



BSI Standards Publication

Information technology — Security techniques — Guidelines for the assessment of information security controls

National foreword

This Published Document is the UK implementation of ISO/IEC TS 27008:2019. It supersedes PD ISO/IEC TR 27008:2011, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Software and systems engineering.

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.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 94767 4

ICS 35.030; 03.100.70

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

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 January 2019.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

**Information technology — Security
techniques — Guidelines for
the assessment of information
security controls**

*Technologies de l'information — Techniques de sécurité —
Lignes directrices pour les auteurs des contrôles de sécurité de
l'information*



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Structure of this document	1
5 Background	2
6 Overview of information security control assessments	3
6.1 Assessment process.....	3
6.1.1 General.....	3
6.1.2 Preliminary information.....	3
6.1.3 Assessment checklists.....	3
6.1.4 Review fieldwork.....	4
6.1.5 The analysis process.....	5
6.2 Resourcing and competence.....	5
7 Review methods	6
7.1 Overview.....	6
7.2 Process analysis.....	7
7.2.1 General.....	7
7.3 Examination techniques.....	7
7.3.1 General.....	7
7.3.2 Procedural controls.....	8
7.3.3 Technical controls.....	8
7.4 Testing and validation techniques.....	8
7.4.1 General.....	8
7.4.2 Blind testing.....	9
7.4.3 Double Blind Testing.....	9
7.4.4 Grey Box Testing.....	9
7.4.5 Double Grey Box Testing.....	10
7.4.6 Tandem Testing.....	10
7.4.7 Reverse.....	10
7.5 Sampling techniques.....	10
7.5.1 General.....	10
7.5.2 Representative sampling.....	10
7.5.3 Exhaustive sampling.....	10
8 Control assessment process	10
8.1 Preparations.....	10
8.2 Planning the assessment.....	12
8.2.1 Overview.....	12
8.2.2 Scoping the assessment.....	13
8.2.3 Review procedures.....	13
8.2.4 Object-related considerations.....	14
8.2.5 Previous findings.....	14
8.2.6 Work assignments.....	15
8.2.7 External systems.....	15
8.2.8 Information assets and organization.....	16
8.2.9 Extended review procedure.....	16
8.2.10 Optimization.....	16
8.2.11 Finalization.....	17
8.3 Conduction reviews.....	17
8.4 Analysis and reporting results.....	18

Annex A (Informative) Initial information gathering (other than IT)	20
Annex B (informative) Practice guide for technical security assessments	24
Annex C (informative) Technical assessment guide for cloud services (Infrastructure as a service)	65
Bibliography	98

Currently in preview, click buy full version

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.

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) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

ISO/IEC TS 27008 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC TS 27008 cancels and replaces ISO/IEC TR 27008:2011.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document supports the Information Security Risk Management process pointed out in ISO/IEC 27001, and any relevant control sets identified

Information security controls should be fit-for-purpose (meaning appropriate and suitable to the task at hand i.e. capable of mitigating information risks), effective (e.g. properly specified, designed, implemented, used, managed and maintained) and efficient (delivering net value to the organization). This document explains how to assess an organization's information security controls against those and other objectives in order either to confirm that they are indeed fit-for-purpose, effective and efficient (providing assurance), or to identify the need for changes (improvement opportunities). The ultimate aim is that the information security controls, as a whole, adequately mitigate information risks that the organization finds unacceptable and unavoidable, in a reasonably cost-effective and business-aligned manner. It offers the flexibility needed to customize the necessary reviews based on business missions and goals, organizational policies and requirements, known emerging threats and vulnerabilities, operational considerations, information system and platform dependencies, and the risk appetite of the organization.

Please refer to ISO/IEC 27007 for guidelines for information security management systems auditing and ISO/IEC 27006 for requirements for bodies providing audit and certification of information security management systems.

Information technology — Security techniques — Guidelines for the assessment of information security controls

1 Scope

This document provides guidance on reviewing and assessing the implementation and operation of information security controls, including the technical assessment of information system controls, in compliance with an organization's established information security requirements including technical compliance against assessment criteria based on the information security requirements established by the organization.

This document offers guidance on how to review and assess information security controls being managed through an Information Security Management System specified by ISO/IEC 27001.

It is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations conducting information security reviews and technical compliance checks.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27017:2015, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27001 for cloud services*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

4 Structure of this document

This document contains a description of the information security control assessment process including technical assessment.

[Clause 5](#) provides background information.

[Clause 6](#) provides an overview of information security control assessments.

[Clause 7](#) presents review methods.

[Clause 8](#) presents the control assessment process.