TECHNICAL **ISO/IEC TS**

First edition
2021-02

Requirements for bodies providing audit and certification of information security management systems —

Part 2: Privacy information management systems

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité —

Partie 2: Systèmes de management des informations de sécurité

Reference number
ISO/IEC TS 27006-2:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
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 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.

This document was prepared by Joint Technical Committee ISO/JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 27006 series can be found on the ISO website.

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

ISO/IEC 27006 sets out criteria for bodies providing audit and certification of information security management systems. If such bodies are also to be accredited as complying with ISO/IEC 27006 with the objective of auditing and certifying privacy information management systems (PIMS) in accordance with ISO/IEC 27701:2019, some additional requirements and guidance to ISO/IEC 27006 are necessary. These are provided by this document.

The text in this document follows the structure of ISO/IEC 27006 and the additional PIMS-specific requirements and guidance on the application of ISO/IEC 27006 for PIMS certification are identified by the letters “PS”.

The primary purpose of this document is to enable accreditation bodies to more effectively harmonize their application of the standards against which they are bound to assess certification bodies.