

ICS 35.040
CCS L 80



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

GB/T 31722-2015

**Information technology -- Security techniques -- Information
security risk management**

信息技术 安全技术 信息安全风险管理

(English Translation)

Issued on: June 2, 2015

Implemented on: February 1, 2016

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

Table of Contents

Foreword...	3
Introduction...	4
1 Scope...	6
2 Normative references...	6
3 Terms and definitions...	6
4 Structure of this Standard...	8
5 Background...	9
6 Overview of the information security risk management process...	10
7 Context establishment...	13
8 Information security risk assessment...	18
9 Information security risk treatment...	29
10 Information security risk acceptance...	34
11 Information security risk communication...	35
12 Information security risk monitoring and review...	36

Foreword

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

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

This Standard uses the translation method to be identical to ISO/IEC

27005.2008 "Information technology - Security techniques - Information security risk management" (English version).

The following changes have been made to this Standard.

- MAKE some editorial changes to the introduction.

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

Drafting organizations of this Standard. China Electronics Standardization

Institute, Shanghai 30Wish Information Security Co., Ltd., CEC Cyberspace Great Wall Co., Ltd., Shandong Computer Science Center, Beijing Information Security Test and Evaluation Center.

Main drafters of this Standard. Xu Yuna, Min Jinghua, Shangguan Xiaoli, Dong Huomin, Zhao Zhangjie, Li Gang, Zhou Mingle.

1 Scope

This Standard provides guidelines for information security risk management.

This Standard supports the general concepts specified in GB/T 22080 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

2 Normative references

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

GB/T 22080-2008 Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001.2005, IDT)

3 Terms and definitions

For the purposes of this document, the terms and definitions given in GB/T 22080-2008, GB/T 22081-2008 and the following apply.

Exchange or sharing of information about risk between the decision-maker and other stakeholders.

4 Structure of this Standard

This Standard contains the description of the information security risk management process and its activities.

Some of this guidance may not be suitable in all cases and so other ways of performing the action may be more appropriate.

Output. Identifies any information derived after performing the activity.

5 Background

The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

6 Overview of the information security risk management process

The context is established first. Then a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level then the task is complete and the risk treatment follows.

7 Context establishment

Depending on the scope and objectives of the risk management, different approaches can be applied. The approach might also be different for each iteration.

8 Information security risk assessment

It is up to the organization to select its own approach to risk assessment based on the objectives and the aim of the risk assessment.

Input. Information on threats obtained from incident reviewing, asset owners, users and other sources, including external threat catalogues.

9 Information security risk treatment

There are four options available for risk treatment. risk reduction (see 9.2), risk retention (see 9.3), risk avoidance (see 9.4) and risk transfer (see 9.5).

Action. The activity or condition that gives rise to the particular risk should be avoided.

10 Information security risk acceptance

Risk treatment plans should describe how assessed risks are to be treated to meet risk acceptance criteria (see 7.2 - Risk acceptance criteria). It is important for responsible managers to review and approve proposed risk treatment plans and resulting residual risks, and record any conditions associated with such approval.

11 Information security risk communication

Input. All risk information obtained from the risk management activities (see Figure 1).

12 Information security risk monitoring and review

.....