

ICS 35.040
CCS L 80



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

GB/T 32923-2016

**Information technology -- Security techniques -- Governance of
information security**

信息技术 安全技术 信息安全治理

(English Translation)

Issued on: August 29, 2016

Implemented on: March 1, 2017

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

Table of Contents

Preface
Introduction
1 Scope
2 Normative reference document
3 Terms and definitions
4 Concept
4.1 General
4.2 Goal
4.3 Expected results
4.4 Relationships
5 Principles and processes
5.1 Overview
5.2 Principle
5.3 Process
Appendix A (informative) Information Security Status Example
Appendix B (informative) Detailed information Security status Example
Reference

Foreword

This standard is drafted in accordance with the rules given in GB/T 1.1-2009.

This standard uses the translation method equivalent to ISO/IEC 27014.:2013 "information technology security technology information security management".

Introduction

This standard provides guidance on information security governance.

Information security has become a key issue in the organization. Not only increasing regulatory requirements, but also the organization of information security measures will be invalid Affect its reputation.

Therefore, it is increasingly necessary for organizational administrators to assume the responsibility of information security oversight in governance responsibilities to ensure the achievement of organizational goals.

In addition, in the organization of the managers, the implementation of managers and responsible for the implementation and operation of information security management system personnel, information security governance Provides a strong bond.

Information security governance provides an indispensable basis for promoting information security initiatives throughout the organization.

Furthermore, effective governance of information security ensures that managers receive reports of information security-related activities that are formed in the business context, Adequate and timely decision-making on information security issues to support the organization's strategic objectives.

Information technology security technology information security governance

1 Scope

This standard provides guidance on the concepts and principles of information security governance. Through this standard, an organization may be responsible for information security within its scope Activities for evaluation, guidance, monitoring and communication.

This standard applies to all types and sizes of organizations.

2 Normative reference documents

The following documents are indispensable for the application of this document. For dated references, only the dated edition applies to this article Pieces. For undated references, the latest edition (including all modifications) applies to this document.

GB/T 29246-2012 Information technology security technology Information security management system overview and vocabulary (ISO/IEC 27000.

2009, IDT)

3 Terms and definitions

GB/T 29246-2012 Definitions and the following terms and definitions apply to this document.

Executive manager

An individual or group of people who fulfill the intent of the organization and assume responsibility for the strategy and strategy assigned by the organization's governor.

Note 1: Execute managers form part of the top management. In order to clarify the role, this standard distinguishes between the two groups in the highest management. the manager and the executive the manager.

Note 2: Executives may include Chief Executive Officer/CEO (CEO), Government Agency Leader,

Chief Financial Officer/CFO, Chief Operating Officer /Operations Director (COO), Chief Information Officer/Information Director (CIO), Chief Information Security Officer/Information Security Director (CISO) and similar roles.

The manager

An individual or group of persons who are responsible for the performance and compliance of the organization.

Note: Governance forms part of top management. In order to clarify the role, this standard distinguishes between the two groups in the highest management. the manager and the executive manager.

Information security governance governanceofinformationsecurity Guide and control the organization of information security activities of the system.

Stakeholder any person or organization that has an impact, is affected or perceived to be affected by the organization's activities.

Note: Decision makers can be stakeholders.

4.1 General

Information security governance requires that information security objectives and strategies be aligned with business objectives and strategies and that compliance with laws, regulations, and