Informationssicherheits-Standard

der ILfD, Arbeitsgruppe Informationssicherheit

(Code of practice in practice)

Version	1.0	
Status	Final	
Datum	07. September 2011	
Dateiname	11-09-07 ILfD Informationssicherheitsstandard - Code of Practice in Practice 1.0.docx	

Verantwortlich	Andreas Schnitzer HvS-Consulting AG	Michael Hochenrieder HvS-Consulting AG
Telefon	+49 (0)89 / 890 63 62 - 40	+49 (0)89 / 890 63 62 - 30
e-Mail	schnitzer@hvs-consulting.de	hochenrieder@hvs-consulting.de

Verantwortlichkeiten

Funktion	Name
Autoren	HvS-Consulting AG (HvS): ▪ Andreas Schnitzer ▪ Michael Hochenrieder ▪ Josef Schmidhuber ▪ Georg Weigert
Review	Lufthansa AG (LH): ▪ Herr Peter Brüggemann ▪ Herr Thomas Piwek Deutsche Flugsicherung (DFS): ▪ Herr Matias Krempel Flughafen München GmbH (FMG): ▪ Herr Harald Englert ▪ Herr Alexander Cmarits ▪ Herr Stephan Lösl Flughafen Frankfurt AG (FraPort): ▪ Herr Lothar Fuchs ▪ Herr Alexander Döhne ▪ Herr Stephan Kaiser

Änderungsverzeichnis

Version	Datum	Status	Änderungen
0.1	15.10.09	Draft	Initiale Erstellung
0.20	01.11.09	Draft	Überarbeitung / Ergänzung
0.30	06.11.09	Draft	Überarbeitung / Ergänzung
0.40	19.11.09	Draft	Überarbeitung / Ergänzung
0.50.	14.12.09	Draft	Überarbeitung / Ergänzung nach Feedback ILfD-TN.
CoPiP 0.1	28.12.09	Draft	Änderung in CoPiP
CoPiP 0.92	12.10.10	Draft	Überarbeitung / Ergänzung
CoPiP 0.93	06.11.10	Draft	Überarbeitung / Ergänzung
CoPiP 0.94	10.11.10	Draft	Überarbeitung / Ergänzung
CoPiP 0.95	17.02.11	Draft	Überarbeitung / Ergänzung, Kapitel 16
CoPiP 0.96	25.02.11	Draft	Überarbeitung / Ergänzung
CoPiP 0.97	09.05.11	Draft	Überarbeitung / Ergänzung
CoPiP 1.0	07.09.11	Final	Finale Version

Inhalt

0 Einleitung

0.1 Die Initiative Luftverkehr für Deutschland (ILfD)

Unter der Schirmherrschaft des Bundesministers für Verkehr, Bau und Stadtentwicklung haben sich die DFS Deutsche Flugsicherung GmbH, Flughafen München GmbH, Fraport AG, und Deutsche Lufthansa AG zur „Initiative Luftverkehr für Deutschland“ zusammengeschlossen. Weitere Bundesministerien und Bundesländer sowie die deutschen Luftverkehrsverbände, Bundesverband der Deutschen Fluggesellschaften (BDF) und Arbeitsgemeinschaft Deutscher Verkehrsflughäfen (ADV), bringen sich ebenso mit ein. Die Initiatoren wollen zum einen die wirtschaftliche Grundlage von Luftfahrt in Deutschland stabilisieren, zum anderen aber auch bereits heute die Weichen stellen für eine starke Position der deutschen Luftverkehrsorganisationen im globalen Wettbewerb.
Die enge Zusammenarbeit von Flughäfen, Airlines und Flugsicherung auf nationaler Ebene hat das Ziel, eine höhere Effizienz des Luftverkehrsstandorts zu erreichen. Der Wettbewerb der global ausgerichteten Airlines entwickelt sich mehr und mehr zu einem Wettbewerb ihrer Gesamtsysteme aus Flughäfen, Flugsicherung und Airlines. Qualität und Effizienz der Zusammenarbeit aller Akteure sowie die regulatorischen und politischen Rahmenbedingungen im Luftverkehr werden damit zu entscheidenden Erfolgsfaktoren für den Standort.

0.2 Die Arbeitsgruppe Informationssicherheit

Die Arbeitsgruppe Informationssicherheit wurde gegründet um

- ein Regelwerk zur Informationssicherheit mit präventiv und reaktiv wirkenden Maßnahmen zu entwickeln, das an den Bedrohungen und Risiken für Informationen und informationsverarbeitende Systeme orientiert ist.
- gemeinsame Positionen im Rahmen der Zusammenarbeit mit dem öffentlichen Bereich bzw. Standardisierungsgremien zu erarbeiten und abzustimmen.
- vertrauensfördernde Maßnahmen zu initiieren, welche die Sicherheit gemeinsamer Schnittstellen bzw. gemeinsam genutzter Infrastrukturen erhöhen.
- gemeinsame Vorhaben der Luftverkehrsorganisationen in Bezug auf Informationssicherheit zu fördern.

0.3 IS-Standard für den Luftverkehr

Information Security Management im Luftverkehr hat, unabhängig von der jeweiligen Stellung der Organisation in der Leistungskette, einen hohen Stellenwert. Ohne ein wirksames Information Security Management System können die Risiken hinsichtlich Vertraulichkeit, Verfügbarkeit und/oder Integrität der für die Leistungserbringung erforderlichen Informationen/Daten gravierend ansteigen.

Die Arbeitsgruppe Informationssicherheit der ILfD hat sich daher darauf verständigt, einen Standard für Informationssicherheit im Luftverkehr analog der international akzeptierten und gültigen Informationssicherheitsnormenreihe ISO 2700x zu definieren.

Der Nutzen eines solchen Standards ist die Schaffung einer einheitlichen, vergleichbaren Sicherheitsbasis für alle daran ausgerichteten Organisationen des Luftverkehrs.

Die Folgen sind

- eine effiziente und praxisnahe Umsetzung von Maßnahmen in gemeinsamen Projekten, Arbeitsgruppen oder Initiativen analog dieses Standards.
- eine sichere Zusammenarbeit von Luftverkehrsorganisationen aufgrund „vertrauenswürdiger" Kooperation gemäß dieses Standards.

Im Rahmen der Arbeitsgruppe Informationssicherheit der ILfD wurde beschlossen, verschiedene Dokumente („Standards") mit unterschiedlichen Zielsetzungen zu erstellen.

1. Informationssicherheits-Standard für den Luftverkehr (Code of Practice)
   Dieser Standard gilt als Ausgangsdokument für einen internationalen Standard in Anlehnung an ISO 27002. Er dient dem gemeinsamen Verständnis von Informationssicherheit.

2. Der Informationssicherheits-Standard der ILfD, Arbeitsgruppe Informationssicherheit (AG IS) (Code of practice in practice)
   Dieser Standard ist ein multilaterales Dokument, dass die Zusammenarbeit zwischen den Partner der ILfD (später auch von weiteren Organisationen, die diesem Dokument „beitreten") gerade bei organisationsübergreifenden Prozessen hinsichtlich Informationssicherheit vereinfachen soll und dadurch einen direkten praktischen Nutzen für die Partner der ILfD und den beigetretenen Organisationen darstellt.

Beide Standards sind Leitfäden für die Implementierung und Steuerung eines Information Security Management Systems in Organisationen der Luftverkehrsbranche. Beide beruhen auf dem internationalen Standard ISO/IEC 27002 (Code of practice for information security management). Luftverkehrsorganisationen sollten über die Ziele und Maßnahmen der ISO/IEC 27002 hinaus die in diesem Standard aufgelisteten Sicherheitsmaßnahmen berücksichtigen.

Das vorliegende Dokument stellt den zweiten Teil dar: den Informationssicherheits-Standard der Arbeitsgruppe Informationssicherheit der ILfD (Code of practice in practice).

Da die Leistungserbringung im Luftverkehr stark von der Zusammenarbeit der einzelnen Teilnehmer geprägt ist, hängt das Information Security Management einer Organisation wesentlich vom Information Security Management der Organisationen ab, mit denen man in der Leistungserbringung zusammenarbeitet. Der vorliegende Standard legt daher auch einen Fokus auf Aspekte der Zusammenarbeit.

1 Anwendungsbereich

1.1 Zielsetzung

Der vorliegende Standard definiert Leitlinien und allgemeine Prinzipien für die Implementierung eines Informationssicherheits-Managementsystems (ISMS) sowie für die sichere Abwicklung des Kern-Flugprozesses in einer vertrauensvollen Zusammenarbeit zwischen den beteiligten Organisationen. Gemäß ISO/IEC 27001 und ISO/IEC 27002 definiert der vorliegende Standard zusätzliche Ziele und Maßnahmen basierend auf den spezifischen Anforderungen des Luftverkehrs.

Dieser Standard sollte als übergreifender Standard gesehen werden, der durch weitere, detaillierte Standards (z.B. ISO 270xx-Serie) aus den Bereichen Technologie, Prozesse und Organisation ergänzt werden kann.

1.2 Zielgruppe

Im Rahmen der an der Initiative ILfD teilnehmenden Unternehmen wurde nachfolgender Geltungsbereich festgelegt. Dabei gilt zu beachten, dass der vorliegende Standard gleichermaßen für interne und externe Mitarbeiter der jeweiligen Organisation anzuwenden ist.

1.2.1 Stufe 1: Am Kern-Flugprozess beteiligte Partner der ILfD

In Stufe 1 gilt der vorliegende Standard für alle am Kern-Flugprozess beteiligten Partner der ILfD:

- Deutsche Lufthansa AG
- DFS Deutsche Flugsicherung GmbH
- Flughafen München GmbH
- Fraport AG

1.2.2 Stufe 2: Alle am Kern-Flugprozess beteiligte Organisationen, die sich auf den Standard verpflichten

Alle am Kern-Flugprozess beteiligten Partner der ILfD sowie weitere Organisationen, die sich auf den Standard verpflichten

- Weitere Flughafenbetreiber
- Flugsicherungen
- Airlines
- Sämtliche am Luftverkehr beteiligten Organisationen (z.B. Abfertiger, Serviceanbieter, etc.)

2 Referenzen

Die folgenden Empfehlungen und internationalen Standards enthalten Bestimmungen, die – soweit sie im vorliegenden Standard referenziert werden – anwendbare Bestimmungen dieses Standards sind.

- ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
- ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management.
- BS 25999-1:2006, Business continuity management – Part 1: Code of practice
- BSI-Standard 100-1, Management für Informationssicherheit
- BSI-Standard 100-2, IT-Grundschutz Vorgehensweise
- BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4, Notfallmanagement

3 Begriffe & Abkürzungen

Siehe ISO/IEC 27000:2009

4 Informationssicherheits-Management in der Luftfahrt

4.1 Struktur dieses Standards

Dieser Standard ist gemäß der ISO/IEC 27002 aufgebaut. In allen Fällen, in denen Maßnahmen der ISO/IEC 27002 ohne Änderung oder Ergänzung angewendet werden können, ist nur eine Referenz auf die ISO/IEC 27002 gesetzt.

In allen Fällen in denen Maßnahmen der ISO/IEC 27002 luftverkehrsspezifische Ergänzungen zur Implementierung bedürfen sind diese luftverkehrsspezifischen Implementierungsrichtlinien direkt in das jeweilige Kapitel integriert.

Zusätzliche ausschließlich für den Bereich Luftverkehr relevante Maßnahmen in bestimmten Anwendungsgebieten sind in Annex A (normativ) beschrieben. Dabei handelt es sich um folgende Anwendungsgebiete:

- 16.1 Sicherheit von Informationen in Webanwendungen und Web-Services (LoT-A-WEB)
- 16.2 Organisationsübergreifende Verbindungen / externe Verbindungen (LoT-A-NET)
- 16.3 Zertifikate / Public Key Infrastructure (LoT-A-PKI)
- 16.4 Identity Management (LoT-A-IDM)

4.2 Analyse & Bewertung von IS-Risiken

4.2.1 Internes IS-Risiko Management

Die in ISO/IEC 27002 Kapitel 4 aufgeführten Maßnahmenziele und Inhalte sollten entsprechend angewendet werden. Das IS-Risiko Management sollte gemäß ISO/IEC 27005 oder BSI-Standard 100-3 erfolgen.

Beim IS-Risiko Management sollten alle Assets (Informationen, Anwendungen, Systeme) für den Kernflugprozess berücksichtigt werden, die mindestens eines der nachfolgenden Kriterien erfüllen:

- Informationen, von deren Integrität, Vertraulichkeit und Verfügbarkeit die Geschäftsprozesse abhängen.
- Systeme und Anwendungen, die besonders sensitive, geschäftskritische oder personenbezogene Daten enthalten und/oder verarbeiten.
- Systeme und Anwendungen, die wichtige oder geschäftskritische Aufgaben unterstützen, die ohne IT-Einsatz nicht möglich sind.
- Systeme und Anwendungen, die bestimmte Massenaufgaben erledigen, die ohne IT-Einsatz nicht zu bewältigen wären.

Die Assets müssen anhand ihres Schutzbedarfs bezüglich des betrachteten Geschäftsprozesses mindestens nach folgenden Kriterien beurteilt werden:

- Vertraulichkeit
- Verfügbarkeit
- Integrität

4.2.2 Organisationsübergreifendes IS-Risiko-Management

Soweit zur Abwicklung gemeinsamer Geschäftsprozesse bei der Betrachtung gemeinsamer Assets notwendig, sollten die zusammenarbeitenden Organisationen das IS-Risiko-Management in folgender Form durchführen:

- Ergebnisse der Schutzbedarfsanalyse mit den 3 Kriterien Vertraulichkeit, Verfügbarkeit und Integrität gemäß Kapitel 4.2.1 jeweils eingeteilt nach den folgenden 5 Stufen:
  - Kein — Kein Schutzbedarf
  - Gering — Geringer Schutzbedarf
  - Mittel — Mittlerer Schutzbedarf
  - Hoch — Hoher Schutzbedarf
  - Sehr hoch — Sehr hoher Schutzbedarf
- Festlegung, ab welchem Schutzbedarf eine detaillierte Risikoanalyse durchgeführt wird
- Betrachtete Bedrohungen
- Betrachtete Schwachstellen
- Potentieller Schaden, eingeteilt nach folgenden 5 Stufen:
  - Sehr gering — Geschäftsprozess verläuft nicht im definierten Rahmen, jedoch nur sehr geringer Schaden
  - Gering — Geschäftsprozess verläuft nicht im definierten Rahmen, geringer Schaden
  - Mittel — Verzögerung des Geschäftsprozesses, moderater Schaden
  - Hoch — Unterbrechung des Geschäftsprozesses, ernsthafter Schaden
  - Sehr hoch — Ausfall des Geschäftsprozesses, gravierender Schaden
- Eintrittswahrscheinlichkeit oder analoges Kriterium, eingeteilt nach folgenden 5 Stufen:
  - Sehr gering — Nach menschlichem Ermessen ausgeschlossen
  - Gering — Weniger als einmal innerhalb 10 Jahren
  - Mittel — Einmal innerhalb drei Jahre
  - Hoch — Einmal innerhalb eines Jahres
  - Sehr hoch — Öfters als einmal innerhalb eines Jahres
- Resultierendes Risiko, eingeteilt nach folgenden 3 Stufen:
  - Gering
  - Mittel
  - Hoch

Die Arbeitsgruppe Informationssicherheit der ILfD beschreibt regelmäßig die oben genannten Kriterien aus der Sicht des Kernflug-Prozesses.
Die Definitionen können projektbezogen in gegenseitigem Einvernehmen der beteiligten Organisationen an die jeweiligen Anforderungen angepasst werden.

Beispiel Risiko Matrix:

Schaden						
	Sehr hoch	Mittleres Risiko	Mittleres Risiko	Hohes Risiko	Hohes Risiko	Hohes Risiko
	Hoch	Mittleres Risiko	Mittleres Risiko	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Geringes Risiko	Mittleres Risiko	Mittleres Risiko	Mittleres Risiko	Hohes Risiko
	Gering	Geringes Risiko	Geringes Risiko	Mittleres Risiko	Mittleres Risiko	Mittleres Risiko
	Sehr gering	Geringes Risiko	Geringes Risiko	Geringes Risiko	Mittleres Risiko	Mittleres Risiko
		Sehr gering	Gering	Mittel	Hoch	Sehr hoch
		Eintrittswahrscheinlichkeit				

4.2.3 Risikobehandlung

Für die analysierten Risiken sind projektspezifisch die entsprechenden Maßnahmen durch die beteiligten Organisationen einvernehmlich festzulegen (siehe Kapitel 4.3) und zu dokumentieren.

4.3 Auswahl von Maßnahmen

Gemäß den Ergebnissen der IS-Risikoanalyse der Organisation (im Fall von organisationsübergreifenden Projekten der beteiligten Organisationen) sollten folgende Maßnahmen ausgewählt und umgesetzt werden:

- Maßnahmen aus der ISO/IEC 27002, soweit sie für diesen Standard zutreffen. (Anmerkung: im vorliegenden Standard schwarz markiert)
- Ergänzende Maßnahmen zu den in der ISO/IEC 27002 genannten Maßnahmen. Diese sind als luftverkehrsspezifische Implementierungsvorgaben in diesem Standard beschrieben. (Anmerkung: im vorliegenden Standard grün markiert!)
- Ergänzende Maßnahmen zu den im Informationssicherheits-Standard für Luftverkehrsorganisationen (Code of Practice) genannten Maßnahmen, die spezifisch für diesen Standard gelten. Diese sind als spezifische Implementierungsvorgaben des IS-Standards der ILfD in diesem Standard beschrieben. (Anmerkung: im vorliegenden Standard braun markiert!)
- Zusätzliche Maßnahmen welche als luftverkehrsspezifische neue Maßnahmen, die nicht in der ISO/IEC 27002 berücksichtigt sind, gefordert werden. Diese sind im Annex A / Kapitel 16 dieses Standards beschrieben.

4.4 Erklärung zur Anwendbarkeit

Die Organisation sollte eine „Erklärung zur Anwendbarkeit“ erstellen, aus der ersichtlich wird, welche Maßnahmen im betreffenden Scope (Anwendungsbereich) umgesetzt werden und welche als „nicht anwendbar“ gesehen werden. Die „Erklärung zur Anwendbarkeit“ sollte einem Partner bei Bedarf zur Einsichtnahme vorgelegt werden.

4.5 Umgang und Dokumentation von Ausnahmen

Werden notwendige Maßnahmen (gemäß „Erklärung zur Anwendbarkeit“) nicht umgesetzt, so muss dies von der Organisation begründet werden.

Bei folgenden besonderen Umständen können Ausnahmen gemacht werden:

- Es sind Ersatzmaßnahmen (Maßnahmen, die nicht unter 4.3 aufgeführt sind) realisiert, die zumindest die gleiche Effizienz und den gleichen Schutzwert aufweisen.
- Aufgrund von objektbezogenen Risikobewertungen wird nachgewiesen, dass Ersatzmaßnahmen mit einem geringeren Schutzwert bzw. der Wegfall einer Maßnahme akzeptiert werden können.

Die Ausnahmen sind umfassend zu dokumentieren. Dazu muss die Organisation eine Ausnahmeerklärung verfassen, die den betroffenen Parteien im Einzelfall (z.B. bei bilateralen Projekten oder bei der Bewertung nach „Level-of-Trust“ (siehe Kapitel 4.6)) vorgelegt werden muss. Diese Erklärung muss eine Risikobewertung beinhalten, die die Auswirkungen auf gemeinsame Geschäftsprozesse bzw. die beteiligten Organisationen darstellt.

4.6 Level-of-Trust der Organisation (Vertrauensstufen)

4.6.1 Einführung

Die Leistungserbringung im Luftverkehr ist – wie in Kapitel 0.3 bereits ausgeführt – durch ein hohes Maß von Zusammenarbeit der beteiligten Organisationen geprägt. Die Gewährleistung der Sicherheit der Informationen und der informationsverarbeitenden Systeme einer einzelnen Organisation im gemeinsamen Geschäftsprozess sowie der dahinter stehenden eigenen Geschäftsprozesse ist mit einem hohen Aufwand an individuellen Vereinbarungen und Überprüfungen verbunden.

Die Arbeitsgruppe Informationssicherheit der ILfD hat sich darauf verständigt, dass überprüfte Vertrauensstellungen (aus der 1:1-Beziehung zweier Organisationen oder durch die Überprüfung durch Externe) in weiteren gemeinsamen Geschäftsprozessen (auch mit dritten Organisationen) anerkannt werden.

Die Vertrauensstufe bzw. „Level-of-Trust der Organisation“ (abgekürzt LoT-O) bezieht sich grundsätzlich auf die jeweilige Organisation. Die Einstufung bezieht sich dabei immer auf den Teil des Kernflugprozesses, der von der jeweiligen Organisation erbracht wird („Scope“; siehe Kapitel 4.4). Hierbei sind v.a. potentielle IS-Risiken, die durch Koppelung der Geschäftsprozesse für die jeweiligen Organisationen entstehen können, zu berücksichtigen.

4.6.2 Stufen des „Level-of-Trust der Organisation“

Zur Einstufung des „Level-of-Trust der Organisation“ (LoT-O) wird eine absteigende sechsstufige Skala verwendet:

- Trusted
- Limited Trust 0
- Limited Trust 1
- Limited Trust 2
- Limited Trust 3
- Untrusted

Für die einzelnen Stufen gilt:

a) Trusted

Die Kategorie „Trusted“ wird nur für organisationseigene Bereiche, Tochterunternehmen oder Geschäftsprozesse angewendet, die vollständig den eigenen Sicherheitsvorgaben unterliegen. Unternehmens- oder konzernfremde Organisationen können nicht in die Kategorie „Trusted“ eingestuft werden.

b) Limited Trust 0

Die Kategorie „Limited Trust 0“ (LT0) bezeichnet fremde Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber folgende Anforderung erfüllen:

- Alle Maßnahmen des vorliegenden Standards sind verbindlich umgesetzt, soweit sie gemäß Kapitel 4.4 anwendbar sind.
- Die Einhaltung der Vorgaben des Standards wurde von einem externen Auditor bestätigt.

b) Limited Trust 1

Die Kategorie „Limited Trust 1“ (LT1) bezeichnet fremde Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein sehr hohes Gesamtniveau der Informationssicherheit erreichen. Dies gilt auch in Bereichen, in denen lediglich mittelbare Gefährdungen für die beteiligten Organisationen bestehen.

Anwendungsbeispiel: Kopplung von Netzwerken

Organisationen werden u.U. den Zugriff von anderen Organisationen mit LT1-Einstufung auf eigene Anwendungen nach dem „Need-to-have-Prinzip“ gestatten, ohne anwendungsspezifische Schutzmaßnahmen (z.B. Web Application Firewalls) und ohne weitere Authentifizierung an der Netzwerkgrenze (z.B. an der Firewall) durchzusetzen.

Dieses Vorgehen ist nur dann angemessen, wenn die andere Organisation über ein sehr hohes Sicherheitsniveau (LT1) verfügt und in diesem Zusammenhang alle relevanten ISMS-Maßnahmen implementiert hat.

c) Limited Trust 2

Die Kategorie „Limited Trust 2“ (LT2) bezeichnet fremde Organisationen oder unternehmenseigene Organisationen, die nicht den eigenen Sicherheitsvorgaben unterliegen, aber ein hohes Gesamtniveau der Informationssicherheit erreichen.

Anwendungsbeispiel: Kopplung von Netzwerken

Organisationen werden u.U. den Zugriff von anderen Organisationen 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 Authentifizierung erzwingen.

Dieses Vorgehen ist nur dann angemessen, wenn die andere Organisation über ein hohes Sicherheitsniveau (LT2) verfügt und in diesem Zusammenhang wichtige ISMS-Maßnahmen (z.B. Security Incident Management) implementiert hat.

c) Limited Trust 3

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

Anwendungsbeispiel: Kopplung von Netzwerken

Organisationen werden u.U. den Zugriff von anderen Organisationen 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 Authentifizierung erzwingen als auch weitere Schutzmaßnahmen (z.B. Content-Filterung, Eingabe-Kontrolle, Rights Management etc.) auf Anwendungsebene implementieren. Dieses Vorgehen ist nur dann angemessen, wenn die andere Organisation Basis-Sicherheitsmaßnahmen (z.B. Virenschutz, Backup/Restore etc.) sowie ein Sicherheitsmanagement implementiert hat.

e) Untrusted

Diese Kategorie bezeichnet alle Organisationen, welche die Anforderungen der Kategorie „Limited Trust 3“ nicht erfüllen.

4.6.3 Kriterien zur Einstufung

Entscheidend für die Einstufung einer Organisation ist der Umsetzungsgrad der in Kapitel 5 bis 15 genannten Maßnahmen. Daneben sind die Anforderungen aus Kapitel 4.4, 4.5 und 4.6 immer umzusetzen. Die Arbeitsgruppe Informationssicherheit der ILfD definiert und überarbeitet jährlich die Anforderungen aus den Kapitel 5 bis 15 für die Einstufung nach LT1, LT2 oder LT3. Die für den jeweiligen LT-O konkret umzusetzenden Maßnahmen sind von den zusammenarbeitenden Organisationen jeweils im Detail festgelegt. Die nachfolgende Tabelle dokumentiert als Richtwert den Umsetzungsgrad der Maßnahmen in Abhängigkeit zum LT (Vertrauensstufe). Die aktuell geltenden Anforderungen sind im Anhang 1 dieses Standards einzusehen und bei Bedarf aktuell bei der Arbeitsgruppe Informationssicherheit der ILfD zu erfragen.

Maßnahmen	LT0	LT1	LT2	LT3
5. Information Security Policy – Weisungen und Richtlinien zur Informationssicherheit	Mandatory	Mandatory	Mandatory	Mandatory
6. Organization of information security – Organisatorische Sicherheitsmaßnahmen und Managementprozess	Mandatory	Überwiegend	Überwiegend	Teilweise
7. Asset management – Verantwortung und Klassifizierung von Informationswerten	Mandatory	Mandatory	-	-
8. Human resources security – Personelle Sicherheit	Mandatory	Überwiegend	Überwiegend	Teilweise
9. Physical and Environmental Security – Physische Sicherheit und öffentliche Versorgungsdienste	Mandatory	Überwiegend	Teilweise	-
10. Communications and Operations Management – Netzwerk- und Betriebssicherheit (Daten und Telefonie)	Mandatory	Überwiegend	Teilweise	Teilweise
11. Access Control – Zugriffskontrolle	Mandatory	Überwiegend	Teilweise	Teilweise
12. Information systems acquisition, development and maintenance – Systementwicklung und Wartung	Mandatory	Teilweise	Teilweise	-
13. Information security incident management - Umgang mit Sicherheitsvorfällen	Mandatory	Überwiegend	Überwiegend	-
14. Business Continuity Management – Notfallvorsorgeplanung	Mandatory	Teilweise	Teilweise	-
15. Compliance – Einhaltung rechtlicher Vorgaben, der Sicherheitsrichtlinien und Überprüfungen durch Audits	Mandatory	Überwiegend	Teilweise	Teilweise

4.6.4 Einstufung

Die Einstufung einer fremden Organisation nach „Level-of-Trust“ kann durch jede Organisation selbst erfolgen. Dabei ist zu dokumentieren, nach welchem Stand der Anforderungen (siehe Kapitel 4.6.3) die Einstufung erfolgte.

Eine Ausnahme bildet die Einstufung „Limited Trust 0“, die nur nach einem Audit durch einen unabhängigen Dritten vergeben werden kann (siehe dazu Kapitel 6.1.8). Die Einstufung nach „Limited Trusted 0“ ist für 2 Jahre gültig. Nach Ablauf der Gültigkeit müssen die Anforderungen erneut erfüllt werden.
Es obliegt der jeweiligen Organisation, in wie weit sie die Einstufungen nach „Level-of-Trust“, die sie nicht selbst sondern Dritte vergeben haben, für gemeinsame Geschäftsprozesse akzeptiert.

Achtung: Der hier beschriebene Level-of-Trust bezieht sich immer auf die gesamte Organisation, daher auch Level-of-Trust der Organisation genannt. Daneben gibt es noch einen Level-of-Trust für bestimmte Anwendungsgebiete (LoT-A), die in Kapitel 16 beschrieben sind.

5 Sicherheitsleitlinie

5.1 Informationssicherheitsleitlinie

Ziel: Richtungsvorgabe und Unterstützung des Managements bei der Informationssicherheit, in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und Regelungen.
Das Management sollte eine klare Richtung der Grundsätze in Einklang mit Geschäftszielen vorgeben und Unterstützung und Engagement für Informationssicherheit durch organisationsweite Veröffentlichung und Aufrechterhaltung einer Informationssicherheitsleitlinie vorgeben.

5.1.1 Leitlinie zur Informationssicherheit

<LT **1** | **2** | **3**>
Maßnahme: Das Management muss eine Informationssicherheitsleitlinie genehmigen, veröffentlichen und alle Angestellten und relevanten Externen davon in Kenntnis setzen.
Die in ISO/IEC 27002 Kapitel 5.1.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben
<LT **1** | **2** | **3**>
Die Leitlinie zur Informationssicherheit sollte mit den vielfältigen Sicherheitsanforderungen in anderen Bereichen des Luftverkehrs (Bsp.: physische Absicherung von Sicherheitsbereichen) abgestimmt werden. Die Abgrenzungen zwischen den einzelnen Bereichen sollten in der Leitlinie oder einem eigenen Dokument dokumentiert werden.

5.1.2 Überprüfung der Informationssicherheitsleitlinie

<LT **1** | **2** | **3**>
Maßnahme: Die Informationssicherheitsleitlinie muss in regelmäßigen Abständen und immer dann überprüft werden, wenn wesentliche Änderungen erfolgen, um ihre Eignung, Angemessenheit und Wirksamkeit auf Dauer sicherzustellen.
Die in ISO/IEC 27002 Kapitel 5.1.2 empfohlenen Maßnahmen gelten entsprechend.

6 Organisation der Informationssicherheit

6.1 Interne Organisation

Ziel: Handhabung der Informationssicherheit innerhalb der Organisation.
Ein Managementrahmen sollte geschaffen werden, um die Umsetzung der Informationssicherheit innerhalb der Organisation einzuführen und zu steuern.
Das Management sollte die Informationssicherheitsleitlinie genehmigen, sicherheitsbezogene Aufgaben zuweisen und die Umsetzung der Informationssicherheit organisationsweit koordinieren und überprüfen.
Bei Bedarf sollten spezifische Informationssicherheitsratschläge bereitgestellt und innerhalb der Organisation verfügbar gemacht werden. Kontakte zu externen Sicherheitsfachkräften oder -gruppen, einschließlich relevanter Behörden, sollten hergestellt werden, um mit industriellen Trends Schritt zu halten, Normen und Bewertungsmethoden zu überwachen sowie geeignete Anlaufstellen zur Behandlung von Sicherheitsvorfällen zu schaffen. Eine interdisziplinäre Vorgehensweise bei der Informationssicherheit sollte gefördert werden.

6.1.1 Engagement des Managements für Informationssicherheit

<LT **1** | **2** | **3**>
Maßnahme: Das Management muss die Informationssicherheit innerhalb der Organisation aktiv unterstützen, indem es eine klare Ausrichtung vorgibt, sein Engagement demonstriert, Aufgaben explizit formuliert und die Verantwortlichkeiten für Informationssicherheit anerkennt.
Die in ISO/IEC 27002 Kapitel 6.1.1 empfohlenen Maßnahmen gelten entsprechend.

6.1.2 Koordination der Informationssicherheit

<LT **1** | **2** | **3**>
Maßnahme: Aktivitäten im Rahmen der Informationssicherheit müssen durch Repräsentanten verschiedener Organisationsbereiche mit relevanten Aufgabenbereichen und Funktionen koordiniert werden.
Die in ISO/IEC 27002 Kapitel 6.1.2 empfohlenen Maßnahmen gelten entsprechend.

6.1.3 Zuweisung der Verantwortlichkeiten für Informationssicherheit

<LT **1** | **2** | **3**>
Maßnahme: Alle Verantwortlichkeiten für Informationssicherheit müssen eindeutig definiert sein.
Die in ISO/IEC 27002 Kapitel 6.1.3 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben
<LT **1** | 2 | 3>
Die Organisation muss einen Verantwortlichen benennen, der als Ansprechpartner für strategische Fragen zur Informationssicherheit Dritten zur Verfügung steht (z.B. für Planung und Umsetzung gemeinsamer Maßnahmen, etc.).

6.1.4 Genehmigungsverfahren für informationsverarbeitende Einrichtungen

<LT **1** | **2** | 3>
Maßnahme: Für neue informationsverarbeitende Einrichtungen muss ein Genehmigungsverfahren durch das Management festgelegt und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 6.1.4 empfohlenen Maßnahmen gelten entsprechend.

6.1.5 Vertraulichkeitsvereinbarungen

<LT **1** | **2** | **3**>

Maßnahme: Anforderungen an Vertraulichkeitsvereinbarungen oder zur Geheimhaltung, die den Schutzbedarf der Organisation für Informationen widerspiegeln, müssen identifiziert und regelmäßig überprüft werden.
Die in ISO/IEC 27002 Kapitel 6.1.5 empfohlenen Maßnahmen gelten entsprechend.

6.1.6 Kontakt zu Behörden

<LT **1** | 2 | 3>

Maßnahme: Geeigneter Kontakt zu relevanten Behörden muss gepflegt werden.
Die in ISO/IEC 27002 Kapitel 6.1.6 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | 2 | 3>

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

6.1.7 Kontakt zu speziellen Interessengruppen

<LT **1** | 2 | 3>

Maßnahme: Geeignete Kontakte zu speziellen Interessengruppen oder anderen Experten-Sicherheitsforen und professionellen Verbänden müssen gepflegt werden.
Die in ISO/IEC 27002 Kapitel 6.1.7 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT 1 | 2 | 3>

Die Organisation muss sich zudem der Kritikalität ihrer Dienstleistungen für die Gesellschaft auf regionaler, nationaler bzw. internationaler Ebene bewusst sein. Sie muss sich deshalb in Verbänden und Zusammenschlüssen engagieren und sich an nationalen und/oder internationalen Programmen beteiligen, um die Sicherheit im Luftverkehr umfassend zu unterstützen.

Aufgrund der besonderen Bedrohungen für den Luftverkehr muss die Organisation die Zusammenarbeit mit anderen Luftverkehrsorganisationen anstreben, um gemeinsam nach Außen aufzutreten. Ein gemeinsamer Auftritt kann die Grundlage für die Auswahl angemessener präventiver und reaktiver Maßnahmen sein:

- Sicherstellen der Interoperabilität von gemeinsam voranzutreibender Maßnahmen
- Zusammenarbeit bei der Alarmierung in Fällen organisationsübergreifender IT-Krisen und bei der Krisen-Bewältigung.

6.1.8 Unabhängige Überprüfung der Informationssicherheit

<LT 1 | 2 | 3>

Maßnahme: Der Ansatz einer Organisation zur Handhabung und Umsetzung der Informationssicherheit (d.h. Maßnahmenziele, Maßnahmen, Leitlinien, Prozesse und Verfahren für Informationssicherheit) muss in regelmäßigen Zeitabständen, oder nach wesentlichen Änderungen an der implementierten Sicherheit von unabhängiger Seite überprüft werden.
Die in ISO/IEC 27002 Kapitel 6.1.8 empfohlenen Maßnahmen gelten entsprechend.

Spezifische Implementierungsvorgaben des IS-Standards der ILfD
<LT 1 | 2 | 3>

Audit für Level-of-Trust – Limited Trust 0
Um den „Level-of-Trust" Status „Limited Trust 0" zu erreichen, ist ein Audit durch einen externen Auditor notwendig (siehe Kapitel 4.6.4). Verantwortlich für die Ausgestaltung und Durchführung dieser Audits ist die Arbeitsgruppe Informationssicherheit der ILfD.

Die Audits werden gemäß ISO 27007 und ISO 27008 durchgeführt; solange diese ISO Normen noch nicht endgültig veröffentlicht sind, gelten die Inhalte der Draft-Versionen entsprechend.

Die Auditoren müssen für ihre Tätigkeit befähigt sein (z.B. Ernennung zum Auditor durch eine offizielle Zertifizierungsstelle für ISO 27001 Audits) und werden von der Arbeitsgruppe Informationssicherheit der ILfD für die Dauer von 3 Jahren ernannt.

Umfang und Dauer des Audits richten sich nach dem zu auditierenden Scope.

Die Dokumentation des Audits erfolgt mit Hilfe einer von der Arbeitsgruppe Informationssicherheit der ILfD offiziell zur Verfügung gestellten Vorlage. Die Ergebnisse des Audits werden in folgender Abstufung dokumentiert:

Abweichungen 1
sind gravierende Mängel im Managementsystem, die dazu führen, dass die Organisation den gewünschten Level-of-Trust nicht erhält, bzw. verliert. Diese Abweichungen werden durch den Auditor auf einem gesondertem Formblatt im Rahmen des Audits dokumentiert und den Verantwortlichen im Schlussgespräch dargestellt.

Abweichungen 2
sind Mängel im Managementsystem, die durch die Organisation umgehend beseitigt werden müssen. Diese Abweichungen werden durch den Auditor auf einem gesondertem Formblatt im Rahmen des Audits dokumentiert und den Verantwortlichen im Schlussgespräch dargestellt. Maßnahmen durch die Organisation sind gemäß der dokumentierten Abweichung erforderlich. Ein Nachaudit ist erforderlich. Dieses ist innerhalb eines halben Jahres durchzuführen.

Empfehlungen
stellen ein Verbesserungspotential dar. Die Bewertung und ggf. daraus abgeleitete Maßnahmen sollen bis zum nächsten Audit durch die Organisation in den Verbesserungsprozess eingebracht werden.

Hinweise
werden durch den Auditor im Bericht als mögliches Verbesserungspotenzial aufgeführt und können im Rahmen des Verbesserungsprozesses als Korrekturen im Managementsystem umgesetzt werden.

Die Ergebnisse aus offiziellen Audits, durchgeführt von unabhängigen Drittorganisationen (Beispiel: ISO 27001 Zertifizierung, durchgeführt von einer akkreditierten Zertifizierungsstelle) werden – soweit der Scope übereinstimmend ist – anerkannt.

Audits für Level-of-Trust – Limited Trust 1, 2 oder 3

Die Einstufung einer fremden Organisation nach „Level-of-Trust – Limited Trust 1, 2 oder 3“ kann gemäß Kapitel 4.6.4 durch jede Organisation selbst erfolgen.
Die Auditoren sollten für ihre Tätigkeit befähigt sein und unabhängig von anderen Einflüssen (z.B. Einbindung in das betreffende Projekt) sein.
Die Dokumentation der Audits sollte mit Hilfe der von der Arbeitsgruppe Informationssicherheit der ILfD zur Verfügung gestellten Vorlage erfolgen (siehe dazu oben).

6.2 Externe

Ziel: Aufrechterhaltung der Sicherheit von Informationen und von informationsverarbeitenden Einrichtungen der Organisation, die von Externen benutzt oder verwaltet werden, die für diese zugänglich sind oder die an Externe kommuniziert werden.
Die Sicherheit von Informationen und informationsverarbeitenden Einrichtungen der Organisation sollte durch die Einführung von Produkten oder Dienstleistungen von Externen nicht beeinträchtigt werden.
Jeglicher Zugang den Externe zu den informationsverarbeitenden Einrichtungen sowie die Verarbeitung und Kommunikation von Informationen durch Externe sollte überwacht werden.
Wenn es geschäftliche Gründe für die Zusammenarbeit mit Externen gibt, die dazu eventuell auch Zugang zu den Informationen und informationsverarbeitenden Einrichtungen der Organisation benötigen, oder wenn eine Dienstleistung oder ein Produkt von Externen bereitgestellt oder ihnen zur Verfügung gestellt wird, so sollte eine Risikoeinschätzung durchgeführt werden, um die Auswirkungen auf die Sicherheit und die Anforderungen an die erforderlichen Maßnahmen zu ermitteln. Maßnahmen sollten mit Externen vereinbart und in einem Vertrag fixiert werden.

6.2.1 Identifizierung von Risiken in Zusammenhang mit Externen

<LT **1** | **2** | **3**>
Maßnahme: Die Risiken für Informationen und informationsverarbeitende Einrichtungen der Organisation, die durch Geschäftsprozesse unter Beteiligung Externer verursacht werden, müssen identifiziert und angemessene Maßnahmen umgesetzt werden, bevor diesen der Zugriff gewährt wird.
Die in ISO/IEC 27002 Kapitel 6.2.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | **2** | **3**>
Alle Externen (Kunden, Lieferanten, Einzelpersonen, Organisationen allgemein) müssen vor Aufnahme einer Geschäftsbeziehung gemäß der für den Einsatzbereich gültigen aktuellen Gesetzgebung überprüft werden.

6.2.2 Adressieren von Sicherheit im Umgang mit Kunden

<LT **1** | **2** | 3>
Maßnahme: Alle identifizierten Sicherheitsanforderungen müssen berücksichtigt sein, bevor Kunden Zugang zu Informationen oder Werten der Organisation gegeben wird.
Die in ISO/IEC 27002 Kapitel 6.2.2 empfohlenen Maßnahmen gelten entsprechend.

6.2.3 Adressieren von Sicherheit in Vereinbarungen mit Dritten

<LT **1** | **2** | 3>

Maßnahme: Vereinbarungen mit Dritten, die den Zugriff, die Verarbeitung, Kommunikation oder Administration von Informationen oder informationsverarbeitenden Einrichtungen der Organisation betreffen, oder die Bereitstellung von Produkten oder Dienstleistungen für informationsverarbeitende Einrichtungen, müssen alle relevanten Sicherheitsanforderungen abdecken.
Die in ISO/IEC 27002 Kapitel 6.2.3 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | **2** | 3>

Bei organisationsübergreifenden Geschäftsprozessen muss vertraglich eine genaue Abgrenzung der Verantwortlichkeiten für die Sicherheit von Assets (Services, Systeme, etc.) festgelegt werden.

7 Management organisationseigener Werte (Assets)

7.1 Verantwortung für organisationseigene Werte (Assets)

Ziel: Erreichen und Erhaltung eines angemessenen Schutzes von organisationseigenen Werten (Assets). Alle organisationseigenen Werte (Assets) sollten einer Person zugerechnet werden können und einen benannten Eigentümer haben.
Für alle organisationseigenen Werte (Assets) sollten Eigentümer bestimmt werden, denen die Verantwortung für die Bereitstellung angemessener Maßnahmen obliegt. Im Einzelfall kann der Eigentümer die Umsetzung bestimmter Maßnahmen delegieren; er bleibt aber verantwortlich für den angemessenen Schutz der Werte.

7.1.1 Inventar der organisationseigenen Werte (Assets)

<LT **1** | **2** | 3>

Maßnahme: Alle organisationseigenen Werte (Assets) müssen eindeutig identifiziert und ein Inventar aller wichtigen organisationseigenen Werte (Assets) erstellt und gepflegt werden.
Die in ISO/IEC 27002 Kapitel 7.1.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | **2** | 3>

Bei organisationsübergreifenden Geschäftsprozessen, müssen im Inventar die zugehörigen Assets eindeutig bezüglich Verantwortlichkeit zugeordnet werden.

7.1.2 Eigentum von organisationseigenen Werten (Assets)

<LT **1** | 2 | 3>

Maßnahme: Alle Informationen und organisationseigenen Werte (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen müssen Eigentum eines bestimmten Teils der Organisation sein.
Die in ISO/IEC 27002 Kapitel 7.1.2 empfohlenen Maßnahmen gelten entsprechend.

7.1.3 Zulässige Nutzung von organisationseigenen Werten (Assets)

<LT **1** | 2 | 3>

Maßnahme: Regeln für den zulässigen Gebrauch von Informationen und organisationseigenen Werten (Assets) in Verbindung mit informationsverarbeitenden Einrichtungen müssen identifiziert, dokumentiert und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 7.1.3 empfohlenen Maßnahmen gelten entsprechend.

7.2 Klassifizierung von Informationen

Ziel: Sicherstellung des angemessenen Schutzes von Informationen. Informationen sollten klassifiziert werden, um den Bedarf, die Prioritäten und den erwarteten Umfang des Schutzes bei der Nutzung von Informationen angeben zu können.
Informationen können einen unterschiedlichen Grad von Sensitivität und Wichtigkeit haben. Manche Elemente können einen zusätzlichen Schutz oder eine besondere Handhabung erfordern. Ein Klassifikationsschema für Informationen sollte zur Anwendung kommen, das ein angemessenes Maß an Schutzniveaus definiert und den Bedarf an spezifischen Maßnahmen zur Handhabung ausdrückt.

7.2.1 Regelungen für die Klassifizierung

<LT **1** | **2** | **3**>
Maßnahme: Informationen müssen bezüglich ihres Werts, gesetzlicher Anforderungen, ihrer Sensitivität und ihrer Kritikalität für die Organisation klassifiziert werden.
Die in ISO/IEC 27002 Kapitel 7.2.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | **2** | **3**>
Um eine organisationsübergreifende Vergleichbarkeit sicherzustellen, sollte die Organisation Informationen, die in übergreifenden Geschäftsprozessen benutzt werden nach folgendem Schema klassifizieren – soweit nicht gesetzliche Regelungen (z.B. Datenschutz, Geheimschutz) zur Anwendung kommen.

Vertraulichkeitsklassen:
Die Zuordnung zu einer Vertraulichkeitsklasse sollte aufgrund des zu erwartenden Schadens für den Geschäftsprozess bei Kenntnisnahme der Information durch Unberechtigte erfolgen.

- Öffentlich: Informationen, deren Bekanntwerden keinen Schaden für den Geschäftsprozess / die beteiligten Organisationen nach sich ziehen kann.
- Intern: Informationen, deren Bekanntwerden einen geringen bis mittleren Schaden für den Geschäftsprozess / die beteiligten Organisationen nach sich ziehen kann.
- 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 muss das „Need-to-know-Prinzip“ gelten. Dies bedeutet, dass nur Personen Zugriff auf Informationen ab Klassifizierung „Intern“ erhalten, die dies zur Erfüllung Ihrer Aufgaben innerhalb des Geschäftsprozesses benötigen.

In Abhängigkeit von der jeweiligen Klassifizierung müssen individuelle Handlungsvorgaben zur Umsetzung des „Need-to-know-Prinzips“ definiert werden.

7.2.2 Kennzeichnung von und Umgang mit Informationen

<LT **1** | **2** | 3>
Maßnahme: Geeignete Verfahren für die Kennzeichnung von und den Umgang mit Informationen müssen in Übereinstimmung mit dem von der Organisation angewandten Klassifizierungsschema entwickelt und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 7.2.2 empfohlenen Maßnahmen gelten entsprechend.

8 Personalsicherheit

Luftverkehrsspezifische Implementierungsvorgaben
Die Anforderungen an personelle Sicherheit im Luftverkehr sind an unterschiedlichen Stellen geregelt (durch Gesetze und Vorgaben anderer Standards, z.B. durch Luftsicherheitsgesetz). Die Anforderungen dieses Standards gelten daher nur insoweit, wie es sich um die Sicherheitsvorgaben handelt, die nicht durch Vorgaben von Gesetzen oder andere Standards abgedeckt werden.

8.1 Vor der Anstellung

Ziel: Sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer ihre Verantwortlichkeiten verstehen und für die vorgesehenen Aufgaben geeignet sind, und um die Risiken durch Diebstahl, Betrug oder Missbrauch von Einrichtungen zu verringern.
Die Verantwortung für Sicherheit sollte vor der Einstellung in entsprechenden Tätigkeitsbeschreibungen und Arbeitsvertragsregelungen behandelt werden.
Alle Bewerber für eine Anstellung, Auftragnehmer und Drittbenutzer sollten angemessen überprüft werden, insbesondere, wenn sie sensitive Tätigkeiten ausführen sollen.
Angestellte, Auftragnehmer und Drittbenutzer von informationsverarbeitenden Einrichtungen sollten eine Verpflichtung auf ihre Sicherheitsaufgaben und -verantwortlichkeiten unterschreiben.

8.1.1 Aufgaben und Verantwortlichkeiten

<LT **1** | 2 | 3>
Maßnahme: Sicherheitsaufgaben und -verantwortlichkeiten von Angestellten, Auftragnehmern und Drittbenutzern müssen im Einklang mit den Informationssicherheitsgrundsätzen der Organisation definiert und dokumentiert werden.
Die in ISO/IEC 27002 Kapitel 8.1.1 empfohlenen Maßnahmen gelten entsprechend.

8.1.2 Überprüfung

<LT **1** | **2** | 3>
Maßnahme: Überprüfungen der Vergangenheit aller Bewerber, Auftragnehmer und Drittbenutzer müssen in Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen ausgeführt werden und sollten den Geschäftsanforderungen, der Klassifizierung der Informationen, die diese verwenden werden, und den erkannten Risiken angemessen sein.
Die in ISO/IEC 27002 Kapitel 8.1.2 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben
<LT **1** | **2** | 3>
Alle Personen müssen gemäß der für den Einsatzbereich gültigen aktuellen Gesetzgebung im Bereich Luftverkehr überprüft werden.

8.1.3 Arbeitsvertragsklauseln

<LT 1 | 2 | 3>
Maßnahme: Als Teil ihrer vertraglichen Auflagen müssen Angestellte, Auftragnehmer und Drittbenutzer den Vertragsklauseln ihres Anstellungsvertrags zustimmen und diesen unterzeichnen; diese Klauseln sollten ihre und die Verantwortlichkeiten der Organisation für Informationssicherheit festlegen.
Die in ISO/IEC 27002 Kapitel 8.1.3 empfohlenen Maßnahmen gelten entsprechend.

8.2 Während der Anstellung

Ziel: Sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer die Informationssicherheitsbedrohungen und -bedenken sowie ihre Verantwortlichkeiten und Pflichten kennen, und dass sie entsprechend ausgestattet sind, die organisationseigene Sicherheitsleitlinie bei ihrer normalen Arbeit zu befolgen, und das Risiko von menschlichen Fehlern zu reduzieren.
Die Verantwortlichkeit des Managements sollte definiert werden, um sicherzustellen, dass Sicherheit während des gesamten Beschäftigungsverhältnisses einer Person zur Anwendung kommt.
Ein angemessenes Niveau bezüglich des Bewusstseins, der Ausbildung und Schulung in Sicherheitsverfahren und des korrekten Gebrauchs von informationsverarbeitenden Einrichtungen sollte allen Angestellten, Auftragnehmern und Drittbenutzern nahe gebracht werden, um potentielle Sicherheitsrisiken zu minimieren. Für die Behandlung von Sicherheitsverstößen sollte ein formales Disziplinarverfahren eingerichtet werden.

8.2.1 Verantwortung des Managements

<LT **1** | **2** | 3>
Maßnahme: Das Management muss verlangen, dass Angestellte, Auftragnehmer und Drittbenutzer Sicherheit in Übereinstimmung mit den festgelegten Leitlinien und Verfahren der Organisation anwenden.
Die in ISO/IEC 27002 Kapitel 8.2.1 empfohlenen Maßnahmen gelten entsprechend.

8.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit

<LT **1** | **2** | **3**>
Maßnahme: Alle Angestellten der Organisation, und, falls relevant, Auftragnehmer und Drittbenutzer, müssen geeignete Sensibilisierungsmaßnahmen in Sachen Informationssicherheit erhalten, und regelmäßig über organisationseigene Leitlinien und Verfahren, die für ihre Arbeit von Bedeutung sind, informiert werden.
Die in ISO/IEC 27002 Kapitel 8.2.2 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben
<LT **1** | **2** | **3**>
Die Sensibilisierung, Ausbildung und Schulung der Mitarbeiter müssen gemäß der für den Einsatzbereich gültigen gesetzlichen Vorgaben erfolgen.

8.2.3 Disziplinarverfahren

<LT 1 | 2 | 3>
Maßnahme: Für Angestellte, die einen Sicherheitsverstoß begangen haben, muss ein formales Disziplinarverfahren eingeleitet werden.
Die in ISO/IEC 27002 Kapitel 8.2.3 empfohlenen Maßnahmen gelten entsprechend.

8.3 Beendigung oder Änderung der Anstellung

Ziel: Sicherstellen, dass Angestellte, Auftragnehmer und Drittbenutzer ordnungsgemäß die Organisation verlassen oder die Anstellung wechseln.
Verantwortlichkeiten sollten etabliert werden, um sicherzustellen, dass Angestellte, Auftragnehmer oder Drittbenutzer die Organisation in geregelter Weise verlassen, und dass die Rückgabe aller Geräte und das Entfernen der Zugangsrechte abgeschlossen sind.
Änderungen von Verantwortlichkeiten und Anstellungen innerhalb einer Organisation sollten genauso behandelt werden wie die Beendigung des jeweiligen Anstellungsverhältnisses oder der Verantwortlichkeiten, wie in diesem Abschnitt beschrieben, und jegliche Neuanstellungen sollten behandelt werden wie in Abschnitt 8.1 beschrieben.

8.3.1 Verantwortlichkeiten bei der Beendigung

<LT **1** | 2 | 3>
Maßnahme: Die Verantwortlichkeiten für das Beenden oder Ändern eines Anstellungsverhältnisses müssen klar definiert und zugewiesen werden.
Die in ISO/IEC 27002 Kapitel 8.3.1 empfohlenen Maßnahmen gelten entsprechend.

8.3.2 Rückgabe von organisationseigenen Werten

<LT **1** | **2** | 3>
Maßnahme: Alle Angestellte, Auftragnehmer und Drittbenutzer müssen alle organisationseigenen Werte (Assets) in ihrem Besitz bei der Beendigung ihres Anstellungsverhältnisses, Vertrags oder Vereinbarung zurückgeben.
Die in ISO/IEC 27002 Kapitel 8.3.2 empfohlenen Maßnahmen gelten entsprechend.

8.3.3 Aufheben von Zugangsrechten

<LT **1** | **2** | **3**>
Maßnahme: Die Zugangsrechte aller Angestellten, Auftragnehmer und Drittbenutzer zu Informationen und informationsverarbeitenden Einrichtungen müssen zurückgenommen werden, wenn ihre Anstellung, Vertrag oder Vereinbarung endet, oder bei Veränderungen angepasst werden.
Die in ISO/IEC 27002 Kapitel 8.3.3 empfohlenen Maßnahmen gelten entsprechend.

9 Physische und umgebungsbezogene Sicherheit

Luftverkehrsspezifische Implementierungsvorgaben
Die Anforderungen an physische Sicherheit im Luftverkehr sind an unterschiedlichen Stellen geregelt (durch Gesetze und Vorgaben anderer Standards). Die Anforderungen dieses Standards gelten daher nur insoweit als es sich um die Sicherheit von physischer Infrastruktur handelt, die nicht durch Vorgaben von Gesetzen oder andere Standards abgedeckt wird (z.B. Rechenzentren, Serverräume, etc.).

9.1 Sicherheitsbereiche

Ziel: Schutz vor unerlaubtem Zutritt zu und Beschädigung und Störung von Organisationsinfrastruktur und der Organisation gehörenden Informationen.
Kritische oder sensitive datenverarbeitende Einrichtungen sollten in Sicherheitsbereichen untergebracht sein, welche durch festgelegte Sicherheitszonen mit angemessenen Sicherheitsbarrieren und Zugangskontrollsystemen geschützt sind.
Diese Maßnahmen sollten im Einklang mit den identifizierten Risiken stehen.

9.1.1 Sicherheitszonen
<LT **1** | **2** | **3**>
Maßnahme: Sicherheitszonen (Hindernisse wie Wände, über Zutrittskarten kontrollierte Zugänge oder mit Pförtnern besetzte Empfangsbereiche) müssen die Abschnitte schützen, die informationsverarbeitende Einrichtungen beherbergen.
Die in ISO/IEC 27002 Kapitel 9.1.1 empfohlenen Maßnahmen gelten entsprechend.

9.1.2 Zutrittskontrolle
<LT **1** | **2** | **3**>
Maßnahme: Sicherheitsbereiche müssen durch angemessene Zutrittskontrollen geschützt sein, um sicherzustellen, dass nur autorisierten Mitarbeitern Zutritt gewährt wird.
Die in ISO/IEC 27002 Kapitel 9.1.2 empfohlenen Maßnahmen gelten entsprechend.

9.1.3 Sicherung von Büros, Räumen und Einrichtungen
<LT **1** | 2 | 3>
Maßnahme: Physischer Schutz für Büros, Räume und Einrichtungen muss geplant und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 9.1.3 empfohlenen Maßnahmen gelten entsprechend.

9.1.4 Schutz vor Bedrohungen von Außen und aus der Umgebung
<LT **1** | 2 | 3>
Maßnahme: Physischer Schutz gegen Feuer, Wasser, Erdbeben, Explosionen, zivile Unruhen und andere Formen natürlicher und von Menschen verursachter Katastrophen muss vorgesehen und umgesetzt sein.
Die in ISO/IEC 27002 Kapitel 9.1.4 empfohlenen Maßnahmen gelten entsprechend.

9.1.5 Arbeit in Sicherheitszonen

<LT 1 | 2 | 3>

Maßnahme: Physischer Schutz und Richtlinien für die Arbeit in Sicherheitszonen muss entwickelt und umgesetzt werden.

Die in ISO/IEC 27002 Kapitel 9.1.5 empfohlenen Maßnahmen gelten entsprechend.

9.1.6 Öffentlicher Zugang, Anlieferungs- und Ladezonen

<LT **1** | 2 | 3>

Maßnahme: Zugangspunkte wie Anlieferungs- und Ladezonen sowie andere Zugangspunkte, an denen unbefugte Personen den Standort betreten können, müssen kontrolliert und, sofern möglich, von informationsverarbeitenden Einrichtungen getrennt werden, um unerlaubten Zutritt zu verhindern.

Die in ISO/IEC 27002 Kapitel 9.1.6 empfohlenen Maßnahmen gelten entsprechend.

9.2 Sicherheit von Betriebsmitteln

Ziel: Verhinderung des Verlusts, der Beschädigung, des Diebstahls oder der Kompromittierung von organisationseigenen Werten (Assets) und Unterbrechung der Aktivitäten einer Organisation.
Betriebsmittel sollten vor physischen Bedrohungen und Bedrohungen aus dem Umfeld geschützt werden.
Es ist notwendig die Betriebsmittel (auch diejenige, die außerhalb der Einrichtungen eingesetzt werden (wie Laptop, PDA, Mobiltelefon) sowie die Wegnahme von Betriebsmitteln) zu schützen, um so das Risiko des unerlaubten Zugriffs zu Informationen zu verringern, als auch die Betriebsmittel vor Verlust und Beschädigung zu schützen. Dabei sollte ebenfalls die Platzierung als auch die Entsorgung der Betriebsmittel in Betracht gezogen werden. Spezielle Maßnahmen können notwendig werden, um Betriebsmittel als auch die unterstützenden Einrichtungen, wie z. B. die Stromversorgung und die Verkabelung, zu schützen.

9.2.1 Platzierung und Schutz von Betriebsmitteln

<LT **1** | **2** | 3>

Maßnahme: Betriebsmittel müssen so platziert und geschützt werden, dass das Risiko durch Bedrohungen aus der Umgebung, durch Katastrophen als auch die Gelegenheit für unerlaubten Zugriff reduziert wird.

Die in ISO/IEC 27002 Kapitel 9.2.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | **2** | 3>

Die Abwicklung des Luftverkehrs bedarf einer umfassenden Information der Passagiere. Die dafür benötigten Betriebsmittel in öffentlichen Bereichen muss die Organisation gegen unberechtigten Zugriff und Zugang speziell schützen, z.B. durch stabile und abzusperrende Gehäuse für PCs, physische und/oder logische Absicherung von Netzwerkdosen etc.

9.2.2 Unterstützende Versorgungseinrichtungen

<LT **1** | **2** | **3**>

Maßnahme: Betriebsmittel müssen vor Stromausfällen und Ausfällen andere Versorgungseinrichtungen geschützt werden.

Die in ISO/IEC 27002 Kapitel 9.2.2 empfohlenen Maßnahmen gelten entsprechend.

9.2.3 Sicherheit der Verkabelung

<LT **1** | 2 | 3>

Maßnahme: Versorgungsleitungen für Strom und Telekommunikation, welche Daten transportieren oder Informationssysteme versorgen, müssen vor Abhören und Beschädigung geschützt sein.
Die in ISO/IEC 27002 Kapitel 9.2.3 empfohlenen Maßnahmen gelten entsprechend.

9.2.4 Instandhaltung von Gerätschaften

<LT **1** | 2 | 3>

Maßnahme: Gerätschaften müssen korrekt instand gehalten und gepflegt werden, um ihre Verfügbarkeit und Vollständigkeit sicherzustellen.
Die in ISO/IEC 27002 Kapitel 9.2.4 empfohlenen Maßnahmen gelten entsprechend.

9.2.5 Sicherheit von außerhalb des Standorts befindlicher Ausrüstung

<LT **1** | 2 | 3>

Maßnahme: Betriebsmittel, welche sich außerhalb des Standorts befinden, müssen unter Beachtung der unterschiedlichen Risiken, die durch den Einsatz außerhalb eines Standorts entstehen, geschützt werden.
Die in ISO/IEC 27002 Kapitel 9.2.5 empfohlenen Maßnahmen gelten entsprechend.

9.2.6 Sichere Entsorgung oder Weiterverwendung von Betriebsmitteln

<LT **1** | 2 | 3>

Maßnahme: Bei jeglicher Gerätschaft, welche Speichermedien enthält, muss vor der Entsorgung überprüft werden, ob alle sensitiven Daten und die lizenzierte Software entfernt oder sicher überschrieben wurden.
Die in ISO/IEC 27002 Kapitel 9.2.6 empfohlenen Maßnahmen gelten entsprechend.

9.2.7 Entfernung von Eigentum

<LT 1 | 2 | 3>

Maßnahme: Betriebsmittel, Informationen oder Software dürfen nicht unberechtigt aus dem Standort entfernt werden.
Die in ISO/IEC 27002 Kapitel 9.2.7 empfohlenen Maßnahmen gelten entsprechend.

10 Betriebs- und Kommunikationsmanagement

10.1 Verfahren und Verantwortlichkeiten

Ziel: Sicherstellung des korrekten und sicheren Betriebs der Informationsverarbeitenden Einrichtungen.
Für das Management und den Betrieb von informationsverarbeitenden Einrichtungen sollten Verantwortlichkeiten und Verfahren definiert sein. Dies beinhaltet die Entwicklung angemessener Betriebsprozesse.
Die Aufteilung von Pflichten (4-Augen-Prinzip) sollte bei Bedarf umgesetzt werden, um so das Risiko von fahrlässigem oder vorsätzlichem Missbrauch zu verringern.

10.1.1 Dokumentierte Betriebsprozesse

<LT **1** | **2** | 3>

Maßnahmen: Betriebsprozesse müssen dokumentiert und gepflegt sein und den Benutzern bei Bedarf bereitgestellt werden.
Die in ISO/IEC 27002 Kapitel 10.1.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | **2** | 3>

Aufgrund der geforderten hohen Verfügbarkeit der Geschäftsprozesse im Luftverkehr muss die Organisation in den Betriebsprozessen dokumentieren unter welchen Umständen Notfall- oder Krisenpläne aktiviert werden (siehe dazu auch Kapitel 13 und 14).

10.1.2 Änderungsverwaltung

<LT **1** | 2 | 3>

Maßnahme: Änderungen an informationsverarbeitenden Einrichtungen und Systemen müssen geregelt durchgeführt werden.
Die in ISO/IEC 27002 Kapitel 10.1.2 empfohlenen Maßnahmen gelten entsprechend.

10.1.3 Aufteilung von Verantwortlichkeiten

<LT 1 | 2 | 3>

Maßnahme: Pflichten und Verantwortungsbereiche müssen aufgeteilt werden, um die Möglichkeiten für unbefugte oder vorsätzliche Veränderung oder Missbrauch von organisationseigenen Werten (Assets) zu reduzieren.
Die in ISO/IEC 27002 Kapitel 10.1.3 empfohlenen Maßnahmen gelten entsprechend.

10.1.4 Aufteilung von Entwicklungs-, Test- und Produktiveinrichtungen

<LT 1 | 2 | 3>

Maßnahme: Entwicklungs-, Test- und Produktiveinrichtungen müssen getrennt sein, um das Risiko des unbefugten Zugriffs auf das Produktivsystem oder ungewollter Änderungen am Produktivsystem zu verhindern.
Die in ISO/IEC 27002 Kapitel 10.1.4 empfohlenen Maßnahmen gelten entsprechend.

10.2 Management der Dienstleistungs-Erbringung von Dritten

Ziel: Umsetzung und Aufrechterhaltung eines angemessenen Grads an Informationssicherheit und Dienstleistungserbringung, in Übereinstimmung mit den Liefervereinbarungen mit Dritten.
Die Organisation sollte die Umsetzung der vertraglichen Vereinbarung überprüfen, die Einhaltung der Vereinbarung überwachen und Änderungen verwalten, um sicherzustellen, dass die gelieferten Dienstleistungen alle mit den Dritten vereinbarten Anforderungen erfüllen.

10.2.1 Erbringung von Dienstleistungen

<LT **1** | 2 | 3>
Maßnahme: Es muss sichergestellt sein, dass die Sicherheitsmaßnahmen, Leistungsbeschreibungen und der Grad der Lieferungen, die in der Liefervereinbarung mit Dritten enthalten sind, von den Dritten umgesetzt, durchgeführt und eingehalten werden.
Die in ISO/IEC 27002 Kapitel 10.2.1 empfohlenen Maßnahmen gelten entsprechend.

10.2.2 Überwachung und Überprüfung der Dienstleistungen von Dritten

<LT 1 | 2 | 3>
Maßnahme: Die von Dritten gelieferten Dienstleistungen, Berichte und Aufzeichnungen müssen regelmäßig überwacht und überprüft werden, und Audits sollten regelmäßig durchgeführt werden.
Die in ISO/IEC 27002 Kapitel 10.2.2 empfohlenen Maßnahmen gelten entsprechend.

10.2.3 Management von Änderungen an Dienstleistungen von Dritten

<LT 1 | 2 | 3>
Maßnahme: Änderungen an der Erbringung von Dienstleistungen, einschließlich des Aufrechterhaltens und Verbesserns der existierenden Sicherheitsleitlinie, Verfahren und Maßnahmen, müssen geregelt werden, und dies unter Berücksichtigung der Kritikalität der betroffenen Geschäftssysteme und Geschäftsprozesse und einer erneuten Risikoeinschätzung.
Die in ISO/IEC 27002 Kapitel 10.2.3 empfohlenen Maßnahmen gelten entsprechend.

10.3 Systemplanung und Abnahme

Ziel: Das Risiko von Systemfehlern und Systemausfällen zu minimieren.
Vorausschauende Planung und Vorbereitung ist notwendig, um sicherzustellen, dass angemessene Kapazitäten und Ressourcen verfügbar bleiben, um die geforderte Systemleistung zu erbringen.
Um das Risiko von Systemüberlastungen zu reduzieren, sollten Abschätzungen für zukünftige Kapazitätsanforderungen durchgeführt werden.
Die Betriebsanforderungen von neuen Systemen sollten ermittelt, dokumentiert und getestet werden bevor diese abgenommen und benutzt werden.

10.3.1 Kapazitätsplanung

<LT 1 | 2 | 3>
Maßnahme: Die Verwendung von Ressourcen muss überwacht und abgestimmt werden, und Abschätzungen für zukünftige Kapazitätsanforderungen sollten getroffen werden, um die geforderte Systemleistung sicherzustellen.
Die in ISO/IEC 27002 Kapitel 10.3.1 empfohlenen Maßnahmen gelten entsprechend.

10.3.2 System-Abnahme

<LT **1** | 2 | 3>

Maßnahme: Kriterien für eine Abnahme von neuen Informationssystemen, Upgrades/Aufrüstungen und neuen Versionen müssen eingeführt und angemessene Tests von Systemen sollten während der Entwicklung und vor der Abnahme durchgeführt werden.
Die in ISO/IEC 27002 Kapitel 10.3.2 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | 2 | 3>

Die Abnahme von Systemen, die in organisationsübergreifenden Prozessen eingesetzt werden, muss einen formalen Prozess beinhalten, der sicherstellt, dass die geforderten Sicherheitsmaßnahmen eingehalten werden.

10.4 Schutz vor Schadsoftware und mobilem Programmcode

Ziel: Schutz der Integrität von Software und Informationen.
Vorsichtsmaßnahmen sind notwendig, um das Einschleusen von Schadsoftware und nicht genehmigtem mobilem Programmcode (Mobile Agenten) zu erkennen und zu verhindern.
Software und informationsverarbeitende Einrichtungen sind durch das Einschleusen von Schadsoftware wie Computer-Viren, Würmern, trojanischen Pferden und logischen Bomben verwundbar. Die Benutzer solcher Systeme sollten auf die Gefahren durch Schadsoftware hingewiesen worden sein. Manager sollten, soweit erforderlich, Maßnahmen zum Schutz vor, bzw. zum Erkennen und Entfernen von Schadsoftware und zur Überwachung von mobilem Programmcode treffen.

10.4.1 Maßnahmen gegen Schadsoftware

<LT **1** | **2** | **3**>

Maßnahme: Erkennung, Verhinderung und Wiederherstellung zum Schutz vor Schadsoftware, sowie eine angemessene Sensibilisierung der Benutzer müssen umgesetzt sein.
Die in ISO/IEC 27002 Kapitel 10.4.1 empfohlenen Maßnahmen gelten entsprechend.

10.4.2 Schutz vor mobiler Software (mobilen Agenten)

<LT 1 | 2 | 3>

Maßnahme: Wo die Verwendung mobilen Programmcodes (mobile Agenten) genehmigt ist, muss die Systemkonfiguration dafür Sorge tragen, dass dieser gemäß einer klar definierten Leitlinie agiert und nicht genehmigter mobiler Programmcode nicht ausgeführt wird.
Die in ISO/IEC 27002 Kapitel 10.4.2 empfohlenen Maßnahmen gelten entsprechend.

10.5 Backup

Ziel: Erhaltung der Integrität und der Verfügbarkeit von Informationen und informationsverarbeitenden Einrichtungen.
Routineverfahren sollten etabliert werden, die die vereinbarte Backup-Methode und Strategie (siehe auch 14.1) implementieren, Backup-Kopien von Daten erstellen und Proben eines rechtzeitigen Wiedereinspielens durchführen.

10.5.1 Backup von Informationen

<LT **1** | **2** | 3>
Maßnahme: Backup-Kopien von Informationen und von Software müssen regelmäßig, im Einklang mit der akzeptierten Backup-Methode, erstellt und getestet werden.
Die in ISO/IEC 27002 Kapitel 10.5.1 empfohlenen Maßnahmen gelten entsprechend.

10.6 Management der Netzsicherheit

Ziel: Informationen in Netzen und die unterstützende Infrastruktur zu schützen.
Das sichere Management von Netzen, die Organisationsgrenzen überspannen, erfordert sorgfältige Überlegungen über den Datenfluss, die legalen Implikationen, Überwachung und Schutz.
Zum Schutz sensitiver Informationen die über öffentliche Netze transportiert werden sollen, können zusätzliche Maßnahmen erforderlich sein.

10.6.1 Maßnahmen für Netze

<LT **1** | **2** | **3**>
Maßnahme: Um Netze vor Bedrohungen zu schützen die Sicherheit von Systemen und Anwendungen in Netzen zu erhalten sowie die übertragenen Informationen zu sichern, muss ein Netz angemessen verwaltet und kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 10.6.1 empfohlenen Maßnahmen gelten entsprechend.

10.6.2 Sicherheit von Netzdiensten

<LT 1 | 2 | 3>
Maßnahme: Sicherheitseigenschaften, Service Levels und Administrationsanforderungen aller Netzdienste müssen ermittelt und in eine Vereinbarung über Netzdienste aufgenommen werden. Dies sollte unabhängig davon sein, ob diese Dienste intern oder von externen Dienstleistern erbracht werden.
Die in ISO/IEC 27002 Kapitel 10.6.2 empfohlenen Maßnahmen gelten entsprechend.

Spezifische Implementierungsvorgabe des IS-Standards der ILfD
<LT **1** | **2** | 3>
Die Interoperabilität von Netzen ist eine entscheidende Komponente bei der Zusammenarbeit in der Leistungserbringung im Luftverkehr. Die Organisation muss daher folgende Mindestanforderungen zur Sicherheit der eigenen Netze einhalten:
Maßnahme: Folgende Mindestanforderungen zur Sicherheit der eigenen Netze müssen eingehalten werden:

- Firewall: Alle Verbindungen zur Organisationen die nicht als „Trusted“ eingestuft sind, werden ohne Ausnahme über geeignete Firewall-Systeme geführt.

- Proxy: Abhängig vom Schutzbedarf der Informationen sollten wo möglich externe Verbindungen über geeignete Reverse Proxy-Systeme mit zusätzlichen Zugriffskontrollmechanismen geführt werden. Hierzu zählen im erweiterten Sinne auch applikationsspezifische Gateways.
- Verschlüsselung: Abhängig vom Schutzbedarf der Informationen und dem verwendeten Transportweg müssen Daten verschlüsselt übertragen werden.
- Authentisierung: Externe User werden an der Netzwerkgrenze grundsätzlich einer Überprüfung unterzogen (z.B. Passwortverfahren, 2-Faktor-Authentisierung, Zertifikate).
- VPN: Der Aufbau von VPNs mittels Tunneltechnologie wird unterstützt (z.B. IPSec, SSL-VPN). Überwachung: Die Nutzung der Services wird protokolliert und überwacht. Interne Systemmeldungen (Log-Files) werden auf erkennbare Missbrauchsversuche (z. B. Passwortraten) überwacht.
- Verfügbarkeit: Die Verfügbarkeit der Systeme wird überwacht.
- Zusatzmaßnahmen: Soweit möglich werden zusätzliche Sicherheitsmaßnahmen wie IDS/IPS Systeme oder spezielles Applikationsdesign (Multi-Tier-Architektur) entsprechend dem jeweils aktuellen Stand der Technik und der jeweiligen Risikosituation eingesetzt.

10.7 Handhabung von Speicher- und Aufzeichnungsmedien

Ziel: Die unerlaubte Veröffentlichung, Veränderung, Entnahme oder Zerstörung von organisationseigenen Werten (Assets) sowie die Störung des Geschäftsbetriebs zu verhindern.
Speicher- und Aufzeichnungsmedien sollten kontrolliert und physisch geschützt werden.
Angemessene Verfahrensanweisungen sollten etabliert werden um Dokumente, Speicher-Medien (z. B. Bänder, Disketten), Ein-/Ausgabedaten und Systemdokumentation vor unerlaubter Veröffentlichung, Veränderung, Entnahme und Zerstörung zu schützen.

10.7.1 Verwaltung von Wechselmedien

<LT **1** | 2 | 3>
Maßnahme: Es müssen Verfahrensanweisungen für den Umgang mit Wechselmedien vorhanden sein.
Die in ISO/IEC 27002 Kapitel 10.7.1 empfohlenen Maßnahmen gelten entsprechend.

10.7.2 Entsorgung von Medien

<LT **1** | 2 | 3>
Maßnahme: Werden Medien nicht länger benötigt, müssen diese geschützt und sicher unter Anwendung formaler Verfahrensanweisungen entsorgt werden.
Die in ISO/IEC 27002 Kapitel 10.7.2 empfohlenen Maßnahmen gelten entsprechend.

10.7.3 Umgang mit Informationen

<LT 1 | 2 | 3>
Maßnahme: Verfahren für den Umgang mit und die Speicherung von Information müssen etabliert werden, um diese Informationen vor unerlaubter Veröffentlichung oder Missbrauch zu schützen.
Die in ISO/IEC 27002 Kapitel 10.7.3 empfohlenen Maßnahmen gelten entsprechend.

10.7.4 Sicherheit der Systemdokumentation

<LT 1 | 2 | 3>
Maßnahme: Systemdokumentation muss vor unbefugtem Zugriff geschützt werden.
Die in ISO/IEC 27002 Kapitel 10.7.4 empfohlenen Maßnahmen gelten entsprechend.

10.8 Austausch von Informationen

Ziel: Erhalt der Sicherheit von Informationen und Software, die innerhalb einer Organisation oder mit Externen ausgetauscht wird.
Der Austausch von Informationen und Software zwischen Organisationen sollte auf einem formalen Regelwerk basieren. Der Austausch sollte im Einklang mit den Austauschvereinbarungen vollzogen werden und mit allen gesetzlichen Anforderungen konform sein (siehe Abschnitt 15).
Verfahren und Standards sollten festgelegt sein, damit Informationen und Medien, die Informationen beinhalten, während des Transports geschützt sind.

10.8.1 Regelwerke und Verfahren zum Austausch von Informationen

<LT **1** | **2** | 3>
Maßnahme: Formale Leitlinien, Verfahren und Maßnahmen müssen vorhanden sein, um den Austausch von Informationen für alle Arten von Kommunikationseinrichtungen zu schützen.
Die in ISO/IEC 27002 Kapitel 10.8.1 empfohlenen Maßnahmen gelten entsprechend.

10.8.2 Vereinbarungen zum Austausch von Informationen

<LT **1** | 2 | 3>
Maßnahme: Vereinbarungen zum Austausch von Informationen zwischen der Organisation und Externen müssen getroffen werden.
Die in ISO/IEC 27002 Kapitel 10.8.2 empfohlenen Maßnahmen gelten entsprechend.

Spezifische Implementierungsvorgaben des IS-Standards der ILfD
<LT **1** | 2 | 3>
Die beteiligten Organisationen geben sich eine einheitliche Vereinbarung zum Austausch von Informationen untereinander. Die Vereinbarung wird regelmäßig oder nach Bedarf durch die Arbeitsgruppe Informationssicherheit der ILfD überarbeitet.

10.8.3 Transport physischer Medien

<LT 1 | 2 | 3>
Maßnahme: Medien, die Informationen beinhalten, müssen vor unbefugtem Zugriff, Missbrauch oder Verfälschung während des Transports, auch über Organisationsgrenzen hinweg, geschützt werden.
Die in ISO/IEC 27002 Kapitel 10.8.3 empfohlenen Maßnahmen gelten entsprechend.

10.8.4 Elektronische Mitteilungen/Nachrichten (Messaging)

<LT 1 | 2 | 3>
Maßnahme: Informationen, die in elektronischen Nachrichtendiensten (Messaging) verwendet werden, müssen angemessen geschützt werden.
Die in ISO/IEC 27002 Kapitel 10.8.4 empfohlenen Maßnahmen gelten entsprechend.

10.8.5 Geschäftsinformationssysteme

<LT 1 | 2 | 3>
Maßnahme: Verfahren und Regelwerke zum Schutz von Informationen, die zwischen Geschäftsanwendungen übertragen werden, müssen entwickelt und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 10.8.5 empfohlenen Maßnahmen gelten entsprechend.

10.9 E-Commerce-Anwendungen

Ziele: Die Sicherheit und die sichere Benutzung von E-Commerce-Anwendungen.
Die mit der Nutzung von E-Commerce-Anwendungen, einschließlich online Transaktionen, verbundenen Auswirkungen auf die Sicherheit sollten bedacht und Anforderungen für Maßnahmen überlegt werden. Die Integrität und Verfügbarkeit von elektronisch bereitgestellten Informationen mittels öffentlich zugänglicher Systeme sollte ebenfalls bedacht werden.

10.9.1 E-Commerce

<LT **1** | **2** | 3>
Maßnahme: Informationen für E-Commerce-Anwendungen, die über öffentliche Netze transportiert werden, müssen gegen betrügerische Aktivitäten, Vertragsstreitigkeiten, unberechtigte Veröffentlichung oder Veränderung geschützt werden.
Die in ISO/IEC 27002 Kapitel 10.9.1 empfohlenen Maßnahmen gelten entsprechend.

10.9.2 Online-Transaktionen

<LT **1** | **2** | 3>
Maßnahme: Informationen von Online-Transaktionen müssen geschützt werden, um unvollständige Übertragungen, Fehlleitungen, unbefugte Veränderung der Inhalte, Veröffentlichung, Verdopplung und Wiedereinspielen zu verhindern.
Die in ISO/IEC 27002 Kapitel 10.9.2 empfohlenen Maßnahmen gelten entsprechend.

10.9.3 Öffentlich verfügbare Informationen

<LT **1** | **2** | 3>
Maßnahme: Die Integrität von Informationen, die auf einem öffentlich zugänglichen System bereitgestellt werden, muss geschützt sein um unbefugte Veränderungen zu verhindern.
Die in ISO/IEC 27002 Kapitel 10.9.3 empfohlenen Maßnahmen gelten entsprechend.

10.10 Überwachung

Ziel: Aufdeckung nicht genehmigter informationsverarbeitender Aktivitäten.
Systeme sollten überwacht und Informationssicherheitsereignisse sollten aufgezeichnet werden. Protokollierungen der Administrationstätigkeiten und von Fehlern sollten dazu genutzt werden sicherzustellen, dass Probleme bei Informationssystemen identifiziert werden.
Alle Organisationen sollten die gesetzlichen Anforderungen an die Überwachung und Protokollierung erfüllen.
Systemüberwachung sollte dazu genutzt werden, die Effektivität der getroffenen Maßnahmen und die Konformität zur Zugriffskontrollregelung zu prüfen.

10.10.1 Auditprotokolle

<LT **1** | 2 | 3>
Maßnahme: Es müssen Auditprotokolle erstellt werden, in denen Benutzeraktivitäten, Fehler und Informationssicherheitsvorfälle festgehalten werden. Sie müssen für einen vereinbarten Zeitraum verwahrt werden, um in zukünftigen Untersuchungen und Überwachungen der Zugriffskontrolle behilflich zu sein.
Die in ISO/IEC 27002 Kapitel 10.10.1 empfohlenen Maßnahmen gelten entsprechend.

10.10.2 Überwachung der Systemnutzung

<LT 1 | 2 | 3>

Maßnahme: Es müssen Verfahren zur Überwachung der Nutzung informationsverarbeitender Einrichtungen entwickelt werden und die Ergebnisse der Überwachungen müssen regelmäßig überprüft werden.

Die in ISO/IEC 27002 Kapitel 10.10.2 empfohlenen Maßnahmen gelten entsprechend.

10.10.3 Schutz von Protokollinformationen

<LT 1 | 2 | 3>

Maßnahme: Protokollierungseinrichtungen und Informationen aus Protokollen müssen vor Verfälschung und unbefugtem Zugang geschützt werden.

Die in ISO/IEC 27002 Kapitel 10.10.3 empfohlenen Maßnahmen gelten entsprechend.

10.10.4 Administrator- und Betreiberprotokolle

<LT **1** | **2** | 3>

Maßnahme: Aktivitäten von Systemadministratoren und Betreibern müssen protokolliert werden.

Die in ISO/IEC 27002 Kapitel 10.10.4 empfohlenen Maßnahmen gelten entsprechend.

10.10.5 Fehlerprotokolle

<LT 1 | 2 | 3>

Maßnahme: Fehler müssen protokolliert und analysiert werden, und es müssen entsprechende Maßnahmen ergriffen werden.

Die in ISO/IEC 27002 Kapitel 10.10.5 empfohlenen Maßnahmen gelten entsprechend.

10.10.6 Zeitsynchronisation

<LT **1** | 2 | 3>

Maßnahme: Die Uhren aller wichtigen informationsverarbeitenden Systeme einer Organisation oder eines Sicherheitsbereichs müssen auf eine vereinbarte, genaue Referenzzeit synchronisiert werden.

Die in ISO/IEC 27002 Kapitel 10.10.6 empfohlenen Maßnahmen gelten entsprechend.

11 Zugangskontrolle

11.1 Geschäftsanforderungen für Zugangskontrolle

Ziel: Kontrolle des Zugangs zu Informationen.
Zugang zu Informationen, Informationsverarbeitenden Einrichtungen und Geschäftsprozessen sollte auf der Basis von Geschäfts- und Sicherheitsanforderungen kontrolliert werden.
Regeln für die Zugangskontrolle sollten Leitlinien für die Verbreitung von Informationen und für deren Autorisierung berücksichtigen.

11.1.1 Regelwerk zur Zugangskontrolle

<LT **1** | **2** | **3**>
Maßnahme: Leitlinien für die Zugangskontrolle müssen basierend auf Geschäfts- und Sicherheitsanforderungen etabliert, dokumentiert und regelmäßig kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 11.1.1 empfohlenen Maßnahmen gelten entsprechend.

11.2 Benutzerverwaltung

Ziel: Befugten Benutzern den Zugang zu Informationssystemen zu sichern und unbefugten Zugang zu Informationssystemen zu verhindern.
Formale Verfahren zur Kontrolle der Zuweisung von Zugangsrechten zu Informationssystemen und Diensten sollten etabliert sein.
Die Verfahren sollten alle Stadien im Lebenszyklus des Benutzerzugangs, von der erstmaligen Registrierung als neuer Benutzer bis zur endgültigen Löschung von Benutzern, die keinen Zugang zu Informationssystemen und Diensten mehr benötigen, abdecken. Besondere Aufmerksamkeit sollte dort, wo es angemessen ist, der Kontrolle der Zuweisung privilegierter Zugangsrechte geschenkt werden, die es ihren Benutzern erlauben Systemeinstellungen zu überschreiben.

11.2.1 Benutzerregistrierung

<LT **1** | **2** | **3**>
Maßnahme: Es muss für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und De-Registrierung zur Vergabe und Rücknahme von Zugangsberechtigungen geben.
Die in ISO/IEC 27002 Kapitel 11.2.1 empfohlenen Maßnahmen gelten entsprechend.

11.2.2 Verwaltung von Sonderrechten

<LT **1** | **2** | **3**>
Maßnahme: Die Zuweisung und Benutzung von Sonderrechten muss eingeschränkt und kontrolliert stattfinden.
Die in ISO/IEC 27002 Kapitel 11.2.2 empfohlenen Maßnahmen gelten entsprechend.

11.2.3 Verwaltung von Benutzerpasswörtern

<LT **1** | **2** | 3>
Maßnahme: Die Zuweisung von Passwörtern muss durch einen formalen Verwaltungsprozess kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 11.2.3 empfohlenen Maßnahmen gelten entsprechend.

11.2.4 Überprüfung von Benutzerberechtigungen

<LT **1** | **2** | 3>

Maßnahme: Benutzerberechtigungen müssen regelmäßig, unter Anwendung eines formalen Prozesses, durch das Management überprüft werden.

Die in ISO/IEC 27002 Kapitel 11.2.4 empfohlenen Maßnahmen gelten entsprechend.

11.3 Benutzerverantwortung

Ziel: Verhindern von unbefugtem Benutzerzugriff, Kompromittierung und Diebstahl von Informationen und informationsverarbeitenden Einrichtungen.

Die Mitarbeit der rechtmäßigen Benutzer ist für eine effektive Sicherheit essentiell.

Benutzer sollten sich ihrer Verantwortung um eine effektive Zugangskontrolle, besonders im Hinblick auf die Verwendung von Passwörtern und die Sicherheit von Gerätschaften, bewusst sein.

Der Grundsatz der leeren/aufgeräumten Schreibtische und des leeren Bildschirms (clean desk and clean screen) sollte umgesetzt sein, um das Risiko unbefugten Zugangs, oder der Beschädigung von Unterlagen, Informationsträgern und Informationsverarbeitenden Einrichtungen, zu verringern.

11.3.1 Passwortverwendung

<LT **1** | **2** | **3**>

Maßnahme: Benutzer müssen aufgefordert werden, guten Sicherheitspraktiken in der Auswahl und der Anwendung von Passwörtern zu folgen.

Die in ISO/IEC 27002 Kapitel 11.3.1 empfohlenen Maßnahmen gelten entsprechend.

11.3.2 Unbeaufsichtigte Benutzerausstattung

<LT **1** | **2** | **3**>

Maßnahme: Benutzer müssen sicherstellen, dass unbeaufsichtigte Ausstattung ausreichend geschützt ist.

Die in ISO/IEC 27002 Kapitel 11.3.2 empfohlenen Maßnahmen gelten entsprechend.

11.3.3 Der Grundsatz des aufgeräumten Schreibtischs und des leeren Bildschirms

<LT 1 | 2 | 3>

Maßnahme: Der Grundsatz des aufgeräumten Schreibtischs für Papiere und Wechselmedien sowie des leeren Bildschirms für informationsverarbeitende Einrichtungen muss Anwendung finden.

Die in ISO/IEC 27002 Kapitel 11.3.3 empfohlenen Maßnahmen gelten entsprechend.

11.4 Zugangskontrolle für Netze

Ziel: Verhinderung von unbefugtem Zugang zu Netzdiensten.

Zugang zu internen wie externen Netzdiensten sollte kontrolliert werden.

Benutzerzugang zu Netzen und Netzdiensten sollte durch die folgenden Punkte vor Kompromittierung geschützt sein:

a) Angemessene Übergänge existieren zwischen dem Netz der Organisation und Netzen, die anderen Organisationen gehören oder öffentlich zugänglich sind;
b) angemessenen Mechanismen zur Authentisierung von Benutzern und Ausstattung werden angewandt;
c) Zugangs- und Zugriffskontrolle für Benutzer von Informationsdiensten wird erzwungen.

11.4.1 Regelwerk zur Nutzung von Netzen

<LT 1 | 2 | 3>

Maßnahme: Benutzer dürfen nur Zugang zu den Netzdiensten bekommen, zu deren Nutzung sie ausdrücklich befugt sind.

Die in ISO/IEC 27002 Kapitel 11.4.1 empfohlenen Maßnahmen gelten entsprechend.

11.4.2 Benutzerauthentisierung für externe Verbindungen

<LT **1** | **2** | **3**>

Maßnahme: Zur Kontrolle des Zugangs von Benutzern mit Fernzugriff müssen angemessene Maßnahmen zur Authentisierung getroffen werden.

Die in ISO/IEC 27002 Kapitel 11.4.2 empfohlenen Maßnahmen gelten entsprechend.

11.4.3 Geräteidentifikation in Netzen

<LT 1 | 2 | 3>

Maßnahme: Die automatische Identifikation von Geräten als Mittel zur Authentisierung von Verbindungen von speziellen Orten und Geräten aus, muss in Betracht gezogen werden.

Die in ISO/IEC 27002 Kapitel 11.4.3 empfohlenen Maßnahmen gelten entsprechend.

11.4.4 Schutz der Diagnose- und Konfigurations-Ports

<LT 1 | 2 | 3>

Maßnahme: Der Zugang und Zugriff auf Diagnose- und Konfigurationsports muss einer Kontrolle unterliegen.

Die in ISO/IEC 27002 Kapitel 11.4.4 empfohlenen Maßnahmen gelten entsprechend.

11.4.5 Trennung in Netzwerken

<LT 1 | 2 | 3>

Maßnahme: Gruppen von Informationsdiensten, Benutzern und Informationssystemen müssen in Netzen getrennt gehalten werden.

Die in ISO/IEC 27002 Kapitel 11.4.5 empfohlenen Maßnahmen gelten entsprechend.

11.4.6 Kontrolle von Netzverbindungen

<LT **1** | **2** | **3**>

Maßnahme: Für gemeinsame Netze, besonders für die, die sich über die Grenzen einer Organisation hinaus erstrecken, muss die Möglichkeit der Benutzer sich an das Netz anzumelden eingeschränkt sein. Diese Einschränkung muss im Einklang mit der Zugangskontroll-Richtlinie und den Anforderungen der Geschäftsanwendungen (siehe 11.1) stehen.

Die in ISO/IEC 27002 Kapitel 11.4.6 empfohlenen Maßnahmen gelten entsprechend.

11.4.7 Routingkontrolle für Netze

<LT 1 | 2 | 3>

Maßnahme: Kontrollen für das Routing in Netzen müssen umgesetzt sein, um sicherzustellen, dass Computerverbindungen und Informationsflüsse nicht das Regelwerk zur Zugangskontrolle von Geschäftsanwendungen verletzen.

Die in ISO/IEC 27002 Kapitel 11.4.7 empfohlenen Maßnahmen gelten entsprechend.

11.5 Zugriffskontrolle auf Betriebssysteme

Ziel: Verhinderung des unbefugten Zugriffs auf das Betriebssystem.
Sicherheitseinrichtungen sollten dazu genutzt werden, den Zugriff zu Betriebssystemen auf befugte Benutzer zu beschränken. Die Einrichtungen sollten die folgenden Fähigkeiten haben:
a) Authentisierung befugter Benutzer gemäß eines definierten Regelwerks zur Zugangskontrolle;
b) Aufzeichnung von erfolglosen und erfolgreichen Authentisierungsversuchen;
c) Aufzeichnung der Verwendung spezieller Systemberechtigungen;
d) Alarmierung, wenn die Sicherheitsregelungen des Systems verletzt werden;
e Bereitstellung angemessener Funktionen zur Authentisierung;
f) Einschränkung der Sitzungsdauer eines Benutzers.

11.5.1 Verfahren für sichere Anmeldung

<LT **1** | **2** | **3**>
Maßnahme: Der Zugang zu Betriebssystemen muss durch ein sicheres Anmeldeverfahren kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 11.5.1 empfohlenen Maßnahmen gelten entsprechend.

11.5.2 Benutzeridentifikation und Authentisierung

<LT **1** | **2** | **3**>
Maßnahme: Alle Benutzer müssen eine eindeutige Benutzerkennung für ihren persönlichen Gebrauch haben, und eine angemessene Authentisierungstechnik muss eingesetzt werden, um die vorgegebene Identität eines Benutzers zu bestätigen.
Die in ISO/IEC 27002 Kapitel 11.5.2 empfohlenen Maßnahmen gelten entsprechend.

11.5.3 Systeme zur Verwaltung von Passwörtern

<LT **1** | **2** | **3**>
Maßnahme: Systeme zur Verwaltung von Passwörtern müssen interaktiv sein und qualitativ hochwertige Passwörter garantieren.
Die in ISO/IEC 27002 Kapitel 11.5.3 empfohlenen Maßnahmen gelten entsprechend.

11.5.4 Verwendung von Systemwerkzeugen

<LT 1 | 2 | 3>
Maßnahme: Die Verwendung von Dienstprogrammen, die in der Lage sind System und Anwendungseinstellungen zu überschreiben, muss eingeschränkt sein und genau kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 11.5.4 empfohlenen Maßnahmen gelten entsprechend.

11.5.5 Session Time-out

<LT 1 | 2 | 3>
Maßnahme: Inaktive Sitzungen müssen nach einer festgelegten Zeitspanne von Inaktivität geschlossen werden.
Die in ISO/IEC 27002 Kapitel 11.5.5 empfohlenen Maßnahmen gelten entsprechend.

11.5.6 Begrenzung der Verbindungszeit

<LT 1 | 2 | 3>
Maßnahme: Einschränkungen der Verbindungszeiten müssen verwendet werden um zusätzliche Sicherheit für Anwendungen mit hohem Risiko zu schaffen.
Die in ISO/IEC 27002 Kapitel 11.5.5 empfohlenen Maßnahmen gelten entsprechend.

11.6 Zugangskontrolle zu Anwendungen und Information

Ziel: Verhinderung des unbefugten Zugangs zu Informationen, die in Anwendungssystemen bereitgestellt werden.
Sicherheitseinrichtungen sollten dazu genutzt werden, den Zugang zu und innerhalb von Anwendungssystemen zu beschränken.
Logischer Zugang zu Anwendungssoftware und Informationen sollte auf berechtigte Benutzer beschränkt sein. Anwendungssysteme sollten:

a) Den Benutzerzugang zu Informationen und Funktionen des Anwendungssystems gemäß des definierten Regelwerks zur Zugangskontrolle kontrollieren;
b) Schutz vor unbefugtem Zugriff durch Werkzeuge, Betriebssystemsoftware und Schadsoftware bieten, die in der Lage sind Anwendungs- und Systemeinstellungen zu überschreiben.
c) Andere Systeme, mit denen Informationsressourcen geteilt werden, nicht kompromittieren.

11.6.1 Einschränkung von Informationszugriff

<LT **1** | **2** | **3**>
Maßnahme: Der Zugriff auf Informationen und Funktionen eines Anwendungssystems durch Benutzer und Supportpersonal muss gemäß dem definierten Regelwerk zur Zugangskontrolle eingeschränkt werden.
Die in ISO/IEC 27002 Kapitel 11.6.1 empfohlenen Maßnahmen gelten entsprechend.

11.6.2 Isolation sensibler Systeme

<LT 1 | 2 | 3>
Maßnahme: Sensitive Systeme müssen sich in einer dedizierten (isolierten) Umgebung befinden.
Die in ISO/IEC 27002 Kapitel 11.6.2 empfohlenen Maßnahmen gelten entsprechend.

11.7 Mobile Computing und Telearbeit

Ziel: Sicherstellen der Informationssicherheit bei der Benutzung von Einrichtungen für mobile Computing und Telearbeit.
Der notwendige Schutz sollte im Einklang mit den Risiken dieser spezifischen Art zu Arbeiten stehen. Wird Mobile Computing benutzt, so sollten die Risiken, die durch die Arbeit in ungeschützten Umgebungen entstehen, berücksichtigt und angemessene Maßnahmen getroffen werden. Im Fall der Telearbeit sollte die Organisation den Schutz des Telearbeitsplatzes sicherstellen und dafür sorgen, dass angemessene Vorkehrungen für diese Art der Arbeit getroffen worden sind.

11.7.1 Mobile Computing und Kommunikation

<LT **1** | 2 | 3>
Maßnahme: Um sich vor den Risiken bei der Verwendung von Mobile Computing und Kommunikationseinrichtungen zu schützen, muss eine formale Leitlinie vorhanden sein und angemessene Maßnahmen getroffen worden sein.
Die in ISO/IEC 27002 Kapitel 11.7.1 empfohlenen Maßnahmen gelten entsprechend.

11.7.2 Telearbeit

<LT 1 | 2 | 3>
Maßnahme: Regelungen und Betriebsanweisungen für Telearbeit sollten entwickelt und implementiert werden.
Die in ISO/IEC 27002 Kapitel 11.7.2 empfohlenen Maßnahmen gelten entsprechend.

12 Beschaffung, Entwicklung und Wartung von Informationssystemen

12.1 Sicherheitsanforderungen von Informationssystemen

Ziel: Sicherzustellen, dass Sicherheit ein integraler Bestandteil von Informationssystemen ist.
Informationssysteme beinhalten Betriebssysteme, Infrastruktur, Geschäftsanwendungen, Standardprodukte, Dienste und von Benutzern entwickelte Anwendungen. Das Design und die Implementierung von Informationssystemen, die Geschäftsprozesse unterstützen, können für die Sicherheit wesentlich sein. Sicherheitsanforderungen sollten vor der Entwicklung und Umsetzung von Informationssystemen identifiziert und vereinbart werden.
Alle Sicherheitsanforderungen sollten während der Phase der Anforderungsspezifikation eines Projektes identifiziert, begründet, vereinbart und als Teil des Geschäftsmodells des Informationssystems dokumentiert sein.

12.1.1 Analyse und Spezifikation von Sicherheitsanforderungen

<LT **1** | 2 | 3>
Maßnahme: Vorgaben von Geschäftsanforderungen an neue Informationssysteme, oder Erweiterungen von bestehenden Informationssystemen müssen die Anforderungen an Sicherheitsmaßnahmen spezifizieren.
Die in ISO/IEC 27002 Kapitel 12.1.1 empfohlenen Maßnahmen gelten entsprechend.

Spezifische Implementierungsvorgaben des IS-Standards der ILfD

<LT **1** | 2 | 3>
Die Erarbeitung von Standards für die Beschaffung, Entwicklung und Wartung von Informationssystemen, die bei Luftverkehrsorganisationen eingesetzt werden, kann zu einer Vereinfachung und Kostenreduktion bei den beteiligten Organisationen führen. Die einzelnen Organisationen sollten daher Ergebnisse von Überprüfungen von Informationssystemen den anderen Organisationen zur Verfügung stellen. Die Organisation, die die Ergebnisse zur Verfügung stellt, tut dies auf freiwilliger Basis und ohne Gewähr auf Richtigkeit.

12.2 Korrekte Verarbeitung in Anwendungen

Ziel: Verhinderung von Fehlern, Verlust oder unberechtigter Veränderung oder Missbrauch von Informationen in Anwendungen.
Es sollten angemessene Maßnahmen, die eine korrekte Verarbeitung sicherstellen, Bestandteil des Entwurfs von Anwendungen, inklusive eigenentwickelter Anwendungen, sein. Diese Maßnahmen sollten die Eingabe, die interne Verarbeitung und die Ausgabedaten prüfen.
Zusätzlichen Maßnahmen können für Systeme notwendig sein, die kritische, sensitive oder wertvolle Informationen verarbeiten oder Auswirkungen auf solche Informationen haben. Diese Maßnahmen sollten auf der Basis von Sicherheitsanforderungen und einer Risikobetrachtung bestimmt werden.

12.2.1 Überprüfung von Eingabedaten

<LT **1** | 2 | 3>
Maßnahme: Die Daten, die in Anwendungen eingegeben werden, müssen überprüft werden um sicherzustellen, dass diese Eingaben korrekt und angemessen sind.
Die in ISO/IEC 27002 Kapitel 12.2.1 empfohlenen Maßnahmen gelten entsprechend.

12.2.2 Kontrolle der internen Verarbeitung

<LT 1 | 2 | 3>

Maßnahme: Um die Beschädigung von Informationen durch Verarbeitungsfehler oder Vorsatz zu entdecken müssen Überprüfungen Bestandteil der Anwendung sein.
Die in ISO/IEC 27002 Kapitel 12.2.2 empfohlenen Maßnahmen gelten entsprechend.

12.2.3 Integrität von Nachrichten

<LT 1 | 2 | 3>

Maßnahmen: Anforderungen für die Sicherstellung von Authentizität und Integrität von Nachrichten in Anwendungen müssen identifiziert und entsprechende Maßnahmen ausgewählt und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 12.2.3 empfohlenen Maßnahmen gelten entsprechend.

12.2.4 Überprüfung von Ausgabedaten

<LT 1 | 2 | 3>

Maßnahme: Die Datenausgabe einer Anwendung müssen überprüft werden, um so sicherzustellen, dass die Verarbeitung gespeicherter Informationen korrekt und den Umständen angemessen ist.
Die in ISO/IEC 27002 Kapitel 12.2.4 empfohlenen Maßnahmen gelten entsprechend.

12.3 Kryptographische Maßnahmen

Ziel: Schutz der Vertraulichkeit, Integrität und Authentizität von Informationen durch Kryptographie.
Eine Leitlinie zum Einsatz von Kryptographie sollte entwickelt werden. Eine Verwaltung kryptographischer Schlüssel sollte zur Unterstützung der kryptographischen Techniken bereitstehen.

12.3.1 Leitlinie zur Anwendung von Kryptographie

<LT **1** | 2 | 3>

Maßnahme: Eine Leitlinie zur Anwendung von kryptographischen Maßnahmen zum Schutz von Informationen muss entwickelt und umgesetzt werden.
Die in ISO/IEC 27002 Kapitel 12.3.1 empfohlenen Maßnahmen gelten entsprechend.

12.3.2 Verwaltung kryptographischer Schlüssel

<LT **1** | 2 | 3>

Maßnahme: Zur Unterstützung der Anwendung kryptographischer Techniken in einer Organisation muss eine entsprechende Schlüsselverwaltung vorhanden sein.
Die in ISO/IEC 27002 Kapitel 12.3.2 empfohlenen Maßnahmen gelten entsprechend.

12.4 Sicherheit von Systemdateien

Ziel: Die Sicherheit von Systemdateien sicherzustellen.
Zugang zu Systemdateien und Programmquellen sollte kontrolliert werden und IT Projekte und unterstützende Aktivitäten auf eine sichere Art und Weise durchgeführt werden. Es sollte sorgfältig vermieden werden sensitive Daten in Testumgebungen offen zu legen.

12.4.1 Kontrolle von Software im Betrieb

<LT 1 | 2 | 3>
Maßnahme: Um die Installation von Software auf Systemen im Betrieb zu kontrollieren müssen entsprechende Verfahren vorgegeben sein.
Die in ISO/IEC 27002 Kapitel 12.4.1 empfohlenen Maßnahmen gelten entsprechend.

12.4.2 Schutz von Test-Daten

<LT 1 | 2 | 3>
Maßnahme: Test-Daten müssen sorgfältig ausgewählt, geschützt und kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 12.4.2 empfohlenen Maßnahmen gelten entsprechend.

12.4.3 Zugangskontrolle zu Quellcode

<LT 1 | 2 | 3>
Maßnahme: Der Zugriff auf Quellcode muss beschränkt sein.
Die in ISO/IEC 27002 Kapitel 12.4.3 empfohlenen Maßnahmen gelten entsprechend.

12.5 Sicherheit bei Entwicklungs- und Unterstützungsprozessen

Ziel: Erhalt der Sicherheit von Software und Informationen von Anwendungssystemen.
Projekt- und Supportumgebungen sollten streng überwacht werden.
Die verantwortlichen Manager für die Anwendungssysteme sollten ebenfalls für die Sicherheit der Projekt- und Supportumgebungen verantwortlich sein. Sie sollten sicherstellen, dass alle vorgeschlagenen Systemänderungen daraufhin kontrolliert werden, dass sie weder die Sicherheit des Systems noch die der Betriebsumgebung kompromittieren.

12.5.1 Änderungskontrollverfahren

<LT **1** | 2 | 3>
Maßnahme: Die Implementierung von Änderungen muss einem formellen Änderungskontrollverfahren unterliegen.
Die in ISO/IEC 27002 Kapitel 12.5.1 empfohlenen Maßnahmen gelten entsprechend.

12.5.2 Technische Kontrolle von Anwendungen nach Änderungen am Betriebssystem

<LT **1** | 2 | 3>
Maßnahme: Wenn Betriebssysteme geändert werden, müssen geschäftskritische Anwendungen überprüft und getestet werden, um sicherzustellen, dass es keine negative Auswirkungen für den Betrieb und die Sicherheit der Organisation gibt.
Die in ISO/IEC 27002 Kapitel 12.5.2 empfohlenen Maßnahmen gelten entsprechend.

12.5.3 Einschränkung von Änderungen an Softwarepaketen

<LT 1 | 2 | 3>
Maßnahme: Veränderungen an Softwarepaketen müssen so weit möglich verhindert, auf die notwendigen Änderungen begrenzt und alle Änderungen müssen streng kontrolliert werden.
Die in ISO/IEC 27002 Kapitel 12.5.3 empfohlenen Maßnahmen gelten entsprechend.

12.5.4 Ungewollte Preisgabe von Informationen

<LT 1 | 2 | 3>
Maßnahme: Gelegenheiten für eine ungewollte Preisgabe von Informationen müssen vermieden werden.

Die in ISO/IEC 27002 Kapitel 12.5.4 empfohlenen Maßnahmen gelten entsprechend.

12.5.5 Ausgelagerte Softwareentwicklung

<LT 1 | 2 | 3>

Maßnahme: Ausgelagerte Softwareentwicklung müssen durch die Organisation überwacht und beaufsichtigt werden.

Die in ISO/IEC 27002 Kapitel 12.5.5 empfohlenen Maßnahmen gelten entsprechend.

12.6 Schwachstellenmanagement

Ziel: Reduktion des Risikos der Ausnutzung veröffentlichter technischer Schwachstellen.
Der Umgang mit technischen Schwachstellen sollte auf eine effektive, systematische und wiederholbare Art umgesetzt sein. Er sollte Messungen beinhalten um die Effektivität nachzuweisen und Betriebssysteme und alle anderen genutzten Anwendungen abdecken.

12.6.1 Kontrolle technischer Schwachstellen

<LT **1** | **2** | **3**>

Maßnahme: Informationen über technische Schwachstellen müssen rechtzeitig für die verwendeten Informationssysteme bezogen werden, die Gefährdung der Organisation gegenüber solchen Schwachstellen bewertet und angemessene Maßnahmen getroffen werden, um das damit verbundene Risiko zu adressieren.

Die in ISO/IEC 27002 Kapitel 12.6.1 empfohlenen Maßnahmen gelten entsprechend.

13 Umgang mit Informationssicherheitsvorfällen

13.1 Melden von Informationssicherheitsereignissen und Schwachstellen

Ziel: Sicherstellen, dass Informationssicherheitsereignisse und Schwachstellen in Verbindung mit Informationssystemen so kommuniziert werden, dass rechtzeitig korrigierende Aktionen ergriffen werden können.
Formale Verfahren für das Melden von Ereignissen und für die Eskalation sollten etabliert sein. Die Meldeverfahren für die verschiedenen Arten von Ereignissen und Schwachstellen, die einen Einfluss auf die Sicherheit organisationseigener Werte haben können, sollten allen Mitarbeitern, Vertragsnehmern und Drittbenutzern bewusst gemacht werden. Sie sollten verpflichtet sein, alle Informationssicherheitsereignisse und Schwachstellen so schnell wie möglich an die ausgewiesene Anlaufstelle zu melden.

13.1.1 Melden von Informationssicherheitsereignissen

<LT **1** | **2** | 3>
Maßnahme: Informationssicherheitsereignisse müssen so schnell wie möglich über die geeigneten Managementkanäle gemeldet werden.
Die in ISO/IEC 27002 Kapitel 13.1.1 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | 2 | 3>
Die Organisation muss ein Security Incident Response Team aufstellen, das entsprechend ausgebildet ist und die Kompetenz besitzt, um umgehend auf Security Incidents zu reagieren und die notwendigen Maßnahmen einzuleiten.

Wenn ein Geschäftsprozess organisationsübergreifend betrieben wird, so müssen – entsprechend den Anforderungen und der Risikobewertung für diesen Geschäftsprozess – die vorhandenen, individuellen Security Incident Management Systeme aufeinander abgestimmt werden oder ggf. ein gemeinsames Security Incident Management der beteiligten Organisationen eingesetzt werden. Die Organisation muss dazu einen Verantwortlichen für Fragen zum Security Incident Management sowie die Kontakte für die operative Durchführung des Security Incident Management benennen.

Die Organisation muss darüber hinaus an vorhandenen organisationsübergreifenden Security Incident Management Systemen teilnehmen, die vom Staat oder privat-rechtlichen Organisationen im Luftverkehrsbereich betrieben werden.

Spezifische Implementierungsvorgaben des IS-Standards der ILfD
<LT **1** | 2 | 3>
Die Organisationen sollten Informationssicherheitsereignisse, die nachvollziehbar von Interesse für andere Organisationen sind, untereinander austauschen.

Um organisationsübergreifend Informationssicherheitsereignisse bearbeiten zu können, sollte die Organisation folgende Informationen über das Ereignis den anderen (betroffenen) Organisationen im Fall der Fälle zur Verfügung stellen – soweit schon vorhanden und soweit die Organisation diese nicht als vertraulich einstuft:
1. Beschreibung des Vorfalls
2. Auswirkungen des Vorfalls
3. Reaktive Maßnahmen zur Schadensbeseitigung
4. Proaktive Maßnahmen

13.1.2 Melden von Sicherheitsschwachstellen
<LT **1** | 2 | 3>
Maßnahme: Alle Angestellten, Auftragnehmer und Drittbenutzer von Informationssystemen und Dienstleistungen müssen verpflichtet sein, alle beobachteten oder vermuteten Sicherheitsschwachstellen in Systemen oder Dienstleistungen festzuhalten und zu melden.
Die in ISO/IEC 27002 Kapitel 13.1.2 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben
<LT **1** | 2 | 3>
Die Organisation muss erkannte Sicherheitsschwachstellen bei organisationsübergreifenden Geschäftsprozessen umgehend an die anderen beteiligten Organisationen melden.
Die Organisation muss an vorhandenen übergreifenden Gremien und Foren, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, teilnehmen, um Sicherheitsschwachstellen untereinander – soweit notwendig und für Dritte interessant – auszutauschen.

Spezifische Implementierungsvorgaben des IS-Standards der ILfD
<LT **1** | 2 | 3>
Die Arbeitsgruppe Informationssicherheit der ILfD unterhält eine Informationsplattform für Informationssicherheitsereignisse (siehe Kapitel 13.1.2) und -schwachstellen. Jede Organisation sollte erkannte Sicherheitsschwachstellen, die nachvollziehbar von Interesse für andere Organisationen sind, auf dieser Informationsplattform zur Verfügung stellen. Die Meldung sollte beinhalten:
- Schwachstelle
- Potentielle Bedrohung
- Potenziell betroffene Systeme/Ressourcen
- Mögliche Auswirkungen auf Geschäftsprozesse

13.2 Umgang mit Informationssicherheitsvorfällen und Verbesserungen

Ziel: Sicherstellen, dass ein einheitlicher und effektiver Ansatz für den Umgang mit Informationssicherheitsvorfällen angewandt wird.
Verantwortlichkeiten und Verfahren sollten etabliert sein, um Informationssicherheitsereignisse und Schwachstellen zu behandeln, sobald sie gemeldet wurden. Ein Prozess der kontinuierlichen Verbesserung sollte auf die Reaktion, Überwachung, Bewertung und den gesamten Umgang mit Informationssicherheitsvorfällen angewandt werden.
Wenn Beweise erforderlich sind, sollten diese gesammelt werden, um die Einhaltung gesetzlicher Anforderungen sicherzustellen.

13.2.1 Verantwortlichkeiten und Verfahren

<LT **1** | 2 | 3>
Maßnahme: Verantwortlichkeiten für den Umgang und Verfahren müssen eingerichtet werden, um eine schnelle, effektive und planmäßige Reaktion auf Informationssicherheitsvorfälle sicherzustellen.
Die in ISO/IEC 27002 Kapitel 13.2.1 empfohlenen Maßnahmen gelten entsprechend.

13.2.2 Lernen von Informationssicherheitsvorfällen

<LT **1** | 2 | 3>
Maßnahme: Es müssen Verfahren vorhanden sein, mit denen Art, Umfang und Kosten von Informationssicherheitsvorfällen bemessen und überwacht werden können.
Die in ISO/IEC 27002 Kapitel 13.2.2 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | 2 | 3>
Die Organisation muss an vorhandenen übergreifenden Organisationen, die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, teilnehmen, um gerade für übergreifende Geschäftsprozesse gemeinsam aus Sicherheitsvorfällen zu lernen und entsprechende Maßnahmen abzuleiten.

Spezifische Implementierungsvorgaben des IS-Standards der ILfD

<LT **1** | 2 | 3>
Organisationsintern gewonnen Erkenntnisse über Sicherheitsereignisse, die für andere Organisationen von Interesse sind, sollten anderen Organisationen zur Verfügung gestellt werden.

13.2.3 Sammeln von Beweisen

<LT 1 | 2 | 3>
Maßnahme: Wenn eine auf einen Informationssicherheitsvorfall folgende Aktion gegen eine Person oder Organisation rechtliche Schritte einschließt (entweder zivil- oder strafrechtlich), so müssen die gesammelten, aufbewahrten und vorgelegten Beweise die für die zuständige Gerichtsbarkeit erforderliche Beweisqualität aufweisen.
Die in ISO/IEC 27002 Kapitel 13.2.3 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT **1** | 2 | 3>
Die Organisation sollte mit CERTs (Computer Emergency Response Team), die vom Staat oder privatrechtlichen Organisationen im Luftverkehrsbereich betrieben werden, zusammenarbeiten.

14 Sicherstellung des Geschäftsbetriebs (BCM)

14.1 Informationssicherheitsaspekte bei der Sicherstellung des Geschäftsbetriebs (Business Continuity Management)

Ziel: Schutz vor Unterbrechungen von Geschäftsaktivitäten, und um kritische Geschäftsprozesse vor den Auswirkungen größerer Störungen von Informationssystemen oder vor Katastrophen zu schützen und ihre rechtzeitige Wiederaufnahme sicherzustellen.
Ein Business Continuity Management Prozess sollte umgesetzt werden, um die Auswirkungen auf die Organisation und die Wiederherstellung nach dem Verlust von Informationswerten (die z. B. Folge von Naturkatastrophen, Unfällen, Geräteausfällen und mutwilligen Beschädigungen sein können) durch eine Kombination vorbeugender und wiederherstellender Maßnahmen auf ein akzeptables Niveau zu minimieren. Dieser Prozess sollte die kritischen Geschäftsprozesse identifizieren und die Anforderungen der Informationssicherheit an Sicherstellung des Geschäftsbetriebs in andere Vorsorge-Anforderungen integrieren, die sich auf Aspekte wie Betrieb, Personal, Material, Transport und Einrichtungen beziehen.
Die Folgen von Katastrophen, Sicherheitsausfällen, den Verlust von Diensten und der Verfügbarkeit von Diensten sollten Gegenstand einer Business Impact Analyse (Analyse der Auswirkungen auf den Geschäftsbetrieb) sein. Notfall-Pläne sollten entwickelt und implementiert werden, um sicherzustellen, dass wesentliche Geschäftsprozesse in der erforderlichen Zeit wiederhergestellt werden können. Informationssicherheit sollte ein integraler Bestandteil des gesamten Prozesses zur Sicherstellung des Geschäftsbetriebs sein sowie von anderen Managementprozessen in der Organisation.
Zur Sicherstellung des Geschäftsbetriebs gehören auch Maßnahmen zur Identifizierung und Reduzierung von Risiken, zusätzlich zum allgemeinen Risikoeinschätzungsprozess, zur Begrenzung der Folgen von schädigenden Vorfällen, und um sicherzustellen, dass die für Geschäftsprozesse nötigen Informationen griffbereit sind.

14.1.1 Einbeziehen von Informationssicherheit in den Prozess zur Sicherstellung von BCM

<LT 1 | 2 | 3>
Maßnahme: In der gesamten Organisation muss ein gelenkter Prozess zur Sicherstellung des Geschäftsbetriebs entwickelt und aufrechterhalten werden, der die für die Sicherstellung des Geschäftsbetriebs (Business Continuity) erforderlichen Informationssicherheitsanforderungen in der Organisation behandelt.
Die in ISO/IEC 27002 Kapitel 14.1.1 empfohlenen Maßnahmen gelten entsprechend.

14.1.2 Sicherstellung des Geschäftsbetriebs und Risikoeinschätzung

<LT 1 | 2 | 3>
Maßnahme: Ereignisse, die Unterbrechungen in Geschäftsprozessen verursachen können, müssen identifiziert sein, zusammen mit Wahrscheinlichkeit und Auswirkung solcher Unterbrechungen und deren Konsequenzen für Informationssicherheit.
Die in ISO/IEC 27002 Kapitel 14.1.2 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT 1 | 2 | 3>
Für den betrachteten Geschäftsprozess müssen die beteiligten Organisationen eine Business Impact Analyse (BIA) durchführen. Diese muss in Anlehnung an BS 25999-1 und BSI-Standard 100-4 folgende Schritte enthalten:

- Auswahl der einzubeziehenden Organisationseinheiten und (Einzel-)Prozesse

- Kritikalitätsanalyse für die betreffenden Assets
  - Festlegung der Kritikalitätskategorien und Schadensszenarien
  - Festlegung der zu betrachtenden Bewertungsperioden
  - Besondere Termine und Ereignisse
  - Kritikalitätsanalyse
- Priorisierung der einzelnen Prozesse
- Erhebung der Ressourcen für Normal- und Notbetrieb
- Kritikalität und Wiederanlaufzeiten der Ressourcen
- Berichtslegung

Werden im laufenden Prozess Assets ausgetauscht, so dass Änderungen in der BIA nicht auszuschließen sind, muss die BIA neu durchgeführt werden. Die am Geschäftsprozess beteiligten Organisationen müssen umgehend darüber informiert werden.

14.1.3 Entwickeln und Umsetzen von Plänen zur Sicherstellung des Geschäftsbetriebs, die Informationssicherheit enthalten

<LT 1 | 2 | 3>

Maßnahme: Pläne müssen entwickelt und umgesetzt werden, um den Betrieb aufrechtzuerhalten oder wiederherzustellen, und um die Verfügbarkeit von Informationen im erforderlichen Maß und im erforderlichen Zeitraum nach Unterbrechungen oder Ausfällen von kritischen Geschäftsprozessen sicherzustellen.
Die in ISO/IEC 27002 Kapitel 14.1.3 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben

<LT 1 | 2 | 3>

Auf Basis der BIA müssen die beteiligten Organisationen einen Notfallplan erstellen. Dieser muss zumindest beinhalten:

- Verantwortlichkeiten
- Notfall-Situationen
- Ausweichmaßnahmen, alternative Betriebsverfahren
- Strukturierung der Notfallpläne
- Detaillierte Beschreibung der relevanten Notfallmaßnahmen
- Regelungen zu Prüfungen und Aktualisierungen der Notfallpläne

14.1.4 Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs

<LT 1 | 2 | 3>

Maßnahme: Ein Rahmenwerk für die Pläne zur Sicherstellung des Geschäftsbetriebs muss bereitgestellt werden, um so sicherzustellen, dass alle Pläne widerspruchsfrei sind, um Informationssicherheitsanforderungen einheitlich zu behandeln, und um Prioritäten für Tests und Instandhaltung zu identifizieren.
Die in ISO/IEC 27002 Kapitel 14.1.4 empfohlenen Maßnahmen gelten entsprechend.

14.1.5 Testen, Instandhaltung und Neubewertung von Plänen zur Sicherstellung von BCM

<LT 1 | 2 | 3>

Maßnahme: Pläne zur Sicherstellung des Geschäftsbetriebs müssen regelmäßig getestet und aktualisiert werden, um sicherzustellen, dass sie auf dem neuesten Stand und wirksam sind.
Die in ISO/IEC 27002 Kapitel 14.1.4 empfohlenen Maßnahmen gelten entsprechend.

Luftverkehrsspezifische Implementierungsvorgaben
<LT 1 | 2 | 3>
Notfallpläne müssen regelmäßig durch die beteiligten Organisationen getestet werden. Die daraus gewonnenen Ergebnisse müssen Input für die Verbesserung und Aktualisierung der Notfallpläne sein. Die Tests müssen dokumentiert werden. Um das Funktionieren der Notfallpläne sicherzustellen, müssen die beteiligten Organisationen folgendes durchführen:

- Test und Abnahme der Notfallpläne vor Inbetriebnahme des Systems / des Geschäftsprozesses
- Test und Abnahme der Notfallpläne bei kritischen System- und Prozessänderungen
- Regelmäßiger Test aller Notfallpläne

Der Umfang der Tests muss sich an der Kritikalität des Geschäftsprozesses orientieren.

15 Einhaltung von Vorgaben (Compliance)

15.1 Einhaltung gesetzlicher Vorgaben

Ziel: Vermeidung von Verstößen gegen Gesetze, amtliche oder vertragliche Verpflichtungen, und gegen jegliche Sicherheitsanforderungen.
Entwicklung, Betrieb, Nutzung und Verwaltung von Informationssystemen können gesetzlichen, amtlichen und vertraglichen Sicherheitsanforderungen unterliegen.
Ratschläge zu spezifischen gesetzlichen Anforderungen sollten von den Rechtsberatern der Organisation oder angemessen qualifizierten Juristen eingeholt werden. Gesetzliche Anforderungen sind von Land zu Land verschieden, und können sich ändern für Informationen, die in einem Land erzeugt und dann in ein anderes Land transferiert werden (d.h. grenzüberschreitender Datenfluss).

15.1.1 Identifikation der anwendbaren Gesetze
<LT 1 | 2 | 3>
Maßnahme: Alle relevanten gesetzlichen, amtlichen und vertraglichen Anforderungen und der Ansatz der Organisation, um diese Anforderungen zu erfüllen, müssen für jedes Informationssystem und für die Organisation ausdrücklich definiert, dokumentiert und aktuell gehalten werden.
Die in ISO/IEC 27002 Kapitel 15.1.1 empfohlenen Maßnahmen gelten entsprechend.

15.1.2 Rechte an geistigem Eigentum
<LT 1 | 2 | 3>
Maßnahme: Angemessene Verfahren sollten umgesetzt werden, um die Einhaltung gesetzlicher, amtlicher und vertraglicher Anforderungen für den Gebrauch von Material, wofür geistige Eigentumsrechte bestehen könnten, und für die Nutzung von urheberrechtlich geschützten Softwareprodukten, sicherzustellen.
Die in ISO/IEC 27002 Kapitel 15.1.2 empfohlenen Maßnahmen gelten entsprechend.

15.1.3 Schutz von organisationseigenen Aufzeichnungen
<LT 1 | 2 | 3>
Maßnahme: Wichtige Aufzeichnungen müssen im Einklang mit gesetzlichen, amtlichen, vertraglichen und geschäftlichen Anforderungen vor Verlust, Zerstörung und Fälschung geschützt werden.
Die in ISO/IEC 27002 Kapitel 15.1.3 empfohlenen Maßnahmen gelten entsprechend.

15.1.4 Datenschutz und Vertraulichkeit von personenbezogenen Informationen

<LT **1** | **2** | **3**>

Maßnahme: Datenschutz und Vertraulichkeit müssen sichergestellt werden, wie in einschlägigen Gesetzen, Vorschriften und gegebenenfalls Vertragsklauseln gefordert.

Die in ISO/IEC 27002 Kapitel 15.1.4 empfohlenen Maßnahmen gelten entsprechend.

15.1.5 Verhinderung des Missbrauchs von informationsverarbeitenden Einrichtungen

<LT 1 | 2 | 3>

Maßnahme: Benutzer müssen davon abgehalten werden, informationsverarbeitende Einrichtungen zu nicht genehmigten Zwecken zu benutzen.

Die in ISO/IEC 27002 Kapitel 15.1.5 empfohlenen Maßnahmen gelten entsprechend.

15.1.6 Regelungen zu kryptographischen Maßnahmen

<LT 1 | 2 | 3>

Maßnahme: Kryptographische Verfahren müssen im Einklang mit allen relevanten Vereinbarungen, Gesetzen und Vorschriften angewandt werden.

Die in ISO/IEC 27002 Kapitel 15.1.6 empfohlenen Maßnahmen gelten entsprechend.

15.2 Einhaltung von Sicherheitsregelungen und -standards sowie technischer Vorgaben

Ziel: Sicherstellung, dass Systeme die organisationsweiten Sicherheitsregelungen und -standards einhalten.
Die Sicherheit von Informationssystemen sollte regelmäßig überprüft werden.
Diese Überprüfungen sollten nach den zugehörigen Sicherheitsregelungen erfolgen, und die technischen Plattformen und Informationssysteme sollten untersucht werden, ob die anzuwendenden Standards für Sicherheitsimplementierungen und die dokumentierten Sicherheitsmaßnahmen eingehalten werden.

15.2.1 Einhaltung von Sicherheitsregelungen und -standards

<LT **1** | **2** | **3**>

Maßnahme: Manager müssen sicherstellen, dass alle Sicherheitsverfahren in ihrem Verantwortungsbereich korrekt angewandt werden, um die Einhaltung von Sicherheitsleitlinien und -standards zu erreichen.

Die in ISO/IEC 27002 Kapitel 15.2.1 empfohlenen Maßnahmen gelten entsprechend.

15.2.2 Prüfung der Einhaltung technischer Vorgaben

<LT **1** | **2** | **3**>

Maßnahme: Informationssysteme müssen regelmäßig auf die Einhaltung von Standards zur Umsetzung von Sicherheit überprüft werden.

Die in ISO/IEC 27002 Kapitel 15.2.2 empfohlenen Maßnahmen gelten entsprechend.

15.3 Überlegungen zu Revisionsprüfungen von Informationssystemen

Ziel: Maximierung der Effektivität und Minimierung der Störungen bei Revisionsprozessen für Informationssysteme.
Maßnahmen zur Sicherung der im Betrieb befindlichen Systeme und der Revisionswerkzeuge während des Audits von Informationssystemen sollten umgesetzt sein.
Darüber hinaus sind Maßnahmen erforderlich, um die Integrität der Revisionswerkzeuge zu schützen und ihren Missbrauch zu verhindern.

15.3.1 Maßnahmen für Revisionen von Informationssystemen

<LT 1 | 2 | 3>
Maßnahme: Anforderungen der Revision und Revisionsaktivitäten, die Prüfungen an im Betrieb befindlichen Systemen betreffen, müssen sorgfältig geplant und vereinbart werden, um das Risiko von Störungen der Geschäftsprozesse auf ein Mindestmaß zu reduzieren.
Die in ISO/IEC 27002 Kapitel 15.3.1 empfohlenen Maßnahmen gelten entsprechend.

15.3.2 Schutz von Revisionswerkzeugen für Informationssysteme

<LT 1 | 2 | 3>
Maßnahme: Der Zugriff auf Tools zur Untersuchung von Informationssystemen muss geschützt werden, um einen möglichen Missbrauch oder eine Gefährdung zu vermeiden.
Die in ISO/IEC 27002 Kapitel 15.3.2 empfohlenen Maßnahmen gelten entsprechend.

16 Annex A – Zusätzliche luftfahrtspezifische Maßnahmen

Dieser Annex definiert zusätzliche Schutzziele, Maßnahmen und Implementierungsvorgaben für spezifische Anwendungsgebiete, die eine besondere Rolle in der engen Zusammenarbeit von Luftverkehrsorganisationen spielen.

In jedem dieser Anwendungsgebiete können durch die Einhaltung von Kriterien „Level-of-Trust“ (LoT-A = Level-of-Trust eines Anwendungsgebietes) erreicht werden.

Achtung: Diese „Level-of-Trust für Anwendungsgebiete“ (LoT-A) sind nicht mit dem „Level-of-Trust einer Organisation“ (LoT-O) zu verwechseln, der durch die Maßnahmen in den Kapiteln 5 bis 15 bestimmt wird!

Erläuterung: Zusammenhang von „Level-of-Trust der Organisation“ (LoT-O) und „Level-of-Trust eines Anwendungsgebietes (LoT-A-xxx)

Für eine effiziente Zusammenarbeit, für die Auswahl von geeigneten Partnern oder für die Vergleichbarkeit von Partnern ist der „Level-of-Trust der Organisation“ (LoT-O) entscheidend. Wird eine Zusammenarbeit in einem der unten beschriebenen speziellen Anwendungsgebiete angestrebt, so muss ein Gesamt-Level-of-Trust für dieses Anwendungsgebiet (LoT-A) bestimmt werden.

Dabei ist zu berücksichtigen, dass die Vertrauensstellung für das Anwendungsgebiet (LoT-A) maximal der Vertrauensstellung des Kommunikationspartners (LoT-O) entsprechen kann (Minimumprinzip; Bsp.: Vertrauensstellung einer Verbindung ergibt LT1, Kommunikationspartner hat als Organisation aber nur LT2 → Verbindung kann auch nur LT2 erreichen und die entsprechenden Sicherheitsmaßnahmen sind zu ergreifen).

16.1 Sicherheit von Informationen in Webanwendungen und Web-Services (LoT-A-WEB)

Ziel: Sicherstellen, dass die Sicherheit von Informationen in und beim Austausch zwischen Webanwendungen/Webservices gewährleistet ist.

ISO/IEC 27002 Bereich 10.9

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

16.1.1 Parameter für die Vertrauensstellung der Webanwendung / des Web-Services

Folgende Parameter werden für die Ermittlung der Vertrauensstellung der Webanwendung / des Web-Services herangezogen.

16.1.1.1 Richtlinie für Webanwendungen/Web-Services

Es ist eine Richtlinie für Webanwendungen / Web-Services vorhanden ist, die im Speziellen die Authentizität und Integrität der Informationen berücksichtigt.

16.1.1.2 Entwicklung von Webanwendungen nach OWASP

Die Entwicklung von Webanwendungen erfolgt gemäß dem Development Guide von OWASP (siehe www.owasp.org). Die für den jeweiligen Anwendungsfall relevanten Regelungen sind umgesetzt.

16.1.1.3 Durchführung von Code Reviews

Die Organisation stellt sicher, dass CodeReviews für die Web-Applikationen durchgeführt werden. Dabei werden die Empfehlungen von OWASP (siehe www.owasp.org) berücksichtigt. Die für den jeweiligen Anwendungsfall relevanten Regelungen sind umgesetzt.

16.1.1.4 Kompetenz von Entwicklern für Webapplikationen

Die Organisation stellt sicher, dass die eingesetzten Entwickler für die Erstellung von sicheren Web-Anwendungen ausgebildet sind.

16.1.1.5 Durchführung von Penetrationstest der Applikationen

Die Organisation führt regelmäßig Penetrationstests der Applikationen gemäß Testing Guide der OWASP (siehe www.owasp.org) durch. Der Tester muss seine Befähigung für die Aufgabe durch entsprechende Nachweise (z. B. Teilnahme an Schulungen) belegt haben. Im laufenden Betrieb ist ebenfalls der Einsatz von generischen Schwachstellenscannern möglich.

16.1.1.6 Durchführung von Penetrationstest der Serverinfrastruktur

Die Organisation führt regelmäßig Penetrationstests der Serverinfrastruktur für Webapplikation durch. Der Einsatz von generischen Schwachstellenscannern für die Serverinfrastruktur ist möglich.

16.1.1.7 Einsatz von Web Application Firewall

Die Organisation setzt zum Schutz von Web-Anwendungen Web-Application Firewalls ein.

16.1.2 Ermittlung der Vertrauensstellung der Webanwendung / des Web-Services (LoT-A-WEB)

Die Vertrauensstellung der Webanwendung / des Web-Services wird wie folgt ermittelt.

Nr.	Richtlinie für Webanwendungen/ Web-Services	Entwicklung von Webanwendungen nach OWASP	Durchführung von Code Reviews	Kompetenz von Entwicklern für Webapplikationen	Durchführung von Penetrationstests der Applikationen	Durchführung von Penetrationstests der Serverinfrastruktur	Einsatz von Web Application Firewall	Maximal möglicher Level of Trust (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	n/a	n/a	n/a	n/a	n/a	n/a	UT

ja= Parameter erfüllt
nein = Parameter nicht erfüllt

Die dargestellte Tabelle wird regelmäßig durch die Arbeitsgruppe Informationssicherheit der ILfD aktualisiert und den Anforderungen angepasst.

Es ist zu berücksichtigen, dass die Vertrauensstellung der Webanwendung / des Web-Services (LoT-A-WEB) maximal der Vertrauensstellung des Kommunikationspartners (LoT-O) entsprechen kann (siehe dazu auch Kapitel 0).

16.1.3 Auswirkungen

Die Vertrauensstellung der Webapplikationen (LoT-A-WEB) muss mindestens so hoch sein, wie der Schutzbedarf bzgl. Vertraulichkeit, Integrität und Verfügbarkeit gemäß folgender Tabelle:

Schutzbedarfskategorie	Geforderter LoT-A-WEB
Sehr hoch	LT1
Hoch	LT1
Mittel	LT2
Gering	LT3

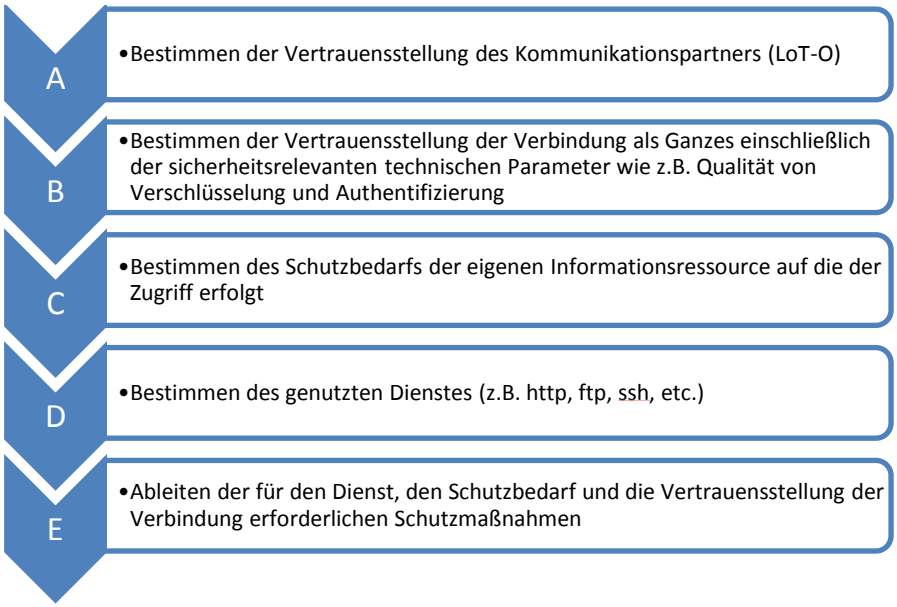
16.2 Organisationsübergreifende Verbindungen / externe Verbindungen (LoT-A-NET)

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

ISO/IEC 27002 Bereich 11.4

16.2.1 Ermittlung der erforderlichen Schutzmaßnahmen

Die Schutzmaßnahmen, die zur Absicherung von externen Verbindungen zu organisationsinternen Systemen zu treffen sind, werden nach folgendem Prozess ermittelt.



A) Bestimmen der Vertrauensstellung des Kommunikationspartners (LoT-O)

Die Vertrauensstellung des Kommunikationspartners erfolgt gemäß Kapitel 4.6 des vorliegenden Standards.

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

Es ist zu berücksichtigen, dass die Vertrauensstellung der Verbindung (LoT-A-NET) maximal der Vertrauensstellung des Kommunikationspartners (LoT-O) entsprechen kann (Bsp.: Vertrauensstellung Verbindung ergibt LT1, Kommunikationspartner hat als Organisation aber nur LT2 → Verbindung kann auch nur LT2 erreichen und die entsprechenden Sicherheitsmaßnahmen sind zu ergreifen).

Die Vertrauensstellung der Verbindung wird anhand der folgenden Parameter ermittelt.

16.2.1.1 Identität des Nutzenden

Bezüglich der Identität des Nutzenden werden drei Kategorien unterschieden:

- Partner: natürliche Person, zugehörig zu Partnerunternehmen
- Intern: natürliche Person, unternehmensintern
- Partnersystem: technische Entität des Partners, IT-System, keine natürliche Person

16.2.1.2 Endgeräteeigner

Bezüglich der Eignerschaft des Endgeräts (=Verfügungsgewalt über Gerät) werden drei Kategorien unterschieden:

- Partner
- Eigen, durch die Organisation verwaltete Endgeräte – sowohl physisch als auch virtualisiert (sofern entsprechend abgeschottet).
- Fremd

16.2.1.3 Anschlusspunkt / Schutz des Endgeräts:

Bezüglich des Anschlusspunkts bzw. des Schutzes des Endgeräts werden vier Kategorien unterschieden:

- Partnernetz, geschützt (PG):
  Bezeichnet Endgeräte und Netzanschlusspunkte die durch physische Maßnahmen zutrittsgeschützt sind. Drahtlose Anschlusspunkte sind mit kryptografischen Maßnahmen nach dem aktuellen Stand der Technik geschützt.
- Partnernetz, öffentlich (PÖ):
  Bezeichnet fest installierte Endgeräte und Netzanschlusspunkte von Partnerunternehmen in öffentlich zugänglichen Bereichen, wie z.B. Schalterhallen, Foyer, Lobby, Flughafenterminal, etc. Drahtlose Anschlusspunkte, die bezüglich der kryptografischen Schutzmaßnahmen nicht dem aktuellen Stand der Technik entsprechen, fallen ebenfalls in diese Kategorie.
- Öffentlich, geschützt (ÖG):
  Bezeichnet Endgeräte, die zeitweise an öffentlichen Netzanschlusspunkten betrieben werden, aber insofern geschützt sind, dass sie während des Einsatzes durch den Nutzer geschützt sind und nach Beendigung des Einsatzes wieder durch physische Maßnahmen zutrittsgeschützt werden. (i.A. Notebooks von Außendienstmitarbeitern Reisenden, etc.)
- Öffentlich, ungeschützt (ÖU):
  Bezeichnet vollständig ungeschützte Endgeräte, Netze und Netzzugangspunkte (z.B. öffentlich zugängliche Internetterminals)

16.2.1.4 Authentisierung der Verbindung

Bezüglich der Authentisierung werden drei Kategorien unterschieden:

- User/PW: Benutzerkennung und Passwort
- 2-Faktor
- Zertifikatsbasierte Authentisierung

16.2.1.5 Transfernetz

Bezüglich des Transfernetzes werden drei Kategorien mit der entsprechenden Verschlüsselung unterschieden:

- Internet:
  - Verschlüsselt, Site-to-Site VPN (sts)
  - Verschlüsselt, Client-to-Site VPN (cts)
  - Unverschlüsselt (u)
- Mietleitung (private oder virtuell private Netze, wie z.B. Leased Lines, eigener Backbone, MPLS VPN, SITA, Starnet, etc.):
  - Verschlüsselt (v)
  - Unverschlüsselt (u)
- Wählleitung (ISDN/PSTN):
  - Verschlüsselt (v)
  - Unverschlüsselt (u)

Nachfolgend dargestellte Tabelle zeigt die maximal mögliche Vertrauensstellung der Verbindung in Abhängigkeit von den jeweiligen technischen Parametern:

Nr.	Anwendungsszenario	Identität des Nutzenden	Endgeräteeigner	Anschlusspunkt / Schutz des Endgeräts	Authen-tisierung	Transfernetz	Maximal möglicher Level of Trust
1	Mitarbeiter des externen Partners, Endgerät des Partners im geschützten Bereich des Partnernetzwerks.	Partner	Partner	PG	User/PW, 2-Faktor	Internet (sts), Mietleitung (v,u), Wählleitung (v,u)	LT1
2	Mitarbeiter des externen Partners mit speziell gesichertem Firmennotebook (in eigener Hoheit, nicht in Partnerhoheit). Beliebige Anschlusspunkte.	Partner	Eigen	PG, PÖ, ÖG	2-Faktor	Internet (cts,sts), Mietleitung (v,u), Wählleitung (v,u)	LT1
3	Mitarbeiter des externen Partners mit Partnerendgerät in dessen Netzwerk (ungeschützten Bereich), 2-Faktor Authentisierung.	Partner	Partner	PÖ	2-Faktor	Internet (sts), Mietleitung (v,u), Wählleitung (v,u)	LT2
4	Mitarbeiter des externen Partners mit Partnerendgerät in dessen Netzwerk (ungeschützten Bereich).	Partner	Partner	PÖ	User/PW	Internet (sts), Mietleitung (v,u)	LT3
5	Mobiler Mitarbeiter des externen Partners mit Partnerendgerät. Netzanschlusspunkt ungeschützt.	Partner	Partner	ÖG	2-Faktor	Internet (cts)	LT2
6	Mitarbeiter des externen Partners mit beliebigem Endgerät. Beliebige Anschlusspunkte.	Partner	Fremd	ÖU	2-Faktor	Internet (cts)	LT3
7	Systemkopplung, nur technische Identitäten, Zugriff aus dem Rechenzentrum des Partnerunternehmens, nur für feste IP-Adressen zugelassen	Partnersystem	Partner	PG	User/PW, Zertifikat	Internet (sts), Mietleitung (v,u)	LT1
8	Systemkopplung, nur technische Identitäten, Zugriff aus dem öffentlich zugänglichen Bereich des Partnerunternehmens, Zertifikatsbasierte Authentisierung.	Partnersystem	Partner	PÖ	Zertifikat	Internet (sts), Mietleitung (v,u)	LT2
9	Systemkopplung, nur technische Identitäten, Zugriff aus dem öffentlich zugänglichen Bereich des Partnerunternehmens, nur für feste IP-Adressen zugelassen.	Partnersystem	Partner	PÖ	User/PW	Internet (sts), Mietleitung (v,u)	LT3
10	Eigener Mitarbeiter auf Reisen oder im Honmeoffice mit speziell gesichertem Firmennotebook, beliebiger Anschlusspunkt.	Intern	Eigen	PG, PÖ, ÖG	2-Faktor	Internet (cts,sts), Mietleitung (v,u), Wählleitung (v,u)	T
11	Eigener Mitarbeiter mit Firmengerät via ISDN.	Intern	Eigen	PG, PÖ, ÖG	2-Faktor	Wählleitung (v,u)	T
12	Eigener Mitarbeiter im Partnernetz (geschützten Bereich) an Endgerät des Partners .	Intern	Partner	PG	User/PW, 2-Faktor	Internet (sts), Mietleitung (v,u), Wählleitung (v,u)	LT1
13	Eigener Mitarbeiter mit Gerät des Partners im ungeschützten Bereich eines Partners.	Intern	Partner	PÖ	2-Faktor	Internet (sts), Mietleitung (v,u), Wählleitung (v,u)	LT1
14	Eigener Mitarbeiter mit Gerät des Partners im ungeschützten Bereich eines Partners.	Intern	Partner	PÖ	User/PW	Internet (sts), Mietleitung (v,u)	LT3
15	Eigener Mitarbeiter mit beliebigem Endgerät. Beliebige Netzanschlusspunkte.	Intern	Fremd	ÖU	2-Faktor	Internet (cts)	LT3
16	Eigener Mitarbeiter mit beliebigem Endgerät via ISDN.	Intern	Fremd	ÖU	User/PW	Wählleitung (v,u)	LT3

Legende:	
	ÖG = Öffentlich, geschütz ÖU = Öffentlich, ungeschützt PG = Partnernetz, geschützt PÖ = Partnernetz, ungeschützt sts = Site-to-Site VPN cts = Client-to-Site VPN v = Verschlüsselt u = Unverschlüsselt

Die dargestellte Tabelle wird regelmäßig durch die Arbeitsgruppe Informationssicherheit der ILfD aktualisiert und den Anforderungen angepasst.

C) Bestimmen des Schutzbedarfs der eigenen Informationsressource
Der Schutzbedarf der eigenen Informationsressource muss auf Basis des vorliegenden Standards definiert werden (siehe Kapitel 4.2.2).

D) Bestimmen des genutzten Dienstes
Der Dienst muss aus dem jeweiligen Verbindungswunsch ersichtlich sein.

E) Ableiten der Schutzmaßnahmen
Jede Organisation muss in Abhängigkeit von Schutzbedarf der internen Informationsressource und Vertrauensstatus der Verbindung für den relevanten Dienst die erforderlichen Schutzmaßnahmen definieren.

Die jeweiligen Schutzmaßnahmen in Abhängigkeit des LoT-A-NET / Schutzbedarf / Dienst müssen definiert werden. Ein Beispiel dazu findet sich in Anlage 2 dieses Dokuments.

16.2.2 Zusätzliche Maßnahmen
Folgende zusätzlichen Maßnahmen sind in allen Fällen zu berücksichtigen.

16.2.2.1 Audits von externen Verbindungen
Externe Übergänge müssen regelmäßig entsprechend aktueller Standards auf Sicherheitsschwachstellen nachvollziehbar auditiert werden.

16.2.2.2 Durchführung von Risikoanalysen für externe Verbindungen
Für Verbindungen die auf der Basis dieser gemeinsamen Parameter und Prozesse aufgebaut sind, kann auf die Durchführung einer formalen Risikoanalyse verzichtet werden. Für Verbindungen, bei denen diese Prozesse und Parameter nicht eingehalten werden können, muss eine formale Risikoanalyse durchgeführt werden.

16.2.3 Auswirkungen bei der Koppelung von Netzwerken
Die folgenden Beispiele haben empfehlenden Charakter. Jede Organisation ist berechtigt, zusätzliche Maßnahmen zu ergreifen oder einzelne empfohlene Maßnahmen nicht anzuwenden, soweit dies dem vorliegenden Standard nicht widerspricht.

Auswirkungen bei Einstufung LoT-A mit „Limited Trust 1 oder besser“
- Organisationen sollten den Zugriff von Kommunikationspartnern mit einer Einstufung als „Limited Trust 1 oder besser“ auf Applikationen nach dem need-to-have Prinzip gestatten. Die Verbindung muss durch eine Firewall abgesichert werden. Darüber hinausgehende applikationsspezifische Schutzmaßnahmen an der Netzwerkgrenze (wie z.B. Reverse Proxy) müssen nicht verpflichtend angewendet werden.

Auswirkungen bei Einstufung LoT-A mit „Limited Trust 2“
- Organisationen sollten den Zugriff von Kommunikationspartnern mit einer Einstufung als „Limited Trust 2“ auf Webapplikationen und Webservices nach dem need-to-have Prinzip gestatten. Die Verbindung sollte durch eine Firewall und einen Reverse Proxy geschützt werden, die sicherstellen, dass Verbindungen nur dann aufgebaut werden können, wenn sich die Nutzer erfolgreich am Netzwerkperimeter authentisiert haben.

- Eine Organisation sollte einem als „Limited Trust 2“ eingestuften Kommunikationspartner keinen Zugriff auf Daten mit sehr hohem Schutzbedarf gewähren, wenn die sich aus dem externen Zugriff ergebenden Sicherheitsimplikationen nicht im Vorfeld im Rahmen einer formalen Risikoanalyse untersucht wurden.

Auswirkungen bei Einstufung LoT-A mit „Limited Trust 3“

- Organisationen sollten Zugriffe von Kommunikationspartnern mit einer Einstufung als „Limited Trust 3“ auf interne Applikationen nur dann gestatten, wenn ein geeignetes Proxysystem auf Applikationsebene sicherstellt, dass die Applikation in der vorgesehenen Weise genutzt wird.
- Allgemein sollten alle Applikationen, die von Kommunikationspartnern der Kategorie „Limited Trust 3“ im Rahmen einer externen Verbindung genutzt werden, im Vorfeld formal auf ihre Resistenz gegenüber Missbrauchsversuchen geprüft worden sein.
- Eine Organisation sollte einem als „Limited Trust 3“ eingestuften Kommunikationspartner keinen Zugriff auf Daten mit hohem oder sehr hohem Schutzbedarf gewähren, wenn die sich aus dem externen Zugriff ergebenden Sicherheitsimplikationen nicht im Vorfeld im Rahmen einer formalen Risikoanalyse untersucht wurden.

16.3 Zertifikate / Public Key Infrastructure (LoT-A-PKI)

Ziel: Definition übergreifender Vereinbarungen zwischen in Unternehmen eingesetzten PKI-Lösungen um die Schutzanforderungen für übergreifende Geschäftsvorfälle und den sicheren Austausch von Informationen z.B. über E-Mail zu erfüllen.

16.3.1 Parameter für die Vertrauensstellung des Zertifikats Managements

Folgende Parameter werden für die Ermittlung der Vertrauensstellung von Zertifikate / Public Key Infrastrukturen herangezogen.

16.3.1.1 Richtlinie für Zertifikats / Public Key Infrastructure Management

Die Organisation besitzt eine Richtlinie für das Zertifikats / Public Key Infrastructure Management, in der Vorgaben und Prozesse geregelt sind.

16.3.1.2 Zentrale Vorgaben an das Zertifikats / Public Key Infrastructure Management System

Die Organisation betreibt ein zentrales Zertifikats Management System. Die Zertifikate werden im Format X509v3 erstellt.

Zu einer PKI, die nicht ausschließlich technischen Zwecken dient, existieren die folgenden Dokumente:

- Certificate Policy (CP)
- Certificate Practice Statement (CPS)

Für jede PKI, die ausschließlich technischen Zwecken dient, müssen technische Dokumentationen existieren, die den Betrieb und die Sicherheitsstandards der PKI dokumentieren

16.3.1.3 Management von Zertifikaten

Für die Vergabe und den Entzug von Zertifikaten sind nachvollziehbare Prozesse definiert.
Gültigkeiten von Zertifikaten sind nachvollziehbar dokumentiert.

16.3.2 Ermittlung der Vertrauensstellung des Zertifikats Managements (LoT-A-PKI)

Die Vertrauensstellung des Identity Managements wird wie folgt ermittelt.

Nr.	Richtlinie zu PKI/Zertifikaten	Zentrale Vorgaben	Management von Zertifikaten	Maximal möglicher Level of Trust (LoT-A-PKI)
1	ja	Ja (CP/CPS ist bei Partner bekannt)	ja	LT1
2	ja	ja	ja	LT2

Die dargestellte Tabelle wird regelmäßig durch die Arbeitsgruppe Informationssicherheit der ILfD aktualisiert und den Anforderungen angepasst.

16.3.3 Auswirkungen: Anerkennung von Zertifikaten / Public Key Infrastructure

Die Anerkennung von Zertifikaten / Public Key Infrastructure sollte auf der Einstufung der anderen Organisation (LoT-O) gemäß Kapitel 4.6 erfolgen. Die folgenden Beispiele haben empfehlenden Charakter. Jede Organisation ist berechtigt, zusätzliche Maßnahmen zu ergreifen oder einzelne empfohlene Maßnahmen nicht anzuwenden, soweit dies dem vorliegenden Standard nicht widerspricht.

Auswirkungen bei Einstufung LoT-A-PKI mit „Limited Trust 1“

- Die Organisation sollte die Public Key Infrastructure einer als „LoT-O 0“, „LoT-O 1“ eingestuften anderen Organisation für alle Anwendungsfälle anerkennen (z.B. durch Cross-Zertifizierung oder Import der jeweiligen CA-Zertifikate), z.B. für
  - Authentisierung von Systemen via Maschinenzertifikate
  - Code-Signaturen
  - Authentifizierung / Signatur & Verschlüsselung

Auswirkungen bei Einstufung LoT-A-PKI mit „Limited Trust 2“

- Die Organisation sollte Zertifikate von Einzelpersonen einer als „LoT-O 2“ oder höher eingestuften anderen Organisation nach vorheriger Prüfung anerkennen. Dies gilt jedoch nur für Signatur & Verschlüsselung ausschließlich von Informationen (z.B. E-Mail, Dokumente).

16.4 Identity Management (LoT-A-IDM)

Ziel: Definition von eindeutigen und sicheren Schnittstellen (Technologien & Standards) für systemübergreifende Plattformen zur zentralisierten Verwaltung von Benutzern bzw. Rollen, deren Konten und ggf. deren Berechtigungen in organisationsübergreifenden Geschäftsprozessen (Föderation).

16.4.1 Parameter für die Vertrauensstellung des Identity Managements

Folgende Parameter werden für die Ermittlung der Vertrauensstellung des Identity Managements herangezogen.

16.4.1.1 Richtlinie für Identity Management

Die Organisation besitzt eine Richtlinie für das Identity Management, in der die Vorgaben und Prozesse für das Identity Management geregelt sind.

16.4.1.2 Zentrale Vorgaben an das Identity Management System

Die Organisation betreibt nur ein zentrales Identity Management System. Die Quellsysteme (z.B. LDAP-Verzeichnisse, ActiveDirectory, dezentrale Datenbanken wie SAP etc.) des Identity Management Systems bieten pro Identität eine eindeutige Verknüpfung zu einer Entität im zentralen Identity Management System.

16.4.1.3 Eindeutige Repräsentation von Entitäten

Im organisationsübergreifenden Identity Management werden folgende Entitäten betrachtet:

- Menschen (People)
- Organisationseinheiten und organisatorische Rollen (Departments)
- Systeme (Systems)

Jede Entität der Organisation im zentralen Identity Management System wird durch eine eindeutige digitale Identität repräsentiert.

16.4.1.4 Verwaltung von Identitäten

Das bei der Organisation betriebene Identity Management stellt folgende zentrale Prozesse zur Verwaltung von digitalen Identitäten bereit und setzt diese in der IT-Infrastruktur um:

- Verwaltung von digitalen Identitäten
  - Erzeugung digitaler Identitäten
  - Ändern (Anpassen, Erweitern, Löschen) von Attributen einer digitalen Identität
  - Systematisches Bereitstellen (Provisionierung) dieser Informationen in angeschlossenen Systemen
  - Deaktivieren/Löschen von digitalen Identitäten
- Verwaltung von Benutzergruppen und Rollen (Berechtigungsprofilen)
  - Aufbereitung bereitgestellter Informationen (aus der Personaladministration und dem Organisationsmanagement) zur automatischen Administration von Rollen und Benutzergruppen
  - Automatische Bereitstellung von Benutzergruppen und Rollen in angeschlossenen Systemen
- Verwaltung von Berechtigungen für digitale Identitäten und Benutzergruppen

Jeder der oben genannten Prozesse ist im Identity Management nachvollziehbar abgebildet und dokumentiert.

16.4.1.5 Vergabe und Entzug von Berechtigungen

Für die Vergabe und den Entzug von Berechtigungen sind revisionssichere Genehmigungsprozesse definiert. Sie sind dezentral in der Organisation zusammen mit den Fachbereichen festgelegt. Die Vergabe

von Berechtigungen geschieht in Abhängigkeit von den individuellen Aufgaben und der Tätigkeitsklassifizierung eines jeden Mitarbeiters. Dabei erhält der Mitarbeiter nur diejenigen Berechtigungen, die er zur Ausübungen seiner Aufgaben tatsächlich benötigt. Die Vergabe sowie der Entzug sind dokumentiert.

16.4.1.6 Gültigkeit von Identitäten

Gültigkeiten von Identitäten sind nachvollziehbar je nach Quellsystem der Identität festgelegt:

1. über ein angeschlossenes Personal-Wirtschaftssystem oder über ein angeschlossenes Corporate Directory (für LT **1**)
2. ansonsten darf die Gültigkeit maximal 365 Tage nicht überschreiten; alternativ muss mindestens einmal jährlich eine Überprüfung der Gültigkeit erfolgen (für LT **2,** LT **3**).

16.4.1.7 Offenlegung von Identitäten

Die Organisation legt auf begründete Anfrage eines Partners, die Identitäten offen.

16.4.2 Ermittlung der Vertrauensstellung des Identity Managements (LoT-A-IDM)

Die Vertrauensstellung des Identity Managements wird wie folgt ermittelt.

Nr.	Richtlinie zu Identity Management	Zentrale Vorgaben an das Identity Management System	Eindeutige Repräsentation von Entitäten	Verwaltung von Identitäten	Vergabe und Entzug von Berechtigungen	Gültigkeit von Identitäten	Offenlegung von Identitäten	Maximal möglicher Level of Trust (LoT-A-IDM)
1	ja	ja	ja	ja	ja	über ein angeschlossenes Coporate Directory oder ein angeschlossenes Personal-Wirtschaftssystem	ja	LT1
2	ja	nein	ja	nein	ja	Gültigkeit < 365 Tage oder jährliche Überprüfung	ja	LT2
3	alle anderen Kombinationen							UT

ja= Parameter erfüllt
nein = Parameter nicht erfüllt

Die dargestellte Tabelle wird regelmäßig durch die Arbeitsgruppe Informationssicherheit der ILfD aktualisiert und den Anforderungen angepasst.

Es ist zu berücksichtigen, dass die Vertrauensstellung de Identity Managements (LoT-A-IDM) maximal der Vertrauensstellung des Kommunikationspartners (LoT-O) entsprechen kann (siehe dazu auch Kapitel 0).

16.4.3 Auswirkungen: Anerkennung von Identitäten

Die Anerkennung von Identitäten sollte auf der Einstufung der anderen Organisation gemäß Kapitel 4.6 erfolgen. Die folgenden Beispiele haben empfehlenden Charakter. Jede Organisation ist berechtigt, zusätzliche Maßnahmen zu ergreifen oder einzelne empfohlene Maßnahmen nicht anzuwenden, soweit dies dem vorliegenden Standard nicht widerspricht.

Auswirkungen bei Einstufung LoT-A-IDM mit „Limited Trust 0“, „Limited Trust 1“ und „Limited Trust 2“

- Die Organisation sollte Identitäten einer als „Limited Trust 0“, „Limited Trust 1“ oder „Limited Trust 2“ eingestuften anderen Organisation durch ein einfaches Genehmigungsverfahren anerkennen. Eine Kopplung von IDM-Systemen unterschiedlicher Organisationen (Föderation) kann nur bei LT 0 oder LT1 erfolgen.

Auswirkungen bei Einstufung LoT-A-IDM mit „Limited Trust 3“ oder „Untrusted“

- Die Identitäten einer als „Limited Trust 3“ oder „Untrusted“ eingestuften Organisation sollten als externe Identitäten auf Basis der definierten Maßnahmen in diesem Standard behandelt werden und nach einem zu definierenden Genehmigungsverfahren eine digitale Identität mit einer eindeutigen Kennzeichnung erhalten.

17 Anlage 1 – Kriterien zur Einstufung

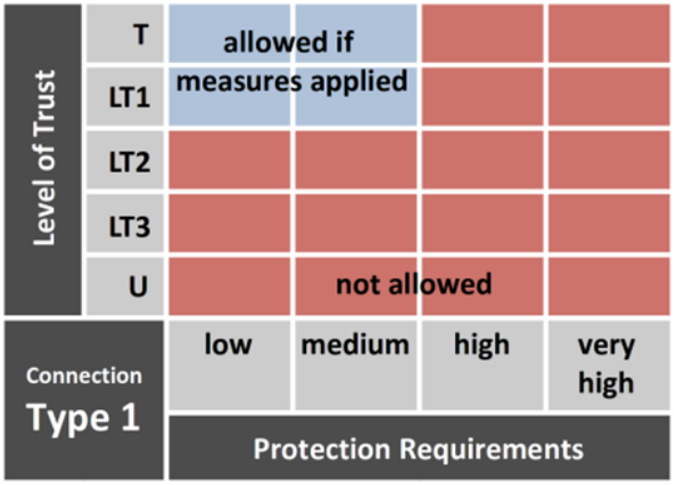
Die aktuellen Kriterien zur Einstufung des LoT-O finden sich in der beiliegenden Excel-Tabelle „11-09-05 CoPiP Controls + Tabellen 1.0.xlsx“.

18 Anlage 2 – Beispiel: Schutzmaßnahmen LoT-A-NET für FTP

Das nachfolgende Beispiel erläutert gem. 16.2.1 die Ableitung der in Abhängigkeit des LoT-A-NET / Schutzbedarf für den Dienst FTP:

18.1 FTP – Variante 1

Der Zugriff nach Variante 1 ist freigegeben für nachfolgend dargestellte Klassifikationen und Schutzbedarfe:

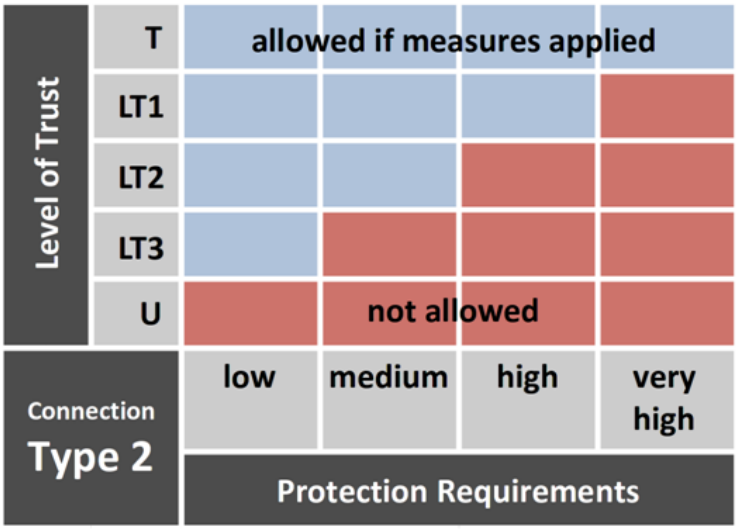


Nachfolgende Tabelle definiert die Schutzmaßnahmen, die für diesen Verbindungstyp umzusetzen sind.

Nr.	Bezeichnung	Anforderung
1	Portfilter	Portfilter an der Firewall erlaubt nur den benötigten Port
2	Authentisierung an der Netzwerkgrenze	Der Nutzer muss sich an der Netzwerkgrenze anmelden. Wahlweise geschieht dies an der Firewall, einem SSL-VPN-Gateway oder einem Proxy System.
3	Kontrolle am Zielsystem	Der Nutzer erhält nur die Rechte, die benötigt werden. Ein Schutz vor dem Übersteigen des Root-Directories des FTP-Servers muss gegeben sein. Ein Zugriff auf Systemdateien muss technisch unterbunden sein.
4	Feste IP-Adresse	Das externe Gerät muss eine eindeutige feste IP-Adresse aufweisen. Ein Zugriff von anderen IP-Adressen muss technisch unterbunden sein.

18.2 FTP – Variante 2

Der Zugriff nach Variante 2 ist freigegeben für nachfolgend dargestellte Klassifikationen und Schutzbedarfe:

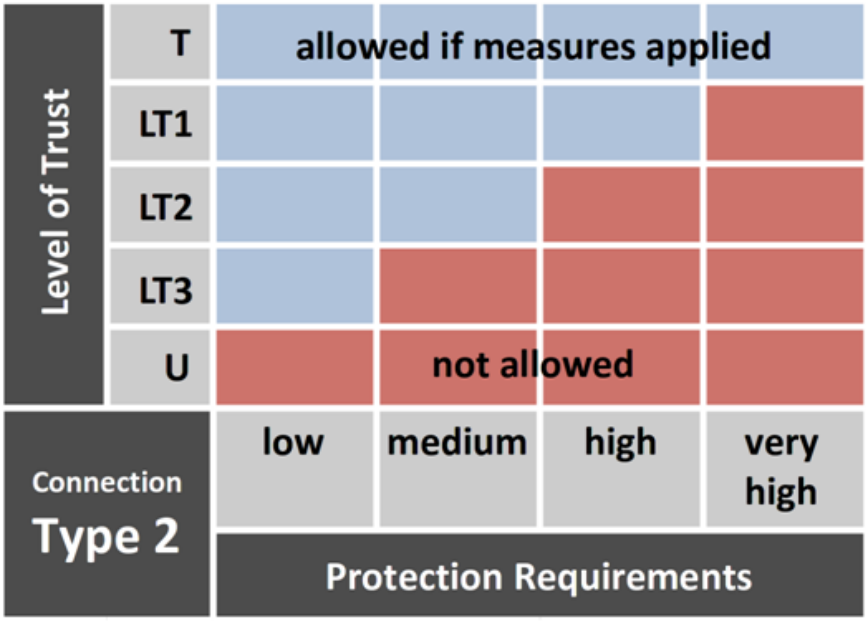


Nachfolgende Tabelle definiert die Schutzmaßnahmen, die für diesen Verbindungstyp umzusetzen sind.

Nr.	Bezeichnung	Anforderung
1	Portfilter	Portfilter an der Firewall erlaubt nur den benötigten Port
2	Reverse Proxy	Ein Reverse Proxy in der DMZ kontrolliert die Verbindung und stellt technisch sicher, dass nur auf Daten zugegriffen wird, für die der Zugriff gestattet ist.
3	Authentisierung an der Netzwerkgrenze	Der Nutzer muss sich an der Netzwerkgrenze anmelden. Wahlweise geschieht dies am SSL-VPN-Gateway oder einem Proxy System.
4	Kontrolle am Zielsystem	Der Nutzer erhält nur die Rechte, die benötigt werden. Ein Schutz vor dem Übersteigen des Root-Directories des FTP-Servers muss gegeben sein. Ein Zugriff auf Systemdateien muss technisch unterbunden sein.
5	Feste IP-Adresse	Das externe Gerät muss eine eindeutige feste IP-Adresse aufweisen. Ein Zugriff von anderen IP-Adressen muss technisch unterbunden sein.
6	Verschlüsselung außerhalb des internen Netzes	Nur bei Verbindungen über unsichere Netze wie z.B. das Internet oder WLAN.

18.3 FTP – Variante 3

Der Zugriff nach Variante 3 ist freigegeben für nachfolgend dargestellte Klassifikationen und Schutzbedarfe:



Nachfolgende Tabelle definiert die Schutzmaßnahmen, die für diesen Verbindungstyp umzusetzen sind.

Nr.	Bezeichnung	Anforderung
1	Portfilter	Portfilter an der Firewall erlaubt nur den benötigten Port
2	Reverse Proxy	Das SSL-VPN Gateway in der DMZ kontrolliert die Verbindung und stellt technisch sicher, dass nur auf Daten zugegriffen wird, für die der Zugriff gestattet ist.
3	Verschlüsselung	Das SSL-VPN Gateway verschlüsselt die Verbindung außerhalb des internen Netzes.
4	Authentisierung an der Netzwerkgrenze	Der Nutzer muss sich am SSL-VPN-Gateway anmelden.
5	Kontrolle am Zielsystem	Der Nutzer erhält nur die Rechte, die benötigt werden. Ein Schutz vor dem Übersteigen des Root-Directories des FTP-Servers muss gegeben sein. Ein Zugriff auf Systemdateien muss technisch unterbunden sein.
6	Feste IP-Adresse	Das externe Gerät muss KEINE eindeutige feste IP-Adresse aufweisen. Ein Zugriff von beliebigen Systemen im Internet ist gestattet.

18.4 FTP – Variante 4

Die Verbindung ist für alle Partner und Schutzbedarfe gestattet.

Lediglich der Schutzbedarf der Daten (nicht des Systems oder der Applikation) darf nicht höher eingestuft sein als „Mittel“. Dies gilt für die Schutzbedarfskategorien Vertraulichkeit, Verfügbarkeit und Integrität.

Soweit die Daten bezüglich ihres Schutzbedarfs höher Kategorisiert wurden besteht die Möglichkeit, die Daten über ein zugelassenes Verfahren (z.B. GPG, oder PGP) zu verschlüsseln und zu signieren. Der Schutzbedarf der verschlüsselten und signierten Daten bezüglich Vertraulichkeit und Integrität kann dann auf „Niedrig“ reduziert werden.