MAURITIAN STANDARD

MS ISO/IEC 27002:2013

Second edition
2014-01-18

Information technology -- Security techniques – Code of practice for Information security controls

PREVIEW

ICS 35.040

Mauritius Standards Bureau
Moka

Gr 21

© MSB 2014

National foreword

This Mauritian Standard is identical with the International Standard **ISO/IEC 27002:2013(E)**, *Information technology -- Security techniques – Code of practice for Information security controls.* It was adopted by the Mauritius Standards Bureau on the recommendation of the Information Technology Standards Committee and approval of the Standards Council on 05 December 2013. It was notified in the Government Gazette on 18 January 2014.*

For the purposes of this standard the following change should be made:

- Wherever the words 'International Standard' appear, referring to this standard, they should be read as 'Mauritian Standard'

This Mauritian Standard cancels and replaces the Mauritian Standard MS ISO/IEC 27002:2005, which has been technically revised.

The following Mauritian Standard is identical to the International Standard, which is referenced in the adopted standard:

International Standard	Corresponding Mauritian Standard
ISO/IEC 27000	**MS ISO/IEC 27000**, *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*

* General Notice No. 90 of 2014

PREVIEW

COPYRIGHT PROTECTED DOCUMENT

© MSB 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, or posting on the internet or an intranet, without prior written permission from Mauritius Standards Bureau at the address below

Mauritius Standards Bureau
Villa Road
Moka
Mauritius

Telephone + (230) 433 3648
Fax + (230) 433 5051/ 433 5150
E-mail msb@intnet.mu

 © MSB 2014 – All rights reserved

Contents

Page

Foreword ..... **v**

0 Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Structure of this standard **1**
4.1 Clauses 1
4.2 Control categories 1

5 Information security policies **2**
5.1 Management direction for information security 2

6 Organization of information security **4**
6.1 Internal organization 4
6.2 Mobile devices and teleworking 6

7 Human resource security **9**
7.1 Prior to employment 9
7.2 During employment 10
7.3 Termination and change of employment 13

8 Asset management **13**
8.1 Responsibility for assets 13
8.2 Information classification 15
8.3 Media handling 17

9 Access control **19**
9.1 Business requirements of access control 19
9.2 User access management 21
9.3 User responsibilities 24
9.4 System and application access control 25

10 Cryptography **28**
10.1 Cryptographic controls 28

11 Physical and environmental security **30**
11.1 Secure areas 30
11.2 Equipment 33

12 Operations security **38**
12.1 Operational procedures and responsibilities 38
12.2 Protection from malware 41
12.3 Backup 42
12.4 Logging and monitoring 43
12.5 Control of operational software 45
12.6 Technical vulnerability management 46
12.7 Information systems audit considerations 48

13 Communications security **49**
13.1 Network security management 49
13.2 Information transfer 50

14 System acquisition, development and maintenance **54**
14.1 Security requirements of information systems 54
14.2 Security in development and support processes 57
14.3 Test data 62

15 Supplier relationships **62**
15.1 Information security in supplier relationships 62

PREVIEW

© ISO/IEC 2013 – All rights reserved

15.2 Supplier service delivery management ... 66

16 Information security incident management ... 67
16.1 Management of information security incidents and improvements ... 67

17 Information security aspects of business continuity management ... 71
17.1 Information security continuity ... 71
17.2 Redundancies ... 73

18 Compliance ... 74
18.1 Compliance with legal and contractual requirements ... 74
18.2 Information security reviews ... 77

Bibliography ... 79

PREVIEW

 © ISO/IEC 2013 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or 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.

ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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.

This second edition cancels and replaces the first edition (ISO/IEC 27002:2005), which has been technically and structurally revised.

PREVIEW

© ISO/IEC 2013 – All rights reserved

0 Introduction

0.1 Background and context

This International Standard is designed for organizations to use as a reference for selecting controls within the process of implementing an Information Security Management System (ISMS) based on ISO/IEC 27001[10] or as a guidance document for organizations implementing commonly accepted information security controls. This standard is also intended for use in developing industry- and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s).

Organizations of all types and sizes (including public and private sector, commercial and non-profit) collect, process, store and transmit information in many forms including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards.

Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to implement a comprehensive suite of information security controls under the overall framework of a coherent management system.

Many information systems have not been designed to be secure in the sense of ISO/IEC 27001[10] and this standard. The security that can be achieved through technical means is limited and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.

In a more general sense, effective information security also assures management and other stakeholders that the organization's assets are reasonably safe and protected against harm, thereby acting as a business enabler.

0.2 Information security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements:

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy, and their socio-cultural environment;

PREVIEW

 © ISO/IEC 2013 – All rights reserved

c) the set of principles, objectives and business requirements for information handling, processing, storing, communicating and archiving that an organization has developed to support its operations.

Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk assessment will help guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks.

ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review.

0.3 Selecting controls

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate.

The selection of controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations. Control selection also depends on the manner in which controls interact to provide defence in depth.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. The controls are explained in more detail below along with implementation guidance. More information about selecting controls and other risk treatment options can be found in ISO/IEC 27005.[11]

0.4 Developing your own guidelines

This International Standard may be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

0.5 Lifecycle considerations

Information has a natural lifecycle, from creation and origination through storage, processing, use and transmission to its eventual destruction or decay. The value of, and risks to, assets may vary during their lifetime (e.g. unauthorized disclosure or theft of a company's financial accounts is far less significant after they have been formally published) but information security remains important to some extent at all stages.

Information systems have lifecycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be taken into account at every stage. New system developments and changes to existing systems present opportunities for organizations to update and improve security controls, taking actual incidents and current and projected information security risks into account.

0.6 Related standards

While this standard offers guidance on a broad range of information security controls that are commonly applied in many different organizations, the remaining standards in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ISMSs and the family of standards. ISO/IEC 27000 provides a glossary, formally defining most of the terms used throughout the ISO/IEC 27000 family of standards, and describes the scope and objectives for each member of the family.

PREVIEW

© ISO/IEC 2013 – All rights reserved

PREVIEW

Information technology — Security techniques — Code of practice for information security controls

1 Scope

This International Standard gives guidelines for 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).

This International Standard is designed to be used by organizations that intend to:

a) select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001;[10]

b) implement commonly accepted information security controls;

c) develop their own information security management guidelines.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.

4 Structure of this standard

This standard contains 14 security control clauses collectively containing a total of 35 main security categories and 114 controls.

4.1 Clauses

Each clause defining security controls contains one or more main security categories.

The order of the clauses in this standard does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, therefore each organization applying this standard should identify applicable controls, how important these are and their application to individual business processes. Furthermore, lists in this standard are not in priority order.

4.2 Control categories

Each main security control category contains:

a) a control objective stating what is to be achieved;

b) one or more controls that can be applied to achieve the control objective.

PREVIEW

© ISO/IEC 2013 – All rights reserved