TECHNICAL REPORT

ISO/TR 11633-2

First edition
2009-11-15

Health informatics — Information security management for remote maintenance of medical devices and medical information systems —

Part 2:
Implementation of an information security management system (ISMS)

Informatique de santé — Management de la sécurité de l'information pour la maintenance à distance des dispositifs médicaux et des systèmes d'information médicale —

Partie 2: Mise en oeuvre d'un système de management de la sécurité de l'information (ISMS)

Reference number
ISO/TR 11633-2:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 11633-2 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

ISO/TR 11633 consists of the following parts, under the general title *Health informatics — Information security management for remote maintenance of medical devices and medical information systems*:

— *Part 1: Requirements and risk analysis*

— *Part 2: Implementation of an information security management system (ISMS)*

Introduction

Progress and spread of technology in information and communication fields and well-arranged infrastructure based on them have brought various changes into modern society. In the healthcare field, information systems formerly closed in each healthcare facility are now connected by networks, and they are coming to the point of being able to facilitate mutual use of health information accumulated in each information system. Such information and communication networks are spreading, not only amongst healthcare facilities but also amongst healthcare facilities and vendors of medical devices or healthcare information systems. By practicing so-called “remote maintenance services” (RMS), it becomes possible to reduce down-time and lower costs.

However, such connections with external organizations have come to bring healthcare facilities and vendors not only benefits but also risks regarding confidentiality, integrity and availability of information and systems, risks which previously received scant consideration.

Based on the information offered by this part of ISO/TR 11633, healthcare facilities and RMS providers will be able to perform the following activities:

— clarify risks originating from using the RMS, where environmental conditions of the requesting vendor site (RSC) and maintenance target healthcare facility site (HCF) can be selected from the catalogue in Annex A;

— grasp the essentials of selecting and implementing both technical and non-technical “controls” to be applied in their own facility against the risks described in this part of ISO/TR 11633;

— request concrete countermeasures from business partners, as this document can identify the relevant security risks;

— clarify the boundary of responsibility between the healthcare facility owner and the RMS provider;

— plan a programme for risk retention or transfer as residual risks are clarified when selecting the appropriate “controls”.

By implementing the risk assessment and employing “controls” referencing this part of ISO/TR 11633, healthcare facilities owners and RMS providers will be able to obtain the following benefits:

— it will only be necessary to do the risk assessment for those organizational areas where this part of ISO/TR 11633 is not applicable, therefore, the risk assessment effort can be significantly reduced;

— it will be easy to show the validity of the RMS security countermeasures to a third party;

— if providing RMS to two or more sites, the provider can apply countermeasures consistently and efficiently.

Health informatics — Information security management for remote maintenance of medical devices and medical information systems —

Part 2: Implementation of an information security management system (ISMS)

1 Scope

This part of ISO/TR 11633 provides an example of selected and applied “controls” for RMS security based on the definition in the ISMS, on the basis of the risk analysis result mentioned in ISO/TR 11633-1. This part of ISO/TR 11633 excludes the handling of the communication problems and the use of encryption method.

This part of ISO/TR 11633 consists of:

— a catalogue of types of security environment in healthcare facilities and RMS providers;

— an example of combinations of threats and vulnerabilities identified under the environment in the “use cases”;

— an example of the evaluation and effectiveness based on the “controls” defined in the ISMS.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO/IEC 13335-1:2004, definition 2.1]

2.2
asset
anything that is of value to the organization

NOTE 1 Adapted from ISO/IEC 13335-1.

NOTE 2 In the context of health information security, information assets include:

a) health information;

b) IT services;

c) hardware;

d) software;

e) communication facilities;

f) media;

g) IT facilities;

h) medical devices that record or report data.

2.3
assurance
result of a set of compliance processes through which an organization achieves confidence in the status of its information security management

2.4
availability
property of being accessible and usable upon demand by an authorized entity

[ISO 13335-1:2004, definition 2.4]

2.5
compliance assessment
processes by which an organization confirms that the information security controls put in place remain both operational and effective

NOTE Legal compliance relates specifically to the security controls put in place to deliver the requirements of relevant legislation such as the European Union Directive on the protection of personal data.

2.6
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[ISO 13335-1:2004, definition 2.6]

2.7
data integrity
property that data have not been altered or destroyed in an unauthorized manner

[ISO/IEC 9797-1:1999, definition 3.1.1]

2.8
information governance
processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed

2.9
information security
preservation of confidentiality, integrity and availability of information

NOTE Other properties, particularly accountability of users, but also authenticity, non-repudiation, and reliability, are often mentioned as aspects of information security, but could be considered as derived from the three core properties in the definition.

2.10
risk
combination of the probability of an event and its consequence

[ISO/IEC Guide 73:2002, definition 3.1.1]

2.11
risk assessment
overall process of risk analysis and risk evaluation

[ISO/IEC Guide 73:2002, definition 3.3.1]

2.12
risk management
coordinated activities to direct and control an organization with regard to **risk**

NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

[ISO/IEC Guide 73:2002, definition 3.1.7]

2.13
risk treatment
process of selection and implementation of measures to modify (typically reduce) **risk**

NOTE Adapted from ISO/IEC Guide 73:2002.

2.14
system integrity
property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system

2.15
threat
potential cause of an unwanted incident, which may result in harm to a system or organization

NOTE Adapted from ISO/IEC 13335-1.

2.16
vulnerability
weakness of an asset or group of assets that can be exploited by a threat

NOTE Adapted from ISO/IEC 13335-1.

3 Abbreviated terms

— HCF Healthcare facility

— ISP Information-stealing programme

— ISMS Information security management system

— PHI Personal health information

— RMS Remote maintenance services

— RSC Remote maintenance service centre

— RSS Remote maintenance service security

— VPN Virtual private network

4 Application of ISMS to remote maintenance services

4.1 Overview

The information security management system (ISMS) is a mechanism that operates as a series of plan/do/check/act processes under the security policy. This series of processes means that the organization plans out proper security measures (plan), puts those security measures into practice (do), reviews those

security measures (check), and reconsiders them if necessary (act). The ISMS is already standardized internationally as ISO/IEC 27001, therefore, it is convenient to construct and operate an ISMS referring to ISO/IEC 27001. This also helps to persuade patients, medical treatment evaluation organizations, and others of the efficacy of the security measures.

General steps of ISMS construction are shown in Figure 1.

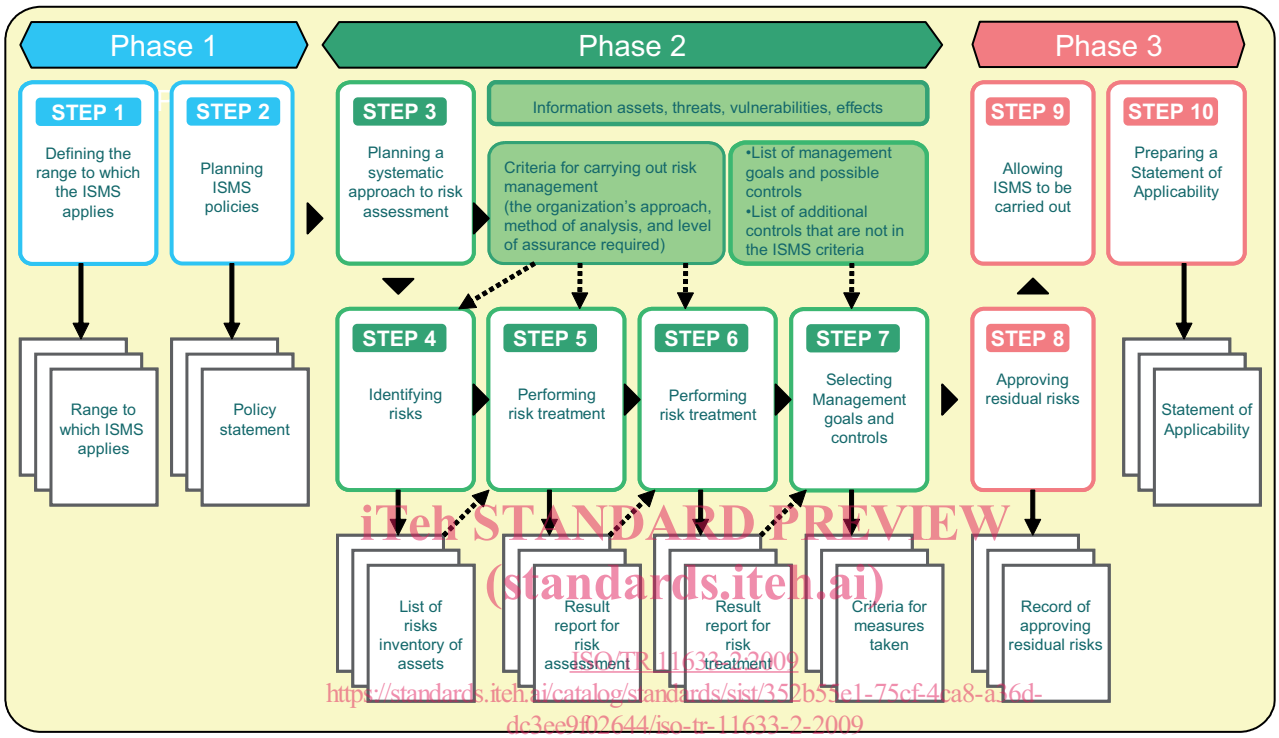

Figure 1 — ISMS steps

Security measures for protecting personal information in the remote maintenance services (RMS) are described below in accordance with the concepts of ISMS.

Both the healthcare organization and the RMS provider should construct the appropriate ISMS. Additionally, the healthcare organization should ideally do the work to adjust the information security management among all RMS providers to protect personal information. The RMS connects the network of the RMS provider and the network of the healthcare organization. After connecting these networks, there are risks of new security holes being created. In the RMS, a different problem may occur in system construction in a single organization, because the RMS acts between the healthcare organization and the remote maintenance service centre (RSC), two organizations that are independent of each other. It will therefore be a burden on both the healthcare organization and RSC, if security measures are not considered an integral part of the RMS from the outset. In this regard, using ISMS (a well-evaluated technique) can be considered as a better way to implement RMS security efficiently.

Under many jurisdictional laws for personal information protection, the healthcare organization will assume the obligations and responsibilities of being custodian of the personal information. In the RMS, the healthcare organization should request, from the RMS provider, appropriate measures for protecting personal information because the provider will access the target device set up in a healthcare facility from the RSC through the network. The healthcare organization must independently adjust all RMS providers' information security management systems that provide the RMS, and confirm that security holes have not been created. Additionally, the healthcare organization should confirm each RMS provider's security level is kept appropriate.

It is necessary to document and comply with the following items to adjust the ISMS:

— security policy;

— security measures standard;

— mapping of security policy;

— selection of solutions;

— operation execution rule;

— security auditing standards;

— security audit and audit trail.

A healthcare organization should write items into the maintenance contract or agreement between the healthcare organization and RMS provider that the RSC implements to ensure appropriate measures in the RSC. As a result, the healthcare organization will distribute the obligation and the responsibility concerning the protection of personal information during maintenance work to the RMS provider through the contract and agreement. The healthcare organization shall construct the appropriate ISMS and, at the same time, shall put into writing in the maintenance contract or the business consignment contract the obligation on the part of the RMS provider of providing supervision as the final authority in charge of personal information management.

The risk analysis and measures are illustrated in this part of ISO/TR 11633 by the ISMS method. Therefore, it is thought that constructing the remote maintenance service security (RSS) with this content will bring advantages to both the healthcare organization and the RSC. When the content of this risk assessment is not complete, additional risk assessment need only be done on parts that are missing.

4.2 Compliance scope

The coverage of the ISMS in the operational model described in Clause 6 of ISO/TR 11633-1 is as follows:

— target device for maintenance in healthcare facility (HCF);

— internal network of healthcare organization;

— route from an rms access point in healthcare organization to the RSC;

— internal network of the RSC;

— equipment management in the RSC.

Because the following risks exist independent of the presence of the RMS, they are excluded from the coverage of the ISMS of this clause:

— threats related to availability of equipment and software that treats protected health information(PHI);

— threats related to computer virus;

— threats related to staff which pertain to adoption, education and training.

4.3 Security policy

In 5.1.1 of ISO/IEC 27002:2005, the desired content to be included in a basic policy is prescribed, as follows:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, including:

   — compliance with legislative, regulatory, and contractual requirements,

   — security education, training, and awareness requirements,

   — business continuity management,

   — consequences of information security policy violations;

e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

When these considerations are applied to RSS, it is necessary to secure the availability of the system, and to secure the integrity, readability, and preservation of patient personal information.

It is necessary for the technical, systematic, human resources and physical safety measures of the RSS to be specified in a basic security policy of the RSS.

The following explanations assume large-scale integrated HCF. Since it is possible that the RSC which receives RMS exists in two or more sections of a large-scale HCF, a united management policy is needed. When the HCF scale and the operation form are different from large-scale integrated HCF, it is important to implement in conformity with the actual situation.

4.4 Assessing risks

In risk assessment, analysis of information assets is performed with regard to the following.

— What threats exists?

— To what extent is each threat possible and what is its frequency of occurrence?

— When the threat is actualized, how much influence does it exert?

The technique of the analysis is broadly classified into the following four approaches.

a) Baseline approach

This is a technique for analysing risk based on the standards and guidelines that are required in the target field. This approach measures security based on standard risk assessment done beforehand in industry.

Though it is advantageous from the perspective of time and cost because the risk need not be evaluated by oneself, the adaptability of the standardized risks to the risks of a specific organization can be problematic.

b) Detailed risk analysis

Carrying out a detailed risk assessment includes risk analysis of details, and an appropriate management plan for management to select. A sizable budget for cost and time are needed for the risk assessment, including securing necessary human resources.

c) Combined approach

This approach combines the baseline approach with the detailed risk analysis and it has the advantages of each.

d) Informal approach

This approach implements risk analysis by exploiting the knowledge and the experience of the staff of the organization. It is difficult for a third party to evaluate the resulting risk analysis because the method is not structured.

The RMS is related to the healthcare organization and the RSC, so the risk analysis should be what both can agree upon. In this part of ISO/TR 11633, the typical use case is modelled, and the risk assessment concerning this model is carried out. Risk analysis by baseline approach a) and the combined approach of c) is enabled by using this risk assessment result. See Table A.1 for the result of the risk assessment. Table A.1 contains the selection of appropriate control purpose and management plan in ISO/IEC 27001 from the result of risk analysis in ISO/TR 11633-1. Table A.1 conforms to ISO/IEC 27001, and is composed of 11 management fields and 133 management plans.

The measures prescribed here specify the procedures which should be observed, at least in performing RMS. The healthcare organization, which is also the administrator of personal information, should evaluate whether the RSC conforms to this part of ISO/TR 11633, and should request that appropriate measures be taken if it does not. Moreover, if the healthcare organization's security level is below the level specified in this part of ISO/TR 11633, necessary measures will have to be put in place. Each RMS provider is expected to implement necessary measures in order to achieve the requirements described in this part of ISO/TR 11633.

4.5 Risks to be managed

This subclause explains some examples from the viewpoint of personal information protection to avoid risks, which should be especially noted in an RMS. It is important to implement sufficient measures against these risks. The risk discussed here is a mere example; the management of other risks is also important.

a) When the RSC handling personal information is managed by the healthcare organization.

In this case, the point that needs particular attention is a leak of information by the third party. Consideration needs to be given to information displayed on computer screens in the work environment and information printed out on paper, as well as to the threat of hacking into the system. The main risks are as follows:

— viewing of screens by persons other than persons concerned in RSC;

— leakage in third party trust;

— leakage from logs generated when data is analysed, from printed paper or cache memory, etc.;

— leakage in the network.

b) When the RSC accesses equipment of the healthcare organization for maintenance by the administrative authority.

In this case, the points that need particular attention are operator error and inappropriate access to the computer (submit operations that are permitted). The main risks are as follows:

— destruction of data in target device due to an operator mistake;

— destruction of data in target device due to malicious or subversive activities;

— leakage and destruction of more important information due to inside intrusion via the maintenance device.

c) When the RSC updates the software.

In this case, care is required not to install malicious software and computer viruses, etc., into the target devices. The main risks are as follows:

— leakage and destruction of data in target device due to malicious software;

— leakage and destruction of important information via internal intrusion due to a computer virus.

4.6 Identification of risks that are not described in this part of ISO/TR 11633

In this part of ISO/TR 11633, risk assessment is performed in accordance with the typical model, so the other use cases are outside its scope. If a business model is different from the model that this part of ISO/TR 11633 assumes, the risk assessment results of this part of ISO/TR 11633 can be misappropriated. There is also a possibility that not all cases can be covered. When coverage of all cases is not possible, it is necessary to conduct a detailed risk analysis using the combined risk assessment approach, not described by this part of ISO/TR 11633.

The risk assessment method in the detailed risk analysis is explained in ISO/TR 11633-1. By adopting the methods of ISO/TR 11633-1, the results of a risk assessment guided by a different business model can be easily integrated with the results of a risk assessment guided by this part of ISO/TR 11633.

4.7 Treating risks

Risk treatment is defined as treatment of the assumed risk in accordance with the results of risk assessment. Risk treatment choices are shown in Table 1. These choices are combined and implemented where necessary.

In the usual risk management process, a combination of these measures is selected by making an overall judgment of the severity of the risk or the ease of implementing the measures. It is especially important to adopt the risk control(s) specified by information privacy protection law and regulations. In this case, it is necessary to control the risk positively, because measures such as risk retention or transfer are not adequate, or to adopt risk avoidance and not treat the personal information object, in law, in the RMS at all.

In this part of ISO/TR 11633, it is recommended that risk control be performed positively based on the ISMS. Concrete measures are explained in detail in Annex A.

Table 1 — Risk treatment

Risk control: Measures are adopted (management plan) to positively reduce damage. • **Risk prevention** — measures to reduce threats and vulnerabilities are implemented. • **Minimization of damage** — measures to reduce the damage when the risk is generated are implemented.	**Risk transfer:** Measures to transfer to third parties by contract, etc. • **Insurance** — utilizes damage insurance and other types of insurance so that the risk is transferred. • **Outsourcing** — information assets and information security measures are entrusted to an outside party.
Risk retention: Approach that accepts risk as belonging to the organization. • **Financing** — this corresponds to accumulating a reserve, etc. • **Nothing is done.**	**Risk avoidance:** Approach when appropriate measures cannot be found. • **Abolition of business** — the business is stopped. • **Destruction of information assets** — the management object is lost.

5 Security management measures for remote maintenance services

The possibility of leakage of personal information such as patient information from the RMS requires the healthcare organization to obtain the help of the RSC to achieve RMS security.

In order to take appropriate security measures for the actualization of the safety of the RMS, the healthcare organization and the RSC should select controls based upon the result of the risk assessment. Regardless of whether or not the RSC is supervised by the healthcare organization, the RSC should ensure the RMS meets security requirements.

Annex A illustrates concretely how to proceed with the safety management measures during RMS for the healthcare organization and the RSC. It is expected that referring to Table 1 will reduce risk assessment time when preparing the RMS.

Even if the RMS is already operational, auditing using Table 1 is recommended to make sure that the risk assessment is adequate.

6 Approving residual risks

Residual risks are those risks where the HCF does not intentionally take sufficient countermeasures or where the HCF is having difficulty with the identification of these risks, or risks that will incur large costs if the HCF wishes to implement full countermeasures as derived by the risk evaluation. When risks remain, even if the HCF performs risk control, risk retention or risk transfer, it is necessary for management to judge whether or not these residual risks are to be approved from a management point of view. When the HCF management approves these residual risks, it means that the HCF accepts the RMS as constituted by risk assessment based on the ISMS.

The HCF approves the residual risks in the whole contract of the RMS, and the RSC operates the RMS while paying attention to residual risks. According to the result of the risk analysis in the RMS illustrated in Annex A, particularly in the RSC, there still is the possibility of leakage of personal information such as PHI. The HCF shall recognize these dangers, take into account guidelines issued by government, and audit appropriate security measures that are taken in the actual RMS.