SLOVENSKI STANDARD
oSIST prEN 16495:2018

01-september-2018

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: prEN 16495

ICS:

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

oSIST prEN 16495:2018 en,fr,de

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 16495

June 2018

ICS 03.100.70; 03.220.50; 35.240.60

Will supersede 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 draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 377.

If this draft becomes a European Standard, 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.

This draft European Standard was established by CEN 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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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. prEN 16495:2018 E

Contents

European foreword

This document (prEN 16495:2018) has been prepared by Technical Committee CEN/TC 377 “Air Traffic Management”, the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

This document will supersede EN 16495:2014.

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

- Adaptation to the structures of ISO/IEC 27002:2013 and ISO/IEC DIS 27009:2015
- Advise on alignment of safety and security management
- Advise on Security specific to development & production and maintenance
- Advise on security assurance
- Informative Annex on

Introduction

This document provides guiding principles based on ISO/IEC 27001:2013 "Information technology — Security techniques — Information security management systems — Requirements" applied to security management systems in aviation organisations. The aim of this document is to extend the contents of ISO/IEC 27002:2013 to the domain of aviation, thus allowing aviation organisations to implement a standardized and specific information security management system (ISMS) and to extend it from the level of an individual organisation to the transorganisational level.

In addition to the security objectives and measures that are set forth in ISO/IEC 27002:2013, security management in aviation organisations are subject to further special requirements: Service delivery in aviation is greatly defined by the cooperation of the individual participants. An organisation's information security management is therefore dependent on the information security management of the organisations with which it cooperates to deliver service. This European Standard 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 European Standard defines guidelines and general principles for the implementation of an information security management system in organisations supporting civil aviation operations.

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.

For the purpose of this European Standard, Air Traffic management is seen as functional expression covering responsibilities of all partners of the air traffic value chain. This includes but is not limited to airspace users, airports and air navigation service providers.

The basis of all requirements in this European Standard 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*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

3 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
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

3.2
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

4 Information security management in aviation

4.1 Structure of this European Standard

This European Standard is structured in line with ISO/IEC 27002. ISO/IEC 27002 is merely referenced in all cases in which its measures can be applied without being amended or supplemented:

- in all cases in which the implementation of ISO/IEC 27002 measures requires supplementation specific to aviation, this has been integrated directly in the respective section;

- implementation examples for specific application areas are described in Annex A (informative). This relates to the following areas:

- security of information in web applications and web services;

- connections between multiple organisations /external connections;

- certificates / Public Key Infrastructure;

- identity Management.

4.2 Aviation specific requirements related to ISO/IEC 27001:2013

ISO/IEC 27001:2013 Requirements on 4.2 "Understanding the needs and expectations of interested parties" are amended by a note:

Interested parties include other organizations with interfaces to the organization which involve network connections and/or the exchange of data and/or information

ISO/IEC 27001:2013 Requirements on 5.3 "Organizational roles, responsibilities and authorities" are amended as follows:

Top Management shall ensure seamlessness of information security management within the own organisation including transorganisational processes.

ISO/IEC 27001:2013 Requirements on 6.1 "Actions to address risks and opportunities" are amended by a new section 6.1.4 "Information security risk information sharing":

The organization shall assess the risk due to external network connections and/or the exchange of data and/or information by:

a) Identifying information flows across external interfaces with other organizations

b) Including such flows and interfaces explicitly in the risk assessment described in 6.1.2

c) Seeking risk assessment and risk treatment information from the organization(s) sharing the external interface and controlling the information which crosses it, as input to the risk assessment

d) Sharing appropriate risk assessment information created in 6.1.2 and risk treatment information created in 6.1.3 with organizations which share the external interface

ISO/IEC 27001:2013 Requirements on 6.1.2c on "Information security risk assessment" are amended by a 3rd item:

Identify system interfaces with other organizations which involve network connections and/or the exchange of data and/or information that may pose a risk to the organization

Add a reference to 27001:2013, 6.1.2 c) 3) to 6.1.2 d) 1) and 2)

ISO/IEC 27001:2013 Requirement s on 7.4 "Communication" are refined by the following note

There will be a need for external communications with organizations with which the organization shares data and/or information and/or network connections, as described in 6.1.4.

ISO/IEC 27001:2013 Requirements on 8.2 "Information risk assessment" are amended as follows:

The organization shall share appropriate risk assessment information with organizations with which it shares data and/or information and/or network connections as described in 6.1.4.

ISO/IEC 27001:2013 Requirements on 8.3 "Information security risk treatment" are amended as follows:

The organization shall share appropriate risk treatment information with organizations with which it shares data and/or information and/or network connections as described in 6.1.4.

5 Information Security policies

5.1 Management direction for Information security

5.1.1 Policies for information security

Additional Implementation guidance for ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 5.1.2.

6 Organisation of information security

6.1 Internal organisation

6.1.1 Information security roles and responsibilities

Additional Implementation guidance for ISO/IEC 27002:2013, 6.1.1

The organisation 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 ISO/IEC 27002:2013, 6.1.2.

6.1.3 Contact with authorities

Additional Implementation guidance for ISO/IEC 27002:2013, 6.1.3

The organisation 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 ISO/IEC 27002:2013, 6.1.4

The organisation should establish an interface to other organisations

Contacts should also consider the needs and expectations of interested parties, in particular organisations with which the organisation 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 organisation 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 organisation 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 ISO/IEC 27002:2013, 6.1.5, apply accordingly.

6.2 Mobile devices and teleworking

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 6.2.

7 Human resources security

7.1 Prior to employment

7.1.1 Screening

Additional Implementation guidance for ISO/IEC 27002:2013, 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.

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 ISO/IEC 27002:2013, 7.1.2.

7.2 During employment

7.2.1 Management responsibilities

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 7.2.1.

7.2.2 Information security awareness, education and training

Additional Implementation guidance for ISO/IEC 27002:2013 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 organisation 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 ISO/IEC 27002:2013, 7.2.3.

7.3 Termination and change of employment

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 7.3.

8 Asset management

8.1 Responsibility for assets

8.1.1 Inventory of assets

Additional Implementation guidance for ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 8.1.3.

8.1.4 Return of assets

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 8.1.4.

8.2 Information classification

8.2.1 Classification of information

Additional Implementation guidance for ISO/IEC 27002:2013, 8.2.1

To ensure comparability across multiple organisations, an organisation should classify the information it uses in shared business processes in a way that is acceptable to and agreed by all partners in the business process. Such information should be classified to ensure that national and commercial interests are appropriately protected.

Confidentiality classes:

Information should be assigned to confidentiality classes on the basis of the anticipated damage to business processes if this information becomes known to unauthorised parties.

Public: information that will not result in any damage to the business process/the organisations involved if it becomes known

Internal: information that will result in low to medium damage to the business process/the organisations involved if it becomes known

Confidential: information that can result in major damage to the business process/the organisations involved if it becomes known

Strictly confidential: information that can result in substantial to existential damage to the business process/the organisations involved if it becomes known

Generally, information should only be shared on a need-to-know basis.

Other information specific to aviation

Business needs and the business impacts associated with these needs may include the public interest in the safe and expeditious provision of the service as well as the commercial interests of the individual stakeholders involved.

8.2.2 Labelling of information

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 8.2.2.

8.2.3 Handling of assets

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 8.2.3.

8.3 Media Handling

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 8.3.

9 Access control

9.1 Business requirement for access control

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.1.

9.2 User access management

9.2.1 User registration and de-registration

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.2.1.

9.2.2 User access provisioning

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.2.2.

9.2.3 Management of privileged access rights

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.2.3.

9.2.4 Management of secret authentication information of users

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.2.4.

9.2.5 Review of user access rights

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.2.5.

9.2.6 Removal or adjustment of access rights

No additional information specific to aviation organisations for ISO/IEC 27002:2013, 9.2.6.

9.2.7 Digital Identity Management

Additional Control for ISO/IEC 27002:2013, 9.2

Control

The organisation should operate a central Identity Management System to provide management of digital identities, their authentication, authorisation, roles and privileges. Validity of an identity should be traceably predetermined relative to the source system of the identity.

Implementation guidance

Source databases (e.g. LDAP, Active Directory, distributed databases such as SAP, etc.) of the Identity Management System should provide a unique relation between an identity and an entity of the central Identity Management System.

The following key processes for managing digital identities should be implemented:

- generation of digital identities;
- change (customise, extend, delete) of attributes of a digital identity;
- disabling/deleting of digital identities;
- systematic provision of digital identity information (including authentication data) to connected
- systems;
- processing of information (from personnel administration and organisational management) for
- automated administration of user groups, roles, and privileges (authorisation profiles);
- systematic provisioning of user groups, roles, and privileges in connected systems.

Each of the above processes associated to the digital Identity Management should be documented and be traceable.

Validity should be implemented through an attached personnel management system or via a connected corporate directory.

Provided manual processes have to be used, the validity period should not exceed a maximum of one year. Revalidation should be done at least once a year by a review.

9.2.8 Unique representation of entities across organisations

Additional Control for ISO/IEC 27002:2013, 9.2

Control

Inter-organisational Identity Management should use a unique representation of entities.