

DIN EN 16495:2019-11 (D/E)

Flugverkehrsmanagement - Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt; Deutsche Fassung EN 16495:2019

Air Traffic Management - Information security for organisations supporting civil aviation operations; German version EN 16495:2019

Inhalt	Seite
Europäisches Vorwort.....	6
Einleitung	7
1 Anwendungsbereich.....	8
2 Normative Verweisungen	8
3 Begriffe und Abkürzungen	8
3.1 Begriffe	8
3.2 Abkürzungen	9
4 Auf EN ISO/IEC 27001:2017 bezogene luftverkehrsspezifische Anforderungen	10
4.1 Aufbau dieser Europäischen Norm.....	10
4.2 Verfeinerung der Anforderungen nach EN ISO/IEC 27001:2017	10
5 Informationssicherheitsrichtlinien.....	11
5.1 Vorgaben der Leitung für Informationssicherheit	11
5.1.1 Informationssicherheitsrichtlinien.....	11
5.1.2 Überprüfung der Informationssicherheitsrichtlinien.....	11
6 Organisation der Informationssicherheit	11
6.1 Interne Organisation.....	11
6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten.....	11
6.1.2 Aufgabentrennung	11
6.1.3 Kontakt mit Behörden	11
6.1.4 Kontakt mit speziellen Interessensgruppen	11
6.1.5 Informationssicherheit im Projektmanagement.....	12
6.2 Mobilgeräte und Telearbeit	12
7 Personalsicherheit.....	12
7.1 Vor der Beschäftigung.....	12
7.1.1 Sicherheitsüberprüfung.....	12
7.1.2 Beschäftigungs- und Vertragsbedingungen.....	13
7.2 Während der Beschäftigung	13
7.2.1 Verantwortlichkeiten der Leitung.....	13
7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung	13
7.2.3 Maßregelungsprozess.....	13
7.3 Beendigung und Änderung der Beschäftigung	13
8 Verwaltung der Werte	13
8.1 Verantwortlichkeit für Werte	13
8.1.1 Inventarisierung der Werte	13
8.1.2 Zuständigkeit für Werte	13
8.1.3 Zulässiger Gebrauch von Werten	14
8.1.4 Rückgabe von Werten	14
8.2 Informationsklassifizierung	14
8.2.1 Klassifizierung von Informationen.....	14
8.2.2 Kennzeichnung von Information.....	14

8.2.3	Handhabung von Werten.....	15
8.3	Handhabung von Datenträgern.....	15
9	Zugangssteuerung.....	15
9.1	Geschäftsanforderungen an die Zugangsteuerung.....	15
9.2	Benutzerzugangsverwaltung.....	15
9.2.1	Registrierung und Deregistrierung von Benutzern	15
9.2.2	Zuteilung von Benutzerzugängen	15
9.2.3	Verwaltung privilegierter Zugangsrechte.....	15
9.2.4	Verwaltung geheimer Authentisierungsinformation von Benutzern	15
9.2.5	Überprüfung von Benutzerzugangsrechten	15
9.2.6	Entzug oder Anpassung von Zugangsrechten	15
9.2.7	Digitales Identitätsmanagement.....	16
9.2.8	Organisationsübergreifende eindeutige Darstellung von Entitäten	16
9.3	Benutzerverantwortlichkeiten.....	17
9.4	Zugangssteuerung für Systeme und Anwendungen.....	17
9.4.1	Informationszugangsbeschränkung	17
9.4.2	Sichere Anmeldeverfahren	17
9.4.3	System zur Verwaltung von Kennwörtern.....	17
9.4.4	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	17
9.4.5	Zugangssteuerung für Quellcode von Programmen	17
9.4.6	Web Application Firewalls	17
10	Kryptographie	18
10.1	Kryptographische Maßnahmen.....	18
10.1.1	Richtlinie zum Gebrauch von kryptographischen Maßnahmen	18
10.1.2	Schlüsselverwaltung	18
11	Physische und umgebungsbezogene Sicherheit.....	19
11.1	Sicherheitsbereiche.....	19
11.1.1	Physische Sicherheitsperimeter	19
11.1.2	Physische Zutrittssteuerung.....	19
11.1.3	Sichern von Büros, Räumen und Einrichtungen	19
11.1.4	Schutz vor externen und umweltbedingten Bedrohungen.....	19
11.1.5	Arbeiten in Sicherheitsbereichen	19
11.1.6	Anlieferungs- und Ladebereiche	19
11.2	Geräte und Betriebsmittel.....	19
11.2.1	Platzierung und Schutz von Geräten und Betriebsmitteln	19
11.2.2	Versorgungseinrichtungen	19
11.2.3	Sicherheit der Verkabelung.....	20
11.2.4	Instandhaltung von Geräten und Betriebsmitteln	20
11.2.5	Entfernen von Werten	20
11.2.6	Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten	20
11.2.7	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	20
11.2.8	Unbeaufsichtigte Benutzergeräte	20
11.2.9	Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren	20
12	Betriebssicherheit	20
12.1	Betriebsabläufe und -verantwortlichkeiten.....	20
12.2	Schutz vor Schadsoftware.....	20
12.3	Sicherung von Information	20
12.4	Protokollierung und Überwachung.....	21
12.4.1	Ereignisprotokollierung	21
12.4.2	Schutz von Protokollinformationen.....	21
12.4.3	Administratoren- und Bedienerprotokolle	21
12.4.4	Uhrensynchronisation.....	21
12.5	Steuerung von Software im Betrieb	21
12.6	Handhabung technischer Schwachstellen.....	21
12.7	Audits von Informationssystemen.....	21

13	Kommunikationssicherheit	21
13.1	Netzwerksicherheitsmanagement	21
13.1.1	Netzwerksteuerungsmaßnahmen	21
13.1.2	Sicherheit von Netzwerkdiensten	22
13.1.3	Trennung in Netzwerken	22
13.2	Informationsübertragung	22
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	22
14.1	Sicherheitsanforderungen an Informationssysteme	22
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	22
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	22
14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	22
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	22
14.2.1	Richtlinie für sichere Entwicklung	22
14.2.2	Verfahren zur Verwaltung von Systemänderungen	23
14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	23
14.2.4	Beschränkung von Änderungen an Softwarepaketen	23
14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	23
14.2.6	Sichere Entwicklungsumgebung	23
14.2.7	Ausgliederte Entwicklung	23
14.2.8	Testen der Systemsicherheit	23
14.2.9	Systemabnahmetest	23
14.3	Testdaten	23
15	Lieferantenbeziehungen	24
15.1	Informationssicherheit in Lieferantenbeziehungen	24
15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen	24
15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen	24
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie	24
15.2	Steuerung der Dienstleistungserbringung von Lieferanten	24
16	Handhabung von Informationssicherheitsvorfällen	24
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	24
16.1.1	Verantwortlichkeiten und Verfahren	24
16.1.2	Meldung von Informationssicherheitsereignissen	24
16.1.3	Meldung von Schwächen in der Informationssicherheit	25
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	25
16.1.5	Reaktion auf Informationssicherheitsvorfälle	25
16.1.6	Erkenntnisse aus Informationssicherheitsvorfällen	25
16.1.7	Sammeln von Beweismaterial	25
17	Informationssicherheitsaspekte beim Business Continuity Management	26
17.1	Aufrechterhalten der Informationssicherheit	26
17.1.1	Planung zur Aufrechterhaltung der Informationssicherheit	26
17.1.2	Umsetzung der Aufrechterhaltung der Informationssicherheit	26
17.1.3	Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit	26
17.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs	27
17.2	Redundanzen	27
18	Compliance	27
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen	27
18.1.1	Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen	27
18.1.2	Geistige Eigentumsrechte	27
18.1.3	Schutz von Aufzeichnungen	28
18.1.4	Privatsphäre und Schutz von personenbezogener Information	28
18.1.5	Regelungen bezüglich kryptographischer Maßnahmen	28
18.2	Überprüfungen der Informationssicherheit	28
18.2.1	Unabhängige Überprüfung der Informationssicherheit	28
18.2.2	Einhaltung von Sicherheitsrichtlinien und -standards	28
18.2.3	Überprüfung der Einhaltung von technischen Vorgaben	28

Anhang A (informativ) Zusätzliche, auf das Flugverkehrsmanagement bezogene Anleitung	29
A.1 Bewertung von Informationssicherheitsrisiken.....	29
A.1.1 Internes Management der Informationssicherheit.....	29
A.2 Probleme der Interoperabilität von Risikobewertungen.....	33
A.2.1 Allgemeines.....	33
A.2.2 Management der Informationssicherheit für mehrere Organisationen.....	33
A.2.3 Anpassung des Sicherheits- und Sicherheitsrisikomanagements.....	33
A.3 Bestimmung von Maßnahmen.....	34
A.4 Vertrauensstufen.....	34
A.4.1 Einleitung.....	34
A.4.2 Skala der Vertrauensstufen.....	34
A.4.3 Klassifizierungskriterien.....	36
A.5 Bericht über die Anwendbarkeit.....	36
A.6 Messung und Auditierung der Sicherheit.....	36
Anhang B (informativ) Beispiele für die Umsetzung	37
B.1 Allgemeines.....	37
B.2 Sicherheit von Informationen in Webanwendungen und Webdiensten (LoT-A-WEB).....	39
B.2.1 Allgemeines.....	39
B.2.2 Parameter für die Vertrauensstufe einer Webanwendung/eines Webdienstes.....	39
B.2.3 Ermittlung der Vertrauensstufe der Webanwendung/des Webdienstes (LoT-A-WEB).....	39
B.2.4 Folgen.....	40
B.3 Organisationsübergreifende Verbindungen/externe Verbindungen (LoT-A-NET).....	40
B.3.1 Ermittlung der notwendigen Schutzmaßnahmen.....	41
B.3.2 Auswirkungen der Kopplung von Netzwerken.....	46
B.4 Zertifikate/Public-Key-Infrastruktur (LoT-A-PKI).....	47
B.4.1 Parameter für die Vertrauensstufe des Zertifikatsmanagements.....	47
B.4.2 Ermittlung der Vertrauensstufe des Zertifikatsmanagements (LoT-A-PKI).....	47
B.4.3 Auswirkungen: Anerkennung von Zertifikaten/PKI.....	48
B.5 Identitätsmanagement (LoT-A-IDM).....	48
B.5.1 Parameter für die Bestimmung der Vertrauensstufe des Identitätsmanagements.....	48
B.5.2 Ermittlung der Vertrauensstufe des Identitätsmanagements (LoT-A-IDM).....	49
B.5.3 Auswirkungen: Anerkennung von Identitäten.....	49
Anhang C (informativ) Vertrauensstufe — Beispiel für die Umsetzung	51
Anhang D (informativ) Anwendung von Maßnahmen in einer Kontrollübersicht — Beispiel für die Umsetzung	67
Anhang E (informativ) Leitlinien für organisationsübergreifende Aspekte in der Luftfahrt	72
Literaturhinweise	74

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

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

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

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

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