

**DELEGIERTE VERORDNUNG (EU) 2022/1645 DER KOMMISSION****vom 14. Juli 2022**

**zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission**

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates vom 4. Juli 2018 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Agentur der Europäischen Union für Flugsicherheit sowie zur Änderung der Verordnungen (EG) Nr. 2111/2005, (EG) Nr. 1008/2008, (EU) Nr. 996/2010, (EU) Nr. 376/2014 und der Richtlinien 2014/30/EU und 2014/53/EU des Europäischen Parlaments und des Rates, und zur Aufhebung der Verordnungen (EG) Nr. 552/2004 und (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates und der Verordnung (EWG) Nr. 3922/91 des Rates <sup>(1)</sup>, insbesondere auf Artikel 19 Absatz 1 Buchstabe g und Artikel 39 Absatz 1 Buchstabe b,

in Erwägung nachstehender Gründe:

- (1) Gemäß den grundlegenden Anforderungen in Anhang II Nummer 3.1 Buchstabe b der Verordnung (EU) 2018/1139 müssen Entwicklungs- und Herstellungsorganisationen für das Management von Sicherheitsrisiken ein Managementsystem einführen und aufrechterhalten.
- (2) Gemäß den grundlegenden Anforderungen in Anhang VII Nummern 2.2.1 und 5.2 der Verordnung (EU) 2018/1139 müssen Flughafenbetreiber und für Vorfeldkontrolldienste zuständige Organisationen für das Management von Sicherheitsrisiken ein Managementsystem einführen und aufrechterhalten.
- (3) Die in den Erwägungsgründen 1 und 2 genannten Sicherheitsrisiken können aus verschiedenen Quellen herrühren, darunter Anfälligkeiten in der Konstruktion oder bei der Instandhaltung, Aspekte der menschlichen Leistungsfähigkeit, Bedrohungen durch das Umfeld und Bedrohungen der Informationssicherheit. Daher sollten die in den Erwägungsgründen 1 und 2 genannten und von den Organisationen eingerichteten Managementsysteme nicht nur Sicherheitsrisiken berücksichtigen, die sich aus zufälligen Ereignissen ergeben, sondern auch sich aus Bedrohungen der Informationssicherheit ergebende Sicherheitsrisiken, bei denen bestehende Anfälligkeiten von Personen mit böswilliger Absicht ausgenutzt werden können. Diese Risiken für die Informationssicherheit nehmen in der Zivilluftfahrt ständig zu, da die derzeitigen Informationssysteme immer stärker vernetzt werden und immer häufiger zum Angriffsziel böswilliger Akteure werden.
- (4) Die mit diesen Informationssystemen verbundenen Risiken beschränken sich nicht auf mögliche Angriffe im Cyberraum, sondern umfassen auch Bedrohungen, die Prozesse und Verfahren sowie die menschliche Leistungsfähigkeit beeinträchtigen können.
- (5) Eine beträchtliche Anzahl von Organisationen wendet bereits internationale Normen wie ISO 27001 an, um die Sicherheit digitaler Informationen und Daten zu verbessern. Allerdings berücksichtigen diese Normen möglicherweise nicht alle Besonderheiten der Zivilluftfahrt.
- (6) Daher sollten Anforderungen für das Management von sich potenziell auf die Flugsicherheit auswirkenden Informationssicherheitsrisiken eingeführt werden.
- (7) Angesichts des hochgradig vernetzten Luftfahrtsystems kommt es darauf an, dass diese Anforderungen die verschiedenen Bereiche der Luftfahrt und deren Schnittstellen abdecken. Daher sollten sie für alle Organisationen gelten, die bereits jetzt über ein Managementsystem im Einklang mit den geltenden Rechtsvorschriften der Union im Bereich der Flugsicherheit verfügen müssen.
- (8) Die in dieser Verordnung festgelegten Anforderungen sollten in allen Bereichen der Luftfahrt einheitlich angewandt werden und sich dabei nur geringfügig auf die bereits für diese Bereiche geltenden Rechtsvorschriften der Union im Bereich der Flugsicherheit auswirken.

<sup>(1)</sup> ABl. L 212 vom 22.8.2018, S. 1.

- (9) Die in dieser Verordnung festgelegten Anforderungen sollten die in Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998 der Kommission <sup>(2)</sup> und in Artikel 14 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates <sup>(3)</sup> festgelegten Anforderungen an die Informationssicherheit und die Cybersicherheit unberührt lassen.
- (10) Die für die Zwecke dieses Rechtsakts verwendete Definition der Informationssicherheit sollte nicht so ausgelegt werden, dass sie von der Begriffsbestimmung der Sicherheit von Netz- und Informationssystemen in der Richtlinie (EU) 2016/1148 abweicht.
- (11) Um Überschneidungen bei den rechtlichen Anforderungen zu vermeiden, sollte in Fällen, in denen unter diese Verordnung fallende Organisationen bereits bestimmten Sicherheitsanforderungen unterliegen, die sich aus anderen in Erwägungsgrund 9 genannten Rechtsakten der Union ergeben und die in ihrer Wirkung den Bestimmungen dieser Verordnung gleichwertig sind, die Einhaltung jener Sicherheitsanforderungen als Erfüllung der in dieser Verordnung festgelegten Anforderungen gelten.
- (12) Unter diese Verordnung fallende Organisationen, die bereits den Sicherheitsanforderungen der Durchführungsverordnung (EU) 2015/1998 unterliegen, sollten auch die Anforderungen von Anhang I (Teil IS.D.OR.230 „Informationssicherheitssystem für externe Meldungen“) dieser Verordnung erfüllen, da die Verordnung (EU) 2015/1998 keine Bestimmungen über die externe Meldung von Störungen der Informationssicherheit enthält.
- (13) Zur Verknüpfung der in den oben genannten Verordnungen vorgeschriebenen Managementsysteme mit den in dieser Verordnung festgelegten Anforderungen an das Informationssicherheitsmanagement sollten die Verordnungen (EU) Nr. 748/2012 <sup>(4)</sup> und (EU) Nr. 139/2014 <sup>(5)</sup> geändert werden.
- (14) Damit die Organisationen ausreichend Zeit haben, um die Einhaltung der mit dieser Verordnung eingeführten neuen Vorschriften und Verfahren sicherzustellen, sollte die Geltung dieser Verordnung erst nach einem Zeitraum von drei Jahren ab ihrem Inkrafttreten beginnen.
- (15) Die in dieser Verordnung festgelegten Anforderungen beruhen auf der Stellungnahme Nr. 03/2021 <sup>(6)</sup>, die von der Agentur gemäß Artikel 75 Absatz 2 Buchstaben b und c sowie Artikel 76 Absatz 1 der Verordnung (EU) 2018/1139 abgegeben wurde.
- (16) Wie nach Artikel 128 Absatz 4 der Verordnung (EU) 2018/1139 vorgeschrieben, hat die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen konsultiert <sup>(7)</sup> —

HAT FOLGENDE VERORDNUNG ERLASSEN:

#### Artikel 1

#### Gegenstand

In dieser Verordnung werden die Anforderungen festgelegt, die die in Artikel 2 genannten Organisationen erfüllen müssen und zwar im Hinblick die Identifizierung und das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit, die für die Zwecke der Zivilluftfahrt eingesetzte Systeme und Daten der Informations- und Kommunikationstechnik beeinträchtigen könnten, sowie im Hinblick auf die Erkennung von Informationssicherheitsereignissen und die Identifizierung solcher Ereignisse, die als Störungen der Informationssicherheit mit potenziellen Auswirkungen auf die Flugsicherheit gelten, sowie mit Blick auf die Reaktion auf diese und die Wiederherstellung.

<sup>(2)</sup> Durchführungsverordnung (EU) 2015/1998 der Kommission vom 5. November 2015 zur Festlegung detaillierter Maßnahmen für die Durchführung der gemeinsamen Grundstandards für die Flugsicherheit (ABl. L 299 vom 14.11.2015, S. 1).

<sup>(3)</sup> Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1).

<sup>(4)</sup> Verordnung (EU) Nr. 748/2012 der Kommission vom 3. August 2012 zur Festlegung der Durchführungsbestimmungen für die Erteilung von Lufttüchtigkeits- und Umweltzeugnissen für Luftfahrzeuge und zugehörige Produkte, Bau- und Ausrüstungsteile sowie für die Zulassung von Entwicklungs- und Herstellungsbetrieben (ABl. L 224 vom 21.8.2012, S. 1).

<sup>(5)</sup> Verordnung (EU) Nr. 139/2014 der Kommission vom 12. Februar 2014 zur Festlegung von Vorschriften und von Verwaltungsverfahren in Bezug auf Flugplätze gemäß der Verordnung (EG) Nr. 216/2008 des Europäischen Parlaments und des Rates (ABl. L 44 vom 14.2.2014, S. 1).

<sup>(6)</sup> <https://www.easa.europa.eu/document-library/opinions>

<sup>(7)</sup> ABl. L 123 vom 12.5.2016, S. 1.

## Artikel 2

### Geltungsbereich

(1) Diese Verordnung gilt für folgende Organisationen:

- a) Herstellungs- und Entwicklungsorganisationen, für die Anhang I (Teil 21) Hauptabschnitt A Abschnitte G und J der Verordnung (EU) Nr. 748/2012 gilt, mit Ausnahme von Entwicklungs- und Herstellungsorganisationen, die ausschließlich an der Entwicklung und/oder Herstellung von ELA2-Luftfahrzeugen im Sinne des Artikels 1 Absatz 2 Buchstabe j jener Verordnung beteiligt sind.
- b) Flugplatzbetreiber und Anbieter von Vorfeldkontrolldiensten, die Anhang III „Teil Organisatorische Anforderungen (Teil-ADR.OR)“ der Verordnung (EU) Nr. 139/2014 unterliegen.

(2) Diese Verordnung lässt die in Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998 und in Artikel 14 der Richtlinie (EU) 2016/1148 festgelegten Anforderungen an die Informationssicherheit und die Cybersicherheit unberührt.

## Artikel 3

### Begriffsbestimmungen

Für die Zwecke der vorliegenden Verordnung gelten folgende Begriffsbestimmungen:

1. „Informationssicherheit“ (information security): die Wahrung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Netz- und Informationssystemen;
2. „Informationssicherheitsereignis“ (information security event): ein identifizierter System-, Dienst- oder Netzzustand, der auf einen möglichen Verstoß gegen das Informationssicherheitskonzept oder ein Versagen von Informationssicherheitskontrollen oder auf eine bis dahin unbekannte Situation hinweist, die für die Informationssicherheit relevant sein kann;
3. „Störung“ (incident): jedes Ereignis im Sinne des Artikels 4 Nummer 7 der Richtlinie (EU) 2016/1148, das sich nachteilig auf die Sicherheit von Netz- und Informationssystemen auswirkt;
4. „Informationssicherheitsrisiko“ (information security risk): auf ein mögliches Informationssicherheitsereignis zurückzuführendes Risiko für die Organisation des Zivilluftfahrtbetriebs sowie für Vermögenswerte, Privatpersonen und andere Organisationen. Informationssicherheitsrisiken bergen das Potenzial, dass Bedrohungen Schwachstellen eines Informationsbestands oder einer Gruppe von Informationsbeständen ausnutzen;
5. „Bedrohung“ (threat): eine potenzielle Verletzung der Informationssicherheit, die vorliegt, wenn durch eine Einrichtung, einen Umstand, eine Handlung oder ein Ereignis ein Schaden verursacht werden könnte;
6. „Schwachstelle“ (vulnerability): eine Anfälligkeit oder eine Schwäche in einem Bestand oder System, in Verfahren, im Design, in der Umsetzung oder bei Maßnahmen zur Informationssicherheit, die ausgenutzt werden und zu einer Verletzung des Informationssicherheitskonzepts führen könnten.

## Artikel 4

### Anforderungen, die sich aus anderen Rechtsvorschriften der Union ergeben

(1) Erfüllt eine in Artikel 2 genannte Organisation bestimmte Sicherheitsanforderungen, die in Artikel 14 der Richtlinie (EU) 2016/1148 festgelegt und den Anforderungen dieser Verordnung gleichwertig sind, so gilt die Einhaltung jener Sicherheitsanforderungen als Erfüllung der dieser Verordnung festgelegten Anforderungen.

(2) Handelt es sich bei einer in Artikel 2 genannten Organisation um einen Betreiber oder eine Stelle, auf die in den nationalen Luftsicherheitsprogrammen der Mitgliedstaaten nach Artikel 10 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates<sup>(\*)</sup> Bezug genommen wird, so gelten die in Nummer 1.7 des Anhangs der Durchführungsverordnung (EU) 2015/1998 festgelegten Cybersicherheitsanforderungen als gleichwertig mit den Anforderungen dieser Verordnung, mit Ausnahme von Punkt IS.D.OR.230 des Anhangs dieser Verordnung, der eingehalten werden muss.

<sup>(\*)</sup> Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72).

(3) Die Kommission kann nach Konsultation der EASA und der in Artikel 11 der Richtlinie (EU) 2016/1148 genannten Kooperationsgruppe Leitlinien für die Bewertung der Gleichwertigkeit der in dieser Verordnung und der Richtlinie (EU) 2016/1148 festgelegten Anforderungen herausgeben.

#### Artikel 5

##### Zuständige Behörde

(1) Für die Bescheinigung und Überwachung der Einhaltung dieser Verordnung ist folgende Behörde zuständig:

- a) In Bezug auf die in Artikel 2 Buchstabe a genannten Organisationen die gemäß Anhang I (Teil 21) der Verordnung (EU) Nr. 748/2012 benannte zuständige Behörde;
- b) in Bezug auf die in Artikel 2 Buchstabe b genannten Organisationen die gemäß Anhang III (Teil ADR.OR) der Verordnung (EU) Nr. 139/2014 benannte zuständige Behörde.

(2) Die Mitgliedstaaten können für die Zwecke dieser Verordnung eine unabhängige und autonome Stelle benennen, die die zugewiesenen Aufgaben und Zuständigkeiten der in Absatz 1 genannten zuständigen Behörden wahrnimmt. In diesem Fall müssen zwischen dieser Stelle und den in Absatz 1 genannten zuständigen Behörden Koordinierungsmaßnahmen festgelegt werden, damit eine wirksame Aufsicht über alle von der Organisation zu erfüllenden Anforderungen gewährleistet ist.

#### Artikel 6

##### Änderung der Verordnung (EU) Nr. 748/2012

Anhang I (Teil 21) der Verordnung (EU) Nr. 748/2012 wird wie folgt geändert:

1. Das Inhaltsverzeichnis wird wie folgt geändert:

- a) Nach der Überschrift von Punkt 21.A.139 wird die folgende Überschrift eingefügt:

**„21.A.139A Informationssicherheitsmanagementsystem“**

- b) Nach der Überschrift von Punkt 21.A.239 wird die folgende Überschrift eingefügt:

**„21.A.239A Informationssicherheitsmanagementsystem“**

2. Nach Punkt 21.A.139 wird folgender Punkt 21.A.139A eingefügt:

**„21.A.139A Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt 21.A.139 vorgeschriebenen Produktionsmanagementsystem muss die Herstellungsorganisation ein Informationssicherheitsmanagementsystem gemäß der Delegierten Verordnung (EU) 2022/1645 der Kommission (\*) einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist.

---

(\*) Delegierte Verordnung (EU) 2022/1645 der Kommission vom 14. Juli 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission (ABl. L 248 vom 26.9.2022, S. 18).“

3. Nach Punkt 21.A.239 wird folgender Punkt 21.A.239A eingefügt:

**„21.A.239A Informationssicherheitsmanagementsystem**

Zusätzlich zu dem nach Punkt 21.A.239 vorgeschriebenen Konstruktionsmanagementsystem muss die Entwicklungsorganisation ein Informationssicherheitsmanagementsystem gemäß der Delegierten Verordnung (EU) 2022/1645 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist.“

## Artikel 7

**Änderung der Verordnung (EU) Nr. 139/2014**

Anhang III (Teil-ADR.AR) der Verordnung (EU) Nr. 139/2014 wird wie folgt geändert:

1. Nach Punkt ADR.OR.D.005 wird folgender Punkt ADR.OR.D.005A eingefügt:

**„ADR.OR.D.005A Informationssicherheitsmanagementsystem**

Der Flugplatzbetreiber muss ein Informationssicherheitsmanagementsystem gemäß der Delegierten Verordnung (EU) 2022/1645 der Kommission (\*) einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist.

(\*) Delegierte Verordnung (EU) 2022/1645 der Kommission vom 14. Juli 2022 zur Festlegung von Vorschriften für die Anwendung der Verordnung (EU) 2018/1139 des Europäischen Parlaments und des Rates im Hinblick auf die Anforderungen an das Management von Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit für Organisationen, die unter die Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission fallen, und zur Änderung der Verordnungen (EU) Nr. 748/2012 und (EU) Nr. 139/2014 der Kommission (ABl. L 248 vom 26.9.2022, S.18).“

2. Punkt ADR.OR.D.007 erhält folgende Fassung:

**„ADR.OR.D.007 Management von Luftfahrt Daten und Luftfahrtinformationen**

- a) Im Rahmen seines Managementsystems muss der Flugplatzbetreiber ein Qualitätsmanagementsystem einführen und aufrechterhalten, das die folgenden Tätigkeiten umfasst:
1. seine Tätigkeiten in Bezug auf Luftfahrt Daten,
  2. seine Tätigkeiten zur Bereitstellung von Luftfahrtinformationen.
- b) Im Rahmen seines Managementsystems muss der Flugplatzbetreiber ein Sicherheitsmanagementsystem einrichten, mit dem der Schutz der Betriebsdaten, die er erhält oder erzeugt oder auf sonstige Weise nutzt, gewährleistet wird, sodass der Zugang zu diesen Daten auf Befugte beschränkt ist.
- c) Im Sicherheitsmanagementsystem müssen folgende Elemente festgelegt werden:
1. Verfahren zur Beurteilung des Datensicherheitsrisikos und dessen Minderung, zur Überwachung und Erhöhung der Sicherheit, für Sicherheitsüberprüfungen und die Verbreitung der daraus gezogenen Lehren;
  2. die zur Erkennung von Sicherheitsverletzungen und zur Alarmierung des Personals durch geeignete Sicherheitswarnungen vorgesehenen Mittel;
  3. die Mittel zur Beherrschung der Auswirkungen von Sicherheitsverletzungen und zur Ermittlung von Abhilfemaßnahmen und Minderungsverfahren, um eine Wiederholung zu verhindern.
- d) Der Flugplatzbetreiber muss gewährleisten, dass sein Personal im Hinblick auf die Sicherheit der Luftfahrt Daten sicherheitsüberprüft ist.
- e) Die mit der Informationssicherheit zusammenhängenden Aspekte müssen nach Punkt ADR.OR.D.005A geregelt werden.“

3. Nach Punkt ADR.OR.F.045 wird folgender Punkt ADR.OR.F.045A eingefügt:

**„ADR.OR.F.045A Informationssicherheitsmanagementsystem**

Die für die Bereitstellung von AMS verantwortliche Organisation muss ein Informationssicherheitsmanagementsystem gemäß der Delegierten Verordnung (EU) 2022/1645 einrichten, umsetzen und pflegen, damit ein ordnungsgemäßes Management der Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können, gewährleistet ist.“

## Artikel 8

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Sie gilt ab dem 16. Oktober 2025.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

Brüssel, den 14. Juli 2022

*Für die Kommission*  
*Die Präsidentin*  
Ursula VON DER LEYEN

---

## ANHANG

## INFORMATIONSSICHERHEIT — ANFORDERUNGEN AN DIE ORGANISATION

## [TEIL-IS.D.OR]

IS.D.OR.100 Umfang

IS.D.OR.200 Informationssicherheitsmanagementsystem

IS.D.OR.205 Bewertung des Informationssicherheitsrisikos

IS.D.OR.210 Umgang mit dem Informationssicherheitsrisiko

IS.D.OR.215 Informationssicherheitssystem für interne Meldungen

IS.D.OR.220 Störungen der Informationssicherheit — Erkennung, Reaktion und Wiederherstellung

IS.D.OR.225 Reaktion auf die von der zuständigen Behörde gemeldeten Beanstandungen

IS.D.OR.230 Informationssicherheitssystem für externe Meldungen

IS.D.OR.235 Auftragsvergabe für Tätigkeiten des Informationssicherheitsmanagements

IS.D.OR.240 Anforderungen an das Personal

IS.D.OR.245 Führen von Aufzeichnungen

IS.D.OR.250 Handbuch zum Informationssicherheitsmanagement (ISMM)

IS.D.OR.255 Änderungen des Informationssicherheitsmanagementsystems

IS.D.OR.260 Kontinuierliche Verbesserung

**IS.D.OR.100 Umfang**

In diesem Teil werden die Anforderungen festgelegt, die die in Artikel 2 dieser Verordnung genannten Organisationen erfüllen müssen.

**IS.D.OR.200 Informationssicherheitsmanagementsystem (ISMS)**

- a) Damit die in Artikel 1 genannten Ziele erreicht werden, muss die Organisation ein Informationssicherheitsmanagementsystem (ISMS) einrichten, umsetzen und pflegen, mit dem sie Folgendes sicherstellt:
1. Festlegung eines Konzepts für die Informationssicherheit, in der die allgemeinen Grundsätze der Organisation im Hinblick auf die potenziellen Auswirkungen von Informationssicherheitsrisiken auf die Flugsicherheit dargelegt werden;
  2. Identifizierung und Überprüfung von Informationssicherheitsrisiken nach Punkt IS.D.OR.205;
  3. Festlegung und Umsetzung der Maßnahmen für den Umgang mit Informationssicherheitsrisiken nach Punkt IS.D.OR.210;
  4. Umsetzung eines Informationssicherheitssystems für interne Meldungen nach Punkt IS.D.OR.215;
  5. Festlegung und Umsetzung nach Punkt IS.D.OR.220 der zur Erkennung von Informationssicherheitsereignissen notwendigen Maßnahmen, Identifizierung solcher Ereignisse, die als Störungen mit potenziellen Auswirkungen auf die Flugsicherheit gelten, es sei denn, dies ist nach Punkt IS.D.OR.205(e) zulässig, sowie Reaktion auf diese Störungen Informationssicherheit und Wiederherstellung;
  6. Umsetzung der Maßnahmen, die von der zuständigen Behörde als unmittelbare Reaktion auf eine Störung oder Schwachstelle der Informationssicherheit mit Auswirkungen auf die Flugsicherheit gemeldet wurden;
  7. Ergreifung geeigneter Maßnahmen nach Punkt IS.D.OR.225, um den von der zuständigen Behörde mitgeteilten Beanstandungen Rechnung zu tragen;
  8. Umsetzung eines Systems für externe Meldungen nach Punkt IS.D.OR.230, damit die zuständige Behörde geeignete Maßnahmen ergreifen kann;
  9. Erfüllung der Anforderungen von Punkt IS.D.OR.235 für den Fall, dass ein Teil der unter Punkt IS.D.OR.200 genannten Tätigkeiten an andere Organisationen vergeben wird;

10. Erfüllung der Anforderung an das Personal nach Punkt IS.D.OR.240;
  11. Erfüllung der Anforderung an das Führen von Aufzeichnungen nach Punkt IS.D.OR.245;
  12. Überwachung der Einhaltung der Anforderungen dieser Verordnung durch die Organisation und Unterrichtung des leitenden Managers bzw. — im Falle von Entwicklungsorganisationen — des Leiters der Entwicklungsorganisation über Beanstandungen, damit Abhilfemaßnahmen wirksam umgesetzt werden;
  13. Schutz der Vertraulichkeit aller Informationen, die die Organisation möglicherweise von anderen Organisationen erhalten hat, unbeschadet geltender Vorschriften über die Meldung von Störungen und abhängig von deren Sensibilitätsgrad.
- b) Zur kontinuierlichen Einhaltung der in Artikel 1 genannten Anforderungen muss die Organisation nach Punkt IS.D.OR.260 einen Prozess für kontinuierliche Verbesserungen implementieren.
- c) Die Organisation muss nach Punkt IS.D.OR.250 alle wesentlichen Prozesse, Verfahren, Aufgaben und Verantwortlichkeiten dokumentieren, die zur Einhaltung von Punkt IS.D.OR.200(a) erforderlich sind, und ein Verfahren zur Änderung dieser Dokumentation festlegen. Änderungen dieser Prozesse, Verfahren, Funktionen und Zuständigkeiten müssen nach Punkt IS.D.OR.255 verwaltet werden.
- d) Die Prozesse, Verfahren, Funktionen und Zuständigkeiten, die von der Organisation festgelegt wurden, um Punkt IS.D.OR.200(a) zu erfüllen, müssen — beruhend auf einer Bewertung der mit diesen Tätigkeiten verbundenen Informationssicherheitsrisiken — der Art und Komplexität ihrer Tätigkeiten entsprechen und können in andere bestehende Managementsysteme integriert werden, die die Organisation bereits eingeführt hat.
- e) Unbeschadet der Meldepflichten gemäß der Verordnung (EU) Nr. 376/2014 des Europäischen Parlaments und des Rates <sup>(1)</sup> und der Anforderungen von Punkt IS.D.OR.200(a)(13) kann die zuständige Behörde der Organisation die Genehmigung erteilen, die unter den Buchstaben a bis d genannten und die diesbezüglichen in den Punkten IS.D.OR.205 bis IS.D.OR.260 enthaltenen Anforderungen nicht umzusetzen, wenn diese zur Zufriedenheit der Behörde nachweist, dass ihre Tätigkeiten, Einrichtungen und Ressourcen sowie die von ihr betriebenen, angebotenen, erhaltenen und aufrechterhaltenen Dienste keine Informationssicherheitsrisiken mit potenziellen Auswirkungen auf die Flugsicherheit weder für ihre eigene noch für andere Organisationen darstellen. Voraussetzung für die Genehmigung ist eine dokumentierte Bewertung des Informationssicherheitsrisikos, die von der Organisation oder einem Dritten nach Punkt IS.D.OR.205 durchgeführt und von ihrer zuständigen Behörde überprüft und genehmigt wurde.

Die Aufrechterhaltung der Gültigkeit dieser Genehmigung wird von der zuständigen Behörde nach dem geltenden Auditzyklus für die Aufsicht und immer dann überprüft, wenn Änderungen im Tätigkeitsumfang der Organisation vorgenommen werden.

#### **IS.D.OR.205 Bewertung des Informationssicherheitsrisikos**

- a) Die Organisation muss alle Elemente ermitteln, die bei ihr vorliegen und die Informationssicherheitsrisiken ausgesetzt sein könnten. Dies schließt Folgendes ein:
1. die Tätigkeiten, Einrichtungen und Ressourcen der Organisation sowie die Dienste, die die Organisation betreibt, erbringt, erhält oder aufrechterhält;
  2. die Ausrüstung, Systeme, Daten und Informationen, die zur Funktionsfähigkeit der unter Nummer 1 aufgeführten Elemente beitragen.
- b) Die Organisation identifiziert die Schnittstellen zu anderen Organisationen, die dazu führen könnten, dass sie gegenseitig Informationssicherheitsrisiken ausgesetzt sind.
- c) In Bezug auf die unter den Buchstaben a und b genannten Elemente und Schnittstellen identifiziert die Organisation die Informationssicherheitsrisiken, die sich auf die Flugsicherheit auswirken können. Für jedes identifizierte Risiko muss die Organisation
1. eine Einstufung des Risikoniveaus gemäß einer vorab von der Organisation definierten Klassifizierung vornehmen;

<sup>(1)</sup> Verordnung (EU) Nr. 376/2014 des Europäischen Parlaments und des Rates vom 3. April 2014 über die Meldung, Analyse und Weiterverfolgung von Ereignissen in der Zivilluftfahrt, zur Änderung der Verordnung (EU) Nr. 996/2010 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2003/42/EG des Europäischen Parlaments und des Rates und der Verordnungen (EG) Nr. 1321/2007 und (EG) Nr. 1330/2007 der Kommission (ABl. L 122 vom 24.4.2014, S. 18).



2. jedes Risiko und dessen Niveau mit den entsprechenden gemäß den Buchstaben a und b identifizierten Elementen oder Schnittstellen verknüpfen.

Bei der in Nummer 1 genannten vordefinierten Klassifizierung müssen das Potenzial des Auftretens des Bedrohungsszenarios sowie die Schwere seiner Folgen für die Sicherheit berücksichtigt werden. Auf der Grundlage dieser Klassifizierung und unter Berücksichtigung der Frage, ob die Organisation über einen strukturierten und wiederholbaren Risikomanagementprozess für den Betrieb verfügt, muss die Organisation feststellen können, ob das Risiko hinnehmbar ist oder ein Tätigwerden nach Punkt IS.D.OR.210 erfordert.

Im Sinne einer leichteren gegenseitigen Vergleichbarkeit der Risikobewertungen müssen bei der Zuweisung des Risikoniveaus nach Nummer 1 einschlägige Informationen berücksichtigt werden, die in Abstimmung mit den unter Buchstabe b genannten Organisationen gewonnen wurden.

- d) Die Organisation muss die nach den Buchstaben a, b und c durchgeführte Risikobewertung immer dann überprüfen und aktualisieren, wenn eine der folgenden Situationen eintritt:
  1. Bei den Elementen, die Risiken für die Informationssicherheit ausgesetzt sind, ist eine Änderung eingetreten.
  2. Bei den Schnittstellen zwischen der Organisation und anderen Organisationen oder bei den von den anderen Organisationen mitgeteilten Risiken ist eine Änderung eingetreten.
  3. Bei den für die Identifizierung, Analyse und Klassifizierung von Risiken verwendeten Informationen und Kenntnissen ist eine Änderung eingetreten.
  4. Aus der Analyse der Störungen der Informationssicherheit haben sich neue Erkenntnisse ergeben.

#### **IS.D.OR.210 Umgang mit dem Informationssicherheitsrisiko**

- a) Die Organisation muss Maßnahmen für nach Punkt IS.D.OR.205 identifizierte und nicht hinnehmbare Risiken entwickeln, rechtzeitig umsetzen und kontinuierlich auf deren Wirksamkeit prüfen. Diese Maßnahmen müssen die Organisation in die Lage versetzen,
  1. die Umstände zu kontrollieren, die zum tatsächlichen Auftreten des Bedrohungsszenarios beitragen;
  2. die Folgen des tatsächlichen Eintretens des Bedrohungsszenarios für die Flugsicherheit zu verringern;
  3. die Risiken zu vermeiden.

Diese Maßnahmen dürfen nicht dazu führen, dass neue potenzielle und nicht hinnehmbare Risiken für die Flugsicherheit entstehen.

- b) Die in Punkt IS.D.OR.240(a) und (b) genannte Person und sonstiges betroffenes Personal der Organisation müssen über das Ergebnis der nach Punkt IS.D.OR.205 durchgeführten Risikobewertung, die entsprechenden Bedrohungsszenarien und die durchzuführenden Maßnahmen unterrichtet werden.

Die Organisation muss auch Organisationen, zu denen sie eine Schnittstelle nach Punkt IS.D.OR.205(b) aufweist, über alle zwischen beiden Organisationen geteilten Risiken informieren.

#### **IS.D.OR.215 Informationssicherheitssystem für interne Meldungen**

- a) Die Organisation muss ein System für interne Meldungen einrichten, das die Erfassung und Bewertung von Informationssicherheitsereignissen, einschließlich solcher, die nach Punkt IS.D.OR.230 zu melden sind, ermöglicht.
- b) Dieses System und das Verfahren nach Punkt IS.D.OR.220 müssen der Organisation Folgendes ermöglichen:
  1. Identifizierung, welche der nach Buchstabe a gemeldeten Ereignisse als Störungen oder Schwachstellen der Informationssicherheit mit potenziellen Auswirkungen auf die Flugsicherheit gelten;
  2. Identifizierung der Ursachen der nach Nummer 1 identifizierten Störungen und Schwachstellen der Informationssicherheit und der dazu beitragenden Faktoren sowie deren Bewältigung im Rahmen des Prozesses für das Sicherheitsrisikomanagement nach den Punkten IS.D.OR.205 und IS.D.OR.220;
  3. Gewährleistung einer Bewertung aller bekannten und relevanten Informationen im Zusammenhang mit den nach Nummer 1 identifizierten Störungen und Schwachstellen der Informationssicherheit;

4. Gewährleistung, dass eine Methode eingeführt wird, nach der die Informationen je nach Bedarf verbreitet werden.
- c) Jeder Auftragnehmer, der die Organisation möglicherweise Informationssicherheitsrisiken aussetzt, die sich auf die Flugsicherheit auswirken können, ist verpflichtet, der Organisation Informationssicherheitsereignisse zu melden. Diese Meldungen müssen nach den in den jeweiligen vertraglichen Vereinbarungen festgelegten Verfahren vorgelegt und nach Buchstabe b bewertet werden.
- d) Die Organisation muss bei Untersuchungen mit jeder anderen Organisation zusammenarbeiten, die einen wesentlichen Beitrag zur Informationssicherheit ihrer eigenen Tätigkeiten leistet.
- e) Die Organisation kann dieses Meldesystem in andere von ihr bereits umgesetzte Meldesysteme integrieren.

#### **IS.D.OR.220 Störungen der Informationssicherheit — Erkennung, Reaktion und Wiederherstellung**

- a) Auf der Grundlage des Ergebnisses der nach Punkt IS.D.OR.205 durchgeführten Risikobewertung und des Ergebnisses nach Punkt IS.D.OR.210 aus dem Umgang mit dem Risiko muss die Organisation Maßnahmen ergreifen, um Störungen und Schwachstellen zu erkennen, die auf das potenzielle Eintreten nicht hinnehmbarer Risiken, die sich auf die Flugsicherheit auswirken können, schließen lassen. Diese Detektionsmaßnahmen müssen die Organisation in die Lage versetzen,
  1. Abweichungen von vorab festgelegten funktionalen Leistungsgrundwerten zu identifizieren;
  2. Warnungen auszulösen, mit denen bei Abweichungen geeignete Gegenmaßnahmen aktiviert werden.
- b) Die Organisation muss Maßnahmen ergreifen, mit denen sie auf alle nach Buchstabe a identifizierten Ereigniszustände reagiert, die sich zu einer Störung der Informationssicherheit entwickeln können oder sich zu einer solchen entwickelt haben. Diese Reaktionsmaßnahmen müssen die Organisation in die Lage versetzen,
  1. die Reaktion auf die Warnhinweise nach Buchstabe a Nummer 2 einzuleiten, indem vordefinierte Ressourcen und Handlungsabläufe aktiviert werden;
  2. die Ausbreitung eines Angriffs einzudämmen und die vollständige Entfaltung eines Bedrohungsszenarios zu verhindern;
  3. den Ausfallmodus der betroffenen Elemente nach Punkt IS.D.OR.205(a) zu steuern.
- c) Die Organisation muss Maßnahmen ergreifen, die der Wiederherstellung nach Störungen der Informationssicherheit dienen, auch gegebenenfalls durch Notfallmaßnahmen. Diese Wiederherstellungsmaßnahmen müssen die Organisation in die Lage versetzen,
  1. den Zustand, der die Störung verursacht hat, zu beseitigen oder ihn auf ein tolerierbares Maß zu beschränken;
  2. innerhalb einer zuvor von der Organisation festgelegten Wiederherstellungszeit einen sicheren Zustand der in Punkt IS.D.OR.205(a) bereits definierten betroffenen Elemente zu erreichen.

#### **IS.D.OR.225 Reaktion auf die von der zuständigen Behörde gemeldeten Beanstandungen**

- a) Nach Erhalt der Mitteilung der Beanstandungen durch die zuständige Behörde muss die Organisation
  1. die Ursache(n) für die Nichteinhaltung und die dazu beitragenden Faktoren ermitteln,
  2. einen Abhilfeplan erstellen;
  3. die Behebung der Beanstandung zur Zufriedenheit der zuständigen Behörde nachweisen.
- b) Die unter Buchstabe a genannten Maßnahmen müssen innerhalb der mit der zuständigen Behörde vereinbarten Frist durchgeführt werden.

#### **IS.D.OR.230 Informationssicherheitssystem für externe Meldungen**

- a) Die Organisation muss ein Meldesystem für die Informationssicherheit einrichten, das den Anforderungen der Verordnung (EU) Nr. 376/2014 und deren delegierten Rechtsakten und Durchführungsrechtsakten genügt, sofern jene Verordnung auf die Organisation anwendbar ist.

- b) Unbeschadet ihrer Verpflichtungen aus der Verordnung (EU) Nr. 376/2014 muss die Organisation sicherstellen, dass alle Störungen oder Schwachstellen der Informationssicherheit, die ein erhebliches Risiko für die Flugsicherheit darstellen können, ihrer zuständigen Behörde gemeldet werden. Darüber hinaus gilt Folgendes:
1. Beeinträchtigt eine solche Störung oder Schwachstelle ein Luftfahrzeug oder zugehörige Systeme oder Komponenten, muss die Organisation dies auch dem Inhaber der Konstruktionsgenehmigung melden.
  2. Beeinträchtigt eine solche Störung oder Schwachstelle von der Organisation verwendete Systeme oder Komponenten, muss die Organisation dies der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation melden.
- c) Die Organisation muss die unter Buchstabe b genannten Zustände wie folgt melden:
1. Sie übermittelt der zuständigen Behörde und gegebenenfalls dem Inhaber der Konstruktionsgenehmigung oder der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation eine Mitteilung, sobald die Organisation von dem Zustand Kenntnis erlangt hat.
  2. Sie übermittelt — sofern dem nicht außergewöhnliche Umstände entgegenstehen — der zuständigen Behörde und gegebenenfalls dem Inhaber der Konstruktionsgenehmigung oder der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation so bald wie möglich, höchstens jedoch 72 Stunden nach dem Zeitpunkt, zu dem sie von dem Zustand Kenntnis erlangt hat, einen Bericht.
- Der Bericht muss in der von der zuständigen Behörde festgelegten Form erstellt werden und alle relevanten Informationen über den der Organisation bekannten Zustand enthalten.
3. Sie übermittelt der zuständigen Behörde und gegebenenfalls dem Inhaber der Konstruktionsgenehmigung oder der für die Konstruktion des Systems oder der Komponente verantwortlichen Organisation einen Folgebericht, in dem sie im Einzelnen darlegt, welche Maßnahmen sie für die Wiederherstellung nach der Störung ergriffen hat oder zu ergreifen beabsichtigt und welche Maßnahmen sie zu ergreifen gedenkt, um ähnliche Störungen der Informationssicherheit in Zukunft zu verhindern.
- Der Folgebericht muss in der von der zuständigen Behörde festgelegten Form vorgelegt werden, sobald diese Maßnahmen festgelegt wurden.

#### **IS.D.OR.235 Auftragsvergabe für Tätigkeiten des Informationssicherheitsmanagements**

- a) Die Organisation muss sicherstellen, dass bei der Vergabe eines Teils der unter Punkt IS.D.OR.200 genannten Tätigkeiten an andere Organisationen die in Auftrag gegebenen Tätigkeiten den Anforderungen dieser Verordnung genügen und dass die beauftragte Organisation unter ihrer Aufsicht arbeitet. Die Organisation muss sicherstellen, dass die mit den vertraglich vereinbarten Tätigkeiten verbundenen Risiken angemessen gemanagt werden.
- b) Die Organisation muss sicherstellen, dass die zuständige Behörde auf Anfrage Zugang zu der unter Vertrag genommenen Organisation hat, um festzustellen, ob die geltenden Anforderungen dieser Verordnung weiterhin eingehalten werden.

#### **IS.D.OR.240 Anforderungen an das Personal**

- a) Der verantwortliche Manager der Organisation oder — im Falle von Entwicklungsorganisationen — der Leiter der Entwicklungsorganisation, der nach der Verordnung (EU) Nr. 748/2012 und der Verordnung (EU) Nr. 139/2014 benannt wurde, auf die in Artikel 2 Absatz 1 Buchstaben a und b der vorliegenden Verordnung Bezug genommen wird, muss über die Befugnis verfügen, sicherzustellen, dass alle nach dieser Verordnung erforderlichen Tätigkeiten finanziert und durchgeführt werden können. Diese Person muss
  1. sicherstellen, dass alle zur Erfüllung der Anforderungen dieser Verordnung erforderlichen Ressourcen zur Verfügung stehen;
  2. das in Punkt IS.D.OR.200(a)(1) genannte Konzept für die Informationssicherheit festlegen und fördern;
  3. nachweisen, dass sie grundlegende Kenntnisse über diese Verordnung besitzt.
- b) Der verantwortliche Manager oder — im Falle von Entwicklungsorganisationen — der Leiter der Entwicklungsorganisation muss zur Gewährleistung der Einhaltung der Anforderungen dieser Verordnung eine Person oder eine Gruppe von Personen benennen und den Umfang ihrer Befugnisse festlegen. Diese Person oder Gruppe von Personen ist gegenüber dem verantwortlichen Manager oder, im Falle von Entwicklungsorganisationen, dem Leiter der Entwicklungsorganisation unmittelbar rechenschaftspflichtig und muss über die erforderlichen Kenntnisse, Ausbildungen und Erfahrungen verfügen, um ihren Aufgaben gerecht werden zu können. Die Verfahren müssen Festlegungen dazu enthalten, wer eine bestimmte Person im Fall einer längeren Abwesenheit jener Person vertritt.

- c) Der verantwortliche Manager oder — im Falle von Entwicklungsorganisationen — der Leiter der Entwicklungsorganisation muss eine Person oder eine Gruppe von Personen benennen, die dafür zuständig ist, die in Punkt IS.D.OR.200(a)(12) genannte Funktion zur Überwachung der Compliance zu verwalten.
- d) Nutzt die Organisation Organisationsstrukturen, Konzepte, Prozesse und Verfahren der Informationssicherheit gemeinsam mit anderen Organisationen oder mit Bereichen ihrer eigenen Organisation, die nicht Teil der Genehmigung oder Erklärung sind, kann der verantwortliche Manager oder, im Falle von Entwicklungsorganisationen, der Leiter der Entwicklungsorganisation — seine Tätigkeiten an eine gemeinsam verantwortliche Person übertragen.

In diesem Fall müssen zwischen dem verantwortlichen Manager der Organisation oder — im Falle von Entwicklungsorganisationen — dem Leiter der Entwicklungsorganisation und der gemeinsam verantwortlichen Person Koordinierungsmaßnahmen festgelegt werden, damit eine angemessene Integration des Informationssicherheitsmanagements innerhalb der Organisation gewährleistet ist.

- e) Der verantwortliche Manager oder der Leiter der Entwicklungsorganisation oder die in Buchstabe d genannte gemeinsam verantwortliche Person ist befugt, die zur Umsetzung von Punkt IS.D.OR.200 erforderlichen Organisationsstrukturen, Konzepte, Prozesse und Verfahren festzulegen und aufrechtzuerhalten.
- f) Die Organisation muss über ein Verfahren verfügen, mit dem sichergestellt wird, dass sie über genügend Personal verfügt, das die Durchführung der unter diesen Anhang fallenden Tätigkeiten wahrnehmen kann.
- g) Die Organisation muss über ein Verfahren verfügen, mit dem sichergestellt wird, dass das unter Buchstabe f genannte Personal über die für die Wahrnehmung seiner Aufgaben erforderliche Kompetenz verfügt.
- h) Die Organisation muss über ein Verfahren verfügen, mit dem sichergestellt wird, dass das Personal die mit den zugewiesenen Funktionen und Aufgaben verbundene Verantwortung anerkennt.
- i) Die Organisation muss sicherstellen, dass die Identität und Vertrauenswürdigkeit des Personals, das Zugang zu Informationssystemen und Daten hat, die den Anforderungen dieser Verordnung unterliegen, angemessen festgestellt wird.

#### **IS.D.OR.245 Führen von Aufzeichnungen**

- a) Die Organisation muss Aufzeichnungen über ihre Tätigkeiten im Bereich des Informationssicherheitsmanagements führen.
  - 1. Die Organisation muss sicherstellen, dass die folgenden Aufzeichnungen archiviert sind und zurückverfolgt werden können:
    - i) jede eingegangene Genehmigung und jede damit verbundene Bewertung des Informationssicherheitsrisikos nach Punkt IS.D.OR.200(e);
    - ii) Auftragsvergaben über Tätigkeiten nach Punkt IS.D.OR.200(a)(9);
    - iii) Aufzeichnungen der wichtigsten in Punkt IS.D.OR.200(d) genannten Prozesse;
    - iv) Aufzeichnungen über die bei der Risikobewertung nach Punkt IS.D.OR.205 ermittelten Risiken zusammen mit den damit verbundenen Maßnahmen zum Umgang mit den Risiken nach Punkt IS.D.OR.210;
    - v) Aufzeichnungen von Störungen und Schwachstellen der Informationssicherheit, die gemäß den Meldesystemen nach Punkt IS.D.OR.215 und Punkt IS.D.OR.230 gemeldet wurden;
    - vi) Aufzeichnungen über Informationssicherheitsereignisse, die möglicherweise neu bewertet werden müssen, um unentdeckte Störungen und Schwachstellen der Informationssicherheit aufzudecken.
  - 2. Die Aufzeichnungen nach Nummer 1 Ziffer i müssen mindestens fünf Jahre nach Ablauf der Gültigkeit der Genehmigung aufbewahrt werden.
  - 3. Die Aufzeichnungen nach Nummer 1 Ziffer ii müssen mindestens fünf Jahre nach Änderung oder Beendigung des Auftrags aufbewahrt werden.
  - 4. Die Aufzeichnungen nach Nummer 1 Ziffern iii, iv und v müssen mindestens fünf Jahre lang aufbewahrt werden.
  - 5. Die Aufzeichnungen nach Nummer 1 Ziffer vi müssen so lange aufbewahrt werden, bis diese Informationssicherheitsereignisse gemäß der Periodizität neu bewertet worden sind, die in einem von der Organisation festgelegten Verfahren definiert wurde.

- b) Die Organisation muss Aufzeichnungen über die Qualifikation und Erfahrung ihres eigenen Personals führen, das an Tätigkeiten des Informationssicherheitsmanagements beteiligt ist.
  - 1. Die Aufzeichnungen über Qualifikation und Erfahrung des Personals müssen so lange aufbewahrt werden, wie die Person für die Organisation tätig ist, und für einen Zeitraum von mindestens drei Jahren, nachdem die Person die Organisation verlassen hat.
  - 2. Mitglieder des Personals erhalten auf Antrag Zugang zu ihren Personalakten. Darüber hinaus muss die Organisation ihnen zum Zeitpunkt des Verlassens der Organisation auf Anfrage eine Kopie ihrer Personalakte aushändigen.
- c) Das Format der Aufzeichnungen muss in den Verfahren der Organisation festgelegt werden.
- d) Die Aufzeichnungen müssen so aufbewahrt werden, dass sie vor Beschädigung, Änderung und Diebstahl geschützt sind, wobei die Informationen bei Bedarf entsprechend dem Niveau der Sicherheitsklassifizierung zu kennzeichnen sind. Die Organisation muss sicherstellen, dass die Aufzeichnungen so aufbewahrt werden, dass Integrität, Authentizität und autorisierter Zugang gewährleistet werden.

#### **IS.D.OR.250 Handbuch zum Informationssicherheitsmanagement (ISMM)**

- a) Die Organisation muss der zuständigen Behörde ein Handbuch zum Informationssicherheitsmanagement (*Information Security Management Manual*, ISMM) und gegebenenfalls zugehörige Handbücher und Verfahren zur Verfügung stellen, die Folgendes enthalten:
  - 1. Eine vom verantwortlichen Manager oder, im Falle von Entwicklungsorganisationen, vom Leiter der Entwicklungsorganisation unterzeichnete Erklärung zur Bestätigung, dass die Organisation ihre Tätigkeiten zu jedem Zeitpunkt in Übereinstimmung mit diesem Anhang und mit dem ISMM ausführt. Ist der verantwortliche Manager oder — im Falle von Entwicklungsorganisationen — der Leiter der Entwicklungsorganisation nicht gleichzeitig der Hauptgeschäftsführer (CEO) der Organisation, muss dieser die Erklärung gegenzeichnen;
  - 2. Titel, Name(n), Pflichten, Rechenschaftspflichten, Zuständigkeiten und Befugnisse der in Punkt IS.D.OR.240(b) und(c) genannten Person(en);
  - 3. gegebenenfalls Titel, Name(n), Pflichten, Rechenschaftspflichten, Zuständigkeiten und Befugnisse der in Punkt IS.D.OR.240(d) genannten gemeinsamen verantwortlichen Person(en);
  - 4. das Informationssicherheitskonzept der Organisation nach Punkt IS.D.OR.200(a)(1);
  - 5. allgemeine Angaben zu Personalstärke und Personalkategorien sowie zum bestehenden System für die Planung der Verfügbarkeit von Personal nach Punkt IS.D.OR.240;
  - 6. Titel, Name(n), Pflichten, Rechenschaftspflichten, Zuständigkeiten und Befugnisse der wichtigsten Personen, die für die Umsetzung von Punkt IS.D.OR.200 verantwortlich sind, einschließlich der Person(en), die für die Überwachung der Compliance nach Punkt IS.D.OR.200(a)(12) verantwortlich ist/sind;
  - 7. ein Organigramm, aus dem die entsprechende Hierarchie der Rechenschaftspflichten und Zuständigkeiten der in den Nummern 2 und 6 genannten Personen hervorgeht;
  - 8. Angaben zu dem in Punkt IS.D.OR.215 genannten System für interne Meldungen;
  - 9. die Verfahren, mit denen festgelegt wird, wie die Organisation die Einhaltung dieses Teils gewährleistet, insbesondere:
    - i) die Dokumentation nach Punkt IS.D.OR.200(c);
    - ii) die Verfahren, mit denen festgelegt wird, wie die Organisation die im Zuge einer Auftragsvergabe nach Punkt IS.D.OR.200(a)(9) vergebenen Tätigkeiten kontrolliert;
    - iii) das ISMM-Änderungsverfahren nach Buchstabe c;
  - 10. die Einzelheiten der derzeit zugelassenen alternativen Nachweisverfahren.
- b) Die Erstausgabe des ISMM muss von der zuständigen Behörde genehmigt werden, die auch ein Exemplar dieses Handbuchs aufbewahrt. Das ISMM muss erforderlichenfalls geändert werden, damit die Beschreibung des ISMS der Organisation aktuell bleibt. Der zuständigen Behörde muss ein Exemplar aller Änderungen des ISMM vorgelegt werden.
- c) Änderungen des ISMM müssen nach einem von der Organisation festgelegten Verfahren verwaltet werden. Änderungen, die nicht in den Anwendungsbereich dieses Verfahrens fallen, sowie Änderungen im Zusammenhang mit den Änderungen nach Punkt IS.D.OR.255(b) müssen von der zuständigen Behörde genehmigt werden.

- d) Die Organisation kann das ISMM mit anderen von ihr verwalteten Managementhandbüchern zusammenführen, sofern durch eindeutige Bezugnahme klar erkennbar ist, welche Teile der Managementhandbücher den verschiedenen Anforderungen dieses Anhangs entsprechen.

#### **IS.D.OR.255 Änderungen des Informationssicherheitsmanagementsystems**

- a) Änderungen des ISMS können nach einem von der Organisation entwickelten Verfahren verwaltet und der zuständigen Behörde mitgeteilt werden. Dieses Verfahren muss von der zuständigen Behörde genehmigt werden.
- b) Für Änderungen des ISMS, die nicht unter das unter Buchstabe a genannte Verfahren fallen, muss die Organisation eine von der zuständigen Behörde erteilte Genehmigung beantragen und erhalten.

In Bezug auf diese Änderungen gilt Folgendes:

1. Der Antrag muss vor solchen Änderungen gestellt werden, damit die zuständige Behörde die fortgesetzte Einhaltung dieser Verordnung überprüfen und erforderlichenfalls die Organisationszulassung und den damit zusammenhängenden Genehmigungsumfang ändern kann.
2. Die Organisation muss der zuständigen Behörde alle Informationen zur Verfügung stellen, die diese zur Bewertung der Änderung anfordert.
3. Die Änderung darf erst nach Eingang der förmlichen Genehmigung durch die zuständige Behörde durchgeführt werden.
4. Während der Umsetzung solcher Änderungen unterliegt die Weiterführung des Betriebs der Organisation den von der zuständigen Behörde vorgegebenen Bedingungen.

#### **IS.D.OR.260 Kontinuierliche Verbesserung**

- a) Die Organisation muss anhand geeigneter Leistungsindikatoren die Wirksamkeit und Ausgereiftheit des ISMS bewerten. Diese Bewertung muss nach einem von der Organisation vorab festgelegten Zeitplan oder nach einer Störung der Informationssicherheit durchgeführt werden.
- b) Werden bei der Bewertung nach Buchstabe a Mängel festgestellt, muss die Organisation die erforderlichen Verbesserungsmaßnahmen ergreifen, damit das ISMS weiterhin den geltenden Anforderungen entspricht und die Informationssicherheitsrisiken auf einem annehmbaren Niveau hält. Darüber hinaus muss die Organisation die Elemente des ISMS, die von den angenommenen Maßnahmen betroffen sind, neu bewerten.
-