Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information
Contents

Foreword ............................................................................................................................................................v
Introduction ........................................................................................................................................................vi
1 Scope ............................................................................................................................................................vi
2 Normative references ....................................................................................................................................1
3 Terms and definitions .................................................................................................................................1
4 Structure of this International Standard ...................................................................................................5
5 Background ..................................................................................................................................................6
6 Overview of the information security risk management process ...........................................................7
7 Context establishment .................................................................................................................................10
8 General considerations ...............................................................................................................................10
9 Basic Criteria ...............................................................................................................................................10
9.1 Risk management approach ................................................................................................................10
9.2 Risk evaluation criteria ........................................................................................................................10
9.3 Impact criteria .........................................................................................................................................11
9.4 Risk acceptance criteria ........................................................................................................................11
10 Scope and boundaries ..............................................................................................................................11
11 Organization for information security risk management ........................................................................12
12 Information security risk assessment .....................................................................................................13
12.1 General description of information security risk assessment ...............................................................13
12.2 Risk identification ..................................................................................................................................13
12.3 Introduction to risk identification .......................................................................................................13
12.4 Identification of assets ..........................................................................................................................14
12.5 Identification of threats ........................................................................................................................14
12.6 Identification of existing controls .......................................................................................................15
12.7 Identification of vulnerabilities ..........................................................................................................15
12.8 Identification of consequences ...........................................................................................................16
13 Risk analysis ...............................................................................................................................................17
13.1 Risk analysis methodologies ...............................................................................................................17
13.2 Assessment of consequences .............................................................................................................18
13.3 Assessment of incident likelihood .....................................................................................................18
13.4 Level of risk determination ...............................................................................................................19
14 Risk evaluation ........................................................................................................................................19
15 Information security risk treatment ........................................................................................................20
15.1 General description of risk treatment ..............................................................................................20

© ISO/IEC 2011 – 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.

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 27005 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 27005:2008) which has been technically revised.
Introduction

This International Standard provides guidelines for information security risk management in an organization, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001. However, this International Standard does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.