

DIN EN 16495

ICS 03.100.70; 03.220.50; 35.240.60

Einsprüche bis 2018-08-08
Vorgesehen als Ersatz für
DIN EN 16495:2014-05

Entwurf

**Flugverkehrsmanagement –
Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt;
Deutsche und Englische Fassung prEN 16495:2018**

Air Traffic Management –
Information security for organisations supporting civil aviation operations;
German and English version prEN 16495:2018

Gestion du trafic aérien –
Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile;
Version allemande et anglaise prEN 16495:2018

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-06-08 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nl@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Luft- und Raumfahrt (NL), 10772 Berlin, Burggrafenstr. 6, 10787 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 142 Seiten

DIN-Normenausschuss Luft- und Raumfahrt (NL)

Nationales Vorwort

Dieses Dokument (prEN 16495:2018) wurde vom Technischen Komitee CEN/TC 377 „Luftverkehrsmanagement“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

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

ISO/IEC 27001:2013 siehe DIN EN ISO/IEC 27001:2017-06

ISO/IEC 27002:2013 siehe DIN EN ISO/IEC 27002:2017-06

ISO/IEC 27009:2016 siehe DIN ISO/IEC 27009:2016-11

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;
- c) Informationen zur entwicklungs-, produktions- und instandhaltungsspezifischen Sicherheit;
- d) Informationen zu Sicherheitsbestätigung;
- e) informativer Anhang mit einem Umsetzungsbeispiel für Anwendung von Maßnahmen bei der behördlichen Aufsicht.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 27001:2017-06, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017*

DIN EN ISO/IEC 27002:2017-06, *Informationstechnik — Sicherheitsverfahren — Leitfaden für Informationssicherheitsmaßnahmen (ISO/IEC 27002:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27002:2017*

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

— Leerseite —

Flugverkehrsmanagement — Informationssicherheit für Organisationen im Bereich der Zivilluftfahrt

Gestion du trafic aérien — Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile

Air Traffic Management — Information security for organisations supporting civil aviation operations

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm

Dokument-Untertyp:

Dokument-Stage: CEN-Umfrage

Dokument-Sprache: D

STD Version 2.9d

Inhalt

	Seite
Europäisches Vorwort	6
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Informationssicherheitsmanagement in der Luftfahrt	9
4.1 Aufbau dieser Europäischen Norm	9
4.2 Auf ISO/IEC 27001:2013 bezogene luftverkehrsspezifische Anforderungen	9
5 Informationssicherheitsleitlinien	10
5.1 Managementausrichtung zur Informationssicherheit	10
5.1.1 Informationssicherheitsleitlinien	10
5.1.2 Überprüfung der Informationssicherheitsrichtlinien	10
6 Organisation der Informationssicherheit	11
6.1 Interne Organisation	11
6.1.1 Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit	11
6.1.2 Aufgabentrennung	11
6.1.3 Kontakt zu Behörden	11
6.1.4 Kontakt mit Interessengruppen	11
6.1.5 Informationssicherheit im Projektmanagement	12
6.2 Mobilgeräte und Telearbeit	12
7 Personalsicherheit	12
7.1 Vor der Anstellung	12
7.1.1 Überprüfung	12
7.1.2 Arbeitsvertragsklauseln	12
7.2 Während der Anstellung	12
7.2.1 Verantwortung des Managements	12
7.2.2 Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit	12
7.2.3 Disziplinarverfahren	13
7.3 Beendigung und Wechsel der Anstellung	13
8 Management von organisationseigenen Werten	13
8.1 Verantwortung für organisationseigene Werte	13
8.1.1 Inventar der organisationseigenen Werte	13
8.1.2 Eigentum von organisationseigenen Werten	13
8.1.3 Zulässiger Gebrauch von organisationseigenen Werten	13
8.1.4 Rückgabe von organisationseigenen Werten	13
8.2 Klassifizierung von Informationen	13
8.2.1 Klassifizierung von Informationen	13
8.2.2 Kennzeichnung von Informationen	14
8.2.3 Handhabung von organisationseigenen Werten	14
8.3 Handhabung von Speicher- und Aufzeichnungsmedien	14
9 Zugangskontrolle	14
9.1 Geschäftsanforderungen für Zugangskontrolle	14
9.2 Benutzerverwaltung	14

9.2.1	An- und Abmeldung von Benutzern.....	14
9.2.2	Zugangsbereitstellung für Benutzer.....	15
9.2.3	Verwaltung von Sonderzugangsrechten	15
9.2.4	Verwaltung geheimer Authentisierungsdaten von Benutzern.....	15
9.2.5	Überprüfung von Benutzerberechtigungen	15
9.2.6	Entziehung oder Anpassung von Zugangsrechten	15
9.2.7	Digitales Identitätsmanagement	15
9.2.8	Organisationsübergreifende eindeutige Darstellung von Entitäten	16
9.3	Benutzerverantwortung	16
9.4	Kontrolle des Zugangs zu Systemen und Anwendungen	16
9.4.1	Einschränkung von Informationszugriffen.....	16
9.4.2	Verfahren für sichere Anmeldung.....	16
9.4.3	Systeme zur Verwaltung von Passwörtern	17
9.4.4	Verwendung von Systemwerkzeugen.....	17
9.4.5	Zugangskontrolle zum Programm Quellcode.....	17
9.4.6	Web Application Firewalls	17
10	Kryptografie	17
10.1	Kryptografische Maßnahmen	17
10.1.1	Leitlinie für die Anwendung kryptografischer Maßnahmen	17
10.1.2	Verwaltung kryptografischer Schlüssel	18
11	Physische und umgebungsbezogene Sicherheit	18
11.1	Sicherheitsbereiche	18
11.1.1	Physische Sicherheitszonen	18
11.1.2	Physische Zutrittskontrollen	18
11.1.3	Sicherung von Büros, Räumen und Einrichtungen	18
11.1.4	Schutz vor Bedrohungen von außen und aus der Umgebung	18
11.1.5	Arbeiten in Sicherheitsbereichen.....	18
11.1.6	Anlieferungs- und Ladezonen	19
11.2	Betriebsmittel.....	19
11.2.1	Platzierung und Schutz von Betriebsmitteln	19
11.2.2	Unterstützende Versorgungseinrichtungen.....	19
11.2.3	Sicherheit der Verkabelung.....	19
11.2.4	Instandhaltung von Gerätschaften.....	19
11.2.5	Entfernung von Werten.....	19
11.2.6	Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude	19
11.2.7	Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln	19
11.2.8	Unbeaufsichtigte Benutzerausstattung.....	19
11.2.9	Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms	19
12	Betriebssicherheit.....	20
12.1	Betriebliche Verfahren und Verantwortlichkeiten	20
12.2	Schutz vor Malware	20
12.3	Backup	20
12.3.1	Datensicherungen	20
12.4	Protokollierung und Überwachung.....	20
12.4.1	Ereignisprotokollierung	20
12.4.2	Schutz von Protokollinformationen.....	20
12.4.3	Administrator- und Betreiberprotokolle	20
12.4.4	Zeitsynchronisierung.....	20
12.5	Kontrolle von Software im Betrieb	20
12.6	Umgang mit technischen Schwachstellen.....	20
12.7	Überlegungen zu Audits von Informationssystemen.....	21
13	Sicherheit in der Kommunikation.....	21
13.1	Management der Netzsicherheit.....	21
13.1.1	Maßnahmen für Netze	21

13.1.2	Sicherheit von Netzdiensten.....	21
13.1.3	Trennung in Netzwerken.....	21
13.2	Informationsübertragung	21
14	Anschaffung, Entwicklung und Instandhaltung von Systemen.....	21
14.1	Sicherheitsanforderungen von Informationssystemen	21
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen.....	21
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzen	22
14.1.3	Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten	22
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen.....	22
14.2.1	Leitlinie für sichere Entwicklung.....	22
14.2.2	Änderungskontrollverfahren.....	22
14.2.3	Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform	22
14.2.4	Einschränkung von Änderungen an Softwarepaketen	22
14.2.5	Leitlinien zur sicheren Systementwicklung	22
14.2.6	Sichere Entwicklungsumgebung.....	22
14.2.7	Ausgelagerte Entwicklung.....	22
14.2.8	System Sicherheitsprüfungen	22
14.2.9	Systemabnahmeprüfung.....	23
14.3	Prüfdaten.....	23
15	Lieferantenbeziehungen	23
15.1	Informationssicherheit bei Lieferantenbeziehungen	23
15.1.1	Informationssicherheitsleitlinie für Lieferantenbeziehungen.....	23
15.1.2	Sicherheitsthemen in Lieferantenverträgen	23
15.1.3	Lieferkette für Informations- und Kommunikationstechnologie.....	23
15.2	Management der Dienstleistungserbringung durch Lieferanten	23
16	Umgang mit Informationssicherheitsvorfällen.....	24
16.1	Umgang mit Informationssicherheitsvorfällen und Verbesserungen	24
16.1.1	Verantwortlichkeiten und Verfahren	24
16.1.2	Melden von Informationssicherheitsereignissen.....	24
16.1.3	Meldung von Informationssicherheitsschwachstellen.....	24
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse.....	24
16.1.5	Reaktion auf Informationssicherheitsvorfälle	24
16.1.6	Lernen von Informationssicherheitsvorfällen	25
16.1.7	Sammeln von Beweisen.....	25
17	Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs.....	25
17.1	Aufrechterhaltung der Informationssicherheit	25
17.1.1	Planung der Aufrechterhaltung der Informationssicherheit.....	25
17.1.2	Implementierung von Verfahren zur Aufrechterhaltung der Informationssicherheit	26
17.1.3	Überprüfung, Überarbeitung und Auswertung von Maßnahmen zur Aufrechterhaltung der Informationssicherheit.....	26
17.1.4	Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs	26
17.2	Redundanzen	26
18	Einhaltung von Vorgaben	27
18.1	Einhaltung gesetzlicher und vertraglicher Anforderungen.....	27
18.1.1	Feststellung anwendbarer Gesetze und vertraglicher Anforderungen.....	27
18.1.2	Rechte an geistigem Eigentum.....	27
18.1.3	Schutz von Aufzeichnungen	27
18.1.4	Privatsphäre und Schutz von personenbezogenen Informationen	27
18.1.5	Leitlinien zu kryptografischen Maßnahmen	27
18.2	Informationssicherheitsprüfungen	27
18.2.1	Unabhängige Überprüfung der Informationssicherheit	27
18.2.2	Einhaltung von Sicherheitsleitlinien und -standards	27
18.2.3	Technische Konformitätsprüfung	27

Anhang A (informativ) Zusätzliche, auf das Flugverkehrsmanagement bezogene Anleitung	28
A.1 Bewertung von Informationssicherheitsrisiken	28
A.1.1 Internes Informationssicherheitsrisiko-Management.....	28
A.2 Probleme der Interoperabilität von Risikobewertungen	32
A.2.1 Allgemeines	32
A.2.2 Management der Informationssicherheit für mehrere Organisationen.....	32
A.2.3 Anpassung des Sicherheits- und Sicherheitsrisikomanagements.....	33
A.3 Auswahl von Maßnahmen	33
A.4 Vertrauensstufen.....	33
A.4.1 Einleitung	33
A.4.2 Skala der Vertrauensstufen	34
A.4.3 Klassifizierungskriterien.....	35
A.5 Bericht über die Anwendbarkeit.....	35
A.6 Messung und Auditierung der Sicherheit.....	35
Anhang B (informativ) Beispiele für die Umsetzung.....	36
B.1 Allgemeines	36
B.2 Sicherheit von Informationen in Webanwendungen und Webdiensten (LoT-A-WEB)	37
B.2.1 Allgemeines	37
B.2.2 Parameter für die Vertrauensstufe einer Webanwendung/eines Webdienstes	37
B.2.3 Ermittlung der Vertrauensstufe der Webanwendung/des Webdienstes (LoT-A-WEB)	37
B.2.4 Folgen.....	38
B.3 Organisationsübergreifende Verbindungen/externe Verbindungen (LoT-A-NET)	39
B.3.1 Ermittlung der notwendigen Schutzmaßnahmen	39
B.3.2 Auswirkungen der Kopplung von Netzwerken	44
B.4 Zertifikate/Public-Key-Infrastruktur (LoT-A-PKI).....	45
B.4.1 Parameter für die Vertrauensstufe des Zertifikatsmanagements	45
B.4.2 Ermittlung der Vertrauensstufe des Zertifikatsmanagements (LoT-A-PKI)	45
B.4.3 Auswirkungen: Anerkennung von Zertifikaten/PKI	45
B.5 Identitätsmanagement (LoT-A-IDM).....	46
B.5.1 Parameter für die Bestimmung der Vertrauensstufe des Identitätsmanagements	46
B.5.2 Ermittlung der Vertrauensstufe des Identitätsmanagements (LoT-A-IDM)	46
B.5.3 Auswirkungen: Anerkennung von Identitäten.....	47
Anhang C (informativ) Vertrauensstufe — Beispiel für die Umsetzung	48
Anhang D (informativ) Anwendung von Maßnahmen in einer Kontrollübersicht — Beispiel für die Umsetzung	64
Literaturhinweise.....	69

Europäisches Vorwort

Dieses Dokument (prEN 16495:2018) wurde vom Technischen Komitee CEN/TC 377 „Luftverkehrsmanagement“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN 16495:2014 ersetzen.

Im Vergleich zur Vorgängerausgabe wurden folgende technische Änderungen vorgenommen:

- Angleichung an den Aufbau von ISO/IEC 27002:2013 und ISO/IEC DIS 27009:2015;
- Ratschläge zur Angleichung von Sicherheitsmanagement;
- Ratschläge zur auf die Entwicklung, Produktion und Wartung bezogenen Sicherheit;
- Ratschläge für die Wahrung der Sicherheit;
- Informativer Anhang zu.

Einleitung

Dieses Dokument enthält auf ISO/IEC 27001:2013 „Information technology — Security techniques — Information security management systems — Requirements“ basierende Leitlinien, die auf Sicherheitsmanagementsysteme in Organisationen im Luftverkehrsbereich angewendet werden. Das Ziel dieses Dokuments besteht in der Erweiterung der Inhalte von ISO/IEC 27002:2013 auf den Bereich der Luftfahrt, um damit Luftfahrtorganisationen zu ermöglichen, ein genormtes und spezielles Informationssicherheitsmanagementsystem (ISMS) umzusetzen und um es vom Niveau einer einzelnen Organisation auf das transorganisatorische Niveau zu erweitern.

Zusätzlich zu den in ISO/IEC 27002:2013 aufgeführten Sicherheitszielen und -maßnahmen unterliegt das Sicherheitsmanagement in Organisationen im Luftverkehrsbereich weiteren speziellen Anforderungen: Die Erbringung von Dienstleistungen in der Luftfahrt ist in hohem Maße von der Zusammenarbeit der einzelnen Beteiligten bestimmt. Das Informationssicherheitsmanagement einer Organisation hängt daher vom Informationssicherheitsmanagement derjenigen Organisationen ab, mit denen die betreffende Organisation zur Erbringung von Dienstleistungen zusammenarbeitet. Diese Europäische Norm 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, und
- die Übereinstimmung hinsichtlich der erforderlichen Sicherheitskontrollen und ihrer Umsetzung.

1 Anwendungsbereich

Diese Europäische Norm legt Leitlinien und allgemeine Grundsätze für die Umsetzung eines Informationssicherheits-Managementsystems in Organisationen im Bereich der Zivilluftfahrt fest.

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

Für die Zwecke dieser Europäischen Norm wird Flugverkehrsmanagement als funktioneller Begriff betrachtet, der die Verantwortlichkeiten aller an der Wertschöpfungskette im Luftverkehr Beteiligten abdeckt. Das betrifft Luftraumnutzer, Flughäfen und Flugsicherungsorganisationen, ist jedoch nicht allein darauf beschränkt.

Grundlage für alle Anforderungen in dieser Europäischen Norm 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*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*

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

**3.1
Flugverkehrsmanagement**
Funktionssystem, 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

3.2

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.

4 Informationssicherheitsmanagement in der Luftfahrt

4.1 Aufbau dieser Europäischen Norm

Der Aufbau dieser Europäischen Norm ist an ISO/IEC 27002 angepasst. In allen Fällen, in denen die Maßnahmen nach ISO/IEC 27002 ohne Änderung oder Ergänzung angewendet werden können, wird lediglich auf ISO/IEC 27002 verwiesen:

- in allen Fällen, in denen die Umsetzung von Maßnahmen nach ISO/IEC 27002 eine für die Luftfahrt spezielle Ergänzung erfordert, wurde das direkt in den betreffenden Abschnitt aufgenommen;
- Umsetzungsbeispiele für besondere Anwendungsbereiche sind im (informativen) Anhang A beschrieben. Das betrifft folgende Bereiche:
- Sicherheit von Informationen in Web-Anwendungen und Web-Diensten;
- Verbindungen zwischen mehreren Organisationen/externe Verbindungen;
- Zertifikate/Infrastruktur mit öffentlichem Schlüssel (en: Public Key Infrastructure);
- Identitätsmanagement.

4.2 Auf ISO/IEC 27001:2013 bezogene luftverkehrsspezifische Anforderungen

ISO/IEC 27001:2013 Die Anforderungen zu 4.2 „Verständnis der Bedürfnisse und Erwartungen interessierter Parteien“ werden durch eine Anmerkung geändert:

Interessierte Parteien umfassen andere Organisationen mit Schnittstellen zur Organisation, die Netzwerkverbindungen und/oder den Daten- und/oder Informationsaustausch

ISO/IEC 27001:2013 Die Anforderungen zu 5.3 „Organisatorische Aufgaben, Zuständigkeiten und Befugnisse“ werden wie folgt geändert:

Die oberste Leitung muss die Nahtlosigkeit des Informationssicherheitsmanagements innerhalb der eigenen Organisation einschließlich transorganisatorischer Prozessen sicherstellen.

ISO/IEC 27001:2013 Die Anforderungen zu 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen“ werden durch einen neuen Unterabschnitt 6.1.4 „Teilen von Informationen zum Informationssicherheitsrisiko“ geändert:

Die Organisation muss das aufgrund von externen Netzwerkverbindungen und/oder dem Daten- und/oder Informationsaustausch das Risiko beurteilen, indem

- a) Informationsflüsse über externe Schnittstellen mit anderen Organisationen identifiziert werden,
- b) die Ströme und Schnittstellen eingeschlossen werden, die explizit in der in 6.1.2 beschriebenen Risiko-beurteilung enthalten sind,

- c) Informationen zur Risikobeurteilung und Risikobehandlung als Eingabe zur Risikobeurteilung von der/den Organisation(en) erhalten, die die externe Schnittstelle teilen und die Informationen kontrollieren, die sie überschreiten, und
- d) entsprechende in 6.1.2 erstellte Informationen zur Risikobeurteilung und in 6.1.3 erstellte Informationen zur Risikobehandlung mit Organisationen, die die externe Schnittstelle teilen, ausgetauscht werden.

ISO/IEC 27001:2013 Die Anforderungen zu 6.1.2 c) zu „Informationssicherheitsrisikoeinschätzung“ werden durch einen dritten Punkt geändert:

Identifizieren von Systemschnittstellen mit anderen Organisationen, die Netzwerkverbindungen und/oder den Daten- und/oder Informationsaustausch umfassen, der für die Organisation ein Risiko darstellen kann.

Es wird eine Verweisung auf 27001:2013, 6.1.2 c) 3) bis 6.1.2 d) 1) und 2) hinzugefügt.

ISO/IEC 27001:2013 Die Anforderungen zu 7.4 „Kommunikation“ werden durch die folgende Anmerkung präzisiert

Es wird einen Bedarf an externer Kommunikation mit Organisationen geben, mit denen die Organisation wie in 6.1.4 beschrieben Daten und/oder Informationen und/oder Netzwerkverbindungen teilt.

ISO/IEC 27001:2013 Die Anforderungen zu 8.2 „Informationssicherheitsrisikoeinschätzung“ werden wie folgt geändert:

Die Organisation muss entsprechende Informationen zur Risikoeinschätzung mit Organisationen teilen, mit denen sie wie in 6.1.4 beschrieben Daten und/oder Informationen und/oder Netzwerkverbindungen teilt.

ISO/IEC 27001:2013 Die Anforderungen zu 8.3 „Informationssicherheitsrisikobehandlung“ werden wie folgt geändert:

Die Organisation muss entsprechende Risikobehandlungsinformationen mit Organisationen erstellen, mit denen sie wie in 6.1.4 beschrieben Daten und/oder Informationen und/oder Netzwerkverbindungen teilt.

5 Informationssicherheitsleitlinien

5.1 Managementausrichtung zur Informationssicherheit

5.1.1 Informationssicherheitsleitlinien

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 5.1.2.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

6.1.1 Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 6.1.1

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

6.1.2 Aufgabentrennung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 6.1.2.

6.1.3 Kontakt zu Behörden

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 mit dem Schutz kritischer Infrastrukturen auf nationaler und Europäischer Ebene beschäftigen.

6.1.4 Kontakt mit Interessengruppen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 6.1.4

Die Organisation sollte eine Schnittstelle zu anderen Organisationen herstellen.

Die Kontakte sollten ebenfalls die Bedürfnisse und Erwartungen von interessierten Parteien, insbesondere Organisationen in Betracht ziehen, mit denen die Organisation Informationssicherheitsrisiken in Bezug auf die Schaffung oder den Beitrag zu Sicherheitsrisiken im Luftverkehr und deren Management teilt.

Die Schaffung von formellen Schnittstellen zu kritischen Organisationen sollten 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 ISO/IEC 27002:2013, 6.1.5, empfohlenen Maßnahmen gelten entsprechend.

6.2 Mobilgeräte und Telearbeit

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 6.2.

7 Personalsicherheit

7.1 Vor der Anstellung

7.1.1 Überprüfung

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 Überprüfung 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.

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

7.1.2 Arbeitsvertragsklauseln

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 7.1.2.

7.2 Während der Anstellung

7.2.1 Verantwortung des Managements

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 7.2.1.

7.2.2 Sensibilisierung, Aus- und Weiterbildung zur Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 Disziplinarverfahren

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 7.2.3.

7.3 Beendigung und Wechsel der Anstellung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 7.3.

8 Management von organisationseigenen Werten

8.1 Verantwortung für organisationseigene Werte

8.1.1 Inventar der organisationseigenen Werte

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 8.1.1

Das Inventar der organisationseigenen Werte sollte an Inventare angeglichen werden, die Konfigurationsinformationen für alle informationsverarbeitenden Werte bereitstellen, einschließlich Software-Patching-Ebenen.

8.1.2 Eigentum von organisationseigenen Werten

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 organisationseigenen Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 8.1.3.

8.1.4 Rückgabe von organisationseigenen Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 8.1.4.

8.2 Klassifizierung von Informationen

8.2.1 Klassifizierung von Informationen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 8.2.1

Um eine organisationsübergreifende Vergleichbarkeit sicherzustellen, sollte die Organisation Informationen, die in übergreifenden Geschäftsprozessen benutzt 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 zieht

Intern: Informationen, deren Bekanntwerden einen geringen bis mittleren Schaden für den Geschäftsprozess/die beteiligten Organisationen nach sich zieht

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 Informationen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 8.2.2.

8.2.3 Handhabung von organisationseigenen Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 8.2.3.

8.3 Handhabung von Speicher- und Aufzeichnungsmedien

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 8.3.

9 Zugangskontrolle

9.1 Geschäftsanforderungen für Zugangskontrolle

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.1.

9.2 Benutzerverwaltung

9.2.1 An- und Abmeldung von Benutzern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.2.1.

9.2.2 Zugangsbereitstellung für Benutzer

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.2.2.

9.2.3 Verwaltung von Sonderzugangsrechten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.2.3.

9.2.4 Verwaltung geheimer Authentisierungsdaten von Benutzern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.2.4.

9.2.5 Überprüfung von Benutzerberechtigungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.2.5.

9.2.6 Entziehung oder Anpassung von Zugangsrechten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.2.6.

9.2.7 Digitales Identitätsmanagement

Zusätzliche Maßnahme für ISO/IEC 27002:2013, 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 Identitäts-Management 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 müssen, 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 ISO/IEC 27002:2013, 9.2

Steuerungsmaßnahme

Im organisationsübergreifenden Identitätsmanagement sollten die Entitäten einheitlich dargestellt werden.

Anleitung für die Umsetzung

Im organisationsübergreifenden Identitätsmanagement sollten folgende Entitäten betrachtet werden:

- Menschen;
- 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 Benutzerverantwortung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.3.

9.4 Kontrolle des Zugangs zu Systemen und Anwendungen

9.4.1 Einschränkung von Informationszugriffen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.4.1.

9.4.2 Verfahren für sichere Anmeldung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.4.2.

9.4.3 Systeme zur Verwaltung von Passwörtern

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.4.3.

9.4.4 Verwendung von Systemwerkzeugen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.4.4.

9.4.5 Zugangskontrolle zum Programm Quellcode

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 9.4.5.

9.4.6 Web Application Firewalls

Zusätzliche Maßnahme für ISO/IEC 27002:2013 9.4

Diese zusätzliche Maßnahme bildet keinen Bestandteil der Norm ISO/IEC 27002:2013.

Ziel: Zum Schutz von bereits fertiggestellten produktiven Web-Applikationen gegen äußere Angreifer.

Die Organisation sollte zum Schutz von Web-Anwendungen Web Application Firewalls einsetzen.

Anleitung für die Umsetzung

Um versuchte Angriffe auf Web-Anwendungen vorausschauend erkennen, protokollieren und abblocken zu können, sollte die nachstehende Anleitung für die Umsetzung befolgt werden:

- eine Basis von Signaturen (oder 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 Web-Anwendung 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 erkennen und blockieren zu können.

10 Kryptografie

10.1 Kryptografische Maßnahmen

10.1.1 Leitlinie für die Anwendung kryptografischer Maßnahmen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 10.1.1.

10.1.2 Verwaltung kryptografischer Schlüssel

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 10.1.2

Die Organisation sollte ein zentrales Zertifikats-Managementsystem betreiben, welches 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) (en: Certificate Policy);
- Erklärung zum Zertifizierungsbetrieb (CPS) (en: Certificate Practice Statement).

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 Sicherheitszonen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 11.1.1

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

11.1.2 Physische Zutrittskontrollen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.1.2

11.1.3 Sicherung von Büros, Räumen und Einrichtungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.1.3

11.1.4 Schutz vor Bedrohungen von außen und aus der Umgebung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.1.4

11.1.5 Arbeiten in Sicherheitsbereichen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.1.5

11.1.6 Anlieferungs- und Ladezonen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.1.6

11.2 Betriebsmittel

11.2.1 Platzierung und Schutz von Betriebsmitteln

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 11.2.1

Ausrüstungen, die in öffentlich zugängigen 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 Unterstützende Versorgungseinrichtungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.2.

11.2.3 Sicherheit der Verkabelung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.3.

11.2.4 Instandhaltung von Gerätschaften

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.4.

11.2.5 Entfernung von Werten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.5.

11.2.6 Sicherheit von Betriebsmitteln und Werten außerhalb der Betriebsgebäude

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.6.

11.2.7 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.7.

11.2.8 Unbeaufsichtigte Benutzerausstattung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.8.

11.2.9 Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 11.2.9.

12 Betriebssicherheit

12.1 Betriebliche Verfahren und Verantwortlichkeiten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.1.

12.2 Schutz vor Malware

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.2.

12.3 Backup

12.3.1 Datensicherungen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 12.3.1

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

12.4 Protokollierung und Überwachung

12.4.1 Ereignisprotokollierung

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 12.4.1

Alle Luftverkehrsnetze und Informationssysteme, die für die Sicherheit des Luftverkehrs kritisch sind 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 ISO/IEC 27002:2013, 12.4.2.

12.4.3 Administrator- und Betreiberprotokolle

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.4.3.

12.4.4 Zeitsynchronisierung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.4.4.

12.5 Kontrolle von Software im Betrieb

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.5.

12.6 Umgang mit technischen Schwachstellen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.6.

12.7 Überlegungen zu Audits von Informationssystemen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 12.7.

13 Sicherheit in der Kommunikation

13.1 Management der Netzsicherheit

13.1.1 Maßnahmen für Netze

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 Netzdiensten

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 13.1.2

Die Netzwerkarchitektur muss 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 ISO/IEC 27002:2013, 13.1.3.

13.2 Informationsübertragung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 13.2.

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

14.1 Sicherheitsanforderungen von Informationssystemen

14.1.1 Analyse und Spezifikation von Informationssicherheitsanforderungen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 müssen 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 Netzen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.1.2.

14.1.3 Schutz von Transaktionen im Zusammenhang mit Anwendungsdiensten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.1.3.

14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen

14.2.1 Leitlinie für sichere Entwicklung

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 14.2.1

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

14.2.2 Änderungskontrollverfahren

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.2.

14.2.3 Technische Prüfung von Anwendungen nach Wechseln der Betriebsplattform

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.3.

14.2.4 Einschränkung von Änderungen an Softwarepaketen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.4.

14.2.5 Leitlinien zur sicheren Systementwicklung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.5.

14.2.6 Sichere Entwicklungsumgebung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.6.

14.2.7 Ausgelagerte Entwicklung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.7.

14.2.8 Systemsicherheitsprüfungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.2.8.

14.2.9 Systemabnahmeprüfung

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 Prüfdaten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 14.3.

15 Lieferantenbeziehungen

15.1 Informationssicherheit bei Lieferantenbeziehungen

15.1.1 Informationssicherheitsleitlinie für Lieferantenbeziehungen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 unabhängige Überprüfung unterzogen werden.

15.1.2 Sicherheitsthemen in Lieferantenverträgen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 15.1.2.

15.1.3 Lieferkette für Informations- und Kommunikationstechnologie

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 15.1.3.

15.2 Management der Dienstleistungserbringung durch Lieferanten

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 15.2.

16 Umgang mit Informationssicherheitsvorfällen

16.1 Umgang mit Informationssicherheitsvorfällen und Verbesserungen

16.1.1 Verantwortlichkeiten und Verfahren

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 16.1.1

Verfahren für Sicherheitsvorfälle sollten regelmäßig geprüft werden, um ihre Genauigkeit sicherzustellen und das Bewusstsein der Verantwortlichkeit 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 Melden von Informationssicherheitsereignissen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden.

Eine angemessene Reaktionszeit der Arbeitsgruppe sollte sichergestellt sein.

16.1.3 Meldung von Informationssicherheitsschwachstellen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 privatrechtlichen 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 ISO/IEC 27002:2013, 16.1.4

16.1.5 Reaktion auf Informationssicherheitsvorfälle

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 16.1.5

16.1.6 Lernen von Informationssicherheitsvorfällen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 16.1.6

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

16.1.7 Sammeln von Beweisen

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 16.1.7

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

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

17 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs

17.1 Aufrechterhaltung der Informationssicherheit

17.1.1 Planung der Aufrechterhaltung der Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 17.1.1

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

Zusätzliche Informationen zu ISO/IEC 27002:2013, 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 Implementierung von Verfahren zur Aufrechterhaltung der Informationssicherheit

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 17.1.2.

17.1.3 Überprüfung, Überarbeitung und Auswertung von Maßnahmen zur Aufrechterhaltung der Informationssicherheit

Zusätzliche Anleitung zur Umsetzung für ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 17.2.

18 Einhaltung von Vorgaben

18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen

18.1.1 Feststellung anwendbarer Gesetze und vertraglicher Anforderungen

Zusätzliche Maßnahme für ISO/IEC 27002:2013, 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 ISO/IEC 27002:2013, 18.1.1

Verpflichtungen zum Schutz kritischer Infrastrukturen auf nationaler und Europäischer Ebene könnten betrachtet werden.

18.1.2 Rechte an geistigem Eigentum

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 18.1.2.

18.1.3 Schutz von Aufzeichnungen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 18.1.3.

18.1.4 Privatsphäre und Schutz von personenbezogenen Informationen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 18.1.4.

18.1.5 Leitlinien zu kryptografischen Maßnahmen

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 18.1.5.

18.2 Informationssicherheitsprüfungen

18.2.1 Unabhängige Überprüfung der Informationssicherheit

Zusätzliche Maßnahme für ISO/IEC 27002:2013, 18.2.1

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

18.2.2 Einhaltung von Sicherheitsleitlinien und -standards

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 18.2.2.

18.2.3 Technische Konformitätsprüfung

Keine zusätzlichen, für Organisationen des Luftverkehrs speziellen Informationen zu ISO/IEC 27002:2013, 18.2.3.

Anhang A (informativ)

Zusätzliche, auf das Flugverkehrsmanagement bezogene Anleitung

A.1 Bewertung von Informationssicherheitsrisiken

A.1.1 Internes Informationssicherheitsrisiko-Management

Um ihre eigene Sicherheitslage verstehen zu können, muss eine Organisation die Sicherheitslage ihrer Partner kennen.

Die Herstellung von Netzverbindungen und der Austausch von Daten beruht 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 4.5 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.

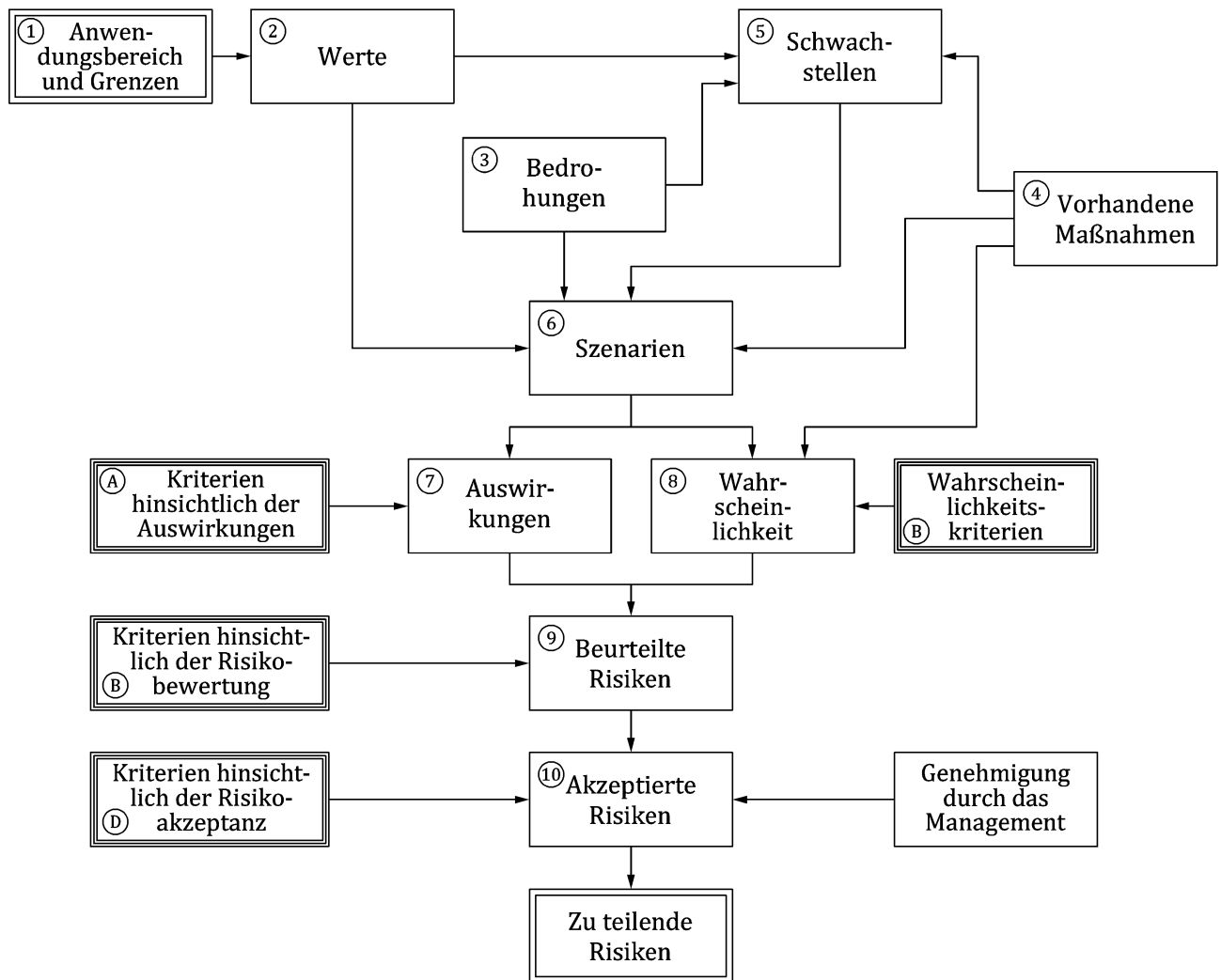
Es muss betont werden, dass das nicht bedeutet, dass die Organisation alles über die Sicherheit ihrer Partner wissen muss. Es werden lediglich genügend Informationen benötigt, um auf der Grundlage von Risikobewertungen das erforderliche Maß an Gewissheit zu erlangen.

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 A entnommen werden.

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

Der zugrunde liegende Prozess der Risikobewertung ist mit ISO/IEC 27005:2011 verträglich. Das 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

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 Szenarium 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.

- 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.

- 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 risikobewertet werden müssen sowie eine Auflistung von Geschäftsprozessen, die sich auf die Werte und ihre Relevanz zusammen mit den entsprechenden Eigentümern der Werte beziehen.

- 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.

— 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.

— 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 so genannten 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.

— 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.

— Bewertung von Folgen:

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

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

— Bewertung des Ausmaßes der Bedrohung:

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

Ergebnisse: Wahrscheinlichkeit von Bedrohungsszenarien (quantitativ und qualitativ).

— 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.

— 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.

— 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 können ebenso relevant sein, da es selbst bei gleichen zugrunde liegenden Verfahren vorkommen kann, dass Themen/Begriffe/Benennungen unterschiedlichen 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 zu verweisenden Karte zur Verfügung;

- 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, und
- 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 Auswahl von Maßnahmen

Maßnahmen sollten in Übereinstimmung mit den Ergebnissen der Informationssicherheitsrisikobewertung ausgewählt und umgesetzt werden:

- Maßnahmen nach ISO/IEC 27002;
- Maßnahmen, die die in ISO/IEC 27002 angegebenen ergänzen. Diese Maßnahmen sind in dieser Europäischen Norm als für die 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 Gewährleistung 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) (en: Level of Trust of the organisation) 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 verwendet:

- 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

Organisationen werden unter bestimmten Umständen den Zugriff von Partnerorganisationen mit LT1-Einstufung auf eigene Anwendungen nach dem „Need-to-have-Prinzip“ gestatten, 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.

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

d) Vertrauensstufe 2

Die Kategorie „Vertrauensstufe 2“ (LT2, en: Limited Trust 3) bezeichnet Drittpartei-Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein hohes Gesamtniveau an Informationssicherheit erreichen.

BEISPIEL 2 Kopplung von Netzwerken

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

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

Organisationen werden unter bestimmten Umständen den Zugriff von Partnern mit LT3-Einstufung auf eigene Anwendungen nach dem „Need-to-have-Prinzip“ gestatten, aber vor dem Verbindungsaufbau an der Netzwerkgrenze (z. B. an der Firewall) sowohl eine explizite Authentisierung fordern 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, welche 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 ISO/IEC 27001:2013, 6.1.3 d), aufstellen. Der „Bericht über die Anwendbarkeit“ sollte einem Partner, wenn nötig, 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.

Anhang B (informativ)

Beispiele für die Umsetzung

B.1 Allgemeines

Anhang A 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.

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

Maßnahmen	LT0	LT1	LT2	LT3
5. Informationssicherheitsleitlinien	vorgeschrieben	vorgeschrieben	vorgeschrieben	vorgeschrieben
6. Organisation der Informationssicherheit	vorgeschrieben	überwiegend	überwiegend	teilweise
7. Personalsicherheit	vorgeschrieben	überwiegend	überwiegend	teilweise
8. Management von organisations-eigenen Werten	vorgeschrieben	vorgeschrieben	—	—
9. Zugangskontrolle	vorgeschrieben	überwiegend	teilweise	teilweise
10. Kryptografie	vorgeschrieben	vorgeschrieben	—	—
11. Physische und umgebungsbezogene Sicherheit	vorgeschrieben	überwiegend	teilweise	—
12. Betriebssicherheit	vorgeschrieben	überwiegend	teilweise	teilweise
13. Sicherheit in der Kommunikation	vorgeschrieben	überwiegend	teilweise	teilweise
14. Anschaffung, Entwicklung und Instandhaltung von Systemen	vorgeschrieben	teilweise	teilweise	—
15. Lieferantenbeziehungen	vorgeschrieben	überwiegend	teilweise	—
16. Umgang mit Informationssicherheitsvorfällen	vorgeschrieben	überwiegend	überwiegend	—
17. Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs	vorgeschrieben	teilweise	teilweise	—
18. Einhaltung von Vorgaben	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 (Minimumprinzip).

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 entsprechenden Sicherheitsmaßnahmen sind entsprechend anzuwenden.

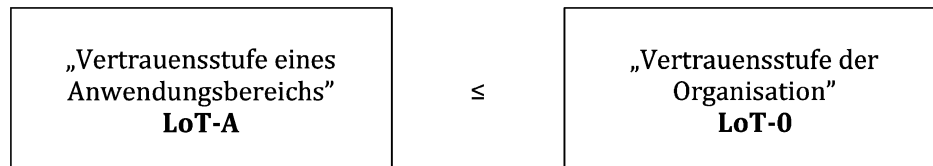


Bild B.1 — LoT-A gegenüber LoT-O

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 gewährleistet 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 nach dem OWASP;
- 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 Web-Dienstes wird nach Tabelle B.2 ermittelt.

Tabelle B.2 — Vertrauensstufe einer Webanwendung/eines Webdienstes

Nr.	Leitlinie für Web-Anwendungen/Web-Dienste	Entwicklung von Webanwendungen nach dem OWASP	Code Reviews	Kompetenz von Entwicklern von Anwendungen	Penetrationsprüfungen von Anwendungen	Penetrationsprüfungen von Infrastrukturen	Web App-lication 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.

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.

B.3.1 Ermittlung der notwendigen Schutzmaßnahmen

B.3.1.1 Allgemeines

Die Maßnahmen, die zum Schutz von externen Verbindungen zu organisationsinternen Systemen umzusetzen sind, sollten nach dem in Bild B.2 dargestellten Prozess ermittelt werden.

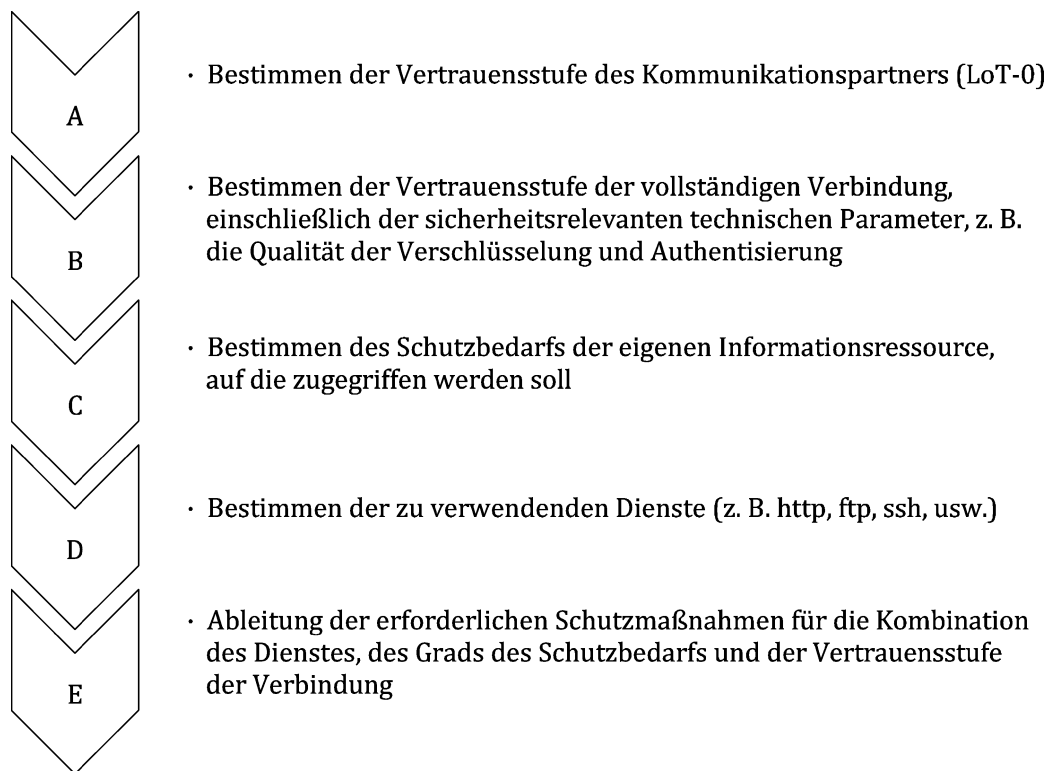


Bild B.2 — Prozess zur Umsetzung des Schutzes von internen Verbindungen

A) Bestimmen der Vertrauensstufe des Kommunikationspartners (LoT-0)

Die Vertrauensstufe sollte nach den in A.4 beschriebenen Regeln bestimmt werden.

B) Bestimmen der Vertrauensstufe der Verbindung (LoT-A-NET)

Die Vertrauensstufe der Verbindung sollte auf der Grundlage der folgenden Parameter bestimmt werden.

C) Bestimmen des Schutzbedarfs der eigenen Informationsressource, auf die zugegriffen werden soll

Der Schutzbedarf der eigenen Informationsressource sollte nach A.1.1 bestimmt werden.

D) Bestimmen der zu verwendenden Dienste

Der Dienst muss aus der angestrebten Verbindung ersichtlich sein.