სსტ ისო/იეკ 27021:2017/2021

საქართველოს სტანდარტი

სსკ: 03.100.70; 35.030

საინფორმაციო ტექნოლოგიები-უსაფრთხოების ტექნიკები-კომპეტენციის მოთხოვნები საინფორმაციო უსაფრთხოების მენეჯმენტის სისტემების პროფესიონალებისათვის

სსტ ისო/იეკ 27021:2017/2021

საინფორმაციო მონაცემები

1 **მიღებულია და დაშვებულია სამოქმედოდ:** სსიპ-საქართველოს სტანდარტებისა და მეტროლოგიის ეროვნული სააგენტოს გენერალური დირექტორის 15/12/2021 წლის № 76 განკარგულებით

2 **მიღებულია „თავფურცლის“ თარგმნის მეთოდით:** სტანდარტიზაციის საერთაშორისო ორგანიზაციის (ისო) სტანდარტი ისო/იეკ 27021:2017 ,, საინფორმაციო ტექნოლოგიები-უსაფრთხოების ტექნიკები-კომპეტენციის მოთხოვნები საინფორმაციო უსაფრთხოების მენეჯმენტის სისტემების პროფესიონალებისათვის”

3 **პირველად**

4 **რეგისტრირებულია:** სსიპ-საქართველოს სტანდარტებისა და მეტროლოგიის ეროვნული სააგენტოს რეესტრში: 15/12/2021 წლის №268-1.3-021696

INTERNATIONAL STANDARD

ISO/IEC 27021

First edition
2017-10

Information technology — Security techniques — Competence requirements for information security management systems professionals

Technologies de l'information — Tecniques de sécurité — Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité

Reference number
ISO/IEC 27021:2017(E)

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

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 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 the following URL: www.iso.org/iso/foreword.html.

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

Introduction

This document is intended for use by:

a) individuals who would like to demonstrate their competence as information security management system (ISMS) professionals, or who wish to understand and accomplish the competence required for working in this area, as well as wishing to broaden their knowledge,

b) organizations seeking potential ISMS professional candidates to define the competence required for positions in ISMS related roles,

c) bodies to develop certification for ISMS professionals which need a body of knowledge (BOK) for examination sources, and

d) organizations for education and training, such as universities and vocational institutions, to align their syllabuses and courses to the competence requirements for ISMS professionals.

This document should be read and used in conjunction with ISO/IEC 27001.