

Information Security Management Systems

Information Security
Management Systems
**Conformity Assessment
Scheme**

ISO/IEC 27001:2005 (JIS Q 27001:2006)



ISMS **JIPDEC**

IT Management Center
Japan Information Processing
Development Corporation

1. Purpose of the ISMS Conformity Assessment Scheme

The Conformity Assessment Scheme for Information Security Management Systems (ISMS) is an internationally consistent third party conformity assessment scheme for information security

management. This scheme is intended to contribute to raising the overall level of information security in Japan and to provide confidence in the level of information security to other countries.

2. International standardization on ISMS

International standards for information security management are developed by the Joint Technical Committee ISO/IEC JTC 1 (Information technology) /SC 27 (IT Security techniques). ISO/IEC 17799:2000 was prepared by the committee and published in 2000. Soon after the publication, a revision process started and subsequently the revised version, ISO/IEC 17799:2005, was issued in 2005. This standard is scheduled to be renumbered as ISO/IEC 27002 in 2007.

ISO/IEC 17799:2000 was published as a Japanese national standard, JIS X 5080:2002 in 2002. Its revised version, ISO/IEC 17799:2005 was also published as JIS Q 27002:2006 in May 2006. Another international standard on ISMS, ISO/IEC 27001:2005, was developed based on the British Standard BS 7799-2:2002 by the same committee and issued in October 2005. This standard was published as a Japanese national standard, JIS Q 27001:2006 in May 2006.

- ISO/IEC 17799:2005 (Information technology – Code of practice for information security management) is an International standard that provides the Code (best practice) for implementing an effective ISMS to those responsible for an organization's information security.
- BS 7799-2:2002 (Information security management systems – Specification with guidance for use) is a British Standard used as the basis of BS 7799 certification.
- ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements) is an international standard that provides requirements for an organization to establish an ISMS.

3. ISMS Certification Criteria (ISO/IEC 27001)

Criteria for the certification under the ISMS scheme (hereinafter referred to as ISMS certification criteria) provide a basis for use by third party certification bodies in assessing the conformity of organizations' ISMS that seek to achieve certification under the ISMS scheme.

In the ISMS scheme, ISMS certification criteria (Ver.0.8) were firstly developed based on both the international standard ISO/IEC 17799 and BS 7799-2. The certification criteria (Ver.0.8) were issued in April 2001 for a pilot project of the ISMS scheme.

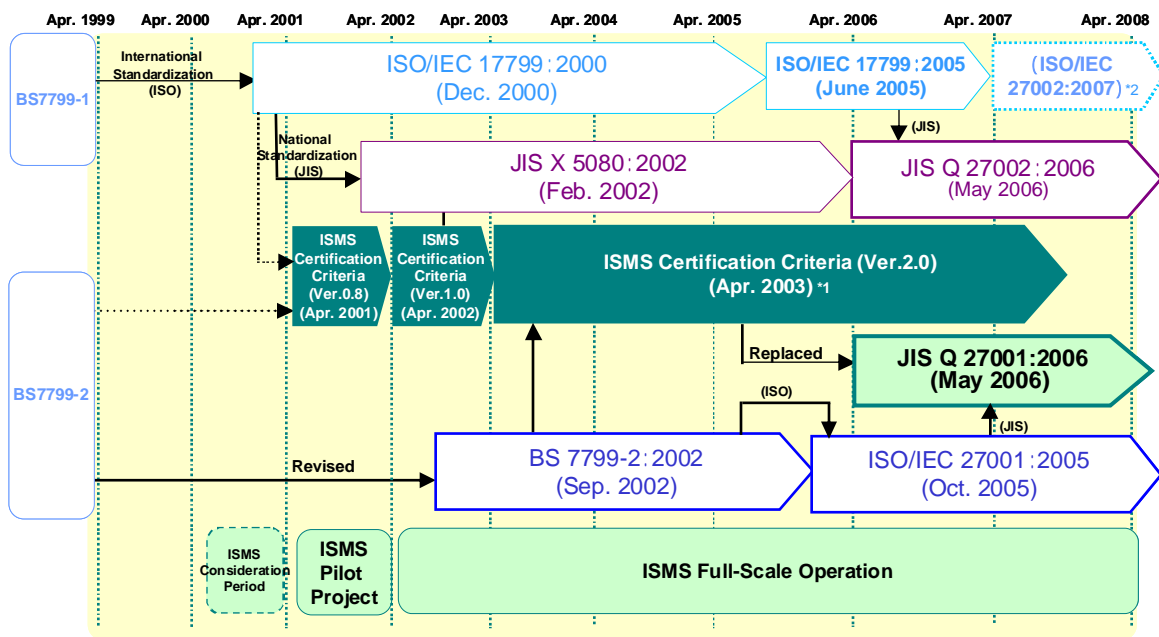
After the pilot project, ISMS certification criteria (Ver.1.0) were issued in April 2002 along with the launch of the full-scale operation of the ISMS scheme. The ISMS certification criteria (Ver.1.0) were then revised in line with the revision of BS 7799-2 and replaced by ISMS certification criteria (Ver.2.0) in April

2003. The criteria (Ver.2.0) have subsequently been used as the basis for ISMS certification under the scheme.

In October 2005, an international standard that specifies requirements for ISMS, ISO/IEC 27001:2005, was published. This standard was translated and published as a national standard JIS Q 27001:2006. Accordingly, the ISMS certification criteria (Ver.2.0) were replaced with JIS Q 27001. Certification activities based on the national standard started following the replacement.

Under the transition schedule on ISMS certification, the transition is to be completed by October 2007 (within 18 months of the publication of JIS Q 27001:2006). The ISMS certification criteria (Ver.2.0) is planned to be abolished at that point.

Development of ISO and JIS Standards on ISMS



NOTE: The abbreviations stand for the following: BS: British Standard, ISO/IEC: International standard, JIS: Japanese Industrial Standard, ISMS certification criteria (version n): JIPDEC criteria

*1: ISMS certification criteria (Ver.2.0) were developed based on British Standard BS 7799-2:2002, and with regard to terms and expressions, compatibility with 5080:2002 is ensured.

*2: The number of ISO/IEC 17799:2005 is to be changed to ISO/IEC 27002 in 2007.

4. Transition Schedule for ISO/IEC 27001 (JIS Q 27001) Implementation

The following transition schedule for ISMS certificates was initiated on the issue date of ISO/IEC 27001 (JIS Q 27001) (20th May 2006). The transition will be completed within 18 months after the issue date of the JIS standard. According to the schedule, there are three different ways 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 and surveillance audit based on Ver.2.0, (2) in the case of an initial audit based on ISO/IEC 27001 (JIS Q 27001) and (3) in the case of transition of its certificate based on Ver.2.0 to ISO/IEC 27001 (JIS Q 27001).

Transition of certification for Ver.2.0 to certification for ISO/IEC 27001

		2005				2006				2007				2008			
		1	4	7	10	1	4	7	10	1	4	7	10	1	4	7	10
Certification Criteria	ISMS certification criteria (Ver. 2.0)	Will be withdrawn															
	ISO/IEC 27001:2005	Issued on Oct. (National Standardization (JIS))															
JIS Q 27001 (ISO/IEC 27001)	Issued on May																
(1) In the case of an initial audit and a surveillance audit based on Ver.2.0	An initial audit and certification based on Ver. 2.0	Completed															
	A Surveillance audit based on Ver.2.0 and transition to JIS Q 27001 (ISO/IEC 27001)	(including a surveillance audit and reassessment)															
(2) In the case of an initial audit based on JIS Q 27001 (ISO/IEC 27001)	An initial audit and certification based on JIS Q 27001 (ISO/IEC 27001)	Initial audit and certification															
	A Surveillance audit based on JIS Q 27001 (ISO/IEC 27001)	Surveillance audit															
(3) In the case of transition of its certificate from Ver.2.0 to JIS Q 27001 (ISO/IEC 27001)	A transition assessment during a surveillance audit or a reassessment	Surveillance audit or reassessment (including a transition assessment to JIS Q 27001)															
		18 months															
		Transition will be completed															

NOTE: "Ver. 2.0" represents "ISMS certification criteria (ver.2.0)".

5. Key concept of an ISMS

An ISMS enables an organization to systematically operate its management system for information security. By establishing the ISMS, the organization can determine the necessary security level, make up plans and distribute its assets based on its own risk assessment in addition to technical countermeasures against each individual issue. The key concept of the ISMS is that an organization is

to equally maintain and improve confidentiality, integrity, and availability of its information assets that should be protected by the organization. In particular, by measuring the effectiveness of controls implemented through risk assessment within the ISMS, the organization is able to improve its information security in a more efficient and effective way.

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

In ISO/IEC 13335-1:2004, the three elements of information security are defined as the following:

- Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes;
- Integrity: The property of safeguarding the accuracy and completeness of assets;
- Availability: The property of being accessible and usable upon demand by an authorized entity.

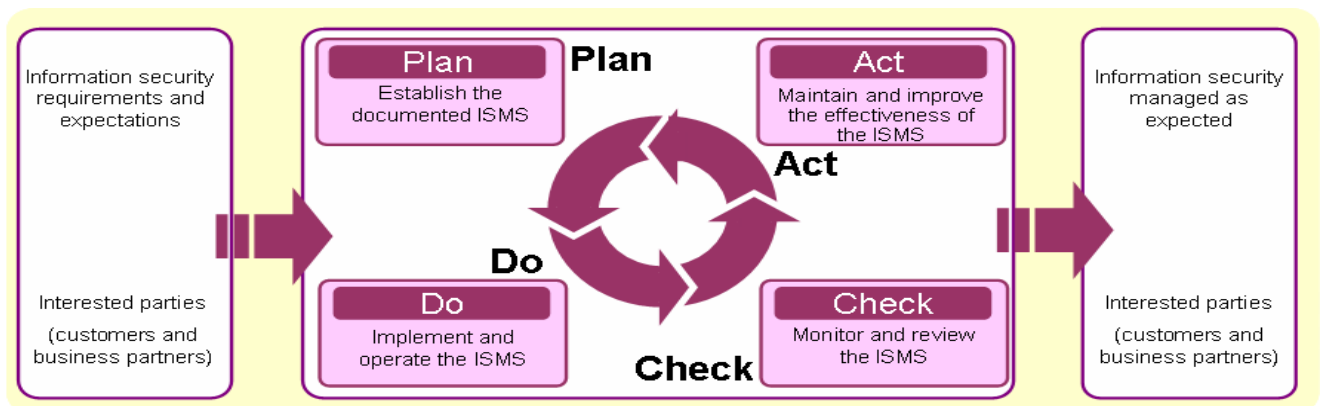
Process Approach Incorporating the PDCA Model

An organization must identify and manage a number of its activities to effectively operate its ISMS. ISO/IEC 27001 (JIS Q 27001) recommends that an organization should adopt a process approach when it establishes, implements, operates, monitors, reviews, maintains and improves the organization's ISMS.

In the process approach, what are referred to as processes are any activities that are managed using management resources in order to transform inputs into outputs. A process approach means identifying the processes within an organization, grasping their interaction, and applying and managing a series of those processes as a system.

The adoption of this process approach provides organizations with the benefit of being able to effectively operate their ISMS, through managing combinations of and interaction among processes together with links of individual processes.

By the application of the "Plan-Do-Check-Act (PDCA)" model to processes associated with information security, the effect (information security managed as expected) of information security satisfying "information security requirements and expectations of interested parties" can be produced through the processes as outputs, from those requirements and expectations put into it as inputs. The main point of the ISO/IEC 27001 (JIS Q 27001) is the continual improvement of the processes that produce the effects by applying this PDCA model.

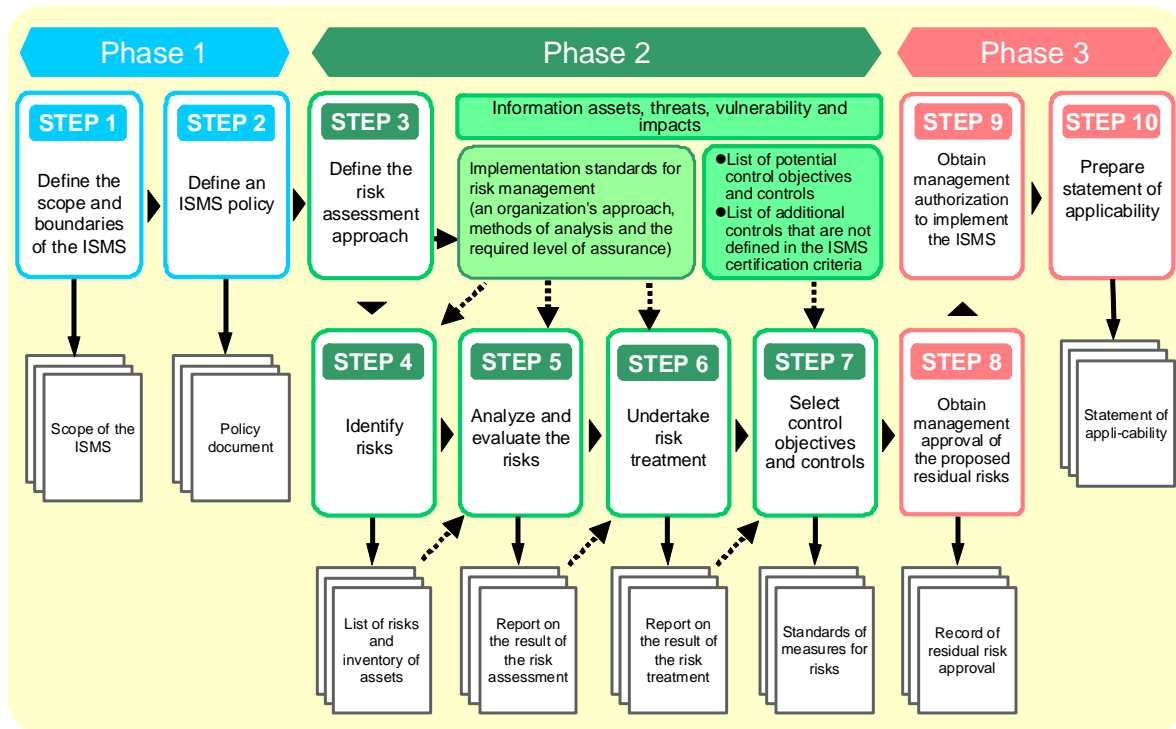


Plan (Establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (Implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (Monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (Maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

6. Establishment of the ISMS

The establishment of the ISMS can be divided into the following three phases.

- Phase 1: Establish the scope and policy of the ISMS (STEP 1 – STEP 2)
- Phase 2: Select controls based on risk assessment (STEP 3 – STEP 7)
- Phase 3: Plan to deal appropriately with risks (STEP 8 – STEP 10)



Phase 1: Establish the scope and policy of the ISMS (STEP 1 – STEP 2)

An organization shall define the scope and boundaries of the ISMS in light of the characteristics of the business, the organization, its location, assets and technology. Then, it shall define an ISMS policy that defines the establishment of the strategic risk management context, the organizational environment where the ISMS is established and maintained, and the overall direction and principles for information security. When defining the ISMS policy, an organization shall take into account the requirements for information security derived from business and legal or laudatory requirements and risk assessment.

Phase 2: Select controls based on risk assessment (STEP 3 – STEP 7)

On the basis of the defined scope and policy of the ISMS, the organization shall define an approach to risk assessment. Then, it shall identify the risks through the identification of threats and vulnerabilities that may cause the loss of confidentiality, integrity and availability on information assets requiring protection, as well as the extent of the potential impact on its business. On the risk assessment, it shall estimate the levels of risks based on the result of the evaluation of business damages by security failure and its likelihood, and then determine whether the risks are acceptable or needs to be treated by using risk acceptance criteria. Where the risks are not acceptable, the organization shall choose how to deal with the risks as risk treatment, that is, applying controls, accepting risks, avoiding risks, or transferring risks. In accordance with the decision on the risk treatment, select appropriate control objectives and controls from the list in the annex A "Control objectives and controls". It is also possible to adopt additional control objectives and controls as necessary.

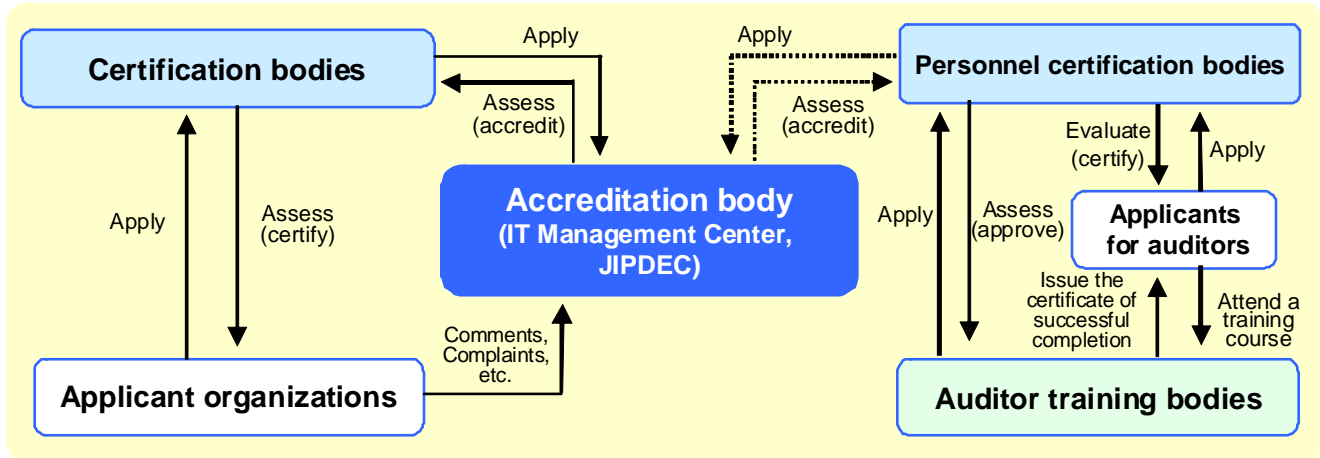
Phase 3: Plan to deal appropriately with risks (STEP 8 – STEP 10)

The organization shall obtain management approval of the proposed residual risks for the selected control objectives and controls, and obtain management authorization to implement the ISMS. The organization shall prepare a statement of applicability describing selected control objectives, controls and the reasons for the selection and the exclusion.

7. 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. With regard to "auditor training bodies", the personnel certification bodies carry out the assessment of those bodies and approve them based on the result of the assessment.



Structure of the ISMS Scheme

Accreditation body: IT Management Center, Japan Information Processing Development Corporation (JIPDEC)

- Operates, maintains and manages the overall ISMS Conformity Assessment Scheme,
- Accredits certification bodies and conducts periodical surveillances and 3- or 4-year re-assessment,
- Provides information on the ISMS Conformity Assessment Scheme, and
- Receives comments and complaints about the ISMS Conformity Assessment Scheme.

Certification bodies

- Achieve accreditation based on Accreditation Criteria for ISMS Certification bodies,
- Carry out assessment and registration of applicant organizations according to the Criteria for the Certification of Information Security Management Systems, and
- Conduct periodical surveillances and 3-year re-assessment of registered organizations.

Applicant organizations: Organizations seeking ISMS certification under the scheme

- Establish the scope and policy of the ISMS,
- Choose a certification body and make an application to the body,
- Undergo the assessment (Stage 1 and Stage 2) based on ISMS certification criteria and are certified and registered based on the result of the assessment, and
- When registered, are able to use the accreditation symbol on commercial documents.

Personnel certification bodies

- Evaluates and certifies ISMS auditors (provisional auditors, auditors and lead auditors) according to Qualification Criteria for ISMS Auditors, and
- Conducts re-evaluation of ISMS auditors every three years for their 3-year renewal of ISMS personnel certification.

Impartiality, Transparency and Objectivity of the ISMS Scheme Operation

The organizational structure for the ISMS scheme has two committees to ensure its impartiality, transparency and objectivity. One of the committees is the Steering Committee comprised of academic and relevant industry experts, and the

other is its sub-committee, the Technical Committee. For further information on the activities of these committees, please visit our website <http://www.isms.jipdec.jp/en/index.html>.

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 "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 an 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.
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 guidance 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 ISMS Certification/Registration Bodies	This document provides procedures for assessing and accrediting certification/registration bodies, and the rights and duties of both applicant and accredited bodies.
Guide for the Accreditation of ISMS Certification Bodies	This document describes general accreditation processes from application to registration and also processes for maintaining the accreditation together with conditions required in each process.
Conditions for the Use of ISMS Accreditation Symbols	This document specifies conditions for the use of ISMS accreditation symbols.

NOTE: In addition, there are some documents which support the promotion of the ISMS Conformity Assessment Scheme. These include practical experiences of certified organizations and the correspondence table of previous and new versions of ISMS certification criteria.

8. Necessity for Achieving ISMS Certification

Achieving ISMS certification under the ISMS scheme enables an organization to develop comprehensive and efficient information security measures and also to enhance its information security structure as well. Furthermore, by obtaining the certification, the organization can have greater confidence in its information security and assure its level of security to

its external and international partners. In addition, by maintaining risk management and implementing appropriate controls, the organization can reduce the likelihood of information security incidents and damages when they actually become obvious. This consequently leads to increased corporate value.

Benefits of developing and managing an ISMS

- **Comprehensive security measures can be developed from the aspect of both technical and personnel management.**
 - Enhancement of staff skills, clarification of responsibilities, improvement in the capability to deal with emergency situations, etc.
 - **Efficient security measures can be undertaken from a comprehensive management viewpoint.**
 - Asset management that considers cost-effectiveness, and the firm establishment of risk management, etc.
- *Effects such as improvement of security awareness are expected to be achieved through the continual implementation of these activities.

Benefits of achieving ISMS certification

- **Externally, confidence in information security can be secured.**
 - Satisfaction of security requirements of customers and trade partners, etc.
 - **Internally, the competitive edge of organizations can be enhanced.**
 - Satisfaction of 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.



●Contact Information●

IT Management Center

Japan Information Processing Development Corporation

Kikai Shinko Kaikan Bldg., 3-5-8 Shibakoen, Minato-ku, Tokyo 105-1011

TEL +81 3-3432-9386 FAX +81 3-3432-6200

URL <http://www.isms.jipdec.jp/en/index.html>

E-MAIL: info@isms.jipdec.jp

Document No.: JIP-ISMS 120-3.31E



Japan Information Processing Development Corporation

Kikai Shinko Kaikan Bldg., 3-5-8 Shibakoen, Minato-ku, Tokyo 105-1011

TEL +81 3-3432-9371 FAX +81 3-3432-9379

URL <http://www.jipdec.jp/eng/>