SLOVENSKI STANDARD
SIST EN 16495:2014

01-april-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 16495:2014**

ICS:

03.220.50	Zračni transport	Air transport
35.240.60	Uporabniške rešitve IT v transportu in trgovini	IT applications in transport and trade

SIST EN 16495:2014 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 16495

January 2014

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 Zivilluftfahrt

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

Contents

Page

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2012 and the following apply.

3.1
Air Traffic Management
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 Information security management systems in aviation

This European Standard is a guideline for implementing and controlling an information security management system in aviation organisations. It is based on the international standard ISO/IEC 27002 (Code of practice for information security management). Aviation organisations have also to consider the security measures listed in this European Standard in addition to the objectives and measures of ISO/IEC 27002.

Information security management has a high priority in aviation regardless of the respective position of the organisation within the service chain. Without an effective information security management system, the risks in connection with the confidentiality, availability and integrity of the information/data required for service delivery increase critically.

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 focusses 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.

4.3 Assessment of information security risks

4.3.1 Internal information security risk management

To understand its own security position, an organisation will need to have an understanding of the security position of its partners.

Making network connections and exchanging data are based on a trust assessment between the parties involved. The extent to which the network traffic and data needs to be controlled and checked is determined by the degree of trust. This is further explored in 4.5.

To enable a secure external connection and data exchange the organisation shall assess the trust it can place in the connection and in the data being received, and ensure itself that the trust assessment is validated.

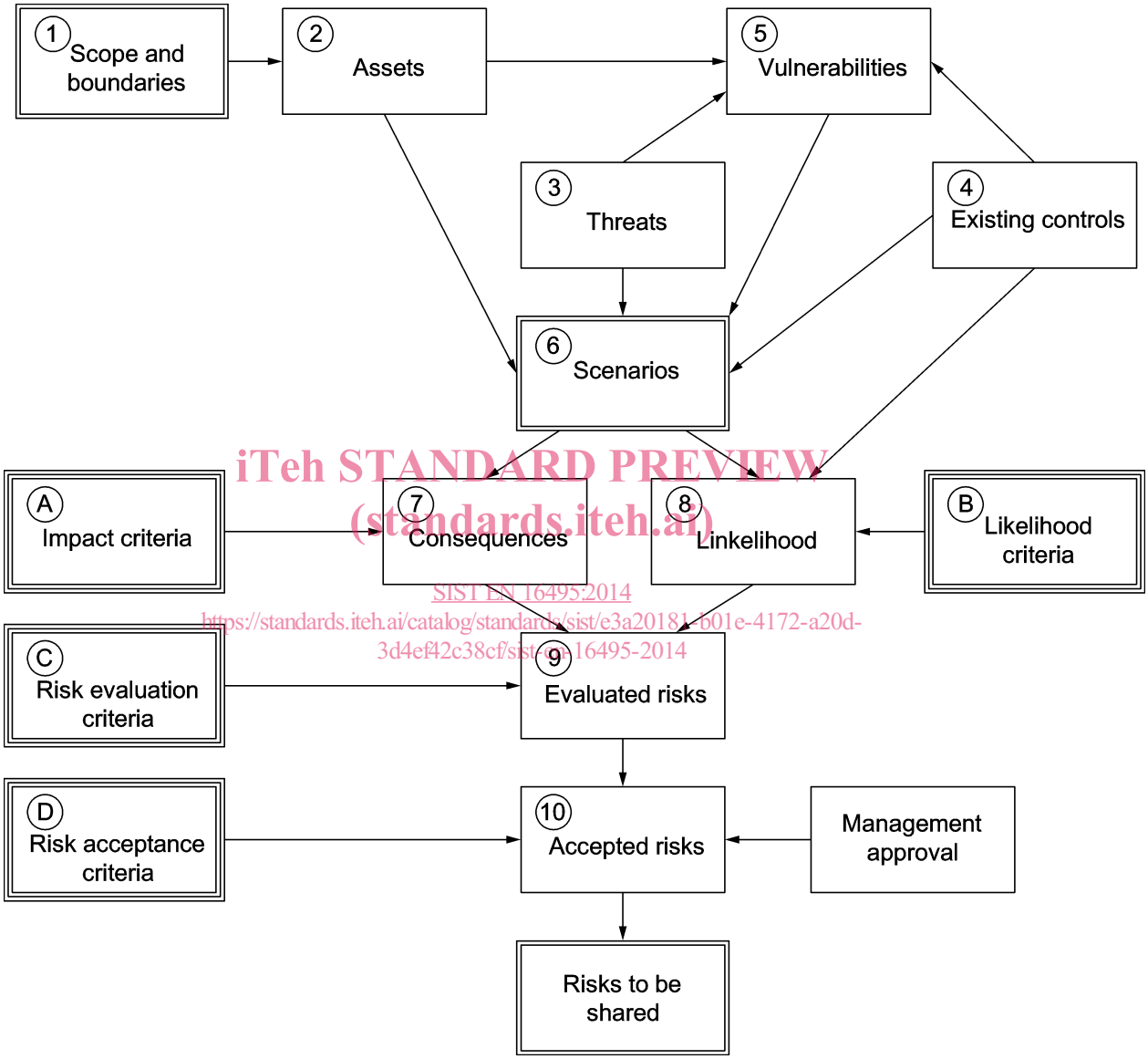
It is important to stress that this does not mean the organisation needs to know everything about its partners' security. What is needed is enough information to provide the required level of assurance, based on risk assessments.

Generic Interconnectivity cases may be constructed and assessed based on a common set of parameters and processes. When these cases apply to concrete interconnectivity cases, additional risk assessments are not necessary. An example of a generic interconnectivity case can be found in Annex A.

Organisations shall share this information to the required level with their partners in civil aviation. This European Standard specifies what information needs to be shared.

The underlying risk assessment process is compatible with ISO/IEC 27005:2011. This applies especially to the terminology used below.

Activities described in subsequent clauses may be conducted in a different order depending on the methodology used.



Key

Boxes with a double line indicate information to be shared as discussed in 4.3.3

Boxes with triple line indicate criteria that have to be established as part of the organisations risk management process. They are then used as fixed inputs to the individual risk assessments

Figure 1

A. Impact criteria

Impact criteria should be developed and specified in terms of the degree of damage or costs to the organisation caused by an information security event.

B. Likelihood evaluation criteria

Likelihood evaluation criteria should be developed that are understood in a similar way by all organisations involved and affected.

C. Risk evaluation criteria

Risk evaluation criteria should be developed for evaluating the organisation's information security risk considering the following:

— the strategic value of the business information process;

— the criticality of the information assets involved;

— legal and regulatory requirements, and contractual obligations;

— operational and business importance of availability, confidentiality and integrity;

— stakeholders' expectations and perceptions, and negative consequences for goodwill and reputation.

D. Risk acceptance criteria

Risk acceptance criteria should be developed and specified.

The **risk assessment process** should include the following steps.

Step 1. Scope and boundaries:

Function: To ensure that all relevant assets are taken into account and to assess risks that might arise through the organisation's boundaries. Additionally, the organisation should provide justification for any exclusion from the scope.

Results: The specification of the assessment scope and boundaries.

Step 2. Assets:

Function: To identify anything that has value to the organisation and which therefore requires protection. An asset shall have a single set of attributes that can be related to threats and vulnerabilities, to allow for analysis in the following steps.

Results: A list of assets to be risk-managed and a list of business processes related to assets and their relevance together with the relevant owners.

Step 3. Threats:

Function: To identify threats which have the potential to harm assets such as information, processes and systems. A threat may arise from within or from outside the organisation.

Results: A list of threats with the identification of threat type and source.

Step 4. Existing controls:

Function: To identify the existing or planned controls to see how they would reduce threat likelihoods and the ease of exploiting vulnerabilities, or the impact of an incident.

Results: A list of all existing and planned controls, their implementation and usage status.

Step 5. Vulnerabilities:

Function: To identify the features inherent to the assets and business processes can be exploited to deliver an attack. Not all vulnerabilities will be known at the time of the assessment (particularly the technical so-called zero-day vulnerabilities). This possibility needs to be addressed in security controls that allow for rapid reassessment of risk when they are discovered.

Results: A list of vulnerabilities in relation to assets, threats and controls.

Step 6. Scenarios:

Function: To identify the effects to the organisation that could be caused by a threat scenario. A threat scenario is the description of a threat exploiting a certain vulnerability or set of vulnerabilities to attack assets, despite existing controls.

Results: A list of threat scenarios with their effects related to the organisation's assets and business processes as well as those of other affected organisations.

Step 7. Consequences (assessment):

Function: To assess the consequences of each scenario, related to asset valuation and based on the business impact criteria.

Results: A list of assessed consequences of an incident scenario expressed with respect to assets and impact criteria.

Step 8. Likelihood:

Function: To assess the likelihood of each scenario occurring.

Results: Likelihood of threat scenarios (quantitative or qualitative).

Step 9. Evaluated Risk:

Function: To turn scenarios into evaluated risks based on the consequences and likelihood and the risk evaluation criteria defined during the context establishment. Aggregation of multiple low or medium risks may result in much higher overall risks and need to be addressed accordingly.

Results: A list of risks ranked according to risk evaluation criteria in relation to the threat scenarios that lead to those risks.

Step 10. Assessed Risk:

Function: To assess the list of ranked risks for acceptability based on the risk acceptance criteria previously defined.

Results: A list of assessed risks with related threat scenarios prioritised according to risk acceptance criteria. This will include information on consequences and likelihood for each risk.

4.3.2 Interoperability issues of risk assessments

Interoperability of risk assessments is an important issue within an environment that can be characterised as “system of systems”. In such an environment, risk assessments covering (sub-parts of) these systems will exist and it is important to identify the correspondences amongst risks identified and mitigation controls proposed in these assessments. This will allow for a coherent security policy for the entire complex system.

In order to achieve interoperability of risk assessments if different risk assessment methodologies are used,

— an understanding about the correspondence between the issues/notions/terms introduced in each of the underlying risk assessment methodologies needs to be established and

— the depth and width of each assessment needs to be compared and assessed in order to understand the assumed environment and the decisions regarding the security level of the system at hand.

Terminology issues might also be relevant, as even if the underlying methods are the same, it might happen that issues/notions/terms are being assigned different semantics.

To ensure comparability across multiple organisations, the organisation shall share at least information on scope and boundaries, threat scenarios and the assessed risks.

Information sharing should be based on the need to know principle to the extent necessary to deal with shared risks. Due to the sensitive nature of the catalogues of assessed risks, these results are usually developed by each organisation internally and are kept internally confidential.

The exchange of the information needs to be backed by appropriately binding confidentiality agreements between the organisations affected.

4.4 Selecting controls

Controls should be selected and implemented in line with the results of the information security risk assessments:

— controls from ISO/IEC 27002;

— controls supplementing those stated in ISO/IEC 27002. These are described in this European Standard as implementation specifications specific to aviation.

4.5 Levels of trust

4.5.1 Introduction

As stated above in 4.2, service delivery in aviation is defined by a high level of cooperation between the organisations involved. Guaranteeing the security of information and the systems that process that information within an individual organisation in a shared business process and the underlying proprietary business processes entails a high level of individual agreements and reviews.

Aviation organisations working in partnership should agree that levels of trust backed by reasonable evidence (from 1:1 relationships between two parties or through third-party verification) be recognised in further shared business processes (including with third parties).

The “Level of Trust of the organisation” (LoT-O) relates to the respective organisation. Classification always relates to the aspect of the shared process handled by the respective organisation. In particular, this takes into account potential information security risks that can arise for the respective party through linking business processes.

In addition to the organisation's overall assessment, a level of trust can also be classified for a specific subarea application area as described in the examples in Annex A.

4.5.2 Scale of trust levels

A six-point scale is used to classify the “Level of Trust”:

— Trusted;

— Limited Trust 0;

— Limited Trust 1;

— Limited Trust 2;

— Limited Trust 3;

— Untrusted.

The general definitions for the different levels should be as follows:

a) Trusted
The “trusted” category is only applied to an organisation's own departments, subsidiaries or business processes that are fully subject to their own security requirements. Third-party organisations cannot be categorised as “trusted”.

b) Limited Trust 0
The “Limited Trust 0” (LT0) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that meet the following requirements:

All the controls of this European Standard have been bindingly implemented. Compliance with the standard has been confirmed by a qualified information security auditor.

NOTE This can be for example a CISA, an ISO/IEC 27001 Lead Auditor or an equivalent professional.

c) Limited Trust 1
The “Limited Trust 1” (LT1) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that have a very high level of information security. This also applies to areas in which there are only indirect risks to partners.

EXAMPLE 1 linking networks

Under specific circumstances, organisations will grant access to their own applications to LT1 partners on a need-to-have basis without implementing application-specific protection measures (e.g. web application firewalls) and without further authentication at edge-of-network (e.g. on the firewall).

This procedure is only appropriate if the partner has a very high security level (LT1) and has implemented all relevant information security management system measures in this context.

d) Limited Trust 2
The “Limited Trust 2” (LT2) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that have a high level of information security.

EXAMPLE 2 linking networks

Under specific circumstances, organisations will grant access to their own applications to LT2 partners on a need-to-have basis, but require explicit authentication at edge-of-network (e.g. on the firewall) before establishing a connection.

This procedure is only appropriate if the partner has a high security level (LT2) and has implemented all key information security management system measures in this context (e.g. security incident management).

e) Limited Trust 3
The “limited trust 3” (LT3) category describes third-party organisations or organisations within the company that are not subject to proprietary security specifications but that have a basic level of information security.

EXAMPLE 3 linking networks

Under specific circumstances, organisations will grant access to their own applications to LT3 partners on a need-to-have basis, but require explicit authentication at edge-of-network (e.g. on the firewall) and other protection measures (e.g.

content filtering, input control, rights management, etc.) before establishing a connection. This procedure is only appropriate if the partner has implemented basic security measures (e.g. virus protection, back-up/restore, etc.) and a security management system.

f) Untrusted
This category describes all organisations that do not meet the requirements of the “Limited Trust 3” category.

4.5.3 Classification criteria

The details of the specific controls to be implemented for the different levels of trust should be worked out by the partners. An example of the Implementation of levels of Trust for an organisation can be found in Annex B.

4.6 Statement of applicability

The organisation should establish a “statement of applicability” in line with ISO/IEC 27001:2013, 4.2.1. j). The “statement of applicability”, should be made known to a partner if necessary.

4.7 Measurement and auditing of security

Measurement of effectiveness of the implemented controls should be carried out considering the guidelines within ISO/IEC 27004:2009.

Internal auditing activities should be carried out taking into account the additional indications presented in the ISO/IEC 27007:2011.

5 Security policy

5.1 Information security policy

Objective: To provide management direction and support for information security.
Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organisation.

5.1.1 Information security policy document

The controls recommended in ISO/IEC 27002:2005, 5.1.1, apply accordingly.

Implementation guidance specific to aviation

The information security policy 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 policy or in a separate document.

5.1.2 Review of the information security policy

The controls (and all subsequent similar sentences) recommended in ISO/IEC 27002:2005, 5.1.2, apply accordingly.

6 Organisational security

6.1 Internal organisation

Objective: To manage information security within the organisation.

A management framework should be established to initiate and control the implementation of information security within the organisation.

Management should approve the information security policy, assign security roles and coordinate and review the implementation of security across the organisation.

If necessary, a source of specialist information security advice should be established and made available within the organisation. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.

6.1.1 Management commitment to information security

The controls recommended in ISO/IEC 27002:2005, 6.1.1, apply accordingly.

6.1.2 Information security co-ordination

The controls recommended in ISO/IEC 27002:2005, 6.1.2, apply accordingly.

6.1.3 Allocation of information security responsibilities

The controls recommended in ISO/IEC 27002:2005, 6.1.3, apply accordingly.

Implementation guidance specific to aviation

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.).

6.1.4 Authorisation process for information processing facilities

The controls recommended in ISO/IEC 27002:2005, 6.1.4, apply accordingly.

6.1.5 Confidentiality agreements

The controls recommended in ISO/IEC 27002:2005, 6.1.5, apply accordingly.

6.1.6 Contact with authorities

The controls recommended in ISO/IEC 27002:2005, 6.1.6, apply accordingly.

Implementation guidance specific to aviation

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.

6.1.7 Contact with special interest groups

The controls recommended in ISO/IEC 27002:2005, 6.1.7, apply accordingly.