TECHNICAL ISO/IEC TS

First edition
2019-01

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

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

Reference number
ISO/IEC TS 27008:2019(E)

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

Published in Switzerland

Contents

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.