TECHNICAL REPORT

ISO/TR 11633-2

Second edition

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)

PROOF/ÉPREUVE

Reference number
ISO/TR 11633-2:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Application of ISMS to remote maintenance services **1**
4.1 Overview 1
4.2 Compliance scope 3
4.3 Security policy 3
4.4 Assessing risks 4
4.5 Risks to be managed 4
4.6 Identification of risks that are not described in this document 5
4.7 Treating risks 5
5 Security management measures for remote maintenance services **6**
6 Approving residual risks **6**
7 Security audit **7**
7.1 Security audit of remote maintenance services 7
7.2 Recommendation of security audit by third parties 7
Annex A (informative) **Example of risk assessment in remote maintenance services** **8**
Bibliography **68**

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO/TR 11633-2:2009), which has been technically revised.

The main changes compared to the previous edition are as follows:

— complete revision of the bibliography;

— update of Figure 1;

— update of Annex A.

A list of all parts in the ISO 11633 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The advancement and spread of technology in the information and communication technology field, and the infrastructure based on them, have brought many changes in how technology and networks are used in modern society. Similarly, in healthcare, information systems once closed systems in each healthcare facility (HCF) are now connected by networks, and are progressing to the point of being able to facilitate mutual use of health information accumulated in these information systems. Such information and communication networks are spreading not only in between HCFs but also between HCFs and vendors of medical devices and healthcare information systems. Maintenance of such systems is paramount to keeping them up-to-date. By practicing so-called 'remote maintenance services' (RMS), it becomes possible to reduce down-time and lower costs for this maintenance activity.

Whilst there are benefits to remote maintenance, such remote connections with external organizations also expose HCFs and vendors to risks regarding confidentiality, integrity and availability of information and systems; risks which previously received scant consideration.

This document stipulates the risk assessment to protect remote maintenance activities, taking into consideration the special characteristics of the healthcare field such as patient safety, and applicable requirements and privacy protections. Although normal remote maintenance is generally done on a contract basis, in the case of medical devices, risk assessment is commonly a legal prerequisite. Therefore, appropriate risk assessment where remote maintenance is provided in any healthcare context should be implemented. The risk assessment examples provided in this document support for HCFs and RMS providers to implement risk assessment effectively.

By implementing the risk assessment process and employing controls referenced in this document, HCFs owners and RMS providers will be able to obtain the following benefits:

— Risk assessment can result in improved efficiency. If the risk assessment document, created through the use of this document, does not fully conform, it may be used in part in a risk assessment of an incompatible area, thus reducing the risk assessment effort required.

— Documented validity of the RMS security countermeasures in place will be available to third parties.

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

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 document gives a guideline for implementation of an ISMS by showing practical examples of risk analysis on remote maintenance services (RMS) for information systems in healthcare facilities (HCFs) as provided by vendors of medical devices or health information systems in order to protect both sides' information assets (primarily the information system itself and personal health data) in a safe and efficient (i.e. economical) manner.

This document consists of:

— application of ISMS to RMS;

— security management measures for RMS;

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TS 11633-1, *Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 1: Requirements and risk analysis*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/TS 11633-1 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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 efficacity of the security measures.

General steps of ISMS construction are shown in Figure 1.

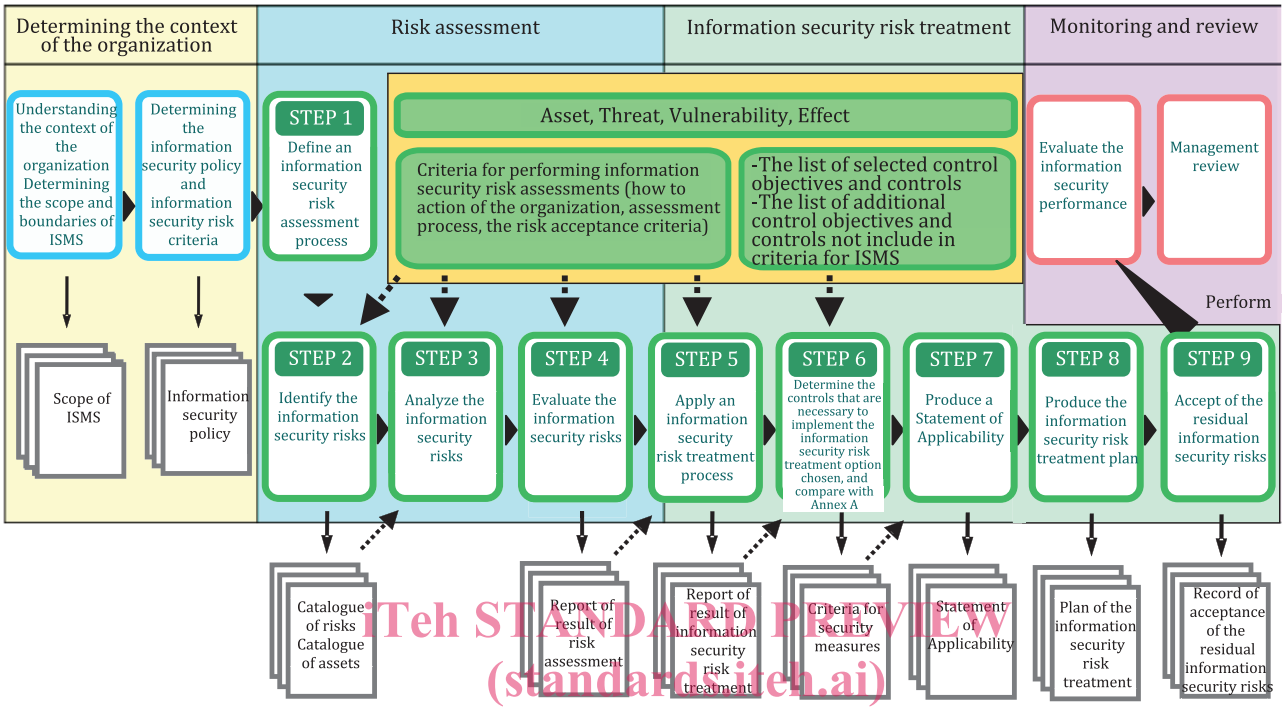

Figure 1 — ISMS steps

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.

The following items should be documented and established in 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 should construct the appropriate ISMS and, at the same time, should 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 document 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 ISO/TS 11633-1:2019, Annex A 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

The desired content included in a basic policy is referred to in ISO/IEC 27002:2013, Clause 5.1.1.

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

The technical, systematic, human resources and physical safety measures of the RSS should 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 document, 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/TS 11633-1. Table A.1 conforms to ISO/IEC 27001, and is composed of 14 management fields and 114 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 document, 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 document, appropriate measures should be put in place. Each RMS provider is expected to implement appropriate measures in order to achieve the requirements described in ISO/TS 11633-1.

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 document

In this document, 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 document assumes, the risk assessment results of this document can be misappropriated. There is also a possibility that not all cases can be covered. When coverage of all cases is not possible, a detailed risk analysis should be conducted using the combined risk assessment approach, not described by this document.

The risk assessment method in the detailed risk analysis is explained in ISO/TS 11633-1. By adopting the methods of ISO/TS 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 document.

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, the risk should be controlled because risk retention or transfer are not typically adequate to meet

these privacy protection laws, otherwise it would be to adopt risk avoidance, which prevent any data that falls in scope of privacy protection law and regulations.

In this document, 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 risk means the following among the risks identified by risk assessment.

— Risk that intentionally does not take sufficient measures

— Risks that are difficult to identify

— Risk that cost is too expensive for complete measures

When risks remain, even if the HCF performs risk control, risk retention or risk transfer, management should judge whether or not these residual risks are 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 should recognize these dangers, take into account guidelines issued by government, and audit appropriate security measures that are taken in the actual RMS.

7 Security audit

7.1 Security audit of remote maintenance services

The purpose of the security audit is to confirm whether the risk management related to security is effectively implemented and to confirm whether an appropriate control based on the risk assessment is done. The security audit comprehensively assesses the conformity of the information security management standard, but it is also possible to focus on auditing the RMS itself. In the security audit of the RMS, the auditor verifies and evaluates, if appropriate, whether controls based on the risk assessment are maintained and operated.

Moreover, it is an effective measure for both the HCF and RSC to evaluate the safety standards of the security by means of the security audit because the result of such audits become an effective evaluative material to improve the solidity of the RMS.

7.2 Recommendation of security audit by third parties

There are the following problems to conduct information security audits as internal audits:

— it is hard to notice that the risks to be assessed are missing;

— objectivity and independence will not be satisfied;

— It takes time to train auditors because specialized knowledge is required;

— it is difficult to make an audit report for the purpose of disclosure.

As mentioned above, the HCF should be audited by an external organization and by an auditor with a high degree of technical knowledge, in order to objectively evaluate the RMS. Performing an external audit based on an appropriate audit procedure facilitates information security certification such as the ISMS. Finally, the HCF can enhance its societal reputation. It is also recommended to adopt external audit to reduce any gap in reliability of the security audit reports of the HCF and RSC.

Annex A
(informative)

Example of risk assessment in remote maintenance services

This annex provides an example of risk assessment of remote maintenance services. The example is shown in Table A.1. The order of the rows in Table A.1 is the same as the relevant clause of ISO/IEC 27001.

Notes for the interpretation of Table A.1 are found on Table A.2 to A.7.

Table A.1 — Example of risk assessment of remote maintenance services

Clause	Subclause	Control objectives	Controls	No	Site	Asset	Example of Threat (C: Confidentiality, I: Integrity, A: Availability)	Example of Control Measures	V	I	L	E
A.5 Information security policies	A.5.1 Management direction for information security	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.	-	-	-	-		-	-	-	-
			The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	-	-	-	-		-	-	-	-
A.6 Organization of information security	A.6.1 Internal organization	To establish a management framework to initiate and control the implementation and operation of information security within the organization.	All information security responsibilities should be defined and allocated.	-	-	-	-		-	-	-	-
			Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.									
			Appropriate contacts with relevant authorities should be maintained.	-	-	-	-		-	-	-	-
			Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.	-	-	-	-		-	-	-	-
			Information security should be addressed in project management, regardless of the type of the project.	-	-	-	-		-	-	-	-
	A.6.2 Mobile devices and teleworking	To ensure the security of teleworking and use of mobile devices.	A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.	-	-	-	-		-	-	-	-