

This is a preview of "BS ISO/IEC 27000:201...". Click here to purchase the full version from the ANSI store.

**BS ISO/IEC 27000:2012**



BSI Standards Publication

**Information technology —  
Security techniques —  
Information security  
management systems —  
Overview and vocabulary**

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

*raising standards worldwide™*



This is a preview of "BS ISO/IEC 27000:201...". [Click here to purchase the full version from the ANSI store.](#)

This British Standard is the UK implementation of ISO/IEC 27000:2012. It supersedes BS ISO/IEC 27000:2009 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2013

Published by BSI Standards Limited 2013

ISBN 978 0 580 73248 5

ICS 01.040.35; 35.040

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2013.

#### **Amendments issued since publication**

<b>Amd. No.</b>	<b>Date</b>	<b>Text affected</b>
-----------------	-------------	----------------------

---

This is a preview of "BS ISO/IEC 27000:201...". [Click here to purchase the full version from the ANSI store.](#)

Second edition  
2012-12-01

---

---

## **Information technology — Security techniques — Information security management systems — Overview and vocabulary**

*Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

---

---

Reference number  
ISO/IEC 27000:2012(E)



This is a preview of "BS ISO/IEC 27000:201...". Click here to purchase the full version from the ANSI store.



## **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2012

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, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "BS ISO/IEC 27000:201...". [Click here to purchase the full version from the ANSI store.](#)

## Foreword

ISO (the International Organisation 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 organisation to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organisations, 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 joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national 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 and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27000 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27000:2009).

## 0 Introduction

### 0.1 Overview

International Standards for management systems provide a model to follow in setting up and operating a management system. This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO/IEC JTC 1/SC 27 maintains an expert committee dedicated to the development of international management systems standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards.

Through the use of the ISMS family of standards, organisations can develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties. These standards can also be used to prepare for an independent assessment of their ISMS applied to the protection of information.

### 0.2 ISMS family of standards

The ISMS family of standards<sup>1)</sup> (see Clause 4) is intended to assist organisations of all types and sizes to implement and operate an ISMS and consists of the following International Standards, under the general title *Information technology — Security techniques (given below in numerical order)*:

- ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary*
- ISO/IEC 27001:2005, *Information security management systems — Requirements*
- ISO/IEC 27002:2005, *Code of practice for information security management*
- ISO/IEC 27003:2010, *Information security management system implementation guidance*
- ISO/IEC 27004:2009, *Information security management — Measurement*
- ISO/IEC 27005:2011, *Information security risk management*
- ISO/IEC 27006:2011, *Requirements for bodies providing audit and certification of information security management systems*
- ISO/IEC 27007:2011, *Guidelines for information security management systems auditing*
- ISO/IEC TR 27008:2011, *Guidelines for auditors on information security management systems controls*
- ISO/IEC 27010:2012, *Information security management guidelines for inter-sector and inter-organisational communications*
- ITU-T X.1051 | ISO/IEC 27011:2008, *Information security management guidelines for telecommunications organisations based on ISO/IEC 27002*
- ISO/IEC FDIS 27013, *Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
- ITU-T X.1054 | ISO/IEC FDIS 27014, *Governance of information security*

---

<sup>1)</sup> Standards identified throughout this subclause with no release year indicated are still under development.

This is a preview of "BS ISO/IEC 27000:201...". [Click here to purchase the full version from the ANSI store.](#)

- ISO/IEC TR 27015, *Information security management guidelines for financial services*
- ISO/IEC WD 27016, *Information security management – Organisational economics*

NOTE The general title "*Information technology — Security techniques*" indicates that these standards were prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

International Standards not under the same general title that are also part of the ISMS family of standards are as follows:

- ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*

### 0.3 Purpose of this International Standard

This International Standard provides an overview of information security management systems, and defines related terms.

NOTE Annex A provides clarification on how verbal forms are used to express requirements and/or guidance in the ISMS family of standards.

The ISMS family of standards includes standards that:

- a) define requirements for an ISMS and for those certifying such systems;
- b) provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements;
- c) address sector-specific guidelines for ISMS; and
- d) address conformity assessment for ISMS.

The terms and definitions provided in this International Standard:

- cover commonly used terms and definitions in the ISMS family of standards;
  - will not cover all terms and definitions applied within the ISMS family of standards; and
- do not limit the ISMS family of standards in defining new terms for use.

This is a preview of "BS ISO/IEC 27000:201...". Click [here](#) to purchase the full version from the ANSI store.

# Information technology — Security techniques — Information security management systems — Overview and vocabulary

## 1 Scope

This International Standard describes the overview and the vocabulary of information security management systems, which form the subject of the ISMS family of standards, and defines related terms and definitions.

This International Standard is applicable to all types and sizes of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations).

## 2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

**NOTE 1** A term in a definition or note which is defined elsewhere in this clause is indicated by boldface followed by its entry number in parentheses. Such a boldface term can be replaced in the definition by its complete definition.

For example:

**attack** (2.4) is defined as “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset** (2.3)”;

**asset** is defined as “any item that has value to the organisation”.

If the term “**asset**” is replaced by its definition:

**attack** then becomes “attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has value to the organisation”.

### 2.1

#### **access control**

means to ensure that access to **assets** (2.4) is authorized and restricted based on business and security requirements

### 2.2

#### **accountability**

assignment of actions and decisions to an entity

### 2.3

#### **analytical model**

algorithm or calculation combining one or more **base** (2.11) and/or **derived measures** (2.21) with associated decision

[ISO/IEC 15939:2007]

### 2.4

#### **asset**

anything that has value to the organisation

**NOTE** There are many types of assets, including: