Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure

(1st Edition)

(Tentative Translation)

April 4, 2018

(Revised May 23, 2019)

Cybersecurity Strategic Headquarters

Critical Infrastructure Expert Panel

Government of JAPAN

(Blank)

Index

1. Introduction

<1> Purpose for the Formulation of This Guide

Information and communications technology has become a widespread phenomenon in the people's living, and it is increasingly becoming an indispensable element in the provision of various services in business activities. Along with the advancement of information and communications technology, the quality of various services and productivity have improved, and there are growing opportunities for the creation of new services. On the other hand, information security risks are also growing, including the growing incidences of information leakage due to cyberattacks and damage caused by service suspensions. Amidst this environment, among CI operators that provide services, which serve as the foundation of the people's living and socioeconomic activities, and there is a need to recognize information security risks as one of the risks of businesses and put in place the appropriate information security measures based on the active involvement of the management.

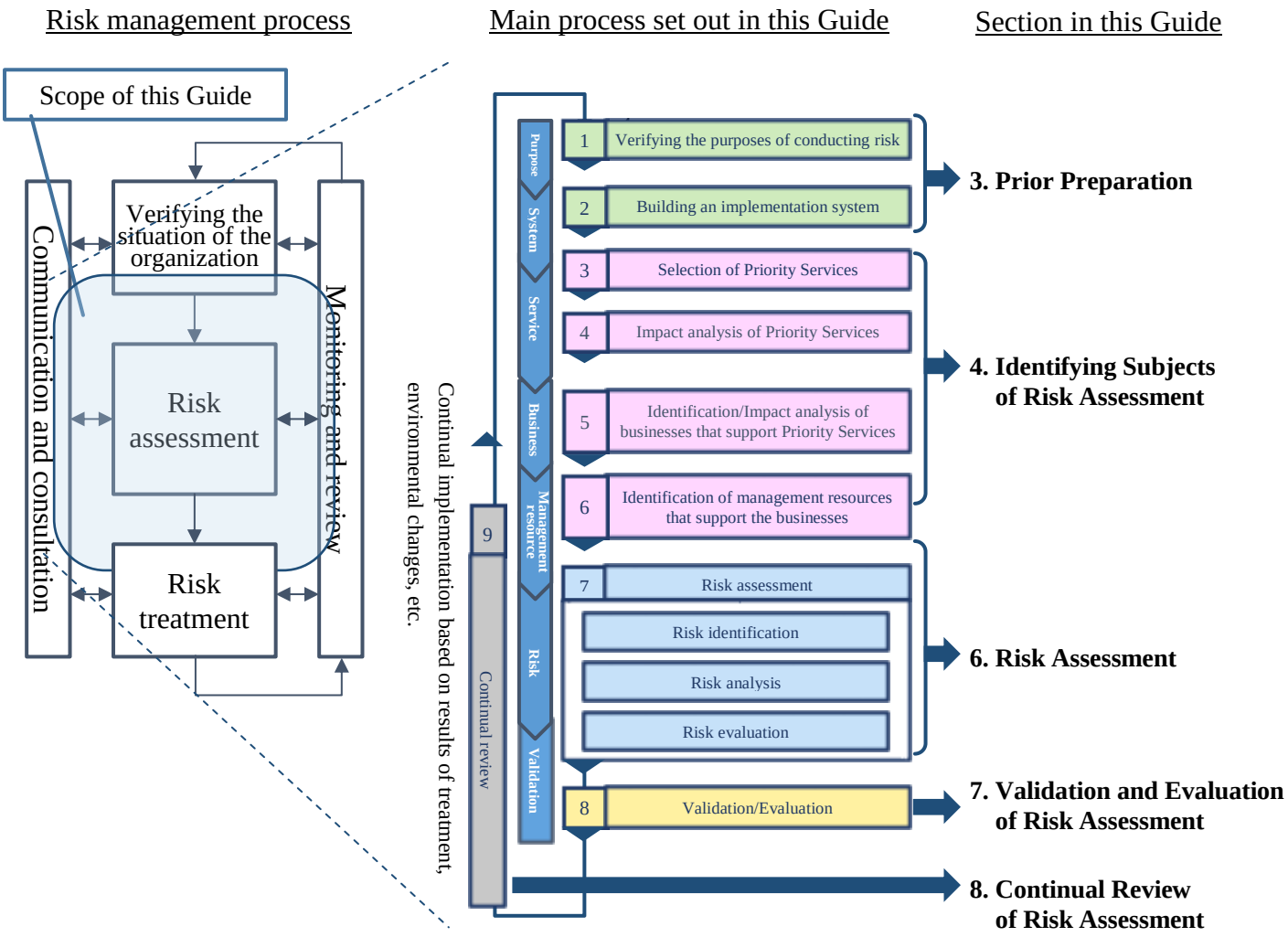
Information security risks are constantly changing as a result of changes in the business environment and demands from interested parties. For this reason, in ensuring the appropriate implementation of the necessary information security measures, it is important to periodically conduct risk assessment based on a recognition of changes to information security risks, and to strategically put in place measures based on the results of the assessment. The importance of risk assessment has already been recognized by many operators, and there is a growing trend for including the conduct of risk assessment in the information security policy established by operators. On the other hand, even while recognizing the importance of risk assessment, there are also many operators that are unable to conduct risk assessment due to reasons such as not having concrete knowledge on how to proceed. Hence, it is difficult to say that the approach of risk assessment and implementation methods have become firmly established.

In light of this situation, this Guide provides a framework for the approach toward risk assessment, in relation to ensuring information security, and for the concrete work procedures. By doing so, it aims to deepen understanding of risk assessment among CI operators, contribute to improving the precision and standard of risk assessment, and at the same time, promote the implementation of information security measures independently by CI operators.

<2> Scope of This Guide

This Guide sets out the main process of risk assessment, which comprises primarily of risk identification, risk analysis, and risk evaluation. At the same time, it also covers the process for identifying the subjects of risk assessment, and a part of the process apart from risk assessment that are included in risk management.

Figure 1 Scope of This Guide



<3> Scope of Application of This Guide

(1) Applicable Operators

This Guide is oriented for utilization by CI operators. In cases where risk assessment methods that focus on certain fields and domains of business have already been established, this Guide is to be used while prioritizing existing manuals and guidelines, and it is recommended to use the contents provided in this Guide to complement existing contents where necessary.

(2) Subjects of Risk Assessment

In the risk assessment set out in this Guide, the risks that are identified consequences of an event (Priority Service outages that are caused by natural disasters or cyberattacks, etc.) related to information assets such as information, information systems, and control systems that make use of IT, which are owned, used or managed by CI operators for the purpose of carrying out the work that is necessary for the provision of their services (hereinafter referred to as information security risks), are applicable.*

(*) CI operators are considered to have risks other than information security risks. This Guide introduces the methods for risk assessment that are limited to the scope of information security risks, but when making decisions on risk evaluations and identifying the options for risk treatment in actuality, it is also important to take into consideration risks other than information security risks, and to consider them comprehensively.

<4> Composition of This Guide

This Guide is composed of the following documents.

Figure 2: Document Composition for This Guide

Document title		Overview
Risk Assessment Guide Based on the Concept of Mission Assurance in Critical Infrastructure		This document
Annex 1	Examples of the Consequences of an Event that Interfere with Businesses	Reference material that sets out examples of the consequences of events leading to interference with businesses (Priority Service outages), based on the perspective required of management resources in order to maintain the business.
Annex 2	Examples of Events That Could Give Rise to Consequences (Threats)	Reference material that sets out the main examples, along with the basic categories of events that could give rise to consequences.
Annex 3 (Forms) (*)	(Form 1) Verifying the Purpose of Conducting Risk Assessment	Worksheet for setting the activity goals of the organization, and for verifying the purposes and policies for conducting risk assessment (including sample form).
	(Form 2) Selection of Priority Services	Worksheet for analyzing the expectations of interested parties, corporate social responsibility (CSR), and legal requirements (compliance), and for selecting the Priority Services (services that are subjected to risk evaluation) (including sample form).
	(Form 3) Impact Analysis for Priority Services	Worksheet for analyzing the lowest minimal tolerance for the scope and standard of services based on the perspective of safety (= a state in which there are no intolerable risks), as an impact analysis of Priority Services, as well as the impact over time in the event that service provision is suspended, and for making decisions on the Maximum Tolerable Period of Disruption (MTPD) (including sample form).
	(Form 4) Identification of Businesses That Support Priority Services, and Impact Analysis of the Businesses	Worksheet for identifying the businesses necessary for the provision of Priority Services, clarifying the minimal level that should be maintained for these businesses, and estimating the impact and MTPD in the event that these businesses are suspended (including sample form).
	(Form 5) Identification of Management Resources That Support the Businesses	Worksheet for clarifying the management resources needed to maintain the minimal level that should be maintained for the businesses necessary for the provision of Priority Services (including sample form).
	(Form 6) Risk Assessment Related to Management Resources	Worksheet that organizes the management resources related to the businesses necessary for the provision of Priority Services, and for identifying, analyzing, and evaluating the risks toward the continuation of these businesses (including sample form).
Annex 4	Examples of Risk Sources	Reference material that sets out the basic categories of risk sources, alongside with the main examples.

(*) In this Guide, Forms 1 to 6 are collectively known as the “Risk Assessment Sheets.”

2. Overview of Risk Assessment

<1> Perspective and Approach of Risk Assessment based on the Concept of Mission Assurance

There are many methods of risk assessment that have already been established and that have a strong implementation track record. However, there is no single "correct answer" in the application of these methods and their implementation procedures. Hence, when operators put risk assessment into practice, it is necessary to fully consider which method to adopt in order for their organization to identify, analyze, and evaluate risks more effectively and efficiently, and to decide on which method to adopt based on their own judgement. When considering this and making this decision, it is important for CI operators, which provide services that fulfill an indispensable role and function in the socioeconomic systems, to take into consideration the concept of mission assurance.

> Concept of Mission Assurance (Excerpt from The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition))
>
> CI services are the very basis of national life and socioeconomic activities and suspension thereof may have a direct and serious negative effect on the safety and ease of the general public. Therefore, stakeholders are required to make efforts to ensure safe and continuous provision of CI services (mission assurance).
>
> Mission assurance in this Cybersecurity Policy does not mean to oblige stakeholders to make a firm commitment to ensuring CIP or maintaining CI functions, but to have them assume their responsibilities in the process of protecting CI services and maintaining the functions thereof. This is the concept to require each stakeholder to properly make efforts for necessary cybersecurity measures.

As explained earlier, this Guide is drawn up based on the assumption that it is to be used by CI operators. Therefore, as a method of risk assessment that is based on the concept of mission assurance, it introduces procedures for putting into practice the identification, analysis, and evaluation of information security risks from the perspective of "ensuring a state that is free from intolerable risks (= safety) and continuing with service provision, in order to determine and demonstrate the roles and functions that the respective CI operators should fulfill within a socioeconomic system."

CI operators need to carry out risk assessment proactively and independently. However, as the precision and standard of their efforts are dependent upon the capacity of the respective CI operators, this Guide aims to ensure a certain level of precision and standard for risk assessment conducted by CI operators, by presenting a perspective of risk assessment based on the concept of mission assurance and the work procedures for reference purposes.

The procedures for risk assessment introduced in this Guide are applicable not only to CI operators, but also to operators in various fields including leading medium-sized enterprises and small and medium-sized enterprises.

<2> Risk Assessment Policy based on the Concept of Mission Assurance

As explained in 2. <1> Perspective and Approach of Risk Assessment Based on the Concept of Mission Assurance, this Guide aims to help CI operators identify, analyze, and evaluate risks as well as identifying the options for risk treatment and visualizing residual risks in order to strategically optimize risks based on the concept of mission assurance. With this in mind, the methods of risk assessment introduced in this Guide follow the policy set out below.

(I) Viewpoint of Risks

CI operators define, as the objectives of their management strategy, the maintenance and continuation of the provision of the necessary services for demonstrating the roles and functions they should fulfill within the socioeconomic system, and therefore perceive risks as “effect of uncertainty on objectives” (based on the definition set out in ISO 31000:2018). However, based on the concept of mission assurance, the risks that this Guide is applicable to are limited to risks that have a negative impact, that is, risks that lead to an undesirable consequence.

(II) Deductive Risk Assessment based on the Concept of Mission Assurance

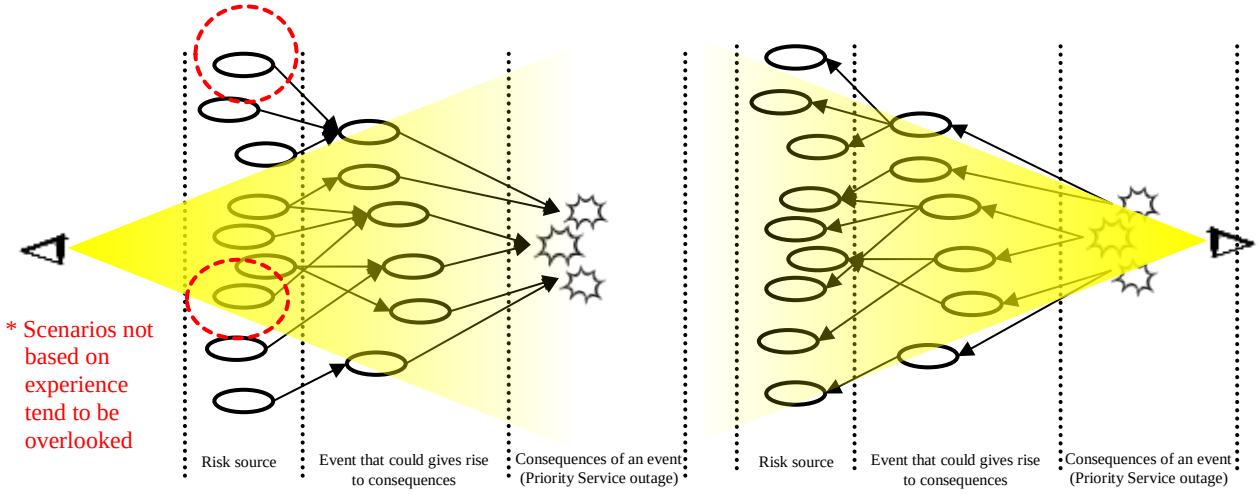
By averting our eyes from events with a low probability of occurrence (even for events that could lead to critical situations in the event that they do occur, these are not deemed to be risks as they have not been experienced in the past, or because they have a low probability of occurrence), the consequences of such an event may result in unexpectedly major disruption. This was the case for the Great East Japan Earthquake. Drawing lessons from the experience of this earthquake, based on the premise of the viewpoint of risk set out in (I) above and on the concept of mission assurance, NISC has adopted an approach that identifies the services necessary for maintenance and continuation in order for CI operators to demonstrate the roles and functions they should fulfill within the socioeconomic system, and while ensuring a state that is free of intolerable risks (=safety), analyzes and evaluates the requirements for management resources and businesses necessary to continue with the provision of the services. Upon conducting all these, it also deductively identifies, analyzes, and evaluates from the consequences of the events to the risk sources that have an impact on these.

(III) Consideration for Efficient Work Processes (Combination with an Inductive Approach)

Although a deductive detailed risk analysis approach is adopted, a method that identifies the combination of hypothetical threats (events) with vulnerabilities (risk sources), through an inductive approach such as event tree analysis, which is implemented by many CI operators, can also have a certain degree of effectiveness on the analysis of risks presumed by CI operators. Accordingly, through the combination with such inductive methods that have proven results, consideration is given to enable the implementation of efficient work processes. Specifically, also taking into consideration the possibility that events that could give rise to consequences and risk sources are overlooked in situations of heavy workload within the CI operators or inadequate knowledge or experience on the part of the worker, this Guide seeks to contribute to enhancing the efficiency of work processes and ensuring comprehensiveness by providing the following materials as points to be aware of in risk analysis: Examples of the Consequences of an Event That Interfere with Businesses (Annex 1), Examples of Events That Could Give Rise to Consequences (Threats) (Annex 2), and Examples of Risk Sources (Annex 4).

Figure 3: Comparison of Approaches

	Inductive approach	Deductive approach
Overview	A method that presumes a risk source and clarifies what happens to the various events and consequences of an event that are derived from that risk source. (Concept) **X** × **Y** → ?	A method that presumes the consequence of an event and which clarifies the various events and risk sources that lead to that consequence. (Concept) **Z** ← ? × ?
Main method	Event tree analysis	Fault tree analysis
Pros	Excellent at individual scenario analysis, and is able to gain effective insight into the matters to be dealt with corresponding to each scenario.	Able to gain a comprehensive understanding of the overall picture through the deductive analysis of scenarios concerning the consequences of an event.
Cons	Difficult to cover all risk sources comprehensively.	In cases with a complex configuration of services provided and work processes, the combinations of analysis results increase exponentially, resulting in a heavy workload.



Inductive approach　　Deductive approach

(IV) Validation

In risk assessment, there is no single and absolute “correct answer”; rather, the results of the assessment can include biases based on the worker’s standpoint as well as knowledge and experience. In cases where the work is shared among many workers, variances may be observed in the granularity and precision of the risk assessment results produced by each worker. Taking these characteristics into consideration, a process called “validation” is incorporated to verify that the contents of the risk assessment conducted are appropriate and relevant toward the achievement of the objective. This validation process includes confirmation of the division of labor related to the management resources and the work supporting the provision of services, and communication between the stakeholders aimed at facilitating mutual understanding of the connections between departments.

(V) Continuous Review of Risk Assessment

In an environment known as VUCA, which lacks transparency, it is necessary to build mechanisms that enable risk management efforts to function continuously and effectively, in order for CI operators to respond flexibly and appropriately to changes in the environment. Thus a process is incorporated, which establishes the necessary systems for the continuous review of the risk assessment results based on validation.

<3> Framework of Risk Assessment based on the Concept of Mission Assurance

Based on the policy set out in 2. <2> Risk Assessment Policy based on the Concept of Mission Assurance, the following figure presents the framework of risk assessment based on the concept of mission assurance.

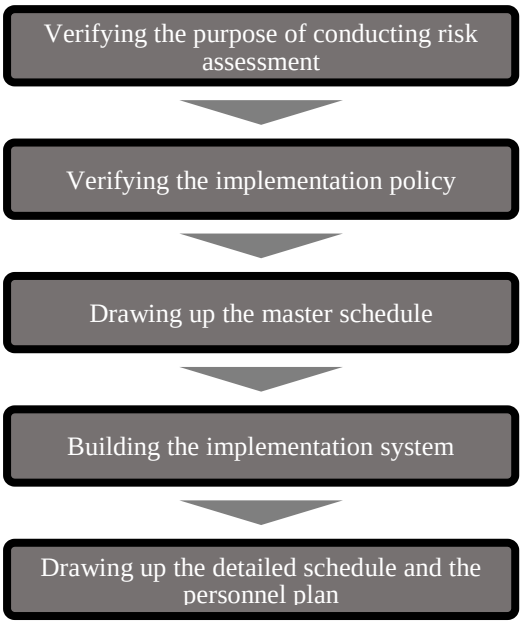
Figure 4: Framework of Risk Assessment based on the Concept of Mission Assurance

Policy	Risk assessment process
(I) Viewpoint of Risks (II) Deductive Risk Assessment based on the Concept of Mission Assurance	4. Identification of the subjects of risk assessment 6. Risk assessment
(III) Consideration for Efficient Work Process (Combination with an Inductive Approach)	(Annex 1) Examples of the Consequences of an Event that lead to Interference with Businesses (Annex 2) Examples of Events That Could Give Rise to Consequences (Threats) (Annex 4) Examples of Risk Sources
(IV) Validation	7. Validation/Evaluation of risk assessment
(V) Continuous Review of Risk Assessment	8. Continuous review of risk assessment

3. Prior Preparation

This chapter sets out the procedures for prior preparations in order to conduct risk assessment based on the concept of mission assurance.

<1> Steps



<2> Contents

(1) Verifying the Purposes of Conducting Risk Assessment

Establish the activity goals of the organization, and verify the purposes for conducting risk assessment for the organization based on these goals. In risk assessment based on the concept of mission assurance, the basic purposes of conducting risk assessment are to establish the organization's activity goals, based on the perspective of continuing to provide the services necessary for the organization to demonstrate the roles and functions it should fulfill within the socioeconomic system, while ensuring a state that is free from intolerable risks (= safety), and to identify, analyze, and evaluate risks in order to strategically optimize risks against those goals, as well as to visualize residual risks.

<Using the Risk Assessment Sheets>

Using "Form 1: Verifying the Purposes of Conducting risk assessment," verify the purposes for conducting risk assessment through the process of organizing the roles and functions that interested parties expect from the organization as a CI operator.

(2) Verifying the Implementation Policy

Establish the organization's policy for conducting risk assessment (*), and verify this within the management and the relevant departments. When doing so, the organization may formulate its implementation policy referring to the framework for risk assessment based on the concept of mission assurance introduced in this Guide.

(*) In this Guide, the policy for conducting risk assessment refers to a policy on the scope and procedures for the activities necessary in order to achieve the objectives of the risk assessment, and which have been agreed upon within the management.

<Using the Risk Assessment Sheets>

Using "Form 1: Verifying the Purposes of Conducting risk assessment," verify the implementation policy alongside the verification of the purposes for conducting risk assessment.

(3) Drawing Up the Master Schedule

Once the policy for conducting risk assessment has been formulated, decide on the period for the implementation of the respective work processes as a part of the implementation policy, and draw up a work schedule (master schedule) for all the risk assessment activities.

Risk assessment includes processes that require authorization from the management. In drawing up the master schedule, it is important to establish situations that serve as important markers of progress management as milestones, and to make adjustments so that the schedule takes these milestones into consideration.

The master schedule is an important baseline that serves as the premise for progress management. It is also the premise for the subsequent procedures of building an implementation system, formulating detailed schedules within each responsible department, and deploying personnel.

(4) Building the Implementation System

Build an implementation system based on the policy for the conduct of risk assessment and the master schedule. When building the implementation system, taking into account the fact that risk assessment based on the concept of mission assurance is an important activity in the management strategy, it is important for the management, as the highest authority in the risk assessment process, to take the lead in promotion and management.

Figures 5 and 6 show a hypothetical implementation system and hypothetical departments in charge of each step in the process (examples) formulated in this Guide.

In Steps 1 to 3 in Figure 6, it is particularly important for the implementing body to communicate regularly with the management, and take action based on an understanding of the policy of risk management for the entire organization. Furthermore, the implementing body in each step of the process does not carry out work in an isolated manner within a specific department; instead, it is important to build mechanisms that facilitate the progress of the work and appropriate communication between the relevant departments, including accurate reports and advice to the management, and then work in cooperation on each step.

Figure 5: Implementation System for Risk Assessment (Example)

System		Role	Main department in charge
Coordination	Risk Assessment General Manager	Ultimately responsible for the achievement of the objectives of risk assessment.	CEO
Audit	Risk Assessment Audit Department	Verifies the validity in the management and promotion of risk assessment from the third-party viewpoint, and assists the Risk Assessment General Manager in decision-making.	Internal Audit Dept.
Management	Risk Assessment Management Director	Responsible for the operational management of risks, and reports to the Risk Assessment General Manager on the results of risk assessment, etc.	CRO
	Risk Assessment Managing Department	Assists the Risk Assessment Manager, and is responsible for the operational management of risks.	Risk Management Dept. Business Administration Dept.
Promotion	Risk Assessment Promotion Manager	Responsible for the promotion of risk assessment.	CIO/CISO
	Risk Assessment Promotion Secretariat	Supervises the Risk Assessment Promotion Department, and is responsible for the overall coordination of risk assessment across the respective departments.	IT Planning Dept.
	Risk Assessment Promotion Department	Implementing body of risk assessment.	Planning Dept. Service Dept. Business Dept. Information Systems Dept.

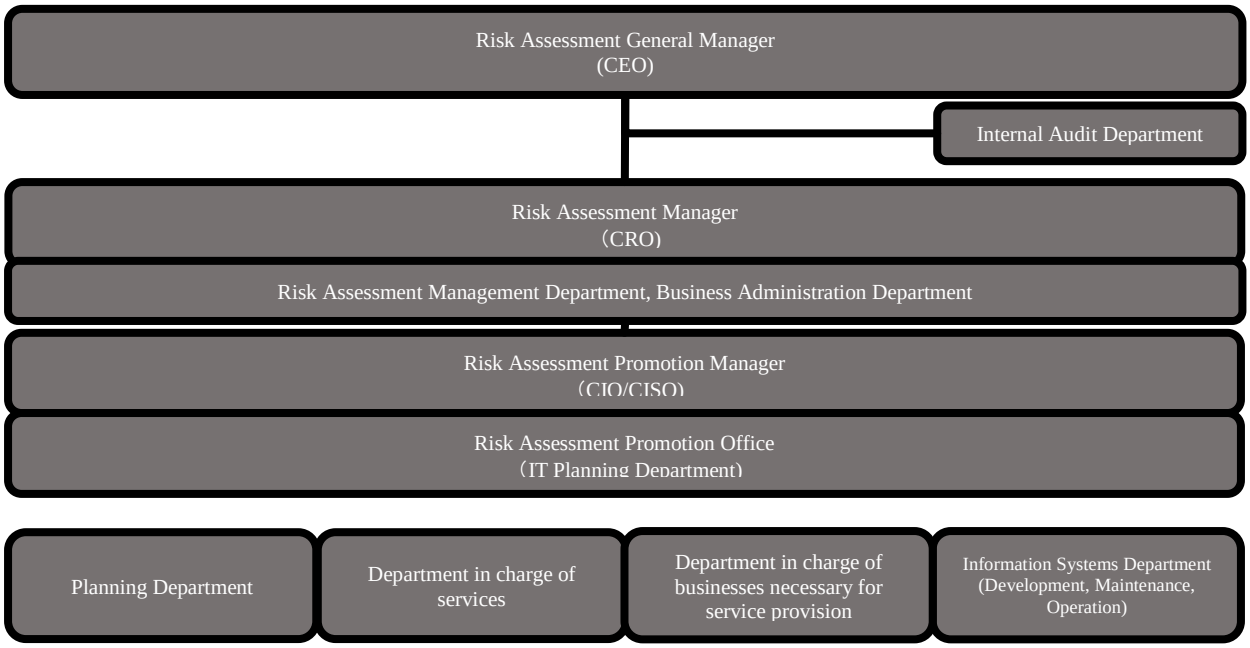


Figure 6: Departments in Charge for Each Step (Example)

STEP	Subject of evaluation	Department in charge of corporate planning	Department in charge of services	Department in charge of businesses necessary for service provision	
		Eg. Corporate Planning Dept. Risk Management Dept.	Eg. XX Business Department	Eg. Sales Dept., Technological Development Dept., R&D Dept., System Dept.	
STEP1: Decision on activity goals	Goals	◎			
STEP2: Selection of Priority Services	Services	◎	○		
STEP3: Impact analysis of Priority Services	Services	○	◎		
STEP4: Identification/Impact analysis of businesses that support Priority Services	Services ⇒ Business		◎	○	
STEP5: Identification of management resources that support businesses	Business ⇒ Management resource			◎	
STEP6: Risk assessment	Management resource ⇒ Risk	○	○	○ (User dept.)	◎ (System dept.)

◎: Main dept. in charge (coordination, etc.)
○: Secondary dept. in charge (Verification of results, etc.)

(5) Drawing Up the Detailed Schedule and the Personnel Plan

Once the implementation system has been fixed, and the departments responsible for each step of the process have been decided, the respective departments in charge should draw up a detailed schedule and a personnel plan (selection of persons in charge of the work and assignment of work).

In personnel planning, in addition to securing experts in areas such as service, work process, and system, there is also a need to consider securing persons-in-charge who can serve as liaisons with the relevant departments, based on the reporting line established within the organization.

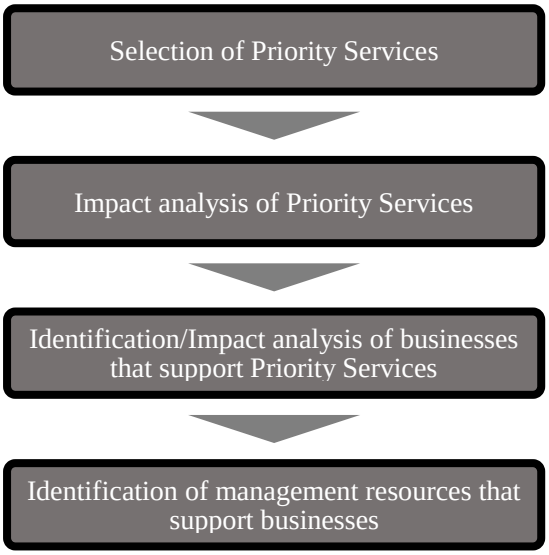
4. Identifying Subjects of Risk Assessment

This chapter sets out the procedures for implementing processes related to identifying the subjects of the risk assessment.

The subjects of risk assessment, based on the concept of mission assurance, are determined by identifying the services necessary for the continued provision of services in order for the CI operator to demonstrate the roles and functions it should fulfill within the socioeconomic system, while ensuring a state that is free of intolerable risks (= safety), and based on the results of analyzing and evaluating the work processes and the requirements for the relevant management resources necessary to achieve this.

This series of work processes are also works to analyze the risk attitude and risk tolerance, which forms the premise for the evaluation criteria (risk criteria) in conducting the subsequent risk evaluation, by capturing the value-chain and supply-chain as well as their impact on the business.

<1> Steps



<2> Implementation Procedures

(1) Selection of Priority Services

With regard to services handled by CI operators, evaluate the degree of importance (order of priority) of services based on the concept of mission assurance, and identify the services that are subject to risk assessment (Priority Services), based on a comprehensive consideration of factors such as positioning from the management perspective (positioning in terms of business management, such as contribution to business performance and dependence of the business on it), needs and expectations of interested parties (customers, suppliers, shareholders, local communities, etc.), corporate social responsibility (CSR), and legal requirements (compliance). The CI services (CISs) listed in Annex 2 of the Guidelines for Safety Principles (5th Edition) (hereinafter referred to as "Safety Principles") are assumed to have been identified as Priority Services.

<Using the Risk Assessment Sheets>

Using "Form 2: Selection of Priority Services," consider the expectations regarding services that interested parties have and legal requirements, and identify the services that are important to operators.

(2) Impact Analysis of Priority Services

With regard to Priority Services, define the minimum tolerable level for the scope and standard of services based on the perspective of safety (= a state that is free of intolerable risks), in order to fulfill the requirements analyzed in "(1) Selection of Priority Services." Furthermore, analyze and evaluate the situations that arise when the provision of Priority Services is completely suspended, as well as the degree of impact with the passing of time, and estimate the Maximum Tolerable Period of Disruption (MTPD) for Priority Services.

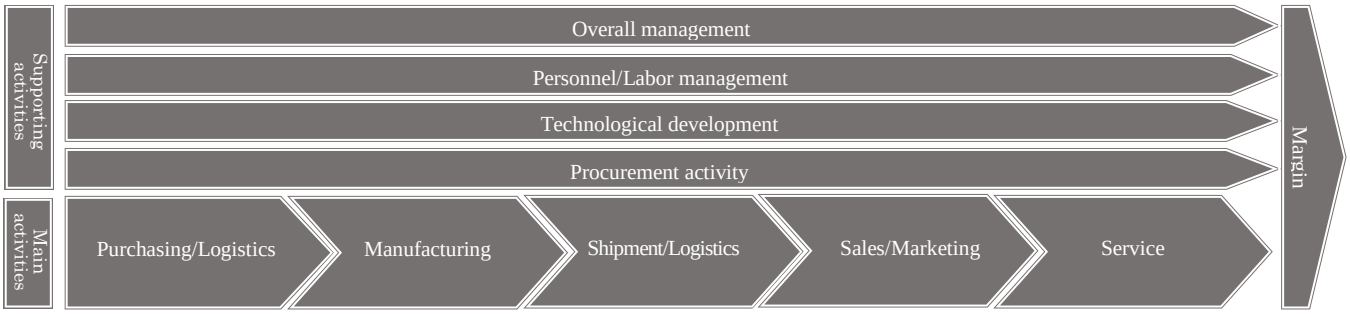
<Using the Risk Assessment Sheets>

Using "Form 3: Impact Analysis for Priority Services," define the minimum tolerable level for the scope and standard of services for fulfilling the expectations of interested parties in the services and other requirements, and analyze and evaluate the impact in the event of a complete suspension in the provision of services. Then, estimate the Maximum Tolerable Period of Disruption (MTPD) for services.

(3) Identification, and Impact Analysis, of Businesses that Support Priority Services

Identify the businesses that are necessary for the provision of Priority Services, and define the minimum tolerable level for these businesses (capacity utilization, rate of operation, etc.). When doing so, it is recommended that the work is carried out while bearing in mind the value-chain of the organization. It is also preferable to conduct an analysis and evaluation of the situations that arise when the business is completely suspended, as well as the degree of impact with the passing of time, and then estimate the Maximum Tolerable Period of Disruption (MTPD) for businesses.

Figure 7: Example of a General Value-Chain



<Using the Risk Assessment Sheets>

Using "Form 4: Identification of Businesses that Support Priority Services, and Impact Analysis of the Businesses," define the scope and standard of the businesses necessary for the provision of Priority Services, in order to fulfill the expectations of interested parties in the services and other requirements, and analyze and evaluate the impact if the business is completely suspended. Then, estimate the Maximum Tolerable Period of Disruption (MTPD) for businesses.

(4) Identifying the Management Resources That Support the Businesses

Identify the management resources that are necessary for the execution of the businesses identified in "(3) Identification, and Impact Analysis, of Businesses That Support Priority Services," and analyze the necessary requirements (conditions, quantity, etc.).

<Using the Risk Assessment Sheets>

Using "Form 5: Identification of Management Resources That Support the Businesses," identify the management resources (information assets, facilities, personnel, lifelines that are owned, used or managed for the execution of businesses necessary for the provision of Priority Services) that support the businesses identified in "Form 4: Identification of Businesses That Support Priority Services, and Impact Analysis of the Businesses."

5. Formulating the Risk Evaluation Policy

This chapter sets out the procedures for carrying out work related to the methods of risk analysis and the formulation of criteria for risk evaluation (risk criteria).

There are various methods of risk evaluation, but in conventional information security risk evaluation, the general method used was to measure the significance of the risk from the perspective of protecting information assets, using the formula "Value of information assets (evaluated based on confidentiality, integrity, and availability) × Size of threat × Degree of vulnerability." This method involves the identification, analysis, and evaluation of risks using an inductive approach of first identifying the information assets, then matching those information assets with hypothetical events drawn up by the organization itself (security incidents). This inductive approach is easy to apply to the empirical work of matching events with past experiences, and could be described as an approach that aims to prevent recurrence of past incidents. Meanwhile, in this method, the processes from identifying the information assets to finally evaluating the risks are completed within the information systems department, thereby raising concerns that it may not be able to adequately analyze and evaluate the impact on services provided based on the concept of mission assurance.

In view of the presence of such issues in conventional methods of evaluating information security risks, this Guide sets out risk evaluation policy (analytical methods and evaluation criteria) that take into consideration the degree of impact, in light of the service levels and business requirements that are demanded of Priority Services based on the concept of mission assurance.

<1> Steps

<2> Procedures

(1) Review of Risk Analysis Methods

This Guide introduces risk analysis using the risk mapping and risk scoring methods, which are adopted by many CI operators.

Generally, risk mapping is an analytical method that involves positioning risks on a matrix with the "degree of impact" and "frequency of occurrence (probability of occurrence, ease of occurrence)," or "value of information assets" and "size of threat × degree of vulnerability" on the horizontal and vertical axes respectively, and then grasping the relative priority relationships of those risks. Risk scoring, on the other hand, is an analytical method that clarifies the risks that need priority treatment, by according a certain score that corresponds to the seriousness of each element and multiplying them.

In risk assessment based on the concept of mission assurance, in order for the organization to demonstrate the roles and functions it should fulfill within the socioeconomic system, the organization's activity goals are established based on the perspective of continuous service provision while ensuring a state that is free from intolerable risks (= safety), and the risks against the goals are strategically optimized. To that end, risks are identified, analyzed, and evaluated, and residual risks are visualized. This is the basic purpose for conducting risk assessment. Hence, the "degree of impact that the consequences of events have on Priority Services and

businesses" and "Frequency of occurrence of events (probability of occurrence, ease of occurrence)" are established as the axes for evaluation.

With regard to the degree of impact that the consequences of events have on Priority Services and businesses, conduct a comprehensive evaluation based on the results of the analysis carried out in Chapter 4. Identifying Subjects of Risk Assessment, for example by using the following elements.

Figure 8: Main Elements for the Evaluation of Degree of Impact

Elements for the evaluation of degree of impact	Overview
Predicted scope and degree of impact on businesses	Evaluate the scope and degree of impact that the consequences of events are expected on the businesses that support Priority Services. With regard to the impact on businesses, consider also the impact on the respective requirements analyzed in Chapter 4. Identifying Subjects of Risk Assessment.
Predicted recovery time	Evaluate the predicted recovery time in cases where the businesses that support Priority Services are suspended or obstructed due to the consequences of events.
Predicted cost of response	Evaluate the predicted costs required in the recovery of those businesses and the management of the consequences of the events in cases where the businesses that support Priority Services are suspended or obstructed due to the consequences of events.
Predicted scope and degree of impact on human lives and the environment	Evaluate the scope and degree of impact that could arise as a result of the consequences of events, in the event that there is a possibility of damage to human lives and the environment.

(2) Deciding on the Risk Criteria

Risk criteria are criteria that serve as a yardstick for evaluating the seriousness of risks, and refer to decision indicators established beforehand with the aim of preventing the occurrence of variance in the evaluation results caused by the personnel in charge of risk assessment work.

Based on the concept of mission assurance, risk criteria are based on the ideas of enabling the fulfilment of the minimum acceptable level of Priority Services as well as recovery within the tolerable period of disruption while taking into consideration the perspective of ensuring a state that is free from intolerable risks (= safety). An illustration of how the risk criteria are established, in cases where the axes of evaluation are "degree of impact that the consequences of events have on Priority Services and businesses" and "frequency of occurrence of events (probability of occurrence, ease of occurrence," are shown on the following page.

Risk criteria must be established corresponding to the purposes of the risk assessment. Furthermore, in the continual review of risk assessment, it is also important to review the settings of the criteria depending on factors such as changes to the environment.

<Illustration of how risk criteria are established>

Cases including those where a business supporting Priority Services has been suspended, where recovery of a business is difficult, or where there is significant damage to human lives or the environment, are evaluated as cases where the consequences of events have a serious impact. In these cases, even if the frequency of occurrence were evaluated as being extremely low, risk criteria are established as "5 or higher" so that the risk can be subjected to risk treatment.

Figure 9: Illustration of How Risk Criteria Are Established

(Example)

Frequency of occurrence		Expected frequency of occurrence of events
5	Extremely high	Frequent
4	High	Occurs about once a year
3	Moderate	Occurs about once every few years
2	Low	Occurs about once every 10 years
1	Extremely low	Occurs in extremely rare and exceptional circumstances

* If risk criteria is 5 or higher, the risks corresponding to the yellow cells are subjected to risk treatment.

Expected frequency of occurrence of events						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Degree of impact on consequences of events				

Degree of impact		Degree of impact (The degree of impact is determined through a comprehensive consideration of the following elements.)			
		Scope and degree of impact on businesses	Predicted recovery time	Cost required for response	Scope and degree of impact on human lives and environment
5	Serious impact	The business in question is suspended.	Recovery of the business itself is difficult.	The operator has to take on heavy costs (including losses during the suspension of the business) that are required for the recovery of the business and to deal with the consequences of the event (including payment of compensation related to information leakage and arrangement for alternative means, etc.).	Results in multiple fatalities.
4	Significant impact	The business in question is obstructed, and it is difficult to maintain the minimum standard for the business.	Recovery of the business within the MTPD of the business is difficult.	The operator has to take on significant costs that are required for the recovery of the business and to deal with the consequences of the event.	Results in one fatality or multiple serious injuries.
3	Moderate impact	The business in question is obstructed, and there are concerns that it may not be possible to maintain the minimum standard for the business.	Recovery of the business within the MTPD of the business is possible.	The operator has to take on moderate costs that are required for the recovery of the business and to deal with the consequences of the event.	Results in one serious injury or multiple light injuries.
2	Small impact	The business in question is obstructed, but the minimum standard of the business is maintained.	Recovery of the business is possible within a time that causes minor obstruction to the business.	The operator has to take on a small amount of costs that are required for the recovery of the business and to deal with the consequences of the event.	Results in one light injury.
1	Minor impact	–	Recovery of the business is possible within a time that does not cause any obstruction to the business.	The operator has to take on minor costs that are required for the recovery of the business and to deal with the consequences of the event.	–

6. Risk Assessment

This chapter sets out the procedures for the organization of the management resources that are related to the businesses necessary for the provision of Priority Services, and the implementation of work for the identification, analysis, and evaluation of risks related to those management resources.

<1> Steps

<2> Procedures

(1) Identification of Risks

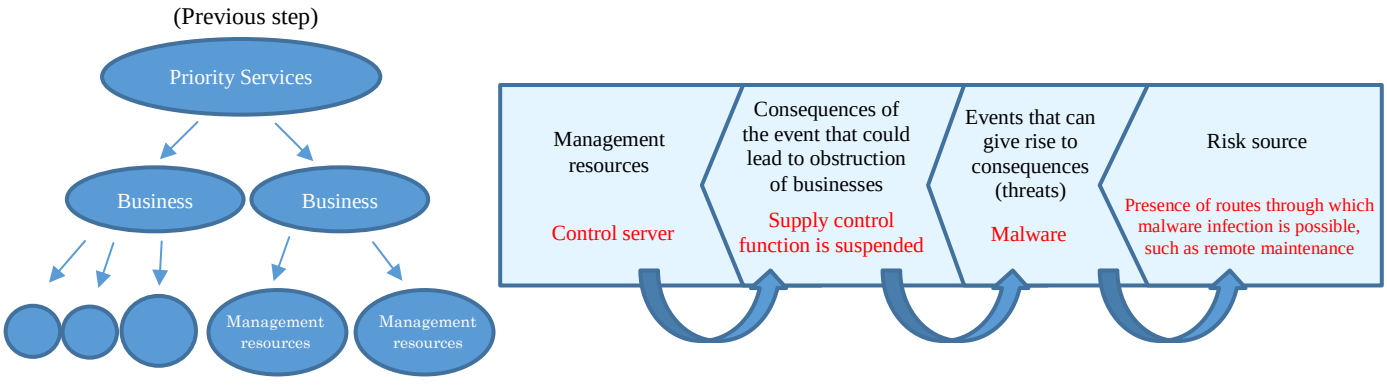
Follow the steps shown below to identify the risk source deductively.

(i) For the management resources that are related to the businesses necessary for the provision of Priority Services, write down the consequences of events that lead to the obstruction of businesses.

(ii) Write down the events that could give rise to consequences for (i) above.

(iii) Write down the risk source that could give rise to the consequences in (i) above, along with the events in (ii) above.

Figure 10: <Example> Illustration of Work Flow when Control Server is the Management Resource



<Using the Risk Assessment Sheets>

Using "Form 6: Risk Assessment Related to Management Resources," identify the consequences of events that could obstruct businesses, the events that could give rise to these consequences, and the risk source, for each management resource (information asset) identified using "Form 5: Identification of Management Resources That Support the Businesses."

(2) Risk Analysis

Follow the steps below to analyze the "degree of impact that consequences of events have on Priority Services and businesses" and the "frequency of occurrence of events," and derive the value of residual risks, which is an input for the risk evaluation.

(i) With regard to the possible impact that the consequences of events could have on Priority Services and businesses, write down the contents, and carry out an evaluation based on the evaluation axes established in Chapter 5. Formulating the Risk Evaluation Policy. (*)

(ii) For the frequency of occurrence of events, carry out an evaluation based on the evaluation axes established in Chapter 5. Formulating the Risk Evaluation Policy. (*)

(iii) Based on the results of (i) and (ii) above, derive the values of residual risk for each risk source based on the evaluation matrix established in Chapter 5. Formulating the Risk Evaluation Policy.

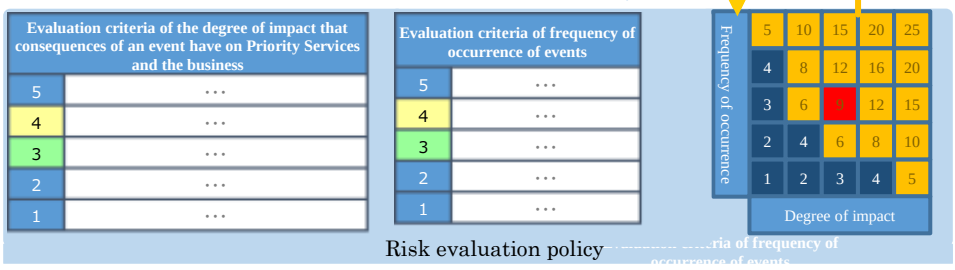
(*) Even in cases where some forms of measures have been put in place, take into consideration the nature of information security measures that their effectiveness tends to become obsolete with technological progress, and conduct both an evaluation prior to the implementation of countermeasures (inherent risks) and after the implementation of countermeasures (residual risks).

Figure 11: <Example> Illustration of Risk Analysis

Risk analysis using risk criteria (refer to Figure 9)

(Example)

Risk identification			Degree of impact that the consequences of an event have on Priority Services and the business				Frequency of occurrence of events			Value of residual risks
Consequences of an event that lead to obstruction to the business	Events that could give rise to consequences	Risk source	Impact of consequences of an event	Before countermeasures	Countermeasures that are currently in place	After countermeasures	Before countermeasures	Countermeasures that are currently in place	After countermeasures	
Leakage of customer information	Bringing out of internal information	Environment that allows people with malicious intentions to take information out	While not directly related to the suspension of the business, the need to conduct investigations and be accountable significantly obstructs the execution of the regular business.	4	Operators of systems that handle customer information are restricted, and the service level where each operator is allowed to operate is also limited to the minimum necessary level.	3	4	Provide employee education	3	9
			:	:	:	:	:	:	:	:



<Using the Risk Assessment Sheets>

Using "Form 6: Risk Assessment Related to Management Resources," analyze and evaluate the degree of impact that the consequences of events have on Priority Services and businesses, as well as the frequency of occurrence of events, and derive the values of the residual risks that are an input for risk evaluation.

(3) Risk Evaluation

Follow the steps below to identify the risks that will be subject to risk treatment. Here, from among the risks identified, select the risks that will be subjected to risk treatment based on company-wide decision-making by the management, and clarify the party within the organization that is responsible for the risks. This is the objective of the process.

(i) Identify the risks with value of residual risk that is higher than the risk criteria, as the subjects of risk treatment.

(ii) From among the risks with value of residual risk that is below the risk criteria, identify those that are subjected to risk treatment after taking into consideration individual matters (*).

(*) Risk criteria are ultimately guidelines used for assessing the order of priority of risk treatment, and the appropriate judgement should be made corresponding to individual matters when actually conducting a risk evaluation.

(iii) For the risks identified in (i) and (ii) above (risks that are subject to risk treatment based on company-wide decision-making by the management), determine the risk owners (departments or divisions, or executives and staff, that are responsible for managing those risks).

(Note) With regard to the risks identified as risks that are subject to risk treatment in this step, monitor them periodically as subjects for company-wide decision-making by the management, carry out a re-evaluation as a part of the continual review of the risk assessment.
With regard to the risks that were not identified as subjects for risk treatment in this step, instead of not acknowledging them as risks, manage them under the responsibility of the responsible department/division or executive officers as subjects for management based on regular work or the division of official duties.

<Using the Risk Assessment Sheets>

Using “Form 6: Risk Assessment Related to Management Resources,” identify the risk source for the value of residual risks that are higher than the risk criteria, and determine the risk owners for those risks.

7. Validation/Evaluation of Risk Assessment

This chapter sets out the procedures for the validation and evaluation of risk assessment.

Variance in precision and granularity can occur in the results of risk assessment through factors such as bias due to the worker's position as well as knowledge and experience, or the division of labor among multiple workers. To eliminate such bias and variance, and to ensure that the contents implemented in the implementing body of the risk assessment are appropriate toward the achievement of the objectives, it is necessary to verify the contents of risk assessment conducted in cooperation with multiple parties concerned, and share those results.

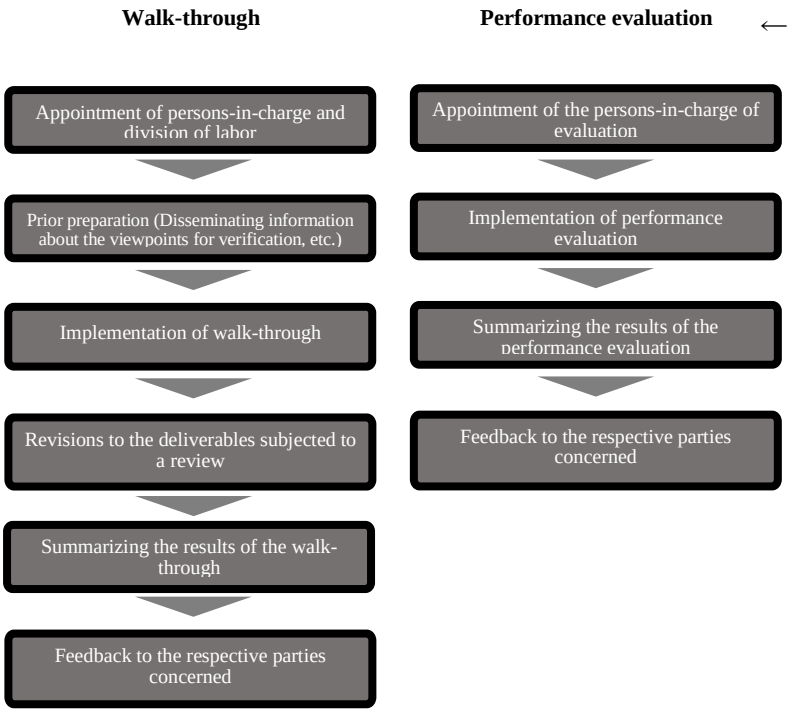
To bring about the realization of effective risk assessment, it is important to give feedback on the results to the interested parties in order to bring about improvements upon an objective evaluation of whether or not the risk assessment was conducted appropriately and adequately. Generally, in cases where evaluation is carried out for a certain project, it will be implemented from the various perspectives of structure, processes, and outcomes. However, when evaluating risk assessment, it is difficult to evaluate the effectiveness of outcomes (the extent to which the purposes of risk assessment have been achieved). Hence, verify the validity of the risk assessment by evaluating whether or not the systems for implementing the risk assessment, and the implementation procedures and activity status for risk assessment, were appropriate and adequate.

As a part of efforts toward such validation, this Guide introduces the verification of the results of analysis through "walk-through" (validation of the contents of risk assessment) and the evaluation of implementation systems and activities through "performance evaluation" (validation of risk assessment work).

Figure 12: Means of validation

Means of validation	Overview	Main implementing bodies
Walk-through (Validation of the contents of risk assessment)	In addition to verifying the contents of the risk assessment in cooperation with multiple parties concerned and confirming their validity, in order to eliminate the bias and variance in the results of the risk assessment, this method aims to share and agree on the results of the validation. It includes verification of the segregation of duties related to businesses that support the provision of services and management resources, and communication among parties concerned with the aim of facilitating mutual understanding of the status of connection between departments.	・Author of the risk assessment sheet (Risk Assessment Promotion Department) (Note) The departments responsible for the relevant businesses, departments using the management resources, legal departments, and risk management departments, etc. also participate as reviewers.
Performance evaluation (Validation of risk assessment work)	This method verifies the validity of the risk assessment by evaluating whether or not the systems for implementing risk assessment, and the implementation procedures and activity statues for the risk assessment are appropriate and adequate. (*) In this Guide, this method is called "performance evaluation," taking reference from the high level structure (HLS) of the ISO management system adopted in ISO22301 and ISO27001.	・Risk Assessment Audit Department (The department that verifies the validity of managing and promoting risk assessment from the position of a third-party such as the internal audit department)

<1> Steps



<2> Procedures

(1) Walk-through

As a means for validating risk assessment in cooperation with multiple parties concerned, the walk-through is implemented in accordance with the following flow, after the completion of work related to the previous step, 6. Risk Assessment, targeted at the series of processes from verifying the purposes of conducting risk assessment to risk evaluation. However, with regard to the target scope and timing for the implementation, for large-scale organizations to proceed with work efficiently, for example, it would be desirable to put effort into carrying out a simple walk-through in which the scope of the persons-in-charge is limited midway through the work.

(i) Appointment of persons-in-charge and division of labor

Appoint persons-in-charge who will implement the walk-through. To implement the walk-through smoothly, it is important to carry out the division of labor, and for the appropriate person-in-charge to participate in the walk-through corresponding to the duties.

Figure 13: Main Roles and Duties in the Walk-through

Role	Duties	Responsible departments (example)
Coordinator	As the role responsible for driving forward the walk-through, this party is responsible for coordination related to the appointment of persons-in-charge for the implementation of the walk-through, coordination of schedules, organizing the viewpoints for verification, and arranging for the deliverables subjected to a review. This role is also responsible for following up on the Risk Assessment Promotion Department on matters such as revisions to the results of risk assessment based on the results of the walk-through.	・Risk Assessment Promotion Secretariat
Explainer	This role is responsible for explaining to the respective persons-in-charge of implementing the walk-through, the purposes of conducting risk assessment that is visualized through the description of deliverables subjected to a review as well as the relationship with the businesses and management resources that support Priority Services and risks.	・ Author of the risk assessment sheet (Risk Assessment Promotion Department)
Reviewer	Based on the explanations from the explanatory role, this role appraises the contents related to the deliverables subjected to a review, based on the viewpoints for verification. From the perspective of minimizing variance in the grading and precision of the risk assessment results, it is necessary not only for the author of the risk assessment sheets (Risk Assessment Promotion Department), but also for parties from departments other than that of the author of the risk assessment sheets to participate, and particularly so for the departments responsible for the relevant businesses and those that use or manage the management resources. From the perspective of ensuring that Priority Services selection and risk evaluation are carried out based on a comprehensive decision, it is important to appoint a reviewer as necessary from persons in the indirect departments such as the corporate planning department, legal department, risk management department, and IR department.	・ Author of the risk assessment sheet (Risk Assessment Promotion Department) ・Planning Department ・Departments responsible for services ・Departments responsible for the businesses that are necessary for the provision of services
Recorder	This role records matters such as the contents of proceedings of the walk-through and issues that have been pointed out.	・Risk Assessment Promotion Secretariat

(*) There are also cases where the same person-in-charge serves in multiple roles, or where roles that are not described here are established.

(ii) Prior preparation (Disseminating information about the viewpoints for verification, etc.)

In order for each party concerned to verify the validity of the results of the risk assessment (contents set out in the Risk Assessment Sheets), and to share and agree on an accurate recognition of the results, it is necessary to formulate the viewpoints for verification in the walk-through beforehand, and to disseminate this information to the respective persons-in-charge implementing the walk-through.

Figure 14: Viewpoints for Verification in the Walk-through (Example)

Purpose of verification	Viewpoints for verification (Example)
To ensure that the contents set out in the Risk Assessment Sheets are fair and proper	・Have services, businesses, management resources, etc. been identified in full without omission? Can the basis for that, such as internal materials used as reference during this identification work, be understood objectively from reading the deliverables? ・Is it possible to rationally explain the decisions made at each step based on the results of the previous step? (Is consistency ensured?) Can the basis for these decisions be understood objectively from reading the deliverables? ・In the selection of Priority Services, have decisions been made based on factors such as the activity goals of the organization, changes in the management environment, relevant laws, and other requirements? Can the basis for these decisions be understood objectively from reading the deliverables? ・With regard to the impact in the event that Priority Services are completely suspended, in addition to direct business partners, do the decisions also take end-users into consideration? ・With regard to the businesses necessary for the provision of Priority Services, in addition to businesses that involve direct contact with customers, are indirect businesses also taken into consideration? ・In the risk analysis, are inherent risks evaluated?
To ensure that the recognition of contents set out in the Risk Assessment Sheets is shared and agreed.	・Do the contents set out in the Risk Assessment Sheet give rise to misunderstanding on the part of the reader, or prevent the fostering of a shared recognition (for example, unclear subject or object, writing that could lead to multiple interpretations)? Are the descriptions only understandable within a specific department, in particular the information systems department (for example, despite the use of highly technical terms, no supplementary explanations for facilitating the understanding of external parties are included)? ・Are there variances in the precision of the contents set out in the Risk Assessment Sheets? ・With regard to the interpretation of the risk criteria, as well as decisions made for the risk evaluation based on the risk criteria, are there any discrepancies in recognition among the parties concerned?

(iii) Implementation of walk-through

The respective persons-in-charge of implementing the walk-through contribute issues that have been pointed out based on the viewpoints for confirmation, and based on their respective roles, coordinate and adjust among their mutual perceptions of the risks, and derive the necessary items to be revised.

In addition, they also verify the points of reflection (points that should be improved on) in the aspects of systems and execution of the risk assessment work, toward the improvement of efficiency in efforts from the next time onward.

(iv) Revisions to the deliverables subjected to a review

With regard to revisions based on the issues that have been pointed out in the walk-through, the author of the deliverables subjected to a review carries out the revisions.

(v) Summarizing the results of the walk-through

With regard to the results of the implementation of the walk-through, in addition to sharing them among the respective parties concerned, the results also become deliverables subjected to a review, which are used to evaluate the validity of processes related to a series of risk assessment activities in (2) Performance Evaluation. For this reason, the coordinator draws up the following deliverables as proof that is related to the implementation of the walk-through.

Figure 15: Proof that Is Related to the Implementation of the Walk-through (Example)

Deliverables that serve as proof	Overview
Walk-through Record Sheet	As proof of the implementation process of the walk-through, this records items such as the date and time of implementation, review subjects, affiliation and name of the participants as well as their roles in the walk-through, and proceedings.
List of Advised Matters in the walk-through	As proof of the implementation process of the walk-through, this records items such as the contents of the issues pointed out, the appraising party, measures in response to the appraisal, and contents of revisions based on the issues that have been pointed out.

(vi) Feedback to the respective parties concerned

After the completion of the series of work related to the walk-through, the coordinator shares the Walk-through Record Sheet and the List of Advised Matters in the Walk-through with the respective parties concerned.

(2) Performance Evaluation

Performance evaluation is a method for the validation of risk assessment by independent persons-in-charge, and is implemented in accordance with the following flow after the completion of the walk-through.

(i) Appointment of the persons-in-charge of evaluation

Appoint persons-in-charge of evaluation, who are responsible for implementing the series of work related to performance evaluation (the number of persons-in-charge should be determined based on the scale of the organization and other factors). In appointing the persons-in-charge of evaluation, it is important to consider the following viewpoints.

Figure 16: Main Viewpoints that Should Be Considered in Appointing Persons-in-charge of Evaluation

Viewpoints that should be considered	Objectives
Independence of the persons-in-charge of evaluation	Similar to an accounting or operation audit, the performance evaluation ensures fairness and objectivity by having a person-in-charge who has been independent from the risk evaluation work up to the previous step carry out the work, leading to the contribution to improving the quality of risk assessment. For this reason, it is also effective that external experts such as consulting companies are used for small and medium-sized enterprises that do not have an internal audit department that is independent from the business departments.
Necessary capabilities/knowledge	In performance evaluation, as the structure and processes are evaluated, there is a need for the persons-in-charge to be equipped with the capacity to comprehend basic documents and to explain to the parties concerned during feedback. It is not necessary to have advanced specialized knowledge of IT and information security only in cases where evaluation is carried out with reference to the viewpoints described later.

(ii) Implementation of performance evaluation

In performance evaluation, from the perspective of ensuring fairness and objectivity, and reducing the work load on the risk assessment promotion department, the basic principle is to check the respective deliverables in the previous step and the work leading up to the walk-through. Specifically, checks are carried out to ensure that there is shared recognition among the relevant departments on the contents set out in the Risk Assessment Sheets, and agreement on the risks that are subjected to risk treatment (processes for building consensus are appropriate). This is done by verifying the quality of the contents set out in the Risk Assessment Sheets, and referring to the Walk-through Record Sheet and the List of Advised Matters in the Walk-through.

It is recommended that the work of checking the respective deliverables is carried out based on the example viewpoints shown below.

Figure 17: Viewpoints for Verification in Performance Evaluation (Examples)

Target deliverables	Viewpoints for verification (examples)
Risk Assessment Sheets	・Are there any obvious omissions? In particular, are there any omissions in the description of the results of the analysis and evaluation of identified risks? ・Are there any obvious errors in the descriptions? For example, despite the measures that have already been put in place, are the evaluation values for the risks higher than before the implementation of those measures? ・For all entries in the sheets, are the names of all the respondent (person filling in the sheet) and persons-in-charge clearly stated without any omission? ・In cases where there are any services or businesses for which risk evaluation has been deferred (e.g. did not make them subjected to risk evaluation), are valid reasons clearly stated in the comment field or other sections? Is it possible to confirm that the deferment has been authorized by the person-in-charge? ・For the risks that are subjected to risk evaluation, have the risk owners been determined? Have the appropriate departments and executive officers, which take

	into account factors such as the scope of impact of the risk in question, been appointed as risk owners?
Walk-through Record Sheet	・Have all risk assessment promotion departments participated in the walk-through and the implementation of the review? In particular, from the perspective of improving the precision of the evaluation results, have experts (parties with a certain level of working experience and knowledge of service provision, the businesses necessary for service provision, and the management resources related to the businesses) participated in the walk-through and the implementation of the review? ・From the perspective of ensuring the objectivity of the evaluation results, have indirect departments such as the legal departments and risk management departments participated in the walk-through and implementation of the review? ・From the perspective of verifying the effectiveness of the walk-through (that it is not a mere formality), have the respective persons-in-charge of the walk-through contributed issues that have been pointed out in light of the viewpoints for verification based on their respective roles? Has it been implemented for an appropriate time and frequency, according to the volume of the contents set out in the Risk Assessment Sheets? ・Have the results of the walk-through been reported appropriately to the management? (Or have the management participated in the walk-through and the implementation of the review?)
List of Advised Matters in the Walk-through	・Have the response policies been organized without any omission with regard to the issues pointed out during the walk-through? Have the organized response policies definitely been reflected in the Risk Assessment Sheets?

(iii) Summarizing the results of the performance evaluation

In cases where points to reflect upon (items that should be improved on) are uncovered as a part of the results of the performance evaluation, list them in preparation for feedback to the respective parties concerned.

(iv) Feedback to the respective parties concerned

After the completion of the series of work related to the performance evaluation, the persons-in-charge of evaluation share the results of the performance evaluation with the respective parties concerned. When doing so, it is recommended that the same results are also shared with the management, who have the final responsibility for the risk treatment, which is considered in the next step.

It is also desirable to share the positive points of the risk assessment process. Having the respective parties concerned recognize the positive points, and rolling out this information across the parties concerned, can contribute to further improving the quality of the risk assessment.

<3> Management of Issues

With regard to the points to be reflected upon (points that should be improved on) in the aspects of systems and execution, which have been uncovered through the risk assessment and validation processes, analyze the causes and identify them as issues. When doing so, register the identified issues in the issue management chart.

Share the issues that have been identified with the respective parties concerned, break them down into task units, and assign them to persons-in-charge while setting deadlines for the resolution. Continuously monitor the

situation until each business has been completed, record the processes and results, and follow-up on each issue.

<Reference> Steps after the Risk Assessment (Identification of the Options of Risk Treatment)

In risk treatment, clearly define how the target risks will be managed, and by when. The methods of management can be broadly categorized into the following four classifications: risk mitigation, risk avoidance, risk transfer, and risk retention. By identifying the method, from among these four methods that will be applied to each risk, clearly define the policy of risk treatment.

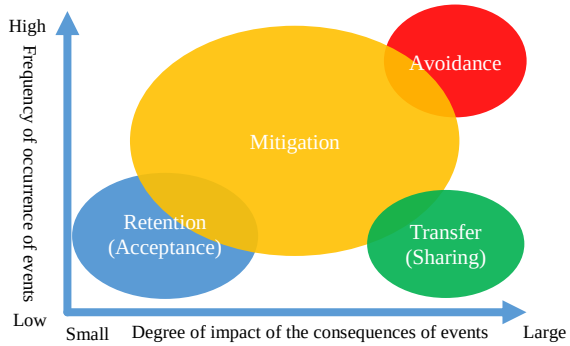
<Options of risk treatment>

Management method	Overview	Classification
<1> Mitigation	Applying the appropriate management measure to risks.	Risk control
(i) Eliminating the risk source	Eliminating the ease of occurrence of the risk and the source of impact on results. (Example: Application of security patches to vulnerabilities)	
(ii) Mitigating the degree of impact	Mitigating the degree of impact on the business operators.	
(iii) Reducing the ease of occurrence	Reducing the frequency and ease of occurrence.	
<2> Avoidance	Avoiding risks by deciding not to start or continue activities that could give rise to risks.	
<3> Transfer (Sharing)	Sharing all or part of the risks with one or more other parties. (Includes risk measures in the monetary aspect, such as by diversifying risks through contracts and taking out insurance policies)	Risk financing
<4> Retention (Acceptance)	Retaining (accepting) the risks through decision-making based on information.	

(Note) In ISO 31000:2018, risk mitigation covers the concept of taking or increasing risks in order to pursue certain opportunities. However, as this Guide is based on the concept of capturing the negative impact on the objectives as risks, this has not been included in the table shown above.

In order to realize effective risk treatment, it is necessary to put in place appropriate measures depending on the frequency of occurrence of events and the degree of impact of the consequences of events. For risks that have been assessed to be significant both in terms of the frequency of occurrence of events and the degree of impact of the consequences of events, it may be considered more advisable to avoid the risks rather than putting effort into reducing the size of those risks. In cases where the degree of impact is large despite a low frequency of occurrence, some may see it preferable to transfer (share) the risks by utilizing cyber insurance or other means. Generally, these views can be summarized as shown in the following figure, corresponding to the frequency of occurrence and degree of impact.

<Risk treatment corresponding to frequency of occurrence and degree of impact (example)>



In identifying the options of risk treatment, it is not always necessarily just one single option identified, but there are cases where measures that span multiple options are identified and implemented. Based on the concept of mission assurance in CI operators in particular, there is also a need to put maximum effort into not selecting the option of risk avoidance, by opting for risk mitigation, risk transfer, or a combination of these two methods.

For events such as information leakage, for example, even in cases where the degree of impact on the consequences of the event is assessed to be low while the frequency of occurrence of the event is assessed to be high, there are also cases where reducing the ease of occurrence may not necessarily be a rational risk treatment; instead, risk treatment methods that eliminate the risk source, such as the application of a security patch, may be considered to be more rational from the aspects of cost and effectiveness.

Ultimately, the decision is made in consideration of the activity goals of the operator and requirements of the interested parties. However, it is important to review the identification of the options of risk treatment while bearing these concepts in mind.

With regard to residual risks after risk treatment, it is necessary to share these among the stakeholders, including the decision-makers (and where necessary, including the supply-chain), and to recognize the nature and extent of these residual risks.

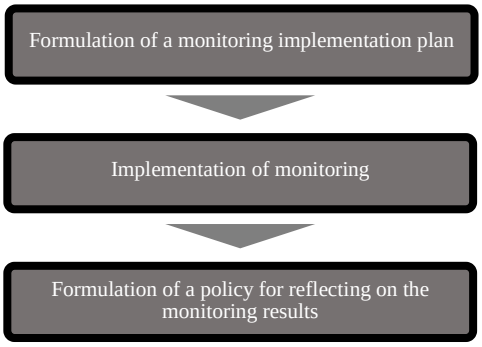
8. Continuous Review of Risk Assessment

A situation where the results of the risk assessment have been acknowledged is expected to change with time. In order to identify the situation that may change or invalidate the risk assessment, as well as other factors, and to appropriately deal with fluctuations in the risks, it is necessary to manage the risks appropriately, and to build systems that enable the continuous and effective functioning of risk management. For example, carry out continuous monitoring of risk assessment results (efforts to continuously inspect and supervise the situation, observe it based on key points, or make decisions, in order to identify the differences with the situation that has been recognized to be the results of the risk assessment), and review the results of the risk assessment where necessary.

This chapter sets out the reference procedures for the implementation of monitoring, aimed at the continuous review of risk assessments.

When conducting risk assessment from the next time, review the necessary systems and operations based on the results of monitoring.

<1>Steps



<2> Procedures

(1) Formulation of a Monitoring Implementation Plan

For the risk assessment results set out in the Risk Assessment Sheets, formulate an implementation plan to carry out the monitoring.

The implementation plan includes plans related to the formulation of a response policy for risk assessment work from the next time, based on the monitoring results.

(2) Implementation of Monitoring

The risk owner carries out monitoring based on the monitoring implementation plan. With regard to monitoring, the basic principle is to implement it for all items identified in the series of processes leading up to the evaluation of the risk in question (all the items written out in each Risk Assessment Sheet), and not merely follow up on the risk treatment for risks that have been identified through risk evaluation (risks that are subject to risk treatment).

It is recommended to take the following viewpoints into account when carrying out monitoring.

- Changes in the situation caused by changes in the external environment, which had been a premise during the conduct of risk assessment. In addition to changes in the technological environment, it is also necessary to take into consideration changes in the economic, political and legal, and social environments.

- Changes in the situation caused by changes in the internal environment, which had been a premise during the implementation of the risk assessment. In particular, it is important to take into consideration changes in the activity goals of the operator, etc., purposes for conducting risk assessment, positioning of services in relation to management (positioning in relation to business management, such as the degree of contribution to the business performance and the degree of dependency for the business), and needs and expectations of the interested parties (customers, suppliers, shareholders, local community, etc.).

(3) Formulation of a Policy for Reflecting on the Monitoring Results

Based on the monitoring results, formulate a response policy for the risk assessment work from the next time.

<Reference> Internal Audit for Risk Management Efforts

It is effective to conduct an internal audit from the perspective of a third-party, as a means of continuous review of the overall risk management effort, including the processes of risk management.

Risk management is the process of managing risks organizationally, and refers to the series of processes including planning the risk treatment based on the risk assessment results, designing the management measures as a means of mitigating the risks, and executing and managing in line with the PDCA cycle (refer to Figure 1 in 1. <2>).

Internal audit is a process that involves the "C" (Check) process in the PDCA cycle of risk management. It is carried out with the aim of checking that the PDCA for risk management is implemented appropriately, and that the respective management measures are implemented effectively. (Refer to the guidelines for details on the PDCA cycle.)

General internal audits are conducted following the process shown below.

1. Prior preparation
   (Defining the purposes of the audit, scope of audit, and audit criteria)

2. Implementation of audit activities
   (Evaluating the audit items through interviews, observation, document reviews, etc.)

3. Drawing up of the audit report
   (Contains the conclusion of the audit, including audit findings based on audit criteria, and recommendations for rectifications and improvements)

4. Follow-up of audit
   (Verification of the completion and effectiveness of rectification measures and improvement measures)

In an internal audit, the overall risk management efforts are checked based on the perspective of whether or not changes in risks caused by environmental changes, etc. have been managed appropriately, issues that call for rectification and improvement are pointed out, and agreement is reached on the measures to put in place and the deadline for these measures. At the same time, verification is carried out on whether or not these have been executed according to plan.

In conducting an internal audit for risk management efforts, it is recommended to take the following viewpoints into consideration from the perspective of whether or not the risks have been managed appropriately, based on the concept of mission assurance.

- Verification of the validity and quality of the risk assessment has been carried out appropriately through a performance evaluation or other means.

- The respective risk treatment implemented as results of the risk assessment has valid contents that keep each risk to an acceptable level, and is executed and implemented appropriately (including validation of risks assessed as not requiring risk treatment).

- Changes in the situation caused by changes in the external or internal environments, which had been the premise during the implementation of the risk assessment, have been monitored, and review of the risk assessment results and risk treatment has been implemented appropriately where necessary.

- There are no risks that have been omitted from consideration or underestimated, based on factors such as new threats and vulnerabilities in information security, trends in serious information security matters, and social trends that raise information security risks.

- Risk assessments are conducted periodically and systematically, and the organization is ready to deal appropriately with changes to the risks.

Annex A. Glossary

Term	Explanation
Event tree analysis	A method for analyzing multiple potential results arising from a single attributed cause. Starting from a certain initial event, it maps out various routes to show what the possible outcomes will be.
Management	An individual or group of individuals that command and manage the organization at the highest order. (In the case of a company, this would refer to institutions such as directors or executive officers responsible for the business, and other important employees at this level (persons holding the position of operating officers, etc.))
Inherent risks	Risks that are inherently present in the hypothetical situation, prior to the implementation of risk treatment or in cases where risk treatment is not carried out.
Maximum Tolerable Period of Disruption (MTPD)	Time taken until the situation reaches an unacceptable level due to the adverse impact that could arise as a result of the non-provision of products or services, or the suspension of business activities.
Supply-chain	Series of activities or interested parties related to the provision of services that goes beyond the boundaries of the organization.
Residual risks	Risks that are remaining after risk treatment.
Events	Emergence of, or changes in, a certain series of peripheral situations.
Consequences of an event	The conclusion of an event that has an impact on the objective.
CI operators	Operators that could have a significant impact on the lives of citizens or socioeconomic activities in the country, in the event of the suspension of services provided or the decline in quality of these services.
Detailed risk analysis	Approach of risk analysis, which involves the detailed analysis of risks related to each asset.
Value-chain	Breaks down and captures the business activities related to the provision of services in functional units, and systemizes them according to their roles and flows.
Fault tree analysis	A method that systematically explores the causes that could give rise to undesirable outcomes from a top-down perspective. It extracts the causes of occurrence of the consequences of events, potential causes that could occur, or factors of occurrence, and identifies and analyzes the conditions and factors for the occurrence of the consequences of events.
Priority Service outages	Of the events with situations where information, information systems, and control systems do not, or cannot, demonstrate their anticipated functions, these are the events for which the level for the provision of Priority Services falls below the minimum level that should be maintained.
Interested parties	Individuals or organizations that are recognized as possibly having an impact on certain decisions or activities, possible being subjected to that impact, or being subjected to that impact.
Risk assessment	Overall process of risk identification, risk analysis, and risk evaluation.
Risk tolerance	The extent of residual risk that the organization or stakeholder can be prepared to take on in order to achieve their goals.
Risk source	Element with the inherent ability to give rise to the risk by itself or through combination with others. The risk source can be tangible or intangible.
Risk attitude	Organizational efforts to conduct a risk assessment, and ultimately retain, take, or avoid the risk.
Risk treatment	Process of correcting a risk. Risk treatment includes the selection of one or more options for correcting the risk, and the implementation of these options. While risk treatment is not addressed in this Guide, reference information is provided on P29 concerning the identification of options for risk treatment, as a part of the process that comes after risk assessment.
Risk identification	Process of uncovering, recognizing, and describing risks. Risk identification includes the identification of the risk source, events, their causes, and the possible consequences.
Risk evaluation	Process of comparing the results of risk analysis with the risk criteria, in order to determine if the risk and/or its size are acceptable or tolerable.
Risk analysis	Process of understanding the nature of risks and determining the level of risk. Risk analysis provides the foundation for decision-making in relation to risk evaluation and risk treatment.
Level of risk	Risks that are expressed as a combination of their degree of impact on the consequences of events and ease of occurrence (frequency of occurrence), or the size of combined risks. A quantified (numerical) evaluation of the level of risk is known as the risk value.

Annex B. References

[1] ISO 31000:2009, Risk management－Principles and guidelines.

[2] IEC/ISO 31010:2009, Risk management－Risk assessment techniques.

[3] ISO Guide73 2009, Risk management－Vocabulary.

[4] ISO/IEC 27005:2011, Information technology－Security techniques－Information security risk management.

[5] ISO 22301:2012, Societal security－Business continuity management systems－Requirements.

[6] ISO 19011:2011, Guidelines for auditing management systems.

[7] Ryosuke Katsumata (2012), ISO22301 TETTEI KAISETSU - BCP/BCMS NO KOCHIKU/UNYO KARA NINSHO SHUTOKU MADE -, Supervised by Newton Consulting Co., Ltd., Ohmsha, Ltd.

[8] RISUKU MANEJIMENTO KIKAKU KATSUYO KENTO KAI (2014), ISO 31000:2009 RISUKU MANEJIMENTO KAISETSU TO TEKIYO GAIDO, Japanese Standards Association

[9] Manabu Sato, Takuro Haneda, Masayuki Nakagawa (2013), ISO 22301 DE KOUCHIKU SURU JIGYO KEIZOKU MANEJIMENTO SHISUTEMU, JUSE Press. Ltd.

[10] Nobutoshi Hatanaka (2008), JOHO SEKYURITEI NO TAME NO RISUKU BUNSEKI/HYOKA DAI 2 HAN – KANKOCHO/KINYU KIKAN/IPPAN KIGYO NI OKERU RISUKU BUNSEKI/HYOKA NO JISSEN -, JUSE Press. Ltd.

[11] NISC (2015), JUYO INFURA NI OKERU JOHO SEKYURITEI TAISAKU NO YUSEN JUNI ZUKE NI KAKARU TEBIKISHO (1st Edition)
<http://www.nisc.go.jp/active/infra/pdf/shishin-tebiki1.pdf>

[12] NISC (2017), JOHO SEKYURITEI KANSA JISSHI TEJUN NO SAKUTEI TEBIKISHO
<http://www.nisc.go.jp/active/general/pdf/SecurityAuditManual.pdf>