

ICS 35.040
CCS L 80



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

GB/Z 32906-2016

**Information security technology -- Guide of construction for
information security in small & medium E-commerce
enterprises**

(English Translation)

Issued on: August 29, 2016

Implemented on: March 1, 2017

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

Table of Contents

Foreword	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Abbreviations	
5 Structure and mode	
5.1 Application Structure	
5.2 Construction mode	
5.2.1 Overview	
5.2.2 Self-built mode	
5.2.3 Resource rental mode	
5.2.4 Store rental model	
5.3 Construction Process	
6 Security Risk	
6.1 Physical Risk	
6.2 Network Risk	
6.3 Host risk	
6.4 Data Risk	
6.5 Application Risk	
7 Security needs	
8 Safety design	
8.1 General principles	
8.2 Safety Structure	
8.3 Physical Security Design Requirements	
8.4 Network Security Design Requirements	
8.5 Host Security Design Requirements	
8.6 Data Security Design Requirements	
8.7 Application Security Design Requirements	
Safety Implementation	
9.1 Physical Security Implementation	
9.1.1 Overview	
9.1.2 Physical Security	

- 9.2 Network Security Implementation
 - 9.2.1 Overview
 - 9.2.2 Access Control Implementation
 - 9.2.3 Intrusion Prevention
 - 9.2.4 Network Equipment Protection
 - 9.2.5 Security Audit
- 9.3 Host Security Implementation
 - 9.3.1 Overview
 - 9.3.2 Stand-alone firewall
 - 9.3.3 Host Access Control
 - 9.3.4 Host Identification
 - 9.3.5 Host Intrusion Prevention
 - 9.3.6 Host malicious code to prevent
 - 9.3.7 Host Security Audit
- 9.4 Data Security Implementation
 - 9.4.1 General
 - 9.4.2 Data integrity testing
 - 9.4.3 Data Backup System
 - 9.4.4 Disaster Recovery
- 9.5 Application Security
 - 9.5.1 Overview
 - 9.5.2 Identity Authentication Security Implementation
 - 9.5.3 Transactional Security
- 10 Deployment of transport management
 - 10.1 Deployment and Installation
 - 10.2 Document Evaluation Review
 - 10.3 Safety Tests
 - 10.3.1 Safety Test Requirements
 - 10.3.2 Test Process Safety Management
 - 10.4 Put into operation
 - 10.5 Safety Management
 - 10.5.1 General requirements
 - 10.5.2 Security Policy
 - 10.5.3 Institutional and Personnel Management
 - 10.5.4 Safety Management System

10.5.5 Security Tracking Management

10.5.6 Information Security Audit Management

10.5.7 Emergency Management

10.6 Operational Risk Control Management

Appendix A (informative) typical model structure diagram

Appendix B (informative) small and medium e-commerce enterprise information security self-mode case

Appendix C (informative) project development process of self-construction or resource leasing mode of small and medium-sized e-commerce enterprises Security Management Case

References

Foreword

This instructional document has been drafted in accordance with the rules given in GB/T 1.1-2009.

Please note that some of this document may be patentable. The issuing agencies of this document do not bear the responsibility of identifying these patents.

This Guidance Document is proposed and managed by the National Technical Committee for Information Security Standardization (SAC/TC260).

The drafting of the guidance of technical documents. Zhejiang Institute of Standardization, Alibaba (China) Co., Ltd., Zhejiang Gongshang University, Zhejiang Economic Information Center, Xiamen Institute of Standardization, Zhejiang University of Science and Technology, Zhejiang Fluttering Dragon Network Technology Co., Ltd., Zhejiang Fuchunjiang Telecom Mobile Group Co., Ltd., Beijing Tian Rong Xin Technology Co., Ltd., Shanghai Tiantai Network Technology Co., Ltd., China Institute of Measurement.

1 Scope

This guidance document gives the construction of small and medium-sized e-commerce enterprise information security structure and mode, security risk, security requirements, security Design, implementation and deployment of safeguards and management of the guide.

The guidance of technical documents for small and medium-sized e-commerce business information security building for the development of e-commerce projects, operation and maintenance of for technical reference.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version applies to this article Pieces. For undated references, the latest edition (including all amendments) applies to this document.

Information Security Technology Information Systems Security Management Requirements
GB/T 20518 Information Security Technology Public Key Infrastructure Digital Certificate
Format GB/T 20988 Information security technology Information system disaster recovery
specifications Information technology - Security technology - Information security
management - Practical rules

3 Terms and definitions

The following terms and definitions apply to this document.

Small and medium e-commerce business smal the use of information network technology
to achieve electronic trading business activities, the annual number of electronic
transactions in the millions of companies below.

4 Abbreviations

The following abbreviations apply to this document.

CA. Certificate Authority (CertificateAuthority) CPU. Central Processing Unit
(CentralProcessingUnit) DDoS. Distributed Denial of Service (DistributedDenialofservice)
DES. Data Encryption Standard (DataEncryptionStandard) ERP. Enterprise Resource
Planning (EnterpriseResourcePlanning) HTTP. Hypertext Transfer Protocol
(HyperTextTransferProtocol) IDC. Internet Data Center (InternetDataCenter) IP. Internet
Protocol (InternetProtocol) IPsec. Internet Security Protocol (InternetProtocolSecurity)