Part 1.Rules for the structure and drafting of standardizing documents.

This document replaces GB/T 29246-2017 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Compared with GB/T 29246-2017, in addition to structural adjustments and editorial changes, the main technical changes are as follows.

- a) The terms "analytical model", "attribute", "data", "decision criteria", "executive management", "ISMS project", "measurement results", "object", "scale", "unit of measurement", "validation" and "verification" are deleted (see Chapter 3 of the 2017 edition);
- b) The terms "interested party" (see 2.41 of the 2017 edition) and "stakeholder" (see 2.82 of the 2017 edition) with the same definition are merged into the term "interested party; stakeholder" (see 3.37);
- c) The description of ISO/IEC 27009 is added (see 5.3.3);
- d) The description of ISO/IEC 27021 is added (see 5.4.10);
- e) The descriptions of some standards in the information security management system family of standards are updated (see Chapter 5; see Chapter 4 of the **2017 edition**).

This document is identical to ISO/IEC 27000.2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary. The following minimal editorial changes are made to this document.

-- In order to coordinate with the existing standards, the name of the standard is changed to "Information security technology - Information security management systems - Overview and vocabulary".

1 Scope

This document provides the overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

The measure (3.42) defined in terms of an attribute and the method for quantifying it.
A person or organization (3.50) that can affect, be affected by, or perceive itself to be

affected by a decision or activity.

4 Information security management systems (ISMS)

Protecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image.

5 ISMS family of standards

The ISMS family of standards consists of inter-related standards, already published or under development, and contains a number of significant structural components. These components are focused on.

Information technology - Security techniques - Guidelines for auditors on information security controls (Information technology - Security techniques - Guidelines for auditors on information security controls)

.....