Information Security Management Systems

Information Security Management Systems

Conformity Assessment Scheme

ISO/IEC 27001:2013 (JIS Q 27001:2014)

ISMS

IMS Promotion Center

JIPDEC

1 Purpose of the ISMS Conformity Assessment Scheme

The Conformity Assessment Scheme for Information Security Management Systems (ISMS) is an internationally consistent third party certification scheme for information security management systems (ISMS).

The purpose of this scheme is to contribute to enhancing overall information security in Japan, as well as to achieve and maintain confidence in the information security across the world.

2 ISMS Overview

Key concept of an ISMS

An ISMS enables an organization to systematically operate its management system for information security. By establishing the ISMS, an organization can determine the necessary security level, create plans, distribute its assets, and operate systems based on its own risk assessment, along with individual technical countermeasures against each issue.

The key concept of the ISMS is to "preserve the confidentiality, integrity and availability of information by applying a risk management process and to give confidence to interested parties that risks are adequately managed". To do this, it is important that the ISMS is to be a part of, and integrated with, the organization's processes and overall management structure.

Three Elements of Information Security（Confidentiality, Integrity and Availability)

In ISMS, the three major elements of information security are defined as the following:

Information security	
Preservation of confidentiality, integrity and availability	
Confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity	property of accuracy and completeness
Availability	property of being accessible and usable upon demand by an authorized entity

NOTE: Other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

(ISO/IEC 27000:2014)

What is ISO/IEC 27001:2013?

ISO/IEC 27001 is an international standard which specifies requirements for establishing, implementing, maintaining and continually improving an organization's ISMS. It describes mainly what an organization should do for the establishment and implementation of an ISMS, rather than how to do it.

- **ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements)**

This standard can be used:

- for managing changes in risks surrounding the organizational management and business processes;

In ISO/IEC 27001, it is specified that an organization shall establish and implement its ISMS, taking into consideration the organization's needs and objectives, information security requirements, processes used, as well as the size and structure of the organization. This is helpful for an organization to reorganize its fundamental businesses to better manage changes in risks surrounding today's organizational management and business processes.

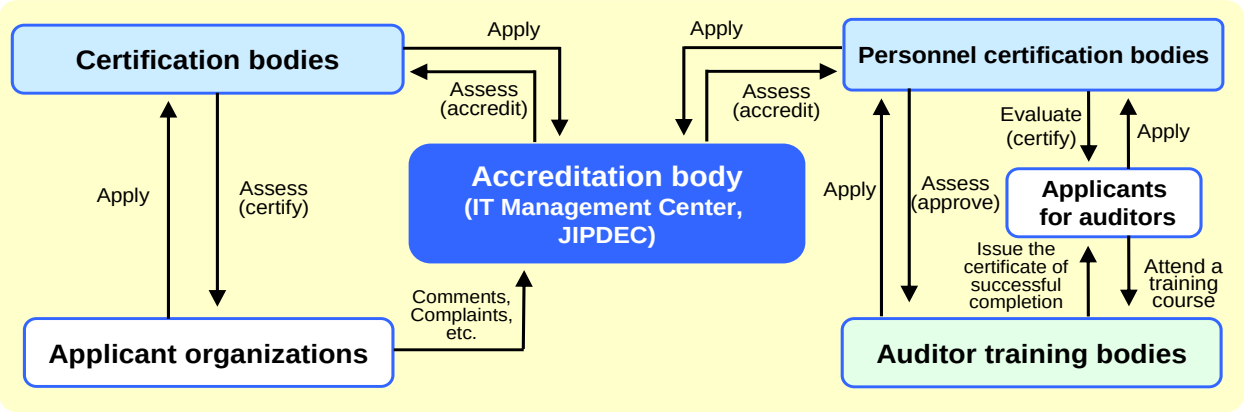
- as criteria to assess the organization's ability to meet its own information security requirements.

ISO/IEC 27001 can be used by internal parties as criteria to assess the organization's ability to meet its own information security requirements through performance evaluation and internal audits. It can also be used by external parties as criteria to assess the ability, which are called as second party audits or third party audits.

3 Operation of the ISMS Conformity Assessment Scheme

The ISMS conformity assessment scheme has a comprehensive structure, composed of "certification bodies" that assess and certify an applicant organization's ISMS based on ISO/IEC 27001; "personnel certification bodies" that certify and register ISMS auditors, and the "accreditation body" that assesses the competence of those bodies in implementing such tasks. Regarding "personnel training bodies", the personnel certification bodies carry out the assessment of those bodies and approve them based on the results.

Structure of the ISMS Scheme



Impartiality, Transparency and Objectivity of the ISMS Scheme Operation

To ensure impartiality, transparency and objectivity of the ISMS scheme, some committees have been set up in JIPDEC: one of them is the Steering Committee comprised of academic and relevant industry experts, and another one is its sub-committee, the Technical Committee. The accreditation review board, which is comprised of experts, has also been set up to consider and decide accreditation of certification bodies and personnel certification bodies.

For further information on the activities on these committees, please visit our website http://www.isms.jipdec.jp/en/index.html

4 Need for Achieving ISMS Certification

Achieving ISMS certification leads an organization to develop comprehensive and efficient information security measures and also to enhance its information security structure. In addition, by obtaining certification, the organization can have greater confidence in its information security to demonstrate its commitment to security to external and international partners. Furthermore, by maintaining risk management and implementing the proper controls, the organization can reduce the likelihood of information security incidents and the damage when such incidents occur. Accordingly, an organization with ISMS certification can increase its corporate value.

Benefits of developing and managing ISMS

Establishing and managing ISMS enables organizations to:

- **develop comprehensive security measures from both technical and personnel management aspects;**
  - enhance staff skills, clarify responsibilities, improve the capability to deal with emergency situations, etc.
- **carry out efficient security measures from a comprehensive management viewpoint;**
  - manage assets in consideration of cost-effectiveness, firmly establish risk management, etc.

□The continual implementation of these activities can be expected to bring further benefits such as raising security awareness to organizations.

Benefits of achieving ISMS certification

Achieving ISMS certification enables organizations to:

- **externally, secure confidence in information security;**
  - fulfill security requirements of customers and trade partners, etc.
- **internally, enhance their competitive edge;**
  - satisfy terms and conditions of bids and e-commerce.

□ISMS certification is one of the requirements to apply for the recognition of specific system operation companies.

5 ISMS Certification Criteria

Certification criteria in the ISMS scheme (ISO/IEC 27001 [JIS Q 27001])

Certification criteria in the ISMS conformity scheme are ISO/IEC 27001:2013 (JIS Q 27001:2014).
ISO/IEC 27001 was translated into Japanese and published as a Japanese national standard, JIS Q 27001.

JIS Q 27001:2006 was issued in March 2006 in line with the publication of ISO/IEC 27001:2005, and then revised and issued in March 2014 as JIS Q 27001:2014 according to the revision of ISO/IEC 27001.

Structure of ISO/IEC 27001

Clause	Overview
4 Context of the organization	*the blue-colored sections are ISMS-specific ones, which are not stated in the ISO MSS common elements.
4.1 Understanding the organization and its context **4.2 Understanding the needs and expectations of interested parties** **4.3 Determining the scope of the information security management system** **4.4 Information security management system**	In this clause, it is specified that an organization shall understand and decide its external and internal issues, the needs and expectations of interested parties, and then determine its ISMS scope taking these items into account.
5 Leadership	
5.1 Leadership and commitment **5.2 Policy** **5.3 Organizational roles, responsibilities and authorities**	Top management's strong leadership is critical to promote the organization's ISMS and enhance awareness of relevant people. This clause describes requirements for top management's roles in the ISMS.
6 Planning	
6.1 Actions to address risks and opportunities **6.1.1 General** **6.1.2 Information security risk assessment** **6.1.3 Information security risk treatment** **6.2 Information security objectives and planning to achieve them.**	It is specified that the organization shall determine risks and opportunities on the ISMS, and define and apply an information security risk assessment and an information security risk treatment. In 6.1.3, the normative annex A "control objectives and controls" is mentioned as part of the requirements that the organization shall compare the controls determined by the organization with those in Annex A, and if any controls in Annex A are excluded, include the justifications for the exclusions into a Statement of Applicability.
7 Support	
7.1 Resources **7.2 Competence** **7.3 Awareness** **7.4 Communication** **7.5 Documented information**	In this clause, the support for the operation of the ISMS is specified in terms of competence and awareness of personnel, communications with interested parties, and documented information required in respective clauses to be controlled and retained.
8 Operation	
8.1 Operational planning and control **8.2 Information security risk assessment.** **8.3 Information security risk treatment**	It is specified that the organization shall plan, implement and control necessary processes to meet information security requirements. It is also specified that the organization shall implement the information security risk assessment and the information security risk treatment plan.
9 Performance evaluation	
9.1 Monitoring, measurement, analysis and evaluation **9.2 Internal audit** **9.3 Management review**	Requirements in this clause specify the evaluation (monitoring, measurement, analysis and evaluation) of information security performance and ISMS effectiveness, internal audits, and management review, are specified.
10 Improvement	
10.1 Nonconformity and corrective action **10.2 Continual improvement**	Requirements in this clause specify the actions taken when nonconformity occurs and on the documentation of such actions. It also specifies on the suitability, adequacy and effectiveness of the ISMS.

- ISO/IEC 27000:2014 (Information technology - Security techniques - Information security management systems – Overview and vocabulary)
  - an international standard that specifies terms and definitions for ISMS. It contains the overview of the ISMS, 27000 family of standards, and terms and definitions used in the 27000 family of standards.
- ISO/IEC 27002:2013 (Information technology – Information technology - Security techniques - Code of practice for information security controls)
  - an International Standard that provides the Code (best practice) for implementing organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

6 Criteria, Procedures, Guides, etc. for the ISMS Scheme

ISO/IEC 27001 (JIS Q 27001) (ISMS certification criteria)	This document is for use by third party certification bodies which assess the conformity of applicant organizations for ISMS certification under this scheme.
ISMS User's Guide	This document provides certain explanations about requirements of the ISMS certification criteria (ISO/IEC 27001 [JIS Q 27001]),
ISMS User's Guide –Risk Management—	This guide supplements the "ISMS User's Guide" and provides explanations with some examples, for better understanding on risk management, particularly risk assessment and risk treatment based on the result of the assessment.
ISMS User's Guide for Medical Organizations	This User's Guide aims to enhance understanding of ISMS among medical organizations.
ISMS User's Guide on Legal Compliance	This document provides guidance for enhanced understanding of the way a suitably designed ISMS enables an organization to comply with legal and regulatory requirements. It is critical for an organization to take into account its legal risks, and an ISMS framework is significantly effective as a means to comply with laws for the protection of personal information.
ISMS User's Guide for Payment Card Industry	This User's Guide aims to support the development of ISMS in the payment card industry. This guide provides a correspondence between ISMS certification criteria and related standards and demonstrates that developing the ISMS is quite effective in complying with these standards.
Local public organizations and information security - the first step forward to ISMS -	This handbook gives guidance to local public organizations on how to identify and deal with specific issues which they might to face in establishing their ISMS.
Guide to Apply ISMS Certification to the Outsourcing of Information Processing	This guide provides organization's staff responsible for and in charge of information security with the way to apply the ISMS conformity assessment scheme when they select third parties to outsource all or part of its information processing operations.
Accreditation Criteria and Guidelines for ISMS Certification Bodies	This document provides requirements for assessment and accreditation of ISMS certification bodies with guidance for the application of the requirements.
Procedures for Accreditation of IMS Certification Bodies	This document provides procedures for assessing and accrediting certification bodies, and the rights and duties of both applicant and accredited bodies.
Guide for Accreditation of IMS Certification Bodies	This document describes general accreditation processes from application to registration, processes for maintaining accreditation, and the conditions required in each process.
Conditions for the Use of the IMS Accreditation Symbol	This document specifies conditions for the use of IMS accreditation symbols.

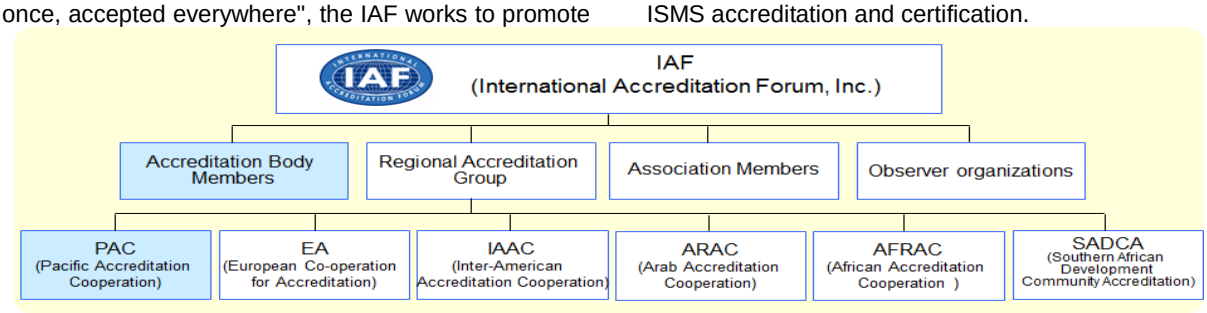
NOTE: In addition, there are some documents (e.g. practical experiences of certified organizations) which support the promotion of the ISMS Conformity Assessment Scheme.

7 IAF Membership

The IAF (International Accreditation Forum, Inc.) is an international association which mainly consists of about 60 Accreditation Body Members involved in conformity assessment programs for such as management systems, products and personnel. In total, more than 90 bodies join in the IAF, including Regional Accreditation Groups (PAC, EA, IAAC, ARAC, AFRAC and SADCA), Association Members (regional/international industrial associations such as those of certification bodies), and Observer organizations.

One of the IAF's objectives is to reduce both organizational and end user risks by developing an internationally consistent system for conformity assessment, to ensure the competence of accreditation bodies in accordance with international standards and increase reliability and effectiveness of accredited certification. To achieve the goal "certified once, accepted everywhere", the IAF works to promote international acceptance of multilateral agreements and facilitate global trade by eliminating technical trade barriers among economies. Certificates issued by certification bodies which are accredited by IAF MLA (multilateral arrangement) member accreditation bodies are internationally reliable due to the equivalence of their accreditation programs, and therefore earn the trust of customers around the world. The JIPDEC Information Management Systems (IMS) Promotion Center has joined in Pacific Accreditation Cooperation (PAC) which is an IAF special recognition regional Group since 2006, and also in the IAF since 2007.

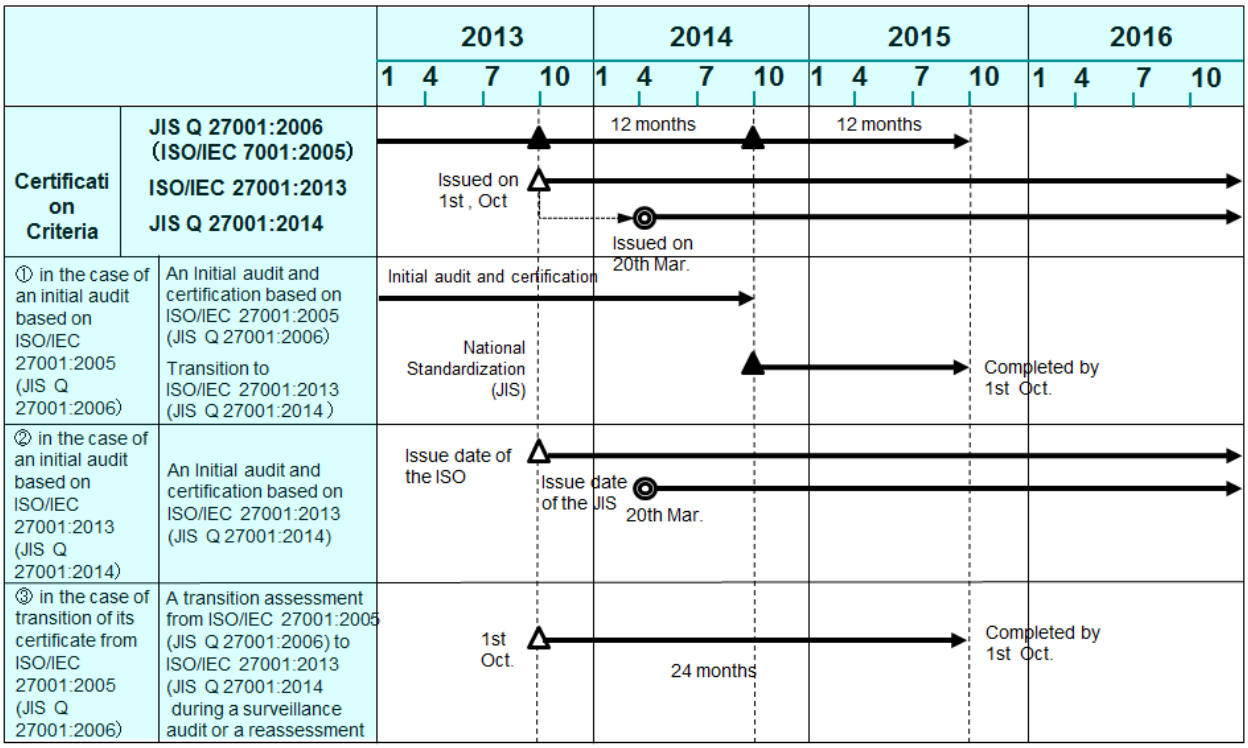
PAC has newly established a MLA for ISMS, extending the scope of MLA (Multilateral Recognition Arrangement) in addition to QMS, EMS, and product certification. IAF has also decided to include ISMS into the scope of IAF MLA. Our center seeks to actively contribute to operating ISMS MLA with a number of experiences on ISMS accreditation and certification.



8 Transition Schedule for JIS Q 27001 Implementation

The transition to ISO/IEC 27001:2013 was initiated with its publication. The transition was launched on the publication date of ISO/IEC 27001:2013 and will be completed within 2 years from the publication date, i.e. by 1 October 2015. This schedule is in line with the resolution of the 27th IAF-ILAC annual meetings held in October 2013.

There are several cases for organizations to make transition of its certificate or to newly obtain a certificate under the scheme. These are (1) in the case of an initial audit based on ISO/IEC 27001:2005, (2) in the case of an initial audit based on ISO/IEC 27001:2013 and (3) in the case of transition of its certificate from ISO/IEC 27001:2005.



In what points has ISO/IEC: 2013 (JIS Q 27001:2014) been mainly revised?

ISO/IEC 27001:2013 (JIS Q 27001:2014) has been revised mainly in consideration of:

- Common elements for ISO management system standards (MSS): it applies the high level structure, identical core text and common terms and definitions specified for all ISO MSS(see page 8);
- Consistency with ISO 31000:2009 (JIS Q 31000:2010)*;

  * ISO 31000:2009 (JIS Q 31000:2010) specifies principles and guidelines on risk management.
- Backward compatibility with ISO/IEC 27001:2005 (JIS Q 27001:2006).

An organization which already has been certified does not have to thoroughly change their ISMS, while it must review and update their ISMS from the management perspective in a planning stage in line with ISO/IEC 27001:2014. The new standard also focuses on the responsibilities of top management; Top management must demonstrate leadership and commitment to the ISMS by, for example, ensuring that the information security policy and objectives are established and compatible with the strategic directions of the organization.

An organization which is aimed at newly achieving ISMS certification can develop a framework with more emphasis on management elements. It leads to enhance the organizational governance to provide a good opportunity to review and improve the organization's overall management system.

It would be noted that the PDCA model is not directly mentioned in ISO/IEC 27001:2013 (JIS Q 27001:2014), but the PDCA approach is also considered in the revised standard.

9 Comparison of ISMS Certification Criteria

Structure of the main body of ISO/IEC 27001

ISO/IEC 27001:2013 (JIS Q 27001:2014) is a management system standard which applies common elements for ISO management systems standards (MSS)* as a basis and specifies ISMS specific requirements indispensable to information security.

The comparison of the structure between ISO/IEC 27001:2013 and ISO/IEC 27001:2006 is shown as below. The structure of ISO/IEC 27001:2013 is consistent with that of ISO MSS.

■ Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
0 Introduction	7 Support	0 Introduction	7 Management review of the ISMS
1 Scope	8 Operation	1 Scope	8 ISMS improvement
2 Normative references	9 Performance evaluation	2 Normative references	Annex A (normative) control objectives and controls
3 Terms and definitions	10 Improvement	3 Terms and definitions	Annex B (informative) OECD principles and this International Standard
4 Context of the organization	Annex A (normative) control objectives and controls	4 Information security management system	Annex C (informative) Correspondence among relevant standards
5 Leadership	Bibliography	5 Management responsibility	Bibliography
6 Planning		6 Internal ISMS audits	

* "common elements for ISO management system standards (MSS)" means "High level structure, identical core text, common terms and core definitions for use in Management Systems Standards" which have been specified in " Annex SL (normative) Proposals for management system standards" of "ISO/IEC Directives, Part 1 — Consolidated ISO Supplement — Procedures specific to ISO" issued in May 2012. Annex SL aims to enhance the consistency and alignment of ISO MSS's by providing the unifying and agreed structure, core text, and definitions. It has been decided that all management system standards to be issued in the future shall apply the Annex SL

.

Structure of "Annex A (normative) control objectives and controls"

Most clauses of "Annex A (normative) control objectives and controls" in ISO/IEC 27001:2005 have been taken over by those of Annex A in ISO/IEC 27001:2013 as well. Three new clauses have been also added to the clauses of Annex A in the 2013 version. Some of them include new contents, while others were made as a result that a clause in the 2005 version was split into two clauses. The structure of control objectives and controls were also reviewed and revised, and some controls have been replaced to other clauses in the 2013 version. As a result of additions, deletions, integrations and changes made to controls, the number of controls, which was 133 in the 2005 version of Annex A, is now 114 in the 2014 version of Annex A.

■ **Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005 (Annex A)**

Annex A, ISO/IEC 27001:2013		Annex A, ISO/IEC 27001:2005	
A.5	*Information security policies*	A.5	Security policy
A.6	*Organization of information security*	A.6	Organization of information security
A.7	*Human resource security*	A.8	Human resources security
A.8	*Asset management*	A.7	Asset management
A.9	*Access control*	A.11	Access control
A.10	*Cryptography*		
A.11	*Physical and environmental security*	A.9	Physical and environmental security
A.12	*Operations security*	A.10	Communications and operations managemen
A.13	*Communications security*		
A.14	*System acquisition, development and maintenance*	A.12	Information systems acquisition, development and maintenance
A.15	*Test data*		
A.16	*Information security incident management*	A.13	Information security incident management
A.17	*Information security aspects of business continuity management*	A.14	Business continuity management
A.18	Compliance	A.15	Compliance

●Contact Information●
JIPDEC IMPC
Roppongi First Building, 9-9 Roppongi 1-chome, Minato-ku Tokyo, 106-0032
TEL　+81 3-5860-7570　　FAX　+81 3-5573-0564
URL　http://www.isms.jipdec.or.jp/en/
Document No.: JIP-ISMS 120-5.0(E)

Roppongi First Building, 9-9 Roppongi 1-chome, Minato-ku Tokyo, 106-0032 JAPAN
TEL　+81 3-5860-7551　　FAX　+81 3-5573-0560
URL　http://www.jipdec.or.jp/eng/

April 2014