BS 7799-3:2017

BSI Standards Publication

Information security management systems

Part 3: Guidelines for information security risk management (revision of BS ISO/IEC 27005:2011)

bsi.

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

Published by BSI Standards Limited 2017

ISBN 978 0 580 97052 8

ICS 03.100.70 | 35.020 | 35.030

The following BSI references relate to the work on this document:
Committee reference IST/33
Draft for comment 17/30354571 DC

Amendments/corrigenda issued since publication

Date	Text affected

Contents

Summary of pages
This document comprises a front cover, and inside front cover, pages i to iv, pages 1 to 31, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard is published by BSI Standards Limited, under licence from The British Standards Institution, and came into effect on 31 October 2017. It was prepared by Technical Committee IST/33, *IT – Security Techniques*. A list of organizations represented on this committee can be obtained on request to its secretary.

Supersession

This British Standard supersedes BS 7799-3:2006 and BS ISO/IEC 27005:2011, which are withdrawn.

Relationship with other publications

BS 7799-3:2006 was produced as a British Standard to provide guidance and advice to support the implementation of the BS ISO/IEC 27001:2005 requirements that related to risk management processes and associated activities. It was withdrawn following the publication of BS ISO/IEC 27005:2008, which effectively fulfilled the same needs, thereby rendering BS 7799-3 redundant. BS ISO/IEC 27005 was revised in 2011 to align it with the vocabulary and concepts embodied in BS ISO 31000.

However, BS ISO/IEC 27005:2011 is not aligned with the requirements of BS EN ISO/IEC 27001:2017 and a revised version of BS ISO/IEC 27005 is still under discussion within ISO/IEC. A new version is not expected in the foreseeable future.

Given this situation, and with the ever-growing user demand for risk management guidance, BS 7799-3 has been updated to align with the requirements of BS EN ISO/IEC 27001:2017 and republished as BS 7799-3:2017 to fill the market gap.

Information about this document

This is a full revision of the standard, and introduces the following principal changes:

- guidance on using the event-consequence approach as well as the asset–threat–vulnerability approach to risk assessment; and
- an explanation of the new requirements for dealing with BS EN ISO/IEC 27001:2017, Annex A controls.

Use of this document

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it were a specification or a code of practice and claims of compliance cannot be made to it.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Any recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of The Shorter Oxford English Dictionary is used (e.g. “organization” rather than “organisation”).

Contractual and legal considerations

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

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

THIS PAGE DELIBERATELY LEFT BLANK

Introduction

This British Standard is intended to assist organizations in addressing the risks and opportunities highlighted by the requirements of BS EN ISO/IEC 27001:2017, principally **6.1** and Clause **8** of that document.

This British Standard is intended to be considered, interpreted and adapted to suit each organization's specific situation. The concepts and approaches are intended to be broadly applicable, but the particular method that any particular organization requires depend on contextual factors (such as its size, sector, maturity, information security risks, compliance obligations and management style) that vary widely in practice.

This British Standard contains the description of the information security assessment and the risk treatment process and its activities.

A general overview of the information security risk assessment and risk treatment processes is given in Clause **4**.

The remainder of this standard is structured as follows:

- communication and consultation in Clause **5**;
- context establishment in Clause **6**;
- risk identification and analysis in Clause **7**;
- information security risk treatment in Clause **8**;
- verification of necessary controls in Clause **9**;
- approval in Clause **10**;
- operation in Clause **11**;
- monitoring, audit and review in Clause **12**; and
- documented information in Clause **13**.

There is a table showing the relationship between this document and the previous edition, BS 7799-3:2006, in Annex A.

1 Scope

This British Standard provides guidance to assist organizations to:

a) fulfil the requirements of BS EN ISO/IEC 27001 concerning risks and opportunities; and

b) define, apply, maintain and evaluate risk management processes in the information security context.

This British Standard is relevant to:

1) organizations who have or are intending to have an information security management system (ISMS) that conforms to BS EN ISO/IEC 27001; and

2) persons that perform or are involved in information security risk management (e.g. interested parties, risk owners and ISMS professionals).

This document is applicable to all organizations, regardless of type, size or nature.

