ISMS User's Guide for Medical Organizations

Guidance on the Application of ISMS Certification Criteria (Ver.2.0)

ISMS: Information Security Management System

8 November 2004

Japan Information Processing Development Corporation

The Medical Information System Development Center

About the Use of the English Version

This English version has been translated and issued by the Japan Information Processing Development Corporation. It is strictly prohibited to use or reproduce this document in violation of copyright, or publish translations. Please note that this translation is a provisional version as a reference for your convenience while using this guide. If you have doubts about the translation, please check with the original version of the guide. Only the original Japanese version has legal force.

KEIRIN この事業は、競輪の補助金を受けて実施したものです。

Preface

The Conformity Assessment Scheme for information security management systems (ISMS) started full-scale operations in Japan in April 2002. The system is designed to contribute to the overall improvement of information security in Japan, and achieve and maintain information security at a level that can be relied on by other countries as well as inside Japan.

The Criteria for the Certification of Information Security Management Systems (Ver. 2.0), which apply to this system, ("ISMS certification criteria" below) are used for practical information security management in many businesses. An increasing number of businesses have been obtaining certification under these criteria.

The Japan Information Processing Development Corporation and ISMS Conformity Assessment Scheme Technical Specialist Department published the ISMS User's Guide in September 2003 and the ISMS User's Guide - Risk Management - in July 2004 to aid understanding and help businesses aiming to obtain ISMS certification. However, as many of the businesses that have obtained the ISMS certification are information processing service companies, we have decided to prepare the guide to spread understanding of the fact that ISMS is a system for all industries. This ISMS User's Guide for medical organizations ("this guide" below) is designed for medical organizations that handle large amounts of customer information.

This guide is intended for managers at medical organizations and the relevant personnel and their supervisors at medical organizations that are considering establishing ISMS or obtaining ISMS certification. We hope this guide will help people in medical organizations understand the ISMS and find it useful when establishing and operating ISMS.

We would like to express our sincere appreciation to everyone who assisted us in the creation of this guide, including the members of the Medical Information Security Committee at the Medical Information System Development Center (MEDIS-DC) and the members of the ISMS Conformity Assessment Scheme Working Committee.

November 2004

ISMS Conformity Assessment Scheme
Technical Specialist Department

Japan Information Processing
Development Corporation

Contents

1. Positioning

1.1 The Background to Information Security

Information is a valuable asset involved in all kinds of activities, whether by individuals or organizations, and as information technology has developed, secure information management has become more and more important. Whether or not information is handled in computers, there is an obvious need for responsibility and secure management of the information possessed. In organizations such as medical organizations, in particular, the information concerns many people, and so is not effective unless the organizations manage the information in a secure way. If information security management is ignored, the resulting damage may affect the organization itself or other organizations or individuals. Leaks of the medical information of individuals are an example of this.

International guidelines for information security management are defined in ISO/IEC 17799, and are used in a wide range of industries, including the financial services and manufacturing industries. In addition, in the medical field, ISO/IEC 17799 is already used as local guidelines for medical information security management in Australia, Canada, the Netherlands, New Zealand, South Africa, and the United Kingdom. Other countries are also showing increasing interest in it. ISO/TC215 has also started to create an information security management guide based on ISO/IEC 17799.

Each field has its own security requirements. While the protection and security of personal information is important for all individuals, companies, endowed institutions, and governments, the medical field has its own security requirements (confidentiality, integrity, and availability). Since medical organizations can access personal information (for example, family history, religion, or personal belief) in order to meet the needs of individuals in providing medical services, the medical information of individuals is considered to be the most confidential of all personal information. The protection of confidentiality is therefore a basic need if the privacy of patients is to be protected.

To guarantee the integrity of medical information, it is also important that the overall lifecycle of management can be verified, from the point where the information is obtained, through the processes of saving, updating, providing, and discarding it. The availability of medical information is also important if effective medical services are to be provided. The weight attached to security management must not be allowed to interfere with medical services. The medical information system also needs to ensure that it can always operate, even during a natural disaster or system failure. The need to guarantee the confidentiality, integrity, and availability of medical information is thus a special feature of the medical field.

As Internet technology has become more commonly used, the need for effective information security management in the medical field has become more urgent. If this technology is used inappropriately, there is an increasing risk to the confidentiality, integrity, and availability of medical information. Many medical services are provided at private or small-scale clinics. These clinics tend not to possess adequate security management systems. All medical organizations must manage the medical information strictly to protect it, regardless of the scale or location of the medical facility or the form of the medical service in question. Clear, simple guidelines specific to medicine are therefore needed on the measures to take and methods for carrying out this management. The use of common guidelines for information security management in the medical field will have obvious benefits for medical organizations, now that more and more patient information is being exchanged electronically between medical organizations.

1.2 Establishing ISMS

Medical information exists in a range of formats. The data is expressed not only in words or numbers but also in the form of photos, figures, videos, or medical images. There are also different kinds of storage formats, such as paper, film, and electronic media. Transfer can be performed by hand, fax, mail, computer network, and many other ways. Whatever forms medical organizations take and however data is transferred and stored, data must be protected appropriately.

The ISMS User's Guide for medical organizations ("this guide") provides guidelines for understanding and implementing Information Security Management Systems (ISMS) in the medical information field which comply with the Criteria for the Certification of Information Security Management Systems (Ver. 2.0) (the "ISMS certification criteria" below). If medical organizations perform medical information security management in accordance with this guide, they will meet the minimum security requirements required to maintain the confidentiality, integrity, and availability of personal medical information.

It is easy for one medical organization to establish an ISMS in its own way. However, as stated in section 1.1, if data is exchanged electronically between more than one medical organization, performing security management using the same management system will make it possible to establish effective controls without omission in a short time.

After ISMS is established, continuous reviews must be carried out. Given this, it is a good idea to follow a standard method when establishing it.

This guide provides an overview of the requirements for medical information security and shows the approach to take to manage and operate the system. The requirements described in this guide are universal requirements which also apply to the long term.

However, with security technology developing rapidly, the sample technology given in this document is not universal, and considerations are not limited to the technology discussed. There is no need for prejudice towards newly developed or improved technologies; any technology that is required to meet the requirements should be employed.

Generally speaking, ISMS is established as a mechanism for managing risk effectively and efficiently in a business area to achieve the goal of an organization. (Reference Criteria: "Clause 3. Terms and Definitions" in the ISMS certification criteria)

Establishing ISMS may also produce the following effects:

- Clarifying the goals of an organization, conveying it and ensuring that it is carried out.
- Continuous management of how the system is being put into practice, to maintain appropriate standards.
- Performing regular reviews, allowing flexible improvements to the required measures or systems
- Recognizing the social environment and demands and reflecting these in the goals of the organization.

The ISMS is intended for the management regarding information security. Establishment of the information security management system means building the framework required to perform the measures that are suited for the value of the information assets an organization possesses, manages, and operates and to realize and maintain compliance with laws and regulations. (Reference Criteria: "1. General" under "Clause 1. Applicable Range" in ISMS certification criteria)

Satisfying the requirements given in this guide in an appropriate way will thus lead to the balanced information security system being established and managed, and gaining trust from stakeholders, including patients.

1.3 The Position of This Guide

This guide has been prepared as a set of guidelines to help medical organizations to establish effective regulations on procedures and ISMS, to carry out the information security management. This guide is not necessarily the only way to establish ISMS. It aims to serve as a set of guidelines for helping medical organizations that are not familiar with the ISMS establish the system.

This guide introduces the terms and conditions that are required to establish ISMS and give the requirements for this, and the purpose and concepts behind the requirements. Although the contents have been written taking into account ISO/IEC 17799 and ISO/TC215, mentioned above, but they are not guidelines for obtaining ISMS certification based on these international standards. However, a further step for medical organizations that have established ISMS following this guide is to obtain ISMS certification to gain the recognition of third parties.

Table 1-1 The Position of This ISMS Guide

	ISMS User's Guide
Intended Organization	Medical Organizations
Intended Readers	mainly management at medical organizations and personnel responsible for establishing ISMS

1.4 Key Points about ISMS

The following are the key points about the information in this guide.

This guide:

- centers on medical organizations.
- refers to the "ISMS certification criteria (Ver. 2.0)" ISMS certification standard.
- refers to the "Japanese Industrial Standards (JIS) Information Technology - Code of practice for information security management" JIS X 5080:2002 ("JIS X 5080" below) as best practice.

- has been written taking into account international trends and trends in Japan to standardize the ISMS Conformity Assessment Scheme.
- uses the Plan-Do-Check-Act (PDCA) model to ensure that there is a continuous improvement process and therefore that a system for managing information security in an effective way has been established and is being maintained.
- uses a process approach based on the PDCA model.
- describes the relationship between risk assessment process, selected controls, and Statements of Applicability (SoA).

1.5 Steps in Establishing ISMS

The nine steps shown in Figure 1-1 are involved in establishing ISMS.

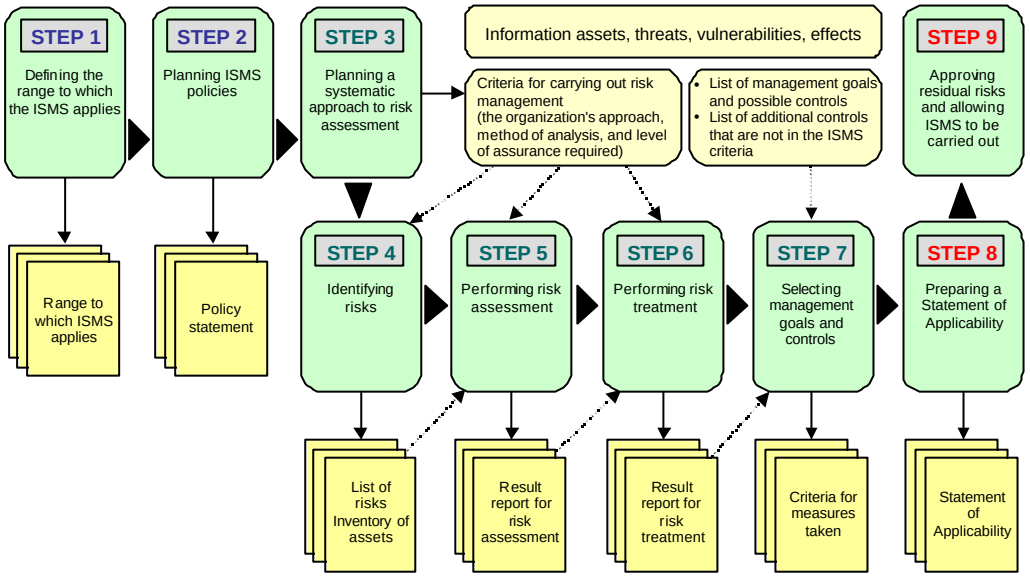


Figure 1-1 Steps Involved in Establishing ISMS

Table 1-2 Steps Involved in Establishing ISMS

ISMS certification criteria (Ver. 2.0)
(1) Defining the range to which the ISMS applies – In terms of the characteristics, organization, location, assets, and technology of the business operation
(2) Planning ISMS policies – In terms of the characteristics, organization, location, assets, and technology of the business operation
(3) Planning a systematic approach to risk assessment (4) Identifying risks (5) Performing risk assessment
(6) Performing risk treatment
(7) Selecting management goals and controls
(8) Preparing a Statement of Applicability
(9) Approving residual risks and allowing ISMS to be carried out

1.6 The Process Approach and PDCA Model

This guide is intended to provide a model to help medical organizations establish, implement, operate, monitor, and maintain ISMS and improve its effectiveness. It is therefore suitable for establishing a system that can deal with changing information risks in the operating environment of a medical organization.

1.6.1 General

In general, it is said that using benchmarking (benchmark criteria) for business operation improvement produces a better outcome. Here, benchmarking means a method that is learned from best practice, whether this is found inside or outside the organization.

This guide has been prepared with reference to best practice in information security management systems, as defined in JIS X 5080, and should help organizations identify and deal with risks more effectively.

The purpose of ISMS benchmarking is to strengthen the information security system against risks in the range to which the system applies, as clarified during risk assessment. To do this, it is important to analyze the environment of business operations in this range and properly understand the status of risks that may affect it. In order to recognize these risks and changes to them correctly, management rules are required that clearly define what must be managed.

Performing this management will clarify the direction and policies of the organization, resulting in shared expectations and verification methods for information security across the organization. In addition, feedback about the results of verification can lead to further improvements, creating a deeply ingrained information security management system. This process can be made more clear with the concept of "process approach," as described in the following section.

1.6.2 The Process Approach

The concept of the process approach has been included in documents such as the quality management system standards (JIS Q 9001: 2000), and is used in many organizations in Japan. In the process approach, every activity that is carried out or managed using business resources is considered to be process converting input into output. It is a methodology (approach) that identifies the business operations (processes) in an organization, so that their relationships can be understood, and puts a set of these processes into practice as a system to carry out the functions of the business (see Figure 1-2).

This guide recommends the use of the "process approach," as it identifies the different activities required to manage information security in an organization. (Reference Criteria: "2. Process Approach" in "Clause 0. Introduction" in the ISMS certification criteria)

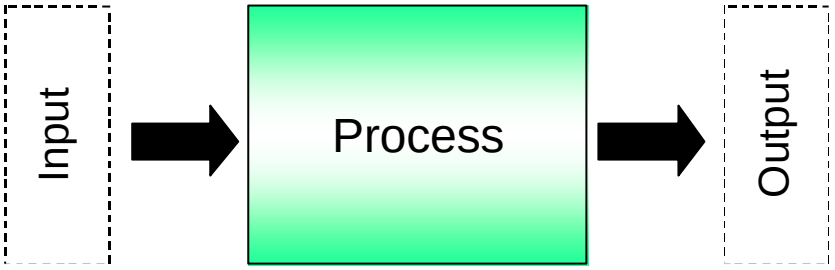


Figure 1-2 The Process Approach

In the process approach, it is necessary to identify from every angle what will be input in each process and what will be output as the result of the process.

This approach is useful for establishing ISMS, to identify the risks to the information assets related to processes, based on items related to information security and has been identified here, so that controls can then be put in place and carried out properly.

The following benefits can be obtained when a medical organization employs the process approach. (Reference Criteria: "2. Process Approach" in "Clause 0. Introduction" in the ISMS certification criteria)

In this approach, the establishing of ISMS is treated as a series of processes, each of which is identified by the process approach. Recognizing the inputs and outputs of each from the relationships between them makes it possible to identify the important issues that are required to establish ISMS.

This guide recommends that the process approach is used to manage ISMS, and also presents the following "PDCA model" as a concept for creating a management system.

1.6.3 The PDCA Model

This guide employs the "PDCA model" shown in Figure 1-3.

The information security requirements and expectations from stakeholders, which will be described later, are considered as inputs. The activities and processes that are required to obtain information security outcomes (managed information security), the outputs which satisfy these requirements and expectations, are treated as ISMS processes. These ISMS processes are organized using the PDCA model, providing opportunities for continuous study and improvement of the information security management system in an organization.

The model used for these criteria is known as the "Plan-Do-Check-Act" (PDCA) model, and it can be applied to any ISMS process. Treating the requirements and expectations of stakeholders about information security as inputs, Figure 1 shows how the information security outcomes (managed information security) satisfying these requirements and expectations are created, by the necessary activities and processes. Figure 1 also shows the relationships between the processes, which will be described in Clauses 4, 5, 6, and 7.

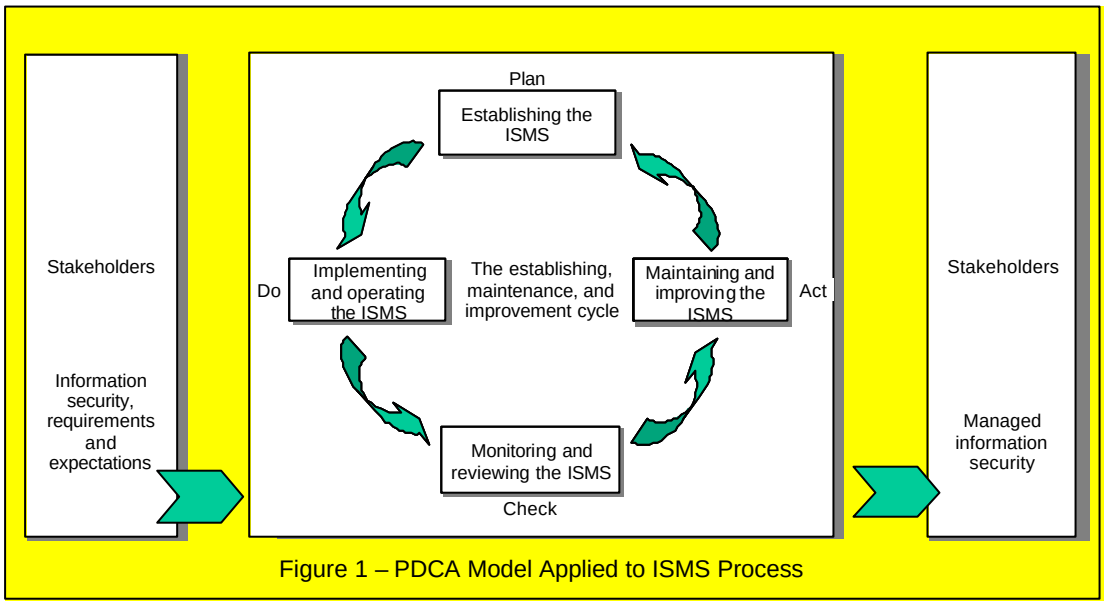


Figure 1 – PDCA Model Applied to ISMS Process

(Quoted from "2. The Process Approach" in "Clause 0. Introduction" in the ISMS certification criteria (Ver. 2.0))

Figure 1-3 PDCA Model

Figure 1-3 shows the many stakeholders involved in a medical organization. In ISO/TS 17090, the technical specifications for the public key platforms used in the life insurance medicine field, there is a list of certificates for hcRole, which includes Medical Doctor, Dentist, Pharmacist, Medical Technologist, Radiological Technologist, and General Nurse. hcRole is an attribute of X.509 (the Public Key Certificate Structure), which is defined by ITU-T (Telecommunication Standardization Sector at International Telecommunication Union, an agency of the United Nations).

If the definitions in "JIS Q 9000:2000 3.3 Organization" are applied to medical organizations, the term "organization" indicates the medical organizations in various forms, the above mentioned certificate holders, and the other people who work at medical organizations. The term "customer" indicates patients, groups of patients, and their families. The term "supplier" indicates the companies that supply goods or services to medical organizations. The term "stakeholder" includes all the above people and organizations, and also organizations established by medical organizations, insurers, pharmacies, and groups of qualified people.

It is important to clarify the ways in which these stakeholders can access information.

2. Normative References

The ISMS certification criteria site the following three standards as normative references. The following section introduces the standards for information security and management systems including standards not in the Reference Criteria: "Clause 2. Normative References" in the ISMS certification criteria (Ver. 2.0).

2.1 JIS X 5080

This is a standard in Japan, and is defined as a Japanese Industrial Standard (JIS) by the Japanese Industrial Standards Committee (JISC) related the establishing and issuance of ISO/IEC 17799. It is a faithful translation into Japanese of ISO/IEC 17799 (*1), and complies strictly with international standards.

(*1) ISO/IEC 17799

This was established and issued as an international standard for management systems for information security in 2000. It is based on a British standard, BS 7799-1: 1999 (*2) and complies to codes of practice.

<Reference>
ISO/IEC 17799 is not a set of certification criteria for a certification or registration system. The ISO plans to take certification criteria equivalent to BS 7799-2 into consideration, and so it may be established and issued in the future.

(*2) BS 7799

This is a British standard for information security, which was established and issued in the United Kingdom in 1995. It contains not only technical measures for information security but also codes of practice for managing personal and organizational resources. A second section was later established as a set of certification criteria in 1998, which produced the standard in a binary form; Part 1 (BS ISO/IEC 17799) and Part 2 (BS 7799-2).

BS ISO/IEC 17799 was created by updating the old BS 7799-1 to comply with the ISO, is entitled "Code of practice for information security management" and contains the best practice.

BS 7799-2 is entitled "Information security management systems - Specification with guidance for use," and contains the requirements for evaluating the compliance of a management system with regard to the organization's information security.

2.2 JIS Q 9001

This is a standard for the requirements of a quality management system, the first edition of which was established in 1994. The second version, which was revised in 2000, is the latest one. The ISMS certification criteria comply with the second version.

In the JIS Q 9000 series, in addition to JIS Q 9001, there is JIS Q 9000, which contains the basic principles and terms of quality management, and JIS Q 9004, which contains guidelines for improving performance.

2.3 TR Q 0008

This is a technical report (TR) of risk management terms that were defined in the ISO/IEC Guide 73 in 2002 and have been translated into Japanese. This is not a standard, but it is used in the ISMS certification criteria as a standard for risk management and for the use of terms.

> This technical report is an upper-level general document that is used for the preparation or revision of any standards that contains aspects of risk management.
>
> This technical report is intended to encourage standardization of writing about risk management and the use of risk management terms. It has been prepared to contribute to mutual understanding between the ISO and IEC members, not as a set of guidelines for carrying out risk management.
>
> (Quoted from "1. Applicable Range" in TR Q 0008: 2003)

<Reference>
The Japanese Industrial Standards Committee, which discusses national standards, discusses the technical reports (TR) as follows, and calls TR Q 0008 "Type II."

2.4 Other References

(1) TR X 0036 -1 to 5 (GMITS)

These are referred to "Guidelines for managing IT security" and contain standards that have been internationalized as ISO/IEC TR 13335. These guidelines are an instruction manual that describes how to build up IT security management, including risk management.

It has been established and issued in a series, starting in 1996, and is composed of the following five parts:

- Part 1: IT Security Concepts and Models
- Part 2: IT Security Management and Planning
- Part 3: Methods for Managing IT Security
- Part 4: Selecting Safeguards
- Part 5: Management Procedures for Network Security

3. Terms and Definitions

The ISMS certification criteria define the terms regarding information security and risk management.

The ISMS certification criteria contain the terms and definitions in the alphabetical order, to achieve compliance with BS7799-2: 2002. The terms therefore appears to be listed in random order, and can be more easily understood if they are divided into the following three categories based on their content.

Table 3-1 Categories of Terms

Definitions of information security terms	3. Information security	
	2. Confidentiality	
	5. Integrity	
	1. Availability	
Definitions of risk management terms	10. Risk management	
	8. Risk assessment	7. Risk analysis
		Risk source
		9. Risk evaluation
	11. Risk treatment	
	6. Risk acceptance	
Definitions of management system terms	4. Information security management system ISMS	
	12. Statement of applicability	

3.1 What is Information Security?

Information that is essential to the operations of an organization must be protected properly. If it is not, there is the risk that the job performance will be affected due to the leaked, inaccurate, or unavailable information. "Information security" means protecting critical information against such risks.

The ISMS certification criteria define information security as follows: (Reference Criteria: "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

To clarify the risks regarding information security, it can be analyzed in terms of the three elements of information security: "confidentiality," "integrity," and "availability."

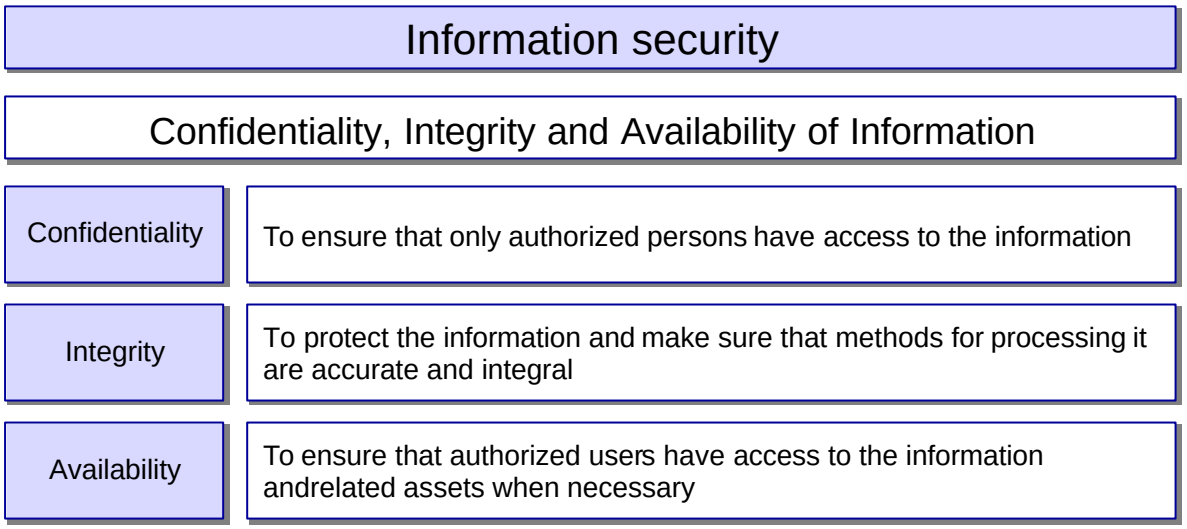


Figure 3-1 Definition of Information Security

The terms "confidentiality," "integrity," and "availability" have been defined and used in the "Guidelines for the Security of Information Systems"[1] (below, the "OECD Guidelines"), which is attached to the "Recommendation of the Council concerning Guidelines for the Security of Information Systems"[2] issued in 1992.

> To protect an information system against harm that may affect the confidentiality, integrity, or availability of the information system.
>
> (Quoted from the OECD Guidelines: 1992)

These three terms are often known by their initials, as the "C.I.A. of information security."

The ISMS certification criteria define the confidentiality, integrity, and availability as follows:

1 Guidelines for the Security of Information Systems, 26 November 1992

2 Recommendation of the Council concerning Guidelines for the Security of Information Systems (adopted by the Council at its 793rd Session of 26-27 November 1992)

2. Confidentiality

Ensuring that only authorized persons have access to the information.
[Refer to JIS X 5080: 2002]

(Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

The confidentiality of information can be assured by "preventing information from leaking."

5. Integrity

To protect that the information and its process methods, so that they are accurate and integral.
[Refer to JIS X 5080: 2002]

(Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

"Integrity" has two meanings. One is to ensure the integrity of the information itself. This is related to "protecting information from tampering."

The other is the integrity of information processing methods. This is related to "protecting the information system from tampering" and "establishing procedures for information processes and assuring that procedures are complied with."

1. Availability

Ensuring that authorized users have access to information and related assets when necessary.
[Refer to JIS X 5080: 2002]

(Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

Availability is related to "information becoming unavailable due to a natural disaster or a system failure."

3.2 What is Risk Management?

The ISMS certification criteria define risk management as follows:

10. Risk management

Controlled activities to instruct and manage an organization to guard against risks.
[Refer to TR Q 0008: 2003]

(Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

This document defines risks as "the probability of occurrence of an event that might interfere with the execution of business activities." The term is also defined as follows in the technical report "Risk management -Vocabulary - Guidelines for use in standards (TR Q 0008:2003)":

> 3.1.1 Risk
>
> A combination of the probability of occurrence (3.1.3) and the outcome (3.1.2) of an event (3.1.4).
>
> Note 1. In general, the term "risk" is only used when the possible result is undesirable.
>
> 2. In some cases, the risk is caused by the probability of deviation from an expected outcome or event.
>
> 3. For more information on security issues, refer to ISO/IEC Guide 51: 1999.
>
> (Taken from "Terms and Definitions" in TR Q 0008: 2003.)

As stated in "Note 2" above, the characteristics of a risk are not dependent on whether the result itself is "good" or "bad" but by the deviation from the expected value. In addition, risk only indicates a "probability."

The report "INTERNAL CONTROL IN THE NEW ERA OF RISKS - Guidelines for Internal Control That Functions Together with Risk Management," which was published by the Study Group on Risk Management and Internal Control at the Ministry of Economy, Trade and Industry in June 2003, defines that "risk is understood in a broad sense and is defined as 'the uncertainty as to whether an event will occur'."

> (1) Definition of Risk
>
> While the word "risk" is generally used to mean the probability of occurrence of a negative outcome, it is in some cases also understood in a broader sense so as to mean "uncertainty," which contains the probability of occurrence of both positive and negative outcomes. A risk to a company is, in a narrower sense, understood as the "probability of an event that might interfere with the execution of business activities" but its meaning has recently been shifted to imply a broader context, i.e., the "uncertainty of the probability of an event that might affect the future profit generation." Thus, the concept of "risk" is rather assuming a more active sense to mean a source of the value of the company.
>
> In these Guidelines, risk is understood in a broad sense and is defined as "the uncertainty of occurrence of an event," based on our notion that risk contains not only the possibility of generation of losses but also the probability of generation of profits or losses resulting from, for instance, a new business launch.
>
> (Quoted from "II-1. Desirable Risk Management" in Part II in "INTERNAL CONTROL IN THE NEW ERA OF RISKS - Guidelines for Internal Control That Functions Together with Risk Management -" June 2003, By Study Group on Risk Management and Internal Control)

The above report interprets "risk" broadly and categorizes it as shown in Table 3-2:

Table 3-2 Definition of Risk

Category	Example
Risks associated with business opportunities	Risks regarding strategic decision-making in the course of corporate management • Risks concerning entry into a new business field • Risks concerning product development strategy and the like
Risks associated with the execution of business activities	Risks concerning the proper and efficient execution of business activities • Risks concerning compliance • Risks concerning information systems and the like

(Extracted from the above report)

Nowadays, in the field of risk management, risk is often understood broadly and considered in a positive sense as a source of corporate value, as shown in Table 3-2. Although "the risks regarding strategic decision-making in the course of corporate management" should not be ignored when establishing ISMS, it is also necessary to try to minimize undesirable results by considering the risks to information security associated with business activities carried out based on these decisions.

In "1. Applicable Range" in the ISMS User's Guide, we have listed positive expectations such as obtaining reliabilities from customers or the general public as one of the advantages an organization may gain by establishing ISMS. Although information security investments may generate direct profits for the company, in many cases the activity is not very visible.

In information security activities, it is important to produce personal, daily motivation in activities at work places and departments, which will reflect "positive feedback from customers" and "activity reports from departments," in the form of information input into the management review (which will be described later) and generate an organizational "revolution." In risk management, it is essential that the following three factors are kept in balance: clarifying risk, taking appropriate measures, and establishing business processes that should be carried out properly.

3.3 What is a Management System?

The ISMS certification criteria define the information security management system (ISMS) as follows:

10. Information security management system ISMS

ISMS is the part of the whole management system where information security is established, implemented, operated, monitored, reviewed, maintained, and improved based on the approach to business risks.

For reference, a management system includes an organization's structure, policies, planning activities, responsibilities, practices, procedures, processes, and management resources.

(Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

The ISMS certification criteria define the Statement of Applicability as follows:

12. Statement of applicability

A document that describes the management objectives and controls that are appropriate for ISMS in an organization based on the results and conclusions of that organization's risk assessment and risk treatment processes.

(Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

4. Importance of Medical Information Security and Necessity of Security Management

4.1 Why Is Medical Information Security Needed?

In the medical field, approaches to medical safety have been employed for a long time. Teams for taking medical safety measures, led by a risk manager, have been formed to prevent mistakes in medical practice in a systematic way, and have taken an active role in analyzing incidents. With their help, medical care processes have continued to improve, achieving more secure medical care. However, many medical organizations do not handle personal information such as patients' medical care data as systematically as they do risk management for mistakes in medical practice. In addition, as medical care sites use more and more IT system, information systems have come to play an important role in the business operation of medical organizations. Since the shutdown of an information system would seriously affect medical services, measures are also required to deal with this. At present, maintaining information security has become an important objective for managers at medical organizations.

If information security cannot be maintained, the following disadvantages will follow. Security management is vital if these disadvantages are to be addressed.

Disadvantages arising from a failure to maintain information security

• Poor medical services and loss of profits	A shutdown of the system will affect medical services and lead to the loss of medical service fees
• A loss of trust and brand image	A loss of trust from patients as a medical organization
• Repair costs required	The costs of time and work to recover the system will arise
• Judicial action and claims for compensation	If information such as personal information or others is leaked, the injured party may bring a lawsuit for damages
• Legal liability	The penalty clauses in the Medical Practitioners' Law, the Medical Service Law, and the Personal Information Protection Law

4.2 Objectives of Medical Information Security

One of the important points when managing information security is to clarify "the purpose for which the information security management is being performed." It is important to define the objectives of medical information security clearly, and manage security to achieve those objectives. The following are examples of some of the more important objectives:

(1) Protecting Personal Information

Medical information is one of the most important types of personal information, and if it is leaked, it could affect the rest of a patient's life. Medical organizations must realize the importance of the information they are handling and manage it appropriately.

The most important measures (controls) here include the following:

Protecting Medical Information:
Keeping medical information confidential to protect personal information

(2) Preventing Mistakes in Medical Practice

If the integrity of medical information is not maintained, medical services may be provided based on incorrect information. Medical organizations must strive to maintain the integrity of medical information to prevent mistakes in medical practice.

The most important measures (controls) here include the following:

Maintaining the Integrity of Medical Information:
Maintaining the integrity of medical information, so that suitable medical services can be provided

(3) Maintaining the Functions of the Medical Organization (The Continuity of Medical Services)

The roles of medical organizations become greater in a major disaster. Even if the social infrastructure has suffered enormous damage, they must recover quickly and continue to provide medical services. They must also put in place suitable defensive measures to handle malicious attacks, to deal with problems such as cyberterrorism.

The most important measures (controls) here include the following:

Keeping Information Systems Available:
Keeping information systems available to maintain the functions of the medical organization

4.3 Information Security and Information Security Management

IT is developing at an extremely high speed, and it cannot be expected that the best information security measures at one time will continue to be the best in the future. While the hardware and software in place may have been the most appropriate choice when it was set up, continuity cannot be guaranteed. It is important to understand that taking measures on information security is not a temporary activity that can be completed by planning measures to respond to expected risks at a certain time, and can only be assured if information security policies are planned and carried out as a continual activity on a daily basis.

It is also important to continue to gather information, establish a security assurance system, and carry out appropriate measures based on those laid down, not only to maintain security but also for when security fails.

In addition, it will be necessary to review regulations, including information security policies and procedures for information security policies, periodically to check whether or not new threats to the assets the organization possesses have appeared or anything in the environment has changed, and continually take the appropriate actions. In the field of information security, in particular, it is important to review this at shorter intervals, as technologies are more developed and the methods of unauthorized access are more complicated.

4.4 Items that Should Be Protected To Ensure Information Security

To ensure information security, the information assets that medical organizations possess must be protected against the different types of threats (which will be described later). The following shows examples of the information assets that a typical medical organization might possess.

Type of Information Asset	Examples of Information Assets
Information	Patient data and medical service data in a computer system e.g. A patient's information written in that patient's file, request forms, or letters of introduction
Software assets	Operational application, system programs
Physical assets	Computer devices: computers, printers Storage media: MO, electromagnetic tape Communication equipment: networks, phones, and communication lines Electrical equipment: power cables, power generators, CVCFs
Services	Environment: machine rooms, whole buildings, and earthquake resistance functions
People (knowledge)	Knowledge such as medical information, operational know-how, and passwords

These information assets must be categorized and organized before they can be managed. The section "5. Categorization and Managing Assets" of JIS X 5080: 2002 shows good examples of the types of assets, but the above table adds people (knowledge) to the categories shown in that section. Given the characteristics of information assets, the knowledge of people might be categorized as "Information." However, this document deliberately separates it into another category, because knowledge is managed in different ways from other information.

4.5 Threats and Vulnerabilities of Medical Information Security

(1) Threats

Factors that cause risks are called "threats." More specifically, a threat is "a potential factor that causes a contingency that may result in loss of or damage to information assets or damage to the organization."

Threats can be classified as follows:

Threat			
Accidental Threats		Intentional Threats	Environmental Threats
Negligence	Failure	Crime	Disaster
Mistyping data Operational errors Wrong connections Others	H/W failures S/W failures Line failures Others	Stealing or tampering with information, Spoofing, Infiltration, Viruses, Cyberterrorism, Physical damage, etc.	Earthquakes Fires Water damage Others

As these threats are "potential factors causing a contingency" the fact that they exist is not an actual problem. A threat only becomes a problem when it has been occurred and has factors that cause actual damage.

(2) Vulnerabilities

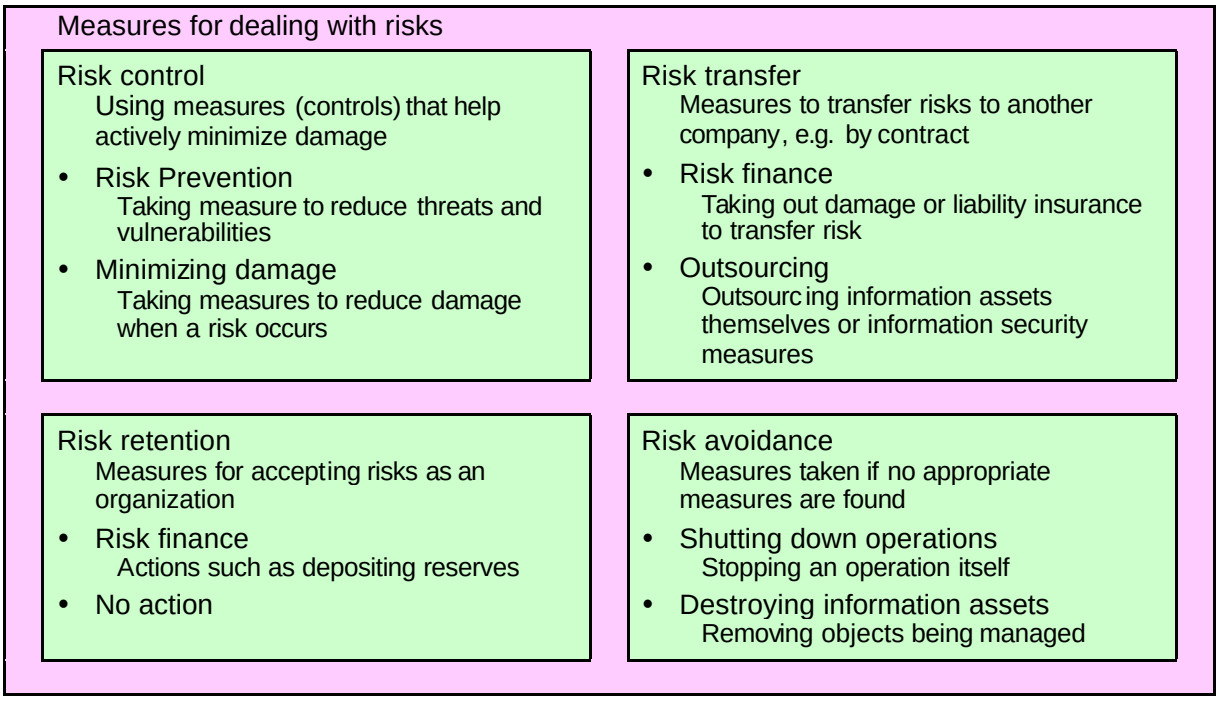
The weaknesses of the information assets that may elicit threats are called "vulnerabilities."

Examples of Vulnerabilities	
Environment	Doors and windows, power supplies, site locations that can be stricken
Hardware	Aging and deterioration of driving parts, malfunctioning of backup circuits, etc.
Software	Missing specifications, access control failure, bugs in programs, etc.
Network	Not encrypted, protection error of communication lines, malfunctioning of backup circuits, etc.
Organization	Errors in educational programs, not-thorough managing third parties
Individual	Lack of skills, low morals, incorrect understanding, etc.
Management	Shortage of budgets, lack of awareness of the information security management, etc.

A vulnerability itself will not become a problem. A risk may be elicited by combining threats and vulnerabilities.

4.6 Medical Information Security and Risk Management

The measures against risks are categorized as follows:



In typical risk management, several measures are combined and carried out, taking into account all the various factors such as the importance of risks and how easy or difficult measures are. "Risk prevention," part of "risk control" is widely recognized as a measure taken for information security. Risk prevention means preventative measures that prevent a risk from occurring and is therefore especially effective for risks that cannot easily be dealt with via financial compensation. For example, it is easy to insure against credit cards forgery, but the large amount of damage caused by a leak of personal information (especially medical information) is difficult to cover with insurance alone. If a medical organization tries to take out insurance, the insurance company may not secure a contract if no other preventative measures have been taken, or the contract may be at a very high rate. Managers at medical organizations considering the most effective combination of measures, taking into account cost effectiveness, is also an important part of risk management.

4.7 Summary of Chapter 4

This chapter has explained the importance of medical information security, and how the information security management system (ISMS) is also important for ensuring information security. It is useful to have an understanding of this when employing methods for proper management of information security. The ISO for the medical field has established a medical version of ISO/IEC 17799, the ISO/TC 215 standards, which take into account the special nature of medical services. It is important that these internationally standardized methods are used, so that security can be managed in a suitable way, so that the proper recognition can be obtained from third parties.

5. Establishing an Information Security Management System (ISMS) in a Medical Organization

Chapters 1 to 4 gave general information about ISMSs. This chapter will describe procedures and key points for establishing ISMSs in medical organizations.

5.1 The Relationship between the Flow of Operations for Managing Medical Security and Procedures for Establishing ISMS

Like ISMS, the system of medical security management, for example managing problems with medical services, is built on the PDCA cycle. Continuously improving the system will make it more secure. However, there is a difference between these two in the "P (Plan)" section. Refer to Figure 5-1 to check on the flow of operations in medical security management to find the difference.

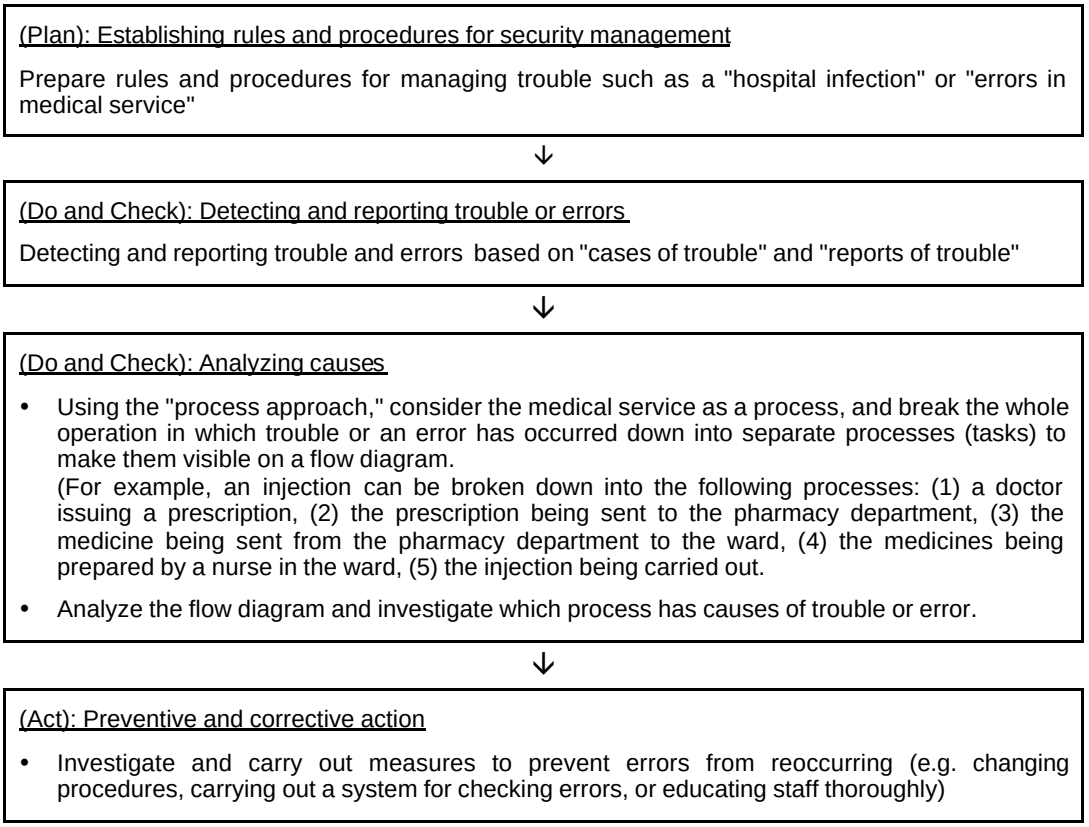


Figure 5-1 Flow Diagram for Medical Security Management

In medical security management, management rules and action procedures are prepared in P and the processes D, C and A are repeated in sequence in daily operations. This is because the medical field has already established management rules and action procedures, such as physical exams, diagnosis, treatments and nursing, based on knowledge accumulated in the past, and therefore has a mechanism for reducing risks and improving security by analyzing these procedures when an accident or mistake is found, and correcting the problem and preventing it from reoccurring as far as possible.

In contrast, due to rapid growth of IT, there are always new security problems (threats) and weak points (vulnerabilities) in information security that cannot be anticipated from past experience alone. For this reason, when an ISMS is established, it is necessary to set the range in which security problems (threats) and weak points (vulnerabilities) might occur during the process P, in order to analyze the risks and consider the measures to take. Based on the results, management rules and action procedures should be prepared before carrying out the other steps, from D onwards.

However, since simply repeating D, C and A cannot address security problems involving the latest technology, it is necessary to check on effectiveness of P by regularly analyzing risks and reconsidering the measures to take.

The process P is therefore more important in establishing an ISMS than it is in medical security management. Whether steps D, C and A can function effectively depends on how step P is carried out.

5.2 Process P in Establishing ISMS (Establishing ISMS)

"Clause 4-2. Establishing ISMS and Managing Operations" in the ISMS certification criteria defines the nine steps (Steps 1 to 9) for Plan (Establishing ISMS) shown in Figure 5-2.

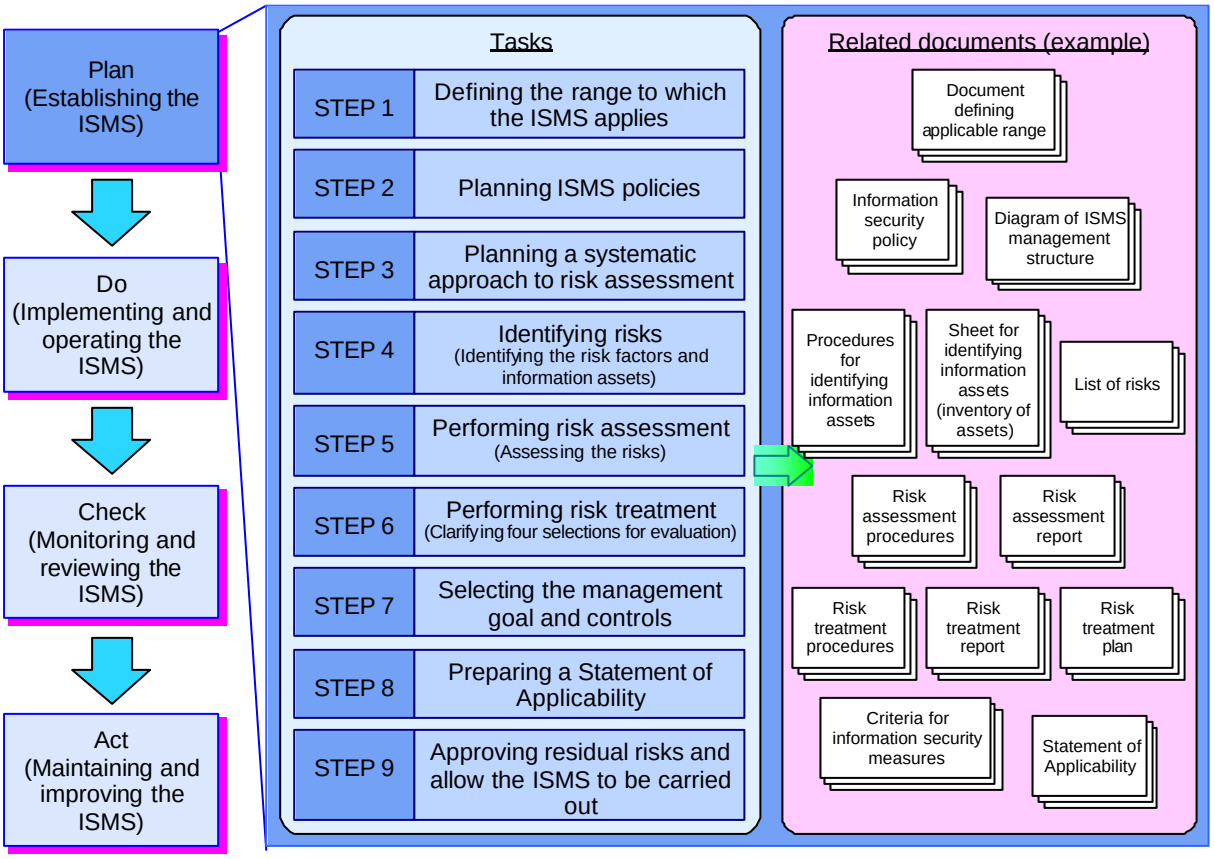


Figure 5-2 The Steps for Plan (Establishing ISMS)

These nine steps are described below:

5.2.1 Step 1 Defining the range to which the ISMS applies

The applicable range is the range to which information security management is applied, and involves several factors, as below.

5.2.1.1 Possible Factors (Aspects) of the Applicable Range

To build a truly effective management system in an organization, the applicable range of the ISMS must be determined, by deciding on one organizational group making up the range that is required for handling important information assets properly.

In the medical field, the medical facilities (such as hospitals, clinics, or care centers) can be defined as one management system to which the range should be applied. Equally, a department (such as an outpatient service department, ward service department, pharmacist's office, or checkout center) can be chosen as the applicable range.

When the applicable range is defined, it is important that it is one complete management system and that its boundaries are clear enough to explain logically.

The ISMS certification criteria requires you to consider and determine the applicable range reasonably, from the following angles. (Reference Criteria: "Clause 4-2. Establishing ISMS and Managing Operations" in the ISMS certification criteria (Ver. 2.0))

- Business operations
- Organizations
- Locations
- Assets
- Technologies

The way in which the applicable range is defined will have a great effect on workloads when the ISMS is established.

It will also affect all the activities for maintaining the information security of applicable objects, including controls, managing operations, and tasks such as identifying information assets and risk assessment.

5.2.1.2 Definition of Applicable Range

Once the applicable range has been determined, a document must be prepared to define this range. This document will help clarify the range itself and how it was determined, which will provide clear criteria for making decisions if the range is changed, or for determining whether an object should be included in the range.

(1) Document Defining the Applicable Range

"B.2.3 ISMS Applicable Range" in the BS7799-2: 2002 Annex B "(Reference) Guidance on the use of this standard" lists the following items that should be included in the document defining the applicable range.

- The processes used to establish the applicable range and the content of the ISMS
- The strategic state of the organization
- The risk management approaches that the organization employs for information security.
- The criteria for risk assessment and the level of guarantees required for information security
- The information assets identified as being in the applicable range of the ISMS

Not all items must be documented. These are simply the key points that should be considered when defining the applicable range. Even when the applicable range has been determined, the document on the definition of the range must continue to be reviewed when the ISMS is established.

(2) Tasks in Defining the Applicable Range

Figure 5-3 shows a summary of the items related to the definition of the applicable range that are required for the ISMS certification criteria.

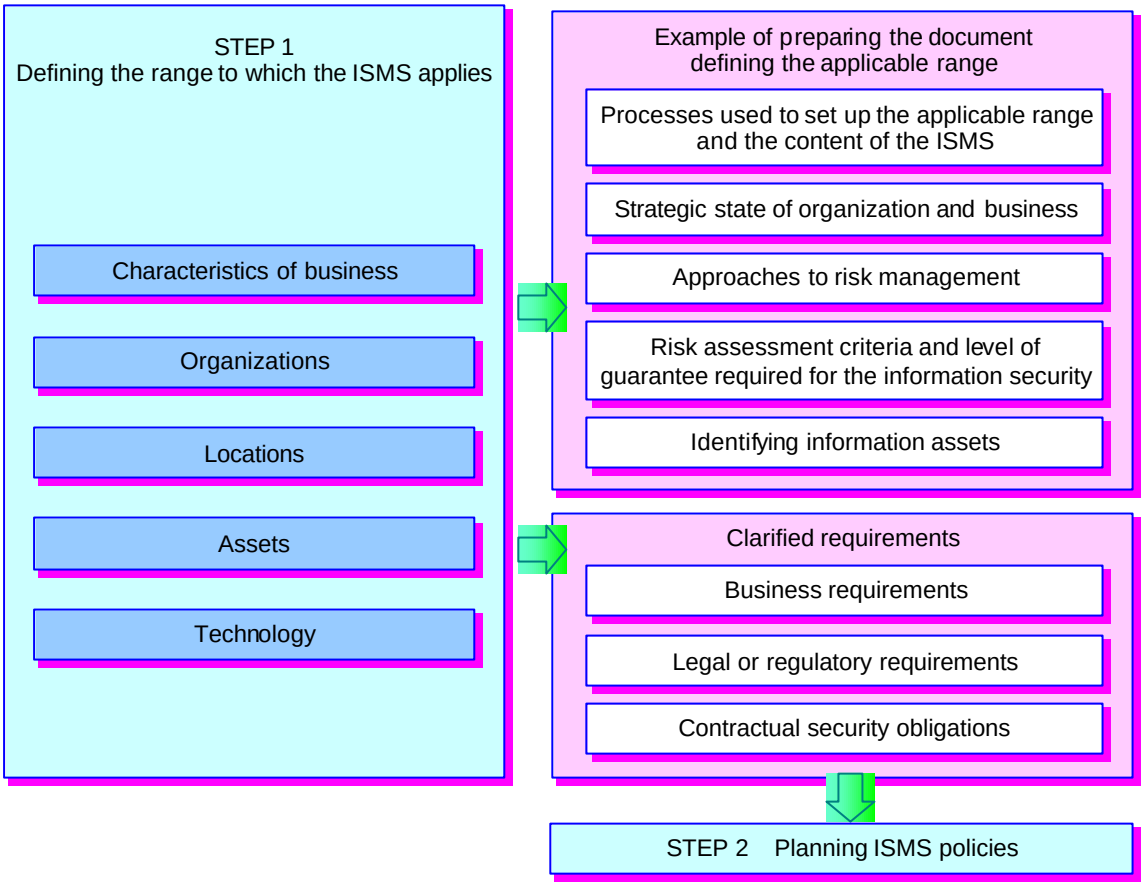


Figure 5-3 Definition of the Applicable Range for the ISMS

Defining the applicable range and considering what management system is appropriate, will also clarify the information security requirements. In particular, when using the requirements for tasks in the step "Planning ISMS Policies," make sure that the following three requirements are clarified.

- Business requirements
- Legal and regulatory requirements
- Contractual security obligations

In medical organizations, care must be taken with the applicable range, since information that has been entered as medical information may be used for billing for medical services or the checking of specimens (outsourced to an external checking agency), and may be accessed by a third party who does not belong to the medical corporation, such as a medical intern.

For example, the accounting systems and computerized physician order entry for medical services share the patients' basic information and work together with billing for ordering and medical services (medical service accounting). If a department is set as the applicable range, it is important to understand what information is entered, referred to, or output, and at which department.

5.2.2 Step 2 Planning ISMS Policies

ISMS policies set out the basic concepts for information management in an organization. The policy document is also a declaration of intent, stating that the organization is liable for information security requirements. Its contents must comply with the business policies (visions) that state the missions and objectives of the medical corporation or institution as well as the codes of conduct (sense of values). For this reason, the policies must state the general focus of information security and act as a guide to action, to regulate the behavior of employees.

Table 5-1 shows the procedures and key points in planning ISMS policies.

Table 5-1 Points in the Procedure of Planning ISMS Policies

	Point	Requirement
(1)	Establishing ISMS policies	(I) Establishing the general focus and acting as a guide to action related to information security
(2)	Structure of organization for establishing the ISMS	(II) Consider the business requirements, legal or regulatory requirements, and contractual security obligations (III) Preparing the environment for the organization and risk management (IV) Establishing the criteria for evaluating risks and defining a risk assessment structure
(3)	Endorsement from management	(V) Obtaining endorsement from management

Points (1) to (3) are discussed in detail below.

5.2.2.1 Planning ISMS Policies

"3.1.1 Information Security Policy Documents" in JIS X 5080 defines the following items that should be included in the policies.

a) The importance of the security as a mechanism that enables information security, its objectives the applicable range, and information sharing to be defined

b) A statement of purpose supporting the objectives and principles of information security

c) A brief description of the security policy, principles, standards and applicable requirements that are especially important for the organization

   1) Complying with regulatory and contractual obligations

   2) The requirements for education on security

   3) Preventing and detecting viruses and other malicious software

   4) Continued business management

   5) Actions to take in response to a breach of security policy

d) A definition of the general liabilities and specific liabilities for information security management including reporting security incidents

e) Reference information for documents that support the policies (e.g. security-specific policies and procedures related to specific information systems or recommended security rules for users)

(Quoted from "3.1.1 Information Security Policy Document" in JIS X 5080: 2002)

These items are just examples. It is not necessary to include all of them in a policy. It is also likely that the contents of this list may change depending on the applicable range defined in the previous step.

The items defined in JIS X 5080 should be taken as points to be considered when planning what should be included in the policy.

Normally, ISMS policies are planned by a representative of the business (for example, a general manager or general information manager) and are distributed to employees, who should be thoroughly familiar with them. In medical organizations, the director of the hospital (or manager of the clinic) should plan these and distribute them to employees.

A medical organization's policies should be displayed at the reception or in the consultation room of the medical organization so that patients are notified of them.

5.2.2.2 Building an Organizational Structure for Establishing the ISMS

The requirements for functions of organizations responsible for establishing ISMS are as follows: "(II) Considering business requirements, legal and regulatory requirements, and contractual security obligations," "(III) Preparing the environment for the organization and risk management," and "(IV) Establishing the criteria for evaluating risks and a defining structure."

The members of the group for establishing the ISMS in the organization should be chosen from within a range that is wide enough for discussing issues related to handling different types of information and also from related departments, taking into account the actual system of ISMS operations.

The information security to be handled in the ISMS should not only to consider the "information risks" and "IT risks," but is also required to address the damage after a risk occurs as well as to handle daily management. To achieve this comprehensive 'management,' people across the medical organization, including the medical service accounting and material departments and organizations at sites that in the range of certification should be involved.

Figure 5-4 shows an example of the organizational structure for establishing an ISMS introduced in the "ISMS User's Guide."

The main roles and responsibilities of the organization are given below, based on this example.

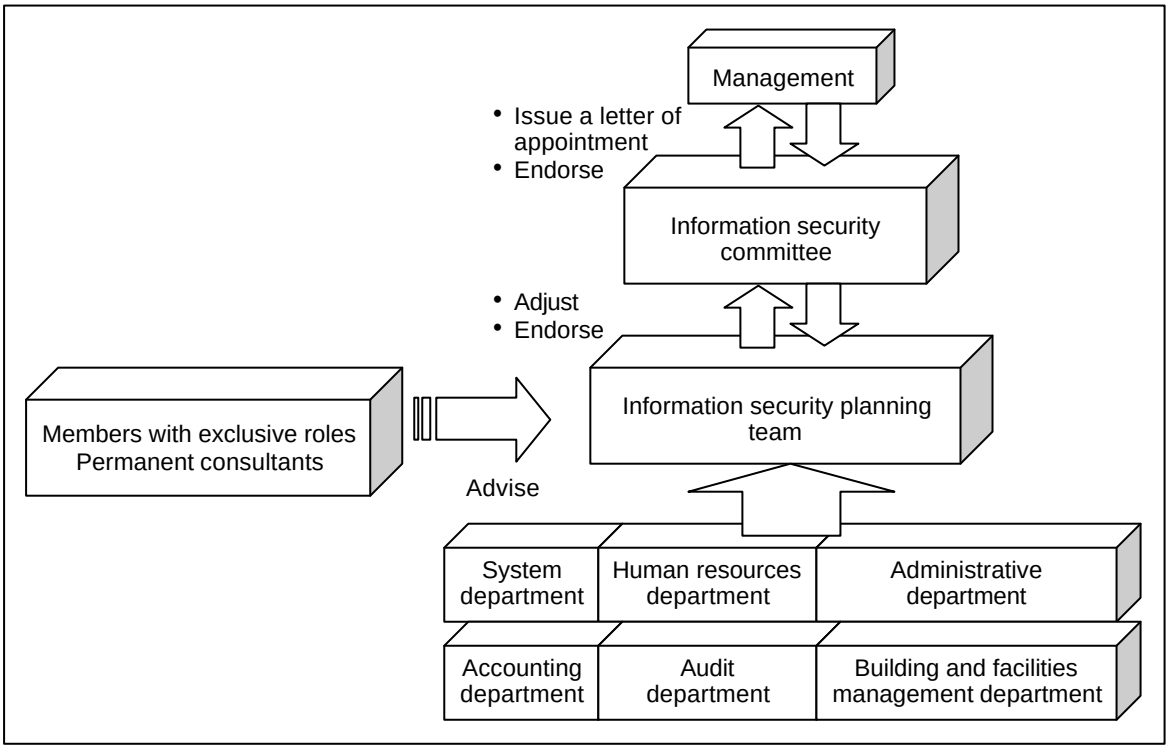


Figure 5-4 Organizational Structure for Establishing an ISMS

Table 5-2 Example of Organizational Structure for Establishing an ISMS in the Medical Field

Management	The director of a hospital, executives (such as the executive director, senior managing director, or managing director)
Information security committee	Can be additional posts in the management committee for medical security Chairman: the assistant director of a hospital Vice chairman: the medical security manager, computing room manager (or director of the information planning department) Committee members: the director of the medical service department or hospital, the director of the pharmacy department or section, the director of the nursing service department (or the general director of the nursing service department), the director of the purser department or the manager of the purser department, the medical security manager, and the computing room manager (or the director of the information planning department)
Information security planning team	Members of the information management department in the computing team, members of the medical security management, members of the business planning team
Departments:	The medical service department, nursing service department, clinical examination department, pathology diagnosis department, radiation department, pharmacy department, regional alliance office, blood transfusion department, surgery and anesthetization department, emergency medical services department, nutrition department, rehabilitation department, home visit services department, medical services accounting department, human resources department, and the purchase (and supply) department

The sample organization structure shown in Table 5-2 is based on a large-scale hospital with at least 500 beds. Middle or small-scale medical organizations does not need to build a structure from every department, but may build a structure using just the organizations and employees who perform management across the organization.

(1) Roles of the Information Security Committee

The ISMS related documents planned by the organization, led by the information security committee, should be reported to stakeholders as rules approved by the organization's management as needed, and reviewed regularly.

The committee should be responsible for how information assets the organization possesses are handled, and should have an understanding of information security as an organization which is sufficient for directing tasks and being able to get things done.

The information security committee plays a leading role for the ISMS in the organization. The following shows examples of the roles the information security committee can play.

- Being the organization that considers the preparation of an environment for risk management
- Being the organization that determines the basis of the content of ISMS related documents, when these are planned
- Considering measures or revising them to further ISMS during the implementation phrase
- Being the organization that considers what measures to take if a security issue occurs during the operation phrase
- Being the organization that considers improvements based on the results of assessment of ISMS operations

(2) Roles of the Information Security Planning Team

The planning team, which is responsible for operations while the ISMS is being established, should consist of members who have a broad understanding of the important information assets within the applicable range, and have enough knowledge to consider how to handle this information. For example, when determining how to handle information assets, there might be different opinions between departments within the applicable range and so there might be a need to adjust the way they benefit or suffer from the plan. The planning team is required to work with stakeholders as a coordinator of conflicts such as these, across the boundaries of departments. To do this, they need communication skills, founded on their ability to coordinate and experience, as well as a high level of knowledge about security.

(3) Specialists and External Consultants

An organization should collect members (if possible, members with one exclusive role) at its own cost before establishing the ISMS. However, the knowledge and experience required in the range for "information security" varies from "IT," to "managerial decisions" and "an understanding of the business," and its members are required to have the ability to look at those areas in balance and as a whole.

The people who have carried the main operations in an organization should know these best. However, they may make decisions based on their own specific point of view. One of the criteria given, "employing external specialists and consultants," is likely to give a macroscopic viewpoint to this decision and function as a way of keeping in touch with the latest information. It is a good idea to use their expertise where necessary, for example by bringing in observers to the information security committee, reviewing the defined documents and planning an audit schedule. However, external specialists and consultants are only people supporting the establishing of the ISMS, and not the stakeholders themselves, so giving them all the authority, including the authority to make final decisions, should be avoided.

In addition, since these people are likely to be able to access highly confident information such as medical information, it is recommended that a nondisclosure agreement is agreed with them, and that the liabilities in the event of judicial action are clarified, given that there is a possibility of information leaks via people.

5.2.2.3 Endorsement from Management

The management is required to present "an information security policy," giving the organization's vision of information security, and to be committed to supporting ISMS activities. This commitment does not mean merely a stamp of endorsement on the completed "information security policy." For more information, refer to "6.1 Management Commitment" in this guide.

The requirement "(V) Obtain endorsement from management" means that it is necessary to establish an information security policy as evidence of a commitment by management to establishing the ISMS. Many other documents describing ISMSs also state that "the information security policy must be endorsed by management."

If management is actively involved in deciding the organization's attitude about how to work on information security, and continues to bear that responsibility and improve the system, information security will have a secure place as part of the culture of the organization.

In organizations where there is a widespread awareness of information security, it is likely that members will naturally take the action intended by management. This is a very important point in rapidly changing environments.

In an organization whose business environment is quickly changing, if processes become stuck in the same pattern, updating them will take a long time, and it may require continual large efforts to ensure that actual operations comply with policy.

In this case, too, if activities are carried out to spread awareness of information security as part of the culture of an organization, even in large-scale organizations with various industry and business categories, members will come to take actions on security in the same way.

5.2.3 Step 3 Planning a Systematic Approach to Risk Assessment

The previous sections have explained "defining the applicable range for ISMS" and "planning the policies for establishing an ISMS." Step 3 will explain about clarifying risk assessment procedures and determination criteria to prepare for the risk assessment required to establish the ISMS. In "Step 4 Identifying Risks" the information assets and their risks will be identified, in "Step 5 Performing risk assessment" the scale of the identified risks will be analyzed, and then in "STEP 6 Perform Risk Treatment" the action to take for each risk will be determined. These are described in a simple and easy-to-understand way for medical organizations.

5.2.3.1 Risk Assessment and Requirement

A risk assessment identifies the risks related to the identified information assets and determines their scale following the procedures set out. (Reference Criteria: "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

Risk assessment makes it possible to understand the following issues related to the information assets an organization possesses.

- What kind of threats exist
- How frequently the threats take place
- How much the assets are affected when the threats occur

As stated in the comparison between ISMS and medical security management in "5.1 The Relationship between the Flow of Operations for Managing Medical Security and Procedures for Establishing ISMS" in this guide, it is also critical to identify risks and analyze and evaluate the magnitude of their effects, in order to take the appropriate action, and ensure medical security.

"New risks and risks that have not been experienced" which have not yet been prepared for in medical security management occur continuously in the information technology (IT) field. These risks must be also considered if appropriate action is to be taken. Make use of the methods used in the ISMS for information assets for assessing new risks and risks that have not been experienced.

5.2.3.2 Planning a Systematic Approach to Risk Assessment

The ISMS certification criteria state that clarifying risk assessment procedures and determination criteria is "planning the systematic approach for risk assessment," as described below: (Reference Criteria: "Clause 4-2. (1) Establishing ISMS" in the ISMS certification criteria (Ver. 2.0))

This activity is necessary, especially if more than one person is responsible for risk assessments for various information assets distributed across the organization.

The following are carried out during the process of establishing a systematic approach to risk assessment:

(1) Selecting an appropriate analysis method
(2) Documenting the assessment procedures
(3) Defining a policy and setting a goal for risk treatment
(4) Identifying the allowed risk level

(1) Selecting an appropriate analysis method

There are various ways of performing risk assessment. Each method has its own characteristics, and both advantages and disadvantages. It is therefore necessary to understand the different methods and their advantages and disadvantages to select a risk assessment method suited to the organization's characteristics.

TR X 0036 "Guidelines for the Management of IT Security; GMITS) introduces the risk assessment methods and lists the four approaches shown in Figure 5-5.

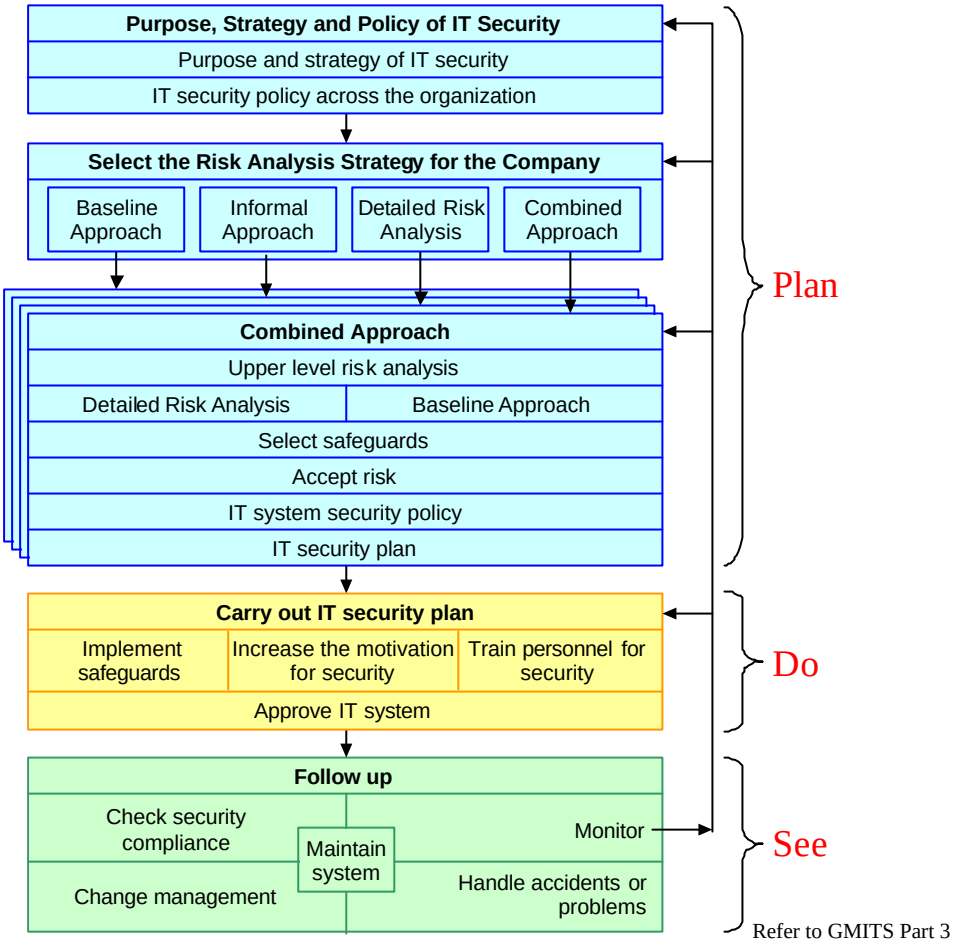


Figure 5-5 Security Management

1) The Baseline Approach

Security is handled without a risk assessment, by referring to general information security criteria and the standards and guidelines used in a specific business or industry.

[Characteristics]
Since this is easy, it can reduce the time and cost required for risk assessment. However, the guidelines may not suit some organizations.

2) Detailed Risk Analysis

Risks are evaluated in terms of the possible effects, threats and vulnerabilities caused by loss of confidentiality, integrity, or availability of information assets, based on their practical expected likelihood given the controls currently in place.

[Characteristics]
Since this makes accurate risk assessment possible, it can be used to select the appropriate controls effectively based on the risk. However, risk assessment takes time and is costly.

3) The Combined Approach

Generally, this is an approach that combines the baseline approach with detailed risk analysis.

[Characteristics]
This approach compensates for the advantages and disadvantages of the two other approaches. However, if the important assets are not identified properly, this approach loses its advantages.

4) The Informal Approach

This approach involves analyzing risks based on the experience or judgment of the organization or person responsible.

[Characteristics]
This makes it possible to do risk assessment without learning new techniques. However, it is possible that mistakes will be made, or procedures will be overlooked, since there is no structure.

The important thing when selecting a risk assessment method in a medical organization is to use a method which suits the facilities and scale of the medical organization you belong to. For example, there are various facilities in a hospital, offering things such as outpatient services, examinations, wards, and rehabilitation, and each has information processing systems where data is exchanged with medical instruments or other systems. In this case, it might be a good idea to use the baseline approach to identify risks, by checking against a check list of possible risks, and then take the minimum necessary action. In a small-scale hospital or clinic, since there is limited equipment and information, it will be possible to use detailed risk analysis to perform more accurate risk assessment.

- The Baseline Approach

Unlike detailed risk assessment, described later, the baseline approach does not analyze the risks themselves for each information asset.

Security is treated in the same way throughout the organization, by referring to general information security criteria and the standards and guidelines used in that specific business or industry. This approach employs controls that can be carried out, allowing the organization to reinforce its handling of security so that there are no missing or overlooked risks.

In the baseline approach, the following two main procedures are carried out:

- Determining the baseline
- Performing gap analysis

The baseline approach creates unique "measurement standards" for information security management to be achieved by the organization. Generally, these measurement standards are called a "baseline."

However, the ISMS certification criteria only define a summary of one management framework for its information security management standards.

If you feel that it does not contain detailed enough descriptions of the controls that you actually want to use, and you want to obtain more detailed information, be sure to refer to JIS X 5080 (ISO/IEC 17799). In particular, for information on newly employed controls, read JIS X 5080 thoroughly. Some normative references are also given in these certification criteria. Refer to these and the following standards.

- BSI-DISC PD3005:2003
- TR X 0036-4

Also refer to the "reference materials" in Annex A of this guide, which lists the laws, guidelines, reports and literature that can be referred to as sample controls for baselines.

There may also be chances to obtain other useful information sources. These include standards and systems for information security that are expected to be planned in the future, and know-how from external consultants. Before determining whether or not it is possible to implement a certain control in practice, collect a suitable amount of information on the control, and consider whether or not the level of information security management that the organization requires can be achieved.

The following is a description of gap analysis.

The purpose of gap analysis is to understand the compliance status with the standards the organization sets.

Compare the management level required by the standards with the actual management level of the business managers to check for areas where there is a big difference, areas where controls obviously need to be applied," and "areas to which too many controls have been applied."

Figure 5-6 shows the deviations between the actual level of measures and the "required guarantee level" set by the organization for each information asset. Although the required guarantee level shown in Figure 5-6 is expressed as a single grade, the required guarantee level is by nature not uniform, but is determined separately for each information asset, based on the attributes and properties of the information asset and its importance within the organization.

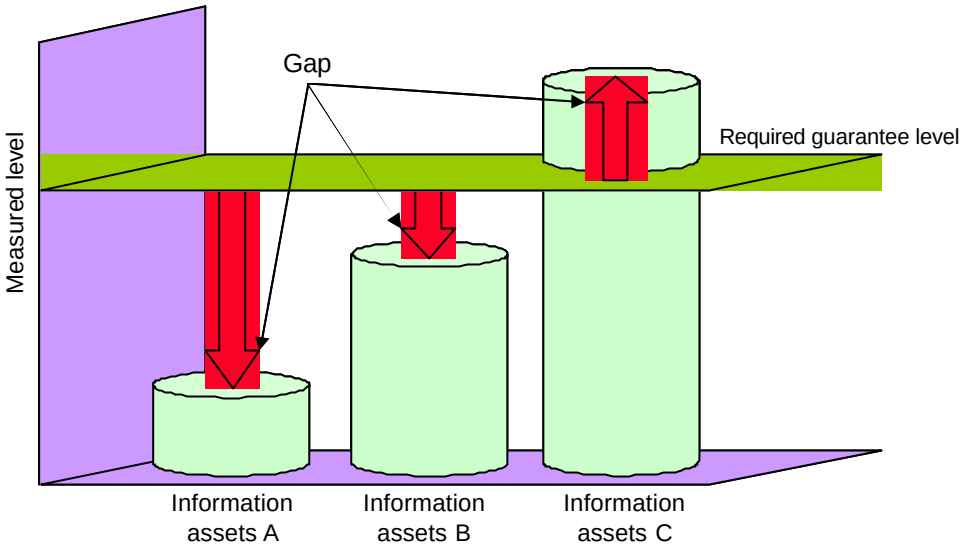


Figure 5-6 Required Guarantee Level

- Detailed Risk Analysis

In detailed risk analysis, the risks related to each information asset are identified individually (see Figure 5-7).

How frequently a risk develops depends on factors such as the probability of occurrence (developing) of a threat, the possibility of the misuse of a weak point in management (vulnerability), and how appealing the information asset is to attackers.

It is therefore necessary to define the range of risk analysis. In cases where processes are mixed together in a complicated way, definitions must be made cautiously, as narrowing the range without sufficient reason will increase the amount of unnecessary task later, or result in risks being ignored.

Figure 15: Risk Management Using Detailed Risk Analysis

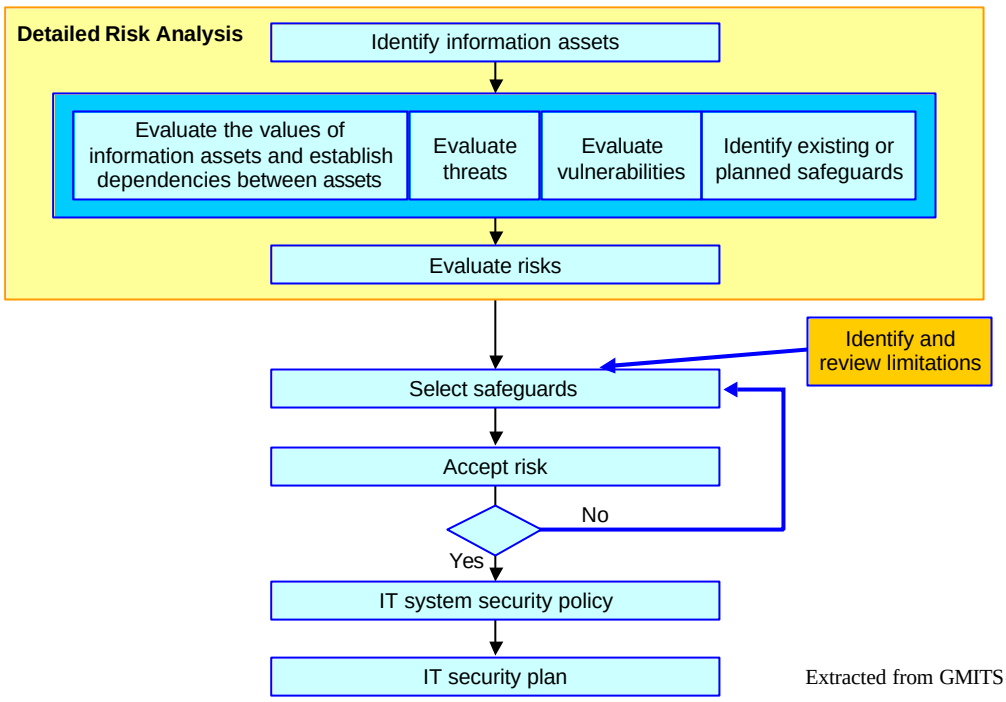


Figure 5-7 Risk Management Using Detailed Risk Analysis

- The Combined Approach

Generally, the combined approach, which combines the baseline approach with detailed risk analysis, is thought to be most effective.

However, it is not easy to determine which approach should be used for a certain situation. The decision on the best approach depends on the security requirements for the information assets (such as business requirements, legal and regulatory requirements, and contractual security obligations, as described earlier). The purpose of the combined approach is to check the risk environment surrounding each information asset, use an appropriate approach for risk analysis, allow the different approaches to compensate for the other's weak points, and to carry out effective risk analysis over the whole applicable range of the ISMS. It is mainly used because if the baseline approach is used alone, imperfect measures may be provided for systems with high risks which require a high level of security measures, and because applying detailed risk analysis to all systems is not practical in terms of efficiency.

Figure 5-8 shows an example of the combined approach defined in GMITS, which was mentioned above.

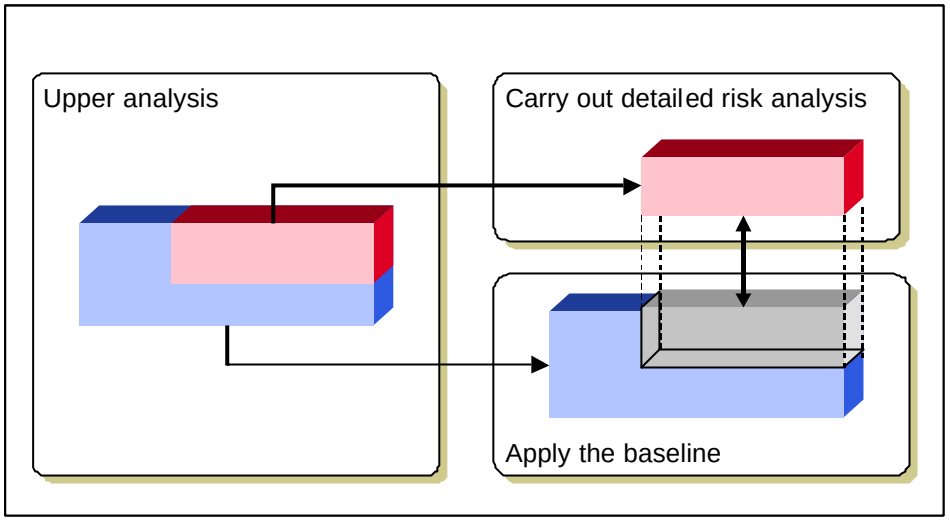


Figure 5-8　The Combined Approach

- The Informal Approach

Unlike the risk analysis methods described above, the informal approach is not a systematic approach. In this approach, generally speaking, risk sources are identified and measures are selected based on the experience and expertise accumulated for a long time by the people in charge in the field.

With this approach, it is not necessary to learn as many techniques to carry out analysis, meaning that the tasks can be started more quickly. It therefore requires fewer human resources and less time than carrying out detailed analysis.

Generally, objectivity is most important in risk analysis and evaluation. It is obvious that the results of this approach may be affected by the individual opinions of the people in charge. However, this approach can still be useful if its applicable range is limited to cases where systematic risk analysis cannot be carried out, it is combined with the other approaches and the issues below are considered.

(2) Documenting assessment procedures

Risk assessment requires that the procedures necessary to perform tasks are documented.

- Definition of risk assessment
- Purpose of risk assessment
- Method of risk assessment

"Method of risk assessment" includes the following criteria, among others:

- Criteria for determining the value of information assets
- Criteria for evaluating threats
- Criteria for evaluating vulnerabilities
- A method for calculating risk values
- How often risk assessments will be made

(3) Defining a policy and setting a goal for risk treatment

Risk treatment is performed by organizations based on the risk values calculated by performing the risk assessment.

In this step, the ways of handling risk which can be selected based on the calculated risk value in the risk management framework are made clear.

The following four ways of dealing with risk are introduced in TR Q 0008, which was mentioned earlier.

- Risk avoidance
- Risk optimization
- Risk transfer
- Risk retention

Details of risk treatment are also described in "5.2.6 Step 6 Performing Risk Treatment" in this guide, using the example of a medical organization.

The way of handling risk selected in this step must also be entered into the ISMS document.

(4) Identifying the acceptable risk level

Here, "acceptable risk" indicates the risk an organization can bear ("risk retention"). In particular, the term "acceptable" implies a positive "will" by the organization to bear the risk.

> 6. Risk acceptance A decision to accept a risk. [See TR Q 0008: 2003]
>
> (Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

The acceptable level of risk is determined in the first place from the results of risk assessment.

In this step, which is defined in the ISMS certification criteria, it is determined whether risk assessment should be performed using the risk value calculated in the procedures for risk assessment documented in (2), and then the procedures for deciding whether to accept risks are confirmed.

5.2.4 Step 4 Identifying Risks

Risk assessment starts from identifying risks. However, the risks being identified are abstract and difficult to get a handle on.

A risk is composed of a causal relationship between several risk sources. Figure 5-9 shows the relationship between risks and risk sources in TR X 0036, making it clear that a risk value is determined from the surrounding "asset values," "threats" and "vulnerabilities."

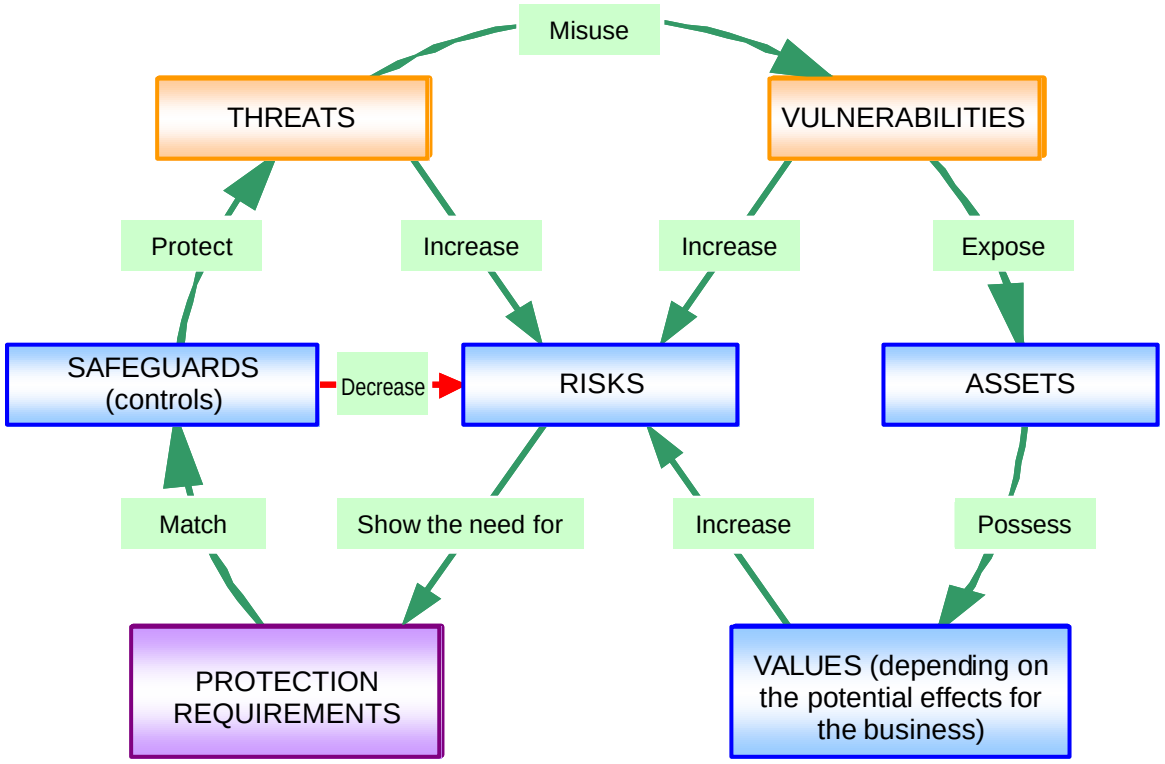


Figure 5-9 The Relationship Between Risks and Risk Sources

When risks are being identified, the following two tasks must be performed:

(1) Sorting out information assets
(2) Clarifying threats and vulnerabilities

Both of these are described below using examples.

(1) Sorting out information assets

In this step, the kinds of information assets possessed in the applicable range for the ISMS in the organization should be checked. Ideally, in order to understand the details of the objects used for ISMS management and select the appropriate control, the attributes and value of each information asset should be clarified. The ISMS certification criteria also require that a "person who is responsible for managing all the information" should be specified when information assets are sorted out.

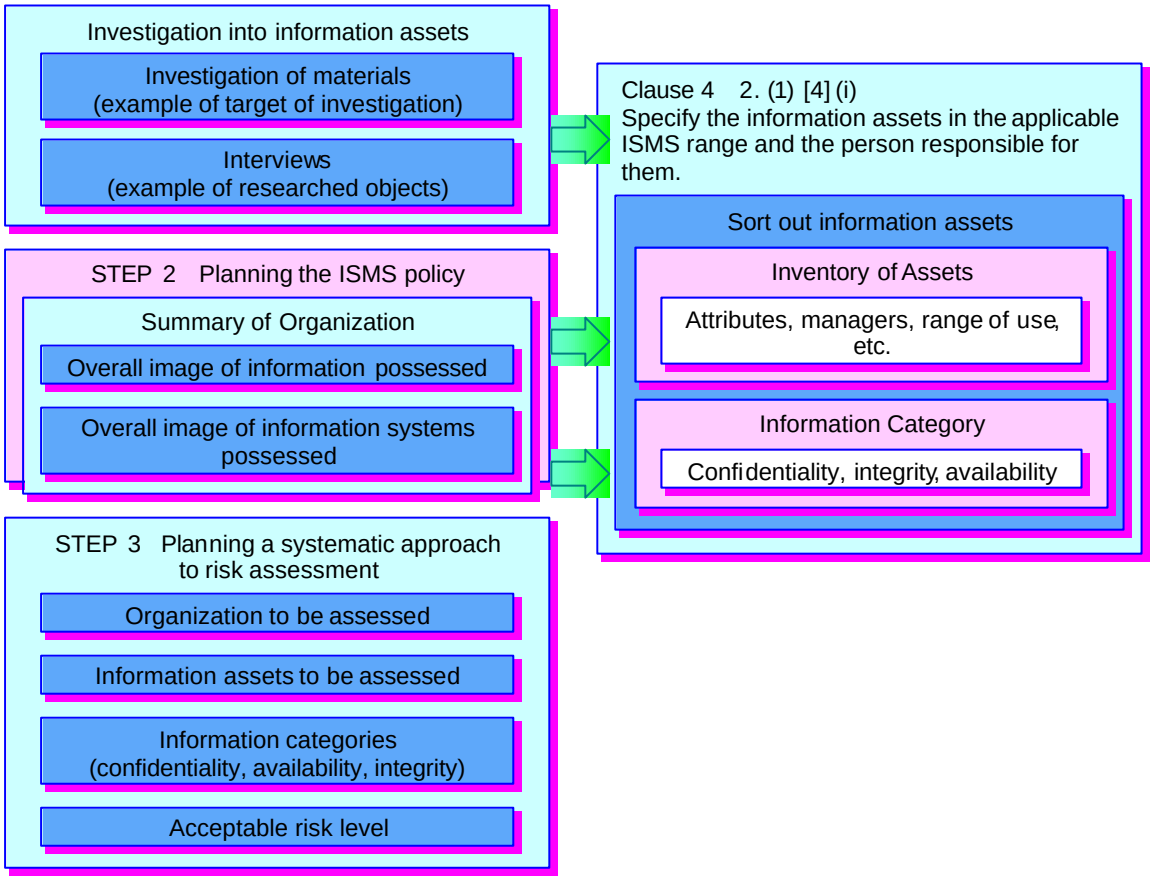


Figure 5-10 Sorting Out Information Assets

1) Preparing an inventory of assets

It is recommended that the "inventory of assets" in "5. Categorizing and Managing Assets" in JIS X 5080: 2002 is prepared.

> An inventory of assets is useful for ensuring that assets are effectively protected, and it may also be required for other business purposes [for example, for reasons related to health, security, insurance, or financial affairs (asset management)]. The process of preparing an inventory of assets is an important aspect of risk management. The organization must clearly understand its assets and their relative value and importance. Based on this information, it can set protection levels which correspond to the value and importance of these assets.
>
> (Quoted from "5.1.1 Inventory of Assets" in JIS X 5080: 2002)

Consider what information should be written in the inventory of assets, with reference to the following items:

- The person responsible for the information (the owner or manager of the information assets)
- The format of the information assets
- The storage format
- The storage location
- The duration of storage
- How assets should be disposed of
- The use of assets
- The range of users (and business processes)
- Dependencies on other processes

Identifying information assets individually and understanding their characteristics will be helpful in identifying the threats and vulnerabilities related to subsequent tasks and determining the value of assets.

2) Examples of information assets

"5. Categorizing and Managing Assets" in JIS X 5080 gives sample assets associated with information assets. JIS X 5080 classifies information assets into four categories: "information," "software assets," "physical assets" and "services," but the category "people" is sometimes added to these. Medical facilities such as hospitals and clinics are special places, where many co-medicals, such as doctors, nurses and operators, who have critical information that may affect human life, work. Consider the possible risks related to these people, and re-consider measures as required.

Table 5-3 Examples of Information Assets

Category of Information Assets	Example
Information assets (information *)	Database and data files, system-related documents, user manuals, training materials, operational and support procedures, continuance plans, alternative arrangements, recorded information
Software assets	Business software, system software, development tools and utilities
Physical assets	Computer devices (processors, display devices, laptops, modems), communication devices (routers, PBXs, facsimiles, answer phones), magnetic media (tapes and discs), other technical devices (power supplies, air conditioning devices), fixtures, old facilities
Services	Computing and communication services, general utilities (e.g. space heating, lighting, power supplies, air conditioning)
People (knowledge)	Doctors, nurses, co-medicals (people who know that information such as patients' information and medical information exists, and how to access this information)

In the above table, electronic data includes the computers processing the data, storage media and firmware. It also refers to information and dialogs on paper, physical facilities and equipment, and the like.

*: In this guide, "information assets" are called "information" in order to avoid confusion with the information asset category.

3) Grouping information assets

It is very likely that the task of sort out the information assets present in the applicable range of the ISMS will create a heavy workload.

"Grouping information assets" is a useful concept which can decrease the workload during risk analysis, and increase the effectiveness of subsequent analysis tasks.

For example, information assets with the same value or attribute (e.g., storage format, storage duration, or usage) can be grouped together. If they are of the same importance or have the same attributes and requires the same security measures, they should be grouped together so that they can be managed effectively.

First of all, information assets should be identified, to determine the appropriate security measures for the applicable range of the ISMS. It is not always important to cover all the information assets in an organization or prepare a detail inventory of assets giving the attributes of each information asset.

4) Information categories (standards for degree of effect)

After preparing an inventory of assets, evaluate the values of the assets. Information assets can be considered as the degree of effect on the important business processes in an organization.

The important factors for risk assessment are identifying and evaluating information assets based on the needs of the organization. For this reason, the values of the main information assets must be evaluated by a manager who understands the business of the organization very well (also called an "information owner").

An organization must develop unique determination criteria for the three C.I.A. elements when judging the values of information assets. Tables 5-4 to 5-6 show sample standards for confidentiality, integrity and availability.

Table 5-4 Sample Standards for Confidentiality

Information Assets (Confidentiality)	Class	Description
1	Published	Can be disclosed and provided to third parties If contents were leaked, there would be little effect on medical operations.
2	Internal Use	Can only be disclosed and provided in a hospital (not available to third parties) If contents were leaked, there would not be much effect on medical operations.
3	Secret	Can only be disclosed and provided to specific parties and departments If contents were leaked, there would be a large effect on medical operations.
4	Highly confidential	Can only be disclosed and provided to specific parties If contents were leaked, there would be large or fatal effects on medical operations.

Table 5-5 Sample Standards for Integrity

Information Assets (Integrity)	Class	Description
1	Unnecessary	Used only for reference. No possible problems.
2	Necessary	If contents were falsified, there would be problems, but these will not affect medical operations very much.
3	Important	If integrity were lost, there would large or fatal effects on medical operations.

Table 5-6 Sample Standards for Availability

Information Assets (Availability)	Class	Description
1	Low	If the information became unavailable, there would be no effect on medical operations.
2	Middle	If the information became unavailable, there would be some effect on medical operations. However, alternative methods could be used for operations, or the process could be delayed until the information became available.
3	High	If the information was not surely available when needed at any time, there would be large or fatal effects on medical operations.

The value of individual information asset is mainly determined by the information manager subjectively, based on the information categories defined in advance, as shown in the examples in Table 5-3.

(2) Clarifying threats and vulnerabilities

The ISMS certification criteria (Ver. 2.0) define risk sources as a set of "threats" to which information assets might be exposed and "vulnerabilities" in management issues. A risk source is a factor that makes risk possible.

> Reference Risk source: A thing or actions that has a potential result. [See TR Q 0008:2003]
>
> (Quoted from section 7 in "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

1) Identifying threats

A "threat" is a potential cause of a security incidents that may cause an information system or organization to be lost or damaged. Threats are caused by "vulnerabilities," which will be described later, and affect the organization of the operations or the organization if they occur. The scale of a threat is determined by evaluating the probability of its occurrence for each factor or information asset.

TR X 0036-1 categorizes and describes threats as shown in Table 5-7.

Table 5-7 Categories of Threats

Artifact Threat		Environmental Threat
Deliberate (planned) threat	Accidental Threat	Environmental Threat
deliberate ⇒ D	accidental ⇒ A	environmental ⇒ E

As with the case of determining the value of information assets above, the person responsible for information management identifies threats that may affect their information assets, based on information on threats provided by users of information, stakeholders in other departments, and external specialists, and creates a list, as shown in Table 5-8.

Table 5-8 Examples and Categories of Threats

Threat	Category (D, A, E)
Earthquake	E
Blackout	D, A, E
Static electricity	E
Operating mistake by operator	D, A
Shortage of human resources (staff)	A
Faulty ID	D
Malicious software	D, A
.....	.....

Refer to the examples in Table 5-8 etc. when identifying threats.

For example, deliberate (planned) threats should be identified and categorized into factors based on the characteristics, features, and vulnerabilities of information assets, taking into account available resources such as the motives of attackers and skills required for attacks.

Accidental threats should be identified using the probabilities of local condition, extreme climate or the potential effects caused by mistakes by personnel or operation errors.

The frequency of occurrence of the treat should then be evaluated.

Frequency must also be sorted out together with the other related departments, as when identifying threats. Based on the list of threats created by the manager, threats should be reviewed based on experience of operations and statistical data that has already been collected.

While the precise method depends on how much accuracy is required for the evaluation, threats are typically divided into three categories: "Low," "Middle," and "High." Table 5-9 shows examples of criteria for determining categories if threats are categorized in this way.

Table 5-9 Criteria for Determining Threat Categories

Threat		
Probability of occurrence	Category	Description
1	Low	There is a low probability. The frequency of occurrence is once a year or less.
2	Medium	There is a moderate probability. The frequency of occurrence is once every half a year or less.
3	High	There is a high probability. The frequency of occurrence is once a month or more.

2) Identifying vulnerabilities

Vulnerabilities are weak points and security holes that may cause threats, and which are specific to an information asset. Vulnerabilities do not cause any damage by themselves, but they may help threats to occur or cause damage or failure. In other words, the vulnerabilities with no potential threats do not need to be taken care of.

Sample categories for vulnerabilities are shown in Table 5-10. When a list of vulnerabilities is made, it will be necessary to sort out their relationship with threats, as shown in Table 5-10.

Table 5-10 Identifying Vulnerabilities

Category of Vulnerability	Examples of Vulnerabilities	Examples of Related Treats
Environment, facilities	Lack of physical protection such as doors and windows	Theft
	Unstable power facilities	Blackout, operation error
	Local conditions that mean that the facilities are easily affected by disasters	Flood, earthquake, disaster
Hardware	Hardware easily affected by changes in temperature or humidity	Malfunction, operation error
	Failure to maintain storage media	Malfunction, information leak
Software	Error in software specifications	Software failure, operation error
	No access controls	Spoofing, tampering, information leak
	Improper passwords	Unauthorized access, tampering, information leak
	No audit trail (log management)	Unauthorized access
	No backup copies	Lack of ability of restore
.....	.....	.....

Vulnerabilities can easily be identified if they are considered in relation to the characteristics and attributes of information assets.

For example, laptop computers has the characteristics "good mobility," "low resistance to shocks" and "can be used in public spaces." These characteristics also indicate vulnerabilities to the threats "being stolen or left behind," "malfunction" and "information leak."

This means that there are totally different vulnerabilities in different environments, such as the environment of use or storage location of the information assets, the progress (stage) of the process, the format and the time. Even information assets of a single type (e.g. laptop computers) may need to be managed in different categories, for example "laptop computer (internal use)" and "laptop computer (external use)" depending on the use and characteristics of that asset.

Evaluating vulnerabilities means evaluating the level of weakness of an information asset. If a weak point is exposed to the public without any security measures being taken, it can be considered to have a High vulnerability. Although the extent to which assets should be categorized will differ for different organizations, vulnerabilities are typically categorized as "Low," "Medium" or "High," as with threats.

5.2.5 Step 5 Performing Risk Assessment

Risk assessment can be performed by determining assessment procedures, creating an inventory of information assets, and clarifying the categories of importance of information assets and the criteria for evaluating threats and vulnerabilities.

The importance of information assets is evaluated by the person responsible for management, who categorizes them into the C.I.A. factors described above.

In some cases, it may be better in terms of objectivity and effectiveness to ask a specialist to evaluate threats and vulnerabilities. An information security auditing system can also be used to enable external specialists to help evaluate vulnerabilities.

(1) Calculating Risk Values

A risk value can simply be calculated using the following formula and the values for the "value of information assets," "scale of threats" and "level of vulnerability."

Risk value = "Value of information assets" × "Threats" × "Vulnerabilities"

(Example)

Elements of information assets	Value of assets
C: confidentiality	4
I: integrity	2
A: availability	1
Threat	3 (if information is leaked to unrelated people, trust will be lost)
Vulnerability	3 (privileges are given to all operators)

The risk value for this case is calculated as follows:

- Risk value for confidentiality: $4 \times 3 \times 3 = 36$
- Risk value for integrity: $2 \times 3 \times 3 = 18$
- Risk value for availability: $1 \times 3 \times 3 = 9$

Figure 5-11 Sample Calculation of Risk Values

After risk values have been calculated, a "look-up table of risks" can be created in a matrix as shown in Table 5-11, to help proceed with subsequent tasks effectively.

Table 5-11 Sample Look-Up Table of Risk Values

	Threat								
	1			2			3		
	Vulnerability								
Information Assets	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

For example, acceptable risk values are as shown in the sample list in Table 5-12.

Table 5-12 Sample List of Acceptable Risks (1)

	Threat								
	1			2			3		
	Vulnerability								
Information Assets	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

Range in which risks are acceptable
Range in which action should be taken to deal with the risk

Table 5-12 "Sample List of Acceptable Risks (1)" assumes that [9] is set as the "acceptable risk level" that defined in section 5.2.3.2 (4) of this guide. In the matrix of risk values created when evaluating risks (the "look-up table of risk values"), the current management of the risks of less than "9" should be accepted, and accepted risks should be managed as "residual risks."

Table 5-13 Sample List of Acceptable Risks (2)

	Threat								
	1			2			3		
	Vulnerability								
Information Assets	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

Range in which risks are acceptable

Range in which action should be taken to deal with the risk

In Table 5-13, "Sample List of Acceptable Risks (2)," if the value of an information asset is the maximum value, "4," action must be taken for it unconditionally, and thus only risk values less than "4" are accepted.

This risk acceptance list only shows the risk environment during risk assessment and therefore, the risk values must be reviewed whenever the value of information assets or the environments of threat and vulnerability changes.

(2) Notes During Working

During risk assessment, it is necessary to plan systematic procedures and follow them during implementation.

For example, risk measurement is described as follows in "Internal Control in the New Era of Risks - Guidelines for Internal Control that Functions Together with Risk Management" by the Study Group on Risk Management and Internal Control of the Ministry of Economy, Trade and Industry.

> Once identified, each risk should be measured in terms of its significance for a company, on the basis of the degree of impact as well as the probability of occurrence. Although it is not always possible to measure all risks quantitatively, it is desirable that risk measurement should be conducted by using rational indices that are acceptable to all parties concerned so that risks can be compared in relative terms from a single unified perspective. One way, for instance, would be to divide the degree of impact and the probability of occurrence of a risk into "major," "medium" and "minor" and evaluate a given risk based on the combination of the degree of its impact and the probability of its occurrence.
>
> <Syncopated>

> In evaluating risk that can be measured only qualitatively, one way would be to rank the degree of its impact and the probability of its occurrence into "major," "medium" and "minor," respectively, based on an assumption substantiated by experience.
>
> (Quoted from "(3) Risk Management" under "II-1. Desirable Risk Management" in Part II in "INTERNAL CONTROL IN THE NEW ERA OF RISKS ~ Guidelines for Internal Control That Functions Together with Risk Management ~" June 2003, By Study Group on Risk Management and Internal Control)

This means that risk values may change even if the calculation method given above is used.

Risk value = "Value of information assets" × "Threats" × "Vulnerabilities"

The above formula is not based on strict logic. It may give different risk values, even for the information assets of the same type and which have similar attributes, because of the value and threats of each information asset, the results of evaluating its vulnerability and the judgment by the person responsible for the evaluation.

The risk value of an information asset can also be calculated for the evaluation by adding its values, threats, and vulnerabilities.

The ISMS certification criteria define the calculation of risk values as a requirement. However, in an extreme case, one possible choice might be adopting a framework of risk assessment determining whether a measure is needed without calculating the risk value, but instead using personal judgment, considering only the points.

For example, the variations in the judgments of the people responsible for evaluation can be equalized to some extent if enough examples are prepared in the initial phases of analysis, and enough explanation is given to the people responsible.

These can be also used as a guide to validating the current measure level, and collected and checked to aid the awareness of information managers who are using the relevant information assets daily (or managing them normally) and evaluating risk values.

5.2.6 Step 6 Performing Risk Treatment

> 11. Risk treatment: The process of selecting and performing controls for changing risks. [Refer to TR Q 0008: 2003]
>
> (Quoted from "Clause 3. Terms and Definitions" in the ISMS certification criteria (Ver. 2.0))

Risk treatment means making any of the following four selections:

- Using the appropriate controls
- Retaining risks
- Avoiding risks
- Transferring risks

Risk treatment should be performed on risks being managed, as clarified in risk assessment.

(1) Using the appropriate controls

The method of "using an appropriate control to reduce risk" is the most common form of risk treatment.

For example, this includes applying the detailed controls described in the appendix of the ISMS certification criteria, or other additional controls.

The concept of risk reduction is shown in Figure 5-12. In this case, it can be seen that the risk can be reduced by "lowering the probability of occurrence of the risk" or "lowering the effects if the risk occurs."

The meanings of the symbols in Figure 5-12 are as follows:

R: Risk
C: Control to reduce risk
E: Exposure after action is taken

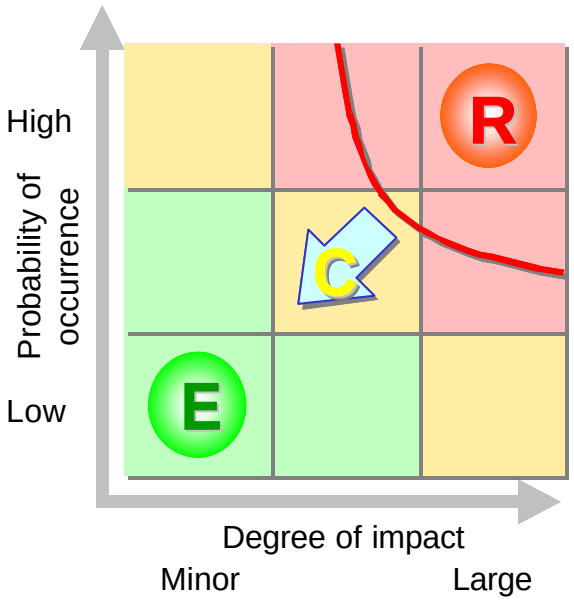


Figure 5-12 Concept of Risk Reduction

One example of reducing the probability of a risk occurring is to "manage people entering and leaving rooms more strictly."

A possible measure to reduce the degree of effects would be "to increase the frequency of backups, to increase the amount of data that can be restored."

In the real world, risks cannot be completely removed by taking measures. In many cases, a measure is performed by investing enough to keep any risks which may occur under the acceptable level, based on ensuring the convenience or a comparison between the cost required to carry out the measure practically and its effects. The residual risks are managed via "risk retention," which is described in the next section.

(2) Retaining risks

"Risk retention" is defined as follows in the ISMS certification criteria.

> Reference Risk retention: covering the losses caused by a certain risk or accepting its benefits.
>
> (Quoted from "Clause 4-2. (1) Establishing the ISMS [6] in the ISMS certification criteria (Ver. 2.0))

Retained risks can be divided into the following two categories:

- Risks that are identified and accepted
- Risks that are not identified, and remain in an organization

Risks that are retained are risks that are identified and accepted. If a risk clearly satisfies the basic policy and evaluation criteria for risk acceptance in an organization, it will be accepted intentionally and objectively.

(3) Avoiding risks

"Risk avoidance" means performing methods to consider the risk treatment and then abolishing an operation or discarding information assets to avoid a risk if it is impossible to prevent it adequately for a reasonable cost or no appropriate measures for dealing with it are found.

For example, personal information is associated with risks such as information leaks and a lack of availability of the appropriate information when required. A possible treatment for preventing these risks is for the person responsible to identify the personal information which the business needs less and discard this data, if the personal information depends on data which each person responsible possesses.

If the organization has a mailing list that does not contribute to its sales, it is subject to risks such as the leakage of personal information by mistake or receiving viruses, so a possible treatment for risk would be to close the mailing list.

These plans are ways of avoiding risks.

For example, if there is a risk that personal information may be leaked, and it is possessed by an individual, there is a risk that it may not be possible to disclose the information appropriately. In contrast, if personal information is of little importance in business, a possible treatment for the risk would be to discard the information.

(4) Transferring risks

Risk transfer means transferring risks to other parties (other organizations or companies) by concluding a contract.

Risk transfer can be divided into two main categories: outsourcing measures for information assets and information security, and using an insurance system as a kind of finance for risks.

As examples of the former method, there is the method of using a collocation service to leave the information assets at an external data center and the method of outsourcing the use of assets. If a medical organization wants to transfer risks by a method like this, such as outsourcing, it is important to clarify the risks that have been transferred, the risks that have not been transferred and the risks that are newly created by the transfer. To clarify what risks have been transferred, it is also important to include security measures in a contract.

The appendix to the ISMS certification criteria defines the following controls for reducing risks that are created by transferring risks.

4. (3) Outsourcing Purpose: To maintain the security of information when the responsibility for processing information is outsourced to another organization.		
Control		
4. (3) [1]	Security requirements for outsourcing contract	The security requirements for an organization that is outsourcing a whole or a part of its management and control of its information system, network or desktop environments must be defined in the contract concluded between the two parties.

(Quoted from "(3) Outsourcing" in "4. Detailed Controls" in the ISMS certification criteria (Ver. 2.0))

In risk management, if the controls defined in the ISMS certification criteria cannot be applied, or if the risk value is above the acceptance level even after the controls have been applied, risk transfer should be considered.

A typical example of risk transfer in the form of risk finance is the use of insurance. For example, this is suitable in a case where the unavoidable threats caused by an earthquake and others would have a great impact on business. Insurance should be considered since this risk has a low probability of occurrence.

In modern times, insurance products to insure companies against the failure of information systems can be bought. For example, this insurance may pay for the costs to allow the system to recover from the results of a risk and buy new equipment.

As this coverage is only a part of the financial insurance against damage, risk treatment using insurance alone has limitations. (For example, it is difficult to compensate for damage to the image of a medical organization by occurring information leakages using insurance.) For this reason, risk treatment using insurance is not effective in all cases. It should only be used as a backup when the use of controls cannot compensate for a risk.

It is also necessary to check the terms of an insurance policy carefully before concluding it, as there will be details such as negligence clauses.

5.2.7 Step 7 Selecting the management goals and controls

From the "Detailed Controls" appendix of the ISMS certification criteria, select a management goal and controls to use for risk treatment. If there is no appropriate management goal or control in "Detailed Controls," an additional control can be created.

It is important to show that this selection is valid, using the results of the risk assessment and risk treatment process.

5.2.8 Step 8 Preparing a Statement of Applicability

In this step, document the management goal and control selected in Step 7, and the reason for choosing them, and prepare a statement of applicability.

It is also necessary to record reasons why any management goals and controls in the "Detailed Controls" appendix have been excluded from the applicable range.

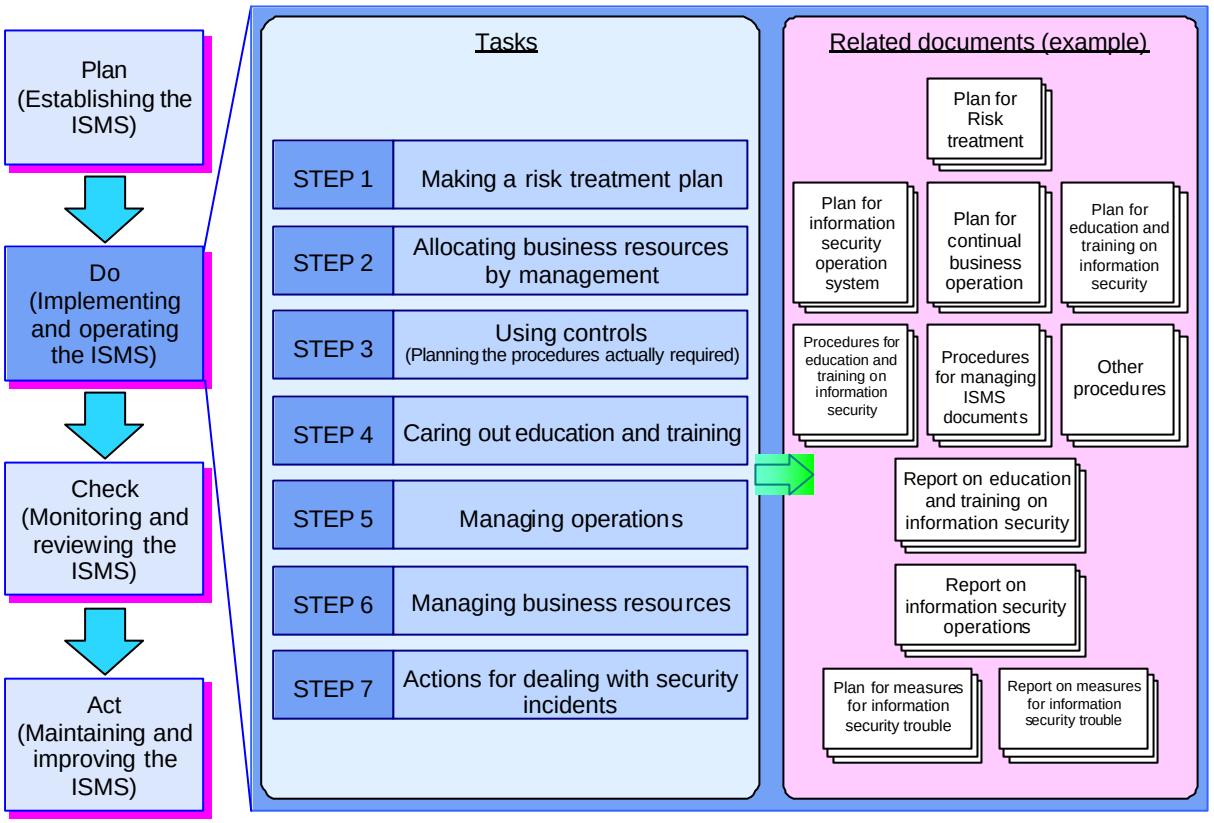
5.2.9 Step 9 Approving residual risks and allowing the ISMS to be carried out

An ISMS has been carried out fully when residual risks are (or are planned to be) below the acceptance risk level or when the management has checked and approved the risk retention as appropriate.

This concludes the nine steps for "Establishing the ISMS." Please note that the steps up to step 6 (risk treatment) are especially important. Recording the results of the treatments and having them approved by a director or the executives of the hospital will show the effect they have on information security for patients and the local society. In addition, if an information security accident or trouble occurs and a lawsuit is brought, these activity records will be very important evidence. We recommend that the results are recorded, with reference to this guide.

5.3 Implementing and Operating the ISMS (Do)

"Clause 4-2. Establishing and manage operations of the ISMS" in the ISMS certification criteria defines the procedures for implementing and operating an ISMS in seven steps, shown in Figure 5-12.
(Reference Criteria: "Clause 4-2. (2) Establishing and operating an ISMS" in the ISMS certification criteria (Ver. 2.0))



Note: All document names are examples

Figure 5-13 Procedures for Implementing and Operating ISMS

5.3.1 Step 1 Making a Risk Treatment Plan

A risk treatment plan is used to clarify the activities that will be carried out to reduce unacceptable risks and a plan for carrying out the controls chosen based on the results of risk assessment.

Business resources required for the risk management are allocated, and tasks are actually carried out, based on this risk treatment plan.

The management is responsible for ensuring that this plan is made. Details of the plan are given in the next chapter "6. Responsibilities of Management." The ISMS certification criteria require that the appropriate activities, responsibilities and priorities of management are defined in the risk treatment plan.

Any errors in the risk treatment plan will mean that controls are not put in place properly, and so all necessary conditions should be considered when building the plan.

A risk treatment plan must not only define controls for reducing risks, but also controls to check whether the controls carried out are working appropriately and effectively and a plan for carrying out controls to detect any errors.

For example, assume that security products such as virus protection, a firewall, and access controls are to be added. When these products are added, in addition to settings for improving security, the plan should include information to indicate the status of these settings and procedures for making settings, taking into account errors detected based on the results of analyzing process logs.

In addition, if an expensive device is required to perform analysis, controls to make sure that it will be effective must be also taken into account during investigation.

The risk treatment plan allows you to easily understand the execution status of the controls for the risks identified by an organization and the progress of the additional measures for the residual risks that have not been reduced to the acceptable level or below.

The following four items should ideally be included in the risk treatment plan:

- Daily schedules
- Priorities
- Detailed work plans
- Responsibilities for carrying out controls

5.3.2 Step 2 Allocating Business Resources by Management

For more information, refer to "6. Responsibilities of Management" in this guide.

5.3.3 Step 3 Using Controls

Use controls starting from the control with the highest priority, following the risk treatment plan.

At this point, document the procedures for operating controls and the case of a security incident or accident, so that they can be understood by stakeholders.

5.3.4 Step 4 Carrying Out Education and Training

For more information, refer to "6.2.2 Training, Awareness and Competence" in this guide.

5.3.5 Step 5 Manage Operations

Prepare procedure manuals to manage the operations needed for the controls in place. All procedure manuals prepared must clearly state the responsibilities of the stakeholders, such as operation managers and users.

The following are examples of items to include in procedure manuals:

- Procedures for backing up
- Procedures for changing
- Procedures for restoring
- Procedures for checking that the system is operating normally
- Procedures for action to deal with emergencies

5.3.6 Step 6 Managing Business Resources

For more information, refer to "6.2 Resource Management" in this guide.

5.3.7 Step 7 Actions for Dealing with Security Incidents

To minimize the damages caused if a security incident occurs, it is important that the damage caused is detected appropriately and then that appropriate action is taken.

It is important that procedure manuals for taking action in a security incident are prepared and checked regularly. It is especially important to define settings for the person responsible for action in the initial phrase, a communication and report system for stakeholders who need them and a series of procedures for taking appropriate action.

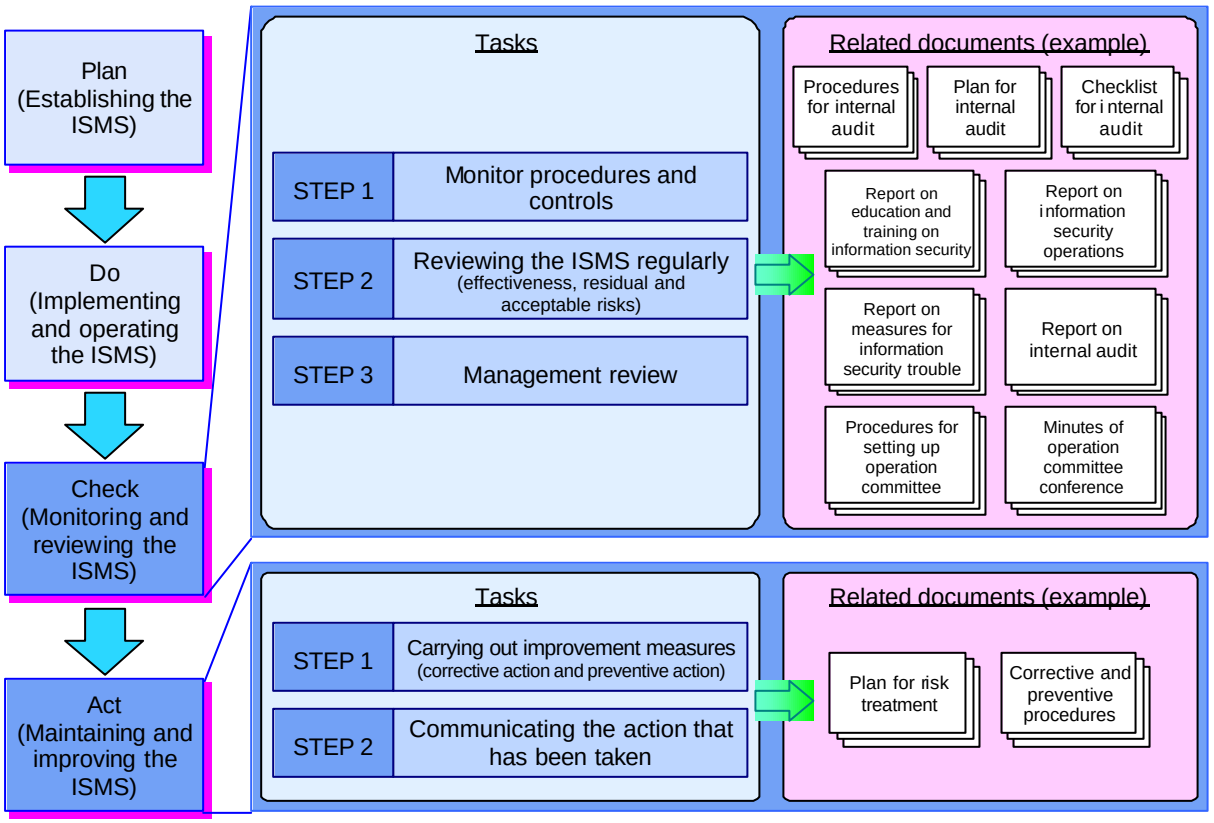
To prevent incidents from reoccurring in the future, it is also important that detected security incidents are reported and that the appropriate action to take is reflected by the whole organization. Make sure that the report on security incidents includes the following:

- Records of security incidents
- Failures of controls
- Details of actions
- Necessary additional controls, etc.

It is important that reports are input for management review so that information security can be continuously improved.

5.4 Monitoring and Reviewing the ISMS (Check) and Maintaining and Improving the ISMS (Act)

"Clause 4-2. Establishing and operating the ISMS" in the ISMS certification criteria defines procedures for (3) Monitoring and reviewing the ISMS and (4) Maintaining and improving the ISMS, as shown in Figure 5-14. (Reference Criteria: "Clause 4-2. (3) Monitoring and reviewing the ISMS and (4) Maintaining and improving the ISMS" in the ISMS certification criteria (Ver. 2.0))



Note: All document names are examples

Figure 5-14 Procedures for Monitoring, Reviewing, Maintaining and Improving the ISMS

The Check phase is mainly used to collect the input data required for management reviews. The management carries out the management review and checks whether the processes are being carried out according to the procedures determined in the first half of the PDCA cycle from "Plan" to "Do," and whether the results expected in the planning phase have been obtained. These are critical tasks in maintaining and continuing to improve the ISMS.

The input data monitored in a management review includes the following:

- Process errors and records of security incidents
- The status of security activities being carried out
- Feedback from stakeholders
- Changes in the environment (e.g., the social and technical environment, legal regulations, and the business environment)
- Feedback from internal audits

The management must make judgments on the following issues as the result of a management review.

- The effectiveness of the ISMS
- The allocation of business resources
- Residual risks and acceptable risk levels

In the Act phase, so that the effectiveness of the ISMS can be continuously improved, corrective and preventive action must be taken based on the data collected in the Check phase.

These activities are defined in detail in "Chapter 5 Responsibilities of Management," "Chapter 6 Management Reviews" and "Chapter 7 Improvement" in the ISMS certification criteria. For details, see "6 Responsibilities of Management" and subsequent chapters in this guide.

5.5 Documentation Requirements

The ISMS certification criteria require the following documents to be included in the ISMS document.

- A statement of information security policy and management goals
- The applicable range of the ISMS and the procedures and controls for supporting the ISMS

- A report of the results of risk assessment
- A risk treatment plan
- Procedure documents that the management determines are necessary to ensure that the processes for information security are planned, operated and managed effectively
- Records required by these criteria
- A statement of applicability

The following two purposes must be considered when ISMS documents are prepared:

- Establishing management procedures
- Managing the register

Please note that "documenting procedures" means "establishing, documenting, carrying out and maintaining procedures." The ISMS certification criteria clearly mentions "procedure documents" in five sections.

Clause 4 3. (1) [5]	Procedure documents that an organization determines are necessary to ensure that the processes for the information security are effectively planned, operated and managed.
Clause 4 3. (2)	The documents required for the ISMS must be protected and managed. Procedure documents should be made to define the management activities necessary to perform the following:
Clause 6 4.	Define the responsibilities and requirements for planning and carrying out audits, reporting results and maintaining records (see Clause 4 3. (3)) in the procedure documents.
Clause 7 2.	An organization must take action to remove causes of nonconformities in the way the ISMS is implemented and operated to prevent them from reoccurring. The procedure document on corrective action must define requirements for the following:
Clause 7 3.	An organization must determine action to prevent nonconformities from occurring. The preventive actions must be appropriate for the impact of the potential problems. The procedure document on preventive action must define requirements for the following:

(Quoted from the sections given above in the ISMS certification criteria (Ver. 2.0))

5.6 Controlling of Records

Records must be created, maintained and controlled as evidence that the ISMS of the organization conforms to the requirements and to show the effects of operations. This means that the records of the status of controls performed in all PDCA processes and records of all the security incidents related to the ISMS must be maintained. When doing this, it is also necessary to take the appropriate legal requirements into consideration.

The following tasks must be performed to control records.

- Documenting the controls required to identify data, store it, protect it, search it, and discard it, and documenting its storage duration
- Defining what must be record, and in what range, in the operation management process
- Defining a storage duration in line with legal requirements if there are set down by a law or regulation

The appendix "12. Conformity" in the ISMS certification criteria lists the following controls:

12. (1) Conformity to legal requirements To avoid violating criminal and civil laws, other laws, regulatory or contractual obligations, and security requirements.		
12. (1) [3]	Protecting records of the organization	The important records in the organization must be protected from loss, damage and tampering.

(Quoted from "12. (1) Conformity to legal requirements" in "Detailed Controls" in the ISMS certification criteria (Ver. 2.0))

5.7 Summary of Chapter 5

This chapter has described the information security management (ISMS) practices in medical organizations, mainly by explaining about the P (Plan: Establishing the ISMS) section of the PDCA cycle, using the example of a medical organization. As a good beginning makes a good ending, if the planning and preparation are done properly, it will be possible to establish a highly effective ISMS.

Once this has been established, it is also important to carry it out (Do), repeatedly review and improve it (Act) and check its effectiveness (Check). Like medical services where nursing plans are established in advance but then changed to match changes in a patient's condition with daily checks, the established ISMS must be reviewed and continuously improved based on daily changes in the state of the information process and the IT environment.

6. Responsibilities of Management

"Chapter 5. Implementing Information Security Management System (ISMS) in Medical Organization" in this guide described the important requirements for establishing, implementing, operating, maintaining and continuing to improve an information security management system (ISMS). While Chapter 5 of the ISMS certification criteria defines the roles of management in those activities in detail, this chapter will describe them from a different perspective.

The management in a medical organization such as a medical corporation is likely to include an executive managing director who is responsible for the operations in the whole organization. This role may be filled by the director of a hospital if only one hospital in the medical corporation is being considered as the applicable range of the ISMS, or the director of the surgical department or nursing service department if only a certain department is being considered.

The roles the management should play in ensuring that the different ISMS activities are carried out in each phase are very important. The applicable range of ISMS management is often limited to a certain hospital or department rather than a whole medical corporation. Even in this case, it is still important to consider the management for a whole medical organization.

The management of a typical organization has the hierarchical structure shown in Figure 6-1, where the management system at a lower level works together with the system one level above to carry out activities.

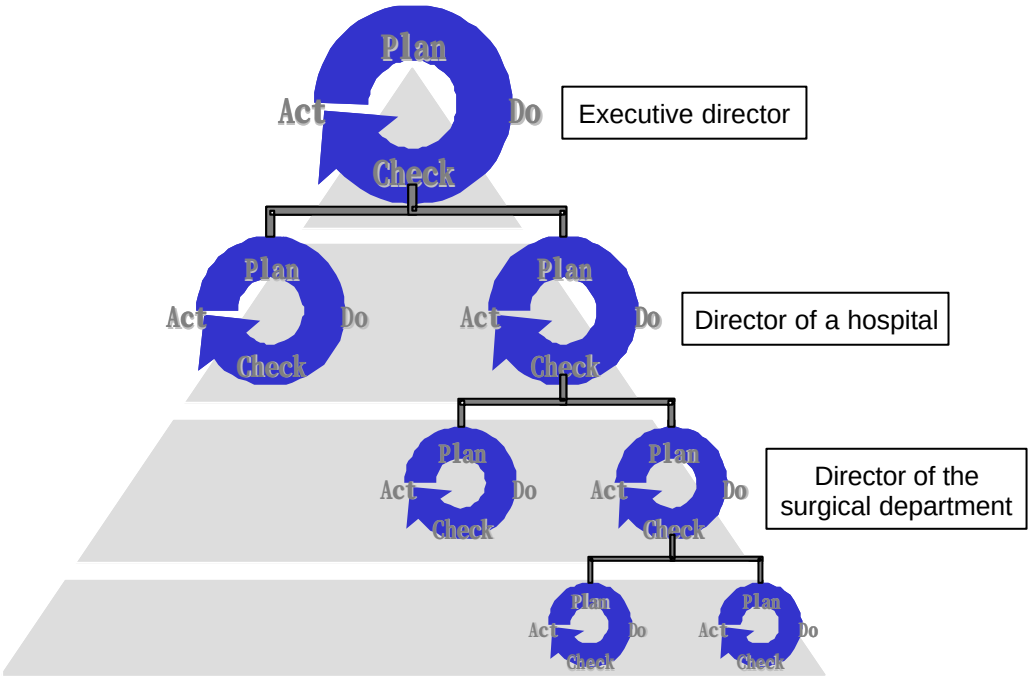


Figure 6-1 Management System for an Example of a Medical Corporation

In the initial phase, while the ISMS is being established, the applicable range is sometimes limited to, for example, a certain hospital or department, in order to concentrate on measures for areas with bigger risks. However, even in this case, the management is responsible for making the collaboration between management systems work, and leading them to the planned goal.

6.1 Management Commitments

One of the most important roles the management should play is making "commitments." This is because the "commitment" that is required in establishing, implementing, operating and maintaining the ISMS and declaring to the stakeholders as an organization who is responsible for information security can only be made by management levels with the rights to do this.
(Reference Criteria: "Clause 5-1. Management Commitments" in the ISMS certification criteria (Ver. 2.0))

The management determines the level at which risks should be accepted. This is because the management has the final responsibility for establishing, implementing, operating and maintaining the ISMS. However, even if the management is responsible for the management system in an organization, it is impossible for it to be involved in all activities.

For this reason, the management should first establish an information security policy that define the direction of the information security plan. For more information on establishing an information security policy, refer to "5.2.2 Step 2 Planning an ISMS policy."

Next, the management should set goals for information security, indicate that the plan should be carried out as a set of measures for information security in the medical organization, and take responsibilities for surely setting it up.

They must also set out the roles and responsibilities for ensuring information security in the medical organization and provide enough business resources to establish, implement, operate, and maintain the ISMS. This is described in "6.2.1 Providing Business Resources" below.

Finally, management themselves should confirm that the ISMS that has been established is functioning effectively as planned, and perform management reviews to make decisions on improving it. This is described in "7. Management Reviews."

6.2 Resource Management

6.2.1 Providing Business Resources

One of the important roles of management is to provide business resources such as "people," "things" and "money." Management must understand the needs of the ISMS and provide the necessary business resources for it. (Reference Criteria: "Clause 5-2. Resource Management" in the ISMS certification criteria (Ver. 2.0))

It will be difficult for the management to establish, implement, operate and maintain the ISMS just by calling for it to happen. The series of processes required to establish the ISMS needs to be allocated business resources.

6.2.2 Training, Awareness and Competence

Of all the business resources, "people" are especially important.

The ISMS certification criteria describe people-related training, awareness and competence in the list of the following four items:

> An organization must ensure that all personnel who are given a clearly defined responsibility are competent to perform the operations required of them in ISMS, by carrying out the following:
>
> (1) Defining the competences required of personnel involved in operations that may affect the ISMS.
> (2) Give appropriate education and training to personnel so that they can gain the necessary competence, or employ suitable personnel if necessary.
> (3) Evaluate the effectiveness of the education and training performed, and the other action that has been taken.
> (4) Maintain records on education and training, skills, experience and qualifications.
>
> (Quoted from "Clause 5 2. Resource Management" in the ISMS certification criteria (Ver. 2.0))

It should not be forgotten that it is people who will establish, implement, operate and maintain the ISMS. If individual in an organization are to carry out their responsibilities related to information security and play the roles expected of them, it is obvious that they must be competent to do this.

Management is responsible for carrying out education and training to ensure that all personnel who are allocated a clearly defined role have the competence to perform the operations required. Ideally, the content of the education and training performed should help all personnel understand the meaning and importance of the information security activities they are involved in, and how they can contribute to achieving the goals of the ISMS.

It is important that the effectiveness of the education and training that has been performed is evaluated, and that the results are used to secure personnel who are competent. The competence required will depend on the operation. Possible categories of competences required for establishing, implementing, operating and maintaining the ISMS are shown in Table 6-1.

Table 6-1 Categories of Competences

Competences associated with management	General management theory and leadership etc.
Competences associated with auditing	General audit theory and audit practices
Competences associated with security technology	The theory and practice of network security, server application security, OS security, firewalls, invasion detection systems, viruses, secure programming and encryption

It is important that these competences are appropriately defined and that whether they have been achieved is checked.

It should also be useful to use a qualification system as a reference for investigating competence. Examples of qualifications and successful applicants for each competence are shown in Table 6-2.

Table 6-2 Qualification Related To Competence

Internal audits	Certified internal auditor (CIA)[3], certified public accountant, certified system auditor [4], system audit engineer [5], certified information system auditor (CISA)[6], ISMS primary auditor, ISMS auditor
Security technology	Information security administrator, senior system administrator [7], certified information security manager (CISM)[8], certified information system security professional (CISSP), system security certified practitioner (SSCP)[9]

[3] Certified internal auditor is a qualification for internal auditors certified by The Institute of Internal Auditors, Inc. (IIA: http://www.theiia.org). The Institute of Internal Auditors was established in the U.S. in 1941 and has 85,000 auditors as members worldwide as of 2003.

[4] Certified system auditor is a qualification for system auditors that is certified by the System Auditors Association of Japan (http://www.saaj.or.jp).

[5] A national examination to certify that successful applicants have system auditing techniques, which is currently held by the Japan Information Processing Development Corporation.

[6] Certified information system auditor is a qualification for system auditors certified by the Information Systems Audit and Control Association (http://www.isaca.org). This association was established in 1967 and has approximately 29,000 members worldwide as of 2003.

[7] Information security administrator and senior system administrator are national examinations for checking that applicants have a certain level of expertise and ability in information security management and system management, and are held by the Japan Information Processing Development Corporation.

[8] Certified information security manager is a qualification that proves that successful applicants have the technical competence required of security managers, and is certified by the Information Systems Audit and Control Association (http://www.isaca.org).

[9] Certified information system security professional and System security certified practitioner are qualifications that prove that successful applicants have the professional abilities required in information security, and are certified by (ISC)[2] (the International Information Systems Security Certification Consortium http://www.isc2.org).

It is also a good idea to refer to reports on the security skill standards that are announced by the Information technology Promotion Agency (IPA) when determining the competences required for information security operations.[10]

There are also several qualifications that are useful for managing medical information. It will become more and more important to manage patients' medical information appropriately to protect the rights and benefits of patients, especially as the Personal Information Protection Law has been established.

[10] http://www.ipa.go.jp/security/fy14/reports/professional/sec-pro-outline.pdf

7. Management Reviews

7.1 General

As stated in section 6.1, it is important to carry out management reviews, which should be the responsibility of a director of a hospital, executive director, or a person who is authorized as responsible for information security management ("the management in a medical organization"). These management reviews are activities which are necessary if tasks are to be performed successfully in the future. They can be thought of as a part of the Check process in the PDCA cycle. The management in a medical organization can use these to find out if the ISMS is functioning effectively as expected and make decisions on improving it.

A management review is a series of processes in which the management in a medical organization finds out the effectiveness of the ISMS and makes decisions on improving it. An ISMS management review must be performed at specified intervals during a year.

A management review also includes the evaluation of opportunities for improving ISMS and the need for the ISMS to change, including its information security policy and goals. The results of a management review must be maintained as records.

7.2 Input to a Management Review

- The results of internal or external audits (for example, nonconformities pointed out by a certification or registration body and issues observed)
- Feedback from the stakeholders, including patients, business partners, and office staff, and from administrative agencies
- Information on new technology that has become available, new products and services announced by vendors, and the like
- The practical status and effects of the preventive and corrective action that has been taken
- Decisions on the need for review of risk assessment of vulnerabilities or threats, which has not been considered by financial, environmental or legal regulations.
- Reports on follow-ups about whether the results of management reviews in the past have been appropriately addressed.
- All changes inside and outside of an organization which may affect the ISMS, such as changes in the business environment (revisions to laws) and changes to the organization
- Cases of trouble related to information security (whether they have occurred in medical organizations inside or outside of the range of the ISMS)

In particular, many medical organizations perform field-level improvements based on trouble. Risk managers often collect and analyze trouble to provide input for reviews of the management in a medical organization, take measures to improve the system, and report their effectiveness and validity to management. It is likely that almost all cases of trouble are related to medical mistakes, but the ISMS requires that the risks related to information security are reviewed as well as these when a management review is performed.

In medical organizations that evaluate the functionalities of a hospital, information management is also included in the evaluation list (check list). If an ISMS management review is performed, it can be considered that information is being managed properly. (Reference Criteria: "Clause 6 2. Input to a Management Review" in the ISMS certification criteria (Ver. 2.0))

7.3 Output from a Management Review

The management in a medical organization must make judgments on management operations, and business decisions based on the information input. The ISMS certification criteria list the following three sample key points for decision making, that is, outputs from the management review:

> The output from the management review must include decisions and actions related to the following:
>
> (1) Improving the effectiveness of the ISMS
> (2) Correcting procedures to helps keep information secure, added as necessary to handle internal or external events that may affect the ISMS.
> (3) The business resources required.
>
> (Quoted from "Clause 6 3. Output from a Management Review" in the ISMS certification criteria (Ver. 2.0).)

In (1) above, the management in a medical organization must present measures for improvement that will make the current ISMS more effective as the output of the management review.

In (2) above, if the internal or external environment of the ISMS has changed, the procedures for the information security must be corrected to account for this environmental change. (Reference Criteria: "Clause 6 3. Output from a Management Review" in the ISMS certification criteria (Ver. 2.0))

Many medical organizations are currently working on implementing electrical care card systems. In an example like this, the risks in medical organizations will change, because the information systems and business processes will change when the new system is implemented. This, if (I) the importance of a business domain is changed or (III) any business process is changed, it must be checked that the information security measure being carried out are still appropriate.

(IV) When a new law is brought to effect, an existing law is corrected, or a new regulation is established or revised, it is important to check that current processes conform to the laws and regulations. More care is need nowadays as laws and regulations are corrected frequently, due to the newly established laws related to IT, the Personal Information Protection Law, and newly published guidelines.

Care should also be taken of (II) and (V). As the information technology is improving rapidly, new threats (such as the appearance of a new method of attach) and new vulnerabilities will be found. The vulnerabilities of existing measures may change, and cause the degree of risk to change as well. It is important to correct procedures for providing information security in response to these environmental changes. In a medical organization, in particular, the system must be protected against malicious software that causes leaks of personal information or breakdowns of the information system (such as computer viruses and worms). It is important that information about threats and vulnerabilities to the information system is collected and analyzed and that timely measures are take to deal with the new threats.

For (3) above, the management in a medical organization must guarantee that it will provide the business resources required to improve the ISMS recognized as necessary in the management review. If there is no guarantee that the business resources required for improvement will be supplied, the improvement will not be performed. Depending on the form of a medical organization, it is possible that new investment may be difficult in the middle of a fiscal year. For example, an important vulnerability may be found in the existing care card system that requires urgent measures. It is very likely that the possibility of this will increase in the future, even if it is not expected currently. Ideally, therefore, flexible use of budgets for systems such as information systems should be allowed.

7.4 Internal Audits

One of the important pieces of input to a management review is the result of an internal audit. The ISMS certification criteria define internal audits in detail.

An internal audit is carried out to evaluate whether the management goals, controls, processes and procedures of the ISMS satisfy the following criteria: (Reference Criteria: "Clause 6 4. Internal Audits" in the ISMS certification criteria (Ver. 2.0))

To obtain an ISMS certificate, the ISMS certification criteria must be complied with. In addition, laws and regulations must naturally be complied with.

Laws related to ISMS included the Personal Information Protection Law (and regional personal information protection regulations for the medical organizations of local authorities), the Building Standards Law, the Fire Defense Law, the Medical Practitioners Law and the Nursing Law.

The various regulations related to medical organizations and agreements with business partners must also be complied with.

In an internal audit, it must be checked that the ISMS is being carried out effectively, maintained and carried out as expected.

Since internal audits must be carried out as planned, auditors take the status and importance of management goals, controls, processes and procedures to be audited into account when planning an audit program, as well as the results of the audit. In carrying out an audit, the criteria, applicable range, frequency and method of the audit must be documented.

The objectivity and fairness of the audit process must be ensured when auditors are selected.

When auditors are selected, it is important that they have different competences from the security operators or managers. For example, an auditor is required to have the following competences when carrying out the series of processes in the audit:

- Planning and carrying out the audit
- Reporting the results
- Proposing corrective and preventive action, etc.

In addition, the organization is required to define the responsibilities of auditors and the series of processes for the audit in the procedure documentation.

If it is difficult to find an auditor with the required competences inside an organization, it is possible to ask an external auditor. Note that auditors cannot audit their own operations, to ensure objectivity.

A manager who is responsible for a process being audited must ensure that action is taken to remove the nonconformity found and its cause without delay. This does not mean that the nonconformity must be corrected immediately. In addition, the corrective actions performed must include a verification of the action that has been taken and a report of the results of verification.

From the viewpoint of governance, the internal audit for the ISMS can be performed effectively as a part of, or in collaboration with, the internal audit of a business audit of the whole medical organization. When performing the audit, it is a good idea to refer to "Guidelines for auditing quality and/or environmental management systems" JIS Q 19011: 2003.

The information security audit system or system audit system may also be used, to ask external specialists to perform an internal audit.

In some medical organizations, an internal audit of the whole business may not have been performed. "(Example) operation management rules for hospitals" attached to the article "Storing medical service records on electronic media" from the Ministry of Health, Labour and Welfare (the former Ministry of Health and Welfare), describes how to carry out an audit for electronic storage systems. It is possible to build and organize the organization for the internal audit starting from the audit of this area. It may be good enough to continuously improve the internal audit while the ISMS is operating, so that the internal ISMS audit can be performed as a part of the business audit of the whole medical organization.

8. Improvement

8.1 Continual Improvement

One of the advantages of establishing ISMS is that security measures can be carried out with certainty, because the director of a hospital, executive director or the person responsible for information security management ("the management in the medical organization") is responsible for continually improving of the information security. In addition to this continual improvement, it can also be expected that the ISMS level of the organization will continue to improve. This improvement is a part of the Act-Improvement process in the PDCA cycle.

It is important to continue to improve the effectiveness of the ISMS using the information security policy, information security goals, the results of audits, analysis of monitored event s, corrective and preventive action and the output from management reviews.

Types of improvement include corrective action and preventive action, which are described in the following sections.

8.1.1 Corrective Action

If nonconformities related to the way the ISMS is implemented or operated are found from the results of an audit and management review, actions must be taken to remove the causes of nonconformities and prevent them from reoccurring. This is called "corrective action."

It is necessary to document the procedures for corrective action, including the following items, which are defined in the ISMS certification criteria: (Reference Criteria: "Clause 7 2. Corrective Action" in the ISMS certification criteria (Ver. 2.0))

In medical organizations, there is the risk that any problem caused by a personal information leak or an error handling the information or information systems may become a problem for society. If an accident occurs, it is important to re-evaluate the threats to and vulnerabilities of the information system when identifying the cause of the accident to ensure that it is prevented from reoccurring.

8.1.2 Preventive Action

If a problem that might cause nonconformity in the future is found from the results of an audit or management review, actions must be taken to prevent the problem from occurring in advance. This is called "preventive action."

It is necessary to document the procedures for preventive action, including the following items, which are defined in the ISMS certification criteria: (Reference Criteria: "Clause 7 3. Preventive Action" in the ISMS certification criteria (Ver. 2.0))

Many medical organizations collect examples of tense moments or near misses in daily medical services and then analyze them, improve them, and, in particular, take preventive actions to prevent trouble. In the future, it will be vital to include trouble related to information security in these cases (of trouble) to analyze and improve them, if systems such as the electronic care card system are to be carried out and used effectively in the future. It is important that risk managers consider these factors when taking preventive action.

It is obvious that taking "preventive action" to prevent potential nonconformities in advance is preferable to taking "corrective action" to alleviate nonconformities that have already occurred. In many cases, preventive action is said to be more cost-effective than corrective action.

It is important to identify possible nonconformities and their causes earlier to take preventive action. When establishing ISMS in an organization, it is necessary to bear in mind that the management process should include a function for identifying changes to risk due to conditions and environmental changes, and a function for learning from cases of trouble, and trouble in other organizations, so that preventive action can be taken in management reviews.