GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 29246-2023 / ISO/IEC 27000:2018

Replacing GB/T 29246-2017

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

信息安全技术 信息安全管理体系 概述和词汇

(ISO/IEC 27000:2018, Information technology - Security techniques - Information security management systems - Overview and vocabulary, IDT)

Issued on: December 28, 2023 **Implemented on: July 1, 2024**

Issued by: State Administration for Market Regulation;
Standardization Administration of PRC.

Table of Contents

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".

Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.

This document was proposed by and is under the jurisdiction of the National Technical Committee on Cybersecurity of Standardization Administration of China (SAC/TC260).

Drafting organizations of this document: China Electronics Cyberspace Great Wall Co., Ltd., China Electronics Standardization Institute, Hangzhou DBAPP Security Co., Ltd.,

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.

This document is applicable to all types and sizes of organization (e.g., commercial enterprises, government agencies, not-for-profit organizations).

The terms and definitions provided in this document:

-- cover commonly used terms and definitions in the ISMS family of standards;

-- do not cover all terms and definitions applied within the ISMS family of standards; and

-- do not limit the ISMS family of standards in defining new terms for use.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

3.1 access control

Means to ensure that access to assets is authorized and restricted based on business and security requirements (3.56).

3.2 attack

Attempts to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

3.3 audit

Systematic, independent and documented processes (3.54) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are

planned and controlled conditions. The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach".

4.4 Why an ISMS is important

Risks associated with an organization's information assets need to be addressed. Achieving information security requires the management of risk, and encompasses risks from physical, human and technology related threats associated with all forms of information within or used by the organization.

The adoption of an ISMS is expected to be a strategic decision for an organization and it is necessary that this decision is seamlessly integrated, scaled and updated in accordance with the needs of the organization.

The design and implementation of an organization's ISMS is influenced by the needs and objectives of the organization, the security requirements, the business processes employed and the size and structure of the organization. The design and operation of an ISMS needs to reflect the interests and information security requirements of all of the organization's stakeholders (including customers, suppliers, business partners, shareholders and other relevant third parties).

In an interconnected world, information and related processes, systems, and networks constitute critical business assets. Organizations and their information systems and networks face security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, fire and flood. Damage to information systems and networks caused by malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

An ISMS is important to both public and private sector businesses. In any industry, an ISMS is an enabler that supports e-business and is essential for risk management activities. The interconnection of public and private networks and the sharing of information assets increase the difficulty of controlling access to and handling of information. In addition, the distribution of mobile storage devices containing information assets can weaken the effectiveness of traditional controls. When organizations adopt the ISMS family of standards, the ability to apply consistent and mutually-recognizable information security principles can be demonstrated to business partners and other interested parties.

Information security is not always taken into account in the design and development of information systems. Further, information security is often thought of as being a technical solution. However, the information security that can be achieved through technical means is limited, and can be ineffective without being supported by appropriate management and procedures within the context of an ISMS. Integrating

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------