ICS 35.030
CCS L80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 20945-2023

Information security technology - Technical specification for network security audit products

信息安全技术 网络安全审计产品技术规范

Issued on: May 23, 2023 **Implemented on: December 1, 2023**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

Foreword

This document is in accordance with the provisions of GB/T 1:1-2020 "Guidelines for Standardization Work Part 1: Structure and Drafting Rules for Standardization Documents" drafting. This document replaces GB/T 20945-2013 "Information Security Technology Information System Security Audit Product Technical Requirements and Test Evaluation Method Compared with GB/T 20945-2013, except for structural adjustment and editorial changes, the main technical changes are as follows:

--- Changed the terms and definitions "event", "security audit", "audit record", "product log", "audit center" and "audit probe" (see 3:3, 3:4, 3:6, 3:7, 3:8, 3:9, 3:1, 3:2, 3:4, 3:5, 3:6, 3:7 of the:2013 edition);

--- Changed the overview (see Chapter 5, Chapter 5 of the:2013 edition);

---Changed the "audit content" (see 6:1:2, 6:1:1:2:1, 6:2:1:2:1 of the:2013 edition);

--- Deleted the "extended analysis interface" (see 6:2:1:2:2:5 of the:2013 edition);

--- Added "custom event" (see 6:1:6:4);

--- Added "product upgrade" (see 6:1:6:5);

---Changed "identification and authentication" (see 6:2:1, 6:1:2:1, 6:2:2:1 of the:2013 edition);

--- Added "user information security" (see 6:2:5);

--- Added "support system safety" (see 6:2:9);

--- Added "environmental adaptability requirements" (see 6:3);

--- Added "performance requirements" (see 6:4);

--- Changed the "safety guarantee requirements" (see 6:5, 6:1:3, 6:2:3 of the:2013 edition);

--- Added the normative appendix "Audit product basic level and enhanced level technical requirements and minimum set of evaluation methods" (see Appendix B): Please note that some contents of this document may refer to patents: The issuing agency of this document assumes no responsibility for identifying patents: This document is proposed and managed by the National Information Security Standardization Technical Committee (SAC/TC260): This document was drafted by: The Third Research Institute of the Ministry of Public Security, Beijing Shenzhou Lvmeng Technology Co:, Ltd:, Beijing Tianrongxin Network Security Technology Co:, Ltd: Company, Qi Anxin Wangshen Information Technology (Beijing) Co:, Ltd:, Venus Information Technology Group Co:, Ltd:, Xi'an Jiaotong University Jabil Network Technology Co:, Ltd:, Institute of Information Engineering, Chinese Academy of Sciences, Hangzhou Meichuang Technology Co:, Ltd:, Sangfor Technology Co:, Ltd:, Shanghai Haishi Information Security Evaluation and Certification Center, Landun Information Security Technology Co:, Ltd:, Huaxin Consulting Design and Research Institute Co:, Ltd:, Changchun Ji Dazhengyuan Information Technology Co:, Ltd:, China Network Security Review Technology and Certification Center, The First Research Institute of the Ministry of Public Security, China Electric Power Science Research Institute Co:, Ltd:, Beijing Shanshi Network Information Technology Co:, Ltd:, Beijing Municipal Information Security Center (Beijing Information Security Evaluation Center), Beijing Baidu Netcom Technology Co:, Ltd:, Changyang Technology (Beijing) Co:, Ltd:, Yuanjiang Shengbang (Beijing) Network Security Technology Co:, Ltd: Ltd: The main drafters of this document: Wang Zhijia, Shen Liang, Lu Zhen, Song Haohao, Gu Jian, Yu You, Hu Weina, Deng Qi, Xiao Ying, Bai Shuang, Liu Yan, Zhang Weifeng, He Jianfeng, An Gaofeng, Han Dongxu, Zhou Jie, Ye Runguo, Xu Tonghai, Sun Xiaoping, Liu Qiang, Zou Yi, Shen Yongbo, Zhao Hua, Yang Chenghao, Yao Shengying, Zhou Zhaodong, Jia Ling, Li Junzuo, Dong Ping: The release status of previous versions of this document and the documents it replaces are as follows:

1 Scope

GB/T 20945-2023 specifies what a network security audit product has to do. Audit is the function that makes everything else in security accountable: it records what happened on the network and who did it, and it is what an investigation reads after an incident and what a regulator asks for. That gives it a requirement most security products do not have - its own records must be trustworthy, which means they must be complete, accurately timestamped, and impossible for an attacker with administrative access to alter or delete quietly, since tampering with the audit trail is a standard step in a serious intrusion. A product that collects logs but cannot protect them is not an audit product. This document specifies the technical requirements for network security audit products and describes the corresponding evaluation methods, so that conformance is tested rather than claimed. It applies to the design, development, testing and evaluation of such products. Under ICS 35.030 and CCS

L80, it is written for the vendors of audit and log management systems, for the testing laboratories that certify them under China's security product regime, and for the organisations selecting one.

This document specifies the technical requirements for network security audit products and describes the evaluation methods: This document applies to the design, development, testing and evaluation of network security audit products:

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text: Among them, dated references For documents, only the version corresponding to the date is applicable to this document; for undated reference documents, the latest version (including all amendments) is applicable to this document:

GB/T 18336:1-2015 Information technology security technology Information technology security assessment criteria Part 1: Introduction and general Model

GB/T 18336:3-2015 Information Technology Security Technology Information Technology Security Assessment Criteria Part 3: Security Assurance Components

GB/T 25069-2022 Information Security Technical Terminology

GB/T 35273-2020 Personal Information Security Specifications for Information Security Technology

3 Terms and Definitions

GB/T 18336:1-2015, GB/T 18336:3-2015 and GB/T 25069-2022 and the following terms and definitions apply used in this document: 3:1 network security network security The maintenance of confidentiality, integrity and availability of information stored, transmitted and processed in the network environment: [Source: GB/T 25069-2022, 3:616] 3:2 abnormal abnormal A deviation from a previously verified condition, state, or behavior observed from documentation, operation, or monitoring:

Note: Generally, the subjects involved in anomalies may be people, equipment, applications, services/processes, data, etc: Because the identified anomalies point to different subjects, they can be divided into Abnormal user behavior, abnormal device operation, abnormal program execution, abnormal service operation, abnormal data, etc: [Source: GB/T 32422-2015, 3:1, modified] 3:3 event incident Attempts to alter the state of an object and cause or may cause abnormal or damaging behavior to occur: [Source: GB/T 25069-2022, 3:552, modified] 3:

4 Security audit securityaudit Independent review and examination of the records and activities of networks, information systems and their components to test the adequacy of

system controls to ensure