GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 29246-2017/ISO / IEC 27000:2016

Replacing GB/T 29246-2012

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

(ISO/IEC 27000:2016, IDT)

信息技术 安全技术 信息安全管理体系 概述和词汇

Issued on: December 29, 2017 **Implemented on: July 01, 2018**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;
Standardization Administration of the People's Republic of China.

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This Standard replaces GB/T 29246-2012, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*; compared with GB/T 29246-2012, the main technical changes are as follows:

-- Increase the constituent standards of the ISMS family of standards from 10 to 19 (see 0.2 and 4.1~4.5; 0.2 and 4.1~4.5 of the 2012 edition);

-- Increase terms and definitions from 46 to 89 (see 2.1~2.89; 2.1~2.46 of the 2012 edition);

-- Change “Classification of terms” to “Terms and term ownership” in the appendix (see Appendix B; Appendix B of the 2012 edition).

This Standard is identical to ISO/IEC 27000:2016 *Information technology - Security techniques - Information security management systems - Overview and vocabulary* by the translation method.

This Standard shall be under the jurisdiction of National Information Security Standardization Technical Committee (SAC/TC 260).

Drafting organizations of this Standard: China Electronics Cyberspace Great Wall Co., Ltd., China Electronics Standardization Institute, China Information Security Research Institute Co., Ltd.

Main drafters of this Standard: Min Jinghua, Shangguan Xiaoli, Xu Yuna, Wang Huili, Luo Fengying, Zuo Xiaodong, Zhou Yachao, Ma Hongjun, Liao Feiming, Huang Kaifeng, Ma Wenhe.

The previous versions which are replaced by this Standard are:

-- GB/T 29246-2012.

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

1 Scope

This Standard provides an overview of information security management systems, and terms and definitions commonly used in the ISMS family of standards. This Standard is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1

access control

Means to ensure that access to assets is authorized and restricted based on business and security requirements (2.63).

2.2

analytical model

Algorithm or calculation combining one or more base measures (2.10) and/or derived measures (2.22) with associated decision criteria (2.21).

2.3

attack

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

2.4

attribute

Property or characteristic of an object (2.55) that can be distinguished quantitatively or qualitatively by human or automated means.

[ISO/IEC 15939:2007, 2.2, modified: “entity” has been replaced by “object” in the definition.]

e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

3.3 Process approach

Organizations need to identify and manage many activities in order to function effectively and efficiently. Any activity using resources needs to be managed to enable the transformation of inputs into outputs using a set of interrelated or interacting activities; this is also known as a process. The output from one process can directly form the input to another process and generally this transformation is carried out under 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”.

3.4 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, vandalism, 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

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

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