GB

NATIONAL STANDARD OF

THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 22081-2016 / ISO/IEC 27002:2013

Replacing GB/T 22081-2008

Information technology - Security techniques - Information security management systems - Code of practice for information security controls

(ISO/IEC 27002:2013, IDT)

信息技术 安全技术

信息安全控制实践指南

Issued on: August 29, 2016 **Implemented on: March 1, 2017**

Issued by: General Administration of Quality Supervision, Inspection and Quarantine;

Standardization Administration Committee.

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 22081-2008 “Information technology - Security techniques - Code of practice for information security management”.

Compared with GB/T 22081-2008, the main technical changes in this Standard are as follows:

- see Annex NA for structural change;
- see Annex NB for change in terms.

This Standard uses translation method to identically adopt ISO/IEC 27002:2013 “Information technology - Security techniques - Code of practice for information security management” as well as its corresponding technical corrigendum (ISO/IEC 27002:2013/COR1:2014).

The Chinese document which has consistency with the international normative reference in this Part is as follow:

- GB/T 29246-2012 “Information technology - Security techniques - Information security management systems - Overview and vocabulary” (ISO/IEC 27000:2009, IDT).

This Standard also made the following informative modifications:

- added the informative Annex NA;
- added the informative Annex NB.

Attention is drawn to the possibility that some of the elements of this Standard may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

This Standard was proposed by and shall be under the jurisdiction of National Technical Committee on Information Security of Standardization Administration of China (SAC/TC 260).

The drafting organizations of this Standard: China Electronics Standardization Institute, CLP Great Wall Internet System Application Co., Ltd., China Information Security Certification Center, Shandong Institute of Standardization, Guangzhou CEPREI Certification Body, Beijing Jiangnan Tian An Technology Co., Ltd., Shanghai Sanwei Guardian Information Security Co., Ltd., China National Accreditation Center for Conformity Assessment, Beijing Times Granville Information Technology Co., Ltd., Heilongjiang Electronic Information

Information technology - Security techniques - Information security management systems - Code of practice for information security controls

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on GB/T 22080 [10];

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Structure of this standard

This Standard contains 14 security control clauses collectively containing a total

Bibliography

[1] ISO/IEC Directives, Part 2

[2] ISO/IEC 11770-1, Information technology Security techniques - Key management - Part 1: Framework

[3] ISO/IEC 11770-2, Information technology - Security techniques - Key management - Part 2: Mechanisms using symmetric techniques

[4] ISO/IEC 11770-3, Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques

[5] ISO 15489-1, Information and documentation - Records management - Part 1: General

[6] ISO/IEC 20000-1, Information technology - Service management - Part 1: Service management system requirements

[7] ISO/IEC 20000-2,1)Information technology - Service management - Part 2: Guidance on the application of service management systems

[8] ISO 22301, Societal security - Business continuity management systems - Requirements

[9] ISO 22313, Societal security - Business continuity management systems - Guidance

[10] GB/T 22080, Information technology - Security techniques - Information security management systems - Requirements

[11] ISO/IEC 27005, Information technology - Security techniques - Information security risk management

[12] ISO/IEC 27007, Information technology - Security techniques - Guidelines for information security management systems auditing

[13] ISO/IEC TR 27008, Information technology - Security techniques - Guidelines for auditors on information security controls

[14] ISO/IEC 27031, Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

[15] ISO/IEC 27033-1, Information technology - Security techniques - Network security - Part 1: Overview and concepts

[16] ISO/IEC 27033-2, Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security

[17] ISO/IEC 27033-3, Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

[18] ISO/IEC 27033-4, Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways

[19] ISO/IEC 27033-5, Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Network (VPNs)

[20] ISO/IEC 27035, Information technology - Security techniques - Information security incident management

[21] ISO/IEC 27036-1, Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts

[22] ISO/IEC 27036-2, Information technology - Security techniques - Information security for supplier relationships - Part 2: Common requirements

[23] ISO/IEC 27036-3, Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for ICT supply chain security

[24] ISO/IEC 27037, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence

[25] ISO/IEC 29100, Information technology - Security techniques - Privacy framework

[26] ISO/IEC 29101, Information technology - Security techniques - Privacy architecture framework

[27] ISO 31000, Risk management - Principles and guidelines

END

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

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