Bundesamt
für Sicherheit in der
Informationstechnik

Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung

Version 2.2, 14. Dezember 2012

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-333
E-Mail: sicherheitsberatung@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Projektmotivation ... 7

Einleitung, Zielgruppe und Ziel dieser Arbeitshilfe ... 8

1 Rechtliche Grundlagen ... 10

2 Aufgabenkatalog ... 11

2.1 ISO 27001, ISO 27006 und IT-Grundschutz ... 11

2.2 Nationaler Plan zum Schutz der Informationsinfrastruktur in Deutschland - Umsetzungsplan Bund (UP Bund) ... 11

2.3 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSIG) ... 12

3 Funktionale Sicht einer Personalprognose ... 13

3.1 Lösungsansatz Metamodell „Standardbehörde“ ... 13

3.2 Initiale Arbeiten ... 14

3.3 Regelmäßige Arbeiten ... 14

3.4 Arbeiten im ersten Jahr ... 14

3.5 Arbeiten in den Folgejahren ... 14

3.6 Vertreterregelung ... 15

3.7 IT-Sicherheitsbeauftragter als IT-Geheimschutzverantwortlicher ... 15

3.8 Fallstudie „Dokumentation der Zeitansätze für das Erstellen eines IT-Sicherheitskonzeptes einer „Standardbehörde“ gemäß Abschnitt 3.1 ... 16

3.9 Rahmenbedingungen für die fachliche Personalprognose ... 16

3.10 Zeitzuschläge für relevante Zusatzfaktoren ... 17

3.10.1 Anzahl der Mitarbeiter ... 18

3.10.2 Grad der Heterogenität der IT-Landschaft und IT-Verfahren ... 18

3.10.3 Anzahl der zu betreuenden Außenstellen ... 18

3.10.4 Anteil der IT-Anwendungen mit einem Schutzbedarf höher als „normal“ ... 18

3.10.5 Hochverfügbarkeitsanforderungen an IT-Anwendungen ... 19

3.11 Zeitabschläge für ausgelagerte Tätigkeiten einer Behörde mit ausgelagerter IT (Outsourcing) ... 19

3.12 Berechnungsmatrix der Bewertungsfaktoren ... 19

3.13 Szenario zur Abschätzung der Personalressource am Beispiel einer „Standardbehörde“ gemäß 3.1 ... 23

3.14 Erläuterungen zur Berechnungsmatrix der Bewertungsfaktoren ... 24

4 Arbeitshilfe zur Berechnung der Personalprognose ... 25

4.1 Fachliche Anforderungen an das Tool ... 25

5 Zusammenfassung, Bewertung und Ausblick ... 27

Anhang ... 29

Literatur- und Quellenverzeichnis ... 52

Abkürzungsverzeichnis ... 55

Abbildungsverzeichnis

Abbildung 1 - Screenshot Berechnungstool - Zu- und Abschlagstabellen 21
Abbildung 2 - Berechnungsmatrix Metamodell „Standardbehörde“ mit 500 Mitarbeitern 22
Abbildung 3 - Berechnungsmatrix Musterbehörde mit leicht erhöhten Anforderungen 23
Abbildung 4 - Berechnungsmatrix mit gekennzeichneten Zuschlagsfeldern 24
Abbildung 5 - Screenshot Berechnungstool - Zusammenstellung der Behörden 26
Abbildung 6 - Grafische Darstellung der Zuschläge für die Anzahl der Mitarbeiter 46
Abbildung 7 - Grafische Darstellung der Zuschläge für die Anzahl der Außenstellen 49

Tabellenverzeichnis

Tabelle 1 - Einmalige strategische Aufgaben des IT-Sicherheitsbeauftragten 16
Tabelle 2 - Regelmäßige operative Aufgaben des IT-Sicherheitsbeauftragten 17
Tabelle 3 - Gegenüberstellung IT-Grundschutz des BSI und der ISO 27001 29
Tabelle 4 - Gegenüberstellung IT-Grundschutz des BSI und der ISO 27002 38
Tabelle 5 - Tätigkeiten des IT-SiBe aus dem UP Bund 41
Tabelle 6 - Tätigkeiten des IT-SiBe aus dem BSI-Gesetz (BSIG) 42
Tabelle 7 - Zusammenstellung Zeitbedarf Erstellung eines IT-Sicherheitskonzeptes 44
Tabelle 8 - Zuschläge für die Anzahl der Mitarbeiter 45
Tabelle 9 - Zuschläge für heterogene IT-Landschaft und IT-Verfahren 47
Tabelle 10 - Zuschläge für die Anzahl der Außenstellen 48
Tabelle 11 - Zuschläge für den Anteil der IT-Anwendungen mit höherem Schutzbedarf 50
Tabelle 12 - Zuschläge für Schutzbedarf mit Hochverfügbarkeitsanforderung 51

Projektmotivation

Im Jahr 2007 beschloss das Bundeskabinett den Nationalen Plan zum Schutz der Informationsinfrastrukturen in Deutschland (Umsetzungsplan Bund, kurz UP Bund) [5] und den Nationalen Plan zum Schutz der Informationsinfrastrukturen mit den strategischen Zielen "Prävention, Reaktion und Nachhaltigkeit" (Umsetzungsplan KRITIS, kurz UP KRITIS) [6] mittels konkreter Maßnahmen und Empfehlungen.

Die Umsetzungspläne sind zentrale Bausteine für die mittel- und langfristige Gewährleistung der IT-Sicherheit auf hohem Niveau in der gesamten Bundesverwaltung und fordern die Etablierung eines Informationssicherheitsmanagementsystems (ISMS), präventive Maßnahmen, Einrichtung eines Krisenmanagements sowie nachhaltigen Schutz vor IT-gestützter Spionage und Sabotage.

In den einzelnen Maßnahmen des UP Bund werden Anforderungen an die IT-Sicherheit und organisatorische Vorkehrungen hierzu eingefordert. Der Mindeststandard umfasst z. B. die Bestellung eines IT-Sicherheitsbeauftragten, die Erstellung und Umsetzung von Sicherheitskonzepten sowie regelmäßige Durchführung von IT-Sicherheitsrevisionen.

Diese hohen fachlichen Anforderungen an das Informationssicherheitsmanagement einerseits und die Übertragung dieser Aufgaben auf die IT-Sicherheitsbeauftragten, die diese zusätzlichen Aufgaben ggf. neben ihrer Linientätigkeit wahrnehmen sollen, andererseits, führten nicht selben zu zeitlichen Verzögerungen bei der Etablierung eines flächendeckenden Sicherheitsmanagements.

Erfahrungen der letzten Jahre haben in Bezug auf die Schaffung von Personalressourcen für diese Aufgaben deutlichen Handlungsbedarf gezeigt.

Einleitung, Zielgruppe und Ziel dieser Arbeitshilfe

Dieses Dokument soll eine Hilfestellung geben, um die Kernaufgaben der IT-Sicherheitsbeauftragten (IT-SiBe) gegenüber der Amtsleitung oder internen Fachgremien aufzuzeigen und die mit der Tätigkeit verbundenen Zeitaufwände darstellen zu können. Bei dem Dokument handelt es sich um eine Handreichung des BSI, die auf langjährigen Erfahrungen der Beratung zur IT-Sicherheit basiert und die Vorgaben des UP Bund [5], der VSA Bund und des BSIG [8] zu Grunde legen.

Ein Ziel des Dokumentes besteht darin Aufgaben zur IT-Sicherheit, Vorgaben zur Prioritätensteuerung und die zeitlichen Aufwände transparent darzustellen. In diesem Dokument wird ein Katalog, in dem die Aufgaben von IT-Sicherheitsbeauftragten, die nachweisbar aus Gesetzen und/oder Verordnungen stammen, abgebildet. Die Arbeitshilfe beschreibt die fachlichen Anforderungen zu den erforderlichen Personalressourcen für ein effektives IT-Sicherheitsmanagement und unterstützt somit die Sicherheitsbeauftragten bei der Ermittlung des Mindestpersonalbedarfs ihrer Behörde.

Die Arbeitshilfe kann Behörden mit besonderen Aufgaben, wie z. B. IT-Dienstleistungszentren oder Sicherheitsbehörden nur bedingt bei der Schätzung des Personalaufwandes unterstützen. Diese Behörden haben besondere Anforderungen an die IT-Sicherheit und benötigen daher individuelle Aufgaben- und Technikanalysen, die über den Rahmen dieser Arbeitshilfe hinausgehen.

Das Dokument erhebt keineswegs den Anspruch zur Begründung von Bedarfsanforderungen für mehr Personal verwendet zu werden, vielfach lassen sich die Aufgaben zur IT-Sicherheit durch Umschichtung des bereits vorhandenen Personals der jeweiligen Behörde bewältigen. Die Erfahrungen des BSI hinsichtlich des Zeitbedarfs zur Herstellung und Erhaltung der IT-Sicherheit begründen sich aus den intensiven Kontakten mit unterschiedlichen Behörden aus unterschiedlichen Ressorts und stellen somit eine breite Basis zur Abschätzung erforderlicher Ressourcen dar. Beurteilungskriterien sind so gewählt worden, dass sie grundsätzlich jede Behörde betreffen. Zudem werden mittels der Arbeitshilfe keine behördenspezifischen individuellen Besonderheiten wie sie beispielsweise bei Sicherheitsbehörden oder bei Behörden, die als Dienstleister fungieren, abgebildet. Der Mehrbedarf dieser Behörden ist durch entsprechende Zuschläge anzugeben.

Der Aufwand für die Vorbereitung einer Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz wird durch dieses Dokument nicht abgedeckt.

Die IT-Sicherheitsbeauftragten sollen mit diesem Dokument in die Lage versetzt werden, für ihre Arbeitsbereiche eine Jahresarbeitsplanung zu erstellen. Es sollen ihre Tätigkeiten und die hierzu notwendigen Arbeitstage (Einheit: PT = Personentage) ermittelt werden, um mit der Amtsleitung die zeitliche Umsetzung ihrer gesetzlichen Aufträge abzustimmen. Aus Gründen der Transparenz wird empfohlen, die Tätigkeiten der IT-Sicherheitsbeauftragten als Projekt mit der Festlegung von Aktivitäten, deren Aufwände und einer begleitenden Meilensteinplanung darzustellen.

Das in diesem Dokument beschriebene Vorgehen entbindet die Behörde nicht von der Notwendigkeit, nach einer Konsolidierungsphase eine Personalbedarfsermittlung nach anerkannten Methoden des Organisationshandbuchs [4] durchzuführen.

Die in der Arbeitshilfe dargestellte Vorgehensweise sollte, soweit aus technischer Sicht möglich, Hinweise auf gesetzliche Verpflichtungen der Behörde bzw. der IT-Sicherheitsbeauftragten zur Wahrnehmung bestimmter Aufgaben im Kontext der IT-Sicherheit enthalten.

Da empirische Daten zur Berechnung der Aufwände für die Tätigkeiten der IT-SiBe derzeit nicht vorliegen, bezieht sich das Dokument auf Schätzungen aus Erfahrungen von Arbeitsaufwänden in der Vergangenheit. Prognosen sind hinreichend gute Schätzungen, die jedoch in Zukunft möglichst durch statistisches Material unterlegt werden sollten. Im Mangel um empirische Daten ist es zulässig und hilfreich mit Aufwandsschätzungen zu beginnen.

Die IT-SiBe sollen angehalten werden ihre Aufwände zu protokollieren, um spätere Untersuchungen stützen zu können. Diese Aufzeichnungen dienen auch zur Projektfortschreibung und Projektsteuerung (Controlling).

1 Rechtliche Grundlagen

Um einen Personalbedarf fundiert zu begründen, bedarf es einer rechtlichen Verankerung der Tätigkeiten eines IT-Sicherheitsbeauftragten.

Die Gewährleistung der Informationssicherheit befindet sich in einem ständigen Wandel und ist eine anspruchsvolle Management-Herausforderung. Hier gilt jedoch in Bezug auf die personellen und finanziellen Ressourcen die Angemessenheit der Maßnahmen zu prüfen und zu wahren.

Bis zur Gewährung des „elektronischen Hausfriedensbruchs“ durch §§ 202a bis 202c StGB [20] sowie der „virtuellen Sachbeschädigung“ durch §§ 303a und 303b StGB [20] war die IT-Sicherheitstechnik bis Mitte 2007 als solche gesetzlich nicht geschützt.

Die rechtliche Pflicht zu effizientem IT-Risikomanagement ergibt sich heute im Wesentlichen aus

- dem Wirtschaftsverwaltungsrecht,
- dem Datenschutzrecht,
- dem Telekommunikationsrecht,
- dem Nationalen Plan zum Schutz der Informationsinfrastrukturen,
- dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes,
- dem Gesetz zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c Grundgesetz (GG) [15] sowie
- aus vertraglichen Vereinbarungen.

Als Auslegungshilfen werden in der Praxis u. a. technische Regelwerke wie ISO 17799/BS 7799 und BS 7799-2/ISO27001, Grundschutzkataloge des BSI, CoBIT, ITIL oder ITSEC/CC herangezogen.

2 Aufgabenkatalog

Der Aufgabenkatalog ist eine Momentaufnahme und gilt zum Zeitpunkt der Erstellung des Dokumentes als abschließend.

Die Aufgaben des IT-Sicherheitsbeauftragten sind in zwei einmalige, strategische und sechs dauerhafte, organisatorische Tätigkeitsschwerpunkte zusammengefasst (Abbildung 2 bis Abbildung 4).

Die einmaligen Aufgaben sind die (toolgestützte) Erstellung von Sicherheitskonzepten nach den BSI-Standards 100-2 [2] und ggf. 100-3 [3], zur IT-Notfallvorsorge sowie zum IT-Notfall- und Krisenmanagement [18]. Zu den regelmäßigen Aufgaben des IT-Sicherheitsbeauftragten zählen unter anderem die Überprüfung und Fortschreibung von Sicherheitskonzepten und des IT-Notfallkonzepts sowie die Sensibilisierung der Mitarbeiter, Beratung und Berichterstattung an die Amtsleitung. In Tabelle 3 bis Tabelle 5 (jeweils die Spalte „MX) sind die aufgezeigten Aufgaben des IT-Sicherheitsbeauftragten diesen acht Tätigkeitsschwerpunkten zugeordnet.

Diese Aufgaben des IT-Sicherheitsbeauftragten umfassen lediglich Arbeiten bis maximal zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH. Aufgaben des Geheimschutzes sind nicht berücksichtigt und werden folglich auch nicht abgebildet.

2.1 ISO 27001, ISO 27006 und IT-Grundschutz

IT-Grundschutz beschreibt mit Hilfe der BSI-Standards 100-1 [1], 100-2 [2], 100-3 [3] und der IT-Grundschutz-Kataloge [19] eine Vorgehensweise zum Aufbau und zur Aufrechterhaltung eines Managementsystems für Informationssicherheit (ISMS). Das damit aufgebaute ISMS erfüllt die Anforderungen von ISO 27001 und ISO 27002.

Die Tabelle 3 bis Tabelle 5 enthalten unverändert die Benennung der „Aktivitäten“, wie sie auch in den Standards bezeichnet werden. Eigenwillige Bezeichnungen der Aktivitäten mit ausgeprägter „Verbalisierung der Tätigkeiten“ würde ggf. in diesem Dokument für fachfremde Leser die Lesbarkeit der Tabelle erleichtern, jedoch in der fachlichen Begründung eher zu Nachfragen und Irritationen führen.

Die Gegenüberstellungen in den Tabelle 3 und Tabelle 4 zeigen die Zuordnung der Inhalte der beiden ISO-Normen zu den Inhalten von IT-Grundschutz. Dementsprechend resultieren Mindestanforderungen an die Implementierung und Aufrechterhaltung eines ISMS, die in einem regelmäßigen wöchentlichen (W), monatlichen (M) oder jährlichen (J) Rhythmus durch den IT-Sicherheitsbeauftragten bearbeitet werden müssen bzw. einmalig (E) anfallen. Die Spalte „Mx“ ordnet die jeweilige Aufgabe einem der Kernaufgaben in der späteren Berechnungsmatrix zu (3.12, Abbildung 3 und Abbildung 3).

2.2 Nationaler Plan zum Schutz der Informationsinfrastruktur in Deutschland - Umsetzungsplan Bund (UP Bund)

Der UP Bund fordert u.a. die Etablierung eines Informationssicherheitsmanagements (ISMS) und die Einrichtung einer IT-Sicherheitsorganisation in jeder Bundesbehörde. Grundlage der Vorgehensweise sind die BSI-Standards 100-1 [1] bis 100-3 [3] nach IT-Grundschutz.

Die im UP Bund geforderten und somit gesetzlich verpflichtenden Tätigkeiten des IT-SiBe sind in Tabelle 5 zusammengestellt. Besondere Beachtung gilt dabei den rot gekennzeichneten Fristen.

Gemäß UP Bund, Ziffer 1.1, Seite 6 [5] ist der Ressort-IT-Sicherheitsbeauftragte und die IT-Sicherheitsbeauftragten für die Behörden der Geschäftsbereiche binnen sechs Monaten nach Verabschiedung des UP Bund zu bestellen.

2.3 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSIG)

Der Bedrohung der Informationssicherheit in Bundesbehörden kann nur durch die Festlegung einheitlicher und strenger Sicherheitsstandards durch eine zentrale Stelle (BSI) begegnet werden.

Die Umsetzung dieser Standards in den Bundesbehörden Vorort ist die Aufgabe der jeweiligen IT-Sicherheitsbeauftragten. Die sich aus dem BSI-Gesetz (BSIG) für den IT-SiBe ergebenen Tätigkeiten sind in Tabelle 6 aufgelistet.

3 Funktionale Sicht einer Personalprognose

Um die Arbeitsaufwände eines IT-Sicherheitsbeauftragten zeitlich quantifizieren zu können, müssen die Tätigkeiten, für die in Kapitel 1 eine rechtliche Verankerung dargestellt wurden, analysiert und formuliert werden (Fachliche Anforderungen, Requirements). Wie in der Betriebswirtschaftslehre empfohlen, soll infolgedessen ein abstrahiertes Metamodell erstellt werden, mit dessen Hilfe danach, mit entsprechenden Einschränkungen und Ergänzungen, reale Abbildungen der Aufwände der jeweils betrachteten Behörden abgeleitet werden können.

Modelle sind ein sehr gutes Instrument, um Wirkungszusammenhänge abzubilden. Dabei dienen sie immer zwei grundlegenden Zielsetzungen: Erstens der Komplexitätsreduktion gegenüber der Realität und damit der Ordnung, Orientierung, Kommunikation und Entscheidungsunterstützung, zweitens dienen sie der Informationsgewinnung und -überprüfung bezüglich des Untersuchungsobjektes.

Im Rahmen dieser Arbeitshilfe wird daher als Ausgangspunkt für die durchzuführenden Untersuchungen zunächst das Modell einer „Standardbehörde“ geschaffen Abschnitt 3.1 und anschließend die anfallenden Tätigkeiten eines IT-Sicherheitsbeauftragten kategorisiert (Abschnitte 3.2 bis 3.5). Unter 3.9 wird anhand einer Fallstudie aufgezeigt, welche Zeitansätze für das Erstellen eines IT-Sicherheitskonzeptes einer „Standardbehörde“ benötigt werden. Nach Analyse der rechtlichen Quellen und Konsolidierung der Zusammenstellungen aus Kapitel 2 ergeben sich sowohl einmalige, strategische als auch regelmäßige, operative Tätigkeitsschwerpunkte eines IT-Sicherheitsbeauftragten, die unter 3.11 aufgezeigt werden.

Diese Tätigkeiten bilden die Grundlage der weiteren Untersuchungen. Im Anschluss werden die von einer „Standardbehörde“ abweichenden Bewertungskriterien erläutert, die bei einer Personalbedarfsprognose zu Zeitzuschlägen bzw. Zeitabschlägen führen.

Zur automatisierten Berechnung dieser herausgearbeiteten Faktoren zu einem konkreten Personalbedarf im Einzelfall wurde ein IT-gestütztes Tool erstellt, das im Kapitel 4 vorgestellt wird.

3.1 Lösungsansatz Metamodell „Standardbehörde“

Eine „Standardbehörde“ wird zunächst wie folgend definiert:

Sie hat

- rund 500 Mitarbeiter,
- eine homogene IT-Landschaft und IT-Verfahren,
- keine Außenstellen,
- normalen Schutzbedarf,
- keine Hochverfügbarkeitsanforderungen an IT-Systeme.

Abweichungen dieses Modells können durch prozentuale Zeitzuschläge bzw. Zeitabschläge korrigiert werden. Die Zuschläge sollten auf alle relevanten behördenspezifischen Rahmenbedingungen eingehen und anhand von gewichteten Wertetabellen Abbildung 1 erfolgen.

3.2 Initiale Arbeiten

Bei der Implementierung eines Informationssicherheitsmanagements (ISMS) fallen in hohem Maße einmalige Arbeiten, wie die Bildung des Sicherheitsteams, die Erstellung einer IT-Sicherheitsleitlinie (Policy), die (toolunterstützte) Erstellung des Sicherheitskonzeptes nach BSI-Standard 100-2 (IT-Grundschutz) [2], das Erstellen eines Kryptokonzeptes [9] und die Erstellung des IT-Notfallvorsorgekonzeptes sowie des IT-Notfall- und des Krisenmanagementkonzeptes [10] an.

Die IT-Sicherheitsbeauftragten der Behörden durchlaufen, möglichst vor Aufnahme ihrer Tätigkeit, ein die Rahmenbedingungen erfüllendes verpflichtendes Fortbildungsprogramm und besuchen Auffrischungskurse oder vergleichbare Veranstaltungen bzw. erwerben Zusatzqualifikationen. Diese Forderung des UP Bund [5] gilt auch für den Vertreter des IT-Sicherheitsbeauftragten und das Sicherheitsteam. Nur so ist sichergestellt, dass alle am Sicherheitsprozess Beteiligten die gleiche Qualifikation besitzen und eine zeitkritische Kommunikation bzw. Eskalation in einem Krisenfall reibungslos funktioniert.

Des Weiteren müssen gemäß IT-Notfall- und Krisenmanagementkonzept Meldewege eingerichtet und publiziert werden, die eine Erreichbarkeit des IT-Sicherheitsbeauftragten bzw. seines Vertreters garantieren.

3.3 Regelmäßige Arbeiten

Zu den regelmäßigen Arbeiten eines IT-Sicherheitsbeauftragten (IT-SiBe) gehören die Fortschreibung der Sicherheitskonzepte und die Aufrechterhaltung des ISMS. Schwerpunkt dieser Arbeiten sind u.a. die Überprüfung und Fortschreibung des Sicherheitskonzeptes, die Überprüfung und die Fortschreibung der IT-Notfall- und Krisenmanagementkonzepte, die Sensibilisierung der Mitarbeiter, die Auswertung von Lagebildern auf Relevanz, die Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, die Bewertung von Informationen über aktuelle Sicherheitsrisiken (z. B. BSI-Lageberichte auswerten, studieren einschlägiger Fachquellen (heise.de und ähnliche)), die Untersuchung sicherheitsrelevanter Vorfälle, Beratungen und die Berichterstattung an die Behördenleitung sowie Teilnahme an weiterbildenden Veranstaltungen und Gremien.

Aufgrund des neugeschaffenen Arbeitsumfeldes ist es für einen IT-Sicherheitsbeauftragten sehr wichtig, mit den IT-Sicherheitsbeauftragen anderer Behörden sowie mit Sicherheitsexperten des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein Kommunikationsnetzwerk aufzubauen und zu pflegen (Networking). Der Erfahrungsaustausch zu akuten Sicherheitsproblemen ist eine unverzichtbare Ressource im Krisenfall.

Neben den genannten Tätigkeiten muss der IT-Sicherheitsbeauftragte nicht nur seine Mitarbeiter schulen, sondern auch sich selbst weiterbilden, um auf dem Stand des technischen Fortschritts bleiben zu können.

3.4 Arbeiten im ersten Jahr

Im ersten Jahr der Einrichtung eines ISMS ergeben sich die einmaligen Arbeiten aus Abschnitt 3.2 sowie die Regelarbeiten aus Abschnitt 3.5 (mit Ausnahme der Überprüfung und Fortschreibung des Sicherheitskonzeptes und der IT-Notfall- und Krisenmanagementkonzepte).

3.5 Arbeiten in den Folgejahren

Der Zeitbedarf in den Folgejahren ergibt sich aus den Regelarbeiten gemäß Abschnitt 3.3. Durch den zu erwartenden Lernkurveneffekt ist anzunehmen, dass sich die Aufgaben eines IT-Sicherheitsbeauftragten routinieren. Die Personalbedarfsprognose sollte demnach mit dem Fortschritt und der Entwicklung der Informationssicherheit dynamisch angepasst werden.

Die Aspekte der Aus- und Weiterbildung der IT-Sicherheitsbeauftragten sind in diesem Dokument nur unzureichend mit zeitlichen Aufwänden dargestellt worden, diese müssen jedoch bei Fortschreibung bzw. in der Berechnung von zeitlichen Ressourcen „mit Bedacht“ eingebracht werden.

Beispielhaft angeführt werden Aufwände zum Besuch von Messen und Kongressen, für Fortbildungsprogramme und Workshops des BSI und der BAköV, für die Mitarbeit in Arbeitskreisen, für das Lesen von Fachzeitschriften und Newslettern, für interne Fachgespräche mit der IT-Abteilung, für die Beschäftigung mit Informationen der Hersteller von Sicherheitsprodukten, ggf. Organisation von Produktpräsentationen der Hersteller.

3.6 Vertreterregelung

Im BSI-Standard 100-2 [2] wird unter Punkt 3.4.4 gefordert, dass der IT-Sicherheitsbeauftragte einen qualifizierten Vertreter hat. Dieser Vertreter sollte gut ausgebildet und im laufenden Betrieb immer über die IT-Sicherheitslage informiert sein, so dass er jederzeit die Aufgabe des IT-Sicherheitsberaters wahrnehmen kann.

Es muss sichergestellt sein, dass im Falle eines Sicherheitsvorfalls die Kommunikationskette funktioniert, d. h. Funktions-E-Mailadressen oder Funktionsnotrufnummern erreichbar sind. Die zu erwartenden Vertretungsfälle wegen Fortbildung, Krankheit oder Urlaub des IT-Sicherheitsbeauftragten müssen in der Arbeitsplatzbeschreibung des Vertreters berücksichtigt werden. Des Weiteren sind dem Vertreter Zeitaufwände für seine eigene IT-Sicherheitsfortbildung sowie für regelmäßige Abstimmungsgespräche mit dem IT-Sicherheitsbeauftragten zuzugestehen.

Im Idealfall ist der Vertreter des IT-Sicherheitsbeauftragten Mitglied des IT-Sicherheitsteams und durch die Wahrnehmung von Teilaufgaben des IT-Sicherheitsbeauftragten in das Tagesgeschäft eingebunden. Der Vertreter muss zu jeder Zeit und ohne zeitliche Verzögerung die Aufgabe des IT-Sicherheitsbeauftragten übernehmen und fortführen können. Bei einer kurzfristigen Übernahme ist eine vorausgehende Einarbeitung in die aktuelle Sicherheitslage der Behörde nicht akzeptabel. Der Vertreter muss jederzeit auf dem gleichen Informationsstand sein, wie der IT-Sicherheitsbeauftragte selbst.

Der für den Vertreter entstehende Personalaufwand für den findet in der Arbeitshilfe respektive im Tool keine Berücksichtigung.

3.7 IT-Sicherheitsbeauftragter als IT-Geheimschutzverantwortlicher

VSA Bund, § 5 Verantwortung und Zuständigkeit

(6) Dienststellen, die VS mit Informationstechnik (IT) verarbeiten, bestimmen verantwortliche Personen mit IT-Fachkenntnissen, z.B. IT-Sicherheitsbeauftragte, die die Geheimschutzbeauftragten bei der Umsetzung der VS-Anweisung unterstützen. Die Verantwortlichen mit IT-Fachkenntnissen sollen nicht zugleich Aufgaben von Systemadministratoren bei für VS eingesetzten IT-Systemen wahrnehmen und müssen in Bezug auf die VS-Anweisung besonders geschult sein. Sie haben ebenfalls ein unmittelbares Vortragsrecht bei der Dienststellenleitung. Werden Verantwortliche mit IT-Fachkenntnissen für Geheimschutzmaßnahmen nicht bestimmt, so verbleiben deren Aufgaben bei den Geheimschutzbeauftragten oder der Dienststellenleitung.

In Behörden, in denen Verschlusssachen mit Informationstechnik verarbeitet werden, kann die Rolle des IT-Geheimschutzverantwortlichen (verantwortliche Personen mit IT-Fachkenntnissen) dem IT-Sicherheitsbeauftragten übertragen werden. In dieser Konstellation fallen nicht unerheblich zusätzliche Arbeitszeiten für den IT-Sicherheitsbeauftragten an, die in der Personalbedarfsermittlung berücksichtigt werden müssen.

3.8 Fallstudie „Dokumentation der Zeitansätze für das Erstellen eines IT-Sicherheitskonzeptes einer „Standardbehörde“ gemäß Abschnitt 3.1

Im Rahmen einer dem BSI vorliegenden Projektarbeit wurde der Prozess „Erstellen eines IT-Sicherheitskonzeptes mit dem Ziel der Zertifizierung“ Schritt für Schritt protokolliert und zeitlich quantifiziert [11]. Da die untersuchte Behörde mit ihren Daten beispielhaft für eine Standardbehörde gemäß der Definition in Abschnitt 3.1 steht, soll das Ergebnis als empirischer Erfahrungswert in die Personalbedarfsprognose mit einfließen. Die hierbei ermittelten Zeitbedarfe sind in Tabelle 7 chronologisch aufgelistet.

Für die Erstellung eines IT-Sicherheitskonzeptes nach IT-Grundschutz auf der Basis von ISO 27001 ohne den Zertifizierungsprozess sind in diesem Projekt 106,5 Personentage ermittelt. Dies entspricht in etwa dem Grundwert, der in den nachfolgenden Betrachtungen (3.9, Tabelle 1 für die einmalige toolunterstützte Erstellung eines Sicherheitskonzeptes nach BSI-Standard 100-2 (IT-Grundschutz) [2] bei einer Standardbehörde gemäß Abschnitt 3.1 gesetzt wird.

3.9 Rahmenbedingungen für die fachliche Personalprognose

Nach Analyse der rechtlichen Quellen und Konsolidierung der Zusammenstellung aus Kapitel 2 ergeben sich sowohl einmalige, strategische als auch regelmäßige, operative Tätigkeitsschwerpunkte. In Anlehnung an die Fallstudie aus 3.8 sowie die z. Zt. im Behördenumfeld eingesetzten Personalressourcen für die Tätigkeiten eines IT-Sicherheitsbeauftragten werden die Zeitansätze für die übrigen Mindeststandards unter Vorbehalt hochgerechnet (Tabelle 1 und Tabelle 2).

- 205 Personentage (PT) entsprechen 1 Arbeitskraft pro Jahr

- Für die zu bewertenden Aufgaben werden folgende Basiswerte pro Jahr zunächst gesetzt:

Einmalige strategische Aufgaben des IT-SiBe	Basiswert in PT
(Toolunterstützte) Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz)	120
Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI Standard 100-4	40

Tabelle 1 - Einmalige strategische Aufgaben des IT-Sicherheitsbeauftragten

Regelmäßige operative Aufgaben des IT-SiBe	Basiswert in PT
Überprüfung und Fortschreibung Sicherheitskonzept, Kryptokonzept	60
Überprüfung und Fortschreibung IT-Notfallvorsorge-konzept sowie IT-Notfall- und Krisenmanagementkonzept inkl. Übungen	30
Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungsaufwand, ohne Schulungsaufwand)	20
Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision	30
Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. der täglichen Sicherheitslage	20
Beratung und Berichterstattung	20

Tabelle 2 - Regelmäßige operative Aufgaben des IT-Sicherheitsbeauftragten

Die Festlegung der „Basiswerte“ sollte entsprechend der Risikosituation sowie dem Fortschritt der Anforderungen und der Entwicklung der Informationssicherheit in der Bundesverwaltung dynamisch angepasst werden.

So kann z. B. der Basiswert für die Sensibilisierung der Mitarbeiter durch Schulungsmaßnahmen gesenkt werden, während durch eine Verschärfung der Risikosituation der entsprechende Basiswert für die Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen steigen kann.

3.10 Zeitzuschläge für relevante Zusatzfaktoren

Ausgehend vom Metamodell aus Abschnitt 3.1 sollen zu den Basiswerten behördenbezogene prozentuale Zeitzuschläge in Abhängigkeit von

- Anzahl der Mitarbeiter,
- Grad der Heterogenität der IT-Landschaft und IT-Verfahren,
- Anzahl der zu betreuenden Außenstellen,
- Anteil der IT-Anwendungen mit einem Schutzbedarf höher als „normal“,
- Hochverfügbarkeitsanforderungen an IT-Anwendungen

berücksichtigt werden. Diese Zeitzuschläge werden für jeden Zusatzfaktor getrennt und innerhalb dieses Faktors nochmals nach den verschiedenen Aufgaben unterschiedlich bewertet (Abbildung 1).

3.10.1 Anzahl der Mitarbeiter

Mit der Anzahl der Mitarbeiter steigen die Zeitaufwände für die Tätigkeit des IT-Sicherheitsbeauftragten. Dies resultiert z. B. aufgrund einer höheren Anzahl von Anfragen an den IT-Sicherheitsbeauftragten und einer größeren Anzahl von durchzuführenden Sensibilisierungsveranstaltungen. Daher werden prozentual ansteigende Zeitzuschläge für die jeweiligen Tätigkeiten gewährt (Abbildung 1).

Dem Einwurf, dass nicht alle Mitarbeiter einer Behörde „en bloc“ in die Berechnung eingehen sollten - Personal ohne IT sei nicht zu berücksichtigen - ist zu widersprechen. Die Informationssicherheit folgt einem ganzheitlichen Ansatz. Alle Personen, die im Umfeld einer Behörde arbeiten, tragen zur Informationssicherheit in der Behörde bei. Angreifer nutzen z. B. Methoden des „social engineering“, die vielfach abseits der Technik liegen, sehr wohl aber integraler Bestandteil der Sicherheit sind. Die Aufwände zur Sensibilisierung der Mitarbeiter, auch für nicht IT-Personal, sind dem Aufgabenbereich des IT-Sicherheitsbeauftragten zuzurechnen.

3.10.2 Grad der Heterogenität der IT-Landschaft und IT-Verfahren

Bei einer inhomogenen IT-Landschaft, muss parallel zu den Komponenten der Windows-Welt, z. B. bei der Modellierung der Grundschutzbausteine, zusätzlich die Sicherheit der weiteren Betriebssystemkomponenten betrachtet werden. Aspekte der Heterogenität wirken sich weit über die Ebene der Betriebssysteme hinaus aus. Exotische und nicht weit verbreitete Anwendungen, neue technische Komponenten, die nur vereinzelt im Markt platziert sind, bedürfen einer besonderen technischen Analyse. Oftmals sind bei diesen Komponenten noch keine dem Standard entsprechenden „Grundschutzmaßnahmen“ zur Absicherung der Technik verfügbar, sodass die IT-Sicherheit mit ergänzenden Risikoanalysen geschaffen und aufrecht erhalten werden muss. Diesem Mehraufwand wird durch einen auf die jeweilige Tätigkeit abgestimmten Zuschlag Rechnung getragen (Abbildung 3 bis Abbildung 4). Für die Erfassung der Heterogenität der Software- und der IT-Systeme steht eine Staffelung von A, B und C zur Verfügung. Für die Kategorie A ist definiert, dass keine Heterogenität vorliegt. Die Kategorie B ist zu wählen, wenn eine durchschnittliche Heterogenität, d. h. es sind in der Regel zwei Betriebssysteme im Einsatz, in einer Behörde vorhanden ist. Behörden, die als IT-Dienstleister fungieren, sowie IT-Sicherheitsbehörden und deswegen über diese durchschnittliche Heterogenität hinaus viele spezielle und hochkomplexe IT-Verfahren verantworten, sind in der Kategorie C einzuordnen.

3.10.3 Anzahl der zu betreuenden Außenstellen

Für die Berücksichtigung der Anzahl der Außenstellen gilt analog das Verfahren in Abschnitt 3.10.1. Der Zuschlag berücksichtigt den erhöhten Aufwand für das IT-Sicherheitsmanagement, wen die Behörde Außenstellen besitzt. Dieser ergibt sich u.a. durch den Anpassungsbedarf von IT-Sicherheits- und Notfallkonzepten an die Infrastruktur von Außenstellen, den erhöhten Aufwand an Dienstreisen zur regelmäßigen Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen und zur Durchführung von Sensibilisierungsveranstaltungen in den Außenstellen. Als eine Außenstelle definierende Kriterien können die Betriebsgröße, z. B. über 20 Personen, die Komplexität der dort betriebenen Informationstechnik, der besondere Schutzbedarf der Informationen oder Anforderungen an sehr hohe Verfügbarkeit verwendet werden. Für den IT-Sicherheitsbeauftragten entsteht ein Mehraufwand ab der ersten Außenstelle.

3.10.4 Anteil der IT-Anwendungen mit einem Schutzbedarf höher als „normal“

Ist das Ergebnis der Schutzbedarfsfeststellung „hoch“ bzw. „sehr hoch“ muss gemäß BSI-Standard 100-2 [2] eine ergänzende Sicherheitsanalyse und eventuell eine Risikoanalyse nach BSI-Standard 100-3 [3] durchgeführt werden. Der für die Risikoanalyse benötigte Zeitaufwand wird auf einen Faktor 2 (verdoppeln) eingeschätzt. Daraus ergibt sich, entsprechend dem prozentualen Anteil dieser Anwendungen gemessen an der Gesamtzahl aller IT-Anwendungen, ein dementsprechend großer prozentualer Zuschlag - Beispiel: Anteil

IT-Anwendungen mit hohem Schutzbedarf ist 25%. Daraus folgt ein Zuschlag von 25% (Abbildung 2 und Abbildung 3).

3.10.5 Hochverfügbarkeitsanforderungen an IT-Anwendungen

Behörden mit Hochverfügbarkeitsanforderungen haben bezüglich der Informationssicherheit einen deutlich erhöhten Aufwand und erhalten dementsprechend einen den jeweiligen Tätigkeiten angepassten, gestaffelten Pauschalzuschlag (Abbildung 2 und Abbildung 3). Beispielhaft ist hier die Anwendung und Umsetzung des Hochverfügbarkeitskompendiums des BSI [17] zu nennen.

3.11 Zeitabschläge für ausgelagerte Tätigkeiten einer Behörde mit ausgelagerter IT (Outsourcing)

Behörden, die ihre IT auslagern, schließen in der Regel mit dem jeweiligen Dienstleister ein Vertrag ab. In diesen Service Level Agreements (SLA) werden Verantwortung und Aufwände für die Informationssicherheit der genutzten IT-Landschaft teilweise auf den Dienstleister übertragen. Da der IT-Sicherheitsbeauftragte dadurch deutlich entlastet wird, ist es erforderlich, vom ermittelten Gesamtzeitaufwand einen prozentualen Abschlag zu subtrahieren (Abbildung 1 und Abbildung 3).

Art und Umfang der „Auslagerung IT“ z. B. Betrieb von Hard- und Software, Verantwortung für die Netzinfrastruktur, Betreuung der Anwender, Abgrenzung von Verantwortlichkeiten, bestimmen den prozentualen Abschlag. In der Berechnungsmatrix wird ein prozentualer Abschlag von 50% angenommen, wenn der gesamte IT-Betrieb ausgelagert ist. Bei Teilauslagerungen ist der Abschlag adäquat anzupassen – hier sind Erfahrungswerte mit Behörden, die mit Outsourcing bereits längerfristige Erfahrungen haben, hilfreich.

3.12 Berechnungsmatrix der Bewertungsfaktoren

In Abbildung 2 und Abbildung 3 ist eine Matrix dargestellt, in der die Kernaufgaben horizontal und die jeweiligen Zu- und Abschlagsfaktoren vertikal angeordnet sind. Zur Erfüllung der Kernaufgaben werden darin gemäß Tabelle 1 und Tabelle 2 zunächst pauschale Zeitwerte gewährt (Spalte „Typischer Aufwand Personentagen“). In einer Zeile über dieser Matrix werden die individuellen Daten der zu berechnenden Behörde hinterlegt. Ausgehend von diesen Daten können dann die jeweiligen prozentualen Zu- und Abschläge (bezogen auf die Basiswerte der Kernaufgaben) ermittelt werden. Die jeweiligen Berechnungsmodus hierzu ergeben sich aus den unter 3.10 und 3.11 dargelegten Verfahren.

Die gezeigten Musterberechnungen beziehen sich auf das in 3.1 definierte Metamodell einer „Standardbehörde“. Die in Abbildung 2 dargestellte Musterbehörde betreibt eine eigene IT, während die Musterbehörde gemäß Abbildung 3 ihren IT-Betrieb ausgelagert hat.

Für jede der 8 Kernaufgaben (2 einmalige und 6 dauerhafte Aufgaben) ergibt sich demgemäß folgende Summenformel in Personentagen (PT):

SUMME PT = Basiswert in PT x (100% + Zuschläge in %)

Im unteren Teil der Abbildungen werden anschließend der Personalbedarfe für das erste Jahr und die Folgejahre errechnet. Im ersten Jahr der Implementierung eines Informationssicherheitsmanagementsystems werden die einmaligen strategischen Kernaufgaben

- (toolunterstützte) Erstellung eines Sicherheitskonzeptes nach den BSI-Standards 100-2 [2] und 100-3 [3]
- Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI-Standard 100-4 [18]
- sowie die regelmäßige operative Kernaufgaben
- Sensibilisierung der Mitarbeiter,
- Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision,
- Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. Sicherheitslage
- Beratung und Berichterstattung

aufaddiert. Für die Folgejahre werden nur noch die regelmäßigen operativen Aufgaben bei der Personalbedarfsermittlung berücksichtigt.

ZUSCHLAGSTABELLEN (nicht linear, degressiv) zu dem Bewertungsaspekt „Anzahl der Mitarbeiter“

Sicherheitskonzept (einmalig)		Weitere Konzepte (einmalig)		Fortschreibung Sicherheitskonzept (dauerhaft)		Fortschreibung weiterer Konzepte (dauerhaft)		Sensibilisierung der Mitarbeiter		Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen		Untersuchung sicherheitsrelevanter Vorfälle	
ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %
0	0%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
501	20%	501	5%	501	20%	501	20%	501	20%	501	20%	501	20%
1.001	50%	1.001	12%	1.001	50%	1.001	50%	1.001	50%	1.001	50%	1.001	50%
1.501	70%	1.501	20%	1.501	70%	1.501	70%	1.501	70%	1.501	70%	1.501	70%
2.501	90%	2.501	22%	2.501	90%	2.501	90%	2.501	90%	2.501	90%	2.501	90%
3.001	120%	3.001	30%	3.001	120%	3.001	120%	3.001	120%	3.001	120%	3.001	120%
4.001	200%	4.001	50%	4.001	200%	4.001	200%	4.001	200%	4.001	200%	4.001	200%
5.001	350%	5.001	90%	5.001	350%	5.001	350%	5.001	350%	5.001	350%	5.001	350%
6.001	500%	6.001	125%	6.001	500%	6.001	500%	6.001	500%	6.001	500%	6.001	500%
8.001	700%	8.001	180%	8.001	700%	8.001	700%	8.001	700%	8.001	700%	8.001	700%

ZUSCHLAGSTABELLEN (nicht linear, degressiv) zu dem Bewertungsaspekt „Anzahl der Außenstellen“

Sicherheitskonzept (einmalig)		Weitere Konzepte (einmalig)		Fortschreibung Sicherheitskonzept (dauerhaft)		Fortschreibung weiterer Konzepte (dauerhaft)		Sensibilisierung der Mitarbeiter		Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen		Untersuchung sicherheitsrelevanter Vorfälle	
ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %	ab	Zuschlag in %
0	0%	0	0%	0	0%	0	0%	0	0%	0	0%	0	0%
1	5%	1	10%	1	5%	1	5%	1	5%	1	5%	1	5%
15	10%	15	30%	15	10%	15	10%	15	10%	15	10%	15	10%
30	40%	30	80%	30	40%	30	40%	30	40%	30	40%	30	40%
60	80%	60	160%	60	80%	60	80%	60	80%	60	80%	60	80%
100	100%	100	200%	100	100%	100	100%	100	100%	100	100%	100	100%
250	300%	250	300%	250	300%	250	300%	250	300%	250	300%	250	300%
500	400%	500	400%	500	400%	500	400%	500	400%	500	400%	500	400%
1.000	500%	1.000	500%	1.000	500%	1.000	500%	1.000	500%	1.000	500%	1.000	500%
1.500	600%	1.500	600%	1.500	600%	1.500	600%	1.500	600%	1.500	600%	1.500	600%

Abbildung 1 - Screenshot Berechnungstool - Zu- und Abschlagstabellen

	IT-Sicherheitsaufgabe	Typischer Aufwand in Personentagen	Zuschlag für Anzahl der Mitarbeiter	Zuschlag für Heterogene IT-Landschaft und IT-Verfahren	Zuschlag für Außenstellen	Anteil der IT-Anwendungen mit hohem Schutzbedarf (verhältnismäßig zu allen IT-Anwendungen)	Zuschlag für Schutzbedarf mit Hochverfügbarkeits-anforderung	Summe in Personentagen (ohne Outsourcing)
	Metamodell Standardbehörde		500	A	0	0%		
initiale Aufgaben	Toolunterstützte Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz), Kryptokonzept	120	0 %	0%	0 %	0%		120
initiale Aufgaben	Erstellung IT-Notfallvorsorge-konzept sowie IT-Notfall- und IT-Krisenmanagementkonzept, BSI-Standard 100-4	40	0 %	0%	0 %	0%	0 %	40
Aktualisierung und Fortschreibung	Überprüfung und Fortschreibung Sicherheitskonzept und Kryptokonzept	60	0 %	0%	0 %	0%		60
Aktualisierung und Fortschreibung	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und IT-Krisenmanage-mentkonzept inkl. Übungen , BSI-Standard 100-4	30	0 %	0%	0 %	0%	0 %	30
Aktualisierung und Fortschreibung	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungs-aufwand, ohne Schulungsaufwand)	20	0%	0%	0%	0%		20
Aktualisierung und Fortschreibung	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Revision und Audits	30	0%	0%	0%	0%		30
Aktualisierung und Fortschreibung	Untersuchung sicherheitsrelevanter Vorfälle, ajour halten (z.B. Heise-Ticker, CERT-Meldungen)	20	0%	0%	0%	0%		20
Aktualisierung und Fortschreibung	Beratung (auch. in IT-Fachverfahren) und Berichterstattung	20	0 %	0%	0 %	0%		20

ERGEBNIS		
1. Jahr	250,00 PT	1,22 Kräfte
Folgejahre	180,00 PT	0,88 Kräfte

OUTSOURCING	
Prozentuale tatsächliche Entlastung der IT-SiBe durch ausgelagerte IT	0%

Abbildung 2 - Berechnungsmatrix Metamodell „Standardbehörde“ mit 500 Mitarbeitern

	IT-Sicherheitsaufgabe	Typischer Aufwand in Personentagen	Zuschlag für Anzahl der Mitarbeiter	Zuschlag für Heterogene IT-Landschaft und IT-Verfahren	Zuschlag für Außenstellen	Anteil der IT-Anwendungen mit hohem Schutzbedarf (verhältnismäßig zu allen IT-Anwendungen)	Zuschlag für Schutzbedarf mit Hochverfügbarkeits-anforderung	Summe in Personentagen (ohne Outsourcing)
	Musterbehörde		**550**	**B**	**10**	**25%**	**X**	
Initiale Aufgaben	Toolunterstützte Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz), Kryptokonzept	120	20 %	30%	5 %	25%		216
	Erstellung IT-Notfallvorsorge-konzept sowie IT-Notfall- und IT-Krisenmanagementkonzept, BSI-Standard 100-4	40	5 %	30%	10 %	25%	50 %	88
Aktualisierung und Fortschreibung	Überprüfung und Fortschreibung Sicherheitskonzept und Kryptokonzept	60	20 %	30%	5 %	25%		108
	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und IT-Krisenmanage-mentkonzept inkl. Übungen , BSI-Standard 100-4	30	20 %	30%	5 %	25%	50 %	69
	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungs-aufwand, ohne Schulungsaufwand)	20	20%	10%	5%	25%		32
	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Revision und Audits	30	20%	20%	5%	25%		51
	Untersuchung sicherheitsrelevanter Vorfälle, ajour halten (z.B. Heise-Ticker, CERT-Meldungen)	20	20%	20%	5%	25%		34
	Beratung (auch in IT-Fachverfahren) und Berichterstattung	20	20 %	10%	5 %	25%		32

ERGEBNIS		
1. Jahr	453,00 PT	2,21 Kräfte
Folgejahre	326,00 PT	1,59 Kräfte

OUTSOURCING	
Prozentuale tatsächliche Entlastung der IT-SiBe durch ausgelagerte IT	0%

Musterbehörde mit

- 550 Mitarbeiter
- heterogene IT-Landschaft und IT-Verfahren
- 10 Außenstellen
- 25% höherer Schutzbedarf
- Hochverfügbarkeitsanforderung

Abbildung 3 - Berechnungsmatrix Musterbehörde mit leicht erhöhten Anforderungen

3.13 Szenario zur Abschätzung der Personalressource am Beispiel einer „Standardbehörde“ gemäß 3.1

In den voranstehenden Tabellen wurden Behörden exemplarisch berechnet. Die Standardbehörde „Meta-modell“ benötigt zur Bewältigung der aufgezeigten gesetzlich geforderten Mindestaufgaben eines IT-SiBe (Aufgabenkatalog unter 2) einen Personalaufwand von 1,22 Kräften (250 PT) im 1. Jahr und 0,88 Kräfte (188 PT) in den folgenden Jahren (Abbildung 2). Schon bei der Berechnung einer durchschnittlichen Bundesbehörde, die von der Standardbehörde nur gering abweicht (550 Mitarbeiter, heterogene IT-Landschaft und IT-Verfahren Kategorie A, 10 Außenstellen, 25% IT-Projekt mit erhöhtem Schutzbedarf und eine Hochverfügbarkeitsanforderung) erhöhen sich diese Werte schon auf 2,21 bzw. 1,59 Kräfte (Abbildung 3).

Zur Erfüllung der Forderungen des UP Bund sind Fristen zu wahren. Das zweite Berechnungsbeispiel weist nach, dass für die Erfüllung der Tätigkeiten eines IT-SiBe bei einer durchschnittlichen Behörde mehr als eine Person verantwortlich sein muss.

Bei Unterbesetzung können die „Kernaufgaben“ des IT-SiBe nicht erledigt werden. Gesetzliche Fristen und Vorgaben, wie sie im UP Bund vorgegeben werden, können keinesfalls eingehalten werden.

3.14 Erläuterungen zur Berechnungsmatrix der Bewertungsfaktoren

In der Abbildung 4 sind die Felder mit Zuschlägen durchnummeriert worden. Die jeweiligen Korrelationen der Kreuzpunkte, die Höhe der Zuschläge, der Verlauf der Zuschläge sowie die Begründungen hierzu sind im Anhang erläutert.

	IT-Sicherheitsaufgabe	Typischer Aufwand in Personentagen	Zuschlag für Anzahl der Mitarbeiter	Zuschlag für heterogene IT-Landschaft und IT-Verfahren	Zuschlag für Aussenstellen	Anteil der IT-Anwendungen mit hohem Schutzbedarf (verhältnismäßig zu allen IT-Anwendungen)	Zuschlag für Schutzbedarf mit Hochverfügbarkeits-anforderung
	Kurzbez. Behörde						
initiale Aufgaben	Toolunterstützte Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz) und Kryptokonzept	**120**	01	09	17	25	33
	Erstellung IT-Notfallvorsorge-konzept sowie IT-Notfall- und IT-Krisenmanagementkonzept, BSI-Standard 100-4	**40**	02	10	18	26	34
Aktualisierung und Fortschreibung	Überprüfung und Fortschreibung Sicherheitskonzept und Kryptokonzept	**60**	03	11	19	27	35
	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und IT-Krisenmanage-mentkonzept incl. Übungen	**30**	04	12	20	28	36
	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungs-aufwand, ohne Schulungsaufwand)	**20**	05	13	21	29	37
	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Revision und Audits	**30**	06	14	22	30	38
	Untersuchung sicherheitsrelevanter Vorfälle, ajour halten (z.B. Heise-Tickert, CERT-Meldungen)	**20**	07	15	23	31	39
	Beratung (auch. in IT-Fachverfahren) und Berichterstattung	**20**	08	16	24	32	40

Abbildung 4 - Berechnungsmatrix mit gekennzeichneten Zuschlagsfeldern

4 Arbeitshilfe zur Berechnung der Personalprognose

Um die bisher gewonnenen Erkenntnisse umsetzen zu können, wurde mit Hilfe von Microsoft Excel® ein Tool entwickelt. Diese Arbeitshilfe ermöglicht eine schnelle Berechnung von Personalprognosen für mehrere Behörden und stellt die Ergebnisse in einer Vergleichstabelle zusammen (Abbildung 4).

Des Weiteren lassen sich die gestaffelten Zu- und Abschläge, die in einer Referenztabelle hinterlegt sind, anpassen (Abbildung 1). Das Tool benötigt zur Berechnung je Behörde lediglich die Parameter gemäß Abschnitt 3.12 und 3.13. Es ist jederzeit möglich, eine weitere Behörde aufzunehmen, sowie eine Behörde aus der Berechnung zu entfernen. Die eingegebenen Behördenparameter können jederzeit aktualisiert werden.

4.1 Fachliche Anforderungen an das Tool

Interoperabilität

Ziel der Arbeitshilfe ist es, mit möglichst geringem Aufwand die Bewertungsparameter einer Behörde zu erfassen und die Beurteilung der relevanten Faktoren automatisiert in die Berechnung einfließen zu lassen. Die Handhabung sollte selbsterklärend sein.

Adaptivität

Die Berechnungsfaktoren der Zu- und Abschläge (gestaffelte Werte) können im Tool ohne großen Aufwand geändert.

Skalierbarkeit

Es wurde darauf geachtet, dass das Tool sowohl für Kleinstbehörden als auch für sehr große Bundesbehörden realistische Zuschlagsfaktoren berücksichtigt.

Die Daten aller Behörden, die in die Anwendung eingegeben worden sind, werden auf dem Tabellenblatt „BESTAND“ (Abbildung 5) aufgelistet. Diese Zusammenstellung ist nach der Kurzbezeichnung der Behörden sortiert. Neu aufzunehmende Behörden werden entsprechend einsortiert. Durch Doppelklicken auf einen Behördennamen (Lang- oder Kurzform) springt die Anwendung in das Berechnungsblatt der entsprechenden Behörde.

BEHÖRDENÜBERSICHT - Last updated : 19.06.2012 - 12:49:23 Uhr — **18 BEHÖRDEN**

Behörde (Langform)	Behörde (Kurzbezeichnung)	Anzahl der Mitarbeiter	Interessen IT-Landschaft und IT-Verfahren vorhanden	Anzahl Anbaustellen	Anteil der IT-Ausnahmen mit hohen Schutzbedarf (verhältnismäßig zu allen IT-Ausnahmen) in %	Schutzbedarf mit Hochverfügbarkeitsanforderung vorhanden	Anteil der ausgelagerten IT in %	Personalbedarf im 1. Jahr in Personentage (PT)	Personalbedarf im 1. Jahr in Personentage (Kräfte)	Personalbedarf im Folgejahr in Personentage (PT)	Personalbedarf im Folgejahr in Personentage (Kräfte)	Personalbedarf im 1. Jahr in Personentage (PT)	Personalbedarf im 1. Jahr in Personentage (Kräfte)	Personalbedarf im Folgejahr in Personentage (PT)	Personalbedarf im Folgejahr in Personentage (Kräfte)
												OHNE OUTSOURCING		(ZUR INFORMATION)	
Behörde A	BA	23	A	0	0		0	250,00	1,22	180,00	0,88				
Behörde B	BB	501	B	3	5		5	363,85	1,77	261,25	1,27	383,00	1,87	275,00	1,34
Behörde C	BC	70	B	1	10		15	298,78	1,46	210,80	1,03	351,50	1,71	248,00	1,21
Behörde D	BD	142	A	0	10		0	275,00	1,34	198,00	0,97				
Behörde E	BE	150	A	0	10		5	261,25	1,27	188,10	0,92	275,00	1,34	198,00	0,97
Behörde F	BF	150	A	0	10		0	275,00	1,34	198,00	0,97				
Behörde G	BG	210	B	1	10	X	0	371,50	1,81	263,00	1,28				
Behörde H	BH	274	B	1	10	X	0	371,50	1,81	263,00	1,28				
Behörde I	BI	290	A	2	10	X	25	232,13	1,13	166,50	0,81	309,50	1,51	222,00	1,08
Behörde J	BJ	500	B	1	25		0	389,00	1,90	275,00	1,34				
Behörde K	BK	1.700	C	10	25		0	606,00	2,96	442,00	2,16				
Behörde L	BL	2.100	C	10	0	X	0	563,50	2,75	412,00	2,01				
Behörde M	BM	2.152	C	3	50	X	0	688,50	3,36	502,00	2,45				
Behörde N	BN	2.500	B	1	23	X	20	447,20	2,18	329,92	1,61	559,00	2,73	412,40	2,01
Behörde O	BO	2.780	A	2	5	X	0	494,80	2,41	375,00	1,83				
Behörde P	BP	3.600	C	45	20	X	0	824,00	4,02	601,00	2,93				
Behörde Q	BQ	5.300	B	8	75	X	0	1.305,00	6,37	1.010,00	4,93				
Behörde R	BR	10.500	B	260	60	X	5	2.635,30	12,86	2.036,80	9,94	2.774,00	13,53	2.144,00	10,46

Abbildung 5 - Screenshot Berechnungstool - Zusammenstellung der Behörden

5 Zusammenfassung, Bewertung und Ausblick

Die Notwendigkeit der Implementierung eines Informationssicherheitsmanagements ist erkannt und wird konsequenterweise auch in übergeordneten Sicherheitsstrategien des Bundes gefordert. Die Bedrohungen durch vorsätzliche Angriffe, das mit Einsatz der Technik generell verbundene Risiko und gesetzliche Grundlagen begründen die Mindestaufgaben eines IT-Sicherheitsbeauftragten. Die Feststellung des Aufwandes leitet mit Begründungen in die Planung erforderlicher Personalressourcen über. Im Bereich der Sicherheit in der IT besteht das generelle Vermittlungsproblem darin, die Risiken bei Betrieb von Informationstechnik darzustellen und daraus die Notwendigkeit personeller Ressourcen zu begründen.

Das Mittel der Wahl zur Lösung der o.a. Herausforderung sind detaillierte Darstellungen der Tätigkeiten des IT-Sicherheitsbeauftragten, die in Summe und ganzheitlich „Informationssicherheit“ gewährleisten. Diese granular strukturierten Tätigkeiten werden auf „personelle“ Aufwände gespiegelt, die in der Folge die Argumentation für erforderliches Fachpersonal bilden. Wesentlich für die Belastbarkeit des Ergebnisses „personelle Aufwände“ sind somit belastbare und strukturierte Auflistungen von Aufgaben im Bereich des Informationssicherheitsmanagements.

Bemessungsmethoden, die eine Aufnahme des Ist-Zustandes zugrunde legen, sind nicht zielführend. Die Bestandsaufnahme der Umsetzung des UP Bund ist ein hinreichender Beleg für den derzeitig unbefriedigenden Ist-Zustand der IT-Sicherheit in der Bundesverwaltung. Die Erwartung ist, zur Gewährleistung der IT-Sicherheit muss hinsichtlich des personellen Ressourceneinsatzes deutlich nachgebessert werden. Die Bemessung der personellen Aufwände muss anhand der Mindeststandards zur IT-Sicherheit als „Soll-Zustand“ dargestellt werden. Es wird erwartet, dass die Standards zur IT-Sicherheit und die gesetzlichen Erfordernisse zur Einhaltung von Datenschutz und Datensicherheit nicht strittig gestellt werden. In allen anderen Fällen fehlt die Basis einer Bemessung der personellen Ressourcenplanung.

Die Arbeitshilfe hat nicht den Anspruch belastbare Berechnungsmodelle für die Behörden zu entwickeln. Sie hat vielmehr das Ziel die Diskussionen um personelle Aufwände zur Gewährleistung der Informationssicherheit anzuregen.

Durch das in der Arbeitshilfe skizzierte Modell einer „Aufwandsschätzung“ wird ein Beitrag geleistet, die in der Vergangenheit teils sehr kontrovers und ergebnisoffenen Diskussionen zu versachlichen.

Konstruktive Kritik an der Arbeitshilfe ist notwendig, weil eine Reihe von Aufgaben bzw. Tätigkeiten eines IT-Sicherheitsbeauftragten bzw. eines Sicherheitsteams bisher nicht oder nur unzureichend erwähnt sind:

Die Aus- und Weiterbildung, in UP Bund als „Flächendeckende Fortbildung“ gefordert, wird weder qualitativ noch quantitativ erfasst.

Aufwände für das operative Sicherheitsmanagement (z. B. Tagesgeschäft, Projektmitarbeit, Projektleitung, Beratung der Mitarbeiter, Abstimmung mit Datenschutz bzw. Personalrat) sind nicht vollständig angeführt.

Die Rolle „Vertreter“ bzw. die Aufwände zur Innenorganisation des Sicherheitsteams lassen sich nur unzureichend quantitativ darstellen. Dies ist keine Besonderheit der IT-Sicherheit, sondern auch in anderen Bereichen werden die personellen Ressourcen für eine ordnungsgemäße Ausfüllung dieser Rolle deutlich unterschätzt.

Die Reaktion auf aktuelle Sicherheitsempfehlungen des BSI, insbesondere CERT-Warnungen, Hersteller-Sicherheitsupdates sowie Patches und die täglichen Lageberichte zu aktuellen Risiken sind Teil des Sicherheitsmanagements. Eine zeitnahe Umsetzung erforderlicher Reaktionen sind i.d.R. nicht von einer Einzelperson zu leisten, sondern erfordern die Zusammenarbeit im Sicherheitsteam. Diese Aktivitäten müssen mit Schätzungen zusätzlich in den Personalbedarf eingebracht werden.

Aufgaben, die gemeinhin als IT-Betrieb gesehen werden, wie z. B. Software-Abnahme und Freigabe-Verfahren, die Mitwirkung bei der Konzeption von Testplänen oder die Bewertung neuer Sicherheitsprodukte, erfordern aus nachvollziehbaren Gründen die Mitwirkung des IT-Sicherheitsteams. Diese Aktivitäten müssen mit Schätzungen zusätzlich in den Personalbedarf eingebracht werden.

Die angeführten Beispiele führen zu der Einschätzung, dass die „Arbeitshilfe zur Feststellung des Aufwandes und zur Planung des personellen Ressourceneinsatzes für IT-Sicherheitsteams in der öffentlichen Verwaltung (des Bundes)“ nur ein Ansatz sein kann. Die personellen Ressourcen sind in der Arbeitshilfe somit nur als „minimaler Ansatz“ zu werten.

Wie wiederholt erwähnt, entbindet das in diesem Dokument beschriebene Vorgehen die Behörde nicht von der Notwendigkeit, nach einer Konsolidierungsphase, eine Personalbedarfsermittlung nach anerkannten Methoden des Organisationshandbuchs durchzuführen. Bei der Anwendung dieser Methode sollte auf die vollständige Erfassung aller Tätigkeiten des IT-Sicherheitsbeauftragten bzw. des IT-Sicherheitsteams geachtet werden.

Die (überbehördliche) Arbeitsgruppe „IT-Fachkräfte“ sollte im Fokus künftiger Diskussionen um Arbeitsinhalte und Tätigkeiten der IT-Sicherheit bleiben. Die Aufgaben der IT-Sicherheit sind Bestandteil, Teilmenge oder Schnittmenge des Arbeitsbereiches „IT-Fachkräfte“. Auf der Basis der Ergebnisse der Arbeitsgruppe

„IT-Fachkräfte“ lassen sich Abstimmprozesse über die Aufgabenverteilung zwischen IT-Betrieb und IT-Sicherheit geradezu vorbildlich durchführen.

Anhang

Gegenüberstellung IT-Grundschutz des BSI und der ISO 27001

Die in diesem Abschnitt referenzierten IT-Grundschutz Kataloge [19] beziehen sich auf die 12. Ergänzungslieferung.

W	M	J	E	Mx	Quelle ISO 27001		Quelle im IT-Grundschutz	
			x	1	4.2	Establishing and managing the ISMS	B 1.0	Sicherheitsmanagement
	x			3	8	ISMS Improvement	M 2.199	Aufrecherhaltung der Informationssicherheit

Tabelle 3 - Gegenüberstellung IT-Grundschutz des BSI und der ISO 27001

Legende: B = Baustein des IT-Grundschutzkataloges, M = Maßnahme des IT-Grundschutzkataloges , Mx = Spaltennummer in der Berechnungsmatrix

Gegenüberstellung IT-Grundschutz des BSI und der ISO 27002

Die in diesem Abschnitt referenzierten IT-Grundschutz Kataloge [19] beziehen sich auf die 12. Ergänzungslieferung.

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz	
			x	1	4.1	Assessing security risks	M 2.195	Erstellung eines Sicherheitskonzepts
			x	1	5.1.1	Information security policy document	M 2.192	Erstellung einer Leitlinie zur Informationssicherheit
	x			3	5.1.2	Review of the information security policy	Aktualisierung der IT-Sicherheitsleitlinie BSI-Standard 100-2, Kapitel 3.3 Erstellung einer IT-Sicherheitsleitlinie, B 1.0 Sicherheitsmanagement M 2.193 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit M 2.199 Aufrechterhaltung der Informationssicherheit	
			x	1	6.1.2	Information security coordination	M 2.193	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz
x				1	6.1.4	Authorization process for information processing facilities	B 1.9 Hard- und Software-Management B 1.0 Sicherheitsmanagement M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.216 Genehmigungsverfahren für IT-Komponenten
x				1	6.1.5	Confidentiality agreements	M 3.55 Vertraulichkeitsvereinbarungen B 1.2 Personal M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
			x	2	6.1.6	Contact with authorities	B 1.3 IT-Notfallmanagement B 1.8 Behandlung von Sicherheitsvorfällen M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen M 6.61 Eskalationsstrategie für Sicherheitsvorfälle M 6.65 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen
x				6	6.1.7	Contact with special interest groups	M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.199 Aufrechterhaltung der Informationssicherheit
			x	1	7.1.1	Inventory of assets	IT-Strukturanalyse, BSI-Standard 100-2, Kapitel 4.1 B 1.0 Sicherheitsmanagement B 1.1 Organisation M 2.139 Ist-Aufnahme der aktuellen Netzsituation

W	M	J	E	Mx	Quelle ISO 27002	Quelle im IT-Grundschutz
						M 2.195 Erstellung eines IT-Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
x				1	7.2.1 Classification guidelines	Schutzbedarfsfeststellung, BSI-Standard 100-2, Kapitel 4.2 B 1.0 Sicherheitsmanagement M 2.195 Erstellung eines IT-Sicherheitskonzepts M 2.217 Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen
x				5	8.1.3 Terms and conditions of employment	M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.2 Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen B 1.2 Personal M 3.1 Geregelte Einarbeitung / Einweisung neuer Mitarbeiter
x				5	8.2.1 Management responsibilities	M 2.198 Sensibilisierung der Mitarbeiterfür Informationssicherheit B 1.13 Sensibilisierung und Schulung zur Informationssicherheit M 2.226 Regelungen für den Einsatz von Fremdpersonal M 3.5 Schulung zu Sicherheitsmaßnahmen
x				7	8.2.3 Disciplinary process	M 2.39 Reaktion auf Verletzungen der Sicherheitsvorgaben B 1.8 Behandlung von Sicherheitsvorfällen M 2.192 Erstellung einer Leitlinie zur

W	M	J	E	Mx	Quelle ISO 27002	Quelle im IT-Grundschutz
						Informationssicherheit M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
x				7	8.2.3 Disciplinary process	M 2.39 Reaktion auf Verletzungen der Sicherheitspolitik B 1.8 Behandlung von Sicherheitsvorfällen M 2.192 Erstellung einer IT-Sicherheitsleitlinie M 3.26 Einweisung des Personals in den sicheren Umgang mit IT
			x	1	9.1.1 Physical security perimeter	M 1.55 Perimeterschutz M 2.17 Zutrittsregelung und –kontrolle B 2.1 Gebäude M 1.10 Verwendung von Sicherheitstüren und –fenstern M 1.17 Pförtnerdienst M 1.19 Einbruchsschutz M 1.50 Rauchschutz
			x	1	9.1.2 Physical entry controls	M 2.17 Zutrittsregelung und –kontrolle B 2.1 Gebäude B 2.9 Rechenzentrum M 1.49 Technische und organisatorische Vorgaben für das Rechenzentrum M 1.58 Technische und organisatorische Vorgaben für Serverräume M 2.6 Vergabe von Zutrittsberechtigungen
			x	5	9.2.5 Security of equipment off-premises	B 2.10 Mobiler Arbeitsplatz B 3.203 Laptop

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz	
							B 5.8	Telearbeit
			x	1	9.2.6	Secure disposal or re-use of equipment	M 2.167 M 2.36 M 4.32 M 4.28	Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten Geregelte Übergabe und Rücknahme eines tragbaren PC Physikalisches Löschen der Datenträger vor und nach Verwendung Software-Reinstallation bei Benutzerwechsel eines Laptops
x				3	10.1.1	Documented operating procedures	M 2.219 B 1.9 B 4.2 M 2.201	Kontinuierliche Dokumentation der Informationsverarbeitung Hard- und Software-Management Netz- und Systemmanagement Dokumentation des Sicherheitsprozesses
x				3	10.1.2	Change management	M 2.221 M 4.78	Änderungsmanagement Sorgfältige Durchführung von Konfigurationsänderungen
x				1	10.1.4	Separation of development, test and operational facilities	M 2.62 M 2.9 M 2.82 M 4.95	Software-Abnahme- und Freigabe-Verfahren Nutzungsverbot nicht freigegebener Software Entwicklung eines Testplans für Standardsoftware Minimales Betriebssystem
x				1	10.2.3	Managing changes to third party services	M 2.221 M 2.34	Änderungsmanagement Dokumentation der Veränderungen an einem bestehenden System

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz	
x				1	10.4.1	Controls against malicious software	B 1.6 B 1.8 M 2.9 M 2.35 M 2.154 M 4.253 M 6.23	Schutz vor Schadprogrammen Behandlung von Sicherheits-vorfällen Nutzungsverbot nicht freigegebenen Hard- und Software Informationsbeschaffung über Sicherheitslücken des Systems Erstellung eines Sicherheitskonzeptes gegen Schadsoftware Schutz vor Spyware Verhaltensregeln bei Auftreten von Schadprogrammen
			x	1	10.5.1	Information back-up	B 1.4 M 6.20 M 6.32 M 6.41	Datensicherungskonzept Geeignete Aufbewahrung der Backup-Datenträger Regelmäßige Datensicherung Übungen zur Datenrekonstruktion
			x	1	10.6.2	Security of network services	B 4.1 B 3.301 B 4.2 B 4.4 B 4.5 M 4.133 M 5.68	Heterogene Netze Sicherheitsgateway (Firewall) Netz- und Systemmanagement VPN LAN-Anbindung eines IT-Systems über ISDN Geeignete Auswahl von Authentikationsmechanismen Einsatz von Verschlüsselungsverfahren zur Netzkommunikation

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz	
			x	1	10.8.1	Information exchange policies and procedures	M 2.393 B 3.402 B 3.404 B 5.2 B 5.3 B 5.14	Regelung des Informationsaustausches Faxgerät Mobiltelefon Datenträgeraustausch Groupware Mobile Datenträger
			x	1	0.8.4	Electronic messaging	B 5.3 M 2.217 M 5.54 M 5.56 M 5.108	Groupeware Sorgfältige Einstufung und Umgang mit Informationen, Anwendungen und Systemen Umgang mit unerwünschten E-Mails Sicherer Betrieb eines Mailservers Kryptographische Absicherung von Groupware bzw. E-Mail
			x	1	10.9.2	On-Line Transactions	B 1.7 M 2.162 M 2.164 M 4.176 M 5.88	Kryptokonzept Bedarfserhebung für den Einsatz kryptographischer Verfahren und Produkte Auswahl eines geeigneten kryptographischen Verfahrens Auswahl einer Authentisierungsmethode für Webangebote Vereinbarung über Datenaustausch mit Dritten
x				6	10.10.1	Audit logging	M 2.64 M 2.110 M 4.81 M 5.9	Kontrolle der Protokolldateien Datenschutzaspekte bei der Protokollierung Audit und Protokollierung der Aktivitäten im Netz Protokollierung am Server

W	M	J	E	Mx	Quelle ISO 27002	Quelle im IT-Grundschutz
			x	1	10.10.3 Protection of log information	M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 2.110 Datenschutzaspekte bei der Protokollierung M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen M 4.93 Regelmäßige Integritätsprüfung
			x	1	11.2 User access management	M 2.30 Regelung für die Einrichtung von Benutzern / Benutzergruppen M 2.31 Dokumentation der zugelassenen Benutzer und Rechteprofile M 2.63 Einrichten der Zugriffsrechte M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle
			x	1	11.2.3 User password management	M 2.11 Regelung des Passwortgebrauchs M 2.22 Hinterlegen des Passwortes M 4.7 Änderung voreingestellter Passwörter M 4.133 Geeignete Auswahl von Authentikationsmechanismen
			x	1	11.4.2 User authentication for external connections	B 4.4 VPN B 4.5 LAN-Anbindung eines IT-Systems über ISDN M 2.7 Vergabe von Zugangs-berechtigungen M 2.220 Richtlinien für die Zugriffs- bzw. Zugangskontrolle M 4.112 Sicherer Betrieb des RAS-Systems
			x	1	11.4.6 Network connection control	B 3.301 Sicherheitsgateway (Firewall) B 4.4 VPN M 2.184 Entwicklung eines RAS-Konzeptes

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz
							M 4.238 Einsatz eines lokalen Paketfilters
				1	11.7.2	Teleworking	M 2.113 Regelungen für Telearbeit M 2.115 Betreuungs- und Wartungskonzept für Telearbeitsplätze M 2.116 Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit M 2.117 Erstellung eines Sicherheitskonzeptes für Telearbeit M 3.21 Sicherheitstechnische Einweisung der Telearbeiter
x				6	12.2.1	Input data validation	M 2.83 Testen von Standardsoftware M 2.363 Schutz gegen SQL-Injection
x				1	12.2.3	Message integrity	M 4.34 Einsatz von Verschlüsselung, Checksummen oder Digitalen Signaturen B 1.7 Kryptokonzept
			x	1	12.3	Cryptographic controls	B 1.7 Kryptokonzept M 2.161 Entwicklung eines Kryptokonzepts
x				1	12.5.1	Change control procedures	M 2.221 Änderungsmanagement M 2.9 Nutzungsverbot nicht freigegebener Hard- und Software M 2.34 Dokumentation der Veränderungen an einem bestehenden System M 2.62 Software-Abnahme- und Freigabe-Verfahren
x				6	12.6.1	Control of technical vulnerabilities	M 2.35 Informationsbeschaffung über Sicherheitslücken des Systems M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und

W	M	J	E	Mx	Quelle ISO 27002		Quelle im IT-Grundschutz	
								Updates
x				7	13.1.1	Reporting information security events	B 1.8 M 3.6 M 6.60	Behandlung von Sicherheits-vorfällen Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern Festlegung von Meldewegen für Sicherheitsvorfälle
x				8	13.2.2	Learning from information security incidents	M 6.66 B 1.8	Nachbereitung von Sicher-heitsvorfällen Behandlung von Sicherheitsvorfällen
			x	1	14.1.1	Including information security in the business continuity management process	B 1.3	Notfallmanagement
x				5	14.1.5	Testing, maintaining and re-assessing business continuity plans	M 6.12 B 1.3 B 1.8	Durchführung von Notfall-übungen Notfallmanagement Behandlung von Sicherheits-vorfällen
			x	3	15.2.1	Compliance with security policies and standards	M 2.199 M 2.182 M 2.193	Aufrechterhaltung der Informationssicherheit Regelmäßige Kontrollen der IT-Sicherheitsmaßnahmen Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit

Tabelle 4 - Gegenüberstellung IT-Grundschutz des BSI und der ISO 27002

Legende: B = Baustein des IT-Grundschutzkataloges, M = Maßnahme des IT-Grundschutzkataloges
Mx = Spaltennummer in der Berechnungsmatrix

Tätigkeiten des IT-SiBe aus dem UP Bund

W	M	J	E	Mx	Quelle	Aufgabenbeschreibung
			x	1	UP Bund, Ziffer 1.1, Seite 5	Einrichtung einer IT-Sicherheitsorganisation mit klaren Zuweisungen von Verantwortlichkeiten innerhalb der Organisation durch die Behördenleitung.
			x	1	UP Bund, Ziffer 1.1, Seite 5	Etablierung eines Informationssicherheitsmanagements (ISMS)
			x	1	UP Bund, Ziffer 1.1, Seite 5	Die IT-Sicherheitsbeauftragten sind aufgrund der Aufgabenübertragung durch die Leitung gegenüber dieser für die IT-Sicherheit in ihrer Behörde verantwortlich
			x	1	UP Bund, Ziffer 1.1, Seite 6	Anwendung der BSI-Standards 100-1 und 100-2 im IT-Sicherheitsmanagement
x				6	UP -Bund, Ziffer 1.1, Seite 6	Gewährleistung der unmittelbaren Berücksichtigung akuter Sicherheitsempfehlungen (insbesondere CERT-Warnungen, Hersteller-Sicherheitsupdates wie Patches) als Teil des Sicherheitsmanagements
			x	8	UP Bund, Ziffer 1.4, Seite 8	Die IT-Sicherheitsbeauftragten der Behörden durchlaufen, möglichst vor Aufnahme ihrer Tätigkeit, ein die Rahmenbedingungen erfüllendes Fortbildungsprogramm
		x		8	UP Bund, Ziffer 1.4, Seite 8	Die IT-Sicherheitsbeauftragten der Behörden besuchen (in der Regel jährliche) Auffrischungskurse oder vergleichbare Veranstaltungen bzw. erwerben Zusatzqualifikationen.
		x		5	UP Bund, Ziffer 1.4, Seite 8	Es werden dem jeweiligen Schutzbedarf angemessene Schulungen der IT-Administratoren und Sensibilisierungen der IT-Nutzer über die sie betreffenden IT-Sicherheitsaufgaben und –maßnahmen durchgeführt.
x				3	UP Bund, Ziffer 2.1, Seite 9	Die Schutzbedarfsanalyse und die Fortschreibungen der kritische IT-gestützte Geschäftsprozesse betreffenden Teile der IT-Sicherheitskonzepte werden in dem jeweiligen Schutzbedarf angemessenen Abständen vorgenommen und wirksam umgesetzt.

W	M	J	E	Mx	Quelle	Aufgabenbeschreibung
x				3	UP Bund, Ziffer 2.2, Seite 9	Anwendung der Technischen Richtlinie des BSI: „Leitfaden für die Auswahl von IT-Sicherheitssystemen für sensible Infrastrukturen“ inklusive Anlagen spätestens im Rahmen der nächsten turnusmäßigen Ersatzbeschaffung
			x	6	UP Bund, Ziffer 2.3, Seite 9	IT-Sicherheitsrevisionen für die kritischen IT-gestützten Geschäftsprozesse werden in der jeweiligen Kritikalität angemessenen Zeitabständen durchgeführt und beinhalten eine der jeweiligen Kritikalität angemessene Suche nach Schwachstellen (Penetrationstest).
		x		1	UP Bund, Ziffer 4.1, Seite 10	Erstellung und Umsetzung von Krypto-konzepten für die behördeninternen IT-Prozesse als ausgewiesener Teil der IT-Sicherheitskonzepte binnen 12 Monaten nach Bereitstellung der Empfehlungen des BSI sowie jährliche Fortschreibung der Konzepte und entsprechende Anpassung der Um-setzungsmaßnahmen
	x			3	UP Bund, Ziffer 4.2, Seite 12	Anwendung der Technischen Richtlinie des BSI „Leitfaden für die Auswahl von IT-Sicherheitssystemen für sensible Infrastrukturen“ nebst Anlagen
	x			3	UP Bund, Ziffer 4.2, Seite 12	Unter Einhaltung der vergaberechtlichen Verpflichtungen und vertragsrechtlichen Bindungen sollen die durch BSI in Zu-sammenarbeit mit dem Beschaffungsamt des BMI geschlossenen Rahmenvereinbarungen genutzt
			x	1 3	UP Bund, Ziffer 5.2, Seite 13	Umsetzung der Nutzerpflichten möglichst binnen 12 Monaten nach ihrer Bereitstellung oder in mit dem BSI abgestimmter angemessener Frist sowie Aufrechterhaltung der Umsetzung im laufenden Betrieb
			x	6	UP Bund, Ziffer 5.2, Seite 13	Unterstützung des BSI durch den IT-SiBe: Das BSI kann, nach Abstimmung von Termin und Umfang mit dem zuständigen Ressort-IT-Sicherheitsbeauftragten sowie dem IT-Sicherheitsbeauftragten der betroffenen Behörde, eine Überprüfung der Einhaltung der Nutzerpflichten in den Behörden durchführen.
			x	6	UP Bund, Ziffer 5.2, Seite 14	Vom BSI festgestellte Mängel bei der Umsetzung der Nutzerpflichten werden innerhalb einer angemessenen Frist behoben.

W	M	J	E	Mx	Quelle	Aufgabenbeschreibung
			x	1	UP Bund, Ziffer 5.3, Seite 14	Definition der Verfügbarkeits- und Vertraulichkeitsanforderungen der identifizierten kritischen Geschäftsprozesse an die genutzten Regierungsnetze und Abstimmung mit dem BSI binnen 12 Monaten nach Verabschiedung des UP Bund
			x	1	UP Bund, Ziffer 5.3, Seite 14	Abstimmung wirtschaftlicher, alternativer Redundanzkommunikationswege mit dem Betreiber des Regierungsnetzes unter Beteiligung des BSI
x				8	UP Bund, Ziffer 6, Seite 14	Frühzeitige Beteiligung der IT-Sicherheitsbeauftragten und, soweit in sicherheitskritischen Bereichen notwendig, Beteiligung des BSI durch die IT-Sicherheitsbeauftragten
x				8	UP Bund, Ziffer 6, Seite 14	Einbeziehung der IT-Sicherheitsaspekte (u.a. Erstellung IT-Sicherheitskonzept / Schutzprofile für sicherheitskritische Komponenten) schon zu Beginn des Konzeptions- und Entwicklungsprozesses
x				7 + 8	UP Bund, Ziffer 7.1, Seite 14	Die Ressorts erklären sich bereit, IT-Sicherheitsvorfälle an das Lage- und Analysezentrum des Bundes zu melden, beginnend binnen 6 Monaten nach Verabschiedung des UP Bund.
x				3	UP Bund, Ziffer 7.1, Seite 16	Beachten der Warnungen des Lage- und Analysezentrums
x				3	UP Bund, Ziffer 7.1, Seite 16	Benennung von Ansprechpartnern für das Lage- und Analysezentrum, insbesondere als Empfänger der Warnungen
			x	1	UP Bund, Ziffer 7.4, Seite 19	Erstellung von IT-Notfallkonzepten binnen 12 Monaten nach Verabschiedung des UP Bund
		x		1	UP Bund, Ziffer 7.4, Seite 19	Die IT-Notfallkonzepte werden durch Fortschreibungen in dem Schutzbedarf angemessenen Abständen aktualisiert und entsprechende IT-Notfallübungen durchgeführt.
		x		6	UP Bund, Ziffer 7.4, Seite 19	Mitwirkung bei behördenübergreifenden Übungen.

Tabelle 5 - Tätigkeiten des IT-SiBe aus dem UP Bund

Legende: B = Baustein des IT-Grundschutzkataloges, M = Maßnahme des IT-Grundschutzkataloges
Mx = Spaltennummer in der Berechnungsmatrix

Tätigkeiten des IT-SiBe aus dem BSI-Gesetz (BSIG)

W	M	J	E	Mx	Quelle	Aufgabenbeschreibung
			x	1	BSIG, § 4	Einrichtung eines hausinternen Meldesystem für Sicherheitsvorfälle
x				7 + 8	BSIG, § 4	Sicherheitsvorfälle an das Krisen- und Lagezentrum des BSI melden
			x	1	BSIG, § 4	Etablierung eines IT-Notfallmanagementsystems
	x			5	BSIG, § 4	Sensibilisierung / Schulung zum Thema „Was ist ein IT-Sicherheitsvorfall ? - wie und an wen ist zu melden?“
			x	1	BSIG § 8 Abs. 1	Rechtliche Grundlage für die Mindest-anforderungen an ein nach UP Bund zu etablierendes ISMS und die damit ver-bundenen Mindesttätigkeiten eines IT-Sicherheitsbeauftragten in einer Bundesbehörde
	x			3	BSIG § 8 Abs. 3	Bedarf an IT-Sicherheitsprodukten nach Vorgaben des BSI beziehen. Aufgabe des IT-Sicherheitsbeauftragten ist es, den jeweiligen Bedarf in seiner Behörde zu ermitteln, sich mit den Vorgaben des BSI zu beschäftigen und den Beschaffungsvorgang zu initiieren.

Tabelle 6 - Tätigkeiten des IT-SiBe aus dem BSI-Gesetz (BSIG)

Legende: B = Baustein des IT-Grundschutzkataloges, M = Maßnahme des IT-Grundschutzkataloges
Mx = Spaltennummer in der Berechnungsmatrix

Zusammenstellung Zeitbedarf Erstellung eines IT-Sicherheitskonzeptes

Thema: „Projektplanung zur Erlangung einer Zertifizierung nach IT-Grundschutz auf der Basis von ISO 27001 für ein IT-Sicherheitskonzept“	Personentage
IT-Strukturanalyse	
Erfassung des IT-Verbundes	3
Netzplanerhebung	3
Erhebung der IT-Systeme	
Aktualisierung der IT-Systeme (Server)	3
Aktualisierung der Netzwerkkomponenten	5
Aktualisierung der IT-Systeme (Handy, Telefonanlage)	2
Aktualisierung der IT-Systeme (Mobiler Client)	0,5
Aktualisierung IT-System PDA	0,5
Aktualisierung IT-System T-Online-PC	0,5
Aktualisierung IT-System Arbeitsplatz PC	0,5
Aktualisierung IT-System Firewall	0,5
Gruppenbildung von Clients	2
Aktualisierung der relevanten IT-Systeme u. Anwendungen	5
Aktualisierung der relevanten IT-Räume	1
Aktualisierung Schutzschränke	0,5
Schutzbedarfsfeststellung	
Aktualisierung Schutzbedarfskategorien	2
Schutzbedarfsfeststellungen IT-Anwendungen	5
Schutzbedarfsfeststellungen IT-Systeme	6
Schutzbedarfsfeststellungen Kommunikationsverbindungen	2
Schutzbedarfsfeststellungen Räume	2
Modellierung	
Modellierung – für jeden Baustein Zielobjekt ermitteln	2
Vormerkung zur ergänzenden Sicherheitsanalyse	0,5
Basissicherheitscheck	
Basissicherheitscheck – B1000 – 1002	2
Basissicherheitscheck – B1003, IT-Notfallkonzept	5
Basissicherheitscheck – B1004, Datensicherungskonzept	1
Basissicherheitscheck – B1006, Virenschutzkonzept	2
Basissicherheitscheck – B1007, Kryptokonzept	3
Basissicherheitscheck – B1011, Outsourcing	1
Basissicherheitscheck – B1012, Archivierung	0,5
Basissicherheitscheck – B1013, Sensibilisierung	3

Basissicherheitscheck – B2001 – 6, Gebäude, Räume usw.	4
Basissicherheitscheck – B2007 – Schutzschrank	1
Basissicherheitscheck – B3001 – 6 – Server, Win	3
Basissicherheitscheck – B3001 – 2 – Server, Unix	2
Basissicherheitscheck – B3201 – Client Win	3
Basissicherheitscheck – B3203– Laptop	1
Basissicherheitscheck – B3204– Client Unix	1
Basissicherheitscheck – B3207– Client Win	2
Basissicherheitscheck – B3208– Internet PC	1
Basissicherheitscheck – B3301– Sicherheitsgateway	1
Basissicherheitscheck – B3302– Router, Switches	3
Basissicherheitscheck – B3404– Handy	0,5
Aktualisierung Netzbausteine	5
Aktualisierung Bausteine IT-Anwendungen	10
Ergänzende Sicherheitsanalyse	
Ergänzende Sicherheitsanalyse - Managementabstimmung für jedes Zielobjekt	3
Risikoanalyse	
Risikoanalyse auf Basis Grundschutz	2
ZW-SUMME der Personentage ohne Zertifizierungsprozess	**106,5**

Basis-Sicherheitscheck II	Personentage
Anstoß noch nicht umgesetzter Maßnahmen	10
Abstimmung IT-Verbund mit dem BSI	2
Ausschreibung	5
Abstimmung mit BSI zu Beantragung Auditor- Testat Aufbau	10
Erstellung Unterlagen Audit-Testat	10
Begleitung des Auditors	15
	ISO-27001-Zertifikat
Anstoß noch nicht umgesetzter Maßnahmen	10
Abstimmung mit BSI zum zertifizierten Verbund	2
Ausschreibung	5
Abstimmung mit BSI zu Beantragung ISO 27001 Zertifikat	10
Unabhängigkeitserklärung vom Auditor einholen	0,5
Erstellung Unterlagen zum Zertifikat	10
Begleitung des Auditors	15
SUMME der Personentage	**211**

Tabelle 7 - Zusammenstellung Zeitbedarf Erstellung eines IT-Sicherheitskonzeptes

Erläuterungen zur Abbildung 4:

Zuschläge für die Anzahl der Mitarbeiter

Nr.	Aktivität	Zuschlag	Verlauf	Begründung für den Zuschlag
01	(Toolunterstützte) Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz)	relativ	linear	Hoher Mehraufwand durch die steigende Anzahl an IT-Komponenten
02	Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI- Standard 100-4	relativ	linear	Mittlerer Mehraufwand durch die steigende Anzahl an IT-Usern
03	Überprüfung und Fortschreibung Sicherheits-konzept, Kryptokonzept	relativ	linear	Mittlerer Mehraufwand durch die steigende Anzahl an IT-Komponenten
04	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept incl. Übungen	relativ	linear	Geringer Mehraufwand durch die steigende Anzahl an IT-Usern
05	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungsaufwand, ohne Schulungsaufwand)	relativ	linear	Hoher Mehraufwand durch die steigende Anzahl an IT-Usern
06	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision	relativ	linear	Mittlerer Mehraufwand durch die steigende Anzahl an IT-Usern
07	Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. der täglichen Sicherheitslage	relativ	linear	Mittlerer Mehraufwand durch die steigende Anzahl an Vorfällen
08	Beratung und Berichterstattung	relativ	linear	Mittlerer Mehraufwand durch die steigende Anzahl an IT-Usern / Vorfällen

Tabelle 8 - Zuschläge für die Anzahl der Mitarbeiter

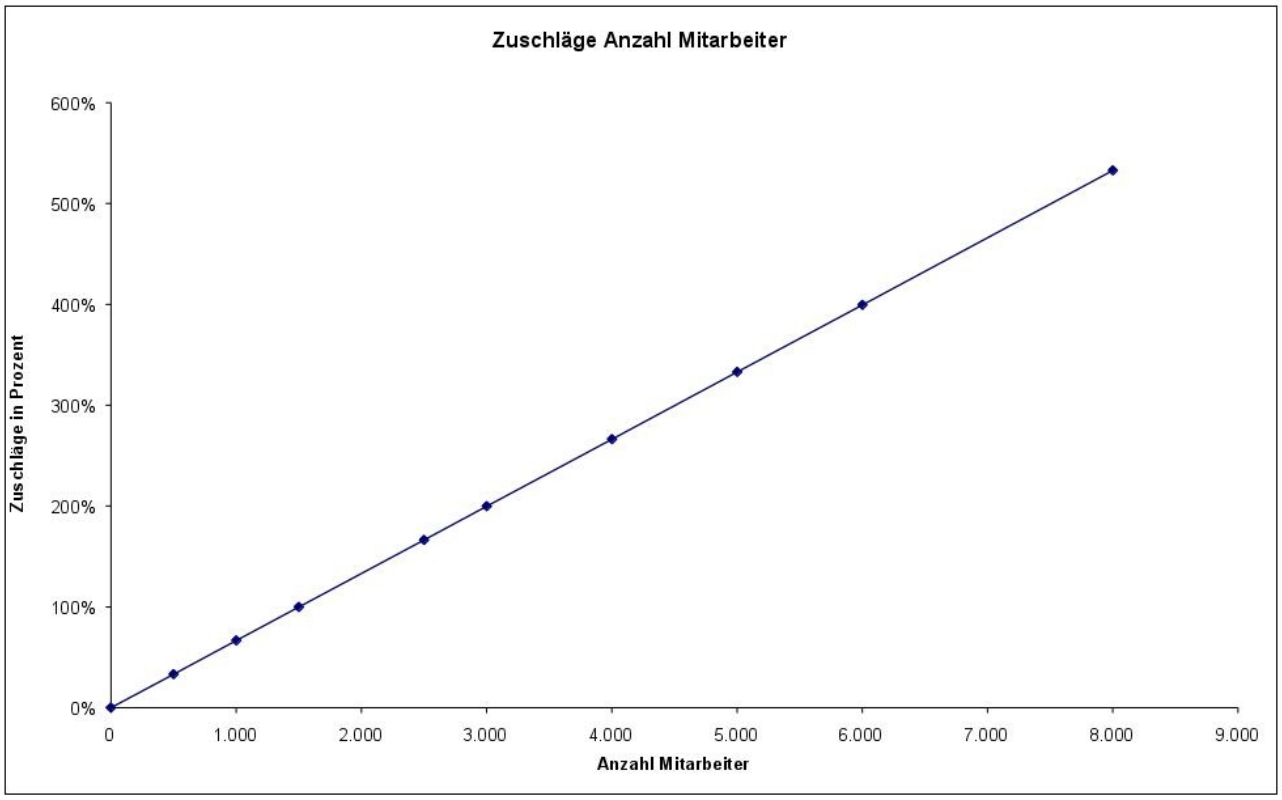

Abbildung 6 - Grafische Darstellung der Zuschläge für die Anzahl der Mitarbeiter

Zuschläge für heterogene IT-Landschaft und IT-Verfahren

Nr.	Aktivität	Zuschlag	Verlauf	Begründung für den Zuschlag
09	(Toolunterstützte) Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz)	30 % pauschal		Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
10	Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI- Standard 100-4	30 % pauschal		Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
11	Überprüfung und Fortschreibung Sicherheitskonzept, Kryptokonzept	30 % pauschal		Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
12	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept incl. Übungen	30 % pauschal		Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
13	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungsaufwand, ohne Schulungsaufwand)	10 % pauschal		Geringer Mehraufwand durch die steigende Anzahl an Gefährdungen
14	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision	20 % pauschal		Mittlerer Mehraufwand durch die steigende Anzahl an Maßnahmen
15	Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. der täglichen Sicherheitslage	20 % pauschal		Mittlerer Mehraufwand durch die steigende Anzahl an Maßnahmen
16	Beratung und Berichterstattung	10 % pauschal		Geringer Mehraufwand durch die steigende Anzahl an Gefährdungen

Tabelle 9 - Zuschläge für heterogene IT-Landschaft und IT-Verfahren

Zuschläge für die Anzahl der Außenstellen

Nr.	Aktivität	Zuschlag	Verlauf	Begründung für den Zuschlag
17	(Toolunterstützte) Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz)	relativ	degressiv	Hoher Mehraufwand durch die steigende Anzahl an Netzwerken / Weitverkehrsanbindungen / Routern / Verzeichnisse usw.
18	Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI- Standard 100-4	relativ	degressiv	Mittlerer Mehraufwand durch die steigende Anzahl an Standorten
19	Überprüfung und Fortschreibung Sicherheitskonzept, Kryptokonzept	relativ	degressiv	Mittlerer Mehraufwand durch die steigende Anzahl an Netzwerken / Weitverkehrsanbindungen / Routern / Verzeichnisse usw.
20	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept incl. Übungen	relativ	degressiv	Geringer Mehraufwand durch die steigende Anzahl an Standorten, Anzahl an Konzepten, Reisezeiten zur Durchführung von IT-Notfallübungen
21	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungsaufwand, ohne Schulungsaufwand)	relativ	degressiv	Hoher Mehraufwand durch die steigende Anzahl an Standorten, Anzahl an Veranstaltungen, Reisezeiten zur Durchführung von Sensibilisierungen
22	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision	relativ	degressiv	Hoher Mehraufwand durch die steigende Anzahl an Standorten, Zunahme der Anzahl der Dienstreisen
23	Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. der täglichen Sicherheitslage	relativ	degressiv	Hoher Mehraufwand durch die steigende Anzahl an Standorten, Zunahme der Anzahl der Dienstreisen
24	Beratung und Berichterstattung	relativ	degressiv	Mittlerer Mehraufwand durch die steigende Anzahl an Standorten

Tabelle 10 - Zuschläge für die Anzahl der Außenstellen

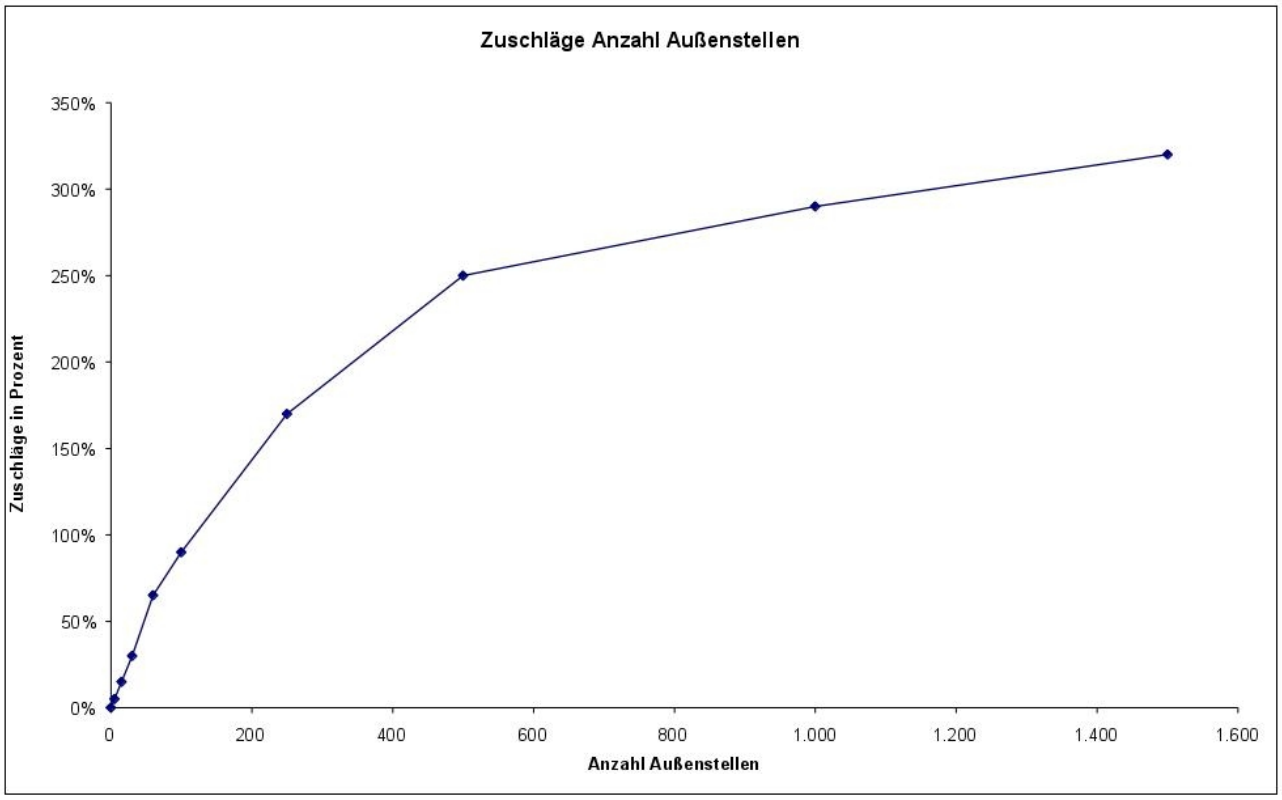

Abbildung 7 - Grafische Darstellung der Zuschläge für die Anzahl der Außenstellen

Zuschläge für den Anteil der IT-Anwendungen mit höherem Schutzbedarf (verhältnismäßig zu allen IT-Anwendungen)

Nr.	Aktivität	Zuschlag	Verlauf	Begründung für den Zuschlag
25	(Toolunterstützte) Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz)	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
26	Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI- Standard 100-4	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
27	Überprüfung und Fortschreibung Sicherheitskonzept, Kryptokonzept	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
28	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept incl. Übungen	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
29	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungsaufwand, ohne Schulungsaufwand)	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Gefährdungen
30	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen
31	Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. der täglichen Sicherheitslage	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Maßnahmen, aufwändigere Untersuchungen, da kritische Geschäftsprozesse
32	Beratung und Berichterstattung	1 % pro Anteil	linear	Hoher Mehraufwand durch die steigende Anzahl an Gefährdungen und die steigende Anzahl an Projektsitzungsteilnahmen durch den IT-SiBe

Tabelle 11 - Zuschläge für den Anteil der IT-Anwendungen mit höherem Schutzbedarf

Zuschläge für Schutzbedarf mit Hochverfügbarkeitsanforderung

Nr.	Aktivität	Zuschlag	Verlauf	Begründung für den Zuschlag
33	(Toolunterstützte) Erstellung Sicherheitskonzept nach BSI-Standard 100-2 und 100-3 (IT-Grundschutz)			Keine Korrelation
34	Erstellung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept, BSI- Standard 100-4	50 % pauschal		Mehraufwand zur Erstellung der Notfall- und Krisenmanagementkonzepte
35	Überprüfung und Fortschreibung Sicherheitskonzept, Kryptokonzept			Keine Korrelation
36	Überprüfung und Fortschreibung IT-Notfallvorsorgekonzept sowie IT-Notfall- und Krisenmanagementkonzept incl. Übungen	50 % pauschal		Mehraufwand zur Erstellung der IT-Notfall- und Krisenmanagementkonzepte
37	Sensibilisierung der Mitarbeiter (ausschließlich Koordinierungsaufwand, ohne Schulungsaufwand)			Keine Korrelation
38	Kontrolle der Wirksamkeit von Sicherheitsmaßnahmen, Audits, Revision			Keine Korrelation
39	Untersuchung sicherheitsrelevanter Vorfälle, aktuell halten bzgl. der täglichen Sicherheitslage			Keine Korrelation
40	Beratung und Berichterstattung			Keine Korrelation

Tabelle 12 - Zuschläge für Schutzbedarf mit Hochverfügbarkeitsanforderung

Literatur- und Quellenverzeichnis

[1] BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[2] BSI-Standard 100-2: IT-Grundschutz Vorgehensweise
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[3] BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[4] Handbuch für Organisationsuntersuchungen und Personalbedarfsermittlung des Bundesministerium des Innern,
http:/www.orghandbuch.de

[5] Nationaler Plan zum Schutz der Informationsinfrastruktur in Deutschland – Umsetzungsplan Bund (UP Bund, Verschlusssache)

[6] Nationaler Plan zum Schutz der Informationsinfrastrukturen mit strategischen Zielen „Prävention, Reaktion und Nachhaltigkeit“ mittels konkreter Maßnahmen und Empfehlungen (UP KRITIS)
https://www.bsi.bund.de/ContentBSI/Themen/Kritis/Umsetzungsplan/umsetzungsplan.htmll

[7] BSI-Leitfaden IS-Revision
https://www.bsi.bund.de/cln_165/ContentBSI/Themen/IS-Revision/Leitfaden/leitfaden.html

[8] Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009,
https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html

[9] Musterkryptokonzept des BSI
https://www.bsi.bund.de/cae/servlet/contentblob/1001616/publicationFile/63745/2010-04-28_Musterkryptokonzept_V12_pdf

[10] Erstellung eines Notfallkonzeptes
https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf
-> Seite 4004, M 6.114 (Stand: 12. Ergänzungslieferung der IT-Grundschutz-Kataloge)

[11] Projektarbeit „Projektplanung zur Erlangung einer Zertifizierung nach IT-Grundschutz für das IT-Sicherheitskonzept des BMI“, Frau Anke Otto, BMI, Referat Z6 (ProjA_ITSiKo.pdf, Verschluss-sache)

[12] Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)
http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf

[13] Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung) vom 31. März 2006
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSA_pdf.pdf

[14] Rechtliche Grundlagen der IT-Sicherheit, Jens Eckhardt, Aufsatz
JURIS DuD 2008, 330-336

[15] Gesetz zum Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zu-sammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern –Vertrag zur Ausführung von Artikel 91c Grundgesetz (GG)
BGBl Teil I 2010 Nr. 26 vom 02.06.2010
http://www.bgbl.de/Xaver/start.xav?startbk=Bundesanzeiger_BGBl
->Teil I -> 2010 -> Nr. 26 vom 02.06.20212

[16] Liste der durch das BSI zertifizierten IT-Grundschutz-Auditoren
https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzZertifikat/Veroeffentlichungen/ISO27001Auditoren/iso27001auditoren_node.html

[17] Hochverfügbarkeitskompendium des BSI
https://www.bsi.bund.de/ContentBSI/Themen/Hochverfuegbarkeit/HVKompendium/hvkompendium.html

[18] BSI-Standard 100-4: Notfallmanagement
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

[19] IT-Grundschutz-Kataloge des BSI, 12. Ergänzungslieferung
https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf

[20] Strafgesetzbuch
http://dejure.org/gesetze/StGB

Abkürzungsverzeichnis

BAköV	Bundesakademie für öffentliche Verwaltung
BNetzA	Bundesnetzagentur
BRH	Bundesrechnungshof
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz)
CC	Common Criteria
CoBIT	Control Objectives for Information and Related Technology
GG	Grundgesetz
GS	IT-Grundschutz
GSB	Geheimschutzbeauftragter
IS	Informationssicherheit
ISMS	Informationssicherheitsmanagementsystem
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
IT-SiBe	IT-Sicherheitsbeauftragter
PT	Personentage
SLA	Service Level Agreement
StGB	Strafgesetzbuch
UP Bund	Umsetzungsplan Bund
UP KRITIS	Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsstrukturen
VSA	Allgemeine Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung) vom 31. März 2006