

<b>STN</b>	<b>Manažérstvo letovej prevádzky Informačná bezpečnosť organizácií podporujúcich prevádzky v civilnom letectve</b>	<b>STN EN 16495</b>  31 0813
------------	--	--

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

Táto norma obsahuje anglickú verziu európskej normy.  
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 12/19

Obsahuje: EN 16495:2019

Oznámením tejto normy sa ruší  
STN EN 16495 (31 0813) z júna 2014

**130143**

EUROPEAN STANDARD

**EN 16495**

NORME EUROPÉENNE

EUROPÄISCHE NORM

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**

**EN 16495:2019 (E)**

<b>Contents</b>	<b>Page</b>
European foreword.....	7
Introduction .....	8
<b>1 Scope .....</b>	<b>9</b>
<b>2 Normative references.....</b>	<b>9</b>
<b>3 Terms, definitions and abbreviations .....</b>	<b>9</b>
<b>3.1 Terms and definitions .....</b>	<b>9</b>
<b>3.2 Abbreviations .....</b>	<b>10</b>
<b>4 Aviation specific requirements related to EN ISO/IEC 27001:2017.....</b>	<b>11</b>
<b>4.1 Structure of this European Standard .....</b>	<b>11</b>
<b>4.2 Refinement of EN ISO/IEC 27001:2017 requirements .....</b>	<b>11</b>
<b>5 Information Security policies .....</b>	<b>11</b>
<b>5.1 Management direction for Information security.....</b>	<b>11</b>
<b>5.1.1 Policies for information security.....</b>	<b>11</b>
<b>5.1.2 Review of the policies for information security.....</b>	<b>11</b>
<b>6 Organization of information security .....</b>	<b>11</b>
<b>6.1 Internal organization.....</b>	<b>11</b>
<b>6.1.1 Information security roles and responsibilities.....</b>	<b>11</b>
<b>6.1.2 Segregation of duties .....</b>	<b>12</b>
<b>6.1.3 Contact with authorities .....</b>	<b>12</b>
<b>6.1.4 Contact with special interest groups.....</b>	<b>12</b>
<b>6.1.5 Information security in project management .....</b>	<b>12</b>
<b>6.2 Mobile devices and teleworking.....</b>	<b>12</b>
<b>7 Human resources security.....</b>	<b>12</b>
<b>7.1 Prior to employment.....</b>	<b>12</b>
<b>7.1.1 Screening.....</b>	<b>12</b>
<b>7.1.2 Terms and conditions of employment.....</b>	<b>13</b>
<b>7.2 During employment .....</b>	<b>13</b>
<b>7.2.1 Management responsibilities .....</b>	<b>13</b>
<b>7.2.2 Information security awareness, education and training.....</b>	<b>13</b>
<b>7.2.3 Disciplinary process.....</b>	<b>13</b>
<b>7.3 Termination and change of employment .....</b>	<b>13</b>
<b>8 Asset management.....</b>	<b>13</b>
<b>8.1 Responsibility for assets.....</b>	<b>13</b>
<b>8.1.1 Inventory of assets.....</b>	<b>13</b>
<b>8.1.2 Ownership of assets .....</b>	<b>13</b>
<b>8.1.3 Acceptable use of assets.....</b>	<b>13</b>
<b>8.1.4 Return of assets .....</b>	<b>14</b>
<b>8.2 Information classification .....</b>	<b>14</b>
<b>8.2.1 Classification of information.....</b>	<b>14</b>
<b>8.2.2 Labelling of information .....</b>	<b>14</b>
<b>8.2.3 Handling of assets .....</b>	<b>14</b>
<b>8.3 Media Handling.....</b>	<b>14</b>
<b>9 Access control.....</b>	<b>14</b>
<b>9.1 Business requirement for access control .....</b>	<b>14</b>
<b>9.2 User access management .....</b>	<b>14</b>

9.2.1	User registration and de-registration .....	14
9.2.2	User access provisioning.....	15
9.2.3	Management of privileged access rights.....	15
9.2.4	Management of secret authentication information of users.....	15
9.2.5	Review of user access rights .....	15
9.2.6	Removal or adjustment of access rights.....	15
9.2.7	Digital Identity Management.....	15
9.2.8	Unique representation of entities across organisations .....	16
9.3	User responsibilities .....	16
9.4	System and application access control .....	16
9.4.1	Information access restriction.....	16
9.4.2	Secure log-on procedures.....	16
9.4.3	Password management system .....	16
9.4.4	Use of privileged utility programs.....	16
9.4.5	Access control to program source code.....	16
9.4.6	Web Application Firewalls .....	16
10	Cryptography .....	17
10.1	Cryptographic controls.....	17
10.1.1	Policy on the use of cryptographic controls.....	17
10.1.2	Key management .....	17
11	Physical and environmental security.....	17
11.1	Secure areas.....	17
11.1.1	Physical security perimeter.....	17
11.1.2	Physical entry controls.....	18
11.1.3	Securing offices, rooms, and facilities.....	18
11.1.4	Protecting against external and environmental threats.....	18
11.1.5	Working in secure areas .....	18
11.1.6	Delivery and loading areas.....	18
11.2	Equipment.....	18
11.2.1	Equipment siting and protection .....	18
11.2.2	Supporting utilities .....	18
11.2.3	Cabling security.....	18
11.2.4	Equipment maintenance.....	18
11.2.5	Removal of assets .....	18
11.2.6	Security of equipment and assets off-premises.....	18
11.2.7	Secure disposal or re-use of equipment.....	18
11.2.8	Unattended user equipment.....	18
11.2.9	Clear desk and clear screen policy .....	18
12	Operations security.....	19
12.1	Operational procedures and responsibilities .....	19
12.2	Protection from malware .....	19
12.3	Information Back-up .....	19
12.4	Logging and monitoring .....	19
12.4.1	Event logging.....	19
12.4.2	Protection of log information.....	19
12.4.3	Administrator and operator logs.....	19
12.4.4	Clock synchronisation.....	19
12.5	Control of operational software .....	19
12.6	Technical Vulnerability Management.....	19
12.7	Information systems audit considerations .....	19
13	Communications security.....	19
13.1	Network security management .....	19

**EN 16495:2019 (E)**

13.1.1	Network controls.....	19
13.1.2	Security of network services.....	20
13.1.3	Segregation in networks.....	20
13.2	Information transfer.....	20
14	System acquisition, development and maintenance.....	20
14.1	Security requirements of information systems.....	20
14.1.1	Information Security requirements analysis and specification.....	20
14.1.2	Securing application services on public networks.....	20
14.1.3	Protecting application services transactions.....	20
14.2	Security in development and support processes.....	20
14.2.1	Secure development policy.....	20
14.2.2	System change control procedures.....	20
14.2.3	Technical review of applications after operating platform changes.....	20
14.2.4	Restrictions on changes to software packages.....	21
14.2.5	Secure system engineering principles.....	21
14.2.6	Secure development environment.....	21
14.2.7	Outsourced development.....	21
14.2.8	System security testing.....	21
14.2.9	System acceptance testing.....	21
14.3	Test data.....	21
15	Supplier relationships.....	21
15.1	Information security in supplier relationships.....	21
15.1.1	Information security policy for supplier relationships.....	21
15.1.2	Addressing security within supplier agreements.....	21
15.1.3	Information and communication technology supply chain.....	21
15.2	Supplier service delivery management.....	21
16	Information security incident management.....	22
16.1	Management of information security incidents and improvements.....	22
16.1.1	Responsibilities and procedures.....	22
16.1.2	Reporting information security events.....	22
16.1.3	Reporting information security weaknesses.....	22
16.1.4	Assessment of and decision on information security events.....	22
16.1.5	Response to information security incidents.....	22
16.1.6	Learning from information security incidents.....	22
16.1.7	Collection of evidence.....	22
17	Information security aspects of business continuity management.....	23
17.1	Information security continuity.....	23
17.1.1	Planning information security continuity.....	23
17.1.2	Implementing information security continuity.....	23
17.1.3	Verify, review and evaluate information security continuity.....	23
17.1.4	Business continuity planning framework.....	24
17.2	Redundancies.....	24
18	Compliance.....	24
18.1	Compliance with legal and contractual requirements.....	24
18.1.1	Identification of applicable legislation and contractual requirements.....	24
18.1.2	Intellectual property rights.....	24
18.1.3	Protection of records.....	24
18.1.4	Privacy and protection of personally identifiable information.....	24
18.1.5	Regulation of cryptographic controls.....	25
18.2	Information security reviews.....	25
18.2.1	Independent review of information security.....	25

<b>18.2.2 Compliance with security policies and standards .....</b>	<b>25</b>
<b>18.2.3 Technical compliance review.....</b>	<b>25</b>
<b>Annex A (informative) Additional guidance related to air traffic management.....</b>	<b>26</b>
<b>A.1 Assessment of information security risks .....</b>	<b>26</b>
<b>A.1.1 Internal information security risk management .....</b>	<b>26</b>
<b>Figure A.1 —Assessment of information security risks .....</b>	<b>27</b>
<b>A.2 Interoperability issues of risk assessments.....</b>	<b>29</b>
<b>A.2.1 General .....</b>	<b>29</b>
<b>A.2.2 Information security risk management for multiple organisations.....</b>	<b>29</b>
<b>A.2.3 Alignment of safety and security risk management.....</b>	<b>30</b>
<b>A.3 Determining controls .....</b>	<b>30</b>
<b>A.4 Levels of trust.....</b>	<b>30</b>
<b>A.4.1 Introduction.....</b>	<b>30</b>
<b>A.4.2 Scale of trust levels.....</b>	<b>31</b>
<b>A.4.3 Classification criteria .....</b>	<b>32</b>
<b>A.5 Statement of applicability.....</b>	<b>32</b>
<b>A.6 Measurement and auditing of security .....</b>	<b>32</b>
<b>Annex B (informative) Implementation examples .....</b>	<b>33</b>
<b>B.1 General .....</b>	<b>33</b>
<b>Table B.1 —Overview of an example for LoT-O .....</b>	<b>33</b>
<b>Figure B.1 —LoT-A versus LoT-O .....</b>	<b>34</b>
<b>B.2 Security of information in web applications and web services (LoT-A-WEB).....</b>	<b>34</b>
<b>B.2.1 General .....</b>	<b>34</b>
<b>B.2.2 Parameters for the Level of Trust of a web application/web service.....</b>	<b>34</b>
<b>B.2.3 Determination of the web application / the web service (LoT-A-WEB) .....</b>	<b>34</b>
<b>Table B.2 —Level of Trust of the web application/the web service .....</b>	<b>35</b>
<b>B.2.4 Consequences.....</b>	<b>35</b>
<b>Table B.3 —Evaluation Criteria for LoT-A-WEB .....</b>	<b>35</b>
<b>B.3 Connections between multiple organisations/external connections (LoT-A-NET) .....</b>	<b>35</b>
<b>B.3.1 Determination of the necessary protection controls.....</b>	<b>35</b>
<b>B.3.1.1 General .....</b>	<b>35</b>
<b>Figure B.2 —Process for implementation of external connection protection .....</b>	<b>36</b>
<b>B.3.1.2 Identity of the User.....</b>	<b>36</b>
<b>B.3.1.3 Owner of the terminal device.....</b>	<b>37</b>
<b>B.3.1.4 Connection point/Protection of the terminal device.....</b>	<b>37</b>
<b>B.3.1.5 Authentication of the connection.....</b>	<b>37</b>
<b>B.3.1.6 Transfer net.....</b>	<b>38</b>

**EN 16495:2019 (E)**

<b>Table B.4 —Maximum Level of Trust depending on the respective technical parameters.....</b>	<b>38</b>
<b>B.3.2 Effects of the coupling of networks.....</b>	<b>40</b>
<b>B.4 Certificates/Public Key Infrastructure (LoT-A-PKI) .....</b>	<b>41</b>
<b>B.4.1 Parameters for the Level of Trust of the certificate management .....</b>	<b>41</b>
<b>B.4.2 Determination of the Level of Trust of the certificate management (LoT-A-PKI).....</b>	<b>41</b>
<b>Table B.5 —Trust of identity management.....</b>	<b>41</b>
<b>B.4.3 Effects: Recognition of Certificates/PKI.....</b>	<b>41</b>
<b>B.5 Identity Management (LoT-A-IDM) .....</b>	<b>42</b>
<b>B.5.1 Parameters for the Level of Trust of Identity Management .....</b>	<b>42</b>
<b>B.5.2 Determination of the Level of Trust of the Identity Management (LoT-A-IDM).....</b>	<b>42</b>
<b>Table B.6 —Level of Trust of the Identity Management.....</b>	<b>43</b>
<b>B.5.3 Effects: Recognition of identities.....</b>	<b>43</b>
<b>Annex C (informative) Level of trust — Implementation Example .....</b>	<b>44</b>
<b>Table C.1 —Further security controls appropriate to different levels of trust.....</b>	<b>44</b>
<b>Annex D (informative) Application of Controls in Regulatory Oversight — Implementation Example .....</b>	<b>58</b>
<b>Figure D.1 —Oversight scheme .....</b>	<b>59</b>
<b>Table D.1 — Mapping of Controls .....</b>	<b>59</b>
<b>Annex E (informativ) Guidance on aviation specific transorganisational aspects.....</b>	<b>63</b>
<b>Bibliography.....</b>	<b>64</b>

## 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.



**EN 16495:2019 (E)****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*

**koniec náhľadu – text ďalej pokračuje v platenej verzii STN**