

<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.

Obsahuje: EN 16495:2014

**119033**

---

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, odbor SÚTN, 2014  
Podľa zákona č. 264/1999 Z. z. v znení neskorších predpisov sa môžu slovenské technické normy rozmnožovať a rozširovať iba so súhlasom Úradu pre normalizáciu, metrológiu a skúšobníctvo SR.

---

ICS 03.220.50; 35.040

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 Zivilluffahrt

This European Standard was approved by CEN on 9 November 2013.

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, 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: Avenue Marnix 17, B-1000 Brussels**

<b>Contents</b>	<b>Page</b>
Foreword.....	4
<b>1 Scope .....</b>	<b>5</b>
<b>2 Normative references .....</b>	<b>5</b>
<b>3 Terms and definitions .....</b>	<b>5</b>
<b>4 Information security management in aviation .....</b>	<b>5</b>
4.1 Structure of this European Standard.....	5
4.2 Information security management systems in aviation .....	6
4.3 Assessment of information security risks .....	6
4.4 Selecting controls.....	10
4.5 Levels of trust .....	10
4.6 Statement of applicability .....	12
4.7 Measurement and auditing of security.....	12
<b>5 Security policy .....</b>	<b>12</b>
5.1 Information security policy.....	12
<b>6 Organisational security.....</b>	<b>13</b>
6.1 Internal organisation .....	13
6.2 External parties.....	14
<b>7 Asset management.....</b>	<b>15</b>
7.1 Responsibility for assets .....	15
7.2 Information classification .....	15
<b>8 Human resources security.....</b>	<b>16</b>
8.1 Prior to employment.....	16
8.2 During employment .....	17
8.3 Termination or change of employment .....	17
<b>9 Physical and environmental security .....</b>	<b>18</b>
9.1 Secure areas.....	18
9.2 Equipment security.....	18
<b>10 Communications and operations management .....</b>	<b>19</b>
10.1 Operational procedures and responsibilities .....	19
10.2 Third party service delivery management.....	19
10.3 System planning and acceptance .....	20
10.4 Protection against malicious and mobile code .....	20
10.5 Back-up.....	20
10.6 Network security management.....	21
10.7 Media handling.....	21
10.8 Exchange of information.....	21
10.9 Electronic commerce services .....	22
10.10 Monitoring .....	22
<b>11 Access control .....</b>	<b>23</b>
11.1 Business requirement for access control.....	23
11.2 User access management.....	23
11.3 User responsibilities .....	25
11.4 Network access control .....	25
11.5 Operating system access control .....	26
11.6 Application and information access control.....	27
11.7 Mobile computing and teleworking.....	27

<b>12</b>	<b>Information systems acquisition, development and maintenance .....</b>	<b>28</b>
<b>12.1</b>	<b>Security requirements of information systems.....</b>	<b>28</b>
<b>12.2</b>	<b>Correct processing in applications .....</b>	<b>28</b>
<b>12.3</b>	<b>Cryptographic controls.....</b>	<b>30</b>
<b>12.4</b>	<b>Security of system files .....</b>	<b>31</b>
<b>12.5</b>	<b>Security in development and support processes .....</b>	<b>31</b>
<b>12.6</b>	<b>Technical Vulnerability Management .....</b>	<b>31</b>
<b>13</b>	<b>Information security incident management.....</b>	<b>33</b>
<b>13.1</b>	<b>Reporting information security events and weaknesses.....</b>	<b>33</b>
<b>13.2</b>	<b>Management of information security incidents and improvements .....</b>	<b>34</b>
<b>14</b>	<b>Business continuity management .....</b>	<b>34</b>
<b>14.1</b>	<b>Information security aspects of business continuity management.....</b>	<b>34</b>
<b>15</b>	<b>Compliance .....</b>	<b>36</b>
<b>15.1</b>	<b>Compliance with legal requirements.....</b>	<b>36</b>
<b>15.2</b>	<b>Compliance with security policies and standards, and technical compliance.....</b>	<b>37</b>
<b>15.3</b>	<b>Information systems audit considerations .....</b>	<b>37</b>
<b>Annex A</b>	<b>(informative) Implementation examples.....</b>	<b>38</b>
<b>A.1</b>	<b>General .....</b>	<b>38</b>
<b>A.2</b>	<b>Security of information in web applications and web services (LoT-A-WEB) .....</b>	<b>39</b>
<b>A.2.1</b>	<b>General .....</b>	<b>39</b>
<b>A.2.2</b>	<b>Parameters for the Level of Trust of a web application / web service .....</b>	<b>39</b>
<b>A.2.3</b>	<b>Determination of the web application / the web service (LoT-A-WEB).....</b>	<b>39</b>
<b>A.2.4</b>	<b>Consequences .....</b>	<b>40</b>
<b>A.3</b>	<b>Connections between multiple organisations /external connections (LoT-A-NET) .....</b>	<b>40</b>
<b>A.3.1</b>	<b>Determination of the necessary protection controls .....</b>	<b>40</b>
<b>A.3.2</b>	<b>Effects of the coupling of networks .....</b>	<b>46</b>
<b>A.4</b>	<b>Certificates / Public Key Infrastructure (LoT-A-PKI).....</b>	<b>47</b>
<b>A.4.1</b>	<b>Parameters for the Level of Trust of the certificate management.....</b>	<b>47</b>
<b>A.4.2</b>	<b>Determination of the Level of Trust of the certificate management (LoT-A-PKI) .....</b>	<b>47</b>
<b>A.4.3</b>	<b>Effects: Recognition of Certificates / PK .....</b>	<b>47</b>
<b>A.5</b>	<b>Identity Management (LoT-A-IDM) .....</b>	<b>48</b>
<b>A.5.1</b>	<b>Parameters for the Level of Trust of Identity Management.....</b>	<b>48</b>
<b>A.5.2</b>	<b>Determination of the Level of Trust of the Identity Management (LoT-A-IDM) .....</b>	<b>48</b>
<b>A.5.3</b>	<b>Effects: Recognition of identities .....</b>	<b>49</b>
<b>Annex B</b>	<b>(informative) Level of Trust – Implementation Example.....</b>	<b>50</b>
<b>Bibliography</b>	<b>.....</b>	<b>60</b>

## **Foreword**

This document (EN 16495:2014) 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 July 2014, and conflicting national standards shall be withdrawn at the latest by July 2014.

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

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, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

## 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, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2012, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security controls*

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