INTERNATIONAL **ISO/IEC**

First edition
2012-10-15

Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Technologies de l'information — Techniques de sécurité — Guide sur la mise en oeuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1

Reference number
ISO/IEC 27013:2012(E)

COPYRIGHT PROTECTED DOCUMENT

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
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

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 27013 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in co-operation with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

Introduction

The relationship between information security and service management is so close that many organizations already recognize the benefits of adopting both standards: ISO/IEC 27001 for information security, and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to conform with the requirements of one International Standard and then make further improvements to conform to the requirements of the other.

There are a number of advantages in implementing an integrated management system which takes into account not only the services provided but also the protection of information assets. These benefits can be experienced whether one standard is implemented before the other, or both standards are implemented simultaneously. Management and organizational processes, in particular, can derive benefit from the similarities between the International Standards and their common objectives.

Key benefits of an integrated implementation include:

a) the credibility, to internal or external customers of the organization, of an effective and secure service;

b) the lower cost of an integrated programme of two projects, where achieving both service management and information security are part of an organization's strategy;

c) a reduction in implementation time due to the integrated development of processes common to both standards;

d) elimination of unnecessary duplication;

e) a greater understanding by service management and security personnel of each others' viewpoints;

f) an organization certified for ISO/IEC 27001 can more easily fulfil the requirements for information security in ISO/IEC 20000-1:2011, subclause 6.6, as both International Standards are complementary in requirements.

The guidance is based upon the published versions of both International Standards, ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011.

This International Standard is intended for use by persons with knowledge of both, either or neither of the International Standards ISO/IEC 27001 and ISO/IEC 20000-1.

It is expected that all readers have access to copies of both International Standards. Consequently, this International Standard does not reproduce parts of either standard. Equally, it does not describe all parts of each International Standard comprehensively. Only those parts where subject matter overlaps are described in detail.

This International Standard does not give guidance associated with the various legislation and regulations outside the control of the organization. These can vary by country and impact the planning of an organization's management system.