

ICS 35.040
CCS L 80



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

GB/T 19715.2-2005

**Information technology -- Guidelines for the management of IT
security -- Part 2: Managing and planning IT security**

信息技术信息技术安全管理指南第2部分：管理和规划信息技术安全

(English Translation)

Issued on: April 19, 2005

Implemented on: October 1, 2005

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine of the People Republic of China, China National
Standardization Administration Committee**

Table of Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Structure

5 Purpose

6 Background

Foreword

GB/T 19715 "Information Technology Information Technology Security Management Guide" is divided into five parts.

--- Part 1. Information technology security concepts and models;

--- Part 2. Management and planning of information technology security;

--- Part 3. Information Technology Security Management Technology;

--- Part 4. Selection of protective measures;

--- Part 5. Protective measures for external connections.

This part is equivalent to the international standard ISO/IEC TR13335-2.:1997 "Information Technology Information Technology Security Management Guide No. 2 Part. Managing and Planning Information Technology Security.

The guides in this section present some of the basic topics of IT security management and the relationships between these topics. These guidelines are for logos and it is useful to manage all aspects of IT security.

This part is proposed by the Ministry of Information Industry of the People's Republic of China this part is under the jurisdiction of the National Information Security Standardization Technical Committee.

This part is composed of China Electronics Technology Standardization Institute (CESI), the 15th Research Institute of China Electronics Technology Group, and China Electronics Technology the 30th Research Institute of the Group and Shanghai Sanshi Guardian Information Security Co., Ltd. were drafted.

Introduction

The purpose of GB/T 19715 is to provide guidance on IT security management, not a solution. Those responsible for IT in the organization Safe individuals should be able to use the information in this standard to meet their specific needs. The main objectives of this standard are.

- a) define and describe concepts related to IT security management;
- b) identify the relationship between IT security management and general IT management;
- c) presented several models that can be used to explain IT security;
- d) Provides general guidance on IT security management.

This standard consists of several parts. Part 1 provides an overview of the basic concepts and models used to describe IT security management. This section Applicable to managers responsible for IT security and managers responsible for the overall security program of the organization.

This section describes management and planning aspects. It is related to the manager of the IT system responsible for the organization. They can be.

- a) IT managers responsible for overseeing the design, implementation, testing, procurement or operation of IT systems;
- b) the manager responsible for the actual use of the IT system;
- c) Of course there are managers responsible for IT security.

Part 3 describes the management activities involved in the life cycle of a project (such as planning, design, implementation, testing, acquisition, or operation).

Safety technology suitable for use.

Part 4 provides guidance on choosing protective measures and how they are supported through the use of baseline models and controls. It also describes How it complements the security techniques described in Part 3 and how to use additional evaluation methods to select protection measures.

Part 5 provides the organization with a guide to connecting its IT system to an external network. This guide contains anti-connection security the choice and use of protective measures, the services supported by those connections, and the additional safeguards for the connected IT systems.

GB/T 19715.2-2005/ISO/IEC TR13335-2:1997 Information Technology Information Technology Security Management Guide Part 2. Managing and planning information technology security

1 Scope

This section of GB/T 19715 addresses some of the basic topics of IT security management and the relationship between these topics. These partial pairs it is useful to identify and manage all aspects of IT security.

It is important to be familiar with the concepts and models presented in Part 1 for a comprehensive understanding of this section.

2 Normative references

The terms of the following documents become the provisions of this part by reference in this part of GB/T 19715. Quotations with dated , all subsequent amendments (not including errata content) or revisions do not apply to this section, however, encouragement is achieved under this section the parties to the agreement study whether the latest versions of these documents can be used. For undated references, the latest edition applies to this section.

GB/T 19715.1-2005 Information technology - Information technology - Safety management guide - Part 1. Information technology security concepts and models (ISO/IEC TR13335-1.:1996, IDT)

3 Terms and definitions

The terms and definitions established in GB/T 19715.1-2005 apply to this section, using the following terms. verifiability, assets, real Sex, availability, baseline control, confidentiality, data integrity, impact, integrity, IT security, IT security strategy, reliability, residual risk, wind Risk, risk analysis, risk management, protective measures, system integrity, threats, vulnerability.

4 Structure

This section has 17 chapters. Chapters 5 and 6 provide information on the purpose and background of this document. Chapter 7 provides successful IT an overview of the various activities involved in security management. Chapters 8 through 16 detail these activities. Chapter 17 provides a summary.

5 Purpose

The purpose of this section is to present various activities related to IT security management and planning, as well as related roles and responsibilities in the organization.

This is generally related to the IT manager responsible for the procurement, design, implementation, or operation of the IT system. In addition to IT security managers, but also

negative Responsible for the IT system to specifically use the activities of the managers concerned. In summary, this section is responsible for any negative management responsibilities related to the organization of IT systems.

People are useful.

6 Background

Government and commercial organizations rely heavily on the use of information for business activities. Confidentiality, integrity, availability, of information and services Loss of verification, authenticity and reliability can have a negative impact on the organization. Therefore, in the organization of protection information and management information technology (IT) security has important needs. In today's environment, this requirement to protect information is particularly important because many organizations pass the IT department.

The network is connected internally and externally.

IT security management is the process of achieving and maintaining confidentiality, integrity, availability, verifiability, authenticity and reliability.

of. IT security management features include.

a) Identify organizational IT security goals, strategies and strategies;

GB/T 19715.2-2005/ISO/IEC TR13335-2:1997