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

Contents

Foreword........................................................................................................................................................................................................................................ iv
Introduction ....................................................................................................................................................................................................................................... v

1 Scope ..................................................................................................................................................................................................................................... 1

2 Normative references ...................................................................................................................................................................................................... 1

3 Terms, definitions and abbreviated terms .......................................................................................................................................................... 1

4 Overviews of ISO/IEC 27001 and ISO/IEC 20000-1 ................................................................................................................................................................. 2
  4.1 Understanding the International Standards ...................................................................................................................................................... 2
  4.2 ISO/IEC 27001 concepts ................................................................................................................................................................................. 2
  4.3 ISO/IEC 20000-1 concepts ............................................................................................................................................................................. 2
  4.4 Similarities and differences ............................................................................................................................................................................. 2

5 Approaches for integrated implementation ......................................................................................................................................................... 3
  5.1 General ...................................................................................................................................................................................................................... 3
  5.2 Considerations of scope .................................................................................................................................................................................. 4
  5.3 Pre-implementation scenarios ............................................................................................................................................................... 5
    5.3.1 General .................................................................................................................................................................................................. 5
    5.3.2 Neither standard is currently used as the basis for a management system .............................................................................................. 5
    5.3.3 A management system exists which fulfils the requirement of one of the standards .................................................................................. 6
    5.3.4 Separate management systems exist which fulfil the requirements of each standard ......................................................................... 6

6 Integrated implementation considerations ......................................................................................................................................................... 7
  6.1 General ...................................................................................................................................................................................................................... 7
  6.2 Potential challenges ..................................................................................................................................................................................... 7
    6.2.1 The usage and meaning of asset .......................................................................................................................................................... 7
    6.2.2 Design and transition of services ....................................................................................................................................................... 8
    6.2.3 Risk assessment and management .................................................................................................................................................. 8
    6.2.4 Differences in risk acceptance levels .............................................................................................................................................. 9
    6.2.5 Incident and problem management .................................................................................................................................................. 9
    6.2.6 Change management .......................................................................................................................................................................... 11
  6.3 Potential gains ................................................................................................................................................................................................ 12
    6.3.1 Use of the Plan-Do-Check-Act cycle .................................................................................................................................................. 12
    6.3.2 Service level management and reporting ........................................................................................................................................ 12
    6.3.3 Management commitment ................................................................................................................................................................. 12
    6.3.4 Capacity management ......................................................................................................................................................................... 13
    6.3.5 Management of third party risk ......................................................................................................................................................... 13
    6.3.6 Continuity and availability management ........................................................................................................................................ 14
    6.3.7 Supplier management ......................................................................................................................................................................... 14
    6.3.8 Configuration management ............................................................................................................................................................... 14
    6.3.9 Release and deployment management ............................................................................................................................................... 15
    6.3.10 Budgeting and accounting .............................................................................................................................................................. 15

Annex A (informative) Correspondence between ISO/IEC 27001 and ISO/IEC 20000-1 ........................................................................ 16


Bibliography ............................................................................................................................................................................................................ 39
**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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO’s adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27013:2012), which has been technically revised.
Introduction

The relationship between information security management and service management is so close that many organizations already recognize the benefits of adopting the two International Standards for these domains: ISO/IEC 27001 for information security management and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to achieve conformity with the requirements specified in one of these International Standards and then make further improvements to achieve conformity with the requirements of the other.

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

Key benefits of an integrated implementation of information security management and service management include the following:

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 effective and efficient management of both services 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) better communication, reduced cost and improved operational efficiency through 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 fulfill the requirements for information security specified in ISO/IEC 20000-1:2011, 6.6, as both International Standards are complementary in requirements.

The guidance in this International Standard is based upon the published versions of both ISO/IEC 27001 and ISO/IEC 20000-1.

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 ISO/IEC 27001 and ISO/IEC 20000-1. Consequently, this International Standard does not reproduce parts of either of those International Standards. 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 provide 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.