Bundesministerium
des Innern

Umsetzungsplan Bund 2017

Leitlinie für Informationssicherheit in der Bundesverwaltung

Inhaltsverzeichnis

1 Einleitung

Erfolgreiches Informationssicherheitsmanagement erfordert ein ausgewogenes Maß an Ablauf- und Aufbauorganisation und einen angemessenen Einsatz von Personal und Technik. Der „Umsetzungsplan für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (Umsetzungsplan Bund – UP Bund) aus dem Jahre 2007 bildet den zentralen Baustein für die Etablierung und Aufrechterhaltung von Prozessen zur mittel- und langfristigen Gewährleistung der Informationssicherheit in der Bundesverwaltung. Die Ziele des UP Bund 2007 haben nach wie vor Bestand und finden sich in den Zielen dieser Neufassung wieder. Geänderte Rahmenbedingungen (fortschreitende Digitalisierung, Verschärfung der IT-Sicherheitslage, neue Regelungen, Konsolidierung der IT des Bundes u.v.m.) machen es erforderlich, den UP Bund anzupassen. Die Neufassung des UP Bund wurde vom IT-Rat, dem zentralen Gremium für ressortübergreifende IT-Fragestellungen in der Bundesverwaltung, beauftragt.

Die Cyber-Sicherheitsstrategie für Deutschland 2016 bildet den ressortübergreifenden strategischen Rahmen für die Aktivitäten der Bundesregierung im Bereich Cyber-Sicherheit. Die hier formulierten strategischen Ziele und Maßnahmen sind zwingend umzusetzen.

Im UP Bund 2017 wurden daher zusätzlich zu den im UP Bund 2007 formulierten Anforderungen an die Informationssicherheit diejenigen Ziele und Maßnahmen aus der Cyber-Sicherheitsstrategie 2016 aus den Handlungsfeldern

1. sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung,
2. gemeinsamer Auftrag von Staat und Wirtschaft und
3. leistungsfähige und nachhaltige Cyber-Sicherheitsarchitektur

aufgenommen, für die die Behörden und weiteren Einrichtungen[1] der Bundesverwaltung zuständig sind.

[1] Zur besseren Lesbarkeit wird im Folgenden nur noch der Begriff der „Einrichtung“ verwendet. Darunter werden im Rahmen dieses UP Bund alle Behörden und weiteren Einrichtungen der Bundesverwaltung verstanden, die originär oder Kraft Entscheidung der zuständigen obersten Bundesbehörde unter den Geltungsbereich des UP Bund fallen. Der Begriff „Ressort“ wird im Zusammenhang mit Regelungen verwendet, die das Ministerium inklusive des jeweiligen Geschäftsbereichs betreffen.

Informationssicherheit umfasst einen umfangreicheren Bereich des Schutzes von Informationen. IT-Sicherheit ist ein Teilbereich der Informationssicherheit und beschäftigt sich gezielt mit dem Schutz der eingesetzten IT. Der UP Bund trifft jedoch keine Vorgaben und Regelungen für den Bereich des Geheim- und Sabotageschutzes.

Der UP Bund 2017 richtet sich auf die Schutzziele der Informationssicherheit, also auf die Vertraulichkeit, Verfügbarkeit und Integrität (inklusive der Unterfälle Authentizität, Zurechenbarkeit und Nichtabstreitbarkeit) der in den Einrichtungen der Bundesverwaltung erhobenen, verarbeiteten und genutzten Informationen.

Informationssicherheitsrelevante Ereignisse und Angriffe müssen systematisch aufgespürt werden (Detektion). Vor diesem Hintergrund legt der UP Bund 2017 nunmehr ein stärkeres Gewicht auch auf das strategische Handlungsfeld Detektion – zusätzlich zu den bereits im UP Bund 2007 genannten Handlungsfeldern Prävention, Reaktion und Nachhaltigkeit.

Auch das Thema der Sensibilisierung gewinnt an Bedeutung. Die besonders häufig erfolgreichen Angriffe, sogenannte Advanced Persistent Threat-Angriffe (APT), gelingen oft dadurch, dass Angreifer gezielt einzelne Mitarbeiterinnen und Mitarbeiter mit maßgeschneiderten E-Mails dazu bringen, Schadsoftware durch Öffnen einer E-Mail-Anlage oder eines in der E-Mail vorhandenen Links unbemerkt auf dem Arbeitsplatz-Rechner zu installieren. Um derartige Angriffe mittels des sogenannten „Social Engineerings“ zu erschweren, müssen Mitarbeiterinnen und Mitarbeiter verstärkt sensibilisiert werden, z.B. auch zum Umgang mit dienstlichen und persönlichen Daten in sozialen Netzwerken sowie im Umgang mit modernen Kommunikationsmitteln.

Die wachsende Verwundbarkeit der digitalen Infrastruktur sowie die damit verbundene Gefährdung staatlicher Strukturen bei terroristischen Angriffen, Angriffen im Cyberraum, Ausfall oder Störung von Informationstechnik oder auch Naturkatastrophen bedingen ein entsprechend darauf ausgerichtetes IT-Krisenmanagement des Bundes. Dieses bildet einen wichtigen Baustein im Rahmen des generellen Krisenmanagements des Bundes.

Wesentlich ist, dass das Informationssicherheitsmanagement nicht isoliert betrachtet werden darf. Es kann seine Wirksamkeit nur im Zusammenspiel mit anderen Bereichen entfalten. Hierbei sind insbesondere die Schnittstellen zum Datenschutz, zum Geheim- und Sabotageschutz, zum Notfall- und Krisenmanagement, aber auch zu den Organisationsbereichen der Einrichtungen der Bundesverwaltung zu nennen.

2 Grundsätze

Der Umsetzungsplan Bund 2017 (UP Bund 2017) ist die Informationssicherheitsleitlinie des Bundes und definiert die verbindlichen Rahmenbedingungen für den Schutz der in der Bundesverwaltung verarbeiteten Informationen und der dabei genutzten IT-Systeme, Dienste und Kommunikationsnetzinfrastrukturen des Bundes.

Er gilt für alle Ressorts und Bundesbehörden[2]. Soweit erforderlich, können die Ressorts den Anwendungsbereich des UP Bund für ihren Geschäftsbereich auf weitere Einrichtungen ausdehnen.

Die Regelungen des UP Bund 2017 sind von den Ressorts im jeweiligen Zuständigkeitsbereich eigenverantwortlich umzusetzen. Die Ressorts können hierzu eigene Durchführungsbestimmungen erlassen oder die Regelungen des UP Bund 2017 in eigene Regelungen und Vorschriften überführen. Bei der Umsetzung sind die Grundsätze der Verhältnismäßigkeit und der Wirtschaftlichkeit zu beachten.

Die Festlegungen in diesem Umsetzungsplan sind als verbindliche und einheitliche Mindestanforderungen zu verstehen. Sie sollen sicherstellen, dass

- in der Bundesverwaltung die aus den rechtlichen Vorgaben und Mindeststandards[3] resultierenden Anforderungen an die Informationssicherheit eingehalten werden,
- die Kontinuität der Geschäftsprozesse der Bundesverwaltung durch ein nachhaltiges sowie einheitliches Informationssicherheitsmanagement und ein angemessenes Mindestsicherheitsniveau hinsichtlich der Verfügbarkeit, der Vertraulichkeit und der Integrität der darin verarbeiten Informationen gewährleistet ist,
- die in der Bundesverwaltung bestehenden Dienst- oder Amtsgeheimnisse gewahrt werden und
- die für die Informationsverarbeitung genutzten IT-Systeme der Bundesverwaltung vor Manipulationen, unberechtigten Zugriffen und Informationsverlust geschützt sind.

[2] Aufgrund der besonderen Erfordernisse an das Informationsmanagement und die Informationstechnik im militärischen Bereich des BMVg einschließlich MAD sowie an die IT der Nachrichtendienste (BND, BfV) kann in diesen Bereichen im jeweils erforderlichen Maß von den Vorgaben des UP Bund abgewichen werden. Gleiches gilt für Einrichtungen des Bundes, die in das Europäische System der Zentralbanken (ESZB) bzw. das Single Resolution Board (SRB) eingebunden sind und diesbezüglich besondere Vorgaben zur Informationssicherheit zu beachten haben.

[3] Mindeststandards nach § 8 Absatz 1 BSIG zur Sicherung der Informationstechnik des Bundes.

Die Festlegung der Mindestanforderungen erfolgt auf Basis der Standards für IT-Grundschutz des BSI in der jeweils gültigen Fassung.

Für den Geltungsbereich des UP Bund 2017 wird bei Anwendung des modernisierten IT-Grundschutzes die darin beschriebene Standard-Absicherung als Mindestanforderung festgelegt, da sie im Wesentlichen der bislang geltenden klassischen IT-Grundschutz-Vorgehensweise entspricht. Eine Konkretisierung erfolgt durch einen Mindeststandard des BSI.

Vor dem Hintergrund der vorliegenden Entwürfe des modernisierten IT-Grundschutzes werden für den UP Bund 2017 folgende Begrifflichkeiten festgelegt:

- Im UP Bund 2007 wurde in Analogie zum bisherigen IT-Grundschutz die Bezeichnung IT-Sicherheitsbeauftragter (IT-SiBe) verwendet. Um Missverständnisse insb. bzgl. der Zuständigkeiten zu vermeiden, wird im UP Bund 2017 weiterhin der Begriff des IT-Sicherheitsbeauftragten verwendet und nicht der im modernisierten Grundschutz vorgesehene Begriff des Informationssicherheitsbeauftragten.
  Nach Inkrafttreten des modernisierten Grundschutzes muss ggf. gesondert über den Umgang bzw. die Abgrenzung des IT-Sicherheitsbeauftragten und des Informationssicherheitsbeauftragten entschieden werden.
- Der UP Bund 2017 verwendet ansonsten einheitlich die im modernisierten Grundschutz vorgesehenen Bezeichnungen Informationssicherheit, Informationssicherheitsprozess etc.
- Die „AG IT-Sicherheitsmanagement“ (AG IT-SiMa) wird in „AG Informationssicherheitsmanagement“ (AG ISM) umbenannt.

Die jeweiligen Zuständigkeiten anderer Stellen, die Schnittstellen zum Informationssicherheitsmanagement besitzen (Datenschutz, Geheim- und Sabotageschutz, Krisen- und Notfallmanagement usw.), bleiben von den in diesem Dokument getroffenen Regelungen unberührt.

Zusätzlich zu den im UP Bund 2017 festgelegten Mindestanforderungen gilt insbesondere:

- Die Mindeststandards des BSI auf Basis § 8 Absatz 1 BSIG sind zu beachten.
- Informationssicherheitsvorfälle sind gemäß der „Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG“ an das BSI zu melden.

- Soweit externe Auftragnehmer für die Bundesverwaltung Leistungen erbringen, sind diese bei der Auftragserteilung auf die Regelungen des UP Bund 2017 oder auf ressorteigene Regelungen/ Vorschriften, die diese umsetzen, im notwendigen Umfang zu verpflichten.
- Die Anforderungen der „Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung von Bund und Ländern“ des IT-Planungsrates sind verbindlich.

Der UP-Bund steht im Einklang mit der „IT-Strategie der Bundesverwaltung“ und ist konform zur „IT-Rahmenarchitektur IT-Steuerung Bund“.

3 Informationssicherheitsmanagementsystem (ISMS)

Das Informationssicherheitsmanagementsystem (ISMS) plant und steuert nachvollziehbar den Informationssicherheitsprozess unter Einbeziehung der definierten Rolleninhaber (Akteure). Dabei bilden die BSI-Standards den notwendigen Rahmen für das ISMS, innerhalb dessen die Ressorts und Einrichtungen eigenverantwortlich angemessene technische und organisatorische Informationssicherheitsmaßnahmen auswählen und umsetzen.

Aufgabe eines ISMS ist es, unter Berücksichtigung der Wirtschaftlichkeit ein dem Schutzbedarf der verarbeiteten Informationen angemessenes Informationssicherheitsniveau zu definieren, umzusetzen und aufrechtzuerhalten.

Hierzu bedarf es einer Informationssicherheitsstrategie sowie einer Informationssicherheitsorganisation und eines Informationssicherheitsprozesses. Die Informationssicherheitsorganisation ist eine Grundvoraussetzung für ein angemessenes und wirksames ISMS und bezieht alle relevanten Akteure ein. Für die Gewährleistung von Informationssicherheit auf einem angemessenen Niveau innerhalb der gesamten Bundesverwaltung bedarf es sowohl innerhalb der einzelnen Ressorts und Einrichtungen als auch übergreifend für die Bundesverwaltung einer entsprechenden Organisationsstruktur, die den Informationssicherheitsprozess übergreifend plant, steuert und kontrolliert.

3.1 ISMS - Organisation und Aufgaben auf Bundesebene

Das ISMS des Bundes verzahnt das ISMS auf Bundesebene mit dem ISMS auf Ebene der Ressorts einschließlich der ISMS auf Ebene der Einrichtungen:

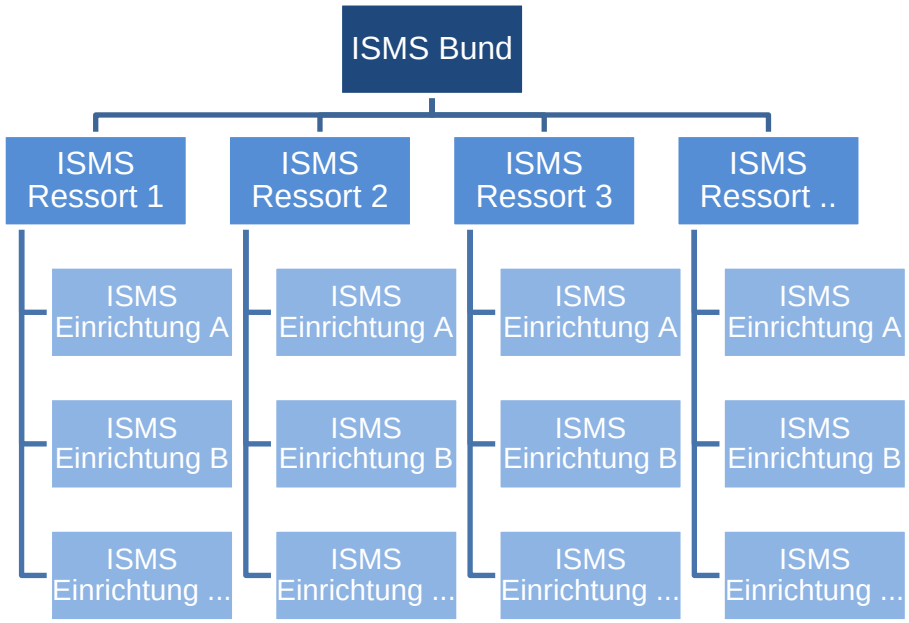

Abbildung 1: ISMS des Bundes

Zur Umsetzung einheitlicher Grundsätze innerhalb der gesamten Bundesverwaltung müssen der Rahmen für Regeln und Maßnahmen zentral vorgegeben und die Informationssicherheitsprozesse aufeinander abgestimmt werden. Dies erfolgt durch die übergreifende Organisation eines ISMS auf oberster Ebene, in dem Zuständigkeiten und Rollen festgelegt sowie Aufgaben verbindlich zugewiesen werden. Dieses ISMS auf Bundesebene wird durch die folgenden Einrichtungen und Rollen geprägt:

IT-Rat Der IT-Rat ist das oberste zentrale IT-Entscheidungsgremium in der Bundesverwaltung und für ressortübergreifende Fragen auf politisch-strategischer Ebene zuständig. Dabei ist er auch für Fragen der Informationssicherheit zuständig und übernimmt die strategische Steuerung des ISMS des Bundes.

Konferenz der IT-Beauftragten der Ressorts Die Konferenz der IT-Beauftragten der Ressorts ist verantwortlich für die operative IT-Steuerung der Bundesverwaltung sowie die Vorbereitung und Umsetzung der Beschlüsse des IT-Rats. Damit kommt ihr auch eine hohe Verantwortung bei der Steuerung des ISMS für die Bundesverwaltung zu.

Arbeitsgruppe Informationssicherheitsmanagement (AG ISM) Die Arbeitsgruppe Informationssicherheitsmanagement (AG ISM) berät die Konferenz der IT-Beauftragten und empfiehlt ihr Maßnahmen zur Sicherstellung angemessener Informationssicherheit in der Bundesverwaltung. Dazu gehört auch die Ausgestaltung und Weiterentwicklung der IT-Krisenreaktionsprozesse des Bundes. Die AG ISM bereitet entsprechende Beschlüsse der Konferenz der IT-Beauftragten vor und setzt diese um. Sie ist somit wesentlicher Bestandteil der IT-Steuerung des Bundes und daher im Rahmen ihrer Zuständigkeit in diese einzubinden.

Die AG ISM ist insbesondere zuständig für:

1. Begleitung der Umsetzung des UP Bund, insbesondere durch:
   a. Detaillierung, Bewertung und Abstimmung von ressortübergreifenden Anforderungen, Vorgaben und Maßnahmen bzgl. der Informationssicherheit in der Bundesverwaltung, unter Berücksichtigung der IT-Konsolidierung des Bundes
   b. Evaluierung und Vorbereitung von Vorschlägen für die notwendige Fortentwicklung des UP Bund zur Vorlage an den IT-Rat über die Konferenz der IT-Beauftragten
   c. Erstellung und Abstimmung eines jährlichen Sachstandsberichts zur Umsetzung des UP Bund für jedes Ressort
2. Weiterentwicklung der ressortübergreifenden IT-Krisenmanagementorganisation sowie des IT-Krisenreaktionsprozesses des Bundes
3. Gewährleistung des ressortübergreifenden Informationsflusses auf Arbeitsebene bzgl. der Belange der Informationssicherheit des Bundes

Näheres regelt die einstimmig zu beschließende Geschäftsordnung der AG ISM.

In diesem Gremium sind neben den obersten Bundesbehörden das BSI und die Bundesakademie für öffentliche Verwaltung (BAköV) vertreten. In dieses Gremium sind die Ressort-IT-SiBe zu entsenden. Anlassbezogen können CERT-Bund, das Nationale IT-Lagezentrum, das Nationale Cyber-Abwehrzentrum und weitere Akteure hinzugezogen werden.

Die Zentralstelle für IT-Beschaffung (ZIB) im Beschaffungsamt des BMI, der Ausschuss für Organisationsfragen der Bundesregierung (AfO), die zentralen IT-Dienstleister des Bundes sowie der/die Betreiber des Informationsverbundes Bonn-Berlin (IVBB)/ des Kerntransportnetzes Bund (KTN-Bund) / der Netze des Bundes (NdB) nehmen als regelmäßige Gäste beratend an den Sitzungen teil.

Die Federführung der AG ISM liegt beim für die Informationssicherheit der Bundesverwaltung zuständigen Referat des BMI.

Ressort-IT-Sicherheitsbeauftragter (Ressort-IT-SiBe) Die/der Ressort-IT-Sicherheitsbeauftragte (Ressort-IT-SiBe) unterstützt die Leitung des Ressorts im Rahmen ihrer/seiner Verantwortung für die Informationssicherheit im Geschäftsbereich, inklusive der Umsetzung des UP Bund. Der/dem Ressort-IT-SiBe kommt dabei die Aufgabe zu, in Abstimmung mit der Leitung des Ressorts Informationssicherheitsziele und Informationssicherheitsstrategien festzulegen und auf deren Umsetzung im eigenen Haus und im nachgeordneten Bereich hinzuwirken.

3.2 ISMS - Organisation und Aufgaben innerhalb des Ressorts/ der Einrichtung

Die Verantwortung für die Gewährleistung der Informationssicherheit trägt die Leitung einer Einrichtung als Teil der allgemeinen Leitungsverantwortung. Sie verantwortet die Einhaltung von gesetzlichen und sonstigen Anforderungen sowie von internen Regelungen, die Übernahme von Restrisiken, das Bereitstellen von Ressourcen für die Informationssicherheit und ist zuständig für die übergreifende Entscheidung hinsichtlich der Informationssicherheitsziele und der Informationssicherheitsstrategie. Die übergreifende Gesamtverantwortung für die Gewährleistung der Informationssicherheit eines Ressorts liegt bei der Leitung des Ressorts.

Für die effektive Wahrnehmung dieser Verantwortung und die effiziente Realisierung angemessener Informationssicherheit unterhält jede Einrichtung ein ISMS auf Basis der jeweils gültigen BSI-Standards. Dies schließt insbesondere die Bestellung einer/ eines IT-SiBe[4] ein.

Die IT-SiBe sind für die Planung, Umsetzung, Prüfung sowie die Verbesserung der Informationssicherheit inklusive der Umsetzung des UP Bund in ihrer Einrichtung zuständig. Sie sind berechtigt und verpflichtet[5], unmittelbar an die jeweilige Leitung zu berichten.

[4] Für sehr kleine Einrichtungen kann der Ressort-IT-SiBe Ausnahmen zulassen, wenn ein anderer IT-SiBe des Geschäftsbereichs die Rolle für diese Einrichtung wahrnimmt.

[5] Dies gilt nicht für die Tätigkeit der/ des IT-SiBe im Rahmen des Geheimschutzes.

Die Ressorts unterhalten zudem ein einrichtungsübergreifendes, ressortweites ISMS und benennen einen Ressort-IT-SiBe für ihren jeweiligen Geschäftsbereich.

Die Ressort-IT-SiBe wirken durch zentrale Planung, Koordination, Steuerung und Dokumentation des Informationssicherheitsprozesses im Ressort auf die Umsetzung der Informationssicherheitsziele und -strategien im Ressort hin. Damit unterstützen sie die Ressort-Leitung im Rahmen ihrer Verantwortung für die Informationssicherheit im Geschäftsbereich.

Die/der Ressort-/ IT-SiBe hat den erforderlichen Informationsfluss im Ressort/ in der Einrichtung zu gewährleisten und akute Sicherheitsempfehlungen und -warnungen als Teil des Informationssicherheitsmanagements unmittelbar zu berücksichtigen.

Wie die Wahrnehmung dieser Verantwortung im jeweiligen Zuständigkeitsbereich der Ressorts konkret organisiert und ausgestaltet wird (etwa durch Delegation), entscheiden die Ressorts in eigener Verantwortung. Dazu gehört ein geeignetes Berichtswesen einzurichten, um den notwendigen Informationsfluss in Richtung der Leitung der Einrichtung durch die/den IT-SiBe zu gewährleisten. Die organisatorische Stellung der/des IT-Sibe sollte diesen zudem in die Lage versetzen, organisationsweit verbindliche Vorgaben und Richtlinien zur Gewährleistung der Informationssicherheit zu formulieren.

Wie viele Personen in welcher Organisationsstruktur und mit welchen Ressourcen Fragen der Informationssicherheit behandeln, hängt von der Größe, Beschaffenheit und Struktur der jeweiligen Einrichtung ab. In größeren Einrichtungen gibt es neben der/dem IT-SiBe typischerweise weitere Rollen, die verschiedene Teilaufgaben zur Gewährleistung einer angemessenen Informationssicherheit wahrnehmen.

Aufgrund der immer komplexer werdenden IT-Infrastrukturen wird die Abstimmung mit anderen Bereichen innerhalb einer Einrichtung, die Schnittstellen zum Informationssicherheitsmanagement besitzen, immer wichtiger, um auch weiterhin Informationssicherheit effizient und effektiv gewährleisten zu können. Zur Behandlung übergreifender Themen sollte jede Einrichtung daher zudem ein Koordinierungsgremium Informationssicherheit etablieren.

Das Koordinierungsgremium Informationssicherheit hat die Aufgabe, das Zusammenwirken aller Organisationseinheiten und Managementdisziplinen in der Einrichtung mit Informationssicherheitsbezug (z.B. der/dem IT-SiBe, der/dem IT-Verantwortlichen, den Fachverantwortlichen, der/dem Sicherheitsbeauftragten, der/dem Datenschutzbeauftragten, der/ dem Notfallbe-

auftragten und dem Risikomanagement sowie in beratender Funktion der/dem Geheim- und Sabotageschutzbeauftragten) und der Leitung der Einrichtung zu koordinieren (siehe Kapitel 3.2.2) und bei Bedarf im Rahmen der jeweiligen Zuständigkeiten Maßnahmen abzustimmen.

3.2.1 Leitlinien zur Informationssicherheit und Sicherheitskonzeption[6]

Informationssicherheit ist im Rahmen eines Informationssicherheitsprozesses gemäß BSI-Standards zu gewährleisten. Dieser Prozess ist in einer ressortbezogenen Leitlinie unter Berücksichtigung der Informationssicherheitsziele und -strategien des Ressorts sowie weiterer, ressortspezifischer Gegebenheiten auf Basis eines PDCA-Modells zu beschreiben[7].

Die Informationssicherheitsziele und -strategien sind in der Informationssicherheitsleitlinie für das Ressort zu dokumentieren.

Einrichtungen erstellen jeweils eine eigene Leitlinie zur Informationssicherheit, die sie aus den ressortweiten Sicherheitszielen und -strategien sowie der Leitlinie des Ressorts ableiten. Die Leitlinie einer Einrichtung muss Regelungen zur geeigneten Einbindung des Koordinierungsgremiums Informationssicherheit in den Informationssicherheitsprozess enthalten.

Zuständig für die Erstellung, Abstimmung und Fortschreibung sowie für die Überprüfung der Einhaltung/ Umsetzung dieser Leitlinien ist die/der jeweilige Ressort-/ IT-SiBe.

Unter Berücksichtigung und Anwendung der BSI-Standards erstellen Einrichtungen eine auf die Einrichtung bezogene Sicherheitskonzeption, die auch Informationssicherheitskonzepte für einzelne Teilbereiche des gesamten Informationsverbundes (z.B. einzelne IT-Verfahren) enthalten kann.

Die Sicherheitskonzeption sowie einzelne Informationssicherheitskonzepte müssen die in ihrem jeweiligen Geltungsbereich verarbeiteten Informationen, die durchgeführte Schutzbedarfsfeststellung sowie die zum Schutz der Informationen erforderlichen technischen und organisatorischen Schutzmaßnahmen (inklusive Maßnahmen zur IT-Notfallvorsorge und IT-

[6] Sicherheitskonzeption gemäß BSI-Standards zum IT-Grundschutz

[7] Das PDCA-Modell berücksichtigt die Planung („Plan“), Umsetzung („Do“), Überprüfung der Umsetzung („Check“) sowie die Verbesserung bzw. Wiederherstellung der Informationssicherheit bzw. des Informationssicherheitsprozesses („Act“). Insbesondere Erkenntnisse aus Sicherheitsvorfällen, Notfällen oder Krisen können im Rahmen des PDCA-Modells zur Verbesserung genutzt werden.

Notfallbewältigung) einschließlich Risikobewertung und ggf. eine kompetenzgerechte Übernahme der Restrisiken dokumentieren. Informationssicherheitskonzepte zu allen kritischen Geschäftsprozessen (vgl. Kapitel 6) sind vorrangig zu erstellen. Die Sicherheitskonzeption sowie die einzelnen Informationssicherheitskonzepte werden durch Fortschreibungen in angemessenen Abständen aktualisiert und wirksam umgesetzt.

Das Koordinierungsgremium Informationssicherheit einer Einrichtung ist entsprechend der in der Leitlinie getroffenen Festlegungen in die Erstellung, Abstimmung, Umsetzung und Fortschreibung der Sicherheitskonzeption sowie einzelner Informationssicherheitskonzepte angemessen einzubinden. Das BSI kann auf Ersuchen der betroffenen Einrichtungen bei der Erstellung und Fortschreibung ihrer Sicherheitskonzeption sowie einzelner Informationssicherheitskonzepte beraten und unterstützen.

3.2.2 Aufbauorganisation, Rollen sowie Personal- und Finanzbedarf

Zur Planung und Steuerung des Informationssicherheitsprozesses bedarf es einer angemessen ausgestatteten Informationssicherheitsorganisation mit einer klaren Zuweisung von Aufgaben und Verantwortlichkeiten innerhalb eines Ressorts bzw. einer Einrichtung. Die zentrale Rolle in dieser Informationssicherheitsorganisation hat die/der Ressort-/ IT-SiBe inne. Die Einbindung der/des IT-SiBe in die Organisationshierarchie sollte an geeigneter Stelle so erfolgen, dass Interessen- und Rollenkonflikte vermieden werden[8].

Verantwortlich für die Bereitstellung der zur Gewährleistung der Informationssicherheit erforderlichen personellen und finanziellen Ressourcen ist die Leitung eines Ressorts/ einer Einrichtung. Unterstützung bei der Bemessung der erforderlichen Personalressourcen im Informationssicherheitsmanagement kann ergänzend zum Organisationshandbuch die „Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung“ des BSI bieten.

[8] Siehe hierzu auch Grundsatzpapier zum Informationssicherheitsmanagement der Rechnungshöfe des Bundes und der Länder (2015, 2. Korrektur): „*Der IT-Sicherheitsbeauftragte muss außerhalb des IT-Managements angesiedelt sein, um Interessen- und Rollenkonflikte zu vermeiden. Zusätzlich ist eine intensive Kontrolle des ISMS durch die Prüfungsinstanzen erforderlich. Die Aufgabenwahrnehmung könnte z. B. in der Zentralabteilung, außerhalb des IT-Referats oder vergleichbaren Organisationseinheiten erfolgen.*“

Wie bereits in Kapitel 3.2 beschrieben sollte zur besseren Verzahnung der verschiedenen Aufgabenbereiche innerhalb einer Organisation, die Schnittstellen zum und Überschneidungen mit dem Informationssicherheitsmanagement haben, zudem ein Koordinierungsgremium Informationssicherheit etabliert werden.

Das Koordinierungsgremium Informationssicherheit hat die Aufgabe, die übergreifenden Themen aus den Bereichen Informationssicherheit, IT-Notfallvorsorge und IT-Risikomanagement in Abstimmung insbesondere mit den für IT, Datenschutz, Geheim- und Sabotageschutz, Notfall- und Krisenmanagement, Risikomanagement sowie Organisation und Finanzen zuständigen Stellen und Externen, die mit der Wahrnehmung dieser Aufgaben betraut sind, zu behandeln und bei Bedarf im Rahmen der jeweiligen Zuständigkeiten Maßnahmen abzustimmen.

Die/der IT-SiBe lädt anlassbezogen, jedoch mindestens einmal jährlich, zu einer Sitzung des Koordinierungsgremiums ein.

Darüber hinaus regelt jede Einrichtung die Zusammensetzung des Koordinierungsgremiums, die jeweiligen Zuständigkeiten, Verantwortlichkeiten, Kompetenzen, Aufgaben sowie die Art und Weise der Zusammenarbeit innerhalb des Koordinierungsgremiums in eigener Verantwortung und dokumentiert diese. Die Einrichtung hat dabei sicherzustellen, dass die Mitglieder des Koordinierungsgremiums über die entsprechende Qualifikation verfügen.

Gibt es in der Einrichtung bereits ein ähnliches Gremium, können auch dessen Aufgaben entsprechend erweitert werden. In diesem Fall ist es Aufgabe der/des IT-SiBe, dafür zu sorgen, dass die übergreifenden Themen aus den o.g. Bereichen in dieses andere Gremium entsprechend eingebracht werden. Um die Bedeutung der Informationssicherheit zu unterstreichen, ist es jedoch ratsam, ein Koordinierungsgremium Informationssicherheit einzurichten und dieses regelmäßig einzuberufen.

3.2.3 IT-Risikomanagement

Damit die Leitung die Entscheidungen zum Umgang mit bestehenden Risiken im Bereich Informationssicherheit angemessen treffen kann, muss sie ausreichend und fortlaufend informiert werden. Ein zentraler Bestandteil des Informationssicherheitsprozesses und ISMS ist daher das IT-Risikomanagement. Für die Planung und Steuerung des IT-Risikomanagements und für die

angemessene Information der Leitung hinsichtlich der Risiken für die Informationssicherheit ist die/der IT-SiBe zuständig.

Das IT-Risikomanagement ist eng mit dem allgemeinen Risikomanagement der Einrichtung (bzw. dem Betriebskontinuitätsmanagement/ Business Continuity Management, BCM) abzustimmen. Der Umgang mit Risiken für die Informationssicherheit sowie die Bewertung möglicher Auswirkungen auf die Einrichtung sollten daher im Koordinierungsgremium Informationssicherheit unter geeigneter Einbeziehung des allgemeinen Risikomanagements der Einrichtung behandelt werden.

Die Leitung der Einrichtung entscheidet über umzusetzende Maßnahmen und übernimmt die Verantwortung für Restrisiken.

4 Personalentwicklung

Die Verbesserung der Informationssicherheit setzt voraus, dass alle Akteure innerhalb des ISMS, insbesondere aber die IT-SiBe, über ein angemessenes Fachwissen verfügen. Um dies zu gewährleisten, bedarf es einer dem jeweils individuell bereits vorhandenen Kenntnisstand entsprechenden Fort- und Weiterbildung[9]. Im Rahmen der Prävention hat die Einrichtung zudem geeignete Maßnahmen zur Sensibilisierung aller Beschäftigten zu konzipieren und regelmäßig durchzuführen.

Die Einrichtungen in der Bundesverwaltung müssen daher geeignete Konzepte für die Fort- und Weiterbildung sowie für die Sensibilisierung und Schulung zur Informationssicherheit erstellen und innerhalb dieses Rahmens die Konzepte auf einem einheitlichen Niveau eigenverantwortlich umsetzen.

Als zentraler Dienstleister für Fortbildung in der Bundesverwaltung unterstützt die BAköV die Einrichtungen des Bundes mit Konzepten und Fortbildungsangeboten. Neben Schulungen und Sensibilisierungen zur Informationssicherheit bietet die BAköV für die Vermittlung notwendiger Kompetenzen in der Bundesverwaltung eine Reihe von Fortbildungsmaßnahmen und Coachings an, wie z. B. Veranstaltungen zum Personalmanagement, Organisation, Haushalt, EU oder für

[9] Siehe u.a. auch Leitfaden „IT-Personal für die öffentliche Verwaltung gewinnen, binden und entwickeln“ des IT-Planungsrates

Führungskräfte, Projektbeteiligte oder Datenschutzschutzbeauftragte. Dieses Fortbildungsprogramm wird laufend bedarfs- und entwicklungsorientiert angepasst und ergänzt, sowie auch als Inhouse-Schulungen angeboten.

Die Fortbildungsangebote, Rahmenverträge, Konzepte und Materialien der BAköV sind so weit wie möglich zu nutzen.

4.1 Aus- und Fortbildung zur Informationssicherheit für verantwortliche Rollen

Die Aus- und Fortbildung ist als wesentlicher Baustein zur Herstellung und zum Erhalt der fachlichen Kompetenz von IT-SiBe, weiteren Beauftragten, den Akteuren im Bereich des ISMS, Führungskräften und IT-Fachpersonal zu etablieren und den aktuellen Entwicklungen anzupassen. Um ein einheitliches Basisniveau hinsichtlich der Kompetenzen und einer angemessenen Ausrichtung an den besonderen Bedürfnissen und Gefährdungen der Informationssicherheit für die Bundesverwaltung sicherzustellen, sind in der Aus- und Fortbildung folgende Rahmenbedingungen zu erfüllen:

- Die BAköV erstellt in Zusammenarbeit mit dem BSI ein geeignetes Basiskonzept für die Fortbildung und Zertifizierung der IT-SiBe und ggf. weiterer verantwortlicher Rollen im ISMS. Für die IT- SiBe der öffentlichen Verwaltung bietet die BAköV in Kooperation mit dem BSI begleitende und vertiefende Fortbildungsveranstaltungen, Aufbau-Kurse sowie themenspezifische Workshops an. Das BSI unterstützt die BAköV fachlich bei der Planung und Durchführung der Jahrestagung für IT- SiBe des Bundes.
  Die BAköV bietet auch einrichtungs- und aufgabenangepasste Fortbildungen im Bereich der Informationssicherheit an.
- IT- SiBe müssen– möglichst vor Aufnahme ihrer Tätigkeit – ein anforderungsgerechtes Fort- bzw. Weiterbildungsprogramm durchlaufen.
- Die mit einer Basisfortbildung erreichte Qualifikation soll durch den Erwerb des Zertifikats „IT-Sicherheitsbeauftragte/r in der öffentlichen Verwaltung" nachgewiesen werden.
- Die Einrichtungen müssen Kenntnisse und Qualifikationen zur Informationssicherheit bei Stellenausschreibungen und Stellenbesetzungen der Bundesverwaltung berücksichtigen, soweit diese für die jeweilige Tätigkeit relevant sind.

- Gleichermaßen ist auch die Integration der Themen der Informationssicherheit in die Aus- und Fortbildung (z.B. der HS Bund und des Bildungs- und Wissenschaftszentrums der Bundesfinanzverwaltung (BWZ) im Geschäftsbereich des BMF) zu gewährleisten.

4.2 Sensibilisierungen

Die Einrichtungen in der Bundesverwaltung haben sicherzustellen, dass alle Beschäftigten die für ihren Arbeitsplatz erforderlichen Informationssicherheitskenntnisse besitzen, informationssicherheitsrelevante Ereignisse frühzeitig als solche erkennen und darauf eigenverantwortlich mit sinnvollen Maßnahmen reagieren können.

Eine zentrale Aufgabe des ISMS ist es, alle Beschäftigten entsprechend der Gegebenheiten der Einrichtung für das Thema Informationssicherheit zu sensibilisieren. Die Maßnahmen zur Sensibilisierung müssen aktuelle technische Entwicklungen, neue Gefährdungen und neu erkannte Angriffsformen auf die Informationstechnologie sowie informationssicherheitsrelevante Besonderheiten der jeweiligen Einrichtung berücksichtigen.

Jede Einrichtung hat daher einen Prozess der Sensibilisierung zu etablieren, der alle Beschäftigten der Einrichtung in angemessenen Abständen erreicht.

Die BAköV unterstützt die Einrichtungen bei der Konzeption, Planung und Umsetzung des einrichtungsspezifischen Sensibilisierungsprozesses.

Einrichtungen haben auf die Gewährleistung der Anforderungen aus Informationssicherheit, Geheimschutz und Datenschutz zu achten und hierzu geeignete Maßnahmen zu ergreifen. Darüber hinaus müssen Einrichtungen, sofern sie die private Nutzung von Internet und elektronischer Kommunikation gestatten, Datenschutz, Informationssicherheit und Fragen der Netiquette im Rahmen von Dienstvereinbarungen und Hausanordnungen regeln sowie entsprechende Sensibilisierungsmaßnahmen für die Beschäftigen durchführen.

5 Evaluierung der Informationssicherheit

Zur Evaluierung der Informationssicherheit wird auf Bundesebene jährlich eine Erhebung des Sachstands zur Umsetzung des UP Bund 2017 durchgeführt. Auf Ebene der Ressorts werden dazu die Maßnahmen des UP Bund 2017 auf Zielorientierung sowie Effektivität hin evaluiert.

Informationssicherheitsmaßnahmen in den Einrichtungen müssen regelmäßig daraufhin überprüft werden, in wieweit sie die Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten Informationen gewährleisten.

Auf Ebene der Einrichtungen sind daher in angemessenen Abständen entsprechende Audits, Reifegradprüfungen, IS-Revisionen und Penetrationstests durchzuführen (siehe Kapitel 5.2).

Die Ergebnisse von Überprüfungen und Tests sowie die daraufhin eingeleiteten Maßnahmen sind in der Informationssicherheitsdokumentation festzuhalten.

5.1 Maßnahmen auf Bundesebene

Zur Evaluierung der Informationssicherheit auf Bundesebene führt die AG ISM jährlich eine Erhebung des Sachstands durch. Diese Erhebung bezieht sich auf die gesamte Bundesverwaltung einschließlich der zentralen IT-Dienstleister des Bundes im Leitungsverbund und der ressortübergreifenden Kommunikationsnetzinfrastruktur des Bundes.

Den Gesamtbericht zum Umsetzungsstand erstellt das BMI aus den Sachstandsberichten der Ressorts und der zentralen IT-Dienstleister im Leistungsverbund. Die Ressorts ihrerseits erstellen ihren Sachstandsbericht aus den Einzelsachstandsberichten ihres Geschäftsbereichs. Die zentralen IT-Dienstleister erstellen jeweils einen eigenen Sachstandsbericht, den sie über das Ressort, dem sie zugeordnet sind, an das BMI übermitteln.

Die Auswahl und Fortentwicklung der Methoden und Instrumente zur Erhebung des Umsetzungsstandes obliegt der AG ISM.

Die AG ISM leitet den Bericht dem IT-Rat über die Konferenz der IT-Beauftragten zur Erörterung zu. Bei Bedarf ist auch eine Kabinettbefassung mit einer Bewertung durch den IT-Rat vorzusehen.

Unabhängig davon werden im Hinblick auf die Evaluierung der Informationssicherheit auf Bundesebene folgende Festlegungen getroffen:

- Controlling-Maßnahmen bezüglich Informationssicherheit, die im Rahmen der IT-Steuerung des Bundes bzw. der IT-Konsolidierung ressortübergreifend etabliert werden sollen, sind zuvor mit der AG ISM abzustimmen.
- Die Methoden zur Evaluierung sind ressourcenschonend auszuwählen, insbesondere sind Doppelerhebungen (aufgrund anderer Controlling-Aktivitäten) zu vermeiden.
- Das Direktionsrecht der Leitungen der Einrichtungen sowie das Aufsichtsrecht der jeweils vorgesetzten Stellen sind angemessen zu beachten.
- Reifegradmodelle, die den Entwicklungsstand der Informationssicherheit beschreiben, können als ergänzende Möglichkeit zur Darstellung in den Sachstandsberichten herangezogen werden.

5.2 Ressort- und einrichtungsinterne Maßnahmen

Informationssicherheitsmaßnahmen müssen regelmäßig auf ihre wirksame Umsetzung, Aktualität, Vollständigkeit und Angemessenheit zur Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität hin überprüft werden. Entscheidend ist dabei, dass die notwendige Unabhängigkeit der Prüfer gewährleistet ist und dass sowohl technische als auch organisatorische und prozessuale Aspekte in die Prüfungen einbezogen werden.

Wie in Kapitel 3.2.1 dargestellt, müssen die Ressorts und Einrichtungen einen kontinuierlichen Verbesserungsprozess für das ISMS auf Basis des PDCA-Modells etablieren.

Zur Überprüfung der Informationssicherheitsmaßnahmen führen Einrichtungen in regelmäßigen Abständen sowie anlassbezogen geeignete Prüfungen z.B. in Form von Audits, Reifegradprüfungen, Revisionen oder Penetrationstests durch. Informationen oder Mitwirkungsleistungen der IT-Dienstleister des Bundes sind im Rahmen der hierfür etablierten Prozesse zu beauftragen. Die Prüfmaßnahmen können intern oder extern (durch geeignete Dritte) erfolgen. Bei der Durchführung von IS-Revisionen sind die Regelungen aus dem Leitfaden des BSI für die IS-Revision auf der Basis des IT-Grundschutzes zu beachten.

Die Anwendung der Mindeststandards, die Ergebnisse von Prüfungen sowie erfolgte Freigaben, die beim Schutz sämtlicher Informationen im Geltungsbereich des UP-Bund durchgeführt wer-

den, hat die/ der IT-SiBe (z.B. durch Konzepte, Zertifikate, Testate) zu dokumentieren, ebenso wie die daraus abgeleiteten Handlungsempfehlungen.

Besonderer Sorgfalt bedarf es vor der Inbetriebnahme neuer, direkt an das Internet angebundener Fachanwendungen. Dazu sind geeignete Maßnahmen (z.B. WebCheck, Penetrationstest) vor Inbetriebnahme durchzuführen und zu dokumentieren. Die Maßnahmen sind wahlweise vom BSI oder von einem vom BSI-zertifizierten Dienstleistungsunternehmen durchzuführen. Sofern das nicht möglich ist, kann ein anderes qualifiziertes und vertrauenswürdiges Dienstleistungsunternehmen beauftragt werden. Hierzu kann die Beratung durch das BSI in Anspruch genommen werden. Wesentliche Mängel sind vor einer Inbetriebnahme zu beseitigen. Die/ der zuständige IT-SiBe ist zu beteiligen.

6 Kritische Geschäftsprozesse

Sicherheitskonzepte, die kritische Geschäftsprozesse berühren, sind durch die/ den IT-SiBe im Rahmen des Informationssicherheitsprozesses prioritär zu behandeln.

Kritische Geschäftsprozesse sind solche, die für die Aufgabenerfüllung und Zielerreichung sowie zur Aufrechterhaltung des Geschäfts- bzw. Dienstbetriebs einer Einrichtung und für die Arbeitsfähigkeit der Bundesverwaltung, eines Ressorts oder einer Einrichtung von essentieller Bedeutung sind.

Für kritische Geschäftsprozesse sind daher im Rahmen des Notfallmanagements insbesondere Maßnahmen zur Sicherstellung der Arbeitsfähigkeit (Business Continuity) unter Anwendung der einschlägigen BSI-Standards zu treffen.

Im Rahmen des Notfallmanagements haben die Ressorts und Einrichtungen die Aufgabe, ihre kritischen Geschäftsprozesse zu identifizieren. Die Identifizierung erfolgt in eigener Verantwortung durch die Ressorts/ Einrichtungen[10].

Kritische Geschäftsprozesse weisen in der Regel einen höheren Schutzbedarf auf, insbesondere im Hinblick auf die Verfügbarkeit. Für die Absicherung von IT-Systemen und -Verfahren zu kri-

[10] Siehe z.B. Hochverfügbarkeitskompendium des BSI, Band AH, Kapitel 3.1 „Leitfaden zur Identifikation und Analyse kritischer Geschäftsprozesse“ oder die Broschüre „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement Leitfaden für Unternehmen und Behörden“ des BMI

tischen Geschäftsprozessen sind daher gegenüber Kapitel 5.2 erhöhte Anforderungen insbesondere im Hinblick auf die Verfügbarkeit, aber ggf. auch im Hinblick auf die Vertraulichkeit und/oder die Integrität zu erfüllen.

Ressorts/ Einrichtungen lassen IT-Systeme und -Verfahren zur Unterstützung kritischer Geschäftsprozesse in regelmäßigen Abständen durch geeignete Maßnahmen auf Risiken oder Mängel untersuchen und beseitigen diese in einer angemessenen Frist.

Die Wirksamkeit der Maßnahmen zur Absicherung der kritischen IT-gestützten Geschäftsprozesse ist gegenüber der Leitung einer Einrichtung nachzuweisen, z.B. durch geeignete Übungen, Auditberichte, Testate oder Zertifikate.

Die/der IT-SiBe unterstützt den Notfallbeauftragten des Ressorts/ der Einrichtung hinsichtlich der Ermittlung der umzusetzenden Maßnahmen zur Gewährleistung der Verfügbarkeit der kritischen IT-gestützten Geschäftsprozesse sowie der Überprüfung der Wirksamkeit der diesbezüglich getroffenen Maßnahmen.

7 Informationssicherheitsanforderungen an Dienstleister und Dienstleistungen

Wenn Externe mit der Erbringung von Dienstleistungen, insbesondere Informationssicherheitsberatung und IS-Revision, aber auch IT-Dienstleistungen im Allgemeinen beauftragt werden, sind Fachkenntnis, Erfahrung, Zuverlässigkeit und Vertrauenswürdigkeit von großer Bedeutung. Dies gilt insbesondere, wenn der Einsatz in sicherheitssensiblen Bereichen wie den kritischen Geschäftsprozessen erfolgt.

Im Rahmen der vergaberechtlichen Verpflichtungen haben die Einrichtungen für IT-Dienstleistungen stets zuverlässige und vertrauenswürdige Anbieter auszuwählen. Die Einrichtungen vereinbaren in Verträgen bzw. in Verwaltungsvereinbarungen mit den IT-Dienstleistern und Dritten ein angemessenes Niveau zur Einhaltung der Informationssicherheit. Dabei sind u.a. die relevanten Gesetze, Vorschriften und internen Regelungen des Ressorts bzw. der beauftragenden Einrichtung zur Informationssicherheit sowie die Regelungen des UP Bund 2017 zu berücksichtigen.

Für Unterauftragnehmer sind die o.g. Pflichten in gleicher Weise festzulegen.

Bei Vergaben nutzen die Einrichtungen vorrangig bestehende Rahmenverträge des Bundes, die durch die Zentralstelle für IT-Beschaffung (ZIB) für alle IKT-Produkte in Abstimmung mit dem BSI bzw. dem Anbieterbeirat des IT-Leistungsverbundes bereitgestellt werden.

Das BSI zertifiziert in seiner Rolle als zentraler Dienstleister für Informationssicherheit in der Bundesverwaltung Unternehmen – aber auch Einrichtungen des Bundes – für Informationssicherheitsberatungen und IS-Revisionen.

Bei Ausschreibungen ist die BSI-Zertifizierung der Dienstleistungsunternehmen bei der Auswahl als Kriterium angemessen zu berücksichtigen.

7.1 IT-Dienstleister und Provider

Für IT-Dienstleister (sowie deren Unterauftragnehmer) und deren Beauftragung gelten dieselben Anforderungen, wie sie in Kapitel „7. Informationssicherheitsanforderungen an Dienstleister und Dienstleistungen“ formuliert sind. Darüber hinaus haben IT-Dienstleister bzw. die beauftragende Einrichtung folgende Anforderungen zu erfüllen:

- Die Einrichtung vereinbart in Verträgen bzw. über Verwaltungsvereinbarungen mit IT-Dienstleistern die Einhaltung aller weiteren, im Rahmen der Leistungserbringung relevanten Vorgaben zur Informationssicherheit. Hierzu gehören z.B. das BSI-Gesetz, die EU-Datenschutzgrundverordnung, das Bundesdatenschutzgesetz, das Sicherheitsüberprüfungsgesetz, die Vorgaben des BSI IT-Grundschutzes zu Outsourcing, die einschlägigen Mindeststandards des BSI, die Leitlinie zur Informationssicherheit des Ressorts bzw. der Einrichtung usw..
- Die Einrichtung verpflichtet den IT-Dienstleister vertraglich bzw. in der Verwaltungsvereinbarung zur Gewährleistung der Informationssicherheit der Daten, die im Auftrag der Einrichtung vom IT-Dienstleister verarbeitet werden.
- Der IT-Dienstleister benennt für die vereinbarte Leistungserbringung einen Ansprechpartner für Informationssicherheit. Dieser hat informationssicherheitsrelevante Vorkommnisse im Zusammenhang mit der vereinbarten Dienstleistung unverzüglich an die/den zuständige/n IT-SiBe auf Seiten des Auftraggebers zu melden.

Für IT-Dienstleister und Provider, die wesentliche IT-Dienstleistungen oder IT-Dienstleistungen in sicherheitssensiblen Bereichen für eine Einrichtung, ein Ressort oder für die Bundesverwaltung erbringen (insb. Cloud-, Netz- und Infrastrukturdienste), gelten darüber hinaus folgende Anforderungen:

- Die IT-Dienstleister müssen über ein angemessenes und wirksames ISMS auf der Basis von BSI IT-Grundschutz verfügen, dessen Geltungsbereich die zu erbringende Dienstleistung vollumfänglich abdeckt. Das ISMS des IT-Dienstleisters und das ISMS des Ressorts/ der Einrichtung sind an den relevanten Schnittstellen angemessen aufeinander abzustimmen. Dies schließt die angemessene Notfallvorsorge und Notfallbewältigung gemäß BSI IT-Grundschutz ein.
- Der/die Auftraggeber/in verpflichtet den IT-Dienstleister dazu, für die Bereiche der vertraglich bzw. in der Verwaltungsvereinbarung geschuldeten Leistungserbringung Informationssicherheitskonzepte auf der Basis von BSI - IT-Grundschutz zu erstellen, diese mit dem Auftraggeber abzustimmen und über die gesamte Dauer der Leistungserbringung ununterbrochen aufrecht zu erhalten und aktuell zu halten.
- Der/die Auftraggeber/in lässt sich, seinen/ihren Aufsichtsorganen und den von ihm/ihr beauftragten Prüfern vom IT-Dienstleister vertraglich bzw. in der Verwaltungsvereinbarung ein angemessenes Prüf-/ IS-Revisionsrecht sowie ein Auskunfts- und Einsichtsrecht einräumen, um z.B. auch während des laufenden IT-Betriebes kurzfristig die Angemessenheit und Wirksamkeit der realisierten Maßnahmen aus den Informationssicherheitskonzepten zu überprüfen. Alternativ bzw. ergänzend kann dem BSI von der Auftraggeberin/vom Auftraggeber ein Prüf-/ IS-Revisionsrecht und ein Auskunfts- und Einsichtsrecht bei dem IT-Dienstleister eingeräumt werden.
- Für Notfälle und den Krisenfall werden besondere Vereinbarungen mit dem IT-Dienstleister (wie z.B. Befugnisse zur Sperrung vom Dienstleister zur Verfügung gestellter Dienste) getroffen und die ggf. erforderliche Beteiligung des BSI oder von Sicherheitsstellen der Ressorts vereinbart.

Der Auftragnehmer hat dafür Sorge zu tragen, dass für Unterauftragnehmer alle o.g. Regelungen in gleicher Weise getroffen werden.

Die konkrete Ausgestaltung dieser Anforderungen ist zwischen Auftraggeber und IT-Dienstleister vertraglich bzw. in Verwaltungsvereinbarungen zu regeln.

7.2 Produkte und produktbegleitende Services

Sichere IT-Produkte und -Systemkomponenten sind eine Voraussetzung für die Implementierung sicherer Informationsinfrastrukturen.

Das BSI veröffentlicht eine aktuelle Liste der vom BSI geprüften IT-Produkte. Es ist in Abstimmung mit dem betreffenden IT-Dienstleister des Bundes zu prüfen, welche vom BSI zertifizierten/zugelassenen Produkte für die jeweiligen Einsatzszenarien verfügbar sind.

Soweit es für den Einsatzzweck/die Anforderungen geeignete, vom BSI zertifizierte, zugelassene oder im Einzelfall empfohlene Produkte gibt, müssen die Ressorts und Einrichtungen diese bei Beschaffungsvorhaben angemessen berücksichtigen. Sofern kein entsprechendes Produkt den Zuschlag erhält bzw. keine geeignet zertifizierten Produkte bzw. Empfehlungen verfügbar sind, sind die Gründe hierfür zu dokumentieren. In jedem Fall müssen die nötigen Informationssicherheitsmaßnahmen gemäß dem zugrunde liegenden Schutzbedarf getroffen und dokumentiert werden.

Produkte sind nur solange zu verwenden, wie informationssicherheitsrelevante Updates zur Verfügung gestellt werden. Der Hersteller ist soweit möglich zu verpflichten, diese für einen angemessenen Zeitraum zu liefern. Ist eine Umstellung des Produktes auf eine aktuelle, mit Updates versorgte Version nicht möglich, sind geeignete Informationssicherheitsmaßnahmen zu treffen und die schnellstmögliche Aktualisierung anzustreben.

8 Informationssicherheit der ressortübergreifenden Kommunikationsnetzinfrastruktur des Bundes

Ressortübergreifend genutzte Kommunikationsnetzinfrastrukturen (Netze und netznahe Dienste) bilden das verlässliche Rückgrat der Kommunikation in der Bundesverwaltung inkl. der Regierungsebene[11]. In Teilbereichen wird zur Sicherstellung der Funktionen des Regierungshandelns in besonderen Lagen eine hohe Verfügbarkeit der ressortübergreifenden Kommunikationsnetzinfrastrukturen gewährleistet. Diese Netze unterliegen daher als zentrale Kommunikati-

[11] Dazu zählt derzeit insbesondere der „Informationsverbund Berlin-Bonn“ (IVBB), der sukzessive in die Netze des Bundes (NdB) migriert wird.

onsnetzinfrastruktur erhöhten Informationssicherheitsanforderungen. Sie verfügen über zentral bereitgestellte, leistungsfähige Schutzmechanismen, die vom BSI vorgegeben und zeitgemäß fortentwickelt werden.

Um die Informationssicherheit in ressortübergreifenden Kommunikationsnetzinfrastrukturen, in den eingesetzten IT-Systemen und in der von Nutzern an diese Netzinfrastrukturen angeschlossenen IT zu gewährleisten, sind die vom BSI formulierten Informationssicherheitsanforderungen an den Nutzer („Nutzerpflichten“) in der als Mindeststandard festgelegten Fassung von den Nutzern einzuhalten.

Die ressortübergreifenden Kommunikationsnetzinfrastrukturen werden von der Bundesverwaltung grundsätzlich für jede Kommunikation innerhalb der Bundesverwaltung und darüber hinaus zur Kommunikation in externe Netze (wie etwa in das Internet) genutzt. Eigene Weitverkehrsnetze oder andere externe Netze dürfen nur in begründeten Ausnahmefällen und mit Zustimmung des BSI angebunden werden. In allen Fällen unterstützt das BSI die Entwicklung sicherer und anforderungsgerechter Lösungen für erforderliche Netzübergänge.

Die ressortübergreifenden Kommunikationsnetzinfrastrukturen sind so zu gestalten, dass sowohl unklassifizierte Daten als auch Verschlusssachen bis zur Einstufung „VS-NUR FÜR DEN DIENSTGEBRAUCH“ ohne zusätzliche Verschlüsselung durch den Nutzer übermittelt werden können. Für den darüber etwaig hinausgehenden erforderlichen Schutz der Vertraulichkeit und Integrität ist die Einrichtung eigenverantwortlich.

8.1 Sicherung der ressortübergreifenden Kommunikationsnetzinfrastruktur

Die ressortübergreifenden Kommunikationsnetzinfrastrukturen haben für die Regierungskommunikation insgesamt eine herausgehobene Bedeutung. Die in Kapitel 7.1 festgelegten Anforderungen gelten für die Betreiber dieser Kommunikationsnetzinfrastrukturen mit folgenden Ergänzungen:

- Das BSI legt im Benehmen mit den Betreibern die Informationssicherheitsanforderungen fest, deren Umsetzung den jeweiligen Betreibern obliegt. Die Planung und Ausgestal-

tung der ressortübergreifenden Kommunikationsnetzinfrastrukturen erfolgt hinsichtlich der Aspekte der Informationssicherheit im Einvernehmen mit dem BSI.

- Das BSI prüft insbesondere die Sicherheitskonzepte und Notfallkonzepte der ressortübergreifenden Kommunikationsnetzinfrastrukturen und gibt diese frei.
- BMI legt fest, wer die Rolle der/des Gesamt-IT- SiBe wahrnimmt sowie die Steuerung der notwendigen Geheimschutzanforderungen vornimmt.
- Das BSI steuert die Implementierung eines ISMS für den Informationsverbund der ressortübergreifenden Kommunikationsnetzinfrastrukturen.
- Bei erheblichen Störungen/Sicherheitsvorfällen, in Notfällen und im Krisenfall ist das BSI einzubinden.
- Das BSI erhält bei den Betreibern, inkl. etwaiger Unterauftragnehmer, geeignete Prüf-, Auskunfts- und Einsichtsrechte (Revisionen, Durchführung von Penetrationstest und Sicherheitsaudits) zur Überprüfung des Umsetzungsstands bzw. der Angemessenheit und Wirksamkeit der in den Informationssicherheitskonzepten festgelegten Maßnahmen.
- Das BSI nimmt die hier beschriebenen Aufgaben und Rollen gegenüber dem jeweils mit der Planung, der Implementierung und dem Betrieb beauftragten Dienstleister für die ressortübergreifenden Kommunikationsnetzinfrastrukturen wahr.
- Das BSI erstellt die VS-Einstufungsliste, legt die Geheimschutzmaßnahmen fest, prüft deren Umsetzung und empfiehlt dem BMI jeweils die Freigabe.

8.2 Informationssicherheitsanforderungen für die Nutzung

Die Informationssicherheit der ressortübergreifenden Kommunikationsnetzinfrastruktur hängt sowohl von den innerhalb des Netzes umgesetzten Informationssicherheitsvorkehrungen als auch von den Informationssicherheitsmaßnahmen der diese ressortübergreifenden Kommunikationsnetzinfrastruktur nutzenden Einrichtungen ab. Sicherheitslücken auf der Seite der Einrichtungen können dabei die Gesamtsicherheit der ressortübergreifenden Kommunikationsnetzinfrastruktur und damit aller anderen Einrichtungen gefährden. Daher werden für die Nutzung der ressortübergreifenden Kommunikationsnetze folgende Mindestanforderungen festgelegt:

- Das BSI definiert unter Beteiligung der Nutzer die für den Schutz dieser Netze notwendigen „Nutzerpflichten“ und die sie ergänzenden angemessenen Informationssicherheitsanforderungen im Rahmen eines Mindeststandards nach § 8 Absatz 1 BSIG.

- Das BSI aktualisiert und ergänzt bei Bedarf diese Anforderungen, um zu gewährleisten, dass sie der sich permanent wandelnden Gefährdungslage sowie den sich verändernden technischen und organisatorischen Rahmenbedingungen gerecht bleiben.
- Die Ressorts bzw. Einrichtungen sorgen für die Umsetzung der Nutzerpflichten und der ergänzenden Informationssicherheitsanforderungen. Die Prüfung der Umsetzung obliegt der/dem IT-SiBe im Rahmen der Evaluation der Informationssicherheit.
- Das BSI kann die Umsetzung der Nutzerpflichten in den Ressorts und Einrichtungen nach Abstimmung mit der/dem jeweiligen Ressort-IT- SiBe überprüfen. Nach Abschluss der Prüfung legt es den Einrichtungen den Prüfbericht mit konkreten Feststellungen und Handlungsempfehlungen unverzüglich vor.
- Die Ressorts bzw. Einrichtungen beheben festgestellte Mängel in angemessener Frist und dokumentieren diese Behebung.

8.3 Erhöhte Verfügbarkeitsbedarfe für die Kommunikationsnetzinfrastruktur des Bundes

Eine Reihe von Geschäftsprozessen in der Bundesverwaltung erfordert Kommunikationsnetze, die auch in besonderen Lagen und Krisen zur Verfügung stehen müssen. Diesbezüglich bestehen an die Netze deutlich höhere Verfügbarkeitsanforderungen als für die Mehrzahl der Geschäftsprozesse.

Die ressortübergreifenden Kommunikationsnetzinfrastrukturen sollen auch für besondere Lagen gehärtet werden, weshalb auch ein besonders gehärteter Netzanschluss für die Nutzer zur Verfügung steht.

Die Ressorts und Einrichtungen haben dennoch zu prüfen, in wieweit eine zusätzliche alternative Kommunikationsmöglichkeit einzurichten und/oder entsprechende Sonderdienste in den bestehenden ressortübergreifenden Kommunikationsnetzinfrastrukturen des Bundes vorzusehen sind, um auch in besonderen Lagen und Krisenfällen sicher kommunizieren zu können.

Im Einvernehmen mit dem BSI sind diese alternativen Redundanzkommunikationswege mit den Betreibern der ressortübergreifenden Kommunikationsnetze abzustimmen, um die ressortübergreifenden Kommunikationsnetze insgesamt nicht zu gefährden.

9 Erkennung, Meldung und Behandlung von informationssicherheitsrelevanten Ereignissen

Vorbeugende Maßnahmen (Prävention) allein sind nicht ausreichend, um ein angemessenes Informationssicherheitsniveau zu gewährleisten. Informationssicherheitsrelevante Ereignisse müssen systematisch aufgespürt (Detektion) und abgewehrt werden (Reaktion). Zur frühen Erkennung von Informationssicherheitsvorfällen bedarf es der kontinuierlichen Analyse aller verfügbaren Informationen. Von der Bundesverwaltung sind vor diesem Hintergrund folgende Anforderungen zu erfüllen:

- Die Ressorts und Einrichtungen treffen geeignete Maßnahmen zur Vorbeugung gegen informationssicherheitsrelevante Ereignisse.
- Die Ressorts und Einrichtungen ergreifen geeignete Maßnahmen zur Detektion und Behandlung von informationssicherheitsrelevanten Ereignissen.
- Die Ressorts und Einrichtungen setzen nach dem Stand der Technik und den Mindeststandards des BSI Informationssicherheitsmaßnahmen zur Reaktion auf und Behandlung von informationssicherheitsrelevanten Ereignissen um bzw. nutzen vom BSI angebotene Dienste zur Behandlung von informationssicherheitsrelevanten Ereignissen.
- Das BSI unterstützt auf Ersuchen der Betroffenen die Ressorts und Einrichtungen bei der Abwehr von Schadprogrammen sowie bei Angriffen durch zusätzliche zentrale Maßnahmen in den ressortübergreifenden Kommunikationsnetzen des Bundes und durch Analyse von Protokoll- und Schnittstellendaten gemäß § 5 BSIG.
- Die Ressorts und Einrichtungen unterstützen das BSI durch Bereitstellung von Protokoll- und Schnittstellendaten zur Erkennung von Anomalien und Gefährdungs-/ Angriffs mustern gemäß § 5 BSIG. Die diesbezüglichen Anforderungen legt das BSI in einem Mindeststandard nach § 8 BSIG Absatz 1 fest.
- Das BSI unterstützt auf Ersuchen der Betroffenen die Ressorts und Einrichtungen bei der Auswahl und Bereitstellung geeigneter Produkte und Dienstleistungen bzgl. der Prävention und Detektion von Informationssicherheitsvorfällen. Die Produkte und Dienstleistungen werden über das BSI oder grundsätzlich über Rahmenverträge bereitgestellt.

Zur Aufbereitung und Auswertung der Informationen ist ein Lage- und Analysezentrum des Bundes beim BSI (CERT-Bund mit BSI-Lagezentrum) eingerichtet worden. Im BSI-Lagezentrum

werden eingehende Meldungen über Informationssicherheitsvorfälle ausgewertet, das CERT-Bund informiert, warnt oder alarmiert im Bedarfsfall.

Hinsichtlich der Zusammenarbeit der Ressorts und Einrichtungen mit dem BSI-Lagezentrum und dem CERT-Bund sind folgende Anforderungen von den Ressorts und den Einrichtungen umzusetzen:

- Ressorts bzw. Einrichtungen stellen dem BSI (CERT-Bund) Warn- und Alarmierungskontakte zur Verfügung.
- CERT-Bund versendet aktuelle Informationen und Warnungen unverzüglich an die o. g. Warn- und Alarmierungskontakte der Ressorts bzw. Einrichtungen.
- Ressorts bzw. Einrichtungen reagieren unverzüglich auf Warnungen von CERT-Bund.
- Der festgelegte Warn- und Alarmierungskontakt eines Ressorts bzw. einer Einrichtung meldet relevante Informationssicherheitsvorfälle gemäß § 4 Absatz 6 BSIG unverzüglich an das BSI-Lagezentrum.
- Bei herausgehobenen Informationssicherheitsvorfällen kann das BSI auf Ersuchen der betroffenen Einrichtungen durch den Einsatz mobiler Teams (Mobile Incident Response Teams, MIRTs) bei der Wiederherstellung der Informationssicherheit oder Funktionsfähigkeit der betroffenen IT-Systeme unterstützen.

10 IT-Notfallprävention und IT-Krisenreaktion

Um Notfällen und Krisen vorzubeugen, sind die Ressorts und Einrichtungen im Rahmen des Krisenmanagements des Bundes verpflichtet, geeignete Notfallmanagement-Prozesse (auch betriebliches Kontinuitätsmanagement, Business Continuity Management, genannt) aufzubauen und aktuell zu halten. Es müssen daher geeignete Präventivmaßnahmen getroffen werden, die zum einen die Robustheit und Ausfallsicherheit der Geschäftsprozesse erhöhen und zum anderen ein schnelles und zielgerichtetes Agieren in einem Notfall oder einer Krise ermöglichen.

IT-Notfallmanagement, d.h. Notfallvorsorge und Notfallbewältigung, hat im Wesentlichen zum Ziel, durch Absicherung bzw. Wiederherstellung der Verfügbarkeit der IT-Services, der IT-Verfahren, der IT-Systeme und insbesondere der Informationen zu garantieren, dass die Geschäfte – jedenfalls im unbedingt erforderlichen Umfang – fortgeführt werden können. IT-Notfallmanagement ist Teil des ganzheitlichen Notfallmanagements und darf nicht isoliert betrachtet werden.

Die Zuständigkeit für die IT-Notfallprävention und die Reaktion bei Krisen im IT-Bereich liegt bei der/dem Notfallbeauftragten eines Ressorts bzw. einer Einrichtung. Gemäß BSI-IT-Grundschutz steuert die/der Notfallbeauftragte alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit. Sie/er ist für die Erstellung, Umsetzung, Pflege und Betreuung des Notfallmanagements der Einrichtung und der zugehörigen Dokumente und Regelungen zuständig. Dies umfasst auch das IT-Notfallmanagement.

Um Notfälle und Krisen zu erkennen und angemessen darauf reagieren zu können, ist hinsichtlich der IT das rechtzeitige Erkennen und Melden von Informationssicherheitsvorfällen an das BSI Grundvoraussetzung, da sich diese zu Notfällen oder sogar Krisen ausweiten können. Für die Bundesverwaltung sind im Rahmen des IT-Notfallmanagements und der IT-Krisenreaktion folgende Anforderungen zu erfüllen:

- Die Ressorts und Einrichtungen melden erkannte Informationssicherheitsvorfälle gemäß der Allgemeinen Verwaltungsvorschrift auf Grundlage § 4 BSIG an das BSI-Lagezentrum (vgl. Kapitel 9).
- Das BSI warnt und alarmiert die noch nicht betroffenen Ressorts und Einrichtungen. Sofern eine ressortübergreifende Vorgehensweise notwendig ist, koordiniert das BSI eine abgestimmte Reaktion im Notfall bzw. eine schnelle Überführung in den Regelbetrieb. Die IT-Dienstleister des Bundes sind in angemessener Weise zu beteiligen.
- Die Ressorts und Einrichtungen erstellen für ihren Zuständigkeitsbereich ein IT-Notfallkonzept (auf Basis des Notfallkonzepts des Ressorts/ der Einrichtung), führen regelmäßig IT-Notfallübungen durch und dokumentieren diese.
- Die/der IT-SiBe eines Ressorts/ einer Einrichtung arbeitet mit der/dem Notfallbeauftragten des Ressorts/ der Einrichtung zusammen, stimmt sich mit dieser/diesem ab und unterstützt diese/diesen in ihrer/seiner Tätigkeit.
- Die Einrichtung wirkt bei einrichtungsübergreifenden Notfallübungen mit.
- Das Koordinierungsgremium Informationssicherheit ist im Rahmen des IT-Notfallmanagements und der IT-Krisenreaktion in geeigneter Weise einzubinden.

11 Informationssicherheit in ressortübergreifenden Vorhaben des Bundes

In einer Vielzahl von Vorhaben der Bundesverwaltung hat IT eine erhebliche Bedeutung. Daher müssen die Projektverantwortlichen noch stärker als bisher darauf achten, dass Anforderungen der Informationssicherheit frühzeitig berücksichtigt und umgesetzt werden. Auch bei Vorhaben, die sich in erheblichem Umfang auf die IT auswirken, wie etwa Bauvorhaben, ist eine frühzeitige Beteiligung der für IT und Informationssicherheit Verantwortlichen notwendig. Im Projektmanagementprozess muss daher von Beginn an die notwendige Informationssicherheit definiert, konzipiert und die Umsetzung eingeplant werden.

Daher sind bei allen ressortübergreifenden Vorhaben des Bundes folgende Mindestanforderungen zu erfüllen:

- Bei ressortübergreifenden Vorhaben ist frühzeitig, d. h. bereits in der Initiierungs- und Konzeptionsphase, sicherzustellen, dass die Aspekte der Informationssicherheit in angemessener Weise berücksichtigt sind.
- Entsprechende Rollen sind durch das federführende Ressort in der Projektorganisation vorzusehen.
- Das BSI ist in geeigneter Weise in beratender Rolle in die Organisations-/ Projektstruktur einzubinden.
- Vor strategischen Entscheidungen in ressortübergreifenden Vorhaben bindet die verfahrensverantwortliche Stelle die AG ISM in Bezug auf Fragen zur Informationssicherheit frühzeitig ein.
- Bei der Digitalisierung u.a. von Verwaltungsprozessen sind bereits bei der Konzeption die Informationssicherheit und der Datenschutz als Erfolgsfaktor einzubinden (Konzepte „Security/Privacy by design“ und „Security/Privacy by default“).

11.1 IT-Konsolidierung des Bundes

Die Verbesserung der Informationssicherheit in der gesamten Bundesverwaltung ist eines der herausragenden Ziele der IT-Konsolidierung des Bundes.

Auf Basis der Vorgaben des UP Bund 2017 sind daher die grundsätzlichen Rahmenbedingungen an die Informationssicherheit hinsichtlich der IT-Konsolidierung des Bundes in einer entspre-

chenden „Richtlinie zur Informationssicherheit der IT-Konsolidierung des Bundes“ weiter zu konkretisieren.

Durch diese Richtlinie soll insbesondere sichergestellt werden, dass die ISMS des Leistungsverbunds, die ISMS der Netzdienstleister und das ISMS der Kundeneinrichtung hinsichtlich der Informationssicherheit in geeigneter Weise kooperieren, um zu gewährleisten, dass jedes ISMS seiner Aufgabenstellung gerecht wird.

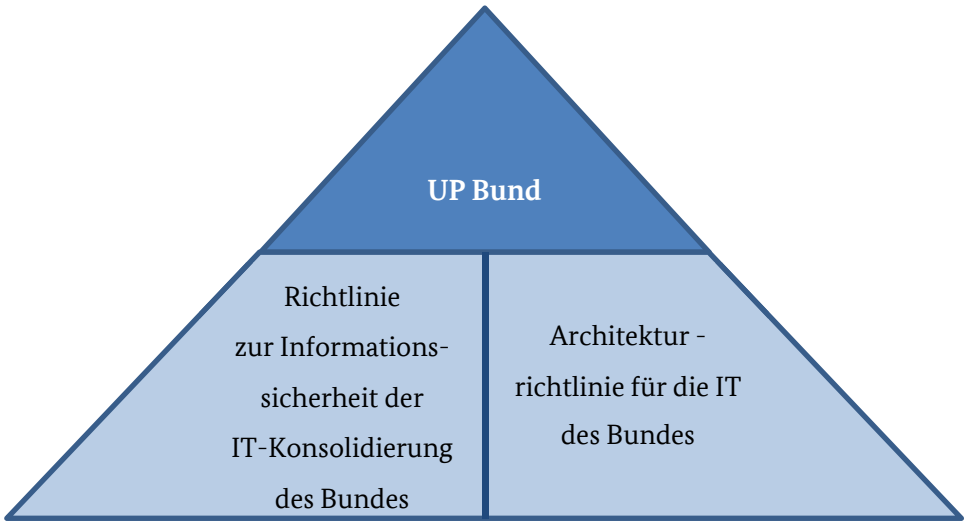

Abbildung 2: Dokumentenpyramide im Zusammenhang mit dem Informationssicherheitsmanagement des Bundes

Diese Richtlinie zur Informationssicherheit ist federführend vom BSI in unmittelbarer Zusammenarbeit mit den beteiligten Ressort-IT-SiBe und den zentralen IT-Dienstleistern sowie den Netzdienstleistern im Leistungsverbund zu erstellen und dem jeweiligen Fortschritt der IT-Konsolidierung des Bundes entsprechend fortzuschreiben. Die Richtlinie ist jeweils nach Befassung in der AG ISM vom IT-Rat zu beschließen.

Zur Beschreibung der Beziehungen und den Aufbau von Informationssystemen sind weitere Richtlinien und Rahmendokumente zu berücksichtigen, vgl. die Dokumentenpyramide in Abbildung 2.

12 Anhang

12.1 Abbildungsverzeichnis

Impressum

Herausgeber

Bundesministerium des Innern

Alt-Moabit 140

10557 Berlin

Ansprechpartner

Referat IT II 4 – IT-Sicherheit in der Bundesverwaltung, IT-Sicherheitsbeauftragter Ressort BMI

Alt-Moabit 140, 10557 Berlin

ITII4@bmi.bund.de

www.bmi.bund.de

Version 1.0

Stand

Juli 2017

Bildnachweis

a-image/shutterstock.com

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.