

DIN EN 16495

ICS 03.100.70; 03.220.50; 35.240.60

Ersatz für
DIN EN 16495:2014-05**Flugverkehrsmanagement –
Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt;
Deutsche und Englische Fassung EN 16495:2019**

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

Gestion du trafic aérien –
Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation
civile;
Version allemande et anglaise EN 16495:2019

Gesamtumfang 145 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (EN 16495:2019) wurde vom Technischen Komitee CEN/TC 377 „Flugverkehrsmanagement“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 131-05-02 AA „Flugverkehrsmanagement (ATM)“ im DIN-Normenausschuss Luft- und Raumfahrt (NL).

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

IEC 62443	siehe	DIN EN IEC 62443-4-1
ISO/IEC 15408 (alle Teile)	siehe	DIN EN ISO/IEC 15408 (alle Teile)
ISO/IEC 27009:2016	siehe	DIN ISO/IEC 27009:2016-11
ISO 28000:2007	siehe	DIN ISO 28000:2015-08

Änderungen

Gegenüber DIN EN 16495:2014-05 wurden folgende Änderungen vorgenommen:

- a) Anpassung an die Strukturen von ISO/IEC 27002:2013 und ISO/IEC DIS 27009:2015;
- b) Informationen zur Ausrichtung des Schutz- und Sicherheitsmanagements wurden aufgenommen;
- c) Informationen zur entwicklungs-, produktions- und instandhaltungsspezifischen Informationssicherheit wurden aufgenommen;
- d) Informationen zur Wahrung der Informationssicherheit wurden aufgenommen;
- e) informativer Anhang D mit einem Umsetzungsbeispiel für Anwendung von Maßnahmen bei der behördlichen Aufsicht wurde aufgenommen;
- f) informativer Anhang E mit Leitlinien für organisationsübergreifende Aspekte in der Luftfahrt wurde aufgenommen.

Frühere Ausgaben

DIN EN 16495: 2014-05

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN IEC 62443-4-1, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung*

DIN EN ISO/IEC 15408 (alle Teile), *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit*

DIN ISO/IEC 27009:2016-11, *Informationstechnik — IT-Sicherheitsverfahren — Sektorspezifische Anwendung der ISO/IEC 27001 — Anforderungen (ISO/IEC 27009:2016)*

DIN ISO 28000:2015-08, *Spezifikation für Sicherheitsmanagementsysteme für die Lieferkette (ISO 28000:2007)*

— Leerseite —

Deutsche Fassung

Flugverkehrsmanagement — Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

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

Diese Europäische Norm wurde vom CEN am 12. Mai 2019 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Rue de la Science 23, B-1040 Brüssel

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	Ausgegliederte 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

Europäisches Vorwort

Dieses Dokument (EN 16495:2019) wurde vom Technischen Komitee CEN/TC 377 „Flugverkehrsmanagement“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Januar 2020, und etwaige entgegenstehende nationale Normen müssen bis Januar 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Dieses Dokument ersetzt EN 16495:2014.

Im Vergleich zur Vorgängerausgabe wurden folgende technische Änderungen vorgenommen:

- Angleichung an den Aufbau von EN ISO/IEC 27002:2017 und ISO/IEC 27009:2016;
- Leitlinien für die Anpassung des Sicherheitsmanagements;
- Leitlinien für die auf die Entwicklung, Produktion und Wartung bezogene Informationssicherheit;
- Leitlinien für die Wahrung der Informationssicherheit;
- informativer Anhang D „Anwendung von Maßnahmen in einer Kontrollübersicht — Beispiel für die Umsetzung“;
- informativer Anhang E „Leitlinien für organisationsübergreifende Aspekte in der Luftfahrt“.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Dieses Dokument enthält auf EN ISO/IEC 27002:2017 „Leitfaden für Informationssicherheitsmaßnahmen“ basierende Leitlinien, die auf Sicherheitsmanagementsysteme in Organisationen im Luftverkehrsbereich angewendet werden. Das Ziel dieses Dokuments besteht in der Erweiterung der Inhalte von EN ISO/IEC 27002:2017 auf den Bereich des Luftverkehrsmanagements, um damit Luftfahrtorganisationen zu ermöglichen, ein genormtes und spezielles Informationssicherheitsmanagementsystem (ISMS) umzusetzen, das den organisationsübergreifenden Aspekten des Luftverkehrsmanagements nach EN ISO/IEC 27001:2017 entspricht.

Zusätzlich zu den in EN ISO/IEC 27001:2017 aufgeführten Sicherheitszielen und -maßnahmen unterliegen Luftverkehrsorganisationen weiteren speziellen Anforderungen: Die Erbringung von Dienstleistungen in der Luftfahrt ist in hohem Maße von der Zusammenarbeit der einzelnen Beteiligten bestimmt. Das Informations-sicherheitsmanagement einer Organisation hängt daher vom Informationssicherheitsmanagement derjenigen Organisationen ab, mit denen die betreffende Organisation zur Erbringung von Dienstleistungen zusammenarbeitet. Dieses Dokument konzentriert sich daher auf die Aspekte der Zusammenarbeit.

Diese Zusammenarbeit erfordert:

- die gemeinsame Nutzung der Ergebnisse von Risikobeurteilungen in der gesamten Geschäftsprozesskette;
- die Übereinstimmung hinsichtlich des erforderlichen Maßes an Vertrauen; die Übereinstimmung hinsichtlich der erforderlichen Sicherheitskontrollen und ihrer Umsetzung.

1 Anwendungsbereich

Dieses Dokument enthält auf EN ISO/IEC 27002:2017 beruhende Leitlinien, die auf die Zivilluftfahrt unterstützende Organisationen angewendet werden, mit dem Schwerpunkt auf Betriebsabläufen im Luftverkehrsmanagement.

Das betrifft Luftraumnutzer, Flughäfen und Flugsicherungsorganisationen, ist jedoch nicht allein darauf beschränkt.

Nicht in den Anwendungsbereich fallen Handlungen der Organisationen, die sich nicht auf die Sicherheit von Tätigkeiten im Bereich der Zivilluftfahrt auswirken, wie z. B. Einzelhandels- und Dienstleistungsunternehmen an Flughäfen und das Management von Unternehmensimmobilien (en: corporate real estate management).

Grundlage für alle Leitlinien in diesem Dokument sind das Vertrauen und die Zusammenarbeit zwischen den Parteien, die am Flugverkehrsmanagement beteiligt sind.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

EN ISO/IEC 27001:2017, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

EN ISO/IEC 27002:2017, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen*

3 Begriffe und Abkürzungen

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000:2018 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1.1

Flugverkehrsmanagement

funktionales System, bestehend aus einer Zusammenfassung der bordseitigen und bodenseitigen Funktionen (Flugverkehrsdienste, Luftraummanagement und Verkehrsflussregelung), die für die sichere und effiziente Bewegung von Luftfahrzeugen in allen Betriebsphasen erforderlich sind und die Verantwortlichkeiten aller Partner in der Wertschöpfungskette des Luftverkehrs erfassen

3.1.2

Vertrauen

Situation, in der eine Partei bereit dazu ist, sich auf die Handlungen einer anderen Partei zu verlassen

Anmerkung 1 zum Begriff: Vertrauen ist mehr als das, was mittels Versicherung erreicht werden kann. Versicherung stellt jedoch ein unterstützendes Instrument für die Vertrauensbildung dar.

3.1.3

organisationsübergreifender Prozess

Prozess zwischen verschiedenen Organisationen, die untereinander als interessierte Parteien auftreten

3.1.4

funktionales System

Kombination von Systemen, Verfahren und Personal mit dem Ziel, eine Funktion im Bereich des Flugverkehrsmanagements zu erfüllen

[Quelle: VERORDNUNG (EG) DER KOMMISSION Nr. 2096/2005, Artikel 2]

3.2 Abkürzungen

API	Anwendungsprogrammierschnittstelle (en: Application Programming Interface)
ATM	Flugverkehrsmanagement (en: Air Traffic Management)
CA	Zertifizierungsstelle (en: Certification Authority)
Abschn.	Abschnitt
CP	Zertifizierungsrichtlinie (en: Certificate Policy)
CPS	Erklärung zum Zertifizierungsbetrieb (en: Certificate Practice Statement)
CS	Zertifikatsleistung (en: Certificate Service)
cts	Client-to-Site VPN
DIM	Digitales Identitätsmanagement (en: Digital Identity Management)
HTTP	Hypertext-Übertragungsprotokoll (en: HyperText Transfer Protocol)
HTTPS	Sicheres Hypertext-Übertragungsprotokoll (en: HyperText Transfer Protocol Secure)
ICAO	Internationale Zivilluftfahrtorganisation (en: International Civil Aviation Authority)
IDM	Identitätsmanagement (en: Identity Management)
ISDN	Diensteintegrierendes Digitalnetz (en: Integrated Services Digital Network)
ITU	Internationale Fernmeldeunion (en: International Telecommunication Union)
LDAP	Leichtes Verzeichniszugriffsprotokoll (en: Lightweight Directory Access Protocol)
LoT-A	Vertrauensniveau für den Anwendungsbereich (en: Level of Trust for the Application Area)
LoT-O	Vertrauensniveau des Unternehmens (en: Level of Trust of the Organization)

PKI	Infrastruktur mit öffentlichem Schlüssel (en: Public Key Infrastructure)
PPr	Partnernetz, geschützt (en: Partner network, protected)
PPu	Partnernetz, öffentlich (en: Partner network, public)
PSTN	öffentliches Wählnetz (en: Public Switched Telephone Network)
PuP	öffentlich, ungeschützt (en: Public, unprotected)
PuP	öffentlich, geschützt (en: Public, protected)
SQL	Strukturierte Abfrage-Sprache (en: Structured Query Language)
sts	Site-to-Site VPN
u	unverschlüsselt
v	verschlüsselt
XSS	Webseitenübergreifendes Skripting (en: Cross-Site Scripting)

4 Auf EN ISO/IEC 27001:2017 bezogene luftverkehrsspezifische Anforderungen

4.1 Aufbau dieser Europäischen Norm

Der Aufbau dieser Europäischen Norm ist an EN ISO/IEC 27009 angepasst.

Leitlinien zu zusätzlichen auf die Luftfahrt bezogenen Maßnahmen und Konzepten in Bezug auf die globalen Public-Key-Infrastrukturen sind in Anhang E enthalten.

4.2 Verfeinerung der Anforderungen nach EN ISO/IEC 27001:2017

Alle Anforderungen nach EN ISO/IEC 27001:2017, die nachstehend nicht aufgeführt werden, gelten unverändert; EN ISO/IEC 27001:2017, 6.1.3 c) wird wie folgt verfeinert:

Die nach 6.1.3 b) festgelegten Maßnahmen sind mit den Maßnahmen in EN ISO/IEC 27001:2017, Anhang A, und mit Anhang A in diesem Dokument zu vergleichen, um zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden.

EN ISO/IEC 27001:2017, 6.1.3 d) wird wie folgt verfeinert.

Es ist eine Erklärung zur Anwendbarkeit zu erstellen, die Folgendes enthält:

- die erforderlichen Maßnahmen [siehe EN ISO/IEC 27001:2017, 6.1.3 b) und c)];
- Gründe für deren Einbeziehung;
- ob die erforderlichen Maßnahmen umgesetzt sind oder nicht; sowie
- Gründe für die Nichteinbeziehung von Maßnahmen aus EN ISO/IEC 27001:2017, Anhang A, oder Anhang A in diesem Dokument.

ANMERKUNG Diese Verfeinerungen sind aufgrund der Einführung neuer sektorspezifischer Maßnahmen in diesem Dokument erforderlich.

5 Informationssicherheitsrichtlinien

5.1 Vorgaben der Leitung für Informationssicherheit

5.1.1 Informationssicherheitsrichtlinien

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 5.1.1

Die Informationssicherheitsleitlinien sollten mit den vielfältigen Sicherheitsanforderungen in anderen Bereichen des Luftverkehrs (z. B. physische Absicherung von Sicherheitsbereichen) abgestimmt werden. Die Abgrenzungen und gegenseitigen Abhängigkeiten zwischen den einzelnen Bereichen sollten in den Leitlinien oder gesonderten Dokumenten dokumentiert werden.

5.1.2 Überprüfung der Informationssicherheitsrichtlinien

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 5.1.2.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 6.1.1

Die Organisation sollte einen Verantwortlichen benennen, der Dritten als Ansprechpartner für strategische Fragen zur Informationssicherheit zur Verfügung steht (z. B. für die Planung und Umsetzung gemeinsamer Maßnahmen usw.).

6.1.2 Aufgabentrennung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 6.1.2.

6.1.3 Kontakt mit Behörden

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 6.1.3

Die Organisation sollte mit den entsprechenden Fach- und Aufsichtsbehörden, insbesondere in den Bereichen IT-Sicherheit und Strafverfolgung, und anderen kritischen Infrastrukturen zusammenarbeiten.

Das umfasst Kontakte zu Behörden, die sich auf nationaler und europäischer Ebene mit dem Schutz kritischer Infrastrukturen beschäftigen.

6.1.4 Kontakt mit speziellen Interessensgruppen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 6.1.4

Die Organisation sollte eine Schnittstelle zu anderen Organisationen herstellen.

Die Kontakte sollten auch die Erfordernisse und Erwartungen interessierter Parteien, insbesondere Organisationen, mit denen die Organisation Informationssicherheitsrisiken in Bezug auf die Schaffung von oder den Beitrag zu Sicherheitsrisiken im Luftverkehr und deren Management teilt, berücksichtigen.

Die Schaffung von formellen Schnittstellen zu kritischen Organisationen sollte in Betracht gezogen werden.

Die Organisation sollte sich außerdem der Kritikalität ihrer Dienstleistungen auf regionaler, nationaler und internationaler Ebene bewusst sein. Sie darf sich deshalb in Verbänden und Zusammenschlüssen engagieren und sich an nationalen und internationalen Programmen beteiligen, um die Sicherheit im Luftverkehr umfassend zu unterstützen.

Aufgrund der besonderen Art der Bedrohungen für den Luftverkehr kann es für die Organisation notwendig sein, mit anderen Luftverkehrsorganisationen zusammenzuarbeiten, um nach außen eine einmütige Position zu vertreten. Ein solcher gemeinsamer Auftritt sollte die Grundlage für die Auswahl angemessener Schutzmaßnahmen und reaktiver Maßnahmen sein:

- Sicherstellung der Interoperabilität der ausgewählten Maßnahmen;
- Unterstützung der Zusammenarbeit bei der Alarmierung bei auftretenden IT-Krisen, die mehrere Organisationen betreffen, sowie bei der Krisen-Bewältigung;
- auf der Grundlage gemeinsam gezogener Lehren aus bereits aufgetretenen Sicherheitsvorfällen.

6.1.5 Informationssicherheit im Projektmanagement

Die in EN ISO/IEC 27002:2017, 6.1.5, empfohlenen Maßnahmen gelten entsprechend.

6.2 Mobilgeräte und Telearbeit

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 6.2.

7 Personalsicherheit

7.1 Vor der Beschäftigung

7.1.1 Sicherheitsüberprüfung

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 7.1.1

Die Auflistung hinsichtlich der Überprüfung wird durch einen Punkt geändert:

- f) Überprüfungen von sozialen Netzwerken (Social Media) sollten als ein zusätzliches Mittel zur Sicherheitsüberprüfung angesehen werden.

Die folgenden Abschnitte werden geändert:

Im Falle mehrerer Partnerorganisationen sollte sichergestellt sein, dass von Partnerorganisationen Hintergrundüberprüfungen auf einem angemessenen Niveau durchgeführt werden, um sicherzustellen, dass der Zugriff auf Daten/Informationen, die von den Partnerorganisationen gemeinsam genutzt werden, die nationalen und geschäftlichen Interessen aller Beteiligten berücksichtigt. In der Luftfahrt umfasst der Zugang zu informationsverarbeitenden Einrichtungen die Entwicklung, den Betrieb und die Aufrechterhaltung von Luftfahrtinformationssystemen.

Für Personen, die die Entwicklung, den Betrieb oder die Aufrechterhaltung eines sicherheitskritischen Systems beeinflussen können, sollte die Organisation auch weitere, detailliertere Überprüfungen in Betracht ziehen.

7.1.2 Beschäftigungs- und Vertragsbedingungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 7.1.2.

7.2 Während der Beschäftigung

7.2.1 Verantwortlichkeiten der Leitung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 7.2.1.

7.2.2 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 7.2.2

Die Herausbildung des Bewusstseins der Angestellten, ihre Ausbildung und Schulung sollte insbesondere in Übereinstimmung mit den maßgeblichen Sicherheitsfestlegungen der Abkommensanhänge und anderer Dokumente der Internationalen Zivilluftfahrtorganisation (ICAO) erfolgen.

Die Organisation sollte sicherstellen, dass Anwendungsentwickler über Fähigkeiten verfügen, die es ihnen ermöglichen, sichere Anwendungen umzusetzen.

7.2.3 Maßregelungsprozess

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 7.2.3.

7.3 Beendigung und Änderung der Beschäftigung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 7.3.

8 Verwaltung der Werte

8.1 Verantwortlichkeit für Werte

8.1.1 Inventarisierung der Werte

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 8.1.1

Die Inventarisierung der Werte sollte an Inventarisierungen angeglichen werden, die Konfigurationsinformationen für alle informationsverarbeitenden Werte bereitstellen, einschließlich Software-Patching-Ebenen.

8.1.2 Zuständigkeit für Werte

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 8.1.2

Wenn Werte in Geschäftsprozessen verwendet werden, an denen mehrere Organisationen beteiligt sind, sollten die Interessen der anderen Organisationen von den Eigentümern der Werte berücksichtigt werden.

8.1.3 Zulässiger Gebrauch von Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 8.1.3.

8.1.4 Rückgabe von Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 8.1.4.

8.2 Informationsklassifizierung

8.2.1 Klassifizierung von Informationen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 8.2.1

Um eine organisationsübergreifende Vergleichbarkeit sicherzustellen, sollte die Organisation Informationen, die in übergreifenden Geschäftsprozessen genutzt werden, so klassifizieren, dass diese Klassifizierung für alle am Geschäftsprozess beteiligten Partner annehmbar ist und sie dieser Klassifizierung zustimmen. Derartige Informationen sollten klassifiziert werden, um sicherzustellen, dass nationale und geschäftliche Interessen in angemessener Weise geschützt werden.

Vertraulichkeitsklassen:

Die Zuordnung von Informationen zu einer Vertraulichkeitsklasse sollte auf der Grundlage des zu erwartenden Schadens für den Geschäftsprozess, falls die Information Unberechtigten zur Kenntnis gelangt, erfolgen.

Öffentlich:	Informationen, deren Bekanntwerden keinen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen
Intern:	Informationen, deren Bekanntwerden einen geringen bis mittleren Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen
Vertraulich:	Informationen, deren Bekanntwerden einen großen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen kann
Streng vertraulich:	Informationen, deren Bekanntwerden einen erheblichen bis existenziellen Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich ziehen kann

Allgemein sollte die gemeinsame Nutzung von Informationen nach dem „Need-to-know-Prinzip“ erfolgen.

Weitere luftverkehrsspezifische Informationen

Geschäftliche Bedürfnisse und die geschäftlichen Auswirkungen in Zusammenhang mit diesen Bedürfnissen können das öffentliche Interesse an einer sicheren und schnellen Erbringung der Dienstleistung einschließen wie auch geschäftliche Interessen von einzelnen Beteiligten.

8.2.2 Kennzeichnung von Information

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 8.2.2.

8.2.3 Handhabung von Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 8.2.3.

8.3 Handhabung von Datenträgern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 8.3.

9 Zugangssteuerung

9.1 Geschäftsanforderungen an die Zugangsteuerung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.1.

9.2 Benutzerzugangsverwaltung

9.2.1 Registrierung und Deregistrierung von Benutzern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.2.1.

9.2.2 Zuteilung von Benutzerzugängen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.2.2.

9.2.3 Verwaltung privilegierter Zugangsrechte

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.2.3.

9.2.4 Verwaltung geheimer Authentisierungsinformation von Benutzern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.2.4.

9.2.5 Überprüfung von Benutzerzugangsrechten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.2.5.

9.2.6 Entzug oder Anpassung von Zugangsrechten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.2.6.

9.2.7 Digitales Identitätsmanagement

Zusätzliche Maßnahme für EN ISO/IEC 27002:2017, 9.2

Steuerungsmaßnahme

Zur Verwaltung digitaler Identitäten, ihrer Authentisierung, Autorisierung, Rollen und Rechte sollte die Organisation ein zentrales Identitätsmanagementsystem betreiben. Die Gültigkeit einer Identität sollte nachvollziehbar in Bezug auf das Quellsystem der Identität vorgegeben sein.

Anleitung für die Umsetzung

Quellendatenbanken (z. B. LDAP-Verzeichnisse, Active Directory, dezentrale Datenbanken wie SAP usw.) des Identitätsmanagementsystems sollten eine eindeutige Beziehung zwischen einer Identität und einer Entität des zentralen Identitätsmanagementsystems herstellen.

Die folgenden Hauptprozesse zur Verwaltung digitaler Identitäten sollten umgesetzt werden:

- Erzeugung digitaler Identitäten;
- Änderung (Anpassung, Erweiterung, Löschung) von Merkmalen einer digitalen Identität;
- Deaktivierung/Löschung digitaler Identitäten;
- systematische Bereitstellung digitaler Identitätsinformationen (einschließlich Authentisierungsdaten) für angeschlossene Systeme;
- Verarbeitung von Informationen (aus der Personalverwaltung und dem Organisationsmanagement) zur automatisierten Verwaltung von Benutzergruppen, Rollen und Rechten (Autorisierungsprofile);
- systematische Bereitstellung von Benutzergruppen, Rollen und Rechten in angeschlossenen Systemen.

Jeder der vorgenannten Prozesse im Zusammenhang mit dem digitalen Identitätsmanagement sollte dokumentiert werden und rückverfolgbar sein.

Die Gültigkeit sollte durch ein angeschlossenes Personalmanagementsystem oder über ein verbundenes Unternehmensverzeichnis umgesetzt werden.

Sofern manuelle Prozesse angewendet werden, sollte die Gültigkeitsdauer ein Jahr nicht überschreiten. Die Festlegung einer neuen Gültigkeitsdauer sollte einmal jährlich durch eine Überprüfung erfolgen.

9.2.8 Organisationsübergreifende eindeutige Darstellung von Entitäten

Zusätzliche Maßnahme für EN ISO/IEC 27002:2017, 9.2

Steuerungsmaßnahme

Im organisationsübergreifenden Identitätsmanagement sollten die Entitäten einheitlich dargestellt werden.

Anleitung für die Umsetzung

Im organisationsübergreifenden Identitätsmanagement sollten folgende Entitäten berücksichtigt werden:

- Personen;
- Organisationseinheiten (z. B. Abteilungen) und organisatorische Rollen;

— Systeme.

Jede Entität der Organisation sollte im zentralen Identitätsmanagementsystem durch eine eindeutige digitale Identität dargestellt werden.

Weitere Informationen

Ein einheitliches System zur organisationsübergreifenden Darstellung von Entitäten stellt die Kompatibilität und Interoperabilität im Identitätsmanagement sicher.

9.3 Benutzerverantwortlichkeiten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.3.

9.4 Zugangssteuerung für Systeme und Anwendungen

9.4.1 Informationszugangsbeschränkung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.4.1.

9.4.2 Sichere Anmeldeverfahren

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.4.2.

9.4.3 System zur Verwaltung von Kennwörtern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.4.3.

9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.4.4.

9.4.5 Zugangssteuerung für Quellcode von Programmen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 9.4.5.

9.4.6 Web Application Firewalls

Zusätzliche Maßnahme für EN ISO/IEC 27002:2017, 9.4

Diese zusätzliche Maßnahme bildet keinen Bestandteil der Norm EN ISO/IEC 27002:2017.

Maßnahme

Die Organisation sollte zum Schutz von Webanwendungen Web Application Firewalls einsetzen.

Anleitung für die Umsetzung

Um versuchte Angriffe auf der Ebene der Webanwendung vorausschauend zu erkennen, zu protokollieren und abzublocken, sollte die nachstehende Anleitung für die Umsetzung befolgt werden:

- eine Basis von Regeln, die verbreitete Angriffe wie z. B. seitenübergreifendes Scripting (XSS) und SQL-Einschleusung abdecken, sollte angewendet und auf dem aktuellen Stand gehalten werden;
- Angriff-Signaturen (oder Regeln) sollten für jede Webanwendung angepasst werden und bei Änderungen an den Anwendungen auf dem aktuellen Stand gehalten werden.

Weitere Informationen

Eine Application Firewall ist eine Art Firewall, die den Eintritt, Austritt und/oder den Zugang von, zu oder durch eine Anwendung oder einen Dienst steuert. Sie funktioniert durch Überwachung und möglicherweise Blockierung des Eintritts, Austritts oder von System Service Calls, die nicht mit der konfigurierten Leitlinie übereinstimmen. Die Web-Application-Firewall-Technik verfügt speziell über die Fähigkeit, eine Reihe von Regeln auf HTTP/HTTPS-Nachrichtenübermittlungen anzuwenden, um viele Angriffsversuche zu erkennen und abzublocken.

Es ist beabsichtigt, dass die Maßnahme auch zum Schutz von bereits fertiggestellten produktiven Webanwendungen gegen äußere Angreifer dienen.

10 Kryptographie

10.1 Kryptographische Maßnahmen

10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 10.1.1.

10.1.2 Schlüsselverwaltung

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 10.1.2

Die Organisation sollte ein zentrales Zertifikats-Managementsystem betreiben, das mit denen der Partner kompatibel ist. Wenn eine Organisation eine PKI betreibt, sollte es ein zentrales Zertifikats-Managementsystem geben.

Die folgenden Dokumente sollten für eine PKI vorhanden sein, die nicht ausschließlich technischen Zwecken dient:

- Zertifizierungsrichtlinie (CP);
- Erklärung zum Zertifizierungsbetrieb (CPS).

Für jede PKI, die ausschließlich technischen Zwecken dient, sollten technische Dokumentationen vorhanden sein, die den Betrieb und die Sicherheitsnormen der PKI dokumentieren.

Für die Vergabe und den Entzug von Zertifikaten sollten verifizierbare Prozesse festgelegt sein.

Die Gültigkeit von Zertifikaten sollte dokumentiert werden.

Weitere Informationen

Das gebräuchlichste Format für Zertifikate ist das ITU X509.

11 Physische und umgebungsbezogene Sicherheit

11.1 Sicherheitsbereiche

11.1.1 Physische Sicherheitsperimeter

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 11.1.1

Notfallmaßnahmen sollten regelmäßig geprüft werden, um sicherzustellen, dass sie keine unzumutbaren physischen Sicherheitsrisiken einbringen, beispielsweise die Wiederherstellung aus Alarmauslösung.

11.1.2 Physische Zutrittssteuerung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.1.2.

11.1.3 Sichern von Büros, Räumen und Einrichtungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.1.3.

11.1.4 Schutz vor externen und umweltbedingten Bedrohungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.1.4.

11.1.5 Arbeiten in Sicherheitsbereichen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.1.5.

11.1.6 Anlieferungs- und Ladebereiche

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.1.6.

11.2 Geräte und Betriebsmittel

11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 11.2.1

Ausrüstungen, die in öffentlich zugänglichen Bereichen eingesetzt werden, sollten gegen unberechtigten Zugriff geschützt werden, z. B. durch feststehende und abzusperrende Gehäuse für PCs, physische und/oder logische Absicherung von Netzwerkdosen usw.

11.2.2 Versorgungseinrichtungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.2.

11.2.3 Sicherheit der Verkabelung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.3.

11.2.4 Instandhaltung von Geräten und Betriebsmitteln

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.4.

11.2.5 Entfernen von Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.5.

11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.6.

11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.7.

11.2.8 Unbeaufsichtigte Benutzergeräte

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.8.

11.2.9 Richtlinien für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 11.2.9.

12 Betriebssicherheit

12.1 Betriebsabläufe und -verantwortlichkeiten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.1.

12.2 Schutz vor Schadsoftware

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.2.

12.3 Sicherung von Information

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 12.3.1

Daten, die kritisch für die Sicherheit des Luftverkehrs sind, sollten innerhalb der in der Risikobeurteilung bestimmten Fristen wiederherstellbar sein.

12.4 Protokollierung und Überwachung

12.4.1 Ereignisprotokollierung

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 12.4.1

Alle Luftverkehrsnetze und für die Sicherheit des Luftverkehrs kritische Informationssysteme oder die nationale Infrastruktur sollten zur Unterstützung von Audits entsprechende Informationssicherheitsereignisse in einer Risikobeurteilung als identifiziert aufzeichnen.

12.4.2 Schutz von Protokollinformationen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.4.2.

12.4.3 Administratoren- und Bedienerprotokolle

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.4.3.

12.4.4 Uhrensynchronisation

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.4.4.

12.5 Steuerung von Software im Betrieb

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.5.

12.6 Handhabung technischer Schwachstellen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.6.

12.7 Audits von Informationssystemen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 12.7.

13 Kommunikationssicherheit

13.1 Netzwerksicherheitsmanagement

13.1.1 Netzwerksteuerungsmaßnahmen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 13.1.1

Es sollte ein übergreifender Netzwerk-Schaltplan für das Netzwerk vorliegen, der alle Eintritts- und Austrittspunkte identifiziert.

Die Risiken bezüglich des Verlustes der Verfügbarkeit für drahtlose Netzwerke sollten in der Risikobeurteilung besonders behandelt werden.

Die drahtlosen Verbindungen sollten nur über bestimmte externe Hosts zur Verfügung stehen.

13.1.2 Sicherheit von Netzwerkdiensten

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 13.1.2

Die Netzwerkarchitektur sollte vor externen Verbindungen zu internen Diensten geschützt werden. Beispielsweise könnten externe Datenanfragen von einem API-Gateway am Netzwerkperimeter zur Verfügung gestellt werden.

13.1.3 Trennung in Netzwerken

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 13.1.3.

13.2 Informationsübertragung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 13.2.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen an Informationssysteme

14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 14.1.1

Die Sicherheitsanforderungen und -maßnahmen sollten die Sicherheitsanforderungen der betroffenen externen Organisationen, die an gemeinsamen Geschäftsprozessen beteiligt sind, berücksichtigen.

Die Sicherheitsanforderungen und -maßnahmen sollten menschliche Faktoren für alle Aspekte der Systemnutzung berücksichtigen, einschließlich direkter und indirekter Schnittstellen, der Konnektivität mit anderen Systemen und Zugriffskontrollen für Benutzer. Die mit der Reaktion auf Sicherheitsvorfälle verbundenen menschlichen Faktoren sollten auch beachtet werden, um sicherzustellen, dass sie die allgemeine Systemsicherheit nicht untergraben.

Systemschnittstellen sollten für den sicheren Transfer von autorisierten Daten in das System oder aus dem System heraus, basierend auf dem geringsten Recht, sorgen.

14.1.2 Sicherung von Anwendungsdiensten in öffentlichen Netzwerken

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.1.2.

14.1.3 Schutz der Transaktionen bei Anwendungsdiensten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.1.3.

14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

14.2.1 Richtlinie für sichere Entwicklung

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 14.2.1

Ein Softwarecode sollte nicht wiederverwendet oder aus nicht vertrauenswürdigen Quellen geteilt werden.

14.2.2 Verfahren zur Verwaltung von Systemänderungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.2.

14.2.3 Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.3.

14.2.4 Beschränkung von Änderungen an Softwarepaketen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.4.

14.2.5 Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.5.

14.2.6 Sichere Entwicklungsumgebung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.6.

14.2.7 Ausgegliederte Entwicklung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.7.

14.2.8 Testen der Systemsicherheit

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.2.8.

14.2.9 Systemabnahmetest

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 14.2.9

Die Abnahme von Systemen, die in organisationsübergreifenden Prozessen eingesetzt werden, sollte einen formalen Prozess beinhalten, der sicherstellt, dass die Systemabnahme-Anforderungen und -kriterien mit der in Abschnitt 4 beschriebenen gemeinsamen Risikobeurteilung in Einklang stehen.

14.3 Testdaten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 14.3.

15 Lieferantenbeziehungen

15.1 Informationssicherheit in Lieferantenbeziehungen

15.1.1 Informationssicherheitsrichtlinie für Lieferantenbeziehungen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 15.1.1

Die Offenlegung von Identitäten gegenüber Partnern sollte Teil der Vereinbarungen sein. In den Vereinbarungen sollten die Bedingungen für die Offenlegung eindeutig festgelegt sein.

Bei Geschäftsprozessen, die mehrere Organisationen betreffen, sollte vertraglich eine genaue Abgrenzung der Verantwortlichkeiten für die Sicherheit von Werten (Assets) (siehe Abschnitt 7) festgelegt werden.

Dienstleister sollten bezüglich ihrer Informationssicherheitsleistung für die wichtigsten Dienstleistungen, die sie Entitäten zur Verfügung stellen, einer unabhängigen Überprüfung unterzogen werden.

15.1.2 Behandlung von Sicherheit in Lieferantenvereinbarungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 15.1.2.

15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 15.1.3.

15.2 Steuerung der Dienstleistungserbringung von Lieferanten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 15.2.

16 Handhabung von Informationssicherheitsvorfällen

16.1 Handhabung von Informationssicherheitsvorfällen und -verbesserungen

16.1.1 Verantwortlichkeiten und Verfahren

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 16.1.1

Verfahren für Sicherheitsvorfälle sollten regelmäßig geprüft werden, um ihre Genauigkeit sicherzustellen und das Verantwortlichkeitsbewusstsein zu fördern.

Die angewendeten Verfahren für den Umgang mit Sicherheitsvorfällen sollten eine effektive Interaktion mit Untersuchern von Flugunfällen erleichtern und alle erforderlichen Untersuchungen zu Flugunfällen und Vorfällen unterstützen.

16.1.2 Meldung von Informationssicherheitsereignissen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 16.1.2

Die Organisation sollte eine Arbeitsgruppe zur Reaktion auf Sicherheitsvorfälle einrichten, die entsprechend ausgebildet ist und über die Fertigkeiten verfügt, umgehend auf Sicherheitsvorfälle zu reagieren und die notwendigen Maßnahmen umzusetzen. Wenn ein Geschäftsprozess organisationsübergreifend betrieben wird, so sollten die einzelnen eingesetzten Arbeitsgruppen zur Reaktion auf Sicherheitsvorfälle — entsprechend

den Anforderungen und der Risikobewertung für diesen Geschäftsprozess — aufeinander abgestimmt werden, oder es sollte gegebenenfalls eine gemeinsame Arbeitsgruppe zur Reaktion auf Sicherheitsvorfälle von den beteiligten Organisationen eingesetzt werden. Die Organisation sollte dazu einen Verantwortlichen für Fragen zum Umgang mit Sicherheitsvorfällen und die Kontakte für die operative Durchführung des Managements von Sicherheitsvorfällen benennen.

Die Organisation sollte darüber hinaus an vorhandenen organisationsübergreifenden Managementsystemen für Sicherheitsvorfälle teilnehmen, die vom Staat oder von privaten Organisationen im Luftverkehrsbereich betrieben werden.

Eine angemessene Reaktionszeit der Arbeitsgruppe sollte sichergestellt sein.

16.1.3 Meldung von Schwächen in der Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 16.1.3

Die Organisation sollte erkannte Sicherheitsschwachstellen bei Geschäftsprozessen, die mehrere Organisationen betreffen, umgehend an die anderen beteiligten Organisationen melden.

Die Organisation sollte in bereits vorhandenen übergreifenden Gremien und Foren, die vom Staat oder von privaten Organisationen im Luftverkehrsbereich betrieben werden, mitarbeiten, um Informationen über Sicherheitsschwachstellen untereinander — soweit notwendig und für Dritte interessant — auszutauschen.

16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 16.1.4

16.1.5 Reaktion auf Informationssicherheitsvorfälle

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 16.1.5

16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 16.1.6

Die Organisation sollte in bereits vorhandenen Organisationen mitarbeiten, die vom Staat oder von privaten Organisationen im Luftverkehrsbereich betrieben werden, um gemeinsam aus Sicherheitsvorfällen, Bedrohungen und Schwachstellen zu lernen und entsprechende Maßnahmen abzuleiten.

16.1.7 Sammeln von Beweismaterial

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 16.1.7

Die Organisation sollte mit Organisationen, die Informationen sammeln und gemeinsam nutzen, zusammenarbeiten, die vom Staat oder von privaten Organisationen im Luftverkehrsbereich betrieben werden.

Die Sammlung und der Schutz von forensischen Beweisen sollten die gesetzlichen Anforderungen respektieren und sollten die Untersuchungstätigkeiten bei Flugunfällen nicht unangemessen behindern.

17 Informationssicherheitsaspekte beim Business Continuity Management

17.1 Aufrechterhalten der Informationssicherheit

17.1.1 Planung zur Aufrechterhaltung der Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 17.1.1

Die an einem gemeinsamen Geschäftsprozess beteiligten Organisationen sollten für den gesamten Vorgang eine Geschäftsauswirkungsanalyse durchführen.

Zusätzliche Informationen zu EN ISO/IEC 27002:2017, 17.1.1

Die Geschäftsauswirkungsanalyse sollte folgende Schritte nach ISO/IEC 27031:2011 enthalten:

- Auswahl der einzubeziehenden Organisationseinheiten und (Einzel-)Prozesse;
- Kritikalitätsanalyse für die betreffenden Werte (Assets);
- Festlegung von Kritikalitätskategorien und Schadensszenarien;
- Festlegung der zu betrachtenden Bewertungszeiträume;
- besondere Termine und Ereignisse;
- Kritikalitätsanalyse;
- Priorisierung der einzelnen Prozesse;
- Übersicht über Ressourcen für Normal- und Notbetrieb;
- Kritikalität und Wiederanlaufzeiten der Ressourcen;
- Berichterstattung.

Werden im laufenden Prozess Werte (Assets) ausgetauscht, so dass Änderungen in der Geschäftsauswirkungsanalyse nicht ausgeschlossen werden können, sollte die Geschäftsauswirkungsanalyse wiederholt werden. Die am Geschäftsprozess beteiligten Partner sollten umgehend darüber informiert werden.

17.1.2 Umsetzung der Aufrechterhaltung der Informationssicherheit

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 17.1.2.

17.1.3 Überprüfen und Bewerten der Aufrechterhaltung der Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für EN ISO/IEC 27002:2017, 17.1.3

Das Rahmenwerk für Kontinuitätspläne sollte einen Terminplan für die Überprüfung und Aktualisierung der Kontinuitätspläne enthalten.

Kontinuitätspläne sollten regelmäßig durch die beteiligten Organisationen gemeinsam geprüft werden. Die daraus gewonnenen Informationen sollten als Eingabe für die Verbesserung und Aktualisierung der Kontinuitätspläne dienen. Die Prüfungen sollten dokumentiert werden. Um das ordnungsgemäße Funktionieren der Kontinuitäts-Kontingenzpläne sicherzustellen, sollten die beteiligten Organisationen folgende Maßnahmen durchführen.

Die Prüfung und Abnahme der Pläne sollte erfolgen vor:

- Inbetriebnahme des Systems/des Geschäftsprozesses;
- kritischen System- und Prozessänderungen.

Der Anwendungsbereich der Prüfungen sollte sich an der Kritikalität des Geschäftsprozesses orientieren.

17.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs

Zusätzliche Maßnahme für EN ISO/IEC 27002:2017, 17.1

Die beteiligten Organisationen sollten einen organisationsübergreifenden Rahmen für den Plan zur Sicherstellung des Geschäftsbetriebs erstellen, der auf der Geschäftsauswirkungsanalyse beruht. Folgendes sollte darin mindestens enthalten sein:

- Personen in verantwortlichen Positionen bezüglich der gemeinschaftlichen Entscheidungsfindung;
- Notfallszenarien, die mehrere Organisationen betreffen;
- alternative Maßnahmen;
- alternative Betriebsverfahren;
- Aufbau der Kontinuitätspläne.

Aufgrund der geforderten hohen Verfügbarkeit von Geschäftsprozessen in der Luftfahrt sollte die Organisation in ihren Betriebsprozessen die Umstände dokumentieren, unter denen Kontinuitäts- oder Krisenpläne aktiviert werden.

17.2 Redundanzen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 17.2.

18 Compliance

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

18.1.1 Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen

Zusätzliche Maßnahme für EN ISO/IEC 27002:2017, 18.1.1

Die besonderen Sicherheitsmaßnahmen zur Erfüllung von Verbindlichkeiten hinsichtlich der Erteilung von Genehmigungen/Lizenzen sollten in einer Leitlinie und dazugehörigen sicherheitsbezogenen Betriebsverfahren dokumentiert werden.

Zusätzliche Informationen für EN ISO/IEC 27002:2017, 18.1.1

Verpflichtungen zum Schutz kritischer Infrastrukturen auf nationaler und europäischer Ebene könnten berücksichtigt werden.

18.1.2 Geistige Eigentumsrechte

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 18.1.2.

18.1.3 Schutz von Aufzeichnungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 18.1.3

18.1.4 Privatsphäre und Schutz von personenbezogener Information

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 18.1.4.

18.1.5 Regelungen bezüglich kryptographischer Maßnahmen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 18.1.5.

18.2 Überprüfungen der Informationssicherheit

18.2.1 Unabhängige Überprüfung der Informationssicherheit

Zusätzliche Maßnahme für EN ISO/IEC 27002:2017, 18.2.1

Aktivitäten für die Systementwicklung sollten unabhängig in regelmäßigen Abständen geprüft werden, um Sicherheit durch Design sicherzustellen.

18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 18.2.2.

18.2.3 Überprüfung der Einhaltung von technischen Vorgaben

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu EN ISO/IEC 27002:2017, 18.2.3.

Anhang A (informativ)

Zusätzliche, auf das Flugverkehrsmanagement bezogene Anleitung

A.1 Bewertung von Informationssicherheitsrisiken

A.1.1 Internes Management der Informationssicherheit

Um ihre eigene Sicherheitslage verstehen zu können, ist es notwendig, dass eine Organisation die Sicherheitslage ihrer Partner kennt.

Die Herstellung von Netzverbindungen und der Austausch von Daten beruhen auf einer Vertrauensbewertung der beteiligten Parteien untereinander. Der Umfang, mit dem der Netzwerkverkehr und die Daten gesteuert und überprüft werden müssen, wird durch das Maß an Vertrauen bestimmt. Dies wird unter A.4 weiter untersucht.

Zur Ermöglichung einer sicheren Verbindung nach außen und eines sicheren Datenaustausches sollte die Organisation das Vertrauen bewerten, das sie in die Verbindung und die empfangenen Daten setzen kann, und sie muss sich davon überzeugen, dass die Vertrauensbewertung validiert ist.

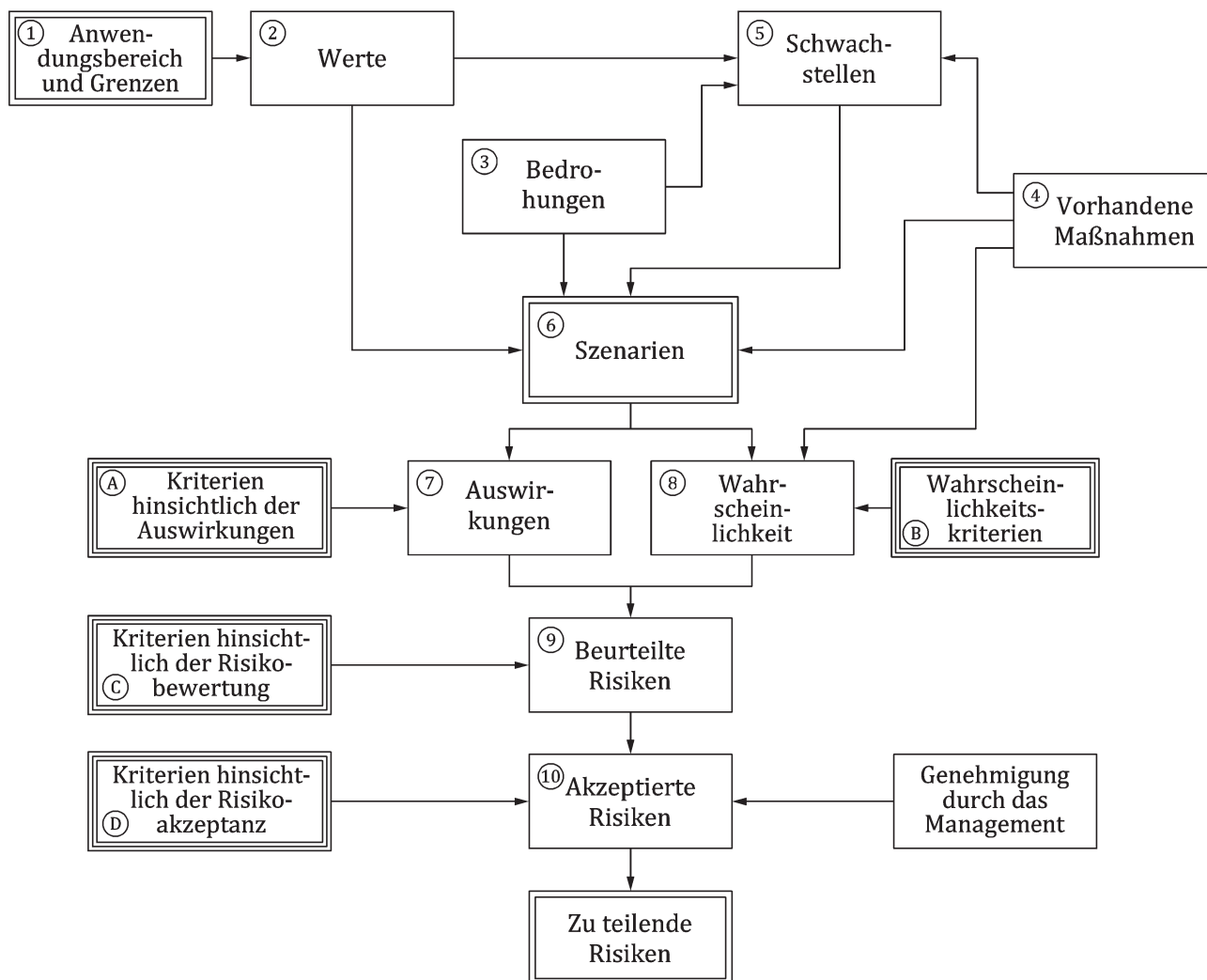
Es muss betont werden, dass das nicht bedeutet, dass die Organisation alles über die Sicherheit ihrer Partner wissen muss. Es werden lediglich genügend Informationen benötigt, um auf der Grundlage von Risikobewertungen das erforderliche Maß an Gewissheit zu erlangen.

Auf der Grundlage einer gemeinsamen Reihe von Parametern und Prozessen können generische Interkonnektivitätsfälle konstruiert und bewertet werden. Wenn diese Fälle auf konkrete Interkonnektivitätsfälle zutreffen, sind keine zusätzlichen Risikobewertungen notwendig. Ein Beispiel für einen generischen Interkonnektivitätsfall kann Anhang C entnommen werden.

Die Organisationen sollten diese Informationen im erforderlichen Maß mit ihren Partnern in der Zivilluftfahrt teilen. Dieses Dokument legt fest, welche Informationen gemeinsam genutzt werden müssen.

Der zugrunde liegende Prozess der Risikobewertung ist in Bild A.1 zusammengefasst. Dies gilt insbesondere für die nachstehend verwendete Terminologie.

In Abhängigkeit von der angewendeten Methodik dürfen die in den nachfolgenden Abschnitten beschriebenen Maßnahmen auch in einer anderen Reihenfolge durchgeführt werden.



Legende

doppelt umrandete Kästchen
dreifach umrandete Kästchen

Informationen, die nach A.2 gemeinsam zu nutzen sind
Kriterien, die als Teil des Risikomanagementprozesses der Organisation festzulegen sind. Sie werden dann als feststehende Eingaben für die einzelnen Risikobewertungen verwendet.

Bild A.1 — Bewertung von Informationssicherheitsrisiken

Kriterien

A Kriterien hinsichtlich der Auswirkungen:

Bezüglich des Ausmaßes von Schäden oder Kosten für die Organisation, die durch ein Informationssicherheitsereignis verursacht werden, sollten Kriterien hinsichtlich der Auswirkungen entwickelt und festgelegt werden.

B Kriterien für die Beurteilung der Wahrscheinlichkeit:

Es sollten Kriterien für die Beurteilung der Wahrscheinlichkeit entwickelt werden, die in ähnlicher Weise von beteiligten und beeinträchtigten Organisationen verstanden werden. Die Wahrscheinlichkeitskriterien werden zur Bewertung des Ausmaßes der Bedrohung in jedem Szenario angewendet.

C Kriterien hinsichtlich der Risikobewertung:

Es sollten Risikobewertungskriterien zur Beurteilung des Informationssicherheitsrisikos der Organisation entwickelt werden, wobei Folgendes zu berücksichtigen ist:

- der strategische Wert des Geschäftsinformationsprozesses;
- die Kritikalität der betroffenen Informationswerte;
- gesetzliche und behördliche Anforderungen und vertragliche Verpflichtungen;
- betriebliche und geschäftliche Bedeutung von Verfügbarkeit, Vertraulichkeit und Integrität;
- Erwartungen und Wahrnehmungen der Beteiligten sowie negative Auswirkungen auf den Geschäftswert und das Ansehen der Organisation.

D Kriterien hinsichtlich der Risikoakzeptanz:

Hinsichtlich der Risikoakzeptanz sollten Kriterien entwickelt und festgelegt werden.

Der Prozess der Risikobewertung sollte folgende Schritte umfassen:

1 Identifizierung von Anwendungsbereich und Grenzen:

Funktion: Sicherstellung, dass alle maßgeblichen Werte berücksichtigt werden, und Bewertung von Risiken, die über die Grenzen der Organisation hinausgehen könnten. Darüber hinaus sollte die Organisation für alle Ausschlüsse aus dem Anwendungsbereich eine Begründung bereithalten.

Ergebnisse: Festlegung des Anwendungsbereiches und der Grenzen der Bewertung.

2 Identifizierung von Werten:

Funktion: Identifizierung von allem, was für die Organisation von Wert ist und dessen Schutz daher erforderlich ist. Ein Wert (Asset) würde über eine individuelle Reihe von Merkmalen verfügen müssen, die auf Bedrohungen und Schwachstellen bezogen werden können, um die Analyse in den folgenden Schritten zu ermöglichen.

Ergebnisse: Eine Auflistung von Werten, die hinsichtlich des Risikos bewertet werden müssen, sowie eine Auflistung von Geschäftsprozessen, die sich auf die Werte und ihre Relevanz zusammen mit den entsprechenden Eigentümern der Werte beziehen.

3 Identifizierung von Bedrohungen:

Funktion: Identifizierung von Bedrohungen, die über das Potential verfügen, Werte, wie z. B. Informationen, Prozesse und Systeme, zu schädigen. Eine Bedrohung kann innerhalb oder außerhalb der Organisation entstehen.

Ergebnisse: Eine Auflistung von Bedrohungen mit Identifizierung der Art und Quelle der Bedrohung.

4 Identifizierung vorhandener Maßnahmen:

Funktion: Identifizierung vorhandener oder geplanter Maßnahmen, um zu erkennen, wie sich dadurch die Wahrscheinlichkeit von Bedrohungen sowie die Einfachheit der Ausnutzung von Schwachstellen oder die Auswirkung eines Ereignisses verringern würden.

Ergebnisse: Auflistung aller bereits durchgeführten und geplanten Maßnahmen, ihrer Umsetzung und des Anwendungsstatus.

5 Identifizierung von Schwachstellen:

Funktion: Identifizierung von Merkmalen der Werte (Assets) sowie von Geschäftsprozessen, die für einen Angriff ausgenutzt werden können. Zum Zeitpunkt der Bewertung werden nicht alle Schwachstellen bekannt sein (insbesondere die technischen sogenannten Zero-Day-Schwachstellen). Diese Möglichkeit muss mittels Sicherheitsmaßnahmen angesprochen werden, die eine schnelle Neubewertung des Risikos bei Entdeckung der Schwachstellen ermöglichen.

Ergebnisse: Auflistung von Schwachstellen bezüglich der Werte, Bedrohungen und Maßnahmen.

6 Identifizierung von Folgen und Auswirkungen (Erstellen von Szenarien):

Funktion: Identifizierung der Auswirkungen auf die Organisation, die durch ein Bedrohungsszenario verursacht werden könnten. Ein Bedrohungsszenario ist die Beschreibung einer Bedrohung, die eine bestimmte Schwachstelle oder Gruppe von Schwachstellen ausnutzt, um trotz vorhandener Kontrollmaßnahmen Werte anzugreifen.

Ergebnisse: Auflistung von Bedrohungsszenarien mit ihren jeweiligen Auswirkungen bezogen auf die Werte und Geschäftsprozesse der Organisation sowie weiterer betroffener Organisationen.

7 Bewertung von Folgen:

Funktion: Bewertung der Folgen jedes Szenarios, bezogen auf die Einschätzung des Wertes (Asset) und auf der Grundlage der Kriterien für die geschäftlichen Auswirkungen.

Ergebnisse: Auflistung der bewerteten Folgen eines Ereignisszenarios, angegeben hinsichtlich der Werte und Auswirkungskriterien.

8 Bewertung des Ausmaßes der Bedrohung:

Funktion: Verwendung der Wahrscheinlichkeitskriterien zur Bewertung des Umfangs der Bedrohung aus jedem Szenario.

Ergebnisse: Wahrscheinlichkeit von Bedrohungsszenarien (quantitativ und qualitativ).

9 Beurteiltes Risiko:

Funktion: Umwandeln von Szenarien in beurteilte Risiken auf der Grundlage der Folgen und des Umfangs der Bedrohung sowie der Risikobewertungskriterien, die während der Herstellung des Zusammenhangs festgelegt wurden. Die Summierung mehrerer kleiner oder mittlerer Risiken kann zu wesentlich größeren Gesamtrisiken führen und muss entsprechend behandelt werden.

Ergebnisse: Auflistung von Risiken, die entsprechend den Risikobewertungskriterien bezüglich der Bedrohungsszenarien, die zu diesen Risiken führen, klassifiziert werden.

10 Bewertung der Risikoakzeptanz:

Funktion: Bewertung der Auflistung klassifizierter Risiken hinsichtlich der Annehmbarkeit auf der Grundlage der zuvor festgelegten Risikoakzeptanzkriterien.

Ergebnisse: Auflistung bewerteter Risiken mit den zugehörigen Bedrohungsszenarien, die entsprechend den Risikoakzeptanzkriterien bevorzugt zu behandeln sind. Das schließt Informationen über die Folgen und die Wahrscheinlichkeit für jedes Risiko ein.

Ohne Kennzeichnung: Identifizieren von geteilten Risiken.

Funktion: Identifizieren der akzeptierten Risiken, die durch Partnerorganisationen beeinflusst sind oder diese beeinflussen können.

Ergebnisse: Eine Auflistung von Risiken und entsprechenden Risikoinformationen, die mit Partnerorganisationen geteilt werden muss.

A.2 Probleme der Interoperabilität von Risikobewertungen

A.2.1 Allgemeines

Die Interoperabilität von Risikobewertungen ist ein wichtiges Problem in einer Umgebung, die als „übergeordnetes System“ gekennzeichnet werden kann. In solch einer Umgebung sind Risikobewertungen, die (Teilbereiche von) diesen Systemen abdecken, vorhanden und es ist wichtig, die Übereinstimmungen zwischen den identifizierten Risiken und den Abschwächungsmaßnahmen, die in diesen Bewertungen vorgeschlagen werden, zu ermitteln. Dadurch wird eine schlüssige Sicherheitspolitik für das gesamte vielschichtige System ermöglicht.

Um die Interoperabilität von Risikobewertungen zu erreichen, wenn unterschiedliche methodische Vorgehensweisen bei der Risikobewertung angewendet werden,

- muss eine Verständigung hinsichtlich der Übereinstimmung zwischen den Themen/Begriffen/Benennungen, die in jede der zugrunde liegenden methodischen Vorgehensweisen für die Risikobewertung eingeführt wurden, erfolgen und
- müssen die Tiefe und Breite jeder Bewertung verglichen und bewertet werden, um die vorausgesetzte Umgebung und die Entscheidungen hinsichtlich des Sicherheitsniveaus des vorliegenden Systems zu verstehen.

Terminologieprobleme könnten ebenso relevant sein, da es selbst bei gleichen zugrunde liegenden Verfahren vorkommen könnte, dass Themen/Begriffen/Benennungen unterschiedliche Bedeutungen zugeordnet sind.

A.2.2 Management der Informationssicherheit für mehrere Organisationen

Um die Vergleichbarkeit über mehrere Organisationen hinweg sicherzustellen, sollten die Organisationen mindestens die Informationen zum Anwendungsbereich und den Grenzen, zu den Bedrohungsszenarien und den bewerteten Risiken gemeinsam nutzen.

Die gemeinsame Nutzung von Informationen sollte darauf beruhen, in dem erforderlichen Maße das Verfahren zu kennen, um mit geteilten Risiken umzugehen. Aufgrund der sensiblen Art der Auflistungen von bewerteten Risiken werden diese Ergebnisse üblicherweise von jeder Organisation intern ermittelt und intern vertraulich behandelt.

Der Austausch der Informationen muss durch bindende Vertraulichkeitsvereinbarungen in geeigneter Form zwischen den betroffenen Organisationen unterstützt werden.

A.2.3 Anpassung des Sicherheits- und Sicherheitsrisikomanagements

Die Sicherheit bildet in vielen Organisationen im Flugverkehrsmanagement Elemente eines allgemeinen Risikomanagements. Dies sollte in der Luftfahrt in einem einheitlichen Sicherheitsansatz widerspiegelt werden hinsichtlich

- einer einheitlichen Darstellung der Prozesse und Werte, die Gegenstand von einzelnen Sicherheitsnachweisen sind;

ANMERKUNG Für das Luftverkehrsmanagement stellt das sich entwickelnde Rahmenwerk der European Air Traffic Management Architecture (EATMA) eine einheitliche Grundlage in Form einer Karte zur Verfügung, auf die Bezug zu nehmen ist.

- eines Ansatzes zu „allen Gefährdungen“, bei dem sowohl „unbeabsichtigte Ereignisse“ bezüglich technischen Versagens, höherer Gewalt, menschlichen Versagens, organisatorischer Schwachpunkte als auch vorsätzlicher Handlungen, d. h. Kriminalität und Terror, berücksichtigt werden;
- eines Ansatzes zu „allen Auswirkungen“, bei dem alle entsprechenden wichtigen Leistungsbereiche der Luftfahrt berücksichtigt werden. Während die Sicherheit als das Ziel zum „Schutz von Leib und Leben“ hervorsticht, müssen andere Bereiche — insbesondere die Leistungsfähigkeit und Wirtschaftlichkeit — ebenfalls berücksichtigt werden.

Die Anpassung der Sicherheit sollte auch die Identifizierung und Lösung von Konflikten zwischen Risikominderungsmaßnahmen umfassen.

A.3 Bestimmung von Maßnahmen

Die Maßnahmen sollten auf der Grundlage der Ergebnisse der Informationssicherheitsrisikobewertung bestimmt und umgesetzt und mit Folgendem verglichen werden:

- Anhang A der ISO/IEC 27001;
- Maßnahmen nach Anhang E, die die in EN ISO/IEC 27002:2017 angegebenen ergänzen. Diese Maßnahmen sind in dieser Europäischen Norm als luftverkehrsspezifische Umsetzungsvorgaben beschrieben.

A.4 Vertrauensstufen

A.4.1 Einleitung

Wie bereits zuvor in 4.2 ausgeführt, ist die Erbringung von Dienstleistungen in der Luftfahrt von einem hohen Maß an Zusammenarbeit zwischen den beteiligten Organisationen geprägt. Die Sicherstellung der Sicherheit der Informationen und der informationsverarbeitenden Systeme einer einzelnen Organisation in einem gemeinsamen Geschäftsvorgang sowie der dahinter stehenden eigenen Geschäftsvorgänge haben ein hohes Maß an individuellen Vereinbarungen und Überprüfungen zur Folge.

Luftfahrtorganisationen, die in Partnerschaft arbeiten, sollten vereinbaren, dass in weiteren gemeinsamen Geschäftsabläufen (einschließlich denen mit dritten Parteien) Vertrauensstufen anerkannt werden, unterstützt durch sinnvolle Nachweise (aus der 1:1-Beziehung zweier Parteien oder über eine Verifizierung durch Dritte).

Die „Vertrauensstufe der Organisation“ (LoT-O) bezieht sich auf die jeweilige Organisation. Die Einstufung bezieht sich dabei immer auf den Teil des gemeinsamen Prozesses, der von der jeweiligen Organisation erbracht wird. Insbesondere werden dabei mögliche Informationssicherheitsrisiken berücksichtigt, die für die jeweilige Partei durch Koppelung der Geschäftsprozesse entstehen können.

Zusätzlich zur Gesamtbewertung der Organisation kann eine Vertrauensstufe auch einer bestimmten Anwendung in einem Teilbereich, wie in den Beispielen in Anhang A beschrieben, zugeordnet werden.

A.4.2 Skala der Vertrauensstufen

Zur Einstufung der „Vertrauensstufe der Organisation“ wird eine sechsstufige Skala angewendet:

- vertrauenswürdig;
- Vertrauensstufe 0;

- Vertrauensstufe 1;
- Vertrauensstufe 2;
- Vertrauensstufe 3;
- nicht vertrauenswürdig.

Die allgemeinen Definitionen für die verschiedenen Stufen sollten wie folgt sein:

a) vertrauenswürdig

Die Kategorie „vertrauenswürdig“ wird nur für organisationseigene Abteilungen, Tochterunternehmen oder Geschäftsprozesse angewendet, die vollständig den eigenen Sicherheitsanforderungen unterliegen. Drittpartei-Organisationen können nicht in die Kategorie „vertrauenswürdig“ eingestuft werden.

b) Vertrauensstufe 0

Die Kategorie „Vertrauensstufe 0“ (LT0, en: Limited Trust 0) bezeichnet Drittpartei-Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, jedoch folgende Anforderungen erfüllen:

Alle Maßnahmen dieser Europäischen Norm sind verbindlich umgesetzt. Die Übereinstimmung mit der Norm wurde von einem qualifizierten Informationssicherheits-Auditor¹ bestätigt.

c) Vertrauensstufe 1

Die Kategorie „Vertrauensstufe 1“ (LT1, en: Limited Trust 1) bezeichnet Drittpartei-Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein sehr hohes Gesamtniveau an Informationssicherheit erreichen. Das trifft auch auf Bereiche zu, in denen lediglich indirekte Risiken für die Partner-Organisationen bestehen.

BEISPIEL 1 Kopplung von Netzwerken

Unter bestimmten Umständen gestatten Organisationen ihren Partnerorganisationen mit LT1-Einstufung den Zugriff auf eigene Anwendungen nach dem „Need-to-have-Prinzip“, ohne anwendungsspezifische Schutzmaßnahmen (z. B. Web Application Firewalls) und ohne weitere Authentisierung an der Netzwerkgrenze (z. B. an der Firewall) durchzusetzen.

Dieses Vorgehen ist nur dann angemessen, wenn der Partner über ein sehr hohes Sicherheitsniveau (LT1) verfügt und in diesem Zusammenhang alle maßgeblichen Informationssicherheitsmanagementsystem-Maßnahmen umgesetzt hat.

d) Vertrauensstufe 2

Die Kategorie „Vertrauensstufe 2“ (LT2, en: Limited Trust 2) bezeichnet Drittpartei-Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein hohes Gesamtniveau an Informationssicherheit erreichen.

BEISPIEL 2 Kopplung von Netzwerken

1 Das kann z. B. ein zertifizierter Informationssystem-Auditor (CISA), ein Auditleiter nach ISO/IEC 27001 oder ein gleichwertiger Sachkundiger sein.

Unter bestimmten Umständen gestatten Organisationen Partnerorganisationen mit LT2-Einstufung den Zugriff auf eigene Anwendungen nach dem „Need-to-have-Prinzip“, fordern jedoch vor dem Verbindungsaufbau an der Netzwerkgrenze (z. B. an der Firewall) eine explizite Authentisierung.

Dieses Vorgehen ist nur dann angemessen, wenn der Partner über ein hohes Sicherheitsniveau (LT2) verfügt und in diesem Zusammenhang alle wichtigen Informationssicherheitsmanagementsystem-Maßnahmen (z. B. Management von Sicherheitsvorfällen) umgesetzt hat.

e) Vertrauensstufe 3

Die Kategorie „Vertrauensstufe 3“ (LT3, en: Limited Trust 3) bezeichnet Drittpartei-Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein Basis-Niveau an Informationssicherheit erreichen.

BEISPIEL 3 Kopplung von Netzwerken

Unter bestimmten Umständen gestatten Organisationen Partnerorganisationen mit LT3-Einstufung den Zugriff auf eigene Anwendungen nach dem „Need-to-have-Prinzip“, fordern jedoch vor dem Verbindungsaufbau an der Netzwerkgrenze (z. B. an der Firewall) sowohl eine explizite Authentisierung als auch weitere Schutzmaßnahmen (z. B. Content-Filterung, Eingabe-Kontrolle, Rechteverwaltung usw.). Dieses Vorgehen ist nur dann angemessen, wenn der Partner Basis-Sicherheitsmaßnahmen (z. B. Virenschutz, Backup/Restore usw.) sowie ein Sicherheitsmanagementsystem umgesetzt hat.

f) nicht vertrauenswürdig

Diese Kategorie bezeichnet alle Organisationen, die die Anforderungen der Kategorie „Vertrauensstufe 3“ nicht erfüllen.

A.4.3 Klassifizierungskriterien

Die Einzelheiten der speziellen Maßnahmen, die für die unterschiedlichen Vertrauensstufen umzusetzen sind, sollten von den Partnern festgelegt werden.

A.5 Bericht über die Anwendbarkeit

Die Organisation sollte einen „Bericht über die Anwendbarkeit“ nach EN ISO/IEC 27001:2017, Anhang A, und den zusätzlichen Maßnahmen dieser Norm aufstellen. Der „Bericht über die Anwendbarkeit“ sollte einem Partner bei Bedarf bekannt gemacht werden.

A.6 Messung und Auditierung der Sicherheit

Die Messung der Wirksamkeit der umgesetzten Kontrollmaßnahmen sollte unter Berücksichtigung der Leitlinien nach ISO/IEC 27004:2016 erfolgen.

Interne Auditierungsmaßnahmen sollten unter Berücksichtigung der zusätzlichen Hinweise in ISO/IEC 27007:2017 durchgeführt werden.

Ein Beispiel für die Anwendung von Maßnahmen in einer Kontrollübersicht ist in Anhang D enthalten.

Anhang B (informativ)

Beispiele für die Umsetzung

B.1 Allgemeines

Anhang B enthält Beispiele für die Festlegung von Vertrauensstufen für eine Organisation (LoT-O) und für besondere Anwendungsbereiche (LoT-A), die eine besondere Rolle bei der engen Zusammenarbeit von Organisationen im Luftverkehrsbereich spielen.

„Vertrauensstufen“ können durch Einhaltung festgelegter Kriterien erreicht werden.

Die „Vertrauensstufe der Organisation“ (LoT-O) ist entscheidend für eine wirksame Zusammenarbeit, die Auswahl geeigneter Partner und die Vergleichbarkeit von Partnern.

Die folgende Tabelle B.1 gibt einen Überblick über ein Beispiel für eine Vertrauensstufe LoT-O. Ein ausführliches Beispiel kann Anhang B entnommen werden.

Die Gliederung der Bezifferung in der Tabelle spiegelt die entsprechende Gliederung der „Maßnahmen“-Abschnitte in EN ISO/IEC 27002:2017 wider.

Tabelle B.1 — Überblick über ein Beispiel für eine Vertrauensstufe LoT-O

Maßnahmen	LT0	LT1	LT2	LT3
5. Informationssicherheitsrichtlinien	vorgeschrieben	vorgeschrieben	vorgeschrieben	vorgeschrieben
6. Organisation der Informationssicherheit	vorgeschrieben	überwiegend	überwiegend	teilweise
7. Personalsicherheit	vorgeschrieben	überwiegend	überwiegend	teilweise
8. Verwaltung der Werte	vorgeschrieben	vorgeschrieben	—	—
9. Zugangssteuerung	vorgeschrieben	überwiegend	teilweise	teilweise
10. Kryptographie	vorgeschrieben	vorgeschrieben	—	—
11. Physische und umgebungsbezogene Sicherheit	vorgeschrieben	überwiegend	teilweise	—
12. Betriebssicherheit	vorgeschrieben	überwiegend	teilweise	teilweise
13. Kommunikationssicherheit	vorgeschrieben	überwiegend	teilweise	teilweise
14. Anschaffung, Entwicklung und Instandhaltung von Systemen	vorgeschrieben	teilweise	teilweise	—
15. Lieferantenbeziehungen	vorgeschrieben	überwiegend	teilweise	—
16. Handhabung von Informationssicherheitsvorfällen	vorgeschrieben	überwiegend	überwiegend	—
17. Informationssicherheitsaspekte beim Business Continuity Management	vorgeschrieben	teilweise	teilweise	—
18. Compliance	vorgeschrieben	überwiegend	teilweise	teilweise

Wird die Zusammenarbeit in einem bestimmten Anwendungsbereich angestrebt, muss eine Vertrauensstufe für diesen Anwendungsbereich festgelegt werden. Beispiele dafür sind in den nachfolgenden Abschnitten angegeben.

Dabei ist zu berücksichtigen, dass die Vertrauensstufe für den Anwendungsbereich (LoT-A) maximal der Vertrauensstufe des Kommunikationspartners (LoT-O) entsprechen kann. Dieses Minimumprinzip ist in Bild B.1 dargestellt.

BEISPIEL Die Vertrauensstufe einer bestimmten Verbindung wird als LT1 festgelegt. Der Kommunikationspartner als Organisation ist jedoch nur als LT2 eingestuft. Daraus folgt, dass die Verbindung lediglich LT2 erreichen kann. Die jeweiligen Sicherheitsmaßnahmen sind entsprechend anzuwenden.

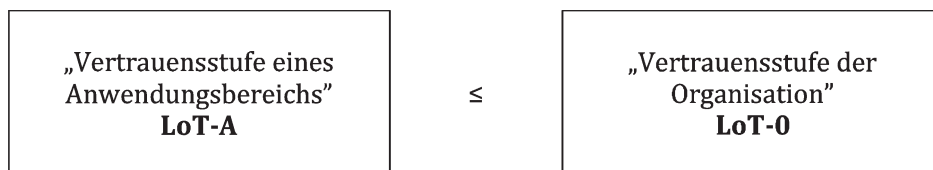


Bild B.1 — LoT A gegenüber LoT-O

B.2 Sicherheit von Informationen in Webanwendungen und Webdiensten (LoT-A-WEB)

B.2.1 Allgemeines

Ziel: Sicherstellung, dass die Sicherheit von Informationen in und beim Austausch zwischen Webanwendungen/Webdiensten sichergestellt ist.

Organisationen des Luftverkehrs tauschen über Webanwendungen/Webdienste untereinander und mit Dritten vermehrt Informationen aus. Für die Sicherheit der Anwendungen ist es entscheidend, welche internen Informationsressourcen für die Anwendungen zur Verfügung gestellt werden.

B.2.2 Parameter für die Vertrauensstufe einer Webanwendung/eines Webdienstes

Folgende Parameter werden für die Ermittlung der Vertrauensstufe der Webanwendung/des Webdienstes herangezogen:

- Leitlinie für Web-Anwendungen/Web-Dienste;
- Entwicklung von Webanwendungen;
- Code-Reviews;
- Kompetenz von Entwicklern für Webanwendungen (siehe 7.2.2);
- Penetrationsprüfungen von Anwendungen;
- Penetrationsprüfungen von Infrastrukturen;
- Web Application Firewalls (siehe 9.4.6).

B.2.3 Ermittlung der Vertrauensstufe der Webanwendung/des Webdienstes (LoT-A-WEB)

Die Vertrauensstufe der Webanwendung/des Webdienstes wird nach Tabelle B.2 ermittelt.

Tabelle B.2 — Vertrauensstufe einer Webanwendung/eines Webdienstes

Konfigurations-Nr.	Leitlinie für Webanwendungen/ Webdienste	Entwicklung von Webanwendungen	Code-Reviews	Kompetenz von Entwicklern von Anwendungen	Penetrationsprüfungen von Anwendungen	Penetrationsprüfungen von Infrastrukturen	Web Application Firewalls	Maximal erreichbare Vertrauensstufe (LoT-A-WEB)
1	ja	ja	ja	ja	ja	ja	ja	LT1
2	ja	nein	nein	nein	ja	ja	nein	LT2
3	ja	nein	nein	nein	ja	ja	nein	LT3
4	ja	nein	nein	nein	nein	ja	nein	LT3
5	nein	nicht anzuwenden	nicht anzuwenden	nicht anzuwenden	nicht anzuwenden	nicht anzuwenden	nicht anzuwenden	UT
ja = Parameter erfüllt nein = Parameter nicht erfüllt								

Es sollte beachtet werden, dass die Vertrauensstufe der Webanwendung/des Web-Dienstes (LoT-A-WEB) maximal der Vertrauensstufe des Kommunikationspartners (LoT-O) entsprechen kann.

B.2.4 Folgen

Die Vertrauensstufe der Webanwendung (LoT-A-WEB) muss mindestens den Grad des Schutzbedarfs erreichen, der den bereits festgelegten Kriterien für die Risikobewertung entspricht. Der Zusammenhang zwischen dem Grad des Schutzbedarfs und der Vertrauensstufe ist in Tabelle B.3 dargestellt.

Tabelle B.3 — Bewertungskriterien für LoT A WEB

Schutzbedarf (Kategorie)	Erforderliche Vertrauensstufe LoT-A-WEB
sehr hoch	LT1
hoch	LT1
mittel	LT2
gering	LT3

B.3 Organisationsübergreifende Verbindungen/externe Verbindungen (LoT-A-NET)

Ziel: Sicherstellung, dass organisationsübergreifende Verbindungen/externe Verbindungen sicher betrieben werden.