

# 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

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

<b>Anhang A (informativ) Zusätzliche, auf das Flugverkehrsmanagement bezogene Anleitung</b> .....	<b>29</b>
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
<b>Anhang B (informativ) Beispiele für die Umsetzung</b> .....	<b>37</b>
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
<b>Anhang C (informativ) Vertrauensstufe — Beispiel für die Umsetzung</b> .....	<b>51</b>
<b>Anhang D (informativ) Anwendung von Maßnahmen in einer Kontrollübersicht — Beispiel für die Umsetzung</b> .....	<b>67</b>
<b>Anhang E (informativ) Leitlinien für organisationsübergreifende Aspekte in der Luftfahrt</b> .....	<b>72</b>
<b>Literaturhinweise</b> .....	<b>74</b>

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

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
<b>Annex A (informative) Additional guidance related to air traffic management.....</b>		<b>26</b>
A.1	Assessment of information security risks .....	26
A.1.1	Internal information security risk management.....	26
<b>Figure A.1 —Assessment of information security risks.....</b>		<b>27</b>
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
<b>Annex B (informative) Implementation examples .....</b>		<b>33</b>
B.1	General .....	33
<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.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
<b>Table B.2 —Level of Trust of the web application/the web service.....</b>		<b>35</b>
B.2.4	Consequences.....	35
<b>Table B.3 —Evaluation Criteria for LoT-A-WEB .....</b>		<b>35</b>
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
<b>Figure B.2 —Process for implementation of external connection protection.....</b>		<b>36</b>
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

<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>