

# DIN EN 16495:2014-05 (D/E)

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt; Deutsche und Englische Fassung EN 16495:2014

Air Traffic Management - Information security for organisations supporting civil aviation operations; German and English version EN 16495:2014

---

<b>Inhalt</b>	<b>Seite</b>
<b>Vorwort</b>	<b>4</b>
<b>1 Anwendungsbereich</b>	<b>5</b>
<b>2 Normative Verweisungen</b>	<b>5</b>
<b>3 Begriffe</b>	<b>5</b>
<b>4 Informationssicherheitsmanagement in der Luftfahrt</b>	<b>5</b>
4.1 Aufbau dieser Europäischen Norm	5
4.2 Informationssicherheitsmanagementsysteme in der Luftfahrt	6
4.3 Bewertung von Informationssicherheitsrisiken	6
4.4 Auswahl von Maßnahmen	10
4.5 Vertrauensstufen	10
4.6 Bericht über die Anwendbarkeit	12
4.7 Messung und Auditierung der Sicherheit	12
<b>5 Sicherheitsleitlinie</b>	<b>13</b>
5.1 Informationssicherheitsleitlinie	13
<b>6 Organisation der Informationssicherheit</b>	<b>13</b>
6.1 Interne Organisation	13
6.2 Externe Parteien	15
<b>7 Management organisationseigener Werte (Assets)</b>	<b>15</b>
7.1 Verantwortung für organisationseigene Werte (Assets)	15
7.2 Klassifizierung von Informationen	16
<b>8 Personalsicherheit</b>	<b>17</b>
8.1 Vor der Anstellung	17
8.2 Während der Anstellung	17
8.3 Beendigung oder Änderung der Anstellung	18
<b>9 Physische und umgebungsbezogene Sicherheit</b>	<b>18</b>
9.1 Sicherheitsbereiche	18
9.2 Sicherheit von Betriebsmitteln	19
<b>10 Betriebs- und Kommunikationsmanagement</b>	<b>20</b>
10.1 Betriebliche Verfahren und Verantwortlichkeiten	20
10.2 Management der Dienstleistungserbringung von Dritten	20
10.3 Systemplanung und Abnahme	21
10.4 Schutz vor Schadsoftware und mobilen Programmcodes	21
10.5 Backup	21
10.6 Management der Netzsicherheit	22
10.7 Handhabung von Medien	22
10.8 Austausch von Informationen	22
10.9 Anwendungen im Rahmen des elektronischen Geschäftsverkehrs	23

10.10	Überwachung .....	23
11	Zugangskontrolle .....	24
11.1	Geschäftsanforderungen für Zugangskontrolle .....	24
11.2	Benutzerverwaltung .....	24
11.3	Benutzerverantwortung .....	26
11.4	Zugangskontrolle für Netze .....	26
11.5	Zugriffskontrolle auf Betriebssysteme .....	27
11.6	Zugangskontrolle zu Anwendungen und Informationen .....	28
11.7	Mobile Computing und Telearbeit .....	29
12	Beschaffung, Entwicklung und Wartung von Informationssystemen .....	29
12.1	Sicherheitsanforderungen von Informationssystemen .....	29
12.2	Korrekte Verarbeitung in Anwendungen .....	30
12.3	Kryptografische Maßnahmen .....	31
12.4	Sicherheit von Systemdateien .....	32
12.5	Sicherheit bei Entwicklungs- und Unterstützungsprozessen .....	32
12.6	Umgang mit technischen Schwachstellen .....	33
13	Umgang mit Informationssicherheitsvorfällen .....	34
13.1	Melden von Informationssicherheitsereignissen und Schwachstellen .....	34
13.2	Umgang mit Informationssicherheitsvorfällen und Verbesserungen .....	35
14	Sicherstellung des Geschäftsbetriebs (Business Continuity Management) .....	36
14.1	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management) .....	36
15	Einhaltung von Vorgaben (Compliance) .....	38
15.1	Einhaltung gesetzlicher Anforderungen .....	38
15.2	Einhaltung von Sicherheitsleitlinien und -standards und technischer Vorgaben .....	39
15.3	Überlegungen zu Audits von Informationssystemen .....	39
Anhang A (informativ) Beispiele für die Umsetzung .....		40
A.1	Allgemeines .....	40
A.2	Sicherheit von Informationen in Webanwendungen und Webdiensten (LoT-A-WEB) .....	41
A.2.1	Allgemeines .....	41
A.2.2	Parameter für die Vertrauensstufe einer Webanwendung / eines Webdienstes .....	41
A.2.3	Ermittlung der Vertrauensstufe der Webanwendung / des Webdienstes (LoT-A-WEB) .....	41
A.2.4	Folgen .....	42
A.3	Organisationsübergreifende Verbindungen / externe Verbindungen (LoT-A-NET) .....	43
A.3.1	Ermittlung der notwendigen Schutzmaßnahmen .....	43
A.3.2	Auswirkungen der Kopplung von Netzwerken .....	47
A.4	Zertifikate/Public-Key-Infrastruktur (LoT-A-PKI) .....	47
A.4.1	Parameter für die Vertrauensstufe des Zertifikatsmanagements .....	47
A.4.2	Ermittlung der Vertrauensstufe des Zertifikatsmanagements (LoT-A-PKI) .....	48
A.4.3	Auswirkungen: Anerkennung von Zertifikaten / PKI .....	48
A.5	Identitätsmanagement (LoT-A-IDM) .....	48
A.5.1	Parameter für die Bestimmung der Vertrauensstufe des Identitätsmanagements .....	48
A.5.2	Ermittlung der Vertrauensstufe des Identitätsmanagements (LoT-A-IDM) .....	49
A.5.3	Auswirkungen: Anerkennung von Identitäten .....	49
Anhang B (informativ) Vertrauensstufe - Beispiel für die Umsetzung .....		50
Literaturhinweise .....		59

# Contents

Page

Foreword.....	4
1 Scope .....	5
2 Normative references .....	5
3 Terms and definitions .....	5
4 Information security management in aviation .....	5
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
5 Security policy .....	12
5.1 Information security policy.....	12
6 Organisational security.....	13
6.1 Internal organisation .....	13
6.2 External parties .....	14
7 Asset management.....	15
7.1 Responsibility for assets .....	15
7.2 Information classification .....	15
8 Human resources security.....	16
8.1 Prior to employment.....	16
8.2 During employment .....	17
8.3 Termination or change of employment .....	17
9 Physical and environmental security .....	18
9.1 Secure areas.....	18
9.2 Equipment security.....	18
10 Communications and operations management .....	19
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
11 Access control .....	23
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

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