SLOVENSKI STANDARD
SIST EN 16495:2019

01-september-2019

Nadomešča:
SIST EN 16495:2014

Upravljanje zračnega prometa - Varnost informacij za organizacije na področju dejavnosti civilnega letalstva

Air Traffic Management - Information security for organisations supporting civil aviation operations

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

Gestion du trafic aérien - Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile

Ta slovenski standard je istoveten z: **EN 16495:2019**

ICS:

03.220.50	Zračni transport	Air transport
35.240.60	Uporabniške rešitve IT v prometu	IT applications in transport

SIST EN 16495:2019 **sl,en,fr**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16495

July 2019

ICS 03.100.70; 03.220.50; 35.240.60

Supersedes EN 16495:2014

English Version

Air Traffic Management - Information security for organisations supporting civil aviation operations

Gestion du trafic aérien - Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

This European Standard was approved by CEN on 12 May 2019.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. EN 16495:2019 E

Contents

Page

European foreword

This document (EN 16495:2019) has been prepared by Technical Committee CEN/TC 377 “Air Traffic Management”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 2020, and conflicting national standards shall be withdrawn at the latest by January 2020.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN 16495:2014.

In comparison with the previous edition, the following technical modifications have been made:

— adaptation to the structures of EN ISO/IEC 27002:2017 and ISO/IEC 27009:2016;

— guidance on alignment of safety and security management;

— guidance on Information Security specific to development and production and maintenance;

— guidance on information security assurance;

— informative Annex D “Application of Controls in Regulatory Oversight — Implementation Example”;

— informative Annex E “Guidance on aviation specific transorganisational aspects”.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

This document provides guiding principles based on EN ISO/IEC 27002:2017 “Code of practice for information security controls” applied to security management systems in aviation organisations. The aim of this document is to extend the contents of EN ISO/IEC 27002:2017 to the domain of air traffic management, thus allowing aviation organisations to implement a standardized and specific information security management system (ISMS), that is in accordance with EN ISO/IEC 27001:2017 transorganisational aspects of air traffic management.

In addition to the security objectives and measures that are set forth in EN ISO/IEC 27001:2017, aviation organisations are subject to further special requirements: Service delivery in aviation is greatly defined by the cooperation of the individual participants. An organization’s information security management is therefore dependent on the information security management of the organisations with which it cooperates to deliver service. This document therefore focuses on aspects of cooperation.

This cooperation requires

— sharing the results of risk assessments along the business process chain;

— agreement on the required level of trust;

— agreement on the required security controls and their implementation.

1 Scope

This document provides guidance based on EN ISO/IEC 27002:2017 applied to organisations supporting civil aviation, with a focus on air traffic management operations.

This includes, but is not limited to, airspace users, airports and air navigation service providers.

Not included are activities of the organisations that do not have any impact on the security of civil aviation operations like for example airport retail and service business and corporate real estate management.

The basis of all guidance in this document is trust and cooperation between the parties involved in Air Traffic Management.

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 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

EN ISO/IEC 27001:2017, *Information technology — Security techniques — Information security management systems — Requirements*

EN ISO/IEC 27002:2017, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2018 and the following apply.

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

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
air traffic management
functional system comprised of an aggregation of the airborne and ground-based functions (air traffic services, airspace management and air traffic flow management) required to ensure the safe and efficient movement of aircraft during all phases of operations and covering responsibilities of all partners of the air traffic transport value chain

3.1.2
trust
situation where one party is willing to rely on the actions of another party

Note 1 to entry: Trust is more than what can be achieved by assurance. However, assurance represents a supporting instrument to trust building.

3.1.3
transorganisational process
process between several organisations that interact as interested parties between each other

3.1.4
functional system
combination of systems, procedures and human resources organised to perform a function within the context of ATM

[SOURCE: COMMISSION REGULATION (EC) No 2096/2005, Article 2]

3.2 Abbreviations

API	Application Programming Interface
ATM	Air Traffic Management
CA	Certification Authority
Ch.	Chapter
CP	Certificate Policy
CPS	Certificate Practice Statement
CS	Certificate Service
cts	Client-to-site VPN
DIM	Digital Identity Management
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICAO	International Civial Aviation Authority
IDM	Identity Management
ISDN	Integrated Services Digital Network
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
LoT-A	Level of Trust for the Application Area
LoT-O	Level of Trust of the Organization
PKI	Public Key Infrastructure
PPr	Partner network, protected
PPu	Partner network, public
PSTN	Public Switched Telephone Network
PuP	Public, unprotected
PuP	Public, protected
SQL	Structured Query Language
sts	Site-to-site VPN
u	Unencrypted
v	Encrypted

XSS Cross-Site Scripting

4 Aviation specific requirements related to EN ISO/IEC 27001:2017

4.1 Structure of this European Standard

This European Standard is structured in line with EN ISO/IEC 27009.

Guidance on additional aviation specific controls and concepts in relation to the global public key infrastructures are included in Annex E.

4.2 Refinement of EN ISO/IEC 27001:2017 requirements

All requirements from EN ISO/IEC 27001:2017 that do not appear below apply unchanged EN ISO/IEC 27001:2017, 6.1.3 c) is refined as follows:

Compare the controls determined in 6.1.3 b) above with those in EN ISO/IEC 27001:2017, Annex A and with Annex A of this document to verity that no necessary controls have been omitted.

EN ISO/IEC 27001:2017, 6.1.3 d) is refined as follows.

Produce a Statement of Applicability that contains:

— the necessary controls [see EN ISO/IEC 27001:2017, 6.1.3 b) and c)];

— a justification for their inclusion;

— whether the necessary controls are implemented or not; and

— a justification for excluding any of the controls in EN ISO/IEC 27001:2017, Annex A or Annex A of this document.

NOTE These refinements are necessary due to the introduction of new sector-specific controls in this document.

5 Information Security policies

5.1 Management direction for Information security

5.1.1 Policies for information security

Additional Implementation guidance for EN ISO/IEC 27002:2017, 5.1.1

The policies for information security should be coordinated with the various security requirements in other areas of aviation (e.g.: physical security of secure areas). The distinctions and mutual dependencies between the individual areas should be documented in the policies or in separate documents.

5.1.2 Review of the policies for information security

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 5.1.2.

6 Organization of information security

6.1 Internal organization

6.1.1 Information security roles and responsibilities

Additional Implementation guidance for EN ISO/IEC 27002:2017, 6.1.1

The organization should appoint a person responsible to serve as a point of contact for strategic information security issues for third parties (e.g. for the planning and implementation of joint measures, etc.).

6.1.2 Segregation of duties

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 6.1.2.

6.1.3 Contact with authorities

Additional Implementation guidance for EN ISO/IEC 27002:2017, 6.1.3

The organization should cooperate with the appropriate specialist and supervisory authorities, particularly in the areas of IT security and prosecution, and with other critical infrastructures as well.

This includes contacts to authorities involved in critical infrastructure protection at the national and European level.

6.1.4 Contact with special interest groups

Additional Implementation guidance for EN ISO/IEC 27002:2017, 6.1.4

The organization should establish an interface to other organisations.

Contacts should also consider the needs and expectations of interested parties, in particular organisations with which the organization shares information security risks in terms of the creation or contribution to aviation safety hazards and the management thereof.

The establishment of formal interfaces to critical organisations should be considered.

The organization should also be aware of the criticality of its services at a regional, national and international level. It may therefore participate in associations and alliances as well as national and international programs to provide comprehensive support to air safety.

Given the special nature of threats to air traffic, the organization may need to cooperate with other aviation organisations to present an agreed position. Such a position should form the basis for the selection of adequate, preventive and reactive measures:

— ensuring the interoperability of the selected measures;

— fostering the cooperation in raising the alarm in the event of IT crises affecting multiple organisations and in crisis management;

— based on lessons learned jointly from security incidents.

6.1.5 Information security in project management

The controls recommended in EN ISO/IEC 27002:2017, 6.1.5, apply accordingly.

6.2 Mobile devices and teleworking

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 6.2.

7 Human resources security

7.1 Prior to employment

7.1.1 Screening

Additional Implementation guidance for EN ISO/IEC 27002:2017, 7.1.1

The list on verification are amended by item.

f) social media checks of should be considered as an additional means for screening

The following paragraphs are amended.

Multiple organisations should ensure that background verification checks are carried out by partner organisations to an appropriate level, to ensure that access to data/information shared between partner organisations takes account of the national and commercial interests of all stakeholders. In aviation access to information processing facilities includes the design, operation and maintenance of aviation information systems.

For persons who can affect the design operation or maintenance of a safety-critical system, the organization should also consider further, more detailed verifications.

7.1.2 Terms and conditions of employment

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 7.1.2.

7.2 During employment

7.2.1 Management responsibilities

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 7.2.1.

7.2.2 Information security awareness, education and training

Additional Implementation guidance for EN ISO/IEC 27002:2017, 7.2.2

Employee awareness, education and training should be performed especially in line with the relevant security provisions of the ICAO Convention annexes and other documents.

The organization should ensure that the competency of application developers will enable them to implement secure applications.

7.2.3 Disciplinary process

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 7.2.3.

7.3 Termination and change of employment

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 7.3.

8 Asset management

8.1 Responsibility for assets

8.1.1 Inventory of assets

Additional Implementation guidance for EN ISO/IEC 27002:2017, 8.1.1

The asset inventory should be aligned with inventories that provide configuration information for all information processing assets, including software patching levels.

8.1.2 Ownership of assets

Additional Implementation guidance for EN ISO/IEC 27002:2017, 8.1.2

Where assets are used in business processes shared by multiple organisations the interests of the other organisations should be taken into account by the owners.

8.1.3 Acceptable use of assets

No additional information specific to aviation organisations for EN ISO/IEC 27002:2017, 8.1.3.