Translated English of Chinese Standard: GB/T39335-2020

www.ChineseStandard.net → Buy True-PDF → Auto-conveyor.

Sales@ChineseStandard.net

GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

GB/T 39335-2020

Information security technology - Guidance for personal information security impact assessment

信息安全技术 个人信息安全影响评估指南

Issued on: November 19, 2020 **Implemented on: June 01, 2021**

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

Table of Contents

Information security technology - Guidance for personal information security impact assessment

1 Scope

This standard provides the basic principles and implementation process, of personal information security impact assessment.

This standard applies to various organizations, to carry out personal information security impact assessment on their own. At the same time, it can provide reference for the supervision, inspection, assessment of personal information security, by the competent regulatory authorities, third-party assessment agencies and other organizations.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) is applicable to this standard.

GB/T 20984 Information security technology - Risk assessment specification for information security

GB/T 25069-2010 Information security technology - Glossary

GB/T 35273-2020 Information security technology - Personal information security specification

3 Terms and definitions

The terms and definitions as defined in GB/T 25069-2010 and GB/T 35273-2020, as well as the following terms and definitions, apply to this document.

3.1

Personal information

Various information, which is recorded electronically or in other ways, which can identify a specific natural person alone OR in combination with other information OR reflect the activities of a specific natural person.

scenarios, the responsible and participating departments and personnel, the identified risks, the list of adopted and proposed security control measures, residual risks, etc.

Therefore, the purpose of the personal information security impact assessment report includes but is not limited to:

a) For the subject of personal information, the assessment report can ensure that, the subject of personal information understands how their personal information is processed AND how to protect it; the subject of personal information is enabled to judge whether there are residual risks, which have not been dealt with.

b) For organizations, which conduct impact assessments, the purpose of the assessment report may include:

1) In the planning stage of a product, service or project, it is used to ensure that, the protection requirements of personal information are fully considered and realized, in the design of the product or service (for example, the achievability, feasibility, traceability, etc.) of the security mechanism;

2) During the operation of products, services or projects, it is used to determine whether the internal and external factors of the operation (such as changes in the operation team, Internet security environment, third-party security control capabilities for information sharing, etc.), laws and regulations have undergone substantial changes; whether it is necessary to review and correct the results of the impact assessment;

3) It is used to establish a responsibility system, to supervise whether security protection measures have been taken, for personal information processing activities, which have security risks, to improve or eliminate the identified risks;

4) It is used to enhance the personal information security awareness of internal employees.

c) For the competent regulatory department, the organization is required to provide a personal information security impact assessment report; the organization may be urged to carry out the assessment AND take effective security control measures. When handling personal information security related complaints, investigating personal information security incidents, etc., the competent supervisory authority can understand the relevant situation, through the impact assessment report, OR use the report as relevant evidence.

d) For the partners of the organization that conducts the impact assessment,

it is used to understand their role and function in the business scenario as a whole, as well as their specific personal information protection work and responsibilities.

4.4 Subjects responsible for assessment

The organization designates the responsible department or person responsible for personal information security impact assessment, who is responsible for the formulation, implementation, improvement of the personal information security impact assessment work process, AND is responsible for the quality of the personal information security impact assessment work results. The responsible department or person is independent AND is not affected by the assessed party. Usually, the department, which takes the lead in the implementation of personal information security impact assessment, is the legal department, the compliance department, or the information security department.

Responsible departments, within the organization, can choose to carry out personal information security impact assessments on their own, OR hire external independent third parties, to undertake specific personal information security impact assessments, based on the specific capabilities of the department.

For specific products, services or projects, the person in charge of the corresponding product, service or project shall ensure the development and smooth progress of personal information security impact assessment activities, AND provide corresponding support.

When the organization conducts the personal information security impact assessment on its own, the competent supervisory authority and the client can request an independent audit, to verify the rationality and completeness of the impact assessment activity. At the same time, the organization allows the competent regulatory authorities to obtain evidence on the impact assessment process AND related information systems or procedures.

4.5 Basic principles of assessment

The basic principle of personal information security impact assessment is as shown in Figure 1.

a) Interview: Refers to the process, in which assessors talk to relevant personnel, to understand, analyze, obtain evidence about the processing of personal information in the information system, the design and implementation of protection measures. The interviewees include product managers, R&D engineers, person in charge of personal information protection, legal responsible personnel, system architects, security administrators, operation and maintenance personnel, human resources personnel, system users.

b) Inspection: Refers to the process, by which the assessor observes, inspects, analyzes the management system, security policies and mechanisms, contract agreements, security configuration and design documents, operation records, etc., in order to understand, analyze or obtain evidence. The objects of inspection are specifications AND mechanisms and activities, such as personal information protection strategy planning and procedures, system design documents and interface specifications, drill results of emergency planning, incident response activities, technical manuals and user/administrator guidelines, operation of the information technology mechanism in the information system hardware/software, etc.

c) Testing: Refers to the process, in which assessors conduct technical testing, through manual or automated security testing tools, to obtain relevant information, AND perform analysis to obtain evidence. The object of the testing is the security control mechanism, such as access control, identification and verification, security audit mechanism, transmission link and storage encryption mechanism, continuous monitoring of important events, testing of incident response capabilities, drill capabilities of emergency planning.

4.6.3 Work form of assessment

From the perspective of implementation subjects, personal information security impact assessment is divided into two forms: self-assessment and inspection assessment.

Self-assessment refers to the organization's self-initiated assessment of its personal information processing behavior. Self-assessment can be carried out by the post or role, which is designated by the organization, to be responsible for assessment and auditing; OR it can entrust an external professional organization to carry out the assessment work.

Inspection assessment refers to the personal information security impact assessment, which is initiated by the upper-level organization of the organization. The upper-level organization is an organization, which has a direct leadership relationship with the organization OR is responsible for

supervision and management. Inspection assessment can also be entrusted to an external professional organization to carry out.

After determining the assessment scale, selecting the assessment method and the assessment work form, the specific process of the assessment implementation can refer to Chapter 5.

5 Implementation process of assessment

5.1 Analysis of assessment necessity

5.1.1 Overview

Personal information security impact assessment can be used for compliance gap analysis; it can also be used for compliance AND to further enhance its own security risk management capabilities and security level. Therefore, the necessity of starting the personal information security impact assessment, depends on the organization's personal information security goals. The organization can select the business scenarios, which need to start the assessment, according to actual needs.

5.1.2 Assessment of compliance gap

5.1.2.1 Overview

When the personal information security goal, which is defined by the organization, is to comply with the baseline requirements of relevant laws, regulations or standards, THEN, the main purpose of personal information security impact assessment is to identify the security control measures, that have been taken for the specific personal information processing activities to be assessed, as well as the gap between the specific requirements of the relevant laws, regulations, standards, such as sharing personal information with a third party in a certain business scenario, whether it obtains the express consent of the subject of personal information.

5.1.2.2 Overall compliance analysis

The organization can analyze the gap, BETWEEN all the personal information processing activities involved in a specific product or service AND the applicable rules, in accordance with applicable laws, regulations, policies and standards, which are related to the protection of personal information. The application scenarios of this assessment method include but are not limited to the following situations:

a) Annual overall assessment of the product or service;

If necessary, the assessor needs to apply for team support, such as a team composed of representatives from the technical department, related business departments, the legal department. The organization's internal personal information security impact assessment requires long-term support, from the organization's management.

The management needs to allocate necessary resources for the personal information security impact assessment team.

5.2.2 Develop an assessment plan

The plan needs to clearly stipulate the work to be done to complete the personal information security impact assessment report, the division of assessment tasks, the assessment schedule. In addition, the plan needs to consider the suspension or cancellation of the scenario to be evaluated. Consider the following aspects, during specific operations:

a) Personnel, skills, experience, abilities;

b) The time required to perform various tasks;

c) The resources required for each step of the assessment, such as automated assessment tools.

Note: When the involved scenes are complex and consume a lot of resources, it is recommended to update and iterate the original plan. For routine assessment activities or situations involving low complexity of the scene to be evaluated, the original plan can be used OR this step can be simplified.

If consultations with related parties are involved, the plan needs to specify the circumstances, under which related parties need to be consulted, who will be consulted, as well as the specific consultation methods (for example, through public opinion surveys, seminars, focus groups, public hearings, online experiences, etc.).

5.2.3 Determine the assessment object and scope

Describe the object and scope of the assessment, from the following three aspects:

a) Describe the basic information of the system, including but not limited to:

1) Purpose and type of personal information in processing;

2) A description of the information system, which supports current or future business processes;

3) Departments or related personnel, who perform information system

management responsibilities, as well as their duties or performance levels;

4) A description of the processing methods and scope of personal information, as well as the roles that have the right to access personal information, etc.;

5) If it is expected to entrust a third party to process, OR share or transfer personal information of the information system with a third party, description of the identity of the above-mentioned third party and the status of the third party's access to the information system, etc.

b) Describe system design information, including but not limited to:

1) Overview of functional (or logical) structure;

2) Overview of the physical structure;

3) List and structure of information system databases, tables and fields, which contain personal information;

4) Schematic diagram of data flow, which is divided by components and interfaces;

5) A schematic diagram of the data flow of the personal information's life cycle, such as the collection, storage, use, sharing of personal information;

6) Description of the time node for notifying the personal information subject AND the time node and work flow chart for obtaining the consent of the personal information subject;

7) A list of interfaces, which can transmit personal information to the outside;

8) Security measures, during the processing of personal information.

c) Describe the processing flow and procedure information, including but not limited to:

1) The identity and user management concept of the information system;

2) Operational concept, including information system or part of its structure using on-site operation, external hosting, or cloud outsourcing;

3) Support concepts, including listing the scope of third parties that can access personal information, their personal information access permissions, the locations where they can access personal information,

corporate acquisitions, mergers and acquisitions, global expansion, etc.

When sorting out the results of data mapping analysis, classify personal information processing activities, based on the type, sensitivity, collection scenario, processing method, related parties, which are involved in the personal information; describe the specific circumstances of each type of personal information processing activity, to facilitate impact analysis and risk assessment of follow-up classification.

Note: For data mapping analysis, refer to Table C.1 and Table C.2 in Appendix C.

5.4 Identification of risk sources

Risk source identification is to analyze which threat sources are faced by personal information processing activities, whether the lack of adequate security measures leads to the existence of vulnerabilities AND triggers security incidents. There are many factors, which determine the occurrence of personal information security incidents. In terms of threat sources, there are internal threat sources and external threat sources, incidents such as data theft as caused by malicious personnel, data leakage as accidentally caused by non-malicious personnel. In terms of vulnerability, there are data damage as caused by physical environment, data leakage, tampering, loss as caused by technical factors, as well as abuse as caused by improper management.

The threat identification and vulnerability identification methods, which are described in GB/T 20984, can be used in the analysis process of personal information security incidents. In order to further simplify the analysis process of the possibility of personal information security incidents, the elements related to the possibility of personal information security incidents are summarized into the following four aspects:

a) Network environment and technical measures. The factors to focus on, during the assessment, include but are not limited to:

   1) Whether the network environment, where the information system processing personal information is located, is an internal network or the Internet; different network environments face different threat sources; information systems, which are connected to the Internet, face higher risks;

   2) The interaction method between the information system, which processes personal information, and other systems, such as whether to use network interfaces for data interaction, whether to embed third-party codes, plug-ins, etc. that can collect personal information. Generally, the more data interactions, the more comprehensive security

measures to prevent risks, such as information leakage and theft;

3) Whether strict identity authentication, access control and other measures are implemented, in the process of personal information processing;

4) Whether boundary protection equipment is deployed, at the network boundary; whether strict boundary protection strategy is configured; whether data leakage prevention technical measures are implemented;

5) Whether to monitor and record the network operation status; whether to mark and analyze the status of personal information internally or when interacting with third parties; whether to discover abnormal traffic and illegal use in a timely manner;

6) Whether technical measures have been taken, to prevent network intrusions, such as virus and Trojan horse backdoor attacks, port scanning, denial of service attacks, etc.;

7) Whether to use encrypted transmission, encrypted storage and other measures, to provide additional protection for personal sensitive information;

8) Whether to audit the personal information processing activities, at each stage of personal information collection, storage, transmission, use, sharing, etc.; whether to alarm abnormal operation behaviors;

9) Whether a complete network security incident early warning, emergency response, reporting mechanism has been established;

10) Whether to conduct regular security inspections, assessments, penetration tests, on the information system; whether to perform patch updates and security reinforcements, in a timely manner;

11) Whether to strengthen the security management of data storage media; whether it has the ability to backup and restore data;

12) Other necessary network security technical safeguard measures.

Note 1: If the organization refers to other network security, data security related national standards, to establish a mature security protection system, it may carry out analysis and assessment, based on its existing foundation.

b) Personal information processing flow. The factors to focus on, during the assessment, include but are not limited to:

1) Whether the judgment of personal sensitive information is accurate;

7) Whether it is clear that external service personnel, who may access personal information, need to comply with personal information security requirements; whether to supervise them;

8) Whether to sign a binding contract and other documents with a third party, which stipulates the purpose, method, data retention period, disposal method if beyond the time limit, after the transfer of personal information to the third party;

9) Whether to conduct regular inspections and audits of third parties' handling of personal information, to ensure that they strictly implement contracts and other agreements;

10) Other necessary measures.

Note 3: If the organization establishes a mature security management system, with reference to other national standards, which are related to network security and data security, it can be analyzed and evaluated, based on its existing foundation.

d) Business characteristics and scale and security situation. The factors to focus on, during the assessment, include but are not limited to:

1) The business's dependence on the processing of personal information;

2) The amount, frequency, user scale, user peak value, etc. of business processing or possible processing of personal information;

3) Whether there have been incidents of personal information leakage, tampering, damage, loss, etc.;

4) Law enforcement and supervision trends, which are related to personal information protection;

5) Situations of network attacks or security incidents, in the near future;

6) Security-related warnings, which have been recently received or publicly released.

After the organization fully understands the corresponding content of the above dimensions, it can identify the measures taken and the current status, through investigations and interviews, consulting supporting documents, functional inspections, technical tests. According to the different dimensions of the analysis of the impact of personal rights and interests in 5.5, it shall carry out a comprehensive assessment of the likelihood of the occurrence of a security incident, from the above four aspects.

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

Full-copy PDF can be purchased from 1 of 2 websites:

1. https://www.ChineseStandard.us

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. https://www.ChineseStandard.net

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - https://www.ChineseStandard.us).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

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