System Infrastructure Non-Functional Requirements Related Grade Table

April 2013

Information-Technology Promotion Agency, Japan
Software Engineering Center

[Usage conditions]

1. The copyright to this document is held by the Information-Technology Promotion Agency, Japan.

2. This document is protected by the Copyright Act of Japan and other international copyright protection conventions and treaties. Except for the exceptions listed in item 3, modification, public transmission, sale, publishing, translation, and adaptation of this document, in whole or in part, without the explicitly written permission of the Information-Technology Promotion Agency, Japan, is strictly prohibited, regardless of whether or not said actions are performed for purposes of profit.

3. The Information-Technology Promotion Agency, Japan grants users of this document to perform the two, and only two, actions mentioned below ((1) and (2)), provided that the following copyright notice is clearly indicated.
   Copyright notice: Copyright © 2010 IPA
   (1) Duplication of this document, in whole or in part.
   (2) Free redistribution of duplications of this document on the condition that the parties to which the duplication is redistributed are put under the same obligations as described on this page.

4. The Information-Technology Promotion Agency, Japan makes no guarantees of this document containing no infringements of the copyrights, patent rights, or other intellectual property rights, such as utility model rights, of third parties, nor does it assume any responsibility for possible errors contained herein. The Information-Technology Promotion Agency, Japan makes no guarantees that the content of this document will conform to the legal requirements for export, technology transfer, and other national laws and regulations of any country or region.

5. Other than the exceptions specified on this page, the Information-Technology Promotion Agency, Japan does not grant any rights nor any license relating to copyrights, patent rights, or other intellectual property rights, such as utility model rights, of the Information-Technology Promotion Agency, Japan or of third parties.

6. The Information-Technology Promotion Agency, Japan shall not be held in any way responsible for damages which may result from using this document in system development, the use of the developed systems, or the inability to use said systems.

7. Please contact the Information-Technology Promotion Agency, Japan's Software Engineering Center with inquiries regarding this document.

• Model system sheet explanatory notes

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 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.
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.

(a) (b) (c) (d)

(a) No. : Sequential property number

(b) Major category : Property category. Same as non-functional requirements grade major category.

(c) Property : Properties of the non-functional requirements envisioned for each model system. Model system names alone are insufficient for a clear understanding of non-functional requirement levels, so the properties of each model system are identified.

(d) Model systems : Representative non-functional requirement model for use as reference for system being developed. Three names have been cited from the system profiling performed by the Critical Infrastructure Information Systems Reliability Research Group and published by the Information-technology Promotion Agency, Japan, and the properties of each have been defined.
(Please see http: //sec.ipa.go.jp/reports/20090409.html (in Japanese) for details on the release of the report by the Critical Infrastructure Information Systems Reliability Research Group.)

• Grade table explanatory notes

No.	Major Category	Middle Category	Minor Category	Minor Category Description	Overlapping Item	Metric	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Impact on Operation Costs	Notes	System with almost no social impact: Selected level	System with almost no social impact: Selection conditions	System with limited social impact: Selected level	System with limited social impact: Selection conditions	System with very significant social impact: Selected level	System with very significant social impact: Selection conditions
A.1.1.1	Availability	Continuity	Operation schedule	Information regarding system operating hours and operation outage.	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 (9:00 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.	2	Outage only at night (9:00 to 21:00) No businesses are done during nightime 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.
A.1.1.2					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 (9:00 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.	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.
A.1.1.3					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.	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.

Item definition (a) (b) (a) (b) (a) (b)

The information to the left of the grade table model system descriptions is, with the exception of the presence / absence of the important item column, the same as the item list, and as such the item list explanatory notes should be referred to.

(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.

(b) Selection conditions : Base value selection conditions. Assuming cases where base values alone are not sufficient to appropriately indicate the non-functional requirements of the system being developed, conditions under which base values are changed are indicated with [-] and [+]. When you wish to lower the non-functional requirement level of the system, check the conditions that correspond to the [-] and adjust the level. Conversely, when you wish to raise the non-functional requirement level of the system, check the conditions that correspond to the [+] and adjust the level.

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 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.
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.

Note: The names of the "model systems" are cited from the system profiling performed by the Critical Infrastructure Information Systems Reliability Research Group and published by the Information-technology Promotion Agency, Japan.
Please refer to the URL http://sec.ipa.go.jp/reports/20090409.html (in Japanese) for details on the release of the report by the Critical Infrastructure Information Systems Reliability Research Group.
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 grades, "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".

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
A.1.1.1	Availability	Continuity	Operation schedule	Information regarding system operating hours and operation outage.	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 (9:00 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.	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.
A.1.1.2					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 (9:00 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.	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.
A.1.1.3					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.	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.
A.1.2.1			Business continuity	Business scope and conditions required to ensure availability		Affected business scope	Internal batch related businesses	Internal online businesses	All internal businesses	External batch related businesses	External online businesses	All businesses		[Metric] The "affected business scope" here refers to the scope which is used for uptime ratio calculation. [Level] "Internal" refers to closed (business) processing within the system. "External" refers to (business) processing which requires coordination with other systems.	2	All internal businesses	The primary businesses handled by the system are internal businesses, and one of the system operation conditions is that all internal businesses are operational. [+] There are also externally provided businesses, which are considered essential.	3	External batch related businesses	The primary businesses handled by the system are external batch processing businesses, and one of the system operation conditions is that all internal businesses and external batch processing businesses are operational. [-] There are no externally provided businesses. [+] Real-time processing with external entities is required for business continuity.	4	External online businesses	The primary businesses handled by the system are real-time processing with external entities, and one of the conditions of system operation is that external online businesses are operational. [-] Real-time processing with external entities is not required for business continuity.
A.1.2.2						Service switchover time	24 hours or longer	Less than 24 hours	Less than 2 hours	Less than 60 minutes	Less than 10 minutes	Less than 60 seconds	X	[Metric] "Service switchover time" refers to the amount of time necessary for a system which has suffered a possible failure (such as temporary business interruption due to hardware failures, etc.) to resume business by taking response measures (for example, performing server switchover in a clustered system). [Impact on Operation Costs] The longer the permitted interruption time, the ratio of manual response as recovery measures will be greater than automatic system response measure implementation, impacting operation costs.	1	Less than 24 hours	There is no business provided to external entities, and a down time of approximately 1 day is acceptable. [-] Failure countermeasures are not necessary. [+] Service switchover has an impact. (Consider the amount of time that interruption is acceptable based on the impact.)	3	Less than 60 minutes	There are online businesses with external entities, but interruptions of several dozen minutes are acceptable. [+] Service switchover has an impact on the online businesses. (Consider the amount of time that interruption is acceptable based on the impact.)	5	Less than 60 seconds	The system must provide real-time response, so instant recovery from system outages is required. [-] Business interruption of up to 1 hour is acceptable.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
A.1.2.3						Required level of business continuity	Business interruption is accepted when a system failure occurs	Business interruption is not accepted when a single failure occurs; processing is continued	Business is continued within service switchover time restrictions even in the event of double failures					[Metric] The "required level of business continuity" is the criteria indicating the extent to which business must be continued in the event of a failure. The equipment and components that make up systems have many single points of failure (SPOF), resulting in many risks of system outage. This requirement based on whether these SPOF are tolerated, or the extent to which continuity is ensured through redundancy measures, etc.	1	Business interruption is not accepted when a single failure occurs; processing is continued	Matched to the acceptable business interruption time when a system failure occurs. [-] With the risks in mind, business outage due to failure occurrence is acceptable. [+] Business outages due to double failures must be prevented, even if resulting in increased cost.	2	Business is continued within service switchover time restrictions even in the event of double failures	Matched to the acceptable business interruption time when a system failure occurs. [-] With the risks in mind, business outage due to double failure is acceptable.	2	Business is continued within service switchover time restrictions even in the event of double failures	Continuation of business is presumed even in the event of a double failure.
A.1.3.1			Recovery objective (When business outage occurs)	Objectives for what should be recovered, to which point, within how much time when a failure results in business outage.		Recovery point objective (RPO)	Recovery not necessary	Up until 5 business days prior to outage (Recovery from weekly backup)	Up until 1 business day prior to outage (Recovery from daily backup)	Up until the point at which failure occurred (Recovery from daily backup + archive)				[Metric] When an RLO specifies business recovery, applicable business data recovery is included in the scope, and business resumption consistency confirmation will be required separately. [Level 3] The "point at which failure occurred" refers to the point immediately after the last transaction which was processed just before the failure. Recovery to the point at which the failure occurred assumes that the transaction journal up to the point of failure is guaranteed. It also assumes that journals are archived, making it possible to restore the system to any desired point up to the point at which the failure occurred.	1	Up until 5 business days prior to outage (Recovery from weekly backup)	Some degree of data loss is acceptable, and restoration shall be performed from weekly backups. [-] Data is not retained, and recovery is not necessary. [+] The effect of data loss is excessive unless restoration from daily backups is performed.	3	Up until the point at which failure occurred (Recovery from daily backup + archive)	Since data loss is not acceptable, the system, in principle, must be recovered to the point at which the failure occurred. [-] Some degree of data loss is acceptable. (Level shall be selected based on data (daily, weekly) to be recovered.)	3	Up until the point at which failure occurred (Recovery from daily backup + archive)	Since data loss is not acceptable, the system, in principle, must be recovered to the point at which the failure occurred.
A.1.3.2						Recovery time objective (RTO)	1 business day or more	Within 1 business day	Within 12 hours	Within 6 hours	Within 2 hours			[Metric] The RTO recovery time differs from the recovery time of the service switchover time (A.1.2.2), indicating the duration time to recover when business continuity measures are not implemented (resulting in a business outage). When an RLO specifies business recovery, applicable business data recovery is included in the scope, and business resumption consistency confirmation will be required separately.	1	Within 1 business day	Determine based on system scale, taking the recovery point objective into consideration. [-] The impact of business outage is small. [+] The impact of business outage is large.	2	Within 12 hours	Determine based on system scale, taking the recovery point objective into consideration. [-] The impact of business outage is small. [+] The impact of business outage is large.	4	Within 2 hours	Recover as soon as possible.
A.1.3.3						Recovery level objective (RLO)	System recovery	Specific businesses only	All businesses					[Metric] This level indicates what should be recovered when a failure results in business outage. [Level 0] System recovery includes not only hardware recovery, but data restoration as well. [Level 1] "Specific businesses" refers to, for example, business whose continuity is required as specified in A.1.2.1 "Affected business scope."	1	Specific businesses only	Only primary businesses require recovery. [+] When impact cannot be separated from individual businesses	2	All businesses	There will be an impact unless all businesses are functional. [-] Impact can be separated from some businesses.	2	All businesses	There will be an impact unless all businesses are functional. [-] Impact can be separated from some businesses.
A.1.4.1			Recovery objective (In event of large-scale disaster)	This metric is the target recovery time in the event of a large-scale disaster. Large-scale disasters refer to damage caused by fires and natural hazards such as earthquakes, as well as man-made damage that are accidental or intentional, which cause extensive damage to the system, or make it difficult to recover the system because lifelines such as power are interrupted.		System resumption objective	Resumption not necessary	Resumption within several months	Resumption within 1 month	Resumption within 1 week	Resumption within 3 days	Resumption within 1 day		[Metric] For large-scale disasters, specific requirements such as RPO, RTO, and RLO are not defined; instead, a general resumption time is set as a system resumption objective. Regarding the recovery level objective (RLO), refer to "Recovery objective (When business outage occurs)".	1	Resumption within several months	Some degree of data loss is acceptable, and restoration shall be performed from weekly backups. [-] Data is not retained, and recovery is not necessary. [+] The impact of business outage is large.	3	Resumption within 1 week	In the event of large-scale disasters, resume business by recovery from retained data. [-] Procurement of replacement equipment and preparation of recovery organization takes time. [+] Impact of business outage is large, and prompt recovery using DR sites is necessary.	4	Resumption within 3 days	Taking restoration of lifelines into consideration, make efforts of system recovery to the maximum extent possible. [+] There are safety requirements, such as possible loss of life or extreme financial losses.
A.1.5.1			Uptime ratio	Percentage of time that the system can provide the requested service under specified usage conditions. "Specified usage conditions" refers to the system's operation schedule and conditions under which business defined by the recovery objective are carried out. The uptime ratio is determined from the amount of time service is interrupted during the operating hours.		Uptime ratio	Less than 95%	95%	99%	99.9%	99.99%	99.999%		[Level] For 24/365 operation, annual business outage totals are shown below for each level. 95% ..... 18.3 days 99% ..... 87.6 hours 99.9% ..... 8.76 hours 99.99% ..... 52.6 minutes 99.999% ..... 5.26 minutes For a system which operates 8 hours a day, 5 days a week, the relationship between service switchover time and uptime ratio is as shown below. 1 hour per week ..... 97.5% 1 hour per month ..... 99.4% 1 hour per year 99.95%	2	99%	Downtime of several hours per year is acceptable. Use the operating hours for the uptime ratio examples in the Notes column as a reference when determining the uptime ratio.	4	99.99%	Downtime of approximately 1 hour per year is acceptable.	5	99.999%	Downtime of only several minutes per year is acceptable.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
A.4.2.1		Recoverability	Availability confirmation	Scope of confirmation of availability requirements.		Confirmation scope	Not performed, or up to simple failures	Failures which permit business to be continued	Some failures which result in business interruption	All failures which result in business interruption				[Level] Level 2 and 3 confirmation scopes include contents defined in level 1.	1	Failures which permit business to be continued	Even when failures which cause business outage occur, recovery methods are clear, and there is no need for confirmation. [-] Failure countermeasures are not considered. [+] When failures which cause business outage occur, restoration methods must be confirmed in advance	2	Some failures which result in business interruption	Countermeasures for failures which cause business outage must be confirmed, but it is possible to limit confirmation for high risk failures and specific types of failures. [-] It can be judged that the impact of failures which cause business outages is extremely small. [+] Confirmation is needed to the maximum extent possible, without consideration to failure types or risks.	3	All failures which result in business interruption	The impact of business outage is extremely large, and confirmation is required in advance for all possible failures. [-] The impact to the system can be limited based on failure types and risks.
B.1.1.1	Performance and scalability	Business processing volume	Business volume during normal operation	Volume of business which have an effect on performance and scalability. Consensus is to be based on envisioned system operation. Instead of selecting a single value for each metric, intended system operation hours, seasonal factors, and the like must also be considered.	X	Number of users	Specific users only	Upper limit is fixed	Used by unspecified number of users					[Overlapping Item] F.2.1.1. The "number of users" is essential for deciding performance and scalability, as well as an item for specifying the system environment, so this item is included in both "Performance and scalability" and "System environment and ecology". [Level] Even if the numerical value for this prerequisite cannot be precisely determined, it is important that at least a tentative value, based on similar systems, etc., should be decided on.	0	Specific users only	This assumes cases where users can be identified since the use is within a department or an organization. [+] When users cannot be identified	1	Upper limit is fixed	This assumes cases where an upper limit is specified. [-] Consensus has been reached that only specific users will use the system.	2	Used by unspecified number of users	This assumes cases where the general public will access the system. [-] It is possible to specify an upper limit.
B.1.1.2						Number of simultaneous users	Access limited to specified users only	Limited number of simultaneous users	Access by unspecified number of users					[Metric] The "number of simultaneous users" refers to the number of users who access the system at any given point.	0	Access limited to specified users only	Assume based on registered users.	1	Limited number of simultaneous users	Confirm what kind of peak model is envisioned for the system.	2	Access by unspecified number of users	Confirm what kind of peak model is envisioned for the system.
B.1.1.3						Data volume	Total data volume is clear	Only primary data volume is clear						[Level 1] "Primary data volume" refers to the data that makes up the majority of the data stored by the system. For example, master tables and temporary storage of main transaction data. When only the volume of primary data has been determined, there is a risk of a need to add disks to handle data which has not been considered.	0	Total data volume is clear	Must be clarified when establishing requirements definitions. [+] The total data volume has not been assessed.	0	Total data volume is clear	Must be clarified when establishing requirements definitions. [+] The total data volume has not been assessed.	0	Total data volume is clear	Must be clarified when establishing requirements definitions. [+] The total data volume has not been assessed.
B.1.1.4						Number of online requests	Number of requests is clear for each process	Number of requests is clear for primary processes only						[Metric] The number of online requests is confirmed, clearly specifying the unit time involved. [Level 1] "Primary processes" refer to the online requests received by the system that make up the majority of received requests. For example, resident information system move-in / move-out processing, Internet shopping system transaction processing, etc. When only the number of requests for primary processes has been determined, there is a risk of insufficient server capabilities due to processes which have not been considered.	0	Number of requests is clear for each process	Must be clarified when establishing requirements definitions. [+] The total number of online requests has not been assessed.	0	Number of requests is clear for each process	Must be clarified when establishing requirements definitions. [+] The total number of online requests has not been assessed.	0	Number of requests is clear for each process	Must be clarified when establishing requirements definitions. [+] The total number of online requests has not been assessed.
B.1.1.5						Number of batch processes	Number of processes is defined for individual processing units	Number of processes is defined for primary processes						[Metric] The number of batch processes shall be confirmed, clearly specifying the unit time involved. When defining requirements, an estimated number of primary processes (especially processes critical for the server) should have been decided on, and performance and scalability shall be considered based on this estimate. If this number has not been clearly specified when defining requirements, assumed values, including the degree to which they are decided, should be used. [Level 1] "Primary processes" refer to the batch processes which take up the majority of the system's processing time. For example, monthly aggregation processing of a personnel payroll processing system or billing system. When only the number of primary batch processes has been determined, there is a risk of insufficient server capabilities due to processes which have not been considered.	0	Number of processes is defined for individual processing units	Must be clarified when establishing requirements definitions. [+] The total number of batch processes has not been assessed.	0	Number of processes is defined for individual processing units	Must be clarified when establishing requirements definitions. [+] The total number of batch processes has not been assessed.	0	Number of processes is defined for individual processing units	Must be clarified when establishing requirements definitions. [+] The total number of batch processes has not been assessed.
B.1.2.1			siness volume expansion	Ratio, over the course of the system's lifecycle, from system operation inception to retirement, between the volume of business at the system's launch and its peak. Comparisons between start date average values and later steady state figures can also be used as needed.		Expansion rate of number of users	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.	0	1-fold	Confirm the user registration / deletion cycles, etc. Also, confirm future outlook. [+] The number of users is expected to increase.	1	1.2-fold	Confirm the user registration / deletion cycles, etc. Also, confirm future outlook. [-] The number of users is fixed. [+] The number of users is expected to increase.	1	1.2-fold	Confirm the user registration / deletion cycles, etc. Also, confirm future outlook. [-] The number of users is fixed. [+] The number of users is expected to increase.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact		System with limited social impact		System with very significant social impact	
							0	1	2	3	4	5			Selected level	Selection conditions	Selected level	Selection conditions	Selected level	Selection conditions
B.1.2.2			Bu			Expansion rate of number of simultaneous users	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.	0 1-fold	Confirm how it is believed the system peak model will change due to an increase in the number of users. [+] The number of users is expected to increase.	1 1.2-fold	Confirm how it is believed the system peak model will change due to an increase in the number of users. [-] The number of users is fixed, or an increase in the number of users is not linked with an increase in the number of accessing users. [+] The number of users is expected to increase.	1 1.2-fold	Confirm how it is believed the system peak model will change due to an increase in the number of users. [-] The number of users is fixed, or an increase in the number of users is not linked with an increase in the number of accessing users. [+] The number of users is expected to increase.
B.1.2.3						Expansion rate of data volume	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.	0 1-fold	Confirm how much the volume of data handled by the system will increase in accordance with business trends. [+] Phased operation and master data storage systems	1 1.2-fold	Confirm how much the volume of data handled by the system will increase in accordance with business trends. [-] Gateway systems which do not store data [+] Phased operation and master data storage systems	1 1.2-fold	Confirm how much the volume of data handled by the system will increase in accordance with business trends. [-] Gateway systems which do not store data [+] Phased operation and master data storage systems
B.1.2.4						Expansion rate of number of online requests	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Metric] The number of online requests shall be confirmed, clearly specifying the unit time involved. [Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.	0 1-fold	Confirm the estimated number of requests that will be the system limit.	1 1.2-fold	Confirm the estimated number of requests that will be the system limit.	1 1.2-fold	Confirm the estimated number of requests that will be the system limit.
B.1.2.5						Expansion rate of number of batch processes	1-fold	1.2-fold	1.5-fold	2-fold	3-fold	10-fold or greater		[Metric] The number of batch processes shall be confirmed, clearly specifying the unit time involved. [Level] The multiplication factor shown for each level is a rough estimate; consensus regarding specific figures is necessary.	0 1-fold	Confirm the number of processes that will be the system limit.	1 1.2-fold	Confirm the number of processes that will be the system limit.	1 1.2-fold	Confirm the number of processes that will be the system limit.
B.1.3.1			Retention period	Period for which data used by the system infrastructure, such as OS or middleware logs, must be retained. Can be specified, as needed, for individual data types. When selecting data to be retained, the scope of the target data must also be defined.		Retention period	6 months	1 year	3 years	5 years	10 years or longer	Permanent retention		[Level] When there is multiple data that must be retained, and the retention periods vary, decision must be made for each type of data involved. [Level 0] Use 6 months when data retention period restrictions are short.	1 1 year	Assumes yearly update of data. [-] There is almost no archived data. [+] There is sufficient disk capacity.	3 5 years	Assumes a retention period defined by taxation systems, etc. [-] The period required for lookups is limited, and data can be transferred to backup media. [+] There is sufficient disk capacity.	4 10 years or longer	Assumes a retention period defined by external requirements etc. guaranteed to end users. [-] The period required for lookups is limited, and data can be transferred to backup media. [+] There is sufficient disk capacity.
B.2.1.1		Performance objective	Online response	Response required during online system utilization. Confirm what level of response is necessary based on the business to be handled by the system. Take into account of peak characteristics and operation during failure, and establish adherence rates for normal operation, peak times, and degraded operation. It is advisable to decide on specific numbers for specific functions and systems. (Ex: Web system search/update/viewing related, etc.)		Adherence rate of response during normal operation	No defined adherence rate	60%	80%	90%	95%	99% or greater		[Level] When there are specific targets and promised values, specify adherence rates for each process. The adherence rate shown for each level is a rough estimate; consensus must be reached regarding concrete response and adherence rate figures.	0 No defined adherence rate	The transaction volume is low. Alternatively, if it is high, it is possible to apply usage restrictions on users. [+] Performance drops result in system evaluation degradation.	3 0.9	Within the managed processes, it is acceptable if 90% of transactions during normal operation achieve the established target. [-] As long as processing is completed, it is acceptable even if is slow. Or there are alternative methods. [+] Performance drops result in system evaluation degradation.	5 99% or greater	Within the managed processes, it is acceptable if 99% of transactions during normal operation achieve the established target. [-] As long as processing is completed, it is acceptable even if is slow. Or there are alternative methods.
B.2.1.2						Adherence rate of response during peak times	No defined adherence rate	60%	80%	90%	95%	99% or greater		[Level] When there are specific targets and promised values, specify adherence rates for each process. The adherence rate shown for each level is a rough estimate; consensus must be reached regarding concrete response and adherence rate figures.	0 No defined adherence rate	The transaction volume is low. Alternatively, if it is high, it is possible to apply usage restrictions on users. [+] Performance drops result in system evaluation degradation.	2 0.8	Within the managed processes, it is acceptable if 80% of transactions during peak operation achieve the established target. [-] As long as processing is completed, it is acceptable even if is slow. Or there are alternative methods. [+] Performance drops result in system evaluation degradation.	4 0.95	Within the managed processes, it is acceptable if 95% of transactions during peak operation achieve the established target. [-] As long as processing is completed, it is acceptable even if is slow. Or there are alternative methods. [+] Performance drops result in system evaluation degradation.
B.2.2.1			Batch response (turnaround time)	Response required during batch system utilization. Confirm what level of response (turnaround time) is necessary based on the business to be handled by the system. It is advisable to take into account peak characteristics and operation during failure, decide on adherence rates for normal operation, peak times, and degraded operation, and establish specific figures for individual functions and systems.		Degree of response adherence during normal operation	No defined degree of adherence	Within specified time	Sufficient capacity is reserved to perform re-execution					[Level 1] The "specified time" does not include re-execution.	0 No defined degree of adherence	There is a comparatively small amount of data, so there are no rules related to batch response order.	2 Sufficient capacity is reserved to perform re-execution	Within the managed processes, it is acceptable if batch processes during normal operation are executed, and, if invalid results are produced, there is sufficient capacity for re-execution. [-] Re-execution is not performed, or there are alternative methods.	2 Sufficient capacity is reserved to perform re-execution	Within the managed processes, it is acceptable if batch processes during normal operation are executed, and, if invalid results are produced, there is sufficient capacity for re-execution. [-] Re-execution is not performed, or there are alternative methods.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
B.2.2.2				(Ex: Daily processes / monthly processes / yearly processes, etc.)		Degree of response adherence during peak times	No defined degree of adherence	Within specified time	Sufficient capacity is reserved to perform re-execution					[Level 1] The "specified time" does not include re-execution.	0	No defined degree of adherence	There is a comparatively small amount of data, so there are no rules related to batch response order.	2	Sufficient capacity is reserved to perform re-execution	Within the managed processes, it is acceptable if batch processes during peak operation are executed, and, if invalid results are produced, there is sufficient capacity for re-execution. If there is no sufficient capacity at peak times, deployment of additional servers, or division of processing must be considered. [-] Re-execution is not performed, or there are alternative methods.	2	Sufficient capacity is reserved to perform re-execution	Within the managed processes, it is acceptable if batch processes during peak operation are executed, and, if invalid results are produced, there is sufficient capacity for re-execution. If there is no sufficient capacity at peak times, deployment of additional servers, or division of processing must be considered. [-] Re-execution is not performed, or there are alternative methods.
B.3.1.1		Resource scalability	CPU scalability	This item is used to confirm CPU scalability. It is based on CPU utilization and the number of open CPU slots when system operation starts. The lower the CPU utilization, the greater its scalability, but also the greater the CPU cost, and resulting waste. CPU addition capacity indicates scalability capacity by checking the presence and quantity of open slots.		CPU utilization	80% or greater	Between 50% and 80%	Between 20% and 50%	Less than 20%			X	[Metric] The "CPU utilization" indicates the ratio of CPU usage by running programs per unit time. Figures may vary greatly depending on what unit time is used, and the characteristics of the operating programs. [Level] The utilization ratio shown for each level is a rough estimate; consensus regarding specific figures is necessary. [Impact on Operation Costs] If the CPU utilization is high, measures such as deployment of additional equipment will be necessary for even minor increases of business volume.	0	80% or greater	This assumes that the system does not involve excessive facility deployment. [+] There are plans for an increase in the number of users in the near future.	1	Between 50% and 80%	This assumes that additional capacity has been prepared in order to accommodate increase in business volume. [-] Low cost has a higher priority over performance and scalability. [+] There are plans for an increase in the number of users in the near future.	1	Between 50% and 80%	This assumes that additional capacity has been prepared in order to accommodate increase in business volume. [-] Low cost has a higher priority over performance and scalability. [+] There are plans for an increase in the number of users in the near future.
B.3.1.2						CPU addition capacity	No addition capacity	1 open slot	2 open slots	3 open slots	4 or more open slots		X	[Level] Equipment with CPU addition capacity costs more than equipment with none. [Impact on Operation Costs] For equipment with no CPU addition capacity, additional equipment installation may become necessary.	0	No addition capacity	Usage is limited to within a department, and CPU scalability is not required.	1	1 open slot	This assumes that the system is capable of accommodating additional CPU installation for system expansion in the next 2 to 3 years.	1	1 open slot	This assumes that the system is capable of accommodating additional CPU installation for system expansion in the next 2 to 3 years.
B.3.2.1			Memory scalability	This item is used to confirm memory scalability. It is based on memory utilization and the number of open memory slots when system operation starts. The lower the memory utilization, the greater its scalability, but also the greater the memory cost, and resulting waste. Memory addition capacity indicates scalability capacity by checking the presence and quantity of open slots.		Memory utilization	80% or greater	Between 50% and 80%	Between 20% and 50%	Less than 20%			X	[Metric] "Memory utilization" indicates the ratio of memory usage by running programs per unit time. Figures may vary greatly depending on what unit time is used, and the characteristics of the operating programs. [Level] The utilization ratio shown for each level is a rough estimate; consensus regarding specific figures is necessary. [Impact on Operation Costs] If the memory utilization is high, measures such as deployment of additional equipment will be necessary for even minor increases in business volume.	0	80% or greater	This assumes that the system does not involve excessive facility deployment. [+] There are plans for an increase in the number of users in the near future.	1	Between 50% and 80%	This assumes that additional capacity has been prepared in order to accommodate increase in business volume. [-] Low cost has a higher priority over performance and scalability. [+] There are plans for an increase in the number of users in the near future.	1	Between 50% and 80%	This assumes that additional capacity has been prepared in order to accommodate increase in business volume. [-] Low cost has a higher priority over performance and scalability. [+] There are plans for an increase in the number of users in the near future.
B.3.2.2						Memory addition capacity	No addition capacity	1 open slot	2 open slots	3 open slots	4 or more open slots		X	[Level] Equipment with memory addition capacity costs more than equipment with none. [Impact on Operation Costs] For equipment with no memory addition capacity, additional equipment installation may become necessary.	0	No addition capacity	Usage is limited to within a department, and memory scalability is not required.	1	1 open slot	This assumes that the system is capable of accommodating additional memory installation for system expansion in the next 2 to 3 years.	1	1 open slot	This assumes that the system is capable of accommodating additional memory installation for system expansion in the next 2 to 3 years.
C.1.1.1	Operability and maintainability	Normal operation	Operating hours	Hours during which system operates. This refers to the hours during which the system is operated, performing online processing, batch processing, and the like, in order to provide services to users and system administrators.	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 (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] A.1.1.1. "Operating hours (normal)" are an overlapping item, as they also indicate the system's availability implementation level. [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.	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.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
C.1.1.2					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 (9:00 to 8:55 the next day)	Uninterrupted 24 hours		[Overlapping Item] A.1.1.2. "Operating hours (specific days)" are an overlapping item, as they also indicate the system's availability implementation level. [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.	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, 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.
C.1.2.2			Backups	Item regarding backups of data used by the system.		Possibility of using external data	Possible to use for recovery of all data	Possible to use for recovery of some data	Not possible to use external data					[Metric] "External data" refers to data stored on systems outside the scope of the relevant system (existing systems linked with the system being developed, etc.). Since the importance of system backup design decreases when system data can be recovered from external data, consideration priority and levels can be lowered.	1	Possible to use for recovery of some data	Necessary data can be recovered from other systems, so it is not necessary to recover all system data from backups. [-] There are external systems which have the same data, so all data for this system can be recovered without using backups.	2	Not possible to use external data	This assumes that backup methods for recovering all data must be considered. [-] There are external systems which have the same data, so in the event of a failure on this system, data from the external system can be used for system recovery.	2	Not possible to use external data	This assumes that backup methods for recovering all data must be considered. [-] There are external systems which have the same data, so in the event of a failure on this system, data from the external system can be used for system recovery.
C.1.2.3						Backup usage scope	No backups	Data loss prevention when failures occur	Recovery from user errors	Long term data storage (archival)				[Level 2] For recovery from user errors, systems have to be able to return processes which, from the system's perspective, have been performed correctly, to their previous state. As such, multiple generations of backups must be managed, and functions such as "Point in Time Recovery" may be necessary.	1	Data loss prevention when failures occur	It is acceptable if restoration of data to the specified recovery point objective (RPO) in the event of a system failure. [-] There is no need to recover the data lost when a failure occurs. [+] The recovery point objective (RPO) is not fixed; recovery must be performed within the specified time depending on the specific failure.	2	Recovery from user errors	Capability of ensuring restoration of data loss including those due to a system administrator's operational error is desirable. [-] Recovery from a system administrator's operational error is ensured by the administrator individually preserving data before carrying out the work, and as such, restoration from backups is not necessary. [+] Use for recovery from data loss as well as for storing past data	3	Long term data storage (archival)	Data history must be stored in accordance with internal control support requirements. [-] Backups are used for data loss recovery purposes only.
C.1.2.4						Backup automation scope	All steps performed manually	Some steps performed manually (tape replacement and backup initiation command entry)	One step performed manually (tape replacement only)	All steps performed automatically			X	[Metric] Backup operation includes the following steps: • Scheduled job startup • Selection of backup target • Selection of backup media (tape replacement) • File transfer When decentralized storage is performed by transporting media, tape replacement is not included here. [Impact on Operation Costs] Automation of backup operation requires hardware and software investments, resulting in increased deployment costs. However, as backup work does not need to be performed by users during operation, operation costs can be expected to decrease.	1	Some steps performed manually (tape replacement and backup initiation command entry)	Backup related operations, including schedule management, are basically performed manually, but batch scripts are created to reduce the number of executed commands to some extent. [-] Scripts are not created, and administrators perform all steps manually. [+] When further reducing backup related administrator operations is desirable	2	One step performed manually (tape replacement only)	Backup related operations are performed automatically using installed backup management software, but since media management (tape replacement) is not supported by hardware, that must be performed manually. [-] Although work will increase, operations are divided into multiple work units and scripted, in order to reduce the impact of failures. [+] If automated media management is desirable	3	All steps performed automatically	This assumes backup related operations (schedule management, media management, job execution, etc.) will be handled automatically by installed management software. [-] Backups will be performed manually by administrators.
C.1.2.5						Backup interval	No backups	Random backups performed in situation such as system configuration changes, etc.	Monthly backups	Weekly backups	Daily backups	Synchronous backups			1	Random backups performed in situation such as system configuration changes, etc.	Master data, etc., which must be restored from backups does not change infrequently during operation, so instead of regular backups, backups are performed when master data is updated. [+] Data which must be restored from backups include transaction data which are constantly updated during system operation.	4	Daily backups	System-wide backups are acquired on a weekly basis. However, in order to satisfy the RPO requirement of restoring the system to the state it was in the previous day, differential backups must be taken daily. [-] RPO requirement is [-]. [+] RPO requirement is [+], or when backup availability is increased by obtaining multiple generations of backups.	5	Synchronous backups	In order to satisfy RTO requirements, updated contents are transferred to a backup site in order to configure a DR site that can immediately be put into operation in the event of a failure. [-] It is acceptable to shut down operation for backup recovery work in the event of a system failure.
C.1.2.6						Backup retention period	No backups retention	Less than 1 year	3 years	5 years	Fixed period of 10 years or longer	Permanently retained		[Metric] Unlike backup generation management, which is primarily performed from the viewpoint of availability, this item concerns backup data storage periods from the viewpoint of maintaining data integrity.	0	No backups retention	Backup data is only used for recovery after a system failure, and is not used for data archival purposes. [+] Backups are also used for data archival purposes.	2	3 years	Company policies stipulate that data update histories must be retained for 3 years. [-] Due to archival capacity limitations, it is not possible to maintain 3 years worth of data on the system. [+] Company or external regulations may change, lengthening the required retention period.	4	Fixed period of 10 years or longer	In accordance with the law, data must, be retained for 10 years. [-] Due to storage capacity limitations, it is not possible to maintain 10 years worth of data on the system. [+] There are no restrictions on storage capacity, and data must be archived permanently.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Impact on operation costs	Notes	System with almost no social impact: Selected level	System with almost no social impact: Selection conditions	System with limited social impact: Selected level	System with limited social impact: Selection conditions	System with very significant social impact: Selected level	System with very significant social impact: Selection conditions
C.1.3.1			Operation monitoring	This item concerns monitoring of entire systems, as well as the hardware and software that make them up (including business applications). Security monitoring is not included within this item. It is considered separately in "E.7.1 Fraud monitoring."		Monitored information	No monitoring performed	Alive monitoring performed	Error monitoring performed	Error monitoring (including trace information) performed	Resource monitoring performed	Performance monitoring performed	X	[Metric] "Monitoring" refers to collecting information and, in accordance with the results, notifying appropriate parties. The objective of this item is the determination of what information should be issued as monitored information. Confirm where monitored information is sent to under "C.4.5.2 Existence of monitoring system." [Level] "Alive monitoring" refers to monitoring of whether the monitored object's status is online or offline. "Error monitoring" refers to monitoring of logs, etc. output by monitored objects to confirm whether errors have occurred. When "trace information" is included, the monitoring function also determines details such as in which module the error occurred. "Resource monitoring" refers to monitoring of logs output by monitored objects, and separately acquired performance information, and the usage of them to determine resource utilization conditions, such as CPU, memory, disk, and network bandwidth utilization. "Performance monitoring" refers to monitoring of logs output by monitored objects, and separately acquired performance information, and the usage of them to determine business application and disk I/O, network transfer and similar response times, and throughput. [Impact on Operation Costs] Error monitoring, resource monitoring, and performance monitoring make identification of fault points easier, and can assist in preventing faults from occurring, leading to lower operation costs involved in maintaining system quality.	2 Error monitoring performed	Administrators can immediately access the system and investigate the status of failures, so only notifications of error occurrences are necessary. [-] All that is necessary is hardware and process alive status monitoring. [+] In order to reduce failure response time, administrators must be able to judge, to some extent, where a failure has occurred without accessing the system.	3 Error monitoring (including trace information) performed	Detailed error information must also be monitored in order that administrators can be notified of the status of failures at night as well, and determine whether immediate response is necessary. [-] Administrators can immediately access the system when failures occur, so there is no need for detailed error information monitoring. [+] Monitoring of resource utilization in addition to error information is desirable in order to prevent failures from occurring.	4 Resource monitoring performed	This assumes that there are thresholds set for CPU utilization ratios, swap occurrences, etc., to monitor signs of service level drops and consider system expansion plans and operation schedules. [-] It is only necessary to detect failures and prompt for action by administrators. [+] A more strict evaluation of system service levels, such as business application response time and throughput is desirable
C.1.3.2						Monitoring interval	No monitoring performed	Non-regular monitoring (manual monitoring)	Regular monitoring (daily intervals)	Regular monitoring (intervals of several hours)	Real-time monitoring (one minute intervals)	Real-time monitoring (one second intervals)			1 Non-regular monitoring (manual monitoring)	This assumes that diagnostic intervals will be irregular because administrators will confirm manually as necessary. [+] Confirmation will not be performed manually. Instead, the system will perform monitoring and notify administrators as necessary.	4 Real-time monitoring (one minute intervals)	It may take some time to detect failures, but the priority is to reduce system monitoring information acquisition costs, so monitoring will be performed in intervals of minutes. [-] Failure detection is performed by application functions, so system infrastructure monitoring requires only regular operation status reporting. [+] Reducing the amount of time needed for failure detection is desirable.	5 Real-time monitoring (one second intervals)	This assumes that monitoring will be performed in intervals of seconds in order to immediately detect failures and take action. [-] In order to avoid the risk of monitoring information acquisition impacting application performance, monitoring will be performed at wider intervals.
C.2.1.1		Maintenance operation	Planned system shutdown	This item concerns planned service outages performed in order to carry out system maintenance operations, such as inspections, region expansion, defragmentation, master data maintenance, and the like.	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] A.1.1.3. "Existence of planned system shutdown" is an overlapping item, as it also indicates the system's availability implementation level. [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.	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.
C.2.2.1			Operation load reduction	This item relates to maintenance operation related work load reduction design.		Maintenance work automation scope	All maintenance work is performed manually	Some maintenance work is automated	All maintenance work is automated				X	[Metric] "Maintenance work" refers to the work performed in order to maintain and manage the system infrastructure together with maintenance operation, and is assumed to incorporate update work such as inspection work and patch application work, etc., region expansion, defragmentation, log rotation, and the like. It does not include fault handling or recovery operations. [Impact on Operation Costs] Automating system infrastructure maintenance operation work requires the installation of special operation management tools and a great deal of front end work. This will result in greater deployment costs, but, thanks to maintenance operation work performed by users becoming simpler, or even unnecessary, operation costs will fall.	0 All maintenance work is performed manually	All maintenance work will be performed manually by administrators. [+] Some maintenance work will be automated.	1 Some maintenance work is automated	Regularly performed processes such as business function startup and shutdown will be automated, but irregularly performed processes, such as log deletion, will be performed manually by administrators. [-] All maintenance work will be performed manually. [+] All maintenance work will be automated.	2 All maintenance work is automated	Business function startup and shutdown, scheduled maintenance operations, etc., will all be performed automatically. [-] Some functions will be performed manually by administrators.
C.4.1.1		Operating environment	Establishment of development environment	This item relates to the environment that is deployed for the purposes of system development work by the user.		Presence of development environment	No system development environment established	Establish development environment limited to part of operating environment	Establish development environment identical to operating environment					[Metric] "Development environment" refers to a system of devices, separate from the production environment, that is expressly for development use. Development phase environments which will be used as production environments after the system is launched are not included in this item. [Level] Select level 0, "No system development environment established" for situations where a development environment is used during the development phase, but upon system launch, the environment is becomes the production environment.	0 No system development environment established	Development is performed on the production environment, and the environment is then put directly into production. [+] In order to perform development while the system is in operation, a development environment is prepared.	1 Establish development environment limited to part of operating environment	A non-cluster development environment is prepared. [-] No system development environment is provided. [+] A development environment equivalent to the production environment is provided.	2 Establish development environment identical to operating environment	A development environment equivalent to the production environment is established. [-] A development environment with only 1 application server is prepared instead of the multiple application servers that exist in the production environment.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
C.4.2.1			Establishment of test environment	This item relates to the environment that is deployed for the purposes of system testing by the user.		Presence of test environment	No system test environment established	Establish together with system development environment	Establish dedicated test environment					[Metric] "Test environment" refers to a system of devices, separate from the production environment, that is expressly for testing. Test phase environments which will be used as production environments after the system is launched are not included in this item. [Level] Select level 0, "No system test environment established" for situations where a test environment is used during the test phase, but upon system launch, the environment is becomes the production environment.	0	No system test environment established	No testing environment is prepared. [+] A testing environment is prepared.	1	Establish together with system development environment	Testing is performed as well on the development environment. [-] No development environment for testing is prepared. [+] A testing environment separate from the development environment is prepared.	2	Establish dedicated test environment	A testing environment separate from the development environment is prepared. [-] A joint development/testing environment is prepared.
C.4.3.1			Manual preparation level	Level of operation manual preparation		Manual preparation level	Standard manuals of each product are used	A normal operation system manual is provided	A normal operation system manual and maintenance operation system manual are provided	A manual customized in accordance with user system operation rules is provided			X	[Level] The normal operation manual contains explanations of standard system infrastructure operation (startup, shutdown, etc.) and functions. The maintenance operation manual contains explanations of system infrastructure maintenance work operations (part replacement, data recovery procedures, etc.) and functions. First-line support related contents (system switchover work, log acquisition procedure, etc.) related to failures are included in the normal operation manual. Information about recovering from backups is contained in the maintenance manual. [Impact on Operation Costs] The creation of manuals customized in accordance with user operation increases deployment costs, but speed up user reference during operation, resulting in reduced operation costs.	0	Standard manuals of each product are used	Administrators will refer to product manuals for information regarding how to operate the system. Users will create operation manuals as needed. [+] Manuals must be obtained from the vendors.	2	A normal operation system manual and maintenance operation system manual are provided	Assuming that users will perform maintenance operations during emergency situations, maintenance manual containing recovery procedures, etc., will be created. [-] All maintenance work is requested to the vendor, so an operation manual with explanations of operations for normal operation will be created. [+] A special operating manual containing user-specific operation rules will be created.	3	A manual customized in accordance with user system operation rules is provided	The creation of a manual which follows user operation center rules is desired. [-] General operation manuals prepared by vendors are sufficient.
C.4.4.1			Remote operation	This item defines whether or not it is possible to perform monitoring and operation via the network from an environment separated from the system installation environment.		Remote monitoring site	No remote monitoring performed	Remote monitoring performed via campus LAN	Remote monitoring performed from remote location				X	[Level] Monitored contents must be confirmed in the corresponding C.1.3.1 "Operation monitoring." [Impact on Operation Costs] Implementing remote monitoring requires special hardware and software deployment, resulting in higher deployment costs. However, with remote monitoring, there is no need for system administrators to physically go to where the servers are installed to check operations, resulting in lowered operation costs.	0	No remote monitoring performed	The number of devices is low, so remote centralized monitoring will not be performed. [+] Even if the number of devices is low, a separate monitoring server will be prepared for remote monitoring.	1	Remote monitoring performed via campus LAN	Remote monitoring will be performed only for servers located in the center, and monitoring of client terminals located in branches will not be performed. [-] Direct monitoring via console will be performed for server equipment as well. [+] Centralized remote monitoring will be performed for client terminal equipment located in branches as well.	2	Remote monitoring performed from remote location	Centralized remote monitoring of all equipment which constitute the system will be performed from a monitoring center. [-] Only server equipment in the center will be remotely monitored, and client terminals in branches will be directly monitored via connected consoles.
C.4.4.2						Remote operation scope	No remote operation performed	Only routine processes are performed from remote	Unspecified processes are performed from remote				X	[Metric] Consider the scope of operations which can be carried out from a remote monitoring site. [Level] Software to perform remote routine processes is inexpensive, while allowing unspecified remote operation results in the need to consider security and other additional aspects, so the level is higher for unspecified remote operation than routine processes. [Impact on Operation Costs] Implementing remote operation requires special hardware and software deployment, resulting in higher deployment costs. However, with remote operation, there is no need for system administrators to physically go to where the servers are installed to perform maintenance operations, resulting in lowered operation costs.	0	No remote operation performed	All maintenance operations will be performed locally on the machines. [+] Remote management terminals will be prepared to perform maintenance operations remotely.	1	Only routine processes are performed from remote	Maintenance operations on equipment will be performed from remote monitoring terminals used to perform centralized monitoring. For security purposes, restrictions on operations that can be executed will be defined in advance. [-] Remote operations will not be performed. [+] Remote operations can be performed without restrictions.	2	Unspecified processes are performed from remote	The operation department and system installation locations are separate, and all operations on the equipment will basically be performed remotely. [-] It is acceptable if only a certain set of remote operations can be performed.
C.4.5.1			External system connection	This item relates to whether or not the system is connected to an external system which affects system operation.		Existence of external system connections	No connections with external systems	Connected to external systems inside the company	Connected to external systems outside the company					[Metric] If connecting to external connections, check their interfaces.	0	No connections with external systems	The system is an intradepartmental system, and is not linked with any other systems. [+] There are other systems to which the system in question connects, such as when transmitting data to systems which store or analyze history data, etc.	1	Connected to external systems inside the company	The system is a company's mission-critical system linking to other systems within the company for order placement/reception, inventory management, etc. [-] There are no other systems with which the system in question exchanges data. [+] The system connects to and exchanges data with systems outside the company.	2	Connected to external systems outside the company	The system is a social infrastructure system that links with many other corporate systems to perform processing. [-] The are no linked external systems.
C.5.1.1		Support structure	Maintenance contract (hardware)	Scope of hardware requiring maintenance.		Maintenance contract (hardware) scope	No maintenance contract	Maintenance contract with each vendor for its own products (hardware) only	Multivendor support contract (some exceptions allowed)	Multivendor support contract (extending to all products which make up system)			X	[Level] "Maintenance contract with each vendor for its own products (hardware) only" refers to the establishment of support contracts with individual vendors who supply the products that make up the system, to provide support service for only said products. "Multivendor support contract" refers to the establishment of a support contract with a vendor who supplies support service for the entire system, and serves as a one-stop support contact for any issues affecting the system, which is made up of products produced by multiple vendors. [Impact on Operation Costs] Support contracts may appear to cause operating costs to rise, but as the costs involved in handling problems when they arise can be significant, support contracts may actually result in lower operating expenses.	1	Maintenance contract with each vendor for its own products (hardware) only	Individual hardware products which constitute the system will be procured, and the system integration will be performed by the user. [+] A systems integrator will perform overall system procurement.	2	Multivendor support contract (some exceptions allowed)	The system will be designed using existing equipment. Support for existing equipment is provided by separate vendors. [-] A one-stop support desk for handling multiple products is not necessary. [+] A one-stop support desk must provide support for all products which constitute the system, with no exceptions.	3	Multivendor support contract (extending to all products which make up system)	A single inquiry desk for system related inquiries will be established, reducing the burden placed on administrators. [-] Central inquiry desk functions are not necessary for some products, such as when special products or existing equipment are used in system establishment.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
C.5.2.1			Maintenance contract (software)	Scope of software requiring maintenance.		Maintenance contract (software) scope	No maintenance contract	Maintenance contract with each vendor for its own products (software) only	Multivendor support contract (some exceptions allowed)	Multivendor support contract (extending to all products which make up system)			X	[Level] "Maintenance contract with each vendor for its own products (software) only" refers to the establishment of support contracts with individual vendors who supply the products that make up the system, to provide support service for only said products. "Multivendor support contract" refers to the establishment of a support contract with a vendor who supplies support service for the entire system, and serves as a one-stop support contact for any issues affecting the system, which is made up of products produced by multiple vendors. [Impact on Operation Costs] Support contracts may appear to cause operating costs to rise, but as the costs involved in handling problems when they arise can be significant, support contracts may actually result in lower operating expenses.	1	Maintenance contract with each vendor for its own products (software) only	Individual software products which constitute the system will be procured, and the system integration will be performed by the user. [+] A systems integrator will perform overall system procurement.	2	Multivendor support contract (some exceptions allowed)	The system will be built using existing software licenses. Support for existing software is provided by separate vendors. [-] A one-stop support desk for handling multiple products is not necessary. [+] A one-stop support desk must provide support for all products which constitute the system, with no exceptions.	2	Multivendor support contract (some exceptions allowed)	A single inquiry desk for system related inquiries will be established, reducing the burden placed on administrators. [-] Central inquiry desk functions are not necessary for some products, such as when special products or existing equipment are used in system establishment.
C.5.3.1			Lifecycle period	The operation maintenance support period, and the actual system operation lifecycle period.		Lifecycle period	3 years	5 years	7 years	10 years or longer				[Metric] "Lifecycle period" here refers to the defined period until the next system renewal. When the lifecycle is longer than the available maintenance periods of the individual products, maintenance extension, upgrades to maintainable versions, etc., are required.	0	3 years	A reorganization will take place within 3 years, and a system renewal will be necessary. [+] The system's lifecycle is specified for about 7 years according to company policies, etc.	2	7 years	The system's lifecycle is determined as 7 years, in accordance with the support period of the software introduced. [-] The support period of the software or hardware introduced is shorter. [+] Due to internal control, etc. factors, the business performed on the system must be continued for 10 years or longer, so the lifecycle has been adjusted accordingly.	3	10 years or longer	Businesses performed on the system will continue for at least 10 years, so the system's lifecycle has been adjusted accordingly. [-] The support period(s) of the introduced software and/or hardware is shorter, so the system's lifecycle has been adjusted accordingly.
C.6.1.1		Other operation management policies	Internal control support	This item relates to whether or not to perform internal control support for IT operation process.		Existence of Internal control support implementation	Internal control support is not specified	Internal control support is performed in accordance with existing company regulations.	New regulations are established, and internal control support is performed in accordance with them.					[Metric] This item confirms whether internal control support will be performed. After confirming whether or not internal control support will be performed, clarify specific support methods (whether control would be carried out during operation, or by implementing functions in the system, etc.).	0	Internal control support is not specified	The system is not subject to internal control, so support will not be offered. [+] The system is not subject to internal control, but the department has decided that internal control support will be provided.	1	Internal control support is performed in accordance with existing company regulations.	In accordance with company regulations, internal control support will be performed. [-] The system is not subject to internal control, so support will not be provided. [+] There are no existing rules, but new rules will be established when the system is constructed.	1	Internal control support is performed in accordance with existing company regulations.	Internal control support will be performed in accordance with legal requirements. [-] There are no laws or company internal control rules, etc., which must be conformed with. [+] There are no existing rules, but new rules will be established when the system is constructed.
C.6.2.1			Service desk	This item relates to whether or not there will be a service desk function which serves as a single point for user contact.		Presence of service desk	Service desk establishment not specified	Existing service desk will be used	New service desk will be established					[Metric] This item confirms whether or not a service desk will be established for communications between users and the vendor. After confirming whether or not a service desk function will be provided, clarify specific implementation methods.	0	Service desk establishment not specified	No service desk functions will be provided for interfacing between the user and vendor; instead, they will be handled individually. [+] A service desk will be established.	1	Existing service desk will be used	There is an existing service desk for interfacing with a vendor with whom there is a multivendor support contract. [-] No service desk will be established. [+] For vendors dealing for the first time, there is no existing service desk.	2	New service desk will be established	The vendor will establish a dedicated service desk function for the system. [-] An existing service desk function will be used.
D.1.1.1	Migratability	Migration period	Migration schedule	The system migration period from migration work planning to the start of operation, dates/times for system outages, whether or not parallel operation will be performed. (Including rollback time for exceptional circumstance, pre-migration backup work, etc.)		System migration period	No system migration	Less than 3 months	Less than 6 months	Less than 1 year	Less than 2 years	2 years or longer			1	Less than 3 months	The system must be constructed within a short amount of time. [+] System construction is performed within a medium to long term span.	4	Less than 2 years	System migration must span a fiscal year. [-] Shorter period of time [+] A longer period of time is required.	5	2 years or longer	The migration process, from planning to operation, must place safety as its highest priority. [-] Shorter period of time
D.1.1.2						Days/times when system outages are possible	No limitations (System can be shut down for as long as needed)	5 days or more	Less than 5 days	1 day (Using scheduled system outage day)	During low usage times (night, etc.)	System outage for system migration is not allowed		[Metric] For some systems, it may not be possible to secure continuous days or time slots for system outage. (For example, 1 full day, followed by a day where the system can only be shut down at night, followed by a scheduled system outage day, when the system can be shut down for a full day.) When this is the case, confirm both days and time slots available for system outage. [Level] Level 0 indicates that the system can be shut down for as long as needed for migration, regardless of system limitations. Levels 1 and over indicate the days/times when system outages are possible, given system outage (business, etc.) related limitations. The higher the level, the greater the effect of system limitations on migration plans, such as days/times when the system can be shut	1	5 days or more	The impact on business is minimal, and system outage of several days or longer is acceptable. [-] Outages will be longer. [+] Outages will be shorter.	4	During low usage times (night, etc.)	System outage is possible during time periods when there is relatively little business. [-]Outages will be longer.	5	System outage for system migration is not allowed	System down time must be minimized. [-] A downtime period will be secured
D.1.1.3						Existence of parallel operation	None	Yes						[Level 1] When parallel operation is used, specify the period, location, etc. F.4.2.3 and F.4.4.3 are related items.	0	None	A sufficient amount of system downtime can be secured for migration, so the need for parallel operation is low. [+] System downtime for migration cannot be secured, so parallel operation will be performed.	1	Yes	There is little available system downtime for migration, so, considering the risks involved in migration, parallel operation is necessary. [-] System downtime for migration can be secured, so parallel operation will not be performed.	1	Yes	System outage is not possible for migration, so migration risk reduction is the highest priority, and parallel operation is essential. [-] System downtime for migration can be secured, so parallel operation will not be performed.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
D.2.1.1		Migration scheme	System deployment scheme	To what degree multi-step deployment schemes are used in system migration and new deployments.		Number of steps for site deployment	No regulations, as there is only 1 site	Simultaneous deployment	Less than 5 steps	Less than 10 steps	Less than 20 steps	20 steps or more		[Level] Depending on site deployment risks, the difficulty may be reversed, with simultaneous deployment being the most difficult. Consider deployment risks of the system for each site and determine the number of steps for site migration.	0	No regulations, as there is only 1 site	No rules on deployment are necessary, as the system is monolithic. [+] System deployment must be considered.	1	Simultaneous deployment	Switchover performed concurrently in order to maximize efficiency. There is little need for phased migration [+] Phased deployment is necessary.	2	Less than 5 steps	Phased deployment is necessary. [-] Concurrent deployment is performed. [+] The number of phases must be increased.
D.2.1.2						Number of steps for business deployment	No regulations, as there is only 1 business	Simultaneous deployment for all businesses	Less than 4 steps	Less than 6 steps	Less than 10 steps	10 steps or more		[Level] Depending on business deployment risks, the difficulty may be reversed, with simultaneous deployment being the most difficult. Consider deployment risks of the system for each business and determine the number of steps for business deployment.	0	No regulations, as there is only 1 business	No rules on deployment are necessary, as the system is monolithic. [+] System deployment must be considered.	1	Simultaneous deployment for all businesses	Switchover performed concurrently in order to maximize efficiency. There is little need for phased migration [+] Phased deployment is necessary.	2	Less than 4 steps	Phased deployment is necessary. [-] Concurrent deployment is performed. [+] The number of phases must be increased.
D.3.1.1		Migration scope (equipment)	Equipment to be replaced	Which equipment used in the system before migration will be replaced with new equipment in the new system.		Equipment / device migration contents	Nothing in migration scope	Hardware replacement of equipment / devices in migration scope	Hardware, OS, and middleware replacement of equipment / devices in migration scope	Total system replacement of equipment / devices in migration scope	Total system replacement and integration of equipment / devices in migration scope			[Level] Reach consensus for each piece of equipment when there are multiple pieces of equipment within the migration scope, and migration contents vary for each.	0	Nothing in migration scope	Facility equipment must be newly installed. [+] There is existing facility equipment.	3	Total system replacement of equipment / devices in migration scope	Migration includes business applications. [-] There is no renewal of business applications. [+] The extent of renewal for the business applications is large.	2	Hardware, OS, and middleware replacement of equipment / devices in migration scope	Renewal of business applications will not be performed, but measures such as preventing to become obsolete and improving performance are necessary. [-] Hardware replacement only [+] Business application renewal will be performed.
D.4.1.1		Migration scope (data)	Migration data volume	The amount of business data which must be migrated (including programs) from the old system.		Migration data volume	Nothing in migration scope	Less than 1TB	Less than 1PB	1PB or more					1	Less than 1TB	Less than 1TB (terabyte) of data (master data, etc.) must be migrated. [+] Over 1TB	2	Less than 1PB	Less than 1PB (petabyte) of data must be migrated. [-] Less than 1TB [+] 1PB or over	3	1PB or more	1PB (petabyte) or more of data must be migrated. [-] Less than 1PB
D.4.1.2						Migration data format	Nothing in migration scope	Same format as migration destination	Different format than migration destination					[Metric] "Data format" refers to data format patterns which must be considered during new system migration, such as application dependant formats, table formats, and character codes. [Level] When there are multiple migration data format patterns, perform data format confirmation for each.	1	Same format as migration destination	The current data format will be used without change. [+] Data format changes are necessary.	2	Different format than migration destination	Data format changes is necessary due to business efficiency improvement and integration, etc. [-] Migration data format will not be changed.	1	Same format as migration destination	In order to secure data continuity and compatibility with other systems, the current data formats will be used without change. [+] Data format changes are necessary.
E.1.1.1	Security	Prerequisites / restrictions	Information security related compliance	This item is for confirming whether or not there are information security related organizational policies, rules, laws, guidelines, etc., which must be observed by users. In the event that there are rules, etc to be observed, measures must be considered to ensure that there are no conflicts with said regulations, etc. Ex) • Information security policy • Act Concerning the Prohibition of Unauthorized Computer Access • Personal Information Protection Law • Electronic Signature Law • Provider Responsibility Law • Act on Regulation of Transmission of Specified Electronic Mail • Sarbanes-Oxley Act • Basic Law for Building an Advanced Info-Communications Network • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISMA • FISC • PCI DSS • PrivacyMark System • TRUSTe Etc. (* The above examples are mainly Japanese laws, systems, etc.)		Existence of applicable company regulations, rules, laws, guidelines, etc.	None	Yes						[Metric] Regulations, laws, guidelines, etc., must be confirmed, and decide security related non-functional requirement item levels in accordance with them.	0	None	Levels must be determined in accordance with user requirements. [+] There are rules, laws, guidelines, etc., which must be conformed with.	0	None	Levels must be determined in accordance with user requirements. [+] There are rules, laws, guidelines, etc., which must be conformed with.	0	None	Levels must be determined in accordance with user requirements. [+] There are rules, laws, guidelines, etc., which must be conformed with.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact		System with limited social impact		System with very significant social impact	
							0	1	2	3	4	5			Selected level	Selection conditions	Selected level	Selection conditions	Selected level	Selection conditions
E.2.1.1		Security risk analysis	Security risk analysis	This item confirms the policy regarding the scope of system threat identification and impact analysis for the developed system. In order to establish an appropriate scope, it is necessary to identify assets, confirm data lifecycles, etc. The scope of countermeasures for identified threats must also be considered.		Risk analysis scope	No analysis	Scope which includes highly important assets, and external connection related areas	Development scope					[Level 1] "External connection related areas" refer to external connections to the Internet, connections to media, etc., used for carrying information and data outside the system, and areas which handle data transactions with external systems. The same meaning is used for all levels.	0 No analysis	Detailed risk analysis will not be performed, but basic measures will be enacted.	1 Scope which includes highly important assets, and external connection related areas	Since important data will be handled, the risk of threats becoming a reality is high. As such, risk analysis is necessary for areas where highly important assets will be handled. [-] There is no threat, such as leakage, of important information (or the risks are accepted). [+] There will be a great deal of information transfer or status changes.	2 Development scope	There is a threat of attacks via network by an unspecified number of attackers. Also, since important data will be handled, the risk of threats becoming a reality is high. As such, risk analysis is necessary for the entire system. [-] Data transfer and modifications, etc., will not occur, so there are no threats due to changes in access rights to related information, etc. (or the threat is accepted).
E.3.1.1		Security diagnostics	Security diagnostics	This item is used to confirm whether or not specialized security testing and inspection will be performed for the system and individual documents (design documentation, environment definition documents, implemented software source code, etc.)		Existence of network diagnostics implementation	None	Yes						[Metric] "Network diagnostics" refer to diagnosis, in a broad sense, of the system. Network diagnostics include visual confirmation of settings, as well as diagnoses of vulnerabilities by performing simulated attacks (penetration testing).	1 Yes	There is a threat of attacks via network by an unspecified number of attackers. As such, analysis of vulnerabilities to network based attacks must be performed. [-] Personnel with expert level security knowledge will give sufficient consideration to network based attack countermeasures, and create relevant documentation.	1 Yes	Important data will be handled, so analysis of vulnerabilities to internal network based attacks must be performed. [-] Personnel with expert level security knowledge will give sufficient consideration to internal network based attack countermeasures, and create relevant documentation.	1 Yes	There is a threat of attacks via network by an unspecified number of external attackers. Also, since important data will be handled, the risk of threats becoming a reality is high. As such, analysis of vulnerabilities to network based attacks must be performed. [-] Personnel with expert level security knowledge will give sufficient consideration to network based attack countermeasures, and create relevant documentation.
E.3.1.2						Existence of Web site diagnostics implementation	None	Yes						[Metric] "Web site diagnostics" refers to security diagnostics of Web servers and Web applications performed on Web sites.	1 Yes	There is a threat of attacks via network from a great number of attackers. As such, analysis of Web application related vulnerabilities must be performed. [-] Web applications will not be used.	1 Yes	Threat of internal network based attacks could occur, so countermeasures must be implemented. [-] There is no need to assume internal attacks. Web applications will not be used.	1 Yes	There is a threat of attacks via network from a great number of attackers. As such, analysis of Web application related vulnerabilities must be performed. [-] Web applications will not be used.
E.5.1.1		Access / usage restrictions	Authentication function	This item confirms whether or not agent (user and equipment, etc.) authentication is performed in order to use assets, and, if so, to what degree. The effectiveness of deterrence can be raised by performing authentication multiple times. Authentication methods include ID/password authentication and IC card authentication, etc.		Authentication of agents with administrative rights	Not performed	1 time	Authentication performed multiple times	Authentication performed multiple times using different authentication methods				[Metric] "Agents with administrative rights" refers to system administrators and business and operation administrators.	1 1 time	In order to prevent attackers from obtaining and abusing administrative privileges, authentication must be performed. [+] Some of the processes which can be executed by those with administrative privileges are critical for business.	2 Authentication performed multiple times	In order to prevent attackers from obtaining administrative privileges and leaking information, etc., authentication must be performed multiple times.	2 Authentication performed multiple times	In order to prevent attackers from obtaining administrative privileges and leaking information, etc., authentication must be performed multiple times. [-] Entities with administrative privileges cannot access the system via external networks.
E.5.2.1			Usage restrictions	This item is for confirming whether or not software or hardware access controls are placed on the usage, etc. of assets by authenticated agents (users and equipment). Ex) Door and storage cabinet locks, USB, CD-RW, keyboard, and other input/output device restrictions, command execution restrictions, etc.		Operation restrictions placed by system measures	None	Only minimum necessary amount of program execution, command operation, and file access is permitted						[Metric] Refers to software measures such as software installation restrictions, usage restrictions, etc.	1 Only minimum necessary amount of program execution, command operation, and file access is permitted	The installation of unauthorized software or the opening of unneeded access paths (ports, etc.) may result in the threat of information leakage becoming a reality. As such, unnecessary methods for accessing this information, etc., must be limited. (There is a possibility that limiting operations may impact convenience and availability.) [-] For terminals which do not serve as bases for attacks on important information, etc., countermeasures based on operational methods will be used.	1 Only minimum necessary amount of program execution, command operation, and file access is permitted	The installation of unauthorized software or the opening of unneeded access paths (ports, etc.) may result in the threat of information leakage becoming a reality. As such, unnecessary methods for accessing this information, etc., must be limited. (There is a possibility that limiting operations may impact convenience and availability.) [-] For terminals which do not serve as bases for attacks on important information, etc., countermeasures based on operational methods will be used.	1 Only minimum necessary amount of program execution, command operation, and file access is permitted	The installation of unauthorized software or the opening of unneeded access paths (ports, etc.) may result in the threat of information leakage becoming a reality. As such, unnecessary methods for accessing this information, etc., must be limited. (There is a possibility that limiting operations may impact convenience and availability.) [-] For terminals which do not serve as bases for attacks on important information, etc., countermeasures based on operational methods will be used.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
E.6.1.1		Data confidentiality	Data encryption	This item is for confirming whether or not encryption of confidential data is performed when transmitting or storing data.		Transmitted data encryption	None	Only authentication information is encrypted	Important information is encrypted					[Level 1] "Only authentication information is encrypted" means that, regardless of whether the system is handling critical information, only authentication information, such as passwords, etc., is encrypted.	1	Only authentication information is encrypted	Encryption will be performed on passwords, etc. that are sent over the network in order to prevent them being obtained by third parties. [-] Authentication information is not be sent over the network.	2	Important information is encrypted	In order to counter the threat of eavesdropping, etc., especially important data must be encrypted when transmitted, even over the local network. (There is a possibility of decreased performance due to encryption of transmitted data.) [-] Physical measures, such as the use of leased lines, are used / The threat of eavesdropping on local networks is accepted / Important data will be handled which does not require confidentiality but does require integrity.	2	Important information is encrypted	In order to counter the threat of eavesdropping, etc., especially important data must be encrypted when transmitted, even over the local network. (There is a possibility of decreased performance due to encryption of transmitted data.) [-] Physical measures, such as the use of leased lines, are used / The threat of eavesdropping on local networks is accepted / Important data will be handled which does not require confidentiality but does require integrity.
E.6.1.2						Encryption of stored data	None	Only authentication information is encrypted	Important information is encrypted					[Level 1] "Only authentication information is encrypted" means that, regardless of whether the system is handling critical information, only authentication information, such as passwords, etc., is encrypted.	1	Only authentication information is encrypted		2	Important information is encrypted	In order to counter the threat of the leakage of important information such as personal information, passwords, etc., stored in databases, on backup tapes, etc., stored data must be encrypted. (There is a possibility that encrypting stored data may impact performance.) [-] Safety will be secured through other multiple measures, such as using tamper-proof devices, authentication measures, operation measures, etc. / Important data will be handled which does not require confidentiality but does require integrity.	2	Important information is encrypted	In order to counter the threat of the leakage of important information such as personal information, passwords, etc., stored in databases, on backup tapes, etc., stored data must be encrypted. (There is a possibility that encrypting stored data may impact performance.) [-] Safety will be secured through other multiple measures, such as using tamper-proof devices, authentication measures, operation measures, etc. / Important data will be handled which does not require confidentiality but does require integrity.
E.7.1.1		Fraud tracking / monitoring	Fraud monitoring	This item is for confirming the scope of fraudulent activity monitoring, the volume of stored monitoring records, and the length for which said monitoring records are retained. The types of logs which should be acquired must be decided based on the specific system and service. When logs are taken, together with fraud monitoring targets, the scope of logs which are checked for fraud must also be defined.		Log acquisition	Not performed	Performed						[Metric] Acquired logs refer to logs such as the following, used to detect fraudulent activities. • Login / logout history (success / failure) • Operation logs Etc.	1	Performed	Logs must be taken so that when unauthorized access occurs, it is possible to confirm who did what, from where, when, and what happened as a result, and take immediate response measures. (There is a possibility that logging processes may impact performance.)	1	Performed	Logs must be taken so that when unauthorized access occurs, it is possible to confirm who did what, from where, when, and what happened as a result, and take immediate response measures. (There is a possibility that logging processes may impact performance.)	1	Performed	Logs must be taken so that when unauthorized access occurs, it is possible to confirm who did what, from where, when, and what happened as a result, and take immediate response measures. (There is a possibility that logging processes may impact performance.)
E.7.1.2						Log retention period	6 months	1 year	3 years	5 years	10 years or longer	Permanent retention			0	6 months	Logs must be retained for an appropriate length of time for purposes of fraudulent activity checking, and in order to maintain an audit trail of successful processes. [-] Log confirmation interval is short. [+] Capacity can be secured for backups, etc.	2	3 years	Logs must be retained for an appropriate length of time for purposes of fraudulent activity checking, and in order to maintain an audit trail of successful processes. [-] Log confirmation interval is short. [+] Capacity can be secured for backups, etc.	3	5 years	Logs must be retained for an appropriate length of time for purposes of fraudulent activity checking, and in order to maintain an audit trail of successful processes. [-] Log confirmation interval is short. [+] Capacity can be secured for backups, etc.
E.7.1.3						Fraud monitoring scope (equipment)	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] The "fraud monitoring scope (equipment)" metric is used to confirm the scope of logs which are to be acquired in order to perform fraudulent access monitoring, etc., for servers, storage devices, etc.	1	Scope which includes highly important assets, and external connection related areas	In order to detect threats when they occur, and immediately launch countermeasures, the scope of servers, storage, etc., to be monitored must be defined.	1	Scope which includes highly important assets, and external connection related areas	In order to detect threats when they occur, and immediately launch countermeasures, the scope of servers, storage, etc., to be monitored must be defined.	2	Entire system	In order to detect threats when they occur, and immediately launch countermeasures, the scope of servers, storage, etc., to be monitored must be defined. Attacks via external networks do not have a limited attack scope, and as such, monitoring must be performed of the entire system.
E.7.1.4						Fraud monitoring scope (network)	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] The "fraud monitoring scope (network)" metric is used to confirm the scope of logs which are to be acquired in order to monitor unauthorized packets, etc., on the network.	1	Scope which includes highly important assets, and external connection related areas	In order to detect threats when they occur, and immediately launch countermeasures, the scope of the network to be monitored must be defined.	1	Scope which includes highly important assets, and external connection related areas	In order to detect threats when they occur, and immediately launch countermeasures, the scope of the network to be monitored must be defined.	2	Entire system	In order to detect threats when they occur, and rapidly launch countermeasures, the scope of the network to be monitored must be defined. Attacks via external networks do not have a limited attack scope, and as such, monitoring must be performed of the entire system.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
E.7.1.5						Fraud monitoring scope (intruders / unauthorized operations, etc.)	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] The "fraud monitoring scope (intruders / unauthorized operations). etc." metric is used to confirm the scope of monitoring consisting of monitoring cameras installed to monitor for intruders, etc.	1	Scope which includes highly important assets, and external connection related areas	In order to detect threats when they occur, and immediately launch countermeasures, the physical scope to be monitored, such as floors, areas, etc. must be defined. [-] Room access management, operation restrictions, etc., are implemented sufficiently.	1	Scope which includes highly important assets, and external connection related areas	In order to detect threats when they occur, and immediately launch countermeasures, the physical scope to be monitored, such as floors, areas, etc. must be defined.	2	Entire system	In order to detect threats when they occur, and immediately launch countermeasures, the physical scope to be monitored, such as floors, areas, etc. must be defined.
E.8.1.1		Network measures	Network control	This item is for confirming whether transmission control is implemented in order to block unauthorized transmissions.		Transmission control	None	Yes						[Level 1] When implementing transmission control, firewall deployment, etc., must also be considered.	1	Yes	In order to prevent threats, such as becoming a stepping stone in attacks, or having information taken away, network controls such as blocking of unauthorized transmissions must be implemented. [-] Threats, such as becoming a stepping stone in attacks, are accepted.	1	Yes	In order to prevent threats, such as becoming a stepping stone in attacks, or having information taken away, network controls such as blocking of unauthorized transmissions must be implemented. [-] Threats, such as becoming a stepping stone in attacks, are accepted.	1	Yes	In order to prevent threats, such as becoming a stepping stone in attacks, or having information taken away, network controls such as blocking of unauthorized transmissions must be implemented. [-] Threats, such as becoming a stepping stone in attacks, are accepted.
E.8.2.1			Fraud detection	This item is for confirming the scope of network based fraud tracking / monitoring detection of fraudulent activities or transmissions within the system.		Fraudulent transmission detection scope	None	Scope which includes highly important assets, and external connection related areas	Entire system					[Metric] Depending on the defined detection scope, the deployment of IDS, etc., must also be considered.	1	Scope which includes highly important assets, and external connection related areas	In order to identify unauthorized transmissions and rapidly deploy countermeasures, fraud detection must be implemented.	1	Scope which includes highly important assets, and external connection related areas	In order to identify unauthorized transmissions and rapidly deploy countermeasures, fraud detection must be implemented.	1	Scope which includes highly important assets, and external connection related areas	In order to identify unauthorized transmissions and rapidly deploy countermeasures, fraud detection must be implemented.
E.8.3.1			Denial of service (DoS) attack avoidance	This item is for confirming whether countermeasures are enacted against congestion caused by attacks on the network.		Network congestion countermeasures	None	Yes							1	Yes	The system must deal with denial of service attacks (DoS/DDoS attacks). (Relates to availability) [-] For DoS/DDoS attacks, countermeasures to some extent are implemented as part of availability requirements, and anything beyond that are accepted.	1	Yes	The system must deal with to denial of service attacks (DoS/DDoS attacks). (Relates to availability) [-] For DoS/DDoS attacks, countermeasures to some extent are implemented as part of availability requirements, and anything beyond that are accepted.	1	Yes	The system must deal with to denial of service attacks (DoS/DDoS attacks). (Relates to availability) [-] For DoS/DDoS attacks, countermeasures to some extent are implemented as part of availability requirements, and anything beyond that are accepted.
E.9.1.1		Malware countermeasures	Malware countermeasures	This item is for confirming the implementation scope of measures to prevent malware (viruses, worms, bots, etc.) from infecting the system, and the timing of malware checking. When countermeasures are implemented, virus pattern file update methods and timing must also be considered, and virus patterns must be kept up to date.		Malware countermeasure implementation scope	None	Scope which includes highly important assets, and external connection related areas	Entire system						1	Scope which includes highly important assets, and external connection related areas	In order to prevent the threat of service interruption, etc., due to malware infection, malware countermeasures must be implemented. [-] An OS, etc., which is not very susceptible to attacks will be used.	1	Scope which includes highly important assets, and external connection related areas	In order to prevent the threat of important information leakage, etc., due to malware infection, malware countermeasures must be implemented. [-] An OS, etc., which is not very susceptible to attacks will be used.	1	Scope which includes highly important assets, and external connection related areas	In order to prevent the threat of important information leakage, etc., due to malware infection, malware countermeasures must be implemented. [-] An OS, etc., which is not very susceptible to attacks will be used.
E.10.1.1		Web measures	Web implementation measures	This item is for confirming whether measures related to Web application-specific threats or vulnerabilities are implemented		Measure enhancement through secure coding, Web server configuration, etc.	None	Measure enhancement						[Metric] The number of Web system attacks is increasing, and when constructing a Web system, measures such as secure coding and Web server configuration must be considered. When implemented, consideration must also be given to specialist review and source code diagnostics as well as tool-based checking in order to evaluate their effectiveness.	1	Measure enhancement	In open systems, in order to counter the threat of leakage of important data contained in databases, etc., as well as spoofing of users, etc., Web server measures must be implemented. [-] Web applications will not be used.	1	Measure enhancement	In open systems, in order to counter the threat of leakage of important data contained in databases, etc., as well as spoofing of users, etc., Web server measures must be implemented. [-] Web applications will not be used.	1	Measure enhancement	In open systems, in order to counter the threat of leakage of important data contained in databases, etc., as well as spoofing of users, etc., Web server measures must be implemented. [-] Web applications will not be used.
E.10.1.2						WAF implementation	None	Yes						[Metric] WAF stands for Web Application Firewall.	0	None	Important information is not handled, so there is no need for WAF deployment.	0	None	There will be no connections to external networks. As such, there is little likelihood of the threat of network based attacks. [+] There is a threat of attacks via internal networks.	1	Yes	In order to counter the threat, such as information leakage or becoming a stepping stone in attacks via system intrusion, device-based intrusion prevention and detection measures must be implemented. [-] Web server measures, unauthorized access prevention measures, and regular log confirmation, etc., are performed.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
F.1.1.1	System environment and ecology	System restrictions / prerequisites	System construction restrictions	This item relates to whether or not there are applicable restrictions when constructing the system, such as company regulations, laws, local governmental ordinances, etc. Ex) • Financial Instruments and Exchange Act • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISC • PrivacyMark System • Construction location restrictions Etc. (* The above examples are mainly Japanese laws, systems, etc.)		System construction restrictions	No restrictions	Possible restrictions (only critical restrictions apply)	Possible restrictions (all restrictions apply)					[Metric] During system development, sometimes it is necessary to handle confidential information, personal information, etc. In order to minimize the risk of their leakage, projects must prepare a development environment which implements risk reduction measures such as restricting personnel that can use the information/data, controlling room access, encrypting information/data, etc. Other restrictions may also apply, such as situations where the planned operation site cannot be used for system construction, and it is necessary to construct the system in a staging environment at a different site and transporting it to the planned operation site, or situations where system construction can only be performed at the planned operation site.	0	No restrictions	There are no particular limitations which affect the system. [+] Legal or regulatory restrictions affect the system, or the system is bound by industry or similar standards and arrangements.	1	Possible restrictions (only critical restrictions apply)	The system is affected by company rules, etc. [-] No legal or regulatory restrictions affect the system, or there are no industry or similar standards or arrangements.	1	Possible restrictions (only critical restrictions apply)	The system is affected by legal restrictions. [-] No legal or regulatory restrictions affect the system, or there are no industry or similar standards or arrangements. [+] There are restrictions placed by company standards which exceed those demanded by legal and regulatory conformance, and conformance is required for all said restrictions.
F.1.2.1			Operating restrictions	This item relates to whether or not there are applicable restrictions when the system is in live operation, such as company regulations, laws, local governmental ordinances, etc. Ex) • Financial Instruments and Exchange Act • ISO/IEC27000 series • Standards for Information Security Measures for the Central Government Computer Systems • FISC • PrivacyMark System • Possibility of remote operation Etc. (* The above examples are mainly Japanese laws, systems, etc.)		Operating restrictions	No restrictions	Possible restrictions (only critical restrictions apply)	Possible restrictions (all restrictions apply)						0	No restrictions	There are no particular limitations which affect the system. [+] Installed center policies, operation related methods such as joint operation methods, and the like act as restrictions on the system.	1	Possible restrictions (only critical restrictions apply)	Consideration is given to centers / machine rooms where certain restrictions may be applied to installations. However, conditions can be adjusted. [+] Installed center policies, operation related methods such as joint operation methods, and the like act as restrictions on the system.	1	Possible restrictions (only critical restrictions apply)	Consideration is given to centers / machine rooms where certain restrictions may be applied to installations. However, conditions can be adjusted. [+] Installed center policies, operation related methods such as joint operation methods, and the like act as restrictions on the system.
F.2.1.1		System characteristics	Number of users	The number of system users (end users).	X	Number of users	Specific users only	Upper limit is specified	Usable by unspecified number of users					[Overlapping Item] B.1.1.1. The "number of users" is essential for deciding performance and scalability, and is an item that defines the system environment as well, so this item is included in both "Performance and scalability" and "System environment and ecology". [Level] Even if the numerical value for this prerequisite cannot be precisely determined, it is important that at least a tentative value, based on similar systems, etc., should be decided on.	0	Specific users only	This assumes cases where users can be identified since the use is within a department. [+] When users cannot be identified.	1	Upper limit is specified	This assumes cases where an upper limit is specified. [-] Consensus has been reached that only specific users will use the system.	2	Usable by unspecified number of users	This assumes cases where the general public will access the system. [-] It is possible to specify an upper limit.
F.2.2.1			Number of clients	The number of clients used by the system, which must be managed.		Number of clients	Specified clients only	Upper limit is specified	Usable by unspecified number of clients						0	Specified clients only	Only specific clients will use the system. [+] The number of clients is expected to grow in the future, and consensus must be obtained regarding the maximum number of clients.	1	Upper limit is specified	A specific value will be determined, and consensus regarding it will be obtained. [+] No upper limit will be specified.	1	Upper limit is specified	A specific value will be determined, and consensus regarding it will be obtained. [+] No upper limit will be specified.
F.2.3.1			Number of sites	The number of sites in which the system is in operation.		Number of sites	Single site	Multiple sites						[Level 1] Specify the exact number when consensus has been reached regarding the number of sites.	0	Single site	Single site system. [+] Multiple sites	1	Multiple sites	Multiple site system. [-] Single site	1	Multiple sites	Multiple site system. [-] Single site
F.2.4.1			Geographical spread	The geographical range over which the system operates.		Geographical spread	Inside site	Within 1 city	Within 1 prefectural area	Within 1 region	Domestic	International		[Level] When the selected level is 5, consideration must also be given to multi-language support, etc. Even for domestic systems, if the geographical reach of the system is expansive, network, logistical, and support handling will also be necessary.	0	Inside site	The access scope will be limited to within the site, and there will be no access from the outside. [+] The access scope will extend outside the site, due to allowing remote access, etc.	0	Inside site	The access scope will be limited to within the site, and there will be no access from the outside. [+] Other offices will also access the system.	4	Domestic	The access scope will not extend overseas. [-] User rights will be limited to company and organization users. [+] The system will be an Internet based system, or similar system, with an access scope that extends overseas.
F.2.5.1			Specification of specific products	This item is for confirming if users have specified the use of open source products, third-party products (ISV/IHV, etc.). Confirmation is from the perspective of whether the selection has an impact on the difficulty of providing support.		Use of specific products	No products specified	Some products specified	Products that are difficult to support are specified						0	No products specified	There is no particular product specified to be used in the system. [+] There are explicit specifications.	1	Some products specified	There are particular products specified to be used in the system. [-] There are no explicit specifications.	0	No products specified	There is no particular product specified to be used in the system. [+] There are explicit specifications.

No.	Major category	Middle category	Minor category	Minor category description	Overlapping item	Metric	Level						Impact on operation costs	Notes	System with almost no social impact			System with limited social impact			System with very significant social impact		
							0	1	2	3	4	5			Selected level		Selection conditions	Selected level		Selection conditions	Selected level		Selection conditions
F.3.1.1		Conformity standards	Product safety standards	This item is for confirming whether product safety standards such as UL60950 are required to be held by products used in the system.		Standard certification	Standard certification not necessary	UL60950 equivalent certification acquired							0	Standard certification not necessary	There is no particular equipment specified for standard certification. [+] There are explicit specifications.	1	UL60950 equivalent certification acquired	There is equipment specified for standard certification. [-] There are no explicit specifications.	0	Standard certification not necessary	There is no particular equipment specified for standard certification. [+] There are explicit specifications.
F.3.2.1			Environmental protection	This item is for confirming whether specified toxic substance usage restriction related standards such as those set out in the RoHS directive are required to be held by products used in the system.		Standard certification	Standard certification not necessary	RoHS directive equivalent certification acquired							0	Standard certification not necessary	There are no particular limitations which affect the system. [+] There are explicit specifications.	1	RoHS directive equivalent certification acquired	RoHS Directive supporting devices are specified. [-] There are no specifications.	0	Standard certification not necessary	There are no particular limitations which affect the system. [+] There are explicit specifications.
F.4.1.1		Conditions of equipment installation environment	Earthquake resistance / seismic isolation	Specifies the effective maximum earthquake intensity which the system environment must be able to withstand. If measures such as building vibration damping are used to, for example, decrease the effective seismic intensity of an earthquake from 7 or greater outside the building to a maximum inside intensity of 4, then set the level for seismic intensity to 4. If it is acceptable for service to be discontinued at or above a given seismic intensity, set the level for that given seismic intensity.		Earthquake resistance intensity	Countermeasures not necessary	Seismic intensity 4 equivalent (50 Gal)	Seismic intensity 5-lower equivalent (100 Gal)	Seismic intensity 6-lower equivalent (250 Gal)	Seismic intensity 6-upper equivalent (500 Gal)	Seismic intensity 7 equivalent (1000 Gal)		[Metric] For buildings containing system environments which have the same degree of vibration inside as out, the effective seismic intensity of the system environment can be expected to be roughly equivalent to the external seismic intensity. As such, the level can be selected based on the exterior seismic intensity. When seismic isolation facilities, etc., guarantee a reduced maximum seismic intensity for the system environment, that seismic intensity can be considered as the effective seismic intensity, and level assignment can be based on it (users may specifically request a higher level assignment). In the event that an earthquake of a certain intensity or greater would result in there being no system users in environments where they could use the system, and as such system continuity becomes unnecessary, the level may be set based on that seismic intensity. In any case, it is unreasonable to set the standard higher than the earthquake resistance intensity of the building itself. [Level 0] The risk of service outage due to earthquakes must be accepted.	2	Seismic intensity 5-lower equivalent (100 Gal)	Seismic intensity 5-lower equivalent. [-] The level is changed in accordance with building or installation environment conditions when the system is installed in a seismically isolated building, etc. [+] When specific values are specified, change to an appropriate level. Consideration must also be given to raising the level when earthquake resistant racks are used in order to prevent accidents or injuries due to rack collapse when installed in an office without seismic isolation.	3	Seismic intensity 6-lower equivalent (250 Gal)	Seismic intensity 6-lower equivalent. [-] The level is changed in accordance with building or installation environment conditions when the system is installed in a seismically isolated building, etc. [+] The level is changed when specific values are specified, in accordance with building or installation environment conditions.	4	Seismic intensity 6-upper equivalent (500 Gal)	Seismic intensity 6-upper equivalent. [-] Consideration is given to the combined building environment and equipment environment, such as installing the system in a seismically isolated building, etc. [+] A value which corresponds to a major earthquake, with a seismic intensity of 7-upper, etc., is specified.
F.4.2.1			Space	This item relates to how much floor space (WxD) and height is necessary. Consideration must also be given to maintenance operation space. Whether or not space for parallel operation of new and old system can be secured for system migration must also be confirmed. If possible, it must be confirmed in advance.		Installation space restrictions (machine room)	No space related restrictions	Design using floor-standing equipment	Design using rack-mount equipment					[Metric] Confirm specific floor space and height. Also note the shape of the space, and any variations in load-bearing by location.	2	Design using rack-mount equipment	The system will be rack-mounted. [-] There are no installation-related restrictions.	2	Design using rack-mount equipment	The system will be rack-mounted. [-] There are no installation-related restrictions.	2	Design using rack-mount equipment	The system will be rack-mounted in a center. [-] There are no installation-related restrictions.
F.4.2.2						Installation space restrictions (installation in office space)	No space related restrictions	Dedicated space can be set aside for system	System must be installed in space also used by people					[Metric] Confirm specific floor space and height. Also note the shape of the space, and any variations in load-bearing by location. [Level] Consider installation space restrictions as already defined prerequisites, and set levels based on the difficulty of installing the system given those requirements. Please note that this is not the difficulty involved in securing the space itself.	1	Dedicated space can be set aside for system	The system will be installed in a server corner, etc., on the office floor. [-] The system will be installed in an area with little foot traffic. [+] Due to operation or monitoring needs, the system must be installed in an area regularly used by people, with no partitions.	2	System must be installed in space also used by people	The equipment will consist of front-end business devices such as terminal devices. [-] From a business perspective, the equipment does not need to be in an area used by people.	2	System must be installed in space also used by people	The equipment will consist of front-end business devices such as terminal devices. [-] From a business perspective, the equipment does not need to be in an area used by people.