INTERNATIONAL STANDARD

**ISO/IEC 29146**

First edition
2016-06-01

**AMENDMENT 1**
**2022-08**

# Information technology — Security techniques — A framework for access management

AMENDMENT 1

*Technologies de l'information — Techniques de sécurité — Cadre pour gestion d'accès*

*AMENDEMENT 1*

Reference number
ISO/IEC 29146:2016/Amd. 1:2022(E)

## COPYRIGHT PROTECTED DOCUMENT

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

# 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 or www.iec.ch/members_experts/refdocs).

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 https://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. In the IEC, see www.iec.ch/understanding-standards.

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

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 and www.iec.ch/national-committees.

# Information technology — Security techniques — A framework for access management

## AMENDMENT 1

*Clause 2*

Replace ISO/IEC 24760-1:2011 with ISO/IEC 24760-1:2019.

*Annex A*

Change the title to:

Common access control models

*A.2.4*

Change the title of the subclause to:

Identifier-based access control (IBAC)

Replace the whole text with the following:

> An identifier-based access control model, idiomatically called “identity-based security”, is based on the authenticated identifier in this document. This model employs mechanisms such as the access control list (ACL) which contains the identifiers of subjects together with corresponding operations allowed or denied to the resource. In this model, functions of PDP and PEP are configured on an ACL which maps subject identifiers to authorized resource access operations.
>
> In IBAC systems’ administration, subject’s accounts should be registered and configured via the ACL to reflect the access privileges assigned to that subject. In subsequent usage of the IBAC system, registered subjects shall first authenticate themselves to the system – possibly using an authentication token issued from the system. Following a successful authentication, the system binds the authenticated subject to the corresponding identifier in the ACL, that identifier being deemed the “authenticated identifier” for the permitted duration of the authorized access.

*A.2.8*

Delete the subclause.

**ICS 35.030**

Price based on 1 pages