MALAYSIAN STANDARD

MS ISO/IEC 27006:2007

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — REQUIREMENTS FOR BODIES PROVIDING AUDIT AND CERTIFICATION OF INFORMATION SECURITY MANAGEMENT SYSTEMS (ISO/IEC 27006:2007, IDT)

ISO/IEC 27006:2007 is endorsed as Malaysian Standard with the reference number MS ISO/IEC 27006:2007

ICS: 35.040

Descriptors: bodies, audit, certification, ISMS

DEPARTMENT OF STANDARDS MALAYSIA

DEVELOPMENT OF MALAYSIAN STANDARDS

The **Department of Standards Malaysia (STANDARDS MALAYSIA)** is the national standardisation and accreditation body.

The main function of the Department is to foster and promote standards, standardisation and accreditation as a means of advancing the national economy, promoting industrial efficiency and development, benefiting the health and safety of the public, protecting the consumers, facilitating domestic and international trade and furthering international cooperation in relation to standards and standardisation.

Malaysian Standards are developed through consensus by committees which comprise of balanced representation of producers, users, consumers and others with relevant interests, as may be appropriate to the subject in hand. To the greatest extent possible, Malaysian Standards are aligned to or are adoption of international standards. Approval of a standard as a Malaysian Standard is governed by the Standards of Malaysia Act 1996 (Act 549). Malaysian Standards are reviewed periodically. The use of Malaysian Standards is voluntary except in so far as they are made mandatory by regulatory authorities by means of regulations, local by-laws or any other similar ways.

The Department of Standards appoints **SIRIM Berhad** as the agent to develop Malaysian Standards. The Department also appoints SIRIM Berhad as the agent for distribution and sale of Malaysian Standards.

For further information on Malaysian Standards, please contact:

Department of Standards Malaysia
Century Square, Level 1 & 2
Block 2300, Jalan Usahawan
63000 Cyberjaya
Selangor D.E.
MALAYSIA

Tel: 60 3 8318 0002
Fax: 60 3 8318 1455

http://www.standardsmalaysia.gov.my

E-mail:central@standardsmalaysia.gov.my

OR

SIRIM Berhad
(Company No. 367474 - V)
1, Persiaran Dato' Menteri
P.O. Box 7035, Section 2
40911 Shah Alam
Selangor D.E.

Tel: 60 3 5544 6000
Fax: 60 3 5510 8095

http://www.sirim.my

Committee representation

The Information Technology, Telecommunication and Multimedia Industry Standards Committee (ISC G) under whose authority this Malaysian standard was adopted, comprises representatives from the following organisations:

Association of Consulting Engineers Malaysia
Institusi Jurutera Malaysia
Jabatan Standard Malaysia
Kementerian Perdagangan Dalam Negeri & Hal Ehwal Pengguna Bahagian Hal Ehwal Pengguna
Kementerian Pertahanan
Kementerian Sains, Teknologi & Alam Sekitar
Kementerian Tenaga, Air dan Komunikasi Malaysia
MIMOS Berhad
Malaysian Administrative, Modernisation and Management Planning Unit
Malaysian Industry-Government Group for High Technology
Malaysian National Computer Confederation
Ministry of International Trade and Industry
Persatuan Industri Komputer dan Multimedia Malaysia
Suruhanjaya Komunikasi dan Multimedia Malaysia
Telekom Malaysia Berhad
Universiti Multimedia
Universiti Teknologi Malaysia

The TC on Information Security which supervised the adoption of ISO/IEC Standard consists of representatives from the following organisations:

Bank Negara Malaysia
CyberSecurity Malaysia
Kementerian Sains, Teknologi dan Inovasi
Kementerian Tenaga, Air dan Komunikasi Malaysia
Malaysian Administrative, Modernisation and Management Planning Unit
Malaysian National Computer Confederation
Malaysian Technical Standards Forum Bhd
Multimedia Development Corporation Sdn Bhd
Pejabat Keselamatan Kerajaan
Persatuan Industri Komputer dan Multimedia Malaysia
Polis Diraja Malaysia
PricewaterhouseCoopers
SIRIM QAS International Sdn Bhd
Suruhanjaya Komunikasi dan Multimedia Malaysia
Teknimuda Sdn Bhd
Telekom Malaysia Berhad
Universiti Teknologi Malaysia

The WG on Requirements, Security Services and Guidelines which recommends adoption of the ISO/IEC Standard consists of representatives from the following organisations:

Bank Negara Malaysia
CyberSecurity Malaysia
EXTOL
Expert
Jabatan Kerja Raya
Malaysian Administrative, Modernisation and Management Planning Unit
Malaysian National Computer Confederation
Pejabat Keselamatan Kerajaan
Persatuan Industri Komputer Dan Multimedia Malaysia
PricewaterhouseCoopers
SIRIM QAS International Sdn Bhd
Scan-Associates
Suruhanjaya Komunikasi dan Multimedia Malaysia
Teknimuda Sdn Bhd
Telekom Malaysia Berhad

FOREWORD

The adoption of the ISO/IEC Standard as a Malaysian Standard was recommended by the Working Group on Requirements, Security Services and Guidelines under the authority of the Information Technology, Telecommunication and Multimedia Industry Standards Committee.

This Malaysian Standard is identical with ISO/IEC 27006:2007, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems,* published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). However, for the purposes of this Malaysian Standard, the following apply:

a) in the source text, 'this International Standard' should read 'this Malaysian Standard';

b) the comma which is used as a decimal sign (if any), to read as a point; and

c) references to International Standard should be replaced by an equivalent Malaysian Standard as follows:

Referenced International Standards	Corresponding Malaysian Standards
ISO/IEC 17799:2005, *Information technology - Security techniques - Code of practice for information security management*	MS ISO/IEC 17799:2005, *Information technology - Security techniques - Code of practice for information security management*

This standard cancels and replaces MS 1537:2002.

Compliance with a Malaysian Standard does not of itself confer immunity from legal obligations.

NOTE. IDT on the front cover indicates an identical standard i.e. a standard where the technical content, structure, wording and presentation of a Malaysian Standard is exactly the same as in an International Standard or is identical in technical content and It may contain the minimal editorial changes specified in clause 4.2 of ISO/IEC Guide 21.

INTERNATIONAL STANDARD

ISO/IEC 27006

First edition
2007-03-01

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27006:2007(E)

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO and IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

The main task of the joint technical committee 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.

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/IEC 27006 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques*.