Non-Functional Requirements Grades Usage Guide [Description Manual]

April 2010

Information-Technology Promotion Agency, Japan
Software Engineering Center

[Usage conditions]

About the Non-functional Requirements Grades Usage Guide [Description Manual]

The Non-functional Requirements Grades Usage Guide is composed of the "Usage Manual" and the "Description Manual" as the shown in diagram below.

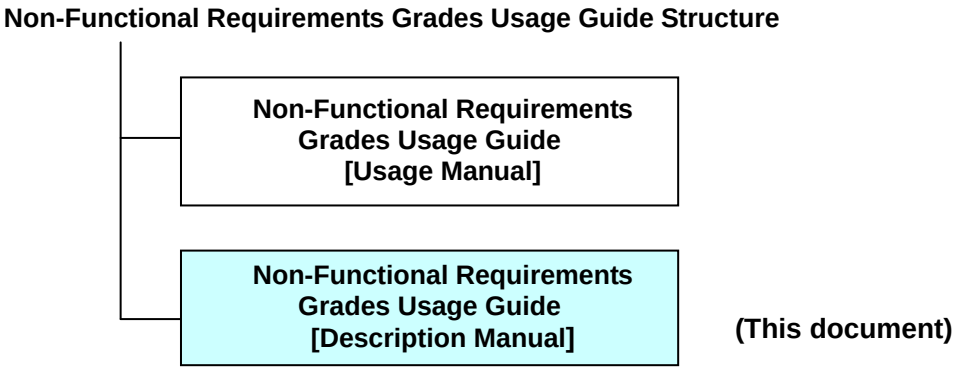


Figure: Non-functional Requirements Grades Usage Guide [Usage Manual] positioning

The objectives of this manual are to provide the background behind the creation of the non-functional requirements grades for visualization of system infrastructure outsourcer requirements, and to provide detailed information regarding non-functional requirements grades tools.

Please refer to the "Usage Manual" for an explanation of how to use the non-functional requirements grades.

The expression "non-functional requirements grades" refers to the Non-functional Requirements Grades Usage Guides and the following 3 tools:

- "System Infrastructure Non-functional Requirements Related Grade Table" (hereafter referred to as the grade table)
- "System Infrastructure Non-functional Requirements Related Item List" (hereafter referred to as the item list)
- "System Infrastructure Non-functional Requirements Related Tree Diagrams" (hereafter referred to as the tree diagrams)

Intended audience of this document

This document is targeted primarily at persons responsible for placing or receiving orders, and who are involved in the provision, proposal, or determination of non-functional requirements during the requirement definition phase or similar phases of the development of information systems such as corporate business systems. This document refers to those placing orders as "users," and those receiving orders as "vendors."

How this document is organized

This document is organized as shown in the table below.

Table: How this Non-functional Requirements Grades Usage Guide [Description Manual] is organized

Chapter number	Chapter title	Overview
Chapter 1	Introduction	Provides an explanation of the background behind the creation of the non-functional requirements grades, their scope, etc.
Chapter 2	Detailed explanation of non-functional requirements grades	Provides an explanation of the non-functional requirements grades specifications and major categories.
Chapter 3	FAQ	Contains frequently asked questions regarding the non-functional requirements grades, and their answers.
Chapter 4	Terminology	Provides an explanation of the non-functional requirements grades terminology.
Chapter 5	Appendix	Provides supplemental information, such as correspondence with other standards.

Table of contents

1. Introduction

1.1 Background and objectives behind the creation of non-functional requirements grades

Information systems have become essential components of social and corporate activities. Figure 1.1.1 shows the historical changes information systems have undergone. Modern businesses cannot exist without information technology (IT), and information system users are not confined to within individual companies, but span across external companies and general consumers. As information systems have become part of society's infrastructure, it has become more important than ever that they provide stable, reliable service. The components which make up information systems, that is, the technologies and products that are applied, are growing in scope and complexity, becoming more open and networked. As such, establishing information systems does not merely consist of applying IT to business, but it is critical that complex system elements be appropriately coordinated in order to provide a stable level of service.

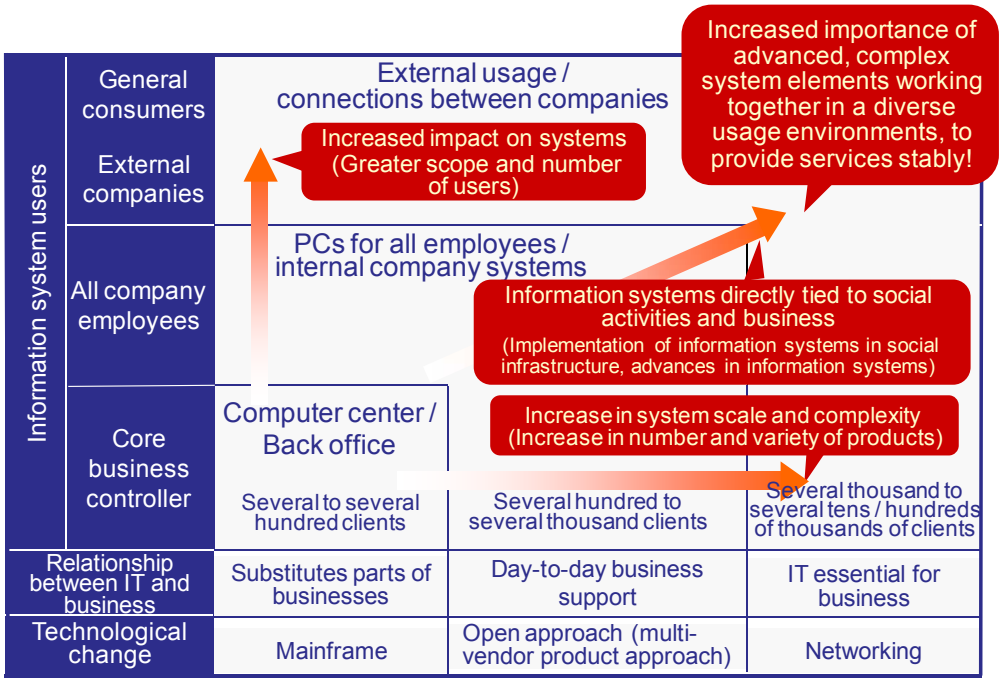


Figure 1.1.1 Information system historical changes

Information systems are composed of business applications which provide their business functions, and the system infrastructures, etc., which support them (Figure 1.1.2). System infrastructures are the structures that provide common services to business applications, and are composed of hardware devices, networking equipment, operating systems and middleware, applications for controlling and operating them, and the like. System infrastructures are critical to stably providing services.

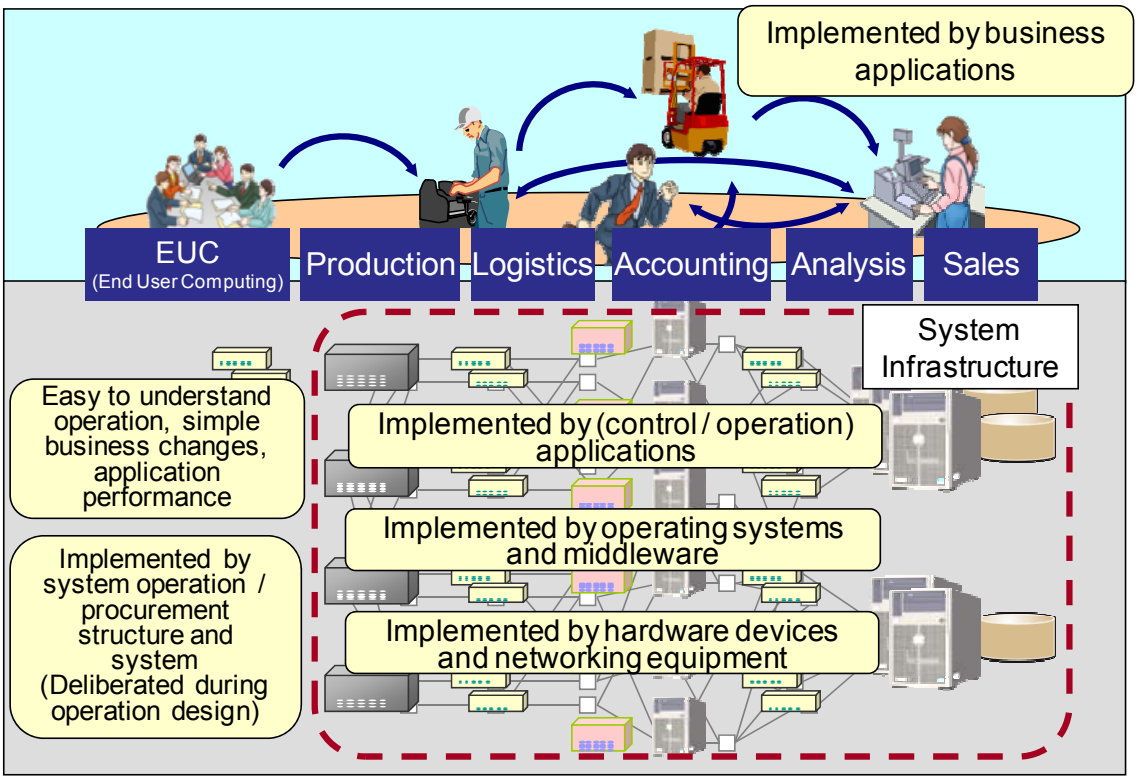


Figure 1.1.2 System infrastructure positioning

Information system requirements can be broadly divided into two categories. (Figure 1.1.3)

The first is business related requirements. These relate to business functions themselves, and as such are called "functional requirements." Examples of these would be requirements such as "We want to share and keep abreast of sales information using the system," or "We want to perform inventory management that is linked to order placement and receipt information." The other category is that of requirements other than "functional requirements," called "non-functional requirements." An example of this would be "We want the system to recover within 3 hours or less in the event of a system failure." System infrastructure related requirements consist primarily of these "non-functional requirements."

The objectives of the non-functional requirements grades are to clarify system infrastructure related non-functional requirements, establish a common understanding of them between users and vendors, construct appropriate information systems, and enable stable provision of services.

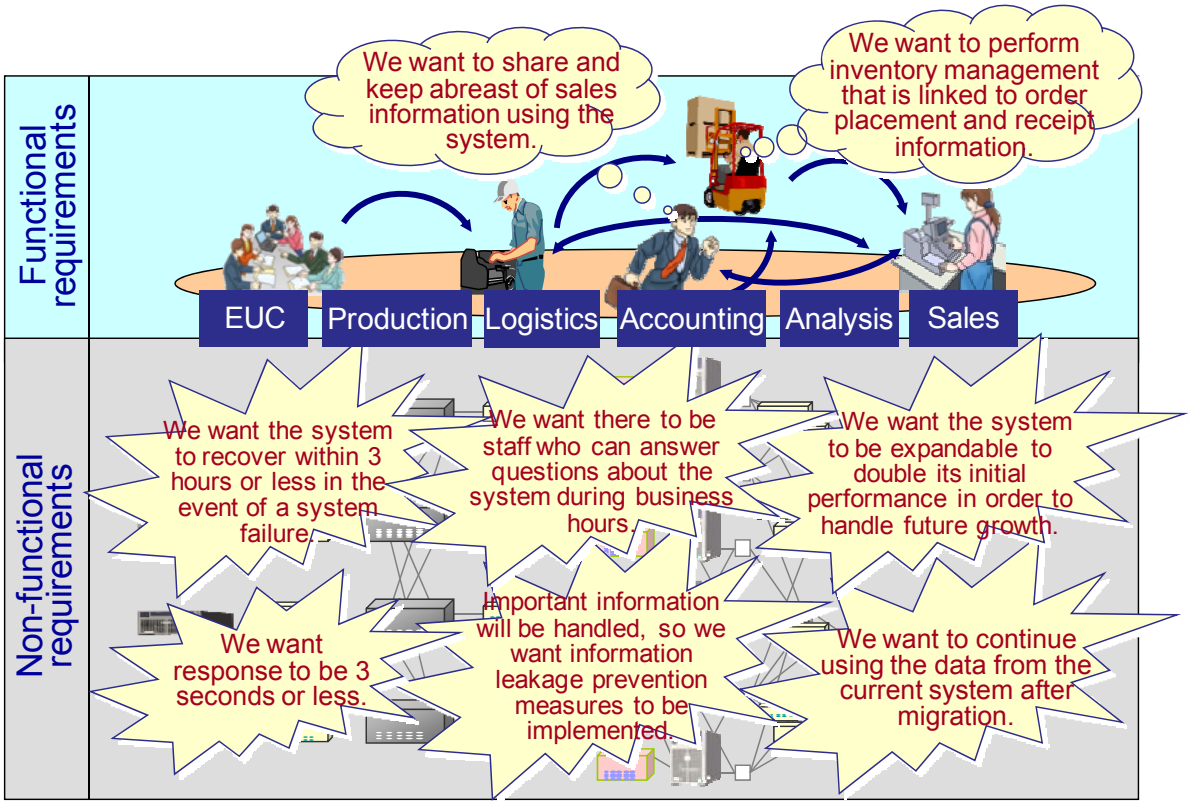


Figure 1.1.3 Overview of functional requirements and non-functional requirements

1.2 Issues regarding non-functional requirements and the non-functional requirements grades resolution approach

As was discussed above, it is important for users and vendors to share an understanding of non-functional requirements when developing an information system. However, in actual information system development scenarios, non-functional requirements that need to be agreed between the users and vendors are often insufficient, having missing areas or being perceived differently. The resulting gaps present obstacles to the development of appropriate information systems.

Figure 1.2.1 shows a visual example of this issue.

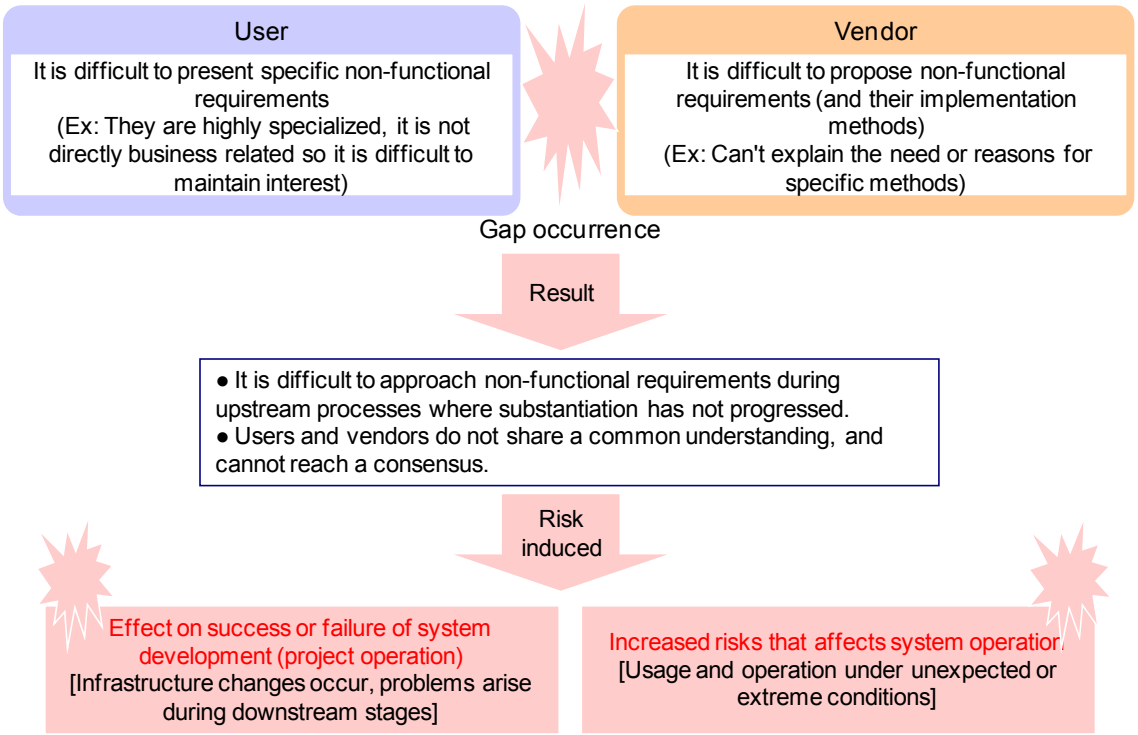


Figure 1.2.1 Issues regarding non-functional requirements

One reason for these gaps is that consideration of non-functional requirements requires some degree of expert knowledge, and it is difficult for users to provide specific non-functional requirements from the initial stages of system development. The relationship between non-functional requirements and business is often difficult to see, or to hold significant interest in. From the vendors' perspective, it is difficult to explain the necessity and validity of non-functional requirements and their implementation methods, making proposals difficult.

The gaps result in information system development going ahead despite non-functional requirements not being clearly defined, causing problems in downstream process development and operation.

Below is an explanation of how the non-functional requirements grades solve these problems.

- They offer tools which can be used by both users and vendors, and which are made open to the public to eliminate missing areas or misunderstandings of non-functional requirements between the two parties that must agree upon them.
- The tools are structured in accordance with the stepwise refinement procedures, and include a usage guide, making it possible for users to rapidly present non-functional requirements.
- By enumerating non-functional requirements implementation levels, it enables vendors to provide concrete implementation methods of non-functional requirements.

1.3 Scope of the non-functional requirements grades

1.3.1 Relationship between non-functional requirements definitions and system infrastructures

In a broad sense, the expression "non-functional requirements" is used literally to refer to all of the requirements of an information system other than the desired functional requirements. As such, as they may include project management related requirements, such as budgetary elements, as well as laws and business rules that affect the business which will be handled by the system, there are many definitions for "non-functional requirements."

The scope of the non-functional requirements grades encompasses those non-functional requirements which are implemented as part of the system infrastructure. The reason for this focus on system infrastructure is that it is important to promote recognition and consensus concerning system infrastructure requirements, which are often overlooked during the requirements definition process due to the emphasis on business application implementation requirements.

The non-functional requirements grades, however, also include requirements considered particularly important when defining system infrastructure requirements that may not necessarily be implemented by the system infrastructure itself. Below are some examples.

- Operation related requirements
  Operating hours and the like are related to information systems as a whole, but are also important for defining performance and availability requirements.
- Security requirements
  These also affect security policies and the like that are areas other than the system infrastructure, but they may also have an impact on system infrastructure non-functional requirements.
- Testing related requirements
  These include the necessity of a testing environment, the scope of the tests and other matters that may have an effect on the scale and structure of the system infrastructure.

Non-functional requirements grades include the requirement items which vendors and users must agree on during the upstream process before information system design is begun.

Unless otherwise stated within this document, the term "non-functional requirements" is used to refer to "requirements primarily implemented within the system infrastructure."

1.3.2 Items within the scope

The non-functional requirements grades cover non-functional requirements which relate to the system infrastructure. Specifically, it divides requirements into six categories: "availability," "performance and scalability," "operability and maintainability," "migratability," "security," and "system environment and ecology."[1]

Table 1.3.2.1 shows the requirements for these major categories, and examples of implementation methods based on them.

[1] Refer to Chapter 3 FAQ Q1 for details regarding how the 6 major categories were organized.

Table 1.3.2.1 The 6 major categories of non-functional requirements grades

Non-functional requirements Major category	Description	Example requirements	Example implementation methods
Availability	Requirements related to maintaining continuous system service availability	• Operation schedule (operating hours, outage plans, etc.) • Operation objectives for failure occurrences, disasters, etc.	• Equipment redundancy, backup center establishment, etc. • Restoration/recovery methods, and restoration/recovery structure establishment
Performance and scalability	System performance and future system expansion related requirements	• Business volume, and estimates on future growth • Attributes of business which will be systematized (peak times, normal operation, degraded operation, etc.)	• Sizing based on performance objectives • Capacity planning (future-oriented equipment and network sizing and allocation)
Operability and maintainability	System operation and maintenance service related requirements	• System operation levels required for system operation • Response levels in the event that a problem occurs	• Establishment of monitoring methods and backup methods • Distribution of roles, organizational structure, training, and preparation of manuals in anticipation of problems that may arise
Migratability	Requirements related to migration of current system assets	• System migration period and schemes • Types of assets to be migrated, and volume of migration	• Migration schedule establishment, migration tool development • Migration organization establishment, migration rehearsal
Security	Requirements related to securing information system safety	• Usage restrictions • Unauthorized access prevention	• Access restrictions, data confidentiality • Fraud tracking, monitoring, detection • Information security training for operators, etc.
System environment and ecology	System installation environment and ecological requirements	• Items related to the system environment, such as earthquake resistance / seismic isolation, weight / space occupation, temperature / humidity, noise, etc. • Items related to ecology, such as amount of CO_2 emissions and energy consumption	• Selection of equipment in accordance with regulations and electrical facilities • System configuration which minimizes the system's environmental load

1.3.3 Items outside the scope

Table 1.3.3.1 shows items which fall out of the scope of the non-functional requirements grades.

Table 1.3.3.1 Items outside the scope, and the reasons they fall outside the scope

No.	Items outside the scope	Reason	Examples
1	Items primarily used to define business applications	These items are easier for users and vendors to recognize than non-functional requirements implemented by the system infrastructure, and there are relatively well-developed tools for clarifying these requirements.	Usability, functionality, portability, etc.
2	Items related to selecting products and solutions for individual users' companies	The selection of individual products and solutions depends on the specific users of the information system, and are not determined by non-functional requirements grades.	Individual specific system configurations, components, products, etc.

1.4 Non-functional requirements grades overview

This section explains the basic concepts behind the non-functional requirements grades, the objectives of the 3 tools that make up the non-functional requirements grades, important points on using them, and how they relate to each other.

1.4.1 Basic concepts behind the non-functional requirements grades

(1) Shared understanding of requirement items by using levels

First, this guide will provide an explanation of the basic non-functional requirements grades approach.

The purpose of the non-functional requirements grades is for users and vendors to reach a consensus on non-functional requirements of system infrastructures, and to eliminate misunderstandings.

1. Non-functional requirement items shall be expressed using quantitative indices.
2. Levels for each item shall be defined in accordance with the differences in costs, architecture, etc.

The non-functional requirements have been organized in accordance with the above policies.

"Reaching a consensus between users and vendors concerning non-functional requirements" refers to both parties determining and agreeing on a defined level for the above requirement items. If requirement items are not defined quantitatively, but instead using vague expressions (for example, "provide a level of performance satisfactory to the user"), even if both parties are able to recognize such requirement items, they may have differing interpretations of it, and thus experience difficulty in reaching consensus regarding how to implement the requirement items, or whether they can be achieved. The non-functional requirements grades establish requirement items in the form of indices, and predefine levels as index values in order to clarify to users and vendors, the difficulty and costs involved in implementing a requirement, as shown in Figure 1.4.1.1.

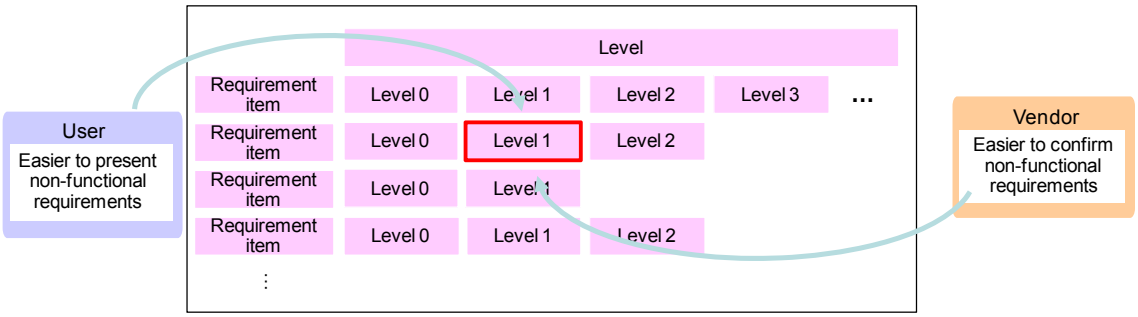


Figure 1.4.1.1 Level establishment for requirement items

These levels, however, serve merely as starting points for consensus formation, and have some degree of breadth. In the end, users and vendors must agree on specific figures.

(2) Selection of requirement items using the grade

The non-functional requirements grades use the concept of "grades."

Individual systems have different purposes, scales, and effects on society. Because systems have such diversity in their characteristics and properties, it is not possible to establish universal non-functional requirements for all systems. Because of this, there are differences in the level of implementation depending on individual combinations and interrelationships between hardware, facilities, operating systems, middleware, operation management approaches, operation management structures, and the like. It is difficult for users to recognize these differences from the initial stages of system development, and difficult for vendors to provide technical explanations. However, if there were a representative reference model that could be used when considering and deciding on system non-functional requirements, deliberation of non-functional requirements could be carried out more smoothly.

The non-functional requirements grades provide a framework for users and vendors to confirm non-functional requirement items from an early stage by expressing the differences between systems as stepwise "grades," and setting requirement item levels for each grade.

(3) Stepwise requirement item refinement

The usage objectives of the tools that make up the non-functional requirements grades are not limited, but were made with the assumption that they would be used for stepwise refinement and consensus formation of non-functional requirements between users and vendors. General descriptions of each tool, their objectives, and the relationships between the tools are explained below. Please refer to Chapter 2 for more information on the tools, and the "Usage Manual" for descriptions on how to use the tools.

1.4.2 General description and the components of the non-functional requirements grades

Figure 1.4.2.1 shows general description of the tools which make up the non-functional requirements grades, and an overall image of the non-functional requirements grades themselves.

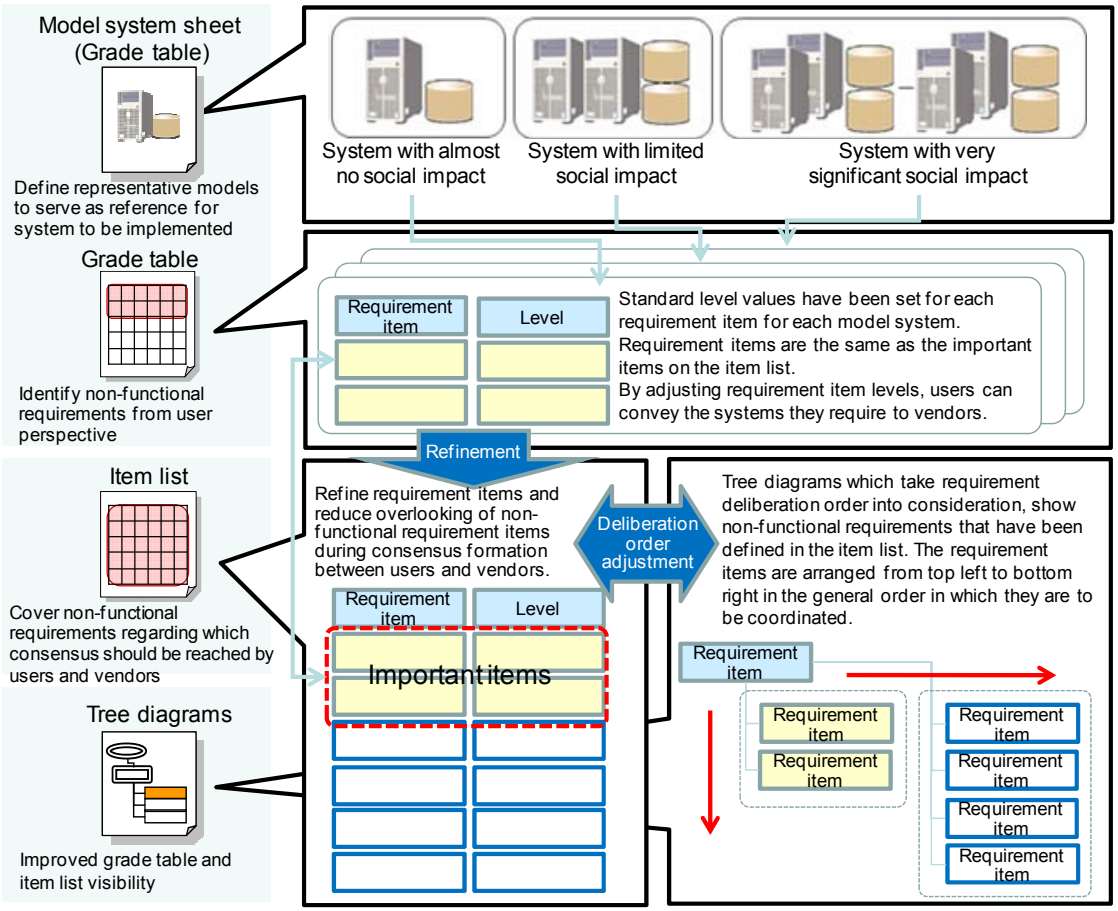


Figure 1.4.2.1 General description of the non-functional requirements grades and overall image

(1) Grade table

The grade table defines the non-functional requirement items and level values for each of the three "grades." Requirement items included in the grade table take user perspectives into account, consisting of items selected based on the fact that they significantly impact system quality and cost. As such, the grade table consists of a table containing the important items derived from the item list, and to the right of the table, the three "grades" and the corresponding set of level values.

The 16 properties in the grade table's model system sheet are used to define the characteristics of the following three model systems:

- System with almost no social impact
- System with limited social impact
- System with very significant social impact

The model system sheet defines, as criteria for users to select model systems, non-functional requirements which represent the properties of each model system. For detailed explanations of each model system, and their corresponding non-functional requirements that have been set, please refer

to the non-functional requirements grades detailed in Chapter 2.

Each model system lists its selected levels and selection conditions. The initial value for each requirement item's level is set as the base value for each selected level. This can be used together with the grade table in order to use the model system's base values as reference when deciding non-functional requirements.

The objectives of model systems are to take a stepwise refinement approach to non-functional requirement items and reaching consensus regarding them, thus making it easy to use grade tables to decide non-functional requirements, as well as eliminating misunderstandings between users and vendors at an early stage by forming consensuses regarding important non-functional requirement items.

(2) Item list

The item list is a structured list of items intended to enable users and vendors to share an understanding of system infrastructure related non-functional requirements, without overlooking any of them. As defined in Table 1.3.2.1, requirement items are divided into 6 major categories. As Figure 1.4.2.2 shows, the item list offers a high level of completeness by systematically organizing and categorizing requirement items into individual major category units.

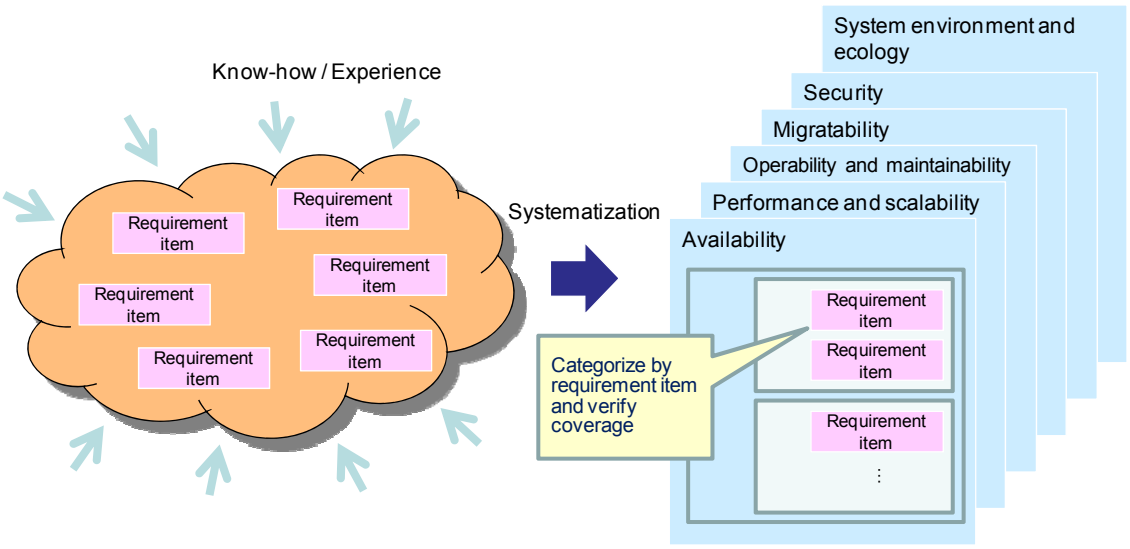


Figure 1.4.2.2 Structuring of requirement items

There are various processes by which users and vendors reach a consensus regarding non-functional requirements, but the objective of the item list is to manage, in an integrated fashion, the confirmation of non-functional requirements that eventually must reach a consensus.

The item list contains non-functional requirement items defined in the grade table, and is meant to be used during stepwise refinement to further break down the requirement items that have been decided with the grade table into more detailed items.

(3) Tree diagrams

Tree diagrams are diagrams which improve the viewability of the grade table and item list, visually depicting the requirement item deliberation order. The objective of the tree diagrams is to make the non-functional requirement item stepwise refinement task more efficient by serving as a reference when using the grade table and item list.

For example, when using the grade table to decide the levels of the important items, users and vendors can use the tree diagrams to gain a bird's-eye-view of the non-functional requirements in order to check which item to decide on next.

2. Detailed explanation of non-functional requirements grades

2.1 Detailed explanation of non-functional requirements grades

Below is a detailed explanation of non-functional requirements grade tools, with specific examples.

2.1.1 Grade table

(1) Model system definitions

The non-functional requirements grades divide systems into three categories[2] based on the guideline to the improvement of information system reliability (referred to hereafter as reliability guidelines) by the Ministry of Economy, Trade and Industry, and the reports by the Critical Infrastructure Information Systems Reliability Research Group of IPA, and specifically define the non-functional requirements of each system. These are hereafter referred to as model systems. Figure 2.1.1.1 shows the definitions of the model systems.

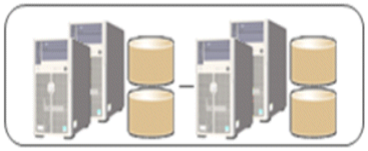
No.	Model system name and concept	General description of the model system
1	System with almost no social impact 	This type of system is used within a specific department of a company to a relatively limited extent. When its functions become degraded or unavailable, the specific department will be significantly affected while others will not. The system assumed here is a very small scale system that is open to the Internet.
2	System with limited social impact 	This type of system provides the infrastructure for corporate activities. When its functions become degraded or unavailable, such corporate activities as well as external users including suppliers and customers will be significantly affected. The system assumed here is a mission-critical system that is restricted to a corporate network.
3	System with very significant social impact 	This type of system provides the infrastructure for people's lives and social/economical activities. When its functions become degraded or unavailable, both of these will be significantly affected. The system assumed here is an infrastructure that is used by the general public.

Figure 2.1.1.1 Model system definitions

[2] There are four types of system categories in the system profiling done by the "Critical Infrastructure Information Systems Reliability Research Group." However, considering the degree of impact such as economic loss level and public influence, for model systems in the non-functional requirements grade, "a system that may have an impact on human lives which may cause extensive economic loss" is included in the "system with very significant social impact."

(2) Model system non-functional requirement items

Model system names alone are insufficient for a clear understanding of the non-functional requirement levels of each system, so the non-functional requirement items which define each model system's properties are identified and summarized in the model system sheet. Figure 2.1.1.2 shows the model system sheet.

No.	Major category	Property	System with almost no social impact	System with limited social impact	System with very significant social impact
Illustration of the model system					
General description of the model system			This type of system is used within a specific department of a company to a relatively limited extent. When its functions become degraded or unavailable, the specific department will be significantly affected while others will not. The system assumed here is a very small scale system that is open to the Internet.	This type of system provides the infrastructure for corporate activities. When its functions become degraded or unavailable, such corporate activities as well as external users including suppliers and customers will be significantly affected. The system assumed here is a mission-critical system that is restricted to a corporate network.	This type of system provides the infrastructure for people's lives and socialeconomical activities. When its functions become degraded or unavailable, both of these will be significantly affected. The system assumed here is an infrastructure that is used by the general public.
1	Availability	Uptime ratio	• Downtime of up to several days per year is accepted (99% uptime ratio).	• Downtime of up to approximately an hour per year is accepted (99.99% uptime ratio).	• Downtime of up to several minutes per year is accepted (99.999% uptime ratio).
2		Recovery objective	• Restoration of data from a weekly backup will be the recovery objective when restoring data upon system recovery.	• Restoration of data within one business day will be the recovery objective when restoring data upon system recovery.	• Restoration of data to the point of outage within several hours will be the recovery objective when restoring data upon system recovery.
3		Large-scale disaster	• The system is expected to be rebuilt in the event of a large-scale disaster.	• The target recovery time is within a week in the event of a large-scale disaster.	• Business continuity is required at a DR (Disaster Recovery) site in the event of a large-scale disaster. • A backup center is established in anticipation of a large-scale disaster.
4	Performance and scalability	Performance objective	• A general performance objective is set, but is less important than other requirements.	• A performance service level is specified.	• A performance service level is specified.
5		Scalability	• Scalability is not considered.	• An expansion plan for the system is established.	• An expansion plan for the system is established.
6	Operability and maintainability	Operating hours	• Service is provided during work hours only, and the system is not in operation during the nighttime.	• A system outage window is secured between the completion of the nighttime batch process and the beginning of business operation.	• The system operates 24/7 to provide non-interrupted service.
7		Backups	• The administrator of the department manually backs up only necessary data.	• A daily backup of the entire system is performed automatically.	• A backup site (DR site) with all data synchronized with the operation site is established.
8		Operation monitoring	• Alive monitoring is performed using various types of hardware and software logs.	• Each business function of the application is monitored to see whether they are operating normally.	• Performance and resource usage is monitored to detect indications of failure.
9		Manuals	• Manuals are created independently by the administrator of the department.	• A maintenance manual is prepared along with the operation manual since a service desk is established to carry out maintenance work.	• The operation manual is customized in accordance with the operation rules of the data center.
10		Maintenance	• Maintenance work is possible whenever necessary.	• Shutting down the system for maintenance work is possible as long as operation during work hours is not affected.	• All maintenance work is performed while the system is online.
11	Migratability	Migration scheme specification	• There are no rules for migration schemes (an agreement is reached based on the scheme proposed by the vendor).	• Applications are proactively integrated and modified to streamline business operation. • System cutover is performed all at once.	• The system is migrated in phases to reduce risks.
12		Migration schedule	• A sufficient number of days for migration is secured.	• System outages due to migration are possible.	• System outages due to migration shall be at minimum.
13		Equipment and data	• Equipment and data are newly developed.	• Equipment and data will have modifications.	• There is migration of equipment and data. However, in order to maintain data consistency and compatibility with other systems, changes to the database structure are limited.
14	Security	Disclosure scope of critical assets	• There are no critical assets that require security measures. (Critical assets refer to information assets that require high security, such as personal information, sensitive information, information with high negotiability, etc.)	• There are critical assets that require security measures, but connections are limited to specific parties.	• There are critical assets that require security measures, and service is provided to an unspecified number of persons.
15	System environment and ecology	Restrictions	• There are no legal or regulatory restrictions, etc.	• There are some legal and/or regulatory restrictions, etc.	• There are legal and/or regulatory restrictions, etc.
16		Earthquake resistance	• A minimum level of earthquake resistance is necessary.	• A regular level of earthquake resistance is necessary.	• A high level of earthquake resistance is necessary.

Figure 2.1.1.2 Model system sheet

Table 2.1.1.1 summarizes the properties of model systems in terms of major category.

Table 2.1.1.1 Model system properties

Major category	Characteristic non-functional requirements
Availability	Uptime ratio, recovery objective, large-scale disaster
Performance and scalability	Performance objective, scalability
Operability and maintainability	Operating hours, backups, operation monitoring, manuals, maintenance
Migratability	Migration scheme specification, migration schedule, equipment and data
Security	Disclosure scope of critical assets
System environment and ecology	Restrictions, earthquake resistance

The model system sheet, as shown in Figure 2.1.1.2, is included in the grade table, and is meant to be used in the first step of stepwise refinement. Please refer to the "Usage Manual", section 1.1 (1)

for more information regarding stepwise refinement.

(3) Grade table example

The grade table consists of a table containing the important items derived from the item list, and to the right of the table, has grades defined for the three model systems. Figures 2.1.1.3 and 2.1.1.4 show examples of the grade table.

This section will explain Figure 2.1.1.4, which shows the grade definition portion of the grade table.

The information to the left of the model system descriptions in the grade table is, with the exception of the presence / absence of the important item column, the same as the item list. Please refer to 2.1.2 for explanations of individual item list items.

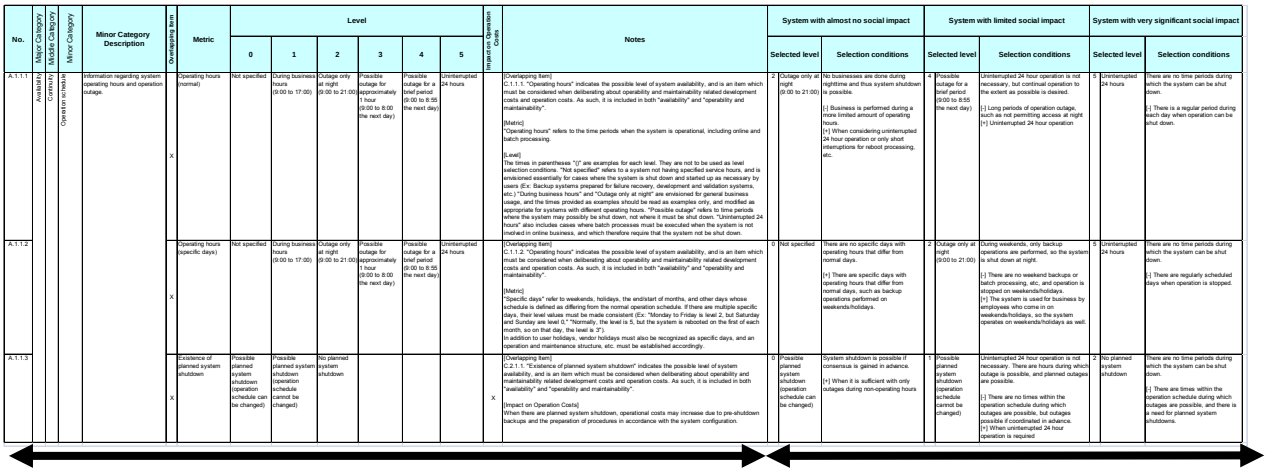


Figure 2.1.1.3 Grade table example (overall)

System with almost no social impact			System with limited social impact			System with very significant social impact		
Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
2	Outage only at night (9:00 to 21:00)	No businesses are done during nighttime and thus system shutdown is possible. [-] Business is performed during a more limited amount of operating hours. [+] When considering uninterrupted 24 hour operation or only short interruptions for reboot processing, etc.	4	Possible outage for a brief period (9:00 to 8:55 the next day)	Uninterrupted 24 hour operation is not necessary, but continual operation to the extent as possible is desired. [-] Long periods of operation outage, such as not permitting access at night [+] Uninterrupted 24 hour operation	5	Uninterrupted 24 hours	There are no time periods during which the system can be shut down. [-] There is a regular period during each day when operation can be shut down.
0	Not specified	There are no specific days with operating hours that differ from normal days. [+] There are specific days with operating hours that differ from normal days, such as backup operations performed on weekends/holidays.	2	Outage only at night (9:00 to 21:00)	During weekends, only backup operations are performed, so the system is shut down at night. [-] There are no weekend backups or batch processing, etc, and operation is stopped on weekends/holidays. [+] The system is used for business by employees who come in on weekends/holidays, so the system operates on weekends/holidays as well.	5	Uninterrupted 24 hours	There are no time periods during which the system can be shut down. [-] There are regularly scheduled days when operation is stopped.
0	Possible planned system shutdown (operation schedule can be changed)	System shutdown is possible if consensus is gained in advance. [+] When it is sufficient with only outages during non-operating hours	1	Possible planned system shutdown (operation schedule cannot be changed)	Uninterrupted 24 hour operation is not necessary. There are hours during which outage is possible, and planned outages are possible. [-] There are no times within the operation schedule during which outages are possible, but outages possible if coordinated in advance. [+] When uninterrupted 24 hour operation is required	2	No planned system shutdown	There are no time periods during which the system can be shut down. [-] There are times within the operation schedule during which outages are possible, and there is a need for planned system shutdowns.

Figure 2.1.1.4 Grade table example (grade definitions)

(4) Explanation of grade definition columns

An explanation of the individual columns is provided below.

(a) Selected level

The level selected from each set of defined non-functional requirement levels for the model system in question. This is made up of the level value, between 0 and 5, and the corresponding level description. The level value selected here is referred to as the base value.

Base values increase their level, in principle, from left to right. However, for some metrics, the levels are inverted, or are the same.

Metrics with inverted levels are arranged in that way because, when defining properties for each model system, properties were defined in conjunction with model system names. For example, "D.4.1.2 Migration data format" corresponds to facilities and data which are properties of migratability. Systems with very significant social impact are defined as prioritizing data continuity and minimizing data format changes. Systems with limited social impact are defined as having some data format changes. As such, the selected level for systems with limited social impact is the largest.

Metrics for which each level is identical have the same base values for any system, but this is because those requirements that will have large risks if not determined are defined as metrics. For example, "B.1.1.3 Data volume" should be determined by the time requirements are defined, so all are defined as level 0.

(b) Selection Conditions

Base value selection conditions. It is assumed that sometimes base values may not be sufficient enough to appropriately indicate the non-functional requirements of a system being developed, so conditions under which base values may change are indicated with [-] and [+].

When you wish to lower the non-functional requirement level of a system, check the conditions that correspond to the [-]. When you wish to raise the non-functional requirement level of a system, check the conditions that correspond to the [+].

(5) Important item selection process

The item list is a tool that lists non-functional requirement items and has 236 metrics. The order in which some of these metrics are decided varies, as does their impact on system infrastructure costs, making some sort of grouping necessary. The metrics have also been selected giving consideration to the fact that having too many items would result in consuming much time in deliberation. These selected metrics were defined as "important items." Metrics with large impacts on cost or quality were chosen as important items, evaluated from the perspectives of both users and vendors.[3]

(6) Grade table utilization image and benefits

When vendor estimates in response to user provided requirement levels do not match user budgets, it is assumed that selected levels will be changed and new estimates requested.

---

[3] Please refer to the non-functional requirements grades "User View Deliberation Committee" report for the evaluation background.

The non-functional requirements grades make it easy to visually confirm how non-functional requirements changes due to cost overruns will affect system infrastructure quality.

(7) Grade table tailoring

The grade table uses 3 model systems to define base values. However, users and vendors can add their own specific organization model systems to the grade table. For example, model systems such as "a model system for company XX's internal system," or "a model system for school library management" can be added. By defining a grade table using an actually operating system, many similar system non-functional requirements can be defined with a greater degree of accuracy.

2.1.2 Item list

(1) Item list example

The item list is a list of non-functional requirement items used for vendor and user confirmation in order to make system infrastructure related judgments necessary for system development and operation. It is composed of "No.", "Major category", "Middle category", "Minor category", "Minor category description", "Overlapping item", "Important item", "Metric", "Level", "Impact on operation costs", and "Notes". Figure 2.1.2.1 shows an item list example.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Important item	Metric	Level						Impact on operation costs	Notes
								0	1	2	3	4	5		
A.1.1.1	Availability	Continuity	Operation schedule	Information regarding system operating hours and operation outage.	x	x	Operating hours (normal)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (8:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] C.1.1.1. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Metric] "Operating hours" refers to the time periods when the system is operational, including online and batch processing. [Level] The times in parentheses "()" are examples for each level. They are not to be used as level selection conditions. "Not specified" refers to a system not having specified service hours, and is envisioned essentially for cases where the system is shut down and started up as necessary by users (Ex: Backup systems prepared for failure recovery, development and validation systems, etc.) "During business hours" and "Outage only at night" are envisioned for general business usage, and the times provided as examples should be read as examples only, and modified as appropriate for systems with different operating hours. "Possible outage" refers to time periods where the system may possibly be shut down, not where it must be shut down. "Uninterrupted 24 hours" also includes cases where batch processes must be executed when the system is not involved in online business, and which therefore require that the system not be shut down.
A.1.1.2					x	x	Operating hours (specific days)	Not specified	During business hours (9:00 to 17:00)	Outage only at night (9:00 to 21:00)	Possible outage for approximately 1 hour (9:00 to 8:00 the next day)	Possible outage for a brief period (8:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] C.1.1.2. "Operating hours" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Metric] "Specific days" refer to weekends, holidays, the end/start of months, and other days whose schedule is defined as differing from the normal operation schedule. If there are multiple specific days, their level values must be made consistent (Ex: "Monday to Friday is level 2, but Saturday and Sunday are level 0," "Normally, the level is 5, but the system is rebooted on the first of each month, so on that day, the level is 3"). In addition to user holidays, vendor holidays must also be recognized as specific days, and an operation and maintenance structure, etc. must be established accordingly.
A.1.1.3					x	x	Existence of planned system shutdown	Possible planned system shutdown (operation schedule can be changed)	Possible planned system shutdown (operation schedule cannot be changed)	No planned system shutdown				x	[Overlapping Item] C.2.1.1. "Existence of planned system shutdown" indicates the possible level of system availability, and is an item which must be considered when deliberating about operability and maintainability related development costs and operation costs. As such, it is included in both "availability" and "operability and maintainability". [Impact on Operation Costs] When there are planned system shutdown, operational costs may increase due to pre-shutdown backups and the preparation of procedures in accordance with the system configuration.

Figure 2.1.2.1 Item list example

(2) Explanation of item list columns

Below is an explanation of the columns, from left to right.

(a) No.

Sequential number indicating major category, middle category, minor category, and metric. Major categories are indicated with a letter (A to F), and each item, from middle category to metric, is a sequential number, separated by periods.

(b) Major category

Broadest category when non-functional requirements are systematically organized.

(c) Middle category

Category indicating which minor categories should be considered as a single unit.

(d) Minor category

Item indicating non-functional requirements which users and vendors reach a consensus.

(e) Minor category description

Explanation of the contents of the minor category, and how it should be approached.

(f) Overlapping item

Item which is repeated in multiple major categories. Since the items are selected from the perspective of the major categories assuming that the subject and order of deliberation is different for each major category, overlaps exist.

This is done to prevent an item from being overlooked due to it being aggregated into only one of the major categories. This column can be checked to see if an item is an overlapping item when considering the overall system, in order to prevent the same item from being reconsidered unnecessarily.

(g) Important item

Item with significant impact on quality and cost when considering non-functional requirements. Items designated as important items are used in structuring the grade table.

(h) Metric

Indices used to quantitatively represent the minor categories. Depending on the system structure, one metric may require multiple consensus levels.

For example, for "B.2.1.1 Adherence rate of response during normal operation," instead of determining the overall system adherence rate, frequently, adherence rates are determined for each service in accordance with the importance and frequency of usage of that service.

(i) Level

Value, from 0 to 6, corresponding to a metric and indicating the value that the item would normally take. Differences between levels indicate gaps in architecture, and the higher the level number, the harder the item is to implement, and generally the higher the development costs.

Development costs refer to those costs incurred from when requirements definition is completed until the system is finished and put in service. It includes all system infrastructure related costs, such as hardware, operating systems, middleware, system design, and installation work.

Level values are established separately for each metric. In other words, even if the same level is selected for each metric, it would have no special meaning. For example, it is not the case that level 3 refers to general systems, level 4 to core systems, and level 5 to advanced social infrastructure systems.

When there are 5 or fewer levels, the levels are listed starting from the left.

(j) Impact on operation costs

Metric indicating possibility of reducing operation costs by increasing development spending.

Operation costs refer to the costs incurred after system launch, for system maintenance and management. This includes operation personnel costs, hardware and middleware maintenance costs, supplies, and the like. Metrics with "X" in their "Impact on operation costs" column are items which may involve a tradeoff between development costs and

operation costs. For example, the "C.1.2.4 Backup automation scope" metric contains "X" in the "Impact on operation costs" column. Compared to level 0, "All steps performed manually," level 3, "All steps performed automatically" involves incorporating automation functions, resulting in higher development costs, but, as the item can then be handled by a small number of personnel during operation, it reduces operation costs.

When selecting levels, one must take note of the "Impact on operation costs" column, and, if it has an "X", give consideration to operation costs and system lifecycles after system construction.

(k) Notes

Supplementary explanation for each metric. Notes provide information which cannot be expressed sufficiently within the structure of the item list. The descriptions especially focus on the following:

- How to address items contained in multiple major categories (overlapping items)
- Specific explanation of the impact on operation costs

In order to clarify which column the notes refer to, the following convention is used.

- Column names are given in brackets, like [Metric] or [Level].
- Comments referring to specific levels are noted with the level number, as in [Level 0].

(3) Non-functional requirements grade levels

In principle, the levels contained in the grade table and item list are set in ascending order of development costs, starting from 0.

For some metrics, the level choice is a binary one, consisting of only either 0 or 1. In principle, in these binary metric cases, the level order is the same as for multiple levels, with the higher value indicating the greater degree of development costs. There are some binary metrics whose cost is not clearly conveyed because of their binary nature. When this is the case, evaluation and level selection is performed from the following three perspectives.

(a) "Simple binary values" for expressing the existence of legal restrictions, countermeasure implementation, etc.
(b) "Risk order" for risks resulting from not establishing specific values
(c) "Difficulty order" based on the difficulty of implementing the item

In all cases, it may be difficult to get a direct impression of development costs, but if there are external restrictions, such as legal, regulatory, or industry restrictions, development costs tend to rise. Likewise, systems without explicitly defined requirements carry high risks, and there is a significant likelihood that their development costs will rise. When requirements are complex and difficult, the difficulty of designing the system also rises, making increased costs likely.

Representative values are set for levels in order for users and vendors to reach more accurate agreements regarding non-functional requirements, but for some items, it is preferable to, in addition to selecting a level, decide upon and reach consensus regarding specific values. For example, the definition of "During business hours" in level 1 of "A.1.1.1 Operating hours (normal)" may differ for individual users and vendors, and may not always correspond exactly with the "9:00 to 17:00" listed

for the level. Similarly, level 1 for "A.1.2.2 Service switchover time" is "Less than 24 hours," and level 2 "Less than 2 hours," but it is possible that a value between these two values is desired.

2.1.3 Tree Diagrams

(1) Tree diagrams definition

Tree diagrams are visual depiction used to increase grade table and item list readability.

The items on the tree diagrams are organized from top left to bottom right in the general order in which they are to be coordinated by users and vendors. Although not specifically defined, the flow from left to right indicates the general middle category consideration order, while the flow from top to bottom indicates the consideration order of individual minor categories.

The metrics are numbered, making it easy to use them with other tools, and the metrics of important items are shaded in order to indicate that they are different than other metrics.

Figure 2.1.3.1 shows an example of a tree diagram

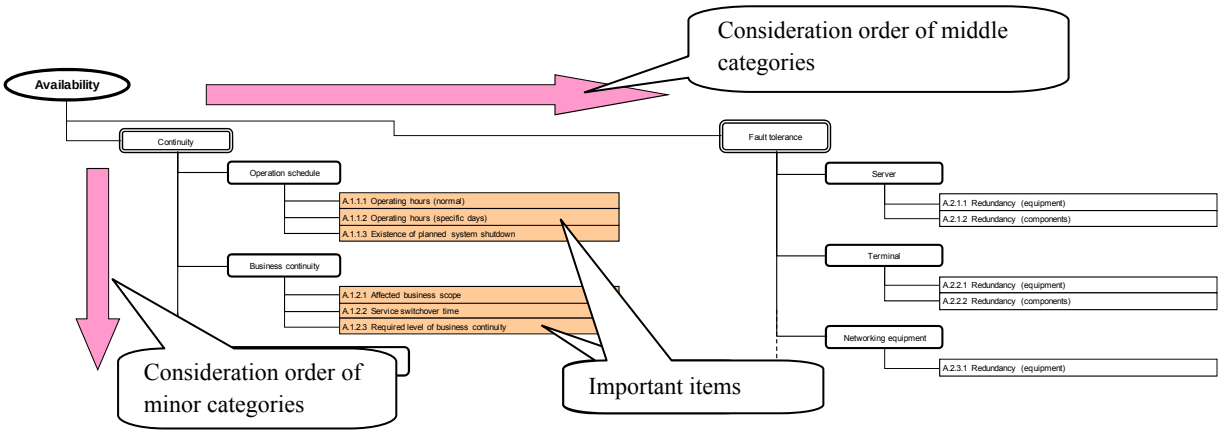


Figure 2.1.3.1 Tree diagram example

(2) Using the tree diagrams

The tree diagrams are used to obtain a bird's eye view of the entire project when considering non-functional requirements.

Specifically, it is used in confirming non-functional requirements consideration order and the scope of items which have already been considered, taking advantage of the fact that the consideration order and important items for each major category metric is presented on a single page.

2.2 Overview of major categories and points of consideration

Below are overviews and points of consideration for each non-functional requirements grade major category.

2.2.1 Availability

(1) Overview

"Availability" is a requirement related to keeping a system continuously available for use. Optimally, systems would continually offer services without any problems. However, in real-world systems, unexpected service outages are caused by a variety of factors, including hardware failures, operating system and software related problems, and disasters. From a system availability standpoint, consideration must be given to how to minimize service outages and, should they occur, their impact, as well as how to guarantee system operation quality.

Availability is composed of 4 middle categories: "Continuity," "Fault tolerance," "Disaster countermeasures," and "Recoverability."

(2) Points of consideration

"Continuity" is a basic requirement of availability, and defines four minor categories: "Operation schedule," "Business continuity," "Recovery objective," and "Uptime ratio." The metrics in each of these minor categories are all important items. In order to clarify availability requirements, one must define what an operational state of the system is, and clarify the system's recovery objectives in the event of failures. The former can be confirmed through the "Operation schedule" minor category and the "Business continuity" minor category's "Affected business scope" metric. The latter can be confirmed through the "Recovery objective" minor category and the "Business continuity" minor category's "Service switchover time" metric. In the end, these definitions are used in determining the uptime ratio. Derived uptime ratios will vary based on how an operational state of a system is defined, so it is important to clarify these definitions. System uptime ratios are calculated from actual system operation results, but also serve as availability requirement estimates, so the "Uptime ratio" minor category is placed in a position as an important item in the "Continuity" middle category. In the "Uptime ratio" metric, level values are expressed as numerical values, and considered as representing to what degree users wish to maintain business continuity. The notes columns of the "Uptime ratio" metric in the grade table and item list contain estimated values for reference use.

"Fault tolerance" categorizes system failure tolerance in terms of individual system component elements. "Fault tolerance" items must be considered in accordance with the contents which have been confirmed for "Continuity." If "Continuity" requirements are not considered when considering "Fault tolerance," gaps may occur between the level of system reliability expected by the user and the measures proposed by the vendor. For example, imagine that the required level for the metric "Recovery level objective (RLO)" of the minor category "Recovery objective (When business outage occurs)" under "Continuity", is "Specific businesses only." If this is the case, it is advisable to provide server redundancy for specific servers which handle important business. However, if the "Service switchover time" metric for the "Business continuity" minor category requires a

switch-over time under 60 seconds, and it is decided that all servers will be provided with redundancy in order to improve reliability from the standpoint of "Fault tolerance," the resulting system configuration will be excessive in comparison to its "Continuity" requirements. In order to prevent this type of perception gap regarding requirements and measures, requirement levels must be confirmed for all items while forming a consensus regarding system configuration.

"Fault tolerance" separates redundancy into equipment level redundancy, and component level redundancy within equipment. This is to prevent the common problem of overlooking fault tolerance requirements for single server configurations in systems with low availability requirements. For example, imagine that a user wants a single server configuration system with no server redundancy, but wishes to be able to continue and restart service provision, even if recovery takes a great deal of time in the event of a hardware failure. In that case, a minimum level of measures must be implemented, such as using redundancy for disks containing data in order to avoid losing data when the server stops. Attention must be paid not to be misled by the general item "equipment redundancy" and overlook support for specific areas.

"Disaster countermeasures" are fault tolerance requirements related to large-scale disasters. This item affects system configuration, such as server and storage configurations. Even if a system initially does not require remote backups, in case this will become necessary in the future, equipment which supports remote backups must be chosen from the start. If equipment which does not support remote backups is chosen, in the worst case scenario, the equipment will have to be replaced, resulting in overlapping investment. The decision during business continuity considerations of whether or not to consider disaster countermeasures significantly impacts costs, so disaster countermeasures are a major system theme.

The "Recoverability" requirement item relates to the abilities of the system to recover the system and restore data in the event of a failure, as well as the effort involved in doing so. It defines two minor categories: "Recovery operations" and "Availability confirmation."

When considering "Continuity," recovery objectives are already clarified, so the objective of this item is clarifying the structures and effort needed to implement those recovery objectives. "Recovery operations" are composed of two metrics: one concerning to what degree recovery from backups will be automated, and one concerning whether or not alternative business will be provided while business is stopped. Both are overlapping items with "Operability and maintainability."

"Availability confirmation" is for clarifying the scope of confirmation that availability requirement items are implemented by the system. Actual confirmation requires simulating system failures and confirming that the system responds as expected. As such, confirmation may be difficult in some cases. The cost of confirmation work may also rise precipitously depending on the system scale. As such, coordination of the confirmation scope must be completed at an early stage of system development.

2.2.2 Performance and scalability

(1) Overview

"Performance and scalability" consists of requirements related to system performance and future system expansion. "Performance" indicates whether or not resources can be used efficiently in providing services, and is generally expressed in terms of response and throughput requirements. "Response" indicates the amount of time between when a party which wants to use a service issues a service request and when the party is provided the service. "Throughput" indicates the amount of services that is provided within a unit time. Failure to clarify requirements may result in slow systems which are not suited to actual use, or in system infrastructures with advanced functionality which exceeds the system's actual needs. There are many different system architectures, so terminology must be clearly defined when defining response and throughput targets.

Frequently, systems are used over a long period of time, during which the number of users and the volume of data stored increase, resulting in overstretched system resources, and the system failing to perform the roles for which it was created. In order to prevent this situation, system scalability must be considered. Typical examples of scalability include replacing individual resources with larger resources (scale up), and deploying additional servers and equipment (scale out). By factoring these in during the requirements definition process, equipment expansion plans can be established more smoothly, and equipment can be pre-configured with extra capacity in order to lower future expansion costs.

"Performance and scalability" is composed of 4 middle categories: "Business processing volume" prerequisites, "Performance objective," a performance related requirement, "Resource scalability," a scalability related requirement, and "Performance quality assurance," a supplementary requirement item.

(2) Points of consideration

In order to establish consensus regarding performance and scalability related non-functional requirements, generally "Business processing volume" is determined first. The image one may have of "business" may be that of functional requirements, but it is important for determining system infrastructure non-functional requirements, and especially essential for performance and scalability requirements. The type of the system as well as a rough estimate of the business volume it will bear as the "Business volume during normal operation" minor category, and the amount of business volume increase that will occur over the system's lifespan as the "Business volume expansion" minor category, must be determined. Even if the "Business volume during normal operation" or amount of "Business volume expansion" are unknown, it is important to clarify why these are unknown, and when they will be determined, as well as to establish tentative values with some degree of margin built in. The "Number of users," "Number of simultaneous users," "Data volume," "Number of online requests," "Number of batch processes," and "Number of business functions" metrics were listed here, but metrics may be selected or supplemented in accordance with system characteristics in order to clarify performance and scalability related requirements.

Taking the assumed ”Business processing volume” into account, "Performance objective" must be

established giving consideration to the system's processing approach, peak-time characteristics, degraded operation, and the like.

The points which need to be considered vary based on processing approaches (batch, online, etc.). Taking the "Batch response" minor category as an example, since batches require much time to process, response targets should be indicated by processing adherence, and decisions should be made regarding whether processing can be performed within specified time slots, whether there is sufficient time for retrying in the event of failures, etc.

For the "Online response" minor category, it is possible not to decide on a single value for the entire system. Instead, adherence rates could be indicated for individual processes based on whether the process is reference-oriented or update-oriented, the importance of the system, etc., and appropriate system performance objectives could be decided by determining what percentage of the processes is capable of completing to perform within the specified timeframe. If targets are set incorrectly, the resulting system may lack processing power and be unable to supply sufficient services, or an unnecessarily costly system may be built.

In order to determine peak time performance objectives, consider for each process, how much the processing load will increase during peak time in comparison to the load during normal periods, whether it is possible to forecast the frequency of peak times and their time periods, and other matters. In order to determine degraded operation performance objectives, it is advisable to confirm the priority or importance of each process.

For "Resource scalability," determine how much resource is used when the system is in operation, or, viewed from a different perspective, how much free capacity there is. In order to indicate how much free capacity there is, utilization rate at time of service initiation, and the "CPU scalability," "Memory scalability," and "Disk scalability" minor categories for physical resource expansion capabilities should be confirmed. If there are other resources, such as printers or middleware, it is recommended that they be added as needed. It is important that the system be designed such that planned scaling up and scaling out are possible in response to future growth.

"Performance quality assurance" examines mechanisms for increasing performance quality.

The "Existence of bandwidth guarantee functionality" minor category is used for confirming whether or not network bandwidth is guaranteed, and, if so, to what degree. Since volume of data, such as images and video, that are handled by systems is growing, the impact of network performance on system response time is becoming larger than the impacts of CPU or memory performance.

The "Performance testing" minor category determines to what degree tests to evaluate "Performance objective" realization are implemented. Depending on the system, conditions after operation begins may differ from conditions during system construction, so regular confirmations may be necessary after operation starts.

2.2.3 Operability and maintainability

(1) Overview

"Operability and maintainability" consists of requirements related to system operation and maintenance service. Operation and maintenance related requirement items are used to determine system operation methods and administrator work procedures, and have a significant influence on the selection of equipment and software to be deployed. If review of these requirements are put off until later under the perception that they do not relate to system development, problems may result, such as not being able to establish the anticipated operation schedule, or being unable to recover from failures because necessary backups had not being taken. In order to prevent problems such as these, sufficient consideration to these requirements should be given during the requirements definitions phase.

Operability and maintainability is composed of 6 middle categories: "Normal operation," "Maintenance operation," and "Operation to ensure business continuity" requirements, which apply to normal operating hours, maintenance hours, and times when faults occur, respectively, as well as "Operating environment," "Support structure," and "Other operation management policies" requirements which define the system environments and structures used to implement system operation.

(2) Points of consideration

"Normal operation" defines, in addition to the "Operating hours" minor category which contains requirement items for times when the system is used, the following 3 minor categories as functions which may be realized by the system infrastructure: "Backups," "Operation monitoring," and "Time synchronization." The "Operating hours" minor category must be considered from both operability and maintainability perspectives as well as availability perspectives, and as such is an overlapping item. Furthermore, the "Operating hours" minor category defines two metrics: "Operating hours (normal)," for normal operation schedules, and "Operating hours (specific days)," for operation schedules other than those for normal operating hours. For situations where there are multiple specific days outside of the normal business operation schedule, such as business operations taking place on weekdays, backup operations on Saturdays, and planned outages on Sundays, confirmation must take place for each type of specific day.

"Maintenance operation" contains minor categories such as "Planned system shutdown," "Patch application policy," and "Maintenance during operation," which relate to the approaches used by and contents of maintenance operations performed in order to maintain system quality. These items significantly affect maintenance work approaches and scheduling, as well as which equipment is used in the system, and as such it is important that they be determined in advance.

"Operation to ensure business continuity" defines items used to determine the response in the event of a system failure, such as "Recovery operations," "System fault detection handling," and "Securing of replacement materials." As with the minor category "Operating hours" of "Normal operation", the minor category "Recovery operations" is an overlapping item in both "Operability

and maintainability" and "Availability." Since there are many items which significantly affect costs, such as the securing of equipment to be deployed as well as personnel and materials, etc., it is important that sufficient consideration be given from both the perspectives of availability and of operability and maintainability.

"Operating environment" defines items related to the environment in which system operation will occur, such as "Establishment of development environment," "Establishment of test environment," "Manual preparation level," and "Remote operation." These items significantly impact system operation methods, and sometimes overlooked items are discovered after actual operation begins, so special care must be given.

"Support structure" defines maintenance contract related items, such as "Maintenance contract (hardware)" and "Maintenance contract (software)," user/vendor role division related items regarding system operation , such as "Division of maintenance work roles" and "Division of first-line support roles," and items related to vendor support structures for user system operations, such as "Operation training" and "Regular reporting meetings." These requirements are often considered to be unrelated to system development and construction, and put off until later, but in reality must be decided in advance in order to secure system quality.

"Other operation management policies" defines ITIL related items, such as "Internal control support," "Service desk," and "Incident management." These items concern whether or not management will be performed, and when users and vendors agree on management being implemented, specific implementation methods must be confirmed. They affect both system design and development work, so advance confirmation must include specific implementation methods.

2.2.4 Migratability

(1) Overview

"Migratability" consists of requirements related to migration of current system assets. Except when a new system is being developed from the ground up, assets from existing systems must be migrated to new systems. This is because if assets cannot be migrated, the system will not be usable, as a whole, even if system development has been completed. As such, it is important to identify requirement items necessary for system migration, establish migration plans, and implement those plans.

Migratability is composed of 5 middle categories: "Migration period," which relates to the migration schedule, "Migration scheme," which relates to how the switchover to the new system will be performed, "Migration scope (equipment)" and "Migration scope (data)," which are used in assessing which assets will be migrated, and "Migration plans," which include rehearsals in preparation for migration work.

(2) Points of consideration

For "Migration period," consideration shall be given from the perspectives of how long the period will be between migration planning and system switchover, whether or not it will be possible to stop the system during this migration work, and whether parallel operation will be required. If parallel operation is required, it is also important to gain consensus regarding the period that the systems would operate in parallel.

The "Migration scheme" contains the "Number of steps for site deployment" minor category, for systems that will be installed at multiple locations, and the "Number of steps for business deployment" minor category, for systems composed of multiple businesses. In either case, the more steps involved in migration or deployment, the longer the period of partial coexistence of both the old and new systems. In situations where the operation of the overall system is maintained to allow coexistence of both old and new systems, considering parallel operation of both systems, it is more difficult to perform a multi-step migration than to perform a single-step migration. However, depending on system deployment risk levels, in some cases the difficulty of single-step deployment may be greater. As such, consider the risks of deployment for individual sites and businesses in deciding the number of steps involved in migration or deployment.

"Migration scope (equipment)" and "Migration scope (data)" shall be confirmed in order to confirm what will be migrated.

For the "Equipment to be replaced" minor category of "Migration scope (equipment)," it is important to confirm the scope of replacement, such as whether only the facilities and equipment of the old system will be replaced with new hardware in the new system, and the resulting system used, or whether the old system will be replaced with an entirely new system. When partial facility or equipment replacement will be performed, it is important to consider whether or not maintenance support will be offered for the hardware and software carried over from the previous system, as well as the compatibility of the facilities and equipment being replaced.

"Migration scope (data)" includes the "Migration data volume," "Migration data format," "Number of migration data media types," and "Difficulty of migration tool(s) (number of conversion rules)" metrics. In particular, when migrating data, facilities and migration tools will be necessary for converting data if data format is different from that of the new system. The complexity of migration tools is indicated by the number of conversion rules. This is important, since if the number of conversion rules increases, it will impact the amount of tool development and conversion operation time required. Furthermore, for each type of migration media that must be used when migrating, consideration must be given to how (the methods involved, the equipment used) they will be imported into the replacing equipment.

"Migration plans" includes confirmations of the "Migration work division," "Rehearsal," and "Problem handling" minor categories.

Specifications must be established regarding the division of duties between users and vendors concerning matters such as investigation of data to be migrated from the old system, extraction and conversion of migration data, importing of data into the production system and checking them. Note that the final migration results must be confirmed by users.

For rehearsals that involve external entities, as with normal rehearsals, the counterparty external system must be clearly identified, and the rehearsal's scope, environment, and the number of rehearsals to be carried out must be specified. Furthermore, if there are changes in the connection specifications which govern connections with the external system, the new system may need to support both new system and existing system specifications. When this is the case, in order to reduce system migration risks, rehearsals involving externally entities must be planned to confirm both connection specifications.

The "Problem handling" minor category is used in determining, in advance, personnel who will be stationed where the migration work is performed, the rollback timing handling plans, etc. Its objective is to respond smoothly in the event that a problem occurs during migration, and it is important that the contents of said response are confirmed.

2.2.5 Security

(1) Overview

"Security" consists of requirements related to ensuring the safety of an information system. If appropriate security measures are not implemented, threats may become a reality, disrupting business which makes use of the information system, and as a result, may incur significant direct and/or indirect social and/or financial damages. In order to prevent this, the security related non-functional requirements which need to be considered when constructing the information system must be identified, and must be reviewed taking care that nothing is overlooked.

Many security related non-functional requirements have an impact on information system performance. For example, there are many requests like encryption processing which place a burden on base information processing. As such, when considering security related non-functional requirements, it is important to also consider performance and scalability related non-functional requirements.

"Security" is composed of "Prerequisites / restrictions," consisting of prerequisites and restrictions related to system security, "Security risk analysis," "Security diagnostics," and "Security risk management," which relate to security management during both development and operation, "Access / usage restrictions," "Data confidentiality," and "Fraud tracking / monitoring," functions used in implementing security measures, and "Network measures," "Malware countermeasures," and "Web measures," the primary combination of functions used for security measures.

(2) Points of consideration

"Prerequisites / restrictions" items are used for confirming, primarily, the law and industry information security standards[4], guidelines, and organizational regulations such as company information security policies, when implementing information system security measures. The regulations, laws, guidelines, etc., which act as "Prerequisites / restrictions" must be confirmed, and security related non-functional requirement item levels decided in accordance with them. For example, there are sometimes, among regulations, etc., which must be complied with, clear security requirements which correspond with the "Authentication function" and "Data encryption" minor categories. When this is the case, non-functional requirements must be decided on such that there are no inconsistencies between the security requirements indicated by these regulations, etc., and selected item levels. The model systems show general examples whose security is not affected by industry standards or company policies, and as such, none of the examples include regulations. As such, the base values in "E.1.1.1 Existence of applicable company regulations, rules, laws, guidelines, etc." of the grade table are level 0 (none) for all model systems. Confirm whether or not there are regulations, laws, guidelines, etc. that must be observed in accordance with industry standards or corporate policies, and if there are, determine an appropriate level to satisfy them.

"Security risk analysis" relates to risk analysis items used in information system development to

[4] These include "Standards for Information Security Measures for the Central Government Computer Systems," "Computer System Safety Measure Standards for Banking and Related Financial Institutions," "Payment Card Industry Data Security Standard (PCI DSS)," etc. Please refer to sections 5.2.6 through 5.2.8.

identify potential threats, and clarify security measure implementation scopes. When considering "Security risk analysis," identify the assets used by the information system (hardware and software assets, as well as information assets), and confirm which of them are to be protected. Furthermore, when forming a consensus regarding security related non-functional requirements, users and vendors must reach an agreement on whether or not the security measures in the item list shall be implemented, as well as on the security risks that remain due to deciding not to implement the measures.

The "Security diagnostics" item is used in forming a consensus regarding security related testing of the information system being developed. When considering "Security diagnostics," also consider more specific diagnostic methods and the diagnostic scope, including which tools, review methods, etc. to use.

The "Security risk management" item is used in forming a consensus regarding how to handle threats and vulnerabilities identified after system operation starts. "Security risk management" includes items related to security patch application scope, timing, etc., and as such must be considered in conjunction with overall patch application scope and timing related items in "Operability and maintainability."

The "Access / usage restrictions" item is used in forming a consensus regarding restriction of access to and usage of assets handled by the information system being developed. When considering "Access / usage restrictions," consider measures for each implementation point (server, storage, etc.).

The "Data confidentiality" is used in forming a consensus regarding maintaining the confidentiality of data handled by or stored in the system being developed. When considering "Data confidentiality," consider the information assets to be protected, and the points at which data confidentiality is implemented. When performing encryption processing in order to maintain confidentiality, consider its effect on performance.

The "Fraud tracking / monitoring" item is used in forming a consensus regarding tracking and monitoring fraudulent behavior that may occur after system operation starts. When considering "Fraud tracking / monitoring," consider the impact on performance that result from taking security logs, etc., in order to detect fraud.

The "Network measures" item defines network security measures. The "Network measures" item is used to consider the deployment of a mechanism or structure for detecting fraudulent behavior and transmissions within the network and for blocking unauthorized transmissions, as well as to consider countermeasures against congestion caused by network based attacks. When server processing power will be increased as congestion countermeasures, it must be considered together with the "Performance and scalability" item's server processing performance related resource scalability item.

"Malware countermeasures" define security countermeasures against malware such as computer

viruses and worms. When considering "Malware countermeasures," consider the impact on performance that result from performing real-time malware detection, etc.

The "Web measures" item defines network security countermeasures against Web application vulnerabilities. When considering "Web measures," consider the impact on performance that result from performing real-time monitoring using WAFs (Web Application Firewalls).

2.2.6 System environment and ecology

(1) Overview

"System environment and ecology" consists of system installation environment and ecological requirements. The system environment section of this consists of "System restrictions / prerequisites," which relate to the conventions corresponding to system installation, and "System characteristics," "Conformity standards," and "Conditions of equipment installation environment," which relate to the users of the system, and its geographical spread. These items are difficult to change at a later stage if restrictions are discovered then, and as such, if definitions are overlooked, requirement definition reworking will be needed causing significant problems, so these items are important items.

The ecology section of this item is composed of "Environmental management." This primarily concerns waste material and CO_2 emission reductions, and energy consumption efficiency improvement. In recent years, there have been an increasing number of countries and regions around the globe with CO_2 reduction requirements and regulatory policies. As such, this is an important item.

(2) Points of consideration

"System restrictions / prerequisites" define two minor categories: "System construction restrictions" and "Operating restrictions." When there are organization rules, laws, regulations, or the like which act as restrictions or prerequisites affecting system construction or operation, consideration must be given to how to conform with them. If the system is constructed without giving these due considerations, it may be necessary at a later time to change the system's structure in order to conform with these restrictions and prerequisites, or to redesign the system. For example, there could be a case where a system is installed in a data center in accordance with rules that govern room access, and while there is a need for remote operation when the system goes into operation, the condition for the need of remote operation had been overlooked during the requirements definition phase.

"System characteristics" defines the "Number of users," "Number of clients," "Number of sites," "Geographical spread," "Specification of specific products," "System utilization scope," and "Multi-language support" minor categories. It is extremely important that users and vendors establish a common understanding regarding these items from an early stage. This is because these items serve as requirements that determine the scale and characteristics of the system. For example, if the number of users or number of clients is defined incorrectly, or insufficient consideration is given to future growth in the system's lifecycle, it may result in resource problems. Establishing a consensus regarding these items from an early stage makes it easy to understand the characteristics of the system being developed.

"Conformity standards" defines 3 minor categories: "Product safety standards," "Environmental protection," and "Electromagnetic interference." Products may be required to meet certain standards, depending on the purpose of the system, its installation environment, and its operating environment.

Product safety regulations, regulations governing the electromagnetic fields generated by equipment, and specified toxic substance usage restriction related standards are sometimes included in system requirements, so compliance with these requirements must be confirmed for the equipment which constitutes the system.

"Conditions of equipment installation environment" defines 7 minor categories: "Earthquake resistance / seismic isolation," "Space," "Weight," "Compatibility with electric facilities," "Temperature (range)," "Humidity (range)," and "Air conditioning capacity." These items tend to be overlooked during the requirements definition phase. For example, if due consideration is not given to the installation environment during the requirements definition phase, when the time comes for the system to actually be installed, it may be found that the floor does not offer sufficient support, the system cannot be installed due to space limitations, or other similar problems may arise.

"Environmental management" defines 4 ecology related minor categories: "Measures to reduce environmental load," "Energy consumption efficiency," "Amount of CO_2 emissions," "Low noise." With regards to the ecology, the number of companies using a green procurement approach, led by government agencies, has been increasing in recent years. There is also a strong likelihood that this trend will be reinforced in the future through legal measures such as carbon taxes. Ecological considerations also relate to corporate social responsibility and the establishment of fair, transparent, and healthy business, and are expected to become an even greater and more important factor in fostering societal trust in companies.

3. FAQ

[Scope of the Non-functional requirements grades]

Q1: Why were these 6 major categories chosen for the non-functional requirements grades?

A1: Various standards and knowledge derived from actual system deployment cases which pertain to the user requirements that should be confirmed when establishing a system infrastructure were aggregated, organized, and categorized into the 6 listed major categories. Standards such as ISO/IEC 9126 were also referred to during this process, but as the non-functional requirements grades primarily focus on non-functional requirements implemented by system infrastructure, they do not cover all of the items included in those standards.

Q2: Are application requirements not included in the non-functional requirements grades' scope?

A2: Functional requirements are primarily implemented through businesses and applications, while non-functional requirements are primarily implemented in the area of systems referred to as "system infrastructure." "System infrastructure" refers to hardware devices such as servers, storage, and network equipment, and software such as operating systems, middleware, and other control and operation management software. The "non-functional requirements grades" cover the non-functional requirements implemented by system infrastructure, and its scope does not include the functional requirements implemented by businesses and applications. However, when carrying out actual system requirements deliberation, the line between system infrastructure and applications is not always clear, and we recognize that there are situations in which these need to be considered together. As such, the non-functional requirements grades also include items which may appear at first glance to be business or application requirements, but which must also be considered as part of system infrastructure consideration (ex: business processing volume, operating hours, etc.).

Q3: Why was the word "grade" chosen?

A3: "Grade" is a conceptual term arrived at when searching for a term to refer to both the stepwise differences between system implementation levels, and the set of requirements which form a system's specifications. It was not chosen to reflect superiority or inferiority; instead, it more closely resembles the categorization of cars into categories such as "luxury grade," "economy grade," and "sports grade," with each grade corresponding to specific demands.

There are differences in implementation standards between information systems, resulting from the combinations and relationships between the hardware, facilities, operating systems, middleware, operation management structures, and operation management systems of which they are composed. It is difficult for users to recognize these differences from the initial stages of system development, and difficult for vendors to provide technical explanations.

Given this situation, it was decided to indicate differences between systems as stepwise "grades," and to establish "non-functional requirements grades" to serve as a structure that assist users and vendors in confirming requirement items.

Q4: Who are the intended users of the non-functional requirements grades?

A4: The intended users of the non-functional requirements grades are primarily persons responsible for placing or receiving orders, and who are involved in the provision, proposal, or determination of non-functional requirements during the requirements definition phase or similar phases of information system development. Non-functional requirements grades documentation refers to those placing orders as "users," and those receiving orders as "vendors." Specifically, based on the "Management Participation in Securing of Requirement Quality Second Edition (SEC BOOKS)," the information system departments of companies placing orders were envisioned as the "users." However, these definitions were made merely as a matter of convenience in providing objective explanations regarding grade usage within this guide, and does not limit who can use the non-functional requirements grades, nor in what way they can use it.

Q5: At what point in a system's life-cycle are the non-functional requirements grades used?

A5: The non-functional requirements grades are intended to be used in processes and activities which deal with non-functional requirements; during the planning processes, requirement definition processes, and development processes of "Japan Common Frame 2007." These correspond to the upstream processes such as the "systemization direction," "systemization planning," and "requirements definition" processes described in "Management Participation in Securing of Requirement Quality Second Edition (SEC BOOKS)." The non-functional requirements grades are a tool for users and vendors to form a consensus regarding non-functional requirements. It was designed with the assumption that its contents would be listed in documentation such as RFPs, requirements definition documents, and estimate proposals, and contained in system design contracts in the form of agreements. Its use is primarily envisioned in upstream processes, but contents organized under the non-functional requirements grades can also be used in system design and testing, so please make use of them as necessary.

[Grade table, item list, and tree diagrams]

Q6: In what order are the levels in the item list arranged?

A6: The values that the metrics could normally attain were organized into 6 levels, from level 0 to level 5. Higher levels indicate higher degree of difficulty, and generally higher development costs. Adjacent level values are chosen such that there are architecture gaps between them, such that when level values are raised or lowered, as a result there will be some sort of structural change(s) in the system's design or implementation in order to satisfy the affected requirements. For some metrics, the level choice is binary, consisting only of either 0 or 1. These simple binary values express, for example, whether or not there are legal

restrictions which affect the system, or the "risk order" for risks resulting from not establishing specific values. These binary values define the level order in situations where the architecture gaps between level values are unclear, making their effect on development costs difficult to grasp, yet where restrictions exist. They also define the level order when the higher the risk the higher the difficulty involved in implementation, resulting in the possibility of higher costs.

Q7: The same metrics appear in multiple major categories. What does this mean?

A7: The non-functional requirements grades assume that the parties involved in considering each major category, and the priority of their consideration, are different. Some items are repeated in order to prevent them being overlooked. The values entered for these items are to be identical for all major categories in which they appear. When multiple people merge the results of their considerations of items in individual major categories, or when major categories are not considered simultaneously, but at different times, check the overlapping item column for "X", indicating overlapping items, and ensure that the results of consideration correspond across major categories.

Q8: What does "Impact on operation costs" indicate?

A8: The levels in the item list and grade table indicate development costs, but when developing a system, the system's total cost including development costs as well as operation costs should be evaluated. Development costs refer to those costs incurred from the time when requirements definition is completed until the time when the system is finished and put in service. Operation costs refer to the costs incurred after the system is launched, for system operation and management. Requirement items defined in the item list include items for which operating costs can be lowered by spending more on development, such as process automation. Items for which there may be a tradeoff between development costs and operating costs are indicated by an "X" in the "Impact on operation costs" column. In some cases, total costs may actually be lower for a system when a level which incurs higher development costs is selected.

Q9: On what basis were the important items covered by the grade table selected?

A9: The non-functional requirements grades item list contains 236 metrics. The order in which some of these metrics are decided varies, as does their impact on system infrastructure costs, making some sort of grouping necessary. Some metrics were selected as important items giving consideration to the fact that simply having too many items would result in consuming much time in deliberation. Items with large impacts on system development costs or quality were chosen as important items, evaluated from the perspectives of both users and vendors.

Q10: What do the tree diagrams show?

A10: The tree diagrams are used to increase grade table and item list readability. The items on a tree diagram go from top left to bottom right in the general order in which they are to be

coordinated by users and vendors. Although not specifically defined, the flow from left to right indicates the general middle category consideration order, while the flow from top to bottom indicates the consideration order of individual minor categories.

[Using the non-functional requirements grades]

Q11: There are too many items to consider at once. What should I do?

A11: The most critical metrics from the item list are listed in the grade table to serve as a starting point in requirements consideration. The grade table not only narrows down metrics to the highly important metrics, but also provides level value selection examples (base values) for the model systems. When considering requirements, one possible approach is to select the most appropriate model system from the grade table, and adjust each metric's selected level to better reflect the requirements of the system actually being developed.

Q12: There are items which don't relate to the system I'm considering. What should I do?

A12: The grade table and item list contain items necessary for system development. They are listed in RFPs and estimate proposals during the requirements definition process, and are included in corresponding agreements. There may be some items which do not need to be considered for some user environments and systems. When that is the case, users and vendors must form a consensus regarding why those items do not need to be considered.

Q13: There are items which can't be decided by the time the contract is entered. What should I do?

A13: When using the non-functional requirements grades, it is best to reach a consensus regarding all item list items during the requirements definition process. However, it may not be possible to decide all requirement items during the upstream process, since, for example, there may be items which cannot be decided until detailed design work has been completed. In the event that there are items which cannot be decided, clarify when and how they will be decided. Contract modifications and multi-phase contracts must also be considered.

Q14: What should I do if there are requirement changes during the development process?

A14: The non-functional requirements grades are intended to be used during the requirements definition process, but can also be used to confirm whether the contents decided therein are properly reflected in system design and construction. It is quite conceivable that during the development process, requirement changes may become necessary. The non-functional requirements grades can be used as a tool for users and vendors to confirm and reach a consensus regarding the contents and degree of the requirement changes.

Q15: Are there any conditions to tool usage?

A15: The copyright to the two usage guides (the "Usage Manual" and "Description Manual") and three tools (the "grade table," "item list," and "tree diagrams") is held by the Information-Technology Promotion Agency, Japan (hereafter "IPA"). It is the desire of IPA that these tools be used widely throughout the world. To this end, IPA has publicly released

these materials, to be used freely, with only the minimum usage conditions needed to maintain the copyright. IPA also provides a "utilization sheet," a spreadsheet version of the item list and grade table which is freely modifiable.
Please refer to the detailed usage conditions listed in each guide and tool.

4. Terminology

	Terminology	Description
[A]	Adherence rate of response	The rate of achievement of system response targets (to what degree, during business processing, the response levels decided as targets for all transactions are achieved). Adherence rate of response = (number of transactions which satisfy defined targets) / (total number of transactions)
	Alive monitoring	Monitoring method used to confirm if an entity being monitored is running.
	Alternative operation	Operation methods for using alternative equipment/systems in the event that a system or some services experience an unrecoverable failure.
	Amount of CO_2 emissions	The amount of CO_2 emissions produced by a system during the course of providing its services. Emissions assessment must include not only the energy consumed by a system as it provides services, but throughout its lifecycle, including equipment production and disposal. Reduction motivation factors are under consideration in the form of the emissions trading, carbon taxes, etc. described in the Kyoto Protocol, whose goal is the reduction of greenhouse gas emissions.
	Ancillary facilities	Facilities pertaining to systems, including buildings in which servers are installed, electrical facilities, racks, etc.
	Assets	System related hardware and software assets, information assets, and businesses.
	Authentication function	Function for identifying users, devices, etc., based on identification information.
	Availability	(1) Ability indicating to what degree required business operations can be implemented at a given time under specified usage conditions. The "Availability" major category is defined to include reliability. (2) Characteristic representing the capability of being accessible and used when requested by permitted agents (users or programs).
[B]	Backup	Storing data in a restorable form on separate media in order to prevent data loss.
	Bandwidth guarantee	Bandwidth refers to network speed, and a bandwidth guarantee is a guarantee of a specific transmission speed to system (network) users.
	Base value	Same as "selected level."
	BtoB (Business to Business)	Transactions between businesses. Often, these consist of fixed transactions between companies which have entered a contract. B2B.
	BtoC (Business to Consumer)	Transactions between companies and consumers via a network. Generally, "consumers" refers to the general public, and systematic demand forecasting is difficult. B2C.

[C]

Terminology	Description
Business	Processing a given requests using functions of a system. This includes not only system functions, but system usage and activities carried out by people.
Business continuity	Ability to utilize functional resources or recover within a matter of moments in order to continue business operations in the event of unforeseen problems such as disasters or failures. BCP (Business Continuity Plan).
Cluster	System configuration in which multiple computers are gathered together into one in order to improve system reliability or processing performance. Methods include cold standby and hot standby.
Compatibility with electric facilities	Degree of compatibility between equipment to be installed and the electrical facility characteristics (electrical supply/voltage/number of circuits, etc.) of a site in which the equipment is to be installed. For example, equipment which can use 100V AC power, supports low power consumption, etc., can be generally considered to offer a high level of compatibility.
Component	Parts which constitute a device or equipment. For example, server components include CPUs, disks, network cards, etc.
Confidentiality	Attribute of preventing access to or viewing of information by unauthorized entities (users or programs).
Conformity standards	International standards, national standards, foreign standards, etc. that a product complies with.
Congestion	Concentrated, high access load which has a significant impact on transmission and processing.
Conversion rule	Rules needed for converting migration data when migrating it to a new system. The amount of development and migration work varies significantly depending on the volume of data which must be converted, and the number of conversion rules.
CPU utilization	The ratio of CPU used by operating systems and applications on a system during processing. This is normally expressed in terms of average utilization per unit time. CPU utilization = (CPU usage time over course of a unit of time) / (Unit of time)
CSR (Corporate Social Responsibility)	This specifically refers to accountability to stakeholders, legal compliance, corporate governance, etc. These consist of voluntary self-governance activities, and differ fundamentally from advertising and public relations activities. The goal of corporate social responsibility is frequently the cultivation of societal trust in order that the company can continue to exist and develop perpetually.

	Terminology	Description
[D]	Data integrity	The guaranteeing that all data is in order. Guarantee that operations can be correctly carried out on data, that resulting quality levels are sufficient, and that changes to data can be detected.
	Data recovery	The restoration of data lost due to an information system failure.
	DB diagnostics (Database diagnostics)	Analysis of existence of settings resulting in database vulnerabilities, etc., in the event of an internal or external attack on the system.
	dB (decibel)	Decibels are, originally, dimensionless units. However, this document uses the term in its conventional sense, as sound pressure level unit (properly expressed as "dBSPL"). The decibel scale is logarithmic, with an increase of 6dB representing a doubling of the initial sound pressure, and an increase of 10dB representing a tripling. For example, 60dB represents roughly triple the sound pressure of 50dB.
	Decentralized storage	Storage of backup data in a location geographically distant from where the information system is installed.
	Defragmentation	Reducing of blank space fragmentation in data storage areas by rearranging said data.
	Denial of service (DoS) attack	Sending a high volume of packets or data to server services, consuming line capacity, memory capacity, etc., in order to overload CPUs, causing service and system processing capability to fall, or the system itself to go down.
	Digital signature	Information appended to electronic documents to verify their validity, or the technologies used to do so (digital signatures can be used to identify signatory parties, detect tampering, etc.).
	Disk utilization	The percentage of a disk's total capacity that is filled with data. Disk utilization = (Disk usage) / (Total disk capacity)
	Double failure	A failure in a system component for which redundancy has been provided, which occurs after a single failure has occurred, and affects the same type of system component. If single-level redundant design has been used for the elements which failed, business will be shut down.
	DR (Disaster Recovery)	Methods or plans for restoring business in the event that an unforeseen event such as a disaster or failure significantly impacts a system.
	DR site	A site housing a system which can be used in place of the normal operation system in the event that the system fails and cannot be recovered due to a large-scale disaster.
[E]	Earthquake resistance	Measures to protect computer equipment from earthquake shakes, such as securing the equipment to their racks.

Terminology	Description
Electric and magnetic field countermeasures	Measures taken to prevent electric and magnetic damage to systems.
Electric leak countermeasures	Measures taken to prevent damage to systems caused by electrical leaks. This includes electrocution countermeasures, leak current break measures, etc. (Related terminology) → Leak current break measures
Energy consumption efficiency	Defined by the "Act on the Rational Use of Energy" (known as the "Energy Saving Law") of Japan as energy consumption, measured as stipulated in said law, divided by composite theoretical performance (as such, the smaller the resulting number, the greater the efficiency level). The less energy needed to achieve the same level of performance, the greater the energy consumption efficiency.
Equipment installation environment conditions	The environment which buildings can supply for equipment installation. Specifically, this includes allowed equipment weight, space, compatibility with electric facilities, temperature, humidity, earthquake resistance / seismic isolation, etc.
Equipment to be replaced	The equipment that makes up a system infrastructure which will be replaced with new equipment.
Error correction	A function for ensuring data integrity that corrects detected errors in data. (Related terminology) → Data integrity
Error detection	A function for ensuring data integrity that detects errors in data. (Related terminology) → Data integrity
Error monitoring	Monitoring method in which errors are detected based on the message output to log files by servers and other equipment which make up the system, or by middleware, applications, etc., running on said equipment.
Expandability of the existing equipment	Ability to improve a system's performance or capacity simply by adding or installing new elements, without disposing of already deployed equipment. Even if a contract specifies that upgrading is possible, if box swaps, etc., are necessary, this capacity is deemed to be low.
External data	Data stored in external systems. This may consist of the aggregation source of data stored on the system being development, or copies of such data.
External system	Systems outside the scope of the developed system (existing systems linked with the system being developed, etc.).

	Terminology	Description
[F]	Fault tolerance	Capability to maintain a specified operational level in the event of a failure.
	Fire prevention measures	Measures taken to prevent fire damage to systems. Includes detection measures, fire extinguishing measures, etc.
	First-line support	The initial investigation work performed by fault reception desks, such as investigation of information systems, or the equipment, software, etc. of which they are composed. This primarily consists of information gathering and problem isolation.
	Floor load	Weight per square meter which a floor can support. The larger this number, the greater the amount of equipment which can be concentrated in an area. Standard office floors have a floor load of 300Kg/m^2, while data centers can have floor loads upwards of 1,000Kg/m^2.
	Floor-standing equipment	Equipment designed to stand on its own directly on a floor. Also referred to as "pedestal" or "tower" form factors.
[G]	Gal	CGS unit which expresses acceleration (1Gal=1cm/sec^2). Named after Galileo Galilei in honor of his discovery of the law of falling bodies. For example, the acceleration due to gravity at the earth's surface is approximately 980Gal. The relationship between earthquake intensity and Gal is said to be as follows: seismic intensity 4 (25 to 80Gal), seismic intensity 5 (80 to 250Gal), seismic intensity 6 (250 to 400Gal), seismic intensity 7 (400Gal or greater).
	Generation management	Management method in which regular backups retain not only the most recent set of data, but past data as well, and data restoration can be performed using any of the retained backup data sets.
	Grade	The set of selected levels for non-functional requirements and the selection conditions that correspond with a model system.
	Grade table	Grade table for system infrastructure non-functional requirements. The non-functional requirements grades provide grade tables for 3 model systems.
[I]	IHV (Independent Hardware Vendor)	Hardware companies which manufacture and sell their own hardware, and are not subsidiaries of specific hardware manufacturers.
	Important item	Item with significant impact on quality and cost during system infrastructure non-functional requirements consideration. Indicated in the item list with an "X" in the important item column, and in the tree diagrams by shading the corresponding metric.
	Incident	A unit representing a failure or a problem encountered by an information system which must be handled by support personnel.

	Terminology	Description
	Information security policy	Indicates an organization's security related policies. In general, these policies contain information security objectives (protection scope), as well as clarifying what actions the organization will implement in order to achieve these objectives, which personnel are involved, etc. Based on these information security policies, standards for measures to be implemented, and procedures for implementing said measures, are established.
	Introduction support	Support, primarily, concerning product usage methods, construction, etc., when deploying new products in a system.
	ISV (Independent Software Vendor)	Software companies which produce and sell their own software, and are not subsidiaries of specific software producers.
[J]	Journal	Saved history and records used in determining the cause of and recovering from system failures and processing errors.
[K]	Key management	Management of keys used in encryption, digital signatures, etc.
[L]	Large-scale disaster	Natural disasters such as earthquakes, typhoons, etc., as well as disasters caused by intentional destructive acts, such as terrorist acts. These may cause direct destruction of systems, or present complications to system business continuity, by shutting off lifelines such as power or water supplies.
	Law on Promoting Green Purchasing	Abbreviated name of the "Act on Promotion of Procurement of Eco-Friendly Goods and Services by the State and Other Entities" of Japan. Green purchasing refers to taking the environment into consideration when purchasing products or services, giving careful thought to the necessity of the purchase, and selecting products and services with minimal environment impacts. This law mandates green purchasing for state and other entities, and calls for green purchasing by local public bodies, companies, and the public. Green purchasing does not consist merely of improving the environment friendliness of consumer activities, but promotes the development of products with minimal environmental load by companies as well, with the potential for changing economic activities as a whole.
	Leak current break measures	Electric leak countermeasures which prevent electric leak currents from entering the system.
	Level	Values, from 0 to 6, corresponding to a metric and indicating what value should be normal for the item. When there are 5 or fewer levels, the levels are listed starting from the left.
	Level of decentralized storage	Degree to which external data storage locations are dispersed.
	Level value	Defined, concrete implementation levels for each metric. Composed of one of the numbers from 0 to 5, and an explanation of what that number represents.

Terminology	Description
Lightning countermeasures	Measures to protect the system from line surges due to lightning.
Line	Transmission channels which networks are composed of.
Load spike	This refers to short periods of loads far higher than the loads experienced during normal operation (a state where the assumed business peak load is exceeded). These are especially common in systems for general users, where the number of clients cannot be limited.
Log rotation	Switchover of log files after specified periods of time, or when they reach specified sizes, and deletion of past logs, in order to prevent log file bloating.
Maintenance during operation	Adding or removing equipment to/from information systems, or replacing components of information systems, while the systems are operational.
Maintenance operation	Operations carried out in order to maintain the system in a properly functioning state. (Related terminology) → Normal operation → Operation to ensure business continuity
Maintenance parts	Replacement parts for hardware.
Maintenance staff	Personnel who perform on-site work such as maintenance operations and failure first-line support.
Malware	Collective term for malicious software, such as computer viruses, worms, spyware, etc.
Memory utilization	The ratio of memory used by the operating systems and applications on a system during processing. Memory utilization = (Amount of memory used) / (Total amount of memory)
Metric	Concrete, standardized index for objective measurement. In the non-functional requirements grades, this refers to the concrete indices which can be used to make objective level judgments when setting levels for each item.
Migration data format	Data formats which must be considered for migrating to a new system, such as application dependent formats, table formatted data, and character encoding.

[M]

Terminology	Description
Model system	Examples of systems with defined non-functional requirement items, based on the Ministry of Economy, Trade and Industry reliability guidelines and IPA Critical Infrastructure Information Systems Reliability Research Group reports. The following three examples are provided. • System with very significant social impact • System with limited social impact • System with almost no social impact
Model system sheet	Collection of representative non-functional requirement items indicating the properties of each model system. Packaged together with the grade table.
Monitoring	Confirmation of whether or not the states of an information system, or the equipment, programs, etc., which constitute the system match the desired states, and notification to designated parties based on those confirmation results, or the mechanism for doing so. (Related terminology) → Alive monitoring → Error monitoring → Resource monitoring
MTBF (Mean Time Between Failures)	Average interval (time) between one system failure and the next. Determined by dividing the total operating hours by the number of failures which have occurred.
MTTR (Mean Time To Repair / Mean Time To Recover)	Average time between when a system failure occurs and when it is recovered. Determined by dividing the total recovery time by the number of failures which have occurred.
Network diagnosis	Analysis of vulnerabilities in servers, networking equipment, etc., by mounting simulated attacks on them.
Network segmentation	Configuring a network by dividing it into multiple areas in accordance with its purposes and the system's structure.
Networking equipment	Equipment used in system LANs, or for connecting externally. Switches, routers, etc.
Normal operation	The operation method designed to be used when all parts of an information system are working properly.
Number of business functions	Number of functions of which business is composed (determined via function configuration diagrams, function information relational diagrams, etc.). Can be substituted with the number of sub-systems, number of screens, etc.
Number of clients	The number of terminals issuing service requests.

[N]

	Terminology	Description
	Number of migration data media types	The number of types of media which must be used in migrating data from the existing system to the new system. This includes, for example, tape, disks, forms, etc. It also includes data transfer via network connection as a media type.
	Number of sites	The number of sites at which a service provision system is deployed. Generally, this refers to the number of sites at which system equipment is installed, such as branch offices, stores, factories, etc.
	Number of steps for business deployment	The number of deployment steps when performing stepwise migration and deployment of business functions onto new systems, when the systems are composed of multiple businesses. For example, when a mission-critical business system composed of 3 business subsystems is migrated in the order of business A - business B - business C, the number of steps for business deployment is 3.
	Number of steps for site deployment	The number of deployment steps when performing stepwise migration and deployment of system infrastructure and data to new systems, when systems are installed at multiple sites. For example, when a mission-critical business system that is used between the head office and branches is migrated in the order of head office - branch A - branch B, the number of steps for site deployment is 3.
[O]	Operating hours	The hours during the day when the system provides services.
	Operation	(1) Series of actions performed on information systems. (2) The work to maintain a system so that the system can stably provide services.
	Operation site	Location in which an operational system is installed
	Operation to ensure business continuity	Operation method designed for the event of a fault occurring within the system, or in a linked external system.
	Operation training	Training regarding actions performed on information systems.
	Overlapping item	Item which is repeated in multiple major categories. Indicated in the grade table and item list with an "X" in the overlapping item column.
[P]	Parallel operation	Operating both new system and existing system in parallel.
	Patch application	Performing of operations, from patch installation to operation confirmation (includes not only patch deployment, but patch validation work as well).

Terminology	Description
Peak time	Time when system is under maximum load due to an increase in processing volume per unit of time, etc.
Performance quality assurance	Items necessary to satisfy or build-in performance requirements.
Planned system shutdown	Planned information system outages for the purpose of maintenance, inspection, etc. Unintended information system outages caused by failures, etc., are called "unplanned system outages."
Point in time recovery (PITR)	Function in data recovery operations using backups for recovering data contents up to a specified point in time.
Power loss countermeasure	Measures enacted to ensure a stable supply of power in the event that a power outage or momentary power interruption should occur.
Preventive maintenance	Replacement of supplies, primarily, at fixed intervals, before failures can occur. There are two approaches to preventative maintenance: one based on how long the supplies have been used, and one based on proactive monitoring results. (Related terminology) → Proactive monitoring
Proactive monitoring	Monitoring of minor equipment errors, resource usage conditions, etc., in order to detect signs of impending problems before critical system failures can occur. Proactive monitoring makes preventive maintenance possible. (Related terminology) → Preventive maintenance
Process margin rate	Target that specifies how many times greater a system's processing capacity is than the desired unit time processing volume. (Setting a high margin results in excessive investment, while setting a low margin results in systems not being able to handle processing loads greater than those envisioned during system design.) Normal process margin rate = (number of processes per unit time during normal operation)/(number of processes per unit time) Peak time process margin rate = (number of processes per unit time during peak times)/(number of processes per unit time) Degraded operation process margin rate = (number of processes per unit time during degraded operation)/(number of processes per unit time)
Rack-mount equipment	Equipment designed to be mounted in 19 inch racks, etc.

[R]

Terminology	Description
RAID (Redundant Arrays of Independent (Inexpensive) Disks)	Technology in which multiple hard disks are combined to improve reliability and accelerate response. RAID1 offers disk mirroring. RAID5 improves reliability by distributing error correcting code across multiple disks.
Recoverability	Capability of restoring a system to required levels in the event of a failure.
Recovery level objective	Target that specifies to what level a system should be restored (system recovery only, restoration to a state where business can be immediately resumed, etc.) when a failure results in a business outage. RLO.
Recovery objective	Targets and objectives for what should be recovered, to what extent, in what amount of time, when a failure results in a business outage. Aggregation of RTO, RPO, and RLO.
Recovery patch	Patch used to fix a product flaw.
Recovery point objective	Target that specifies up to what point a system should be restored using backup data when a failure results in a business outage. RPO.
Recovery tasks	Tasks involved in restoring a system to a required level in the event of a failure.
Recovery time objective	Target time it takes to recover to RPO and RLO specified targets in the event that a failure causes a business outage. RTO. The total time it takes for a system to recover is used as the Mean Time To Repair (MTTR) in uptime ratio calculation.
Redundancy	The state or property of a system being designed or planned to provide alternatives in the event of a fault, deploying one or more spare functional units to be used in case one unit experiences a fault.
Remote monitoring	Monitoring environment implementation method where monitoring results are sent to a location other than the one where the monitored entities are located.
Remote operation	Operating environment implementation method where operations and maintenance work on an information system are performed from a location other than the one where the information system itself is located.
Required level of business continuity	Degree to which business must be continued in the event of a failure.
Resource	Collective term for assets necessary for satisfactory information system operation, such as CPU, memory, storage, etc.
Resource monitoring	Monitoring method which confirms whether or not monitored resources are excessive or deficient.

Terminology	Description
Response	The amount of time between when a request is sent to a system, etc., and when a response (result) is received. In the case of batch processing, this is synonymous with turnaround time (time until first results are received). (Related terminology) → Turnaround (time)
Retry	A function for ensuring data integrity that re-executes processing when a data error is detected. For example, this includes command re-execution by hardware such as arithmetic units or registers. (Related terminology) → Data integrity
RLO (Recovery Level Objective)	Target that specifies to what level a system should be restored (system recovery only, restoration to a state where business can be immediately resumed, etc.) when a failure results in a business outage.
RoHS directive (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment)	Regulations, established by the European Union, which restrict the use of certain hazardous substances in electrical and electronic equipment. These take into consideration the environmental impact of disposing of electrical and electronic equipment which contains hazardous substances. It defines the maximum concentration tolerance of 6 materials (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyl, and polybrominated diphenyl ether). It applies to electrical and electronic equipment marketed in European Union member nations.
Rolling upgrade	The method for applying patches to cluster or dual architecture systems without stopping operation, by using switchover or degraded operation, and applying patches to individual nodes sequentially.
RoSPA (The Royal Society for the Prevention of Accidents)	British Royal Society for the Prevention of Accidents. Defines noise standards, etc., for the prevention of work accidents.
Route	The path taken by data passing through a network.
RPO (Recovery Point Objective)	Target that specifies up to what point a system should be restored using backup data when a failure results in a business outage.

Terminology	Description
RTO (Recovery Time Objective)	Target time it takes to recover to RPO and RLO specified targets in the event that a failure causes a business outage. The total time it takes for a system to recover is used as the Mean Time To Repair (MTTR) in uptime ratio calculation. (Related terminology) → RPO → RLO → MTTR
Scale out	One approach to improving server processing capabilities. Multiple parallel servers are used to increase overall system server processing capabilities.
Scale up	One approach to improving server processing capabilities. CPUs are added, or replaced with higher performance units, in order to improve server processing capabilities.
Scheduled maintenance	Maintenance work which is performed regularly. This includes hardware maintenance, such as replacing and refilling supplies, and software maintenance, such as deleting unnecessary logs in order to free up disk space.
Second-line support	Support performed after first-line support. Second-line support includes failure location identification, and failure cause determination, correction, confirmation, and provisional workaround measures.
Secure coding	Programming method to avoid vulnerabilities from being introduced into source code.
Security	In the context of this grades standard, "information security" which protects the system's information assets. In a broad sense, "security" also includes "safety" (state of people or objects being free of injuries or damage), but when this grade standard refers to "security," it does not include that sense of the term.
Security patch	Patches which are used to repair security holes.
Security risk	An undesirable state or condition of an asset which should be protected by the system.
Security risk analysis	Identifying and analyzing possible security risks and security threats.
Security risk countermeasure	Measures implemented via technologies or operation methods to ensure information security.

[S]

Terminology	Description
Seismic countermeasures	Measures taken to prevent earthquake damage to systems. This includes earthquake resistance measures, seismic isolation measures, and shake control measures. (Related terminology) → Earthquake resistance → Seismic isolation
Seismic isolation	Measures for reducing the amount of vibration imparted by earthquakes to equipment.
Selected level	Level selected for envisioned model systems. Composed of level values and level descriptions. (Related terminology) → Base value
Server monitoring	Monitoring of servers which constitute an information system, and/or the software which provides server functions. Node monitoring.
Service	Benefits offered by a system. System here refers to an IT system.
Service desk	Organization function that performs information system maintenance, and provides service support for daily operations to system users.
Service switchover time	The time required to switch services over from one unit to another in systems with redundancy achieved through cluster configuration, etc. Synonymous with "down time." (Related terminology) → Uptime ratio → MTTR
Shared center	Shared data centers or server groups which can be used when large-scale disasters occur and system recovery is not possible.
Single failure	A failure in a single element of a system for which redundancy has been provided. Business can be continued by using an alternative element.
Skill level	Level of skill in business functions and products which constitute an information system.
Software distribution	Distributing software recovery patches, version upgrade files, etc. to the equipment which constitutes an information system.
Sorry action	When a system is under heavy load, the issuing of notifications to users, such as reporting that "the system is currently under heavy use," and/or informing users of alternatives, instead of merely failing to respond to user requests. When sorry action design is not performed, systems often give no response when under heavy loads.

	Terminology	Description
	SPOF (Single Point of Failure)	Components which will cause a system outage when a failure occurs in them.
	Standby equipment	Backup equipment used to replace servers or terminals in the event of a failure.
	Storage	Devices which store data, and are one of the components which make up a system.
	System	Collective term for, primarily, hardware, software, and other facilities. Synonymous with IT system. In its broad sense, the term "system" also includes people, but the non-functional requirements grades use a more narrow definition of system, which does not include people.
	System migration period	The amount of time taken between work planning to actual new system production operation when migrating from an existing system to a new system.
[T]	Threat	System attacks, triggers, operation mistakes, setting mistakes, etc., with the potential to create security risks.
	Throughput	The amount of work a system can process within a unit of time. Serves as a system processing capability index.
	Turnaround time	The amount of time between when a request is sent to a system, etc., and when results are received. (Related terminology) → Response
[U]	UL60950	Globally famous IT equipment related product safety standard. Standard established by the American independent safety standard development, testing, and certification organization, Underwriters Laboratories Inc. (UL).
	Uptime ratio	Ratio of time that the system actually provided services to the amount of time that it was supposed to provide services. Operating hour ratio. The amount of time during which the system was incapable of providing services is expressed as the average down time. Generally, uptime ratios are determined using the following formula. Uptime ratio = MTBF / (MTBF + MTTR) (Related terminology) → MTBF (Mean Time Between Failures) → MTTR (Mean Time To Repair / Mean Time To Recover)

	Terminology	Description
[V]	VCCI (Voluntary Control Council for Interference by Information Technology Equipment)	Abbreviated name of the Voluntary Control Council for Interference by Information Technology Equipment, a voluntary Japanese industry group which implements countermeasures against electromagnetic interference affecting radio receivers, television receivers, etc., caused by information technology devices such as personal computers, fax machines, etc. There are two voluntary regulations: VCCI Class A and Class B. The domestic environment oriented Class B is the more stringent of the two.
	Vulnerability	Possibilities and factors which must be considered even if security measures are implemented (possibility of attacks, operation errors, user carelessness, rule violations, etc.)
[W]	WAF (Web Application Firewall)	Firewall which detects and blocks data transmitted in attacks targeting Web servers and Web applications.
	Web site diagnostics	Security diagnostics of Web servers and Web applications performed for Web sites.

5. Appendix

5.1 Activities in Japan that are related to non-functional requirements

In addition to the non-functional requirements grades, there are other "non-functional requirement" related standards and guidelines. In order to indicate the differences between the non-functional requirements grades and other activities, and clarify the position of the non-functional requirements grades, the diagram below shows the relationship between the grades and other guidelines in terms of the processes in which their use is intended for.

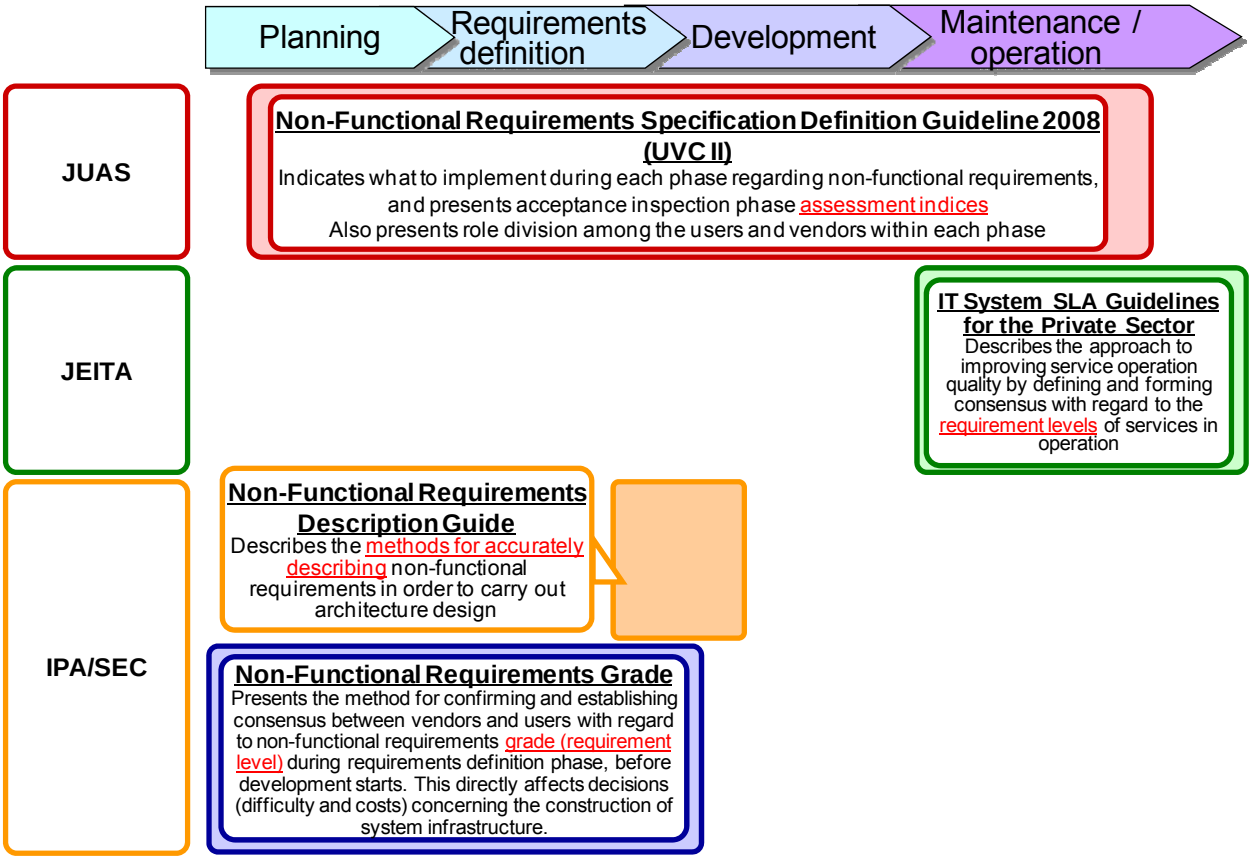


Figure 5.1.1 Intended processes and the various standardization activities

The primary objectives of the non-functional requirements grades are the confirmation and consensus formation between users and vendors of requirement items and requirement levels during the upstream process. The non-functional requirements grades were designed under the assumption that it would be used together with other guidelines with different objectives. The relationships between the grades and other guidelines are shown below.

5.1.1 Relationship with JUAS "Non-Functional Requirements Specification Definition Guideline 2008"

The "Non-Functional Requirements Specification Definition Guideline 2008" (hereafter referred to as "UVC II") was established by the Japan User Association of Information Systems (JUAS), and

organizes, from a system user perspective, the non-functional requirement items which must be validated by users during system acceptance inspection. Specifically, it indicates how to define requirements during each phase, from the upstream process to the downstream process, with a special focus on how to decide on requirement definition items which can be measured, and providing key points to be verified. It contains 10 categories of non-functional requirement items, covering a broad scope: functionality, reliability, usability, efficiency, maintainability, portability, failure prevention, effectiveness, operability, and technological requirements.

There are differences in the scopes of non-functional requirement items covered by the UVC II and the non-functional requirements grades. The non-functional requirements grades' scope extends to the non-functional requirements used in evaluating a system infrastructure, and the grades indicate requirement levels for each system infrastructure construction difficulty for each requirement item. Because of this, many of the items focused on by UVC II, such as functionality, usability, portability, which are not directly tied to system infrastructure evaluation, fall outside of the non-functional requirements grades' scope.

When using both of these, UVC II can be used to define system-wide non-functional requirements, from the upstream process to acceptance inspection. During the upstream process, it is more effective to use the "non-functional requirements grades" in order to confirm and form consensuses regarding specific non-functional requirements which should be met by the system infrastructure.

5.1.2 Relationship with JEITA "IT System SLA Guidelines for the Private Sector"

The objectives of the third edition of the "IT System SLA Guidelines for the Private Sector," established by the Japan Electronics and Information Technology Industries Association (JEITA), are the improvement of SLAs which serve as indices for evaluating the IT service quality provided by information systems, and the improvement of IT service operation levels making use of SLAs. The "SLA Application Scope Expansion Related Investigative Report," published in March, 2009, provides integrated indices which tie system development SLAs and development to operation.

The non-functional requirements grades primarily indicates requirement levels to serve as development phase evaluations, and is used at a different time than SLAs, which indicate service levels during operation. When using both, it is possible to tailor the timing of their use to different situations, such as when establishing development contracts and establishing operation contracts.

5.1.3 Relationship with IPA/SEC "Non-Functional Requirements Description Guide"

The "Non-Functional Requirements Description Guide," established in July, 2008 by the Information-Technology Promotion Agency, Japan / Software Engineering Center (IPA/SEC), defines descriptive tools, such as description item template generation, for efficiently, inclusively describing non-functional requirements thoroughly and accurately in order to perform system architecture design.

The non-functional requirements grades can be used by those defining non-functional requirements to confirm requirement levels during the planning and requirement definition phases, referring to the Non-Functional Requirements Description Guide to describe requirement definitions in more detail.

5.2 Relationship with other activities

Standards have been referred to during the establishment of the non-functional requirements grades, using their conceptual approach, quoting them, using their terminology, etc. The non-functional requirements grades were developed to be usable on its own for users and vendors to reach consensus regarding non-functional requirements, and must be considered in conjunction with other regulations, etc., in the event that there are other regulations, etc., with which the system must conform.

Below is an explanation of relationships with other standards.

5.2.1 Relationship with ISO/IEC 9126-1:2001

"ISO/IEC 9126-1:2001(JIS X0129-1: 2003)[5]" (hereafter referred to as "ISO/IEC 9126") is one of the leading non-functional requirements related standards. ISO/IEC 9126 is an international standard which defines software quality characteristics from both the positions of external and internal quality.

It cannot be compared across the board with the non-functional requirements grades, which extends to system infrastructures, but the terminology used in ISO/IEC 9126 was used in the non-functional requirements grades whenever possible. Table 5.2.1.1 shows which ISO/IEC 9126 items would correspond with which major categories of the non-functional requirements grades if the software quality characteristic defining ISO/IEC 9126 were considered as a standard defining system infrastructure quality characteristic.

As the table shows, there are some ISO/IEC 9126 quality sub-characteristics which do not correspond to major categories of the non-functional requirements grades. The reason for this is that, as the scope described in section 1.3 shows, the objective of the non-functional requirements grades is visualization of system infrastructure related user requirements, and as such it does not include many items which relate to the quality of applications realized mainly from software. For example, "Usability" is a quality of software-based applications, but not of system infrastructures.

[5] As of December, 2009, the ISO/IEC 25000 series which replaces ISO/IEC 9126, referred to as "SQuaRE (Software Product Quality Requirements and Evaluation)," is under active development. In addition to the overall ISO/IEC 25000:2005 guide, other standards, such as ISO/IEC 25030:2007 Quality Requirements, have also been published.

Table 5.2.1.1 Correspondences between ISO/IEC 9126 and the non-functional requirements grades

Characteristic	Definition	Quality sub-characteristic	Definition	Corresponding major category
Functionality	Ability of software to provide functions that match explicit or implicit needs when used under specified conditions	Suitability	Ability of software product to provide a set of functions appropriate for specified tasks and concrete user objectives	N/A
		Accuracy	Ability of software product to provide correct results or effects with the required level of precision, or the ability to provide acceptable results or effects	N/A
		Interoperability	Ability of software product to interact with one or more specified systems	N/A
		Security	Ability of software product to protect information or data in order to prevent unauthorized persons or systems from reading or modifying information or data, and to prevent authorized persons or systems from being denied access to information or data	Security
		Functionality Compliance	Ability of software product to conform to function related standards, conventions, or legal or similar regulations	Security, System environment and ecology
Reliability	Ability of software product to maintain a specified level of performance when used under specified conditions	Maturity	Ability of software product to avoid faults resulting from failures which potentially exists within the software	Availability
		Fault tolerance	Ability of software product to maintain a specified level of performance in the event that a faulty section of software is executed, or a specified interface condition infringement occurs	Availability
		Recoverability	Ability of software product to re-establish a specified level of performance in the event of a fault, and to restore directly affected data	Availability, operability and maintainability
		Reliability compliance	Ability of software product to conform to reliability related standards, conventions, or legal or similar regulations	System environment and ecology
Usability	Ability of software product to be understandable, learnable, operable, and attractive to users when used under specified conditions	Understandability	Attribute of software product wherein users are able to understand whether the software is appropriate for performing certain tasks under certain usage conditions, and how the software can be used to do so	N/A
		Learnability	Attribute of software product wherein users are able to learn how to utilize software	Operability and maintainability
		Operability	Attribute of software product wherein users are able to operate and manage operation of the software	Operability and maintainability
		Attractiveness	Attribute of software product which makes them attractive to users	N/A
		Usability compliance	Ability of software product to conform to usability related standards, conventions, style guides, or similar regulations	System environment and ecology
Efficiency	Ability of software product to provide appropriate performance in comparison to the resources it consumes under explicitly stated conditions	Time behavior	Ability of software product to provide appropriate response times, processing times, and processing capacity when executing software functions under explicitly stated conditions	Performance and scalability
		Resource utilization	Ability of software product to use appropriate amounts and types of resources when executing software functions under explicitly stated conditions	Performance and scalability
		Efficiency compliance	Ability of software product to conform to efficiency related standards or conventions	Performance and scalability, system environment and ecology
Maintainability	Ability of software product related to the ease of modification	Analyzability	Attribute of software product related to software fault diagnosis / identification of fault causes, and identification of software modification locations	Operability and maintainability
		Changeability	Attribute of software product related to ability to make specified modifications	N/A
		Stability	Attribute of software product related to ability to avoid unpredicted effects caused by software modification	N/A
		Testability	Attribute of software product related to ability to confirm validity of modified software	N/A
		Maintainability compliance	Ability of software product to conform to maintainability related standards or conventions	Operability and maintainability, system environment and ecology
Portability	Ability of software product related to transferring software from one environment to another	Adaptability	Attribute of software product related to the ability to adapt to a specified different environment without the need for additional operations or means other than those provided in advance	Migratability
		Installability	Attribute of software product related to their installation in specified environments	System environment and ecology
		Co-existence	Attribute of software product related to the ability to use them together with other independent software within shared environments with shared resources	Migratability
		Replaceability	Ability of software product to replace other specified software products within identical environments and for the same objectives	Migratability
		Portability compliance	Ability of software product to conform to portability related standards or conventions	System environment and ecology

5.2.2 Relationship with Japan Common Frame 2007

The Japan Common Frame 2007 provides a common framework to users and vendors for work related to system construction. It is a comprehensive stipulation, reflecting industry consensus, of the work items and roles involved in a system, from system conceptualization to disposal, independent of work processes, development models, development techniques, or development tools. It also includes software centered system related work, based on the software license process (SLCP-JCF2007) international standard, ISO/IEC 12207:2007(JIS X 0160), with unique Japanese enhancements and expansions, especially in the upstream process.

During the establishment of the non-functional requirements grades, the Japan Common Frame 2007 was regarded as an industry standard for system construction work and processes, and the items and role divisions specified therein were taken into consideration.

5.2.3 Relationship with the Information System Reliability Improvement Related Guideline

The Information System Reliability Improvement Related Guideline (Reliability Guideline) was made in response to the growing impact that information system failures have on society. The first edition was published by the Ministry of Economy, Trade, and Industry in 2006, and the second edition published in March, 2009. With this background, focus was especially placed on reliability and safety related non-functional requirements, with the objective of improving standards in those areas. The guideline indicates implementation items related to improved reliability for both users and vendors during development, operation, and fault occurrences, as well as key technical points and notes for each category.

The non-functional requirements grades use the system profile names provided by the Critical Infrastructure Information Systems Reliability Research Group which was one of the measures related to the Reliability Guideline, and redefine and present three model systems. The non-functional requirements grades themselves were considered in conjunction with the Ministry of Economy, Trade, and Industry as a "shared understanding support tool" for requirement definitions, one of the themes of the Ministry's reliability improvement initiatives, and is positioned as one of the other activities which are positioned around the Reliability Guideline.

5.2.4 Relationship with ISO/IEC 15408(Common Criteria)

ISO/IEC 15408:1999 is an international standard which defines information system and component equipment and software security evaluation standards. It is composed of three sections: ISO/IEC 15408-1:2005, ISO/IEC 15408-2:2008, and ISO/IEC 15408-3:2008. The non-functional requirements grades use the basic system security related concepts and terminologies used in ISO/IEC 15408.

ISO/IEC 15408 is an international standardization of the security evaluation standards, called the Common Criteria, developed by the CC Project, composed of 6 nations in Europe and North America. The ISO/IEC 15408 based "Japan Information Security Evaluation and Certification Scheme" is widely used across the globe (including Japan). Inside Japan, as well, ISO/IEC 15408

based evaluation and certification systems are used for system procurement, primarily by governmental organizations[6]. Below are some examples.

(1) Cases in which they are used for specific system component elements
In some cases, ISO/IEC 15408 based evaluation and certification are requirements for security products used in systems. This is especially common for system components with advanced security needs, such as IC cards, encryption products, and firewalls.
(2) Cases in which ISO/IEC 15408 based security design specifications are required
ISO/IEC 15408 defines security design specifications, called Security Targets (ST). When demanding advanced security from systems being developed, ISO/IEC 15408 based security design specification creation and third-party evaluation organization content validity evaluations are sometimes required.

System requirements such as these affect system development costs, so whether or not they are required must be confirmed in advance.

5.2.5 Relationship with ISO/IEC 27000 series

The ISO/IEC 27000 series is an international standard related to ISMS (Information Security Management Systems) which systematize measures which must be implemented by organizations in order to secure and maintain information security.

As of the end of December, 2009, ISO/IEC 27001:2005 (requirement items) and ISO/IEC 27002:2005 (guidelines for implementation) had been published[7]. In Japan, the "ISMS Conformity Assessment System" has been rolled out to assess and certify ISO/IEC 27001 compliance, and has been widely adopted by businesses and organizations.

ISMS establishes technological, physical, human resource, and organizational management measures, not only for systems but also for the organizations which operate them, and is implemented throughout an organization, extending all the way to the executive level. The non-functional requirements grades' scope extends to system requirement derivation, but ISO/IEC 27002 specifies concrete controls as best practices when deriving physical, human resource, and organizational security requirements for system users and operators, and as such may serve as a reference.

When deriving security requirements for systems in operation within ISMS certified organizations (or organizations planning on receiving ISMS certification), coordination must be performed for ISMS established technical management measures. These primarily correspond to the "Access / usage restrictions," "Fraud tracking / monitoring," and "Network measures" item list middle categories.

---

[6] Please refer to the "Guidebook for Procurement Using ISO/IEC 15408 (Ministry of Economy, Trade and Industry Commerce and Information Policy Bureau Office of Information Security Policy)."

[7] As of the end of December, 2009, the ISO/IEC 27000 series is in active development, with publications such as ISO/IEC 27005:2008 (information security risk management) and ISO/IEC 27006:2007 (requirements for bodies providing audit and certification) in addition to those listed above.

5.2.6 Relationship with Standards for Information Security Measures for the Central Government Computer Systems

The Standards for Information Security Measures for the Central Government Computer Systems (Uniform Governmental Standards) contain Japanese governmental organization (governmental ministry) information security measure standards. These standards must be observed when constructing systems for governmental organizations, and compliance of security requirement derived results with these Uniform Governmental Standards must be thoroughly confirmed.

The Uniform Governmental Standards divide security measures which should be implemented into "fundamental" (mandatory measures) and "enhanced" (voluntary measures) categories, and do not mandate that all security measures be implemented. As such, when using the non-functional requirements grades in creating systems for governmental organization use, Uniform Governmental Standards mandatory security measures must be implemented, and the non-functional requirements grades may be used as a reference when deriving non-mandatory security measure requirements.

The information security measures defined in the Uniform Governmental Standards take a wide view of security, and include measures related to "availability" of systems in the event of system disasters or failures, and "operability and maintainability" for maintaining the system. Conformity with Uniform Governmental Standards must be confirmed sufficiently when considering "availability" and "operability and maintainability" requirements as well.

5.2.7 Relationship with Computer System Safety Measure Standards for Banking and Related Financial Institutions

The Computer System Safety Measure Standards for Banking and Related Financial Institutions (FISC Safety Measure Standards) are security measure standards for banking and related financial institutions in Japan, established by The Center for Financial Industry Information Systems. Normally, conformance with FISC Safety Measure Standards is a procurement requirement when constructing a financial institution system, so when deriving security requirements, one must thoroughly confirm that the results conform with the FISC Safety Measure Standards.

As with the Uniform Governmental Standards, the FISC Safety Measure Standards divides security measures which should be implemented into two categories: mandatory items and voluntary items. When using the non-functional requirements grades in a financial institution system, the FISC Safety Measure Standards can be followed for security measures mandated by them, and the non-functional requirements grades used as a reference when deriving requirements for non-mandatory security measures.

Due to the nature of financial systems, the measures stipulated by the FISC Safety Measure Standards include many items related to "availability" in the face of system disasters or failures, and to operation facility, etc. "system environment and ecology." As such, when considering "availability" and "system environment and ecology" requirements, one must thoroughly confirm conformance with FISC Safety Measure Standards.

5.2.8 Relationship with the Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is an international security standard defined by the credit industry, and applies to security used to protect credit card information handled by credit card member stores and payment processors.

PCI DSS compliance is required for systems handling credit card information, such as the credit card systems of credit card member stores, so when deriving related system security requirements, one must thoroughly confirm that the results conform to PCI DSS.

When using the non-functional requirements grades on a system to which PCI DSS applies, the PCI DSS can be followed for requirements mandated by it, and the non-functional requirements grades used as a reference when deriving requirements for items not explicitly required by the PCI DSS.

5.3 Reference materials

The materials [1] to [11], [19] and [20] are in Japanese only.

[1] Information-Technology Promotion Agency, Japan / Software Engineering Center (IPA/SEC) "Japan Common Frame 2007 - Management and Business Division Participation in System Development and Transactions," Ohmsha, October 1, 2007

[2] Information-Technology Promotion Agency, Japan / Software Engineering Center (IPA/SEC) "Management Participation in Securing of Requirement Quality - Critical Points for IT Implementation from the Ultra-Upstream Stage - Second Edition," Ohmsha, May 25, 2006

[3] Ministry of Economy, Trade and Industry Software Development Strengthening and Promotion Task Force Requirement Engineering and Design Development Technology Research Group Non-Functional Requirement and Architecture WG, "Non-Functional Requirement Description Guide," *http://sec.ipa.go.jp/reports/20080717/NFRdescription__guideline.pdf*, July 2008

[4] Japan User Association of Information Systems (JUAS) "Non-Functional Requirement Specification Definition Guideline 2008," July 2008

[5] Japan Electronics and Information Technology Industries Association (JEITA) Solution Service Business Committee,
"IT System SLA Guidelines for the Private Sector - Third Edition," Nikkei Business Publications, October 2, 2006

[6] Japan Electronics and Information Technology Industries Association (JEITA) Solution Service Business Committee,
"SLA Application Scope Expansion Related Investigative Report," Japan Electronics and Information Technology Industries Association,
March 2009

[7] Ministry of Economy, Trade and Industry, "Information System Reliability Improvement Related Guideline,"
http://www.meti.go.jp/press/20060615002/20060615002.html, June 15, 2006

[8] Ministry of Economy, Trade and Industry, "Information System Reliability Improvement Related Guideline - Second Edition,"
http://www.meti.go.jp/press/20090324004/20090324004-4.pdf, March 24, 2009

[9] Ministry of Economy, Trade and Industry Commerce and Information Policy Bureau Office of Information Security Policy,
"Guidebook for Procurement Using ISO/IEC 15408,"
http://www.meti.go.jp/policy/netsecurity/downloadfiles/CCguide__ver2__0.pdf,
August 11, 2004

[10] National Information Security Center (NISC), "Standards for Information Security Measures for the Central Government Computer Systems,"
http://www.nisc.go.jp/active/general/kijun01.html,
February 3, 2009

[11] The Center for Financial Industry Information Systems (FISC), "Computer System Safety

Measure Standards for Banking and Related Financial Institutions - Description Manual (7th Edition)," The Center for Financial Industry Information Systems (FISC), March 2006

[12] ISO/IEC 9126-1:2001(Software engineering -- Product quality -- Part 1: Quality model), 2001

[13] ISO/IEC 15408-1:2005(Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model), 2005

[14] ISO/IEC 15408-2:2005(Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements), 2005

[15] ISO/IEC 15408-3:2005(Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements), 2005

[16] ISO/IEC 27001:2005(Information security management systems - Requirements), 2005

[17] ISO/IEC 27002:2005(Code of practice for information security management), 2005

[18] PCI Security Standards Council, "Payment Card Industry(PCI) Data Security Standard - Requirements and Security Assessment Procedures Version 1.2," *https://www.pcisecuritystandards.org/security__standards/pci__dss.shtml*, October 2008

[19] Information-Technology Promotion Agency, Japan / Software Engineering Center (IPA/SEC), Critical Infrastructure Information Systems Reliability Research Group Report, *http://sec.ipa.go.jp/reports/20090409.html*, April 2009

[20] Ministry of Economy, Trade and Industry, Non-Functional Requirements grades "User View Deliberation Committee" Report, *http://www.meti.go.jp/policy/it__policy/softseibi/hikinou__grade.pdf*, June 2009