GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 20274.1-2023

Replacing GB/T 20274.1-2006

Information Security Technology - Evaluation Framework for Information Systems Security Assurance - Part 1: Introduction and General Model

信息安全技术

信息系统安全保障评估框架

第 1 部分：简介和一般模型

Issued on: March 17, 2023 **Implemented on: October 1, 2023**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Information Security Technology - Evaluation Framework for Information Systems Security Assurance - Part 1: Introduction and General Model

1 Scope

This document provides the basic concept and model of information system security assurance, and proposes the evaluation framework for information system security assurance.

This document is applicable to guide system builders, operators, service providers and evaluators in carrying out information system security assurance work.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 18336.1-2015 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1: Introduction and General Model

GB/T 25069-2022 Information Security Techniques - Terminology

3 Terms and Definitions

What is defined in GB/T 25069-2022 and GB/T 18336.1-2015, and the following terms and definitions are applicable to this document.

3.1 information system

Information system refers to a combination of applications, services, information technology assets or other information processing components.

NOTE 1: information system is usually composed of computers or other information terminals and related equipment, and carries out information processing or process control in accordance with certain application objectives and rules.

NOTE 2: typical information systems, such as: office automation system, cloud computing platform / system, Internet of Things, industrial control system and systems adopting mobile Internet technology, etc.

[source: GB/T 29246-2017, 2.39, modified]

3.2 information system security assurance

Information system security assurance refers to a series of appropriate behaviors or processes that guarantee the security attributes, functions and efficiency of information system.

3.3 organizational security policies

Organizational security policies refer to number of security rules, procedures, practices and guidelines established by an organization to guarantee its operation.

[source: GB/T 25069-2022, 3.817]

4 Overview

The relevant parties related to the evaluation of information system security assurance generally include information system builders, information system operators, service providers and evaluators, etc.

Information system builders include planning, design and engineering implementation personnel. Builders take the general description language, method and structure as a reference, and express their information system security assurance requirements from the fields of techniques, management and engineering of information system security assurance. Adopting this document can help builders better describe their information system security demands, and prepare information system security assurance schemes and specifications that comply with the requirements of their operating environment. Builders can understand the current situation of their information system security assurance based on the evaluation of information system security assurance, and further perfect and continuously improve their information system security assurance capabilities based on the evaluation results.

Information system operators take the general description language, method and structure as a reference, and express their information system security assurance requirements from the fields of techniques and management of information system security assurance. Operators can adopt this document to communicate more effectively with information system builders and other relevant personnel, and understand each other. Operators can understand the current situation of their information system security assurance based on the evaluation of information system security assurance, and further perfect and continuously improve their information system security assurance capabilities based on the evaluation results, so as to gain confidence in information system security assurance.

Service providers take the general description language, method and structure as a reference, and express relevant information system security assurance requirements from the fields of techniques, management and engineering of information system security assurance, and effectively communicate and implement projects with system operators and builders.

assurance class, security management assurance class and security engineering assurance class. Members of the classes are called subclasses.

The security assurance subclass is a combination of several sets of security assurance requirements, which aim at the same security assurance purpose, but differ in strength and degree. The subclasses of the security technical assurance class, security management assurance class and security engineering assurance class are respectively security technical assurance subclass, security management assurance subclass and security engineering assurance subclass. Members of the subclasses are called security assurance components. Each security assurance subclass consists of one or multiple security assurance components that implement the security assurance purpose.

The security assurance component is a collection that describes an explicit security assurance requirement, and it is an optional minimum security assurance requirement collection included in the structure defined in this document. The security assurance component is a specific control measure for information security assurance to realize the security assurance purpose of its security assurance subclass. In accordance with the different fields, to which, the security assurance requirements belong, they are divided into security technical assurance component, security management assurance component and security engineering assurance component. The security assurance component consists of optional security assurance elements.

The security assurance component is the specific control measure for information security assurance to realize the security assurance purpose. The dependencies among security assurance components and the operations allowed by security assurance components are described below.

a) Dependencies among security assurance components.

   There may be dependencies among the security assurance components. When a security assurance component cannot adequately express security assurance requirements and depends on the existence of another security assurance component, dependencies arise. The dependencies may exist among the internal components of security technical assurance, security management assurance and security engineering assurance, or among the components of security technical assurance, security management assurance and security engineering assurance.

b) Operations allowed by security assurance components.

   The security assurance components are used as defined in this document. Or the security assurance components are tailored by using the operations allowed by the security assurance components, so as to satisfy specific security policies or combat specific threats. The security assurance components specify and define whether the components allow the operations of “assign” and “select”, under what circumstances these operations can be used on the components, and the consequences of using these operations. Any security assurance components allow the operations of “repeat” and “refine”. These four operations are described below:

assumptions, threats and organizational security policies, etc.

In the management system, the existing management and organizational structure, the corresponding rules and regulations used, and the involved important assets of the information system shall be described.

a) Description of organization: describe the management / application / development / integration / support, etc. related to the information system within the organization, especially the organization related to security assurance management.

b) Description of management systems, laws and regulations: list the corresponding rules and regulations, and relevant laws and regulations currently in use related to the management of the information system.

c) Description of system assets: describe the physical assets (referring to various hardware and physical facilities in the information system), software assets (application software and system software, etc.) and information assets (referring to valuable information related to the information system itself and various related information of office, management and business stored, processed and transmitted by the information system generated during the information system life cycle of information system planning and organization, development and procurement, implementation and delivery, operation and maintenance, and disposal) of the information system.

In the technical system, the various existing applications, corresponding network infrastructure and the technical standards adopted shall be described.

Starting from the perspectives of business and application, and based on the technical system, the business system shall classify and describe the main business applications of the organization. In addition, through the business process and business information flow (describing the interface and corresponding data flow of the main business application; the data flow description shall include the type of data and the general mode of data transmission), it shall make further interpretations.

6.2.3 Confirmation of security environment

The security environment includes all explicitly related legal policies, organizational policies and physical environment, which defines the operating environment of the information system. In order to establish a secure environment, the information system operators shall analyze these factors.

In the description of assumptions, security threats and organizational security policies, the following contents shall be noted:

a) Statement of assumptions: if the environment satisfies the assumptions, the information system is considered secure;

b) Statement of security threats: point out all threats found in the security analysis related to the information system.

NOTE 1: this document describes a threat in terms of threat motives, assumed method of attack, any weakness on which the attack is based, and the name of the asset being attacked. The evaluation of security risks is realized by providing the possibility of the actual occurrence of each threat, the possibility of successful implementation of the threat and the possible damages and consequences.

c) Statement of organizational security policies: clarify relevant policies and rules.

NOTE 2: for specific information systems, such policies may be explicitly mentioned, whereas for information systems in general, it may be necessary to assume the organization's security policies.

6.2.4 Confirmation of security assurance goals

The environmental security analysis results are used to clarify the security goals, confront the threats and illustrate the identified organizational security policies and assumptions. The security assurance goals shall be consistent with the stated legal and regulatory requirements, organizational environmental requirements and physical environment of the operation of the information system.

The purpose of confirming the security assurance goals is to clarify all security considerations and point out which security issues are directly addressed by the information system, and which are addressed by its environment. This classification is based on a process that combines engineering judgment, security policies, economic factors and acceptable risk decision-makings.

6.2.5 Confirmation of security assurance elements

The security assurance elements of the information system are to subdivide the security assurance goals into a series of security assurance requirements of the information system and its environment. Once these requirements are satisfied, it can be guaranteed that the information system can achieve its security assurance goals.

The security assurance elements shall be proposed respectively from the technical assurance requirements of the security technical field, the management assurance requirements of the security management field and the engineering assurance requirements of the security engineering field.

closed-loop structure of the information system life cycle. At any point in the information system life cycle, the security assurance elements of techniques, management and engineering shall be integrated to implement security assurance of the information system.

a) Planning and organization stage: due to the organization's mission requirements and business requirements, the demands for the construction and application of information system security assurance are generated. In this stage, the risks and policies of the information system shall be added to the decision-makings of the construction and application of the information system. From the beginning of information system construction, the security assurance elements of the system shall be comprehensively considered, so that the construction of the information system and the construction of information system security assurance can be synchronously planned, implemented and applied.

b) Development and procurement stage: this stage is the refinement, thoroughness and concrete embodiment of the planning and organization stage. In this stage, management activities, such as: system demand analysis, consideration of system operation demands, system design, and related budge application and project preparation, etc. are carried out. In this stage, based on system demands, risks and policies, the information system security assurance shall be considered as a whole in the design and construction of the system; from a global perspective, an overall planning for the information system security assurance shall be established. In accordance with the specific requirements, the overall technical and management security assurance or design of the system shall be evaluated, so as to ensure that the overall planning of the information system satisfies the organization's construction requirements, and relevant national regulations, industry codes and other requirements of the organization.

c) Implementation and delivery stage: in this stage, the organization can ensure the service capability of the construction organization through the requirements for the security service qualifications of the construction side and the qualification requirements for the information security professionals; the organization can also supervise and evaluate the implementation of the construction process through the engineering assurance of information system security assurance, and finally ensure the security of the delivered system.

d) Operation and maintenance stage: after the information system enters the operation and maintenance stage, the comprehensive assurance of the management, operation and maintenance of the information system, and the capabilities of the users is the fundamental guarantee for the secure and normal operation of the information system. After the information system is put into operation, it is not unchangeable. With the changes of business and demands, and the external environment, new requirements will be generated, or the original requirements will be strengthened, thus, re-entering the initial planning stage of the information system.

e) Disposal stage: when the assurance of the information system cannot satisfy the

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------