PD ISO/IEC TR 27023:2015

BSI Standards Publication

Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

bsi.

...making excellence a habit.™

National foreword

This British Standard is the UK implementation of ISO/IEC TR 27023:2015.

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.

ISBN 978 0 580 87610 3

ICS 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 July 2015.

Amendments issued since publication

Date	Text affected

PD ISO/IEC TR 27023:2015

TECHNICAL REPORT

ISO/IEC TR 27023

First edition
2015-07-01

Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

Technologies de l'information — Techniques de sécurité — Mappage des édtions révisées de l'ISO/IEC 27001 et de l'ISO/IEC 27002

Reference number
ISO/IEC TR 27023:2015(E)

Contents

Page

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*, SC 27, *IT Security techniques*.

Introduction

Both standards, ISO/IEC 27001 and ISO/IEC 27002, have been revised as part of the normal standards maintenance process, and the results of this revision process are contained in ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

This Technical Report contains the following tables:

— Clause 4, Table 1 — Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005;

— Clause 5, Table 2 — Comparison between ISO/IEC 27002:2005 and ISO/IEC 27002:2013;

— Clause 5, Table 3 — Comparison between ISO/IEC 27002:2013 and ISO/IEC 27002:2005.

These tables can be used to determine where requirements or controls in the old standards went, or where requirements or controls in the new standards have come from. Where a relationship is stated, it does not mean that the content is identical.

This Technical Report is designed to provide a factual correspondence between the old and new editions of ISO/IEC 27001 and ISO/IEC 27002 respectively, and so by intention it does not provide any explanatory commentary on why a change has been made or the significance of the change. Users of this Technical Report need to evaluate the significance of the changes in context with regard to their particular application and implementation of the revised editions of these standards.

For ISO/IEC 27002, the comparison was based on control objectives, controls, and implementation guidance.

Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

1 Scope

The purpose of this Technical Report is to show the corresponding relationship between the revised versions of ISO/IEC 27001 and ISO/IEC 27002.

This Technical Report will be useful to all users migrating from the 2005 to the 2013 versions of ISO/IEC 27001 and ISO/IEC 27002.

2 Normative references

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

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions contained in ISO/IEC 27000:2014 apply.

4 Comparison between revised editions of ISO/IEC 27001

Table 1 — Comparison between ISO/IEC 27001:2013 and ISO/IEC 27001:2005

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
4.1	Understanding the organization and its context	8.3	Preventive action
4.2 a)	Understanding the needs and expectations of interested parties		New requirement
4.2 b)	Understanding the needs and expectations of interested parties	5.2.1 c)	Provision of resources
		7.3 c) 4)	Review output
		7.3 c) 5)	Review output
4.3	Determining the scope of the information security management system	4.2.1 a)	Establish the ISMS
4.3 a)	Determining the scope of the information security management system	4.2.1 a)	Establish the ISMS
		4.2.3 f)	Monitor and review the ISMS
4.3 b)	Determining the scope of the information security management system	4.2.3 f)	Monitor and review the ISMS