YD

COMMUNICATION INDUSTRY STANDARD

OF THEPEOPLE'S REPUBLIC OF CHINA

YD/T 1730-2008

Implementation guide for security risk assessment of telecom network and internet

电信网和互联网安全风险评估实施指南

Issued on: January 14, 2008 **Implemented on: January 14, 2008**

Issued by: Ministry of Information Industry of PRC

Table of Contents

Implementation guide for security risk assessment of telecom network and internet

1 Scope

This standard specifies the elements of risk assessment for telecom network and internet security, the relationship between the elements, the implementation process, the form of work, the principles to be followed, the different requirements and implementation points at different stages of the life cycle of telecom network and internet.

This standard applies to the risk assessment work of the telecom networks and the internet.

This standard can be used as an overall guidance document for the security risk assessment of telecom network and internet. For the security risk assessment of specific networks, please refer to the security protection requirements and security protection testing requirements of specific networks.

2 Normative references

The provisions in following documents become the provisions of this Standard through reference in this Standard. For the dated references, the subsequent amendments (excluding corrections) or revisions do not apply to this Standard; however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB/T 5271.8-2001 Information technology - Vocabulary - Part 8: Security

GB/T 9361-2000 Security requirements for computer field

GB/T 19716-2005 Information technology - Code of practice for information security management

YD/T 754-95 General rules for electrostatic protection of communication rooms

YD/T 5026-2005 Installation and design standard for cabling duct in the room of telecommunication

YD 5002-94 Design standard for fire protection of posts & communications building

YD 5098-2005 Specifications of engineering design for lightning protection and

4.4.5 Confidentiality principle

The assessor shall sign relevant non-disclosure agreements and non-invasive agreements with the assessed network and service operators, so as to protect the interests of the assessed party.

5 Implementation of risk assessment

5.1 Preparation for risk assessment

The preparation of the risk assessment is the guarantee of the effectiveness of the whole risk assessment process. Implementing a risk assessment is a strategic consideration; the results will be affected by the organization's business strategy, business processes, security requirements, system size, structure, etc. Therefore, before the implementation of a risk assessment, the following preparations shall be made:

a) Obtain support and cooperation;

b) Determine the objectives of the risk assessment;

c) Determine the content of the risk assessment;

d) Form a risk assessment team;

e) Conduct research on the assessed subject;

f) Determine the assessment basis and method.

5.1.1 Get support and cooperation

The self-assessment shall be approved by the managing-personnel who are responsible for the relevant work of the organization. The tasks of the relevant management and technical personnel in the risk assessment work shall be clarified. For the inspection assessment, the network and service operators under assessment have the responsibility and obligation to support and cooperate, so as to ensure the smooth progress of the inspection assessment.

5.1.2 Determine objectives

The preparation stage of risk assessment shall clarify the objectives of risk assessment, and provide guidance for the process of risk assessment.

The goal of risk assessment for system of telecom network and internet is to identify the technical and management vulnerabilities, threats faced, possible risks of system of telecom network and internet; be clear with the objective risks; propose and implement appropriate security protection measures in a targeted manner; thereby reducing the

occurrence of security events; meeting the security requirements of the sustainable development of the organization's business; maintaining and improving the organization's competitive advantage, profitability and corporate image; meeting the requirements of the country and industry for system of telecom network and internet.

5.1.3 Determine the content

Determining the risk assessment content, based on the risk assessment objective, is the premise of completing the risk assessment. The content of the security risk assessment of the system of telecom network and internet can be all the assets and management institutions in the entire system of telecom network and internet, OR it can be the independent assets and related departments of a certain part of the system of telecom network and internet. The content of risk assessment includes management security risks and technical security risks. The risk assessment content of management security includes security management organization, security management system, personnel security management, system building management, system operation and maintenance management, etc. The risk assessment content of technical security includes business/application security, network security, equipment security, physical environment security, etc.

5.1.4 Form a team

Appropriate risk assessment management and implementation teams shall be formed to support the advancement of the entire risk assessment process. The risk assessment team for self-assessment can be formed by the relevant business key-personnel, technical personnel and management personnel of the development, maintenance and management of the network and service operators. The risk assessment team for inspection assessment may consist of a competent authority and assessment agency. The assessment team shall be able to ensure that the risk assessment work is carried out effectively.

5.1.5 Research the assessed object

The risk assessment team shall conduct sufficient research on the assessment objects, in the system of telecom network and internet. The research content shall include the network structure and network environment; the main hardware and software and the data and information contained therein; the personnel of management, maintenance and use. Focus on researching the asset value, existing vulnerabilities and threats of the assessed object, so as to lay the foundation for the selection of the basis and method of risk assessment AND the implementation of the assessment.

The survey of assessed objects can be carried out by a combination of questionnaire survey and on-site interview. Questionnaire is a question form, that provides a set of management or operation control questions for technical or management personnel to fill in; on-site interview is for assessors to observe and collect information, on the physical environment and operation of the assessed party.

certain conditions and circumstances, which is the most difficult part of vulnerability identification. Incorrect, ineffective, or not properly implemented security measures can be a vulnerability in themselves.

The methods used in vulnerability identification mainly include questionnaire survey, tool detection, manual verification, document review, penetration testing, etc. It shall be noted that, when identifying the asset vulnerabilities of has-been-running system of telecom network and internet, it is necessary to avoid affecting the normal operation of the system of telecom network and internet, as much as possible; it shall be completed in the experimental environment of equal conditions, as much as possible.

Vulnerability identification takes assets as the core; identifies the vulnerabilities that may be exploited by threats for each asset; evaluates the severity of the vulnerabilities. It can also be identified from the physical environment, equipment and systems, network, business/application, etc.; then combined with assets and threats. The data for vulnerability identification shall come from the owners and users of assets, experts in the business field of the system of telecom network and internet, as well as professionals in software and hardware, etc.

Vulnerability identification is mainly carried out from two aspects: technology and management. Technical vulnerability involves security issues at the physical environment layer, equipment and system layer, network layer, business/application layer. Management vulnerability can be divided into technical management vulnerability and organization management vulnerability. The former is related to specific technical activities, whilst the latter is related to the management environment.

For different identification objects, the specific requirements for vulnerability identification shall be implemented, with reference to the corresponding technical or management standards. For example, the vulnerability identification of the physical environment can be implemented, with reference to the technical indicators in such standards as GB/T 9361-2000, YD/T 5026-2005, YD 5098-2005, YD 5002-94, YD/T 754-95; the vulnerability identification of the equipment and network can refer to the technical indicators in the standards, such as YDN 126-2005 and YDN 127-2005; the identification of management vulnerability can refer to the requirements in the standards, such as GB/T 19716-2005, ISO/IEC 17799-2005, ISO/IEC 13335.1-2004, to carry out inspections of security management systems and their implementation, and identify management loopholes and deficiencies.

Table 9 provides a reference for the content of vulnerability identification.

taken. If the risk result is within the acceptable range, the risk is acceptable and the existing risk shall be maintained. If the risk result is out of acceptable range, it is an unacceptable risk; then it is necessary to formulate a risk treatment plan and take new security measures to reduce and control the risk.

It shall comprehensively consider the risk control cost and the impact of the risk; combine the security level of the network or system, where the asset is located, to propose an acceptable risk threshold.

5.7.3 Risk treatment plan

For unacceptable risks, a risk treatment plan shall be developed based on the vulnerabilities and threats that lead to the risk. The risk treatment plan specifies the new security measures to compensate the vulnerability; reduces the loss as caused by the security event; or reduces the occurring possibility of security event, the expected effects, the implementation conditions, the schedule, the responsible departments, etc. The selection of security measures shall fully take into account the possible constraints of organization, capital, environment, personnel, time, law, technology, social culture, considering both management and technology; the management measures can be used as a supplement to technical measures. The selection and implementation of security measures shall refer to relevant national and industry standards.

After selecting new security measures for unacceptable risks, in order to ensure the effectiveness of security measures, re-assessment shall be carried out to determine whether the residual risk, after the implementation of new security measures that has been reduced to an acceptable level. The assessment of residual risk can be carried out according to the risk assessment process of this standard; it can also be appropriately reduced.

For some risks, after the selection of new security measures, the risk assessment result of residual risk is still within the unacceptable range. In this case, it shall be considered whether to accept this risk OR further increase the corresponding security measures.

5.8 Risk assessment documents

5.8.1 Requirements for risk assessment documents

During the risk analysis process of the system of telecom network and internet, it shall record the risk assessment process; keep it as an assessment document. It shall meet (but not be limited to) the following requirements:

a) Ensure that documents are approved prior to publication;

b) Ensure that changes to the document and the current revision status are identifiable;

c) Ensure that the distribution of the documentation is properly controlled AND that the relevant version of the applicable documentation is available at the time of use;

d) Prevent the unintended use of obsolete documents; if obsolete documents need to be retained for any purpose, they shall be properly identified.

Controls required for identification, storage, protection, retrieval, shelf life, disposal shall also be specified, in relevant documents which are formed during the risk assessment process.

5.8.2 Risk assessment documents

Risk assessment documents include assessment process documents and assessment result documents, which are generated in the entire risk assessment process. Risk assessment documents include (but are not limited to) the following items:

a) Risk assessment plan: Describe the objectives, scope, personnel, assessment methods, form of assessment results, implementation progress of risk assessment;

b) Risk assessment procedure: Clarify the purpose, responsibilities, process, relevant document requirements of risk assessment, as well as various assets, threats, vulnerability identification, judgment basis, which are required for the implementation of this assessment;

c) Asset identification list: Identify assets, according to the asset classification method, which is determined by the organization in the risk assessment procedure document; form an asset identification list; specify the person/department responsible for the asset;

d) List of important assets: According to the results of asset identification and assignment, form a list of important assets, including the name, description, type, importance, responsible person/department, etc. of the important asset;

e) Threat list: According to the results of threat identification and assignment, form a threat list, including threat name, type, source, motivation, frequency of occurrence;

f) Vulnerability list: According to the results of vulnerability identification and assignment, form a vulnerability list, including the name, description, type, severity of specific vulnerabilities;

g) Confirmation table of existing security measures: According to the confirmation results of security measures that have been taken, form a confirmation table of existing security measures, including the name, type, function description, implementation effect of existing security measures;

6.3 Risk assessment of design stage

The risk assessment, in the design stage, needs to put forward the security function requirements, in the construction plan, according to the operating environment and the importance of the assets which are specified in the start-up stage; judge the compliance of the security function, as the basis for the risk control of the procurement process.

The assessment object, at this stage, is the construction plan. It shall assess, in a detailed manner, the description of the threat, the list of assets such as specific equipment and software that will be used, the security function requirements of these assets.

The assessment at this stage includes the following:

a) Whether the physical and natural environment, internal and external intrusion and other threats which are faced after the construction of the system of telecom network and internet, have been analyzed; whether the overall security strategy for the construction of the system of telecom network and internet has been formulated;

b) Whether certain measures have been taken to deal with possible failures of the system of telecom network and internet; whether risks that may arise from access to other networks have been considered;

c) Whether the development method is selected, according to the development scale, time and network characteristics; whether the software, hardware and network involved are analyzed and selected, according to the design and development plan and user needs;

d) Assess the vulnerabilities of the technical implementation, in the design or prototype, as well as personnel and organizational management, including the management vulnerabilities in the design process and the inherent vulnerabilities of the technology platform;

e) The impact of the security control measures and security technical assurance means, which are used in the design activities, on the risk results; this assessment needs to be repeated, after the security requirements and design changes.

The risk assessment in the design stage shall determine the compliance of the security functions, which are provided by the construction plan, with the security protection requirements of the system of telecom network and internet. The assessment results shall ultimately be reflected in the design report or construction implementation plan of the system of telecom network and internet.

6.4 Risk assessment of implementation stage

The purpose of the risk assessment, in the implementation stage, is to identify risks in the development and implementation process of the system of telecom network and internet, according to the security requirements and operating environment of the system of telecom network and internet; meanwhile, conduct security testing and quality control during the implementation and acceptance of the system of telecom network and internet, based on the threats analyzed in the design stage and the established security control measures.

The assessment object at this stage is the realization degree of security measures, so as to determine whether security measures can resist the influence of existing threats and vulnerabilities.

The risk assessment in the implementation stage includes assessment at two stages: the development stage and the implementation delivery stage.

The specific assessment content, in the development stage, includes:

a) Assess the impact of relevant standards for risk assessment in the communications industry, on security requirements;

b) Assess whether security requirements effectively support the functions of system of telecom network and internet;

c) Assess the assets, threats, vulnerabilities of system of telecom network and internet; and analyze the relationship between costs and benefits, so as to determine the most appropriate preventive measures in compliance with relevant laws, policies, standards, functional needs;

d) Assess the security activities in the development stage, including the content of security development, monitoring of the development process, prevention of security problems, response to requirements changes, monitoring of external threats.

The specific assessment contents, in the implementation delivery stage, include:

a) According to the actual built system of telecom network and internet, analyze the threats they face in detail;

b) According to the construction goals and security requirements, conduct acceptance tests on the security functions of the system of telecom network and internet; evaluate whether the security functions can resist security threats;

c) Assess whether an organizational management system, which is consistent with the overall security strategy, has been established;

Appendix A

(Normative)

Calculation method of asset value

This Appendix introduces several calculation methods of asset value. The appraiser can EITHER flexibly choose the corresponding calculation method according to the actual situation, OR adopt other calculation methods.

A.1 Logarithmic method

Usually, according to the actual experience of the system of telecom network and internet, the highest one of the three security attributes has the greatest impact on the final asset value. In other words, the assignment of the overall security attribute does not increase linearly, with the increase of the three attribute values; the higher attribute value has greater weights. Therefore, the following formula can be used to calculate the asset value:

$$\text{Asset Value} = \text{Round1}\{\text{Log}_2[(\alpha \times 2^I + \beta \times 2^V + \gamma \times 2^A]\}$$

In which, I stands for social influence assignment; V stands for business value assignment; A stands for availability assignment; Round 1{} means rounding-off, retaining 1 decimal place; Log2[] means taking the logarithm with the base 2; α, β and γ represent the weights of social influence, service value, and availability, respectively. According to specific network conditions, the network and service operators may determine the values of α, β, γ --- $\alpha \geq 0$, $\beta \geq 0$, $\gamma \geq 0$, and $\alpha + \beta + \gamma = 1$.

The calculated asset value is rounded up, so as to determine the grade of asset value.

A.2 Matrix method

The characteristic of the matrix method is to establish the corresponding matrix of the asset's social influence, business value, and availability; meanwhile, it determines the asset value in advance according to a certain method. To use this method, it is necessary to first determine the asset's social influence, business value, and availability; then, check the matrix to obtain the asset value.

For example, by using the logarithmic method to determine the asset value in the matrix in advance, and setting $\alpha = \beta = \gamma = 1/3$; then, it may obtain the asset value judgment matrix, as shown in Table A.1.

Appendix B

(Normative)

Calculation method of risk value

This appendix describes several methods for calculating the risk value of an asset. The assessor can EITHER choose the appropriate risk value calculation method according to the specific situation, OR adopt other calculation methods. When an asset is composed of several sub-assets, the risk value of each sub-asset can be calculated separately first, then, the total risk value can be calculated by a certain calculation method (such as the addition method).

B.1 Multiplication method

Considering that the factors such as asset value, threat value, and vulnerability value -- which affect the asset risk value of the system of telecom network and internet -- these factors are positively correlated with the risk value. Therefore, these factors can be multiplied, so as to obtain the risk value of a certain vulnerability corresponding to the asset value. The calculation formula is as follows:

Risk value = Asset value × Threat value × Vulnerability value

According to the value range of each factor, which affects the risk value, it can be known that the value range of adopting multiplication method to calculate risk value is 1 ~ 125. In order to realize the control and management of risks, this standard conducts hierarchical processing on the risk value, which divides the risk level into 5 levels, as shown in Table 12. Each level represents the severity level of the corresponding risk. The higher the level, the higher the risk. higher. Table B.1 provides a risk level classification method. The risk level corresponding to the risk value can be determined according to Table B.1.

Table 8.1 -- Determination of risk level

Risk value	1~10	11~30	31~60	61~90	91~125
Risk level	1	2	3	4	5

B.2 Matrix method

The characteristic of the matrix method is to establish the corresponding matrix of asset value level, threat level, and vulnerability level, which determines the risk level in advance according to a certain method. When using this method for the risk of each asset, it is necessary to firstly determine the assignment for the asset value level, threat level, and vulnerability level; then, check the matrix to obtain the risk level.

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

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