Chinastandards.org

ICS 35.240
CCS A 90

GA

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GA/T 913-2010

Information security technology - Security technology requirements for database security audit products

信息安全技术 数据库安全审计产品安全技术要求

(English Translation)

Issued on: January 1, 1970 **Implemented on: January 13, 2019**

Issued by: Ministry of Public Security

Preview: page 1 of 5 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-913-2010

Chinastandards.org

Table of Contents

Foreword
1 Scope
2 Normative references
3 Terms and definitions
4 General description
4.1 Classification of safety technical requirements
4.2 Classification of Security Levels.
5 Safety function requirements
5.1 Audit Generation Unit Component Requirements
5.2 Audit response unit component requirements
5.3 Audit processing unit component requirements
5.4 Identification and authentication
5.5 Security Management
5.6 Audit logs
6 Security requirements
6.1 Development
6.2 Guidance documents
6.3 Life cycle support
6.4 Testing
6.5 Vulnerability assessment
7 Classification requirements
7.1 Safety function requirements
7.2 Security requirements

Foreword

This standard was drafted in accordance with the rules of GB/T 1.1-2009.

This standard replaces GA/T 913-2010 "Security Technical Requirements for Information Security Technology Database Security Audit Products" and GA/T 913-2010 the main technical changes are as follows.

-Added the contents of "Classification of Security Technical Requirements" and "Classification of Security Levels" (see 4.1, 4.2);

Preview: page 2 of 5 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-913-2010

--Modified the contents of "Data Collection", "Collection Strategy", and "Security Alert" (see 5.1.1, 5.1.2, 5.2.1, 2010) 4.1.1, 4.1.4, 4.2.1 of the annual version);

-Deleted the contents of "Remote Confidential Transmission" and "Trusted Management Host" (see 5.2.3 and 5.2.4 of the 2010 version);

-Added the content of "Remote Security Management" (see 5.5.3);

-Unified "safety function requirements" and "own safety function requirements" into "safety function requirements" (see Chapter 5, 2010 Chapters 4 and 5 of the annual edition);

-Modify the "security assurance requirements" to "security assurance requirements" and adjust the corresponding content (see Chapter 6, Chapter 6 of the 2010 edition);

-The levels are uniformly divided into basic and enhanced levels (see Chapter 7, Chapter 7 of the 2010 edition).

This standard was proposed by the Cyber Security Bureau of the Ministry of Public Security.

This standard is under the jurisdiction of the Information System Security Standardization Technical Committee of the Ministry of Public Security.

This standard was drafted. Computer Information System Security Product Quality Supervision and Inspection Center of the Ministry of Public Security (Third Research Institute of the Ministry of Public Security), Hangzhou Anheng Information Technology Co., Ltd.

1 Scope

This standard specifies the security function requirements, security guarantee requirements, and classification requirements for database security audit products.

This standard applies to the design, development, and testing of database security audit products.

2 Normative references

The following documents are essential for the application of this document. For dated references, only the dated version applies to this document.

For undated references, the latest version (including all amendments) applies to this document.

GB/T 18336.3-2015 Information technology security technology Information technology security assessment guidelines Part 3. Security assurance components GB/T 25069-2010 Information Security Technology Terminology

Preview: page 3 of 5 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-913-2010

3 Terms and definitions

GB/T 18336.3-2015 and GB/T 25069-2010 and the following terms and definitions apply to this document.

Database security audit product A product that records, analyzes, and responds to user actions when accessing the database.

Audit record

Data generated by auditing the user's access to the database.

Audit log

Data generated by the audit of the database security audit product itself.

Audit producing unit A functional unit that collects and generates audit records.

Audit responding unit A functional unit that responds to a specified event.

Audit processing unit Functional unit for statistics and management of audit records.

4.1 Classification of safety technical requirements

This standard divides the database security audit product security technical requirements into two categories. security function requirements and security assurance requirements. Among them, safety Functional requirements are specific requirements for the security functions that database security audit products should have; security assurance requirements are for database security audits the product's life cycle process puts forward specific requirements, including development, guidance documents, life cycle support and testing.

4.2 Classification of security levels

The security level of the database security audit product is divided into basic level and enhanced according to the strength of its security function requirements and security assurance requirements.

Level, in which the security requirements refer to GB/T 18336.3-2015.

5.1.1 Data Collection

The product should be able to gather at least the following information about database operation behavior from the target environment.

a) Event subject. source IP address, source MAC address, source port, and operating user;

b) Event object. destination IP address, destination MAC address, destination port and operation object. The operation object includes database, data Data tables, data table

Preview: page 4 of 5 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-913-2010

fields, etc .;

c) the date and time of the event;

d) Event type. such as data operation class, structure operation class, transaction operation class, user management class and other auxiliary operation classes;

e) Event description. specific content of the operation, such as operation statements;

f) Event result. success or failure, number of affected rows, response time, number of returned rows, etc.

5.1.2 Collection Strategy

The product should be able to set a collection strategy based on a combination of the following conditions.

a) the subject of the event;

b) the object of the event;

c) the date and time of the event;

d) event type;

e) keywords for event descriptions;

f) Event results.

5.1.3 Audit record generation

When an audit event occurs, the product should generate audit records in a timely manner in accordance with the collection strategy.

5.1.4 Impact on the system

The data collection method and process should not have a significant impact on the performance of the database.

5.1.5 Communication encryption support

When users access the database using the encryption method supported by the product, the product should have the ability to collect the information in 5.1.1.

5.2.1 Security alarm

The product should be able to alert the following abnormal events.

a) Custom violation events, such as deleting important data, affecting rows and returning rows exceeding thresholds;

Preview: page 5 of 5 shown, 10 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-913-2010