Bundesministerium des Innern, für Bau und Heimat

Bundesamt für Sicherheit in der Informationstechnik

Lernpfad

Informationssicherheitsmanagement in der öffentlichen Verwaltung

Fortbildungsangebot der BAköV in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik

Brühl / Rheinland Dezember 2021
Version 1.0

Dieser Lernpfad wurde von der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat (BAköV) gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellt. Er ersetzt den bis 2021 verwendeten Leitfaden „Informationssicherheit in der öffentlichen Verwaltung“. Die Inhalte dieses Lernpfads dürfen ausschließlich in Absprache mit der BAköV verwendet werden.

Herausgeber:

Bundesakademie für öffentliche Verwaltung
im Bundesministerium des Innern, für Bau und Heimat
Willy-Brandt-Str. 1
50321 Brühl

Telefon: 0228 / 99 629-0
02232 / 929-0

E-Mail: poststelle@bakoev.bund.de

Internet: https://www.bakoev.bund.de
https://www.ifosbund.de
https://lernplattform.intranet.bund.de
https://digitalakademie.bund.de

Inhaltsverzeichnis

1 Warum eine systematische Qualifizierung in der Informationssicherheit wichtig ist und wie Sie Ihren eigenen Lernpfad finden

Die Informationssicherheit der öffentlichen Verwaltung ist von einer ständig veränderten und anhalten Bedrohungslage betroffen. Die Gewährleistung von effektiver Informationssicherheit geht zudem mit steigenden Praxisanforderungen einher, was nicht zuletzt durch die voranschreitende behördliche Digitalisierung geprägt ist. Denn in den meisten Fällen werden bei Digitalisierungsmaßnahmen Prozesse geschaffen, die eine Sicherheitsbewertung erfordern. Ohne systematische Qualifizierung, die auch die Besonderheiten in der öffentlichen Verwaltung im Blick hat, ist es schwer, diesen Herausforderungen zu begegnen.

Um die oft komplexen Fragen angemessen beantworten zu können, sind neben technischen und juristischen Kenntnissen verstärkt Managementkompetenzen gefragt. Zahlreiche Berührungen zu angrenzenden Fachgebieten wie dem Datenschutz und dem Geheimschutz haben das Anforderungsprofil im behördlichen Informationssicherheitsmanagement (ISM) genauso komplex werden lassen wie die Informationssicherheit selbst.

Die im behördlichen ISM beschäftigten Kolleginnen und Kollegen – allen voran die IT-Sicherheitsbeauftragten - weisen in der Regel sehr unterschiedliche Qualifikationen vor. Informatikerinnen und Informatiker, Physikerinnen und Physiker, Volljuristinnen und Volljuristen sowie Verwaltungswirtinnen und Verwaltungswirte sind ebenso vertreten wie Beschäftigte mit weiteren Hintergründen wie den Wirtschaftswissenschaften oder den Sozialwissenschaften. Nicht selten fehlt den Juristinnen und Juristen oder den Verwaltungswirtinnen und Verwaltungswirten das technische Know-How. IT-Beschäftigten fehlen hingegen oft die rechtlichen Aspekte der Informationssicherheit. Einige haben einen ausgeprägten Verwaltungsbezug, öfter aber auch Erfahrungen aus der Privatwirtschaft. Es gibt Beschäftigte mit langjähriger Erfahrung in der Bundesverwaltung, aber außerhalb des behördlichen ISM. Demgegenüber haben neue Beschäftigte in der Bundesverwaltung hin und wieder schon wichtige Sicherheitserfahrungen in der Privatwirtschaft sammeln können. Die Qualifikationslage im behördlichen ISM ist damit sehr heterogen und es gilt, Standardkompetenzen zu vermitteln, damit die behördliche Informationssicherheit in der Bundesverwaltung ein möglichst einheitlich hohes Niveau erreichen kann.

Um diesem Auftrag gerecht zu werden, hat die Bundesakademie unter Mitwirkung von Kolleginnen und Kollegen des BSI im Jahr 2021 einen praxis- und bedarfsorientierten **Lernpfad für Informationssicherheitsma-**

nagement in der öffentlichen Verwaltung entwickelt. Der Lernpfadentwicklung ging mit einer Modernisierung des Fortbildungsangebots der BAköV einher, die die Aspekte Hybridisierung der Lernformate, Digitalisierung, Modularisierung, Nachhaltigkeit und Flexibilisierung zum Gegenstand hatte. Auf Basis moderner methodisch-didaktischer Erkenntnisse und unter Berücksichtigung digitaler Lernformate haben wir ein Gesamtkonzept entwickelt, das in seinen jeweiligen modularen Bausteinen eine nachhaltige Maximierung des Lernerfolgs verspricht. Dabei berücksichtigen wir die äußerst heterogenen Ausgangslagen in puncto individueller Qualifikation und individuellem Fortbildungsbedarf. Dies ermöglicht je nach persönlicher Situation einen individuellen Einstieg in den Lernpfad und damit eine eigene „Lernreise“ durch die Informationssicherheit.

Für alle Ebenen sehen wir Angebote vor: Für Einsteigende, Erfahrene und Fortgeschrittene. Die Nachhaltigkeit des Lernerfolgs gewährleisten wir durch verschiedene Angebote zur Vertiefung und zum Erfahrungsaustausch, aber nicht zuletzt durch unser Zertifikat „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“.

Jede Beschäftigte und jeder Beschäftigte kann quasi so lange auf ihrem bzw. seinen Lernpfad unterwegs sein, wie es der jeweilige Fortbildungsbedarf erfordert. Die digitalen Formate ermöglichen uns zudem, Kolleginnen und Kollegen zu adressieren, denen z. B. aus Gründen familiärer Verpflichtungen eine Präsenzveranstaltung in der Vergangenheit nicht möglich war. Wo aus methodischen und didaktischen Gründen der Mehrwert von Präsenzen indes größer ist, haben wir diesen Aspekt beispielsweise in Erfahrungsaustauschen gestärkt. So konnten wir einen Lernpfad entwickeln, auf dem für jede und jeden etwas dabei ist.

Für dieses Angebot haben wir neben unseren langjährigen Fortbildungserfahrungen im Bereich der Informationssicherheit auch Anregungen aus dem Kreis der Teilnehmenden unserer Veranstaltungen berücksichtigt. Allen, die insofern mitgewirkt haben,– allen voran den Kolleginnen und Kollegen aus dem BSI – möchten wir an dieser Stelle herzlich danken. Denn Fortbildung ist keine Einbahnstraße. Sie lebt vom gemeinsamen Erfahrungsaustausch und kann sich so stetig weiterentwickeln, genauso wie wir gemeinsam den hier vorliegenden Lernpfad stetig weiterentwickeln werden. Wir freuen uns, Sie damit auf ihrem individuellen „Sicherheitsweg“ begleiten zu können. Gerne beraten wir Sie, um den für Sie richtigen Weg zu finden. Sprechen Sie uns einfach an! Die jeweils aktuelle Version des Lernpfads ist unter www.bakoev.bund.de veröffentlicht.

Wir wünschen Ihnen viel Freude auf Ihrem Lernpfad – Ihre Lehrgruppe 5

2 Ziele

Anliegen dieses Lernpfades ist es, Beschäftigte der Bundesverwaltung:

- in den relevanten Bereichen der Informationssicherheit nachhaltig zu sensibilisieren und fortzubilden;
- für die Tätigkeiten als IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung zu befähigen, zu zertifizieren und permanent fortzubilden.

Das Fortbildungsangebot richtet sich in erster Linie an Beschäftigte der Bundesverwaltung. Beschäftigte aus Ländern und Kommunen können als Gäste nach den Teilnahmebedingungen der BAköV teilnehmen.

3 Anforderungsprofile

Die Anforderungsprofile für die öffentliche Verwaltung sind je nach Tätigkeit unterschiedlich und können spezifische Ausprägungen haben. Dies berücksichtigend basiert der Lernpfad auf folgendem gestuften Anforderungskonzept:

3.1 Einstieg: Basiskompetenzen (Basissensibilisierung)

Alle Bundesbeschäftigen müssen grundsätzlich über allgemeine Basiskompetenzen verfügen, um in Zusammenhängen der Informationssicherheit möglichst souverän agieren zu können. Dies umfasst im Wesentlichen folgende Aspekte:

- Bedeutung der Informationssicherheit,
- Kenntnis der allgemeinen Rechtsgrundlagen der EU-DSGVO und des BDSG, Vorgaben und Handlungsempfehlungen des BSI und deren Praxisbezug,
- Erkennen personenbezogener Daten und darüberhinausgehender behördlicher Informationen,
- Rechte betroffener Personen,
- Rollenverständnis zu Informationssicherheitsbeauftragten, Datenschutzbeauftragten, Verantwortlichkeit und Auftragsverarbeitung,
- Erkennen von potentiellen Risiken,
- Kennen von geeigneten technischen und organisatorischen Maßnahmen zur Prävention und Abwehr von Risiken,
- Grundkenntnisse über Meldeprozesse.

3.2 Nächster Schritt: Vertiefung und Aufbaukompetenzen

Je nach behördlicher Funktion sind vertiefende oder aufbauende Kompetenzen erforderlich, um das behördliche Sicherheitsniveau zu steigern. Hierzu zählen im Wesentlichen:

- Ausgeprägtere Kenntnis der wesentlichen Rechtsgrundlagen, u. a. auch Einblicke in Grundschutzfragen.
- Anwendung wichtiger technischer und organisatorischer Sicherheitsmaßnahmen.
- Grundkenntnisse Risikobewertung.
- Kenntnis und Anwendung von Meldeprozessen.

3.3 Spezialkompetenzen

Einige Bundesbeschäftige müssen über vertiefte funktionale Spezialkompetenzen verfügen, um in komplexen Zusammenhängen der Informationssicherheit, souverän agieren zu können, u.a.

- Organisation (z.B. Prozessmanagement)
- Innerer Dienst (z.B. Gebäudeaspekte, Beschaffungen)
- IT-Beschäftigte (z.B. Administration)
- Digitalisierungsbeauftragte (z.B. digitale Strategien)
- Datenschutzbeauftragte (z.B. juristische Kenntnisse)

3.4 IT-Sicherheitsbeauftragte

Der Umsetzungsplan Bund 2017, hieraus abgeleitet die BSI-Standards der 200er-Reihe und der BSI-Grundschutz fordern von IT-Sicherheitsbeauftragten ein hohes Maß an Fachwissen, insbesondere in den Bereichen der technischen und organisatorischen Informationssicherheit, der Grundschutz-Methodik sowie Management-/Kommunikationskompetenzen. Dies betrifft alle Bereiche der behördlichen Informationssicherheit, damit IT-Sicherheitsbeauftragte ihren Beratungs- und Überwachungsaufgaben entsprechen können. Die Kompetenzanforderungen erreichen hier ein sehr hohes Niveau, das auch Spezialwissen umfasst.

Diese zuvor genannten Anforderungsprofile finden ihren Niederschlag im Angebot der BAköV.

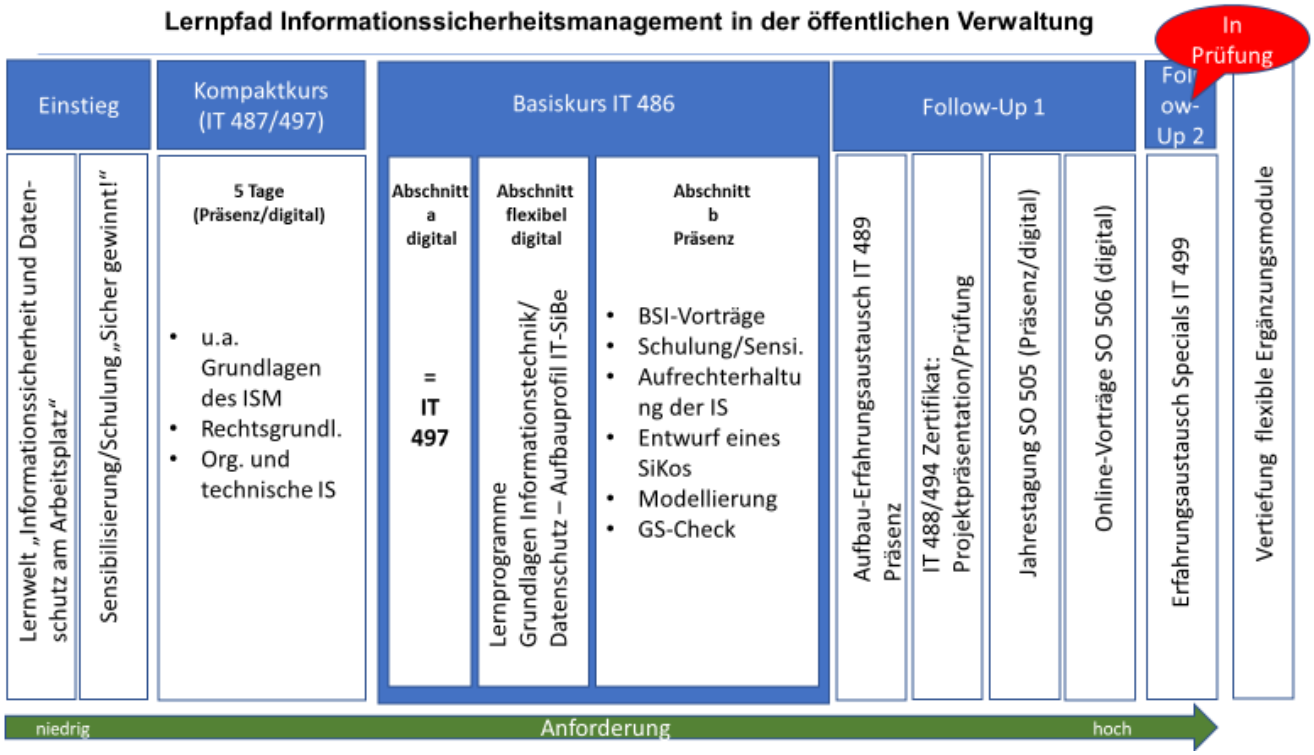
4 Überblick zum Lernpfad

Dieser Lernpfad geht davon aus, dass die Aufgaben in relevanten Bereichen der Informationssicherheit innerhalb der öffentlichen Verwaltung vielfältig sind und dass Tätigkeiten laufbahnübergreifend wahrgenommen

werden. Ebenfalls wird berücksichtigt, dass hinsichtlich des Wissensstandes, des Aufgabenfeldes bzw. zukünftigen Einsatzgebietes sowie der Erfahrungen unterschiedliche Voraussetzungen eingebracht werden.

Die Gestaltung der Fortbildung muss deshalb flexibel sein und den individuellen Vorkenntnissen, Berufserfahrungen und Aufgabenfeldern Rechnung tragen. Daher ist das Fortbildungsangebot modular und flexibel aufgebaut. Wir ermöglichen Ihnen damit das Erstellen eines individuellen Lernpfads (Auswahl der zu besuchenden Veranstaltungen).

Für die Entscheidung über den individuellen Fortbildungsweg besteht die Möglichkeit, sich von der BAköV in einem Interview beraten zu lassen. Die BAköV stellt auch einen Selbsteinschätzungstest im Fortbildungsportal des Bundes zur Verfügung. Eine Gesamtübersicht zum Lernpfad können Sie der nachstehenden Übersicht entnehmen:



Der Lernpfad ist so aufgebaut, dass Sie je nach eigener Qualifikation auf allen Anforderungsebenen flexibel einsteigen können. Niemand „muss“ alle Ebenen absolvieren. Weitere Informationen zu den JAP-Nummern (z.B. IT 486) finden Sie in IFOS Bund (www.ifosbund.de). Nachstehend erläutern wir Ihnen die verschiedenen Ebenen des Lernpfads:

4.1 Einstieg Basissensibilisierung

Zum Einstieg in das Thema „Informationssicherheitsmanagement in der öffentlichen Verwaltung“ und zu Erlangung erster Basiskenntnisse empfehlen wir neben der Lernwelt „Informationssicherheit und Datenschutz am Arbeitsplatz“ (IDAP) im Fortbildungsportal des Bundes den Besuch von Seminaren und Webinaren aus dem Rahmenvertrag „Sicher gewinnt!“. Beide Elemente haben das Ziel, erste Grundlagen für die praxiskonforme Anwendung der Informationssicherheit zu entwickeln. Die Inhalte können zielgruppenspezifisch adressiert werden (u.a. IT-Beschäftigte, Führungskräfte)

1	Lernwelt „Informationssicherheit und Datenschutz am Arbeitsplatz“	**Online**	**120 Min**
2	Seminare/Webinare der Initiative Sicher gewinnt! zur Basissensibilisierung	**Online**	**180 Min**

4.2 Vertiefung von Grundlagen

Vertiefte Grundkenntnisse können mit dem 5-tägigen Kurs „Informationssicherheit in der öffentlichen Verwaltung – Basis kompakt“ – IT 487 (Präsenz) und IT 497 (inhaltsgleich, aber digital) ausgeprägt werden. Die inhaltlichen Module können Sie der nachstehenden Übersicht entnehmen.

Modul	Inhalt	Format	Tag
1	**Grundlagen der Informationssicherheit** • Rolle und Aufgaben des Informations-/ IT-Sicherheitsbeauftragten • Grundbegriffe der Informationssicherheit • Bedrohungen / Gefährdungen • Abgrenzung Informationssicherheit zum Datenschutz • Die Dienstleistungen des Bundesamtes für Sicherheit in der Informationstechnik	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**1**
2	**Rechtliche Rahmenbedingungen** • IT-Sicherheitsgesetz 2.0 • EU-DSGVO und BDSG • Geheimschutz • Urheberrecht • Haftungsrecht (inkl. Fehlermanagement)	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**1**

BSI	IT-Sicherheitsbeauftragte - Partner der Geheimschutzbeauftragten (120 Min. inkl. Q&A)	**Online-Vortrag**	**2**
BSI	IT-Konsolidierung - IT-Sicherheit (90 Min. inkl. Q&A)	**Online-Vortrag**	**2**
3	**Grundlagen des Informationssicherheitsmanagements (ISMS)** • Standards und Normen im Überblick (ISO 2700x, ITIL, ISO 20000, COBIT) • BSI-Standards zur Informationssicherheit 200-1, 200-2, 200-3, 200-4 • Mindeststandards des BSI (das Thema Mindeststandards wird im Übrigen durchgehend, zugehörig zu den Bausteinen behandelt) • Informationssicherheitsorganisation in Behörden • Einordnung der ISMS-Organisation einer Behörde in die Sicherheitsstrukturen der öffentlichen Verwaltung • Entwicklung und Stellenwert einer Leitlinie zur Informationssicherheit	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen** **Übung in Gruppen** **Vorstellung/Besprechung**	**2** **3**
BSI	Forensische Aspekte und Maßnahmen bei infizierten Rechnersystemen (60 Min. inkl. Q&A)	**Online-Vortrag**	**3**
4	**Grundlagen Organisatorische Informationssicherheit** **Schulung und Sensibilisierung, u.a.** • Entwicklung von Schulungs- und Sensibilisierungskonzepten • Schulungsinhalte	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**3**
5	**Grundlagen Zugangs- und Zugriffsschutz** **Organisatorische Informationssicherheit** • Datensicherungskonzept • Sichere Cloud-Nutzung • Software- und APP-Management • Schutz vor Schwachstellen und Schadsoftware	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**4**
6	**Grundlagen Organisatorische und technische Informationssicherheit** • Notfallmanagement und Behandeln von Sicherheitsvorfällen	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen**	**5**

	• Virtualisierung • Betrieb von Netzkomponenten • Mobile Geräte • Verschlüsselung und Elektronische Signatur		
BSI	Informationssicherheitsprodukte des BSI (60 Minuten inkl. Q&A)	**Online-Vortrag**	**5**

4.3 IT-Sicherheitsbeauftragte und Beschäftigte ISMS

Für IT-Sicherheitsbeauftragte und Beschäftigte im behördlichen Informationssicherheitsmanagement, die über ein hohes Maß an Kompetenzen in der Informationssicherheit verfügen müssen, bieten wir den Kurs „Informationssicherheitsmanagement in der öffentlichen Verwaltung“ – IT 486 an. Letztlich geht es bei diesen Zielgruppen auch um die Ausprägung von Managementkompetenzen, was den Titel des Kurses ausmacht.

Inhaltlicher Gegenstand des Kurses ist das Handbuch „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“, dass die BAköV in Zusammenarbeit mit dem BSI seit vielen Jahren anbietet, stetig aktualisiert und den Teilnehmenden zur Verfügung stellt. Die Inhalte des Handbuchs sind Gegenstand der Zertifizierungsprüfung (vgl. Ziff. 6.4). Aus diesem Grund wird der Kurs Zertifikatsinteressierten empfohlen.

Der in seinen Lernformaten „hybride“ IT 486 besteht aus drei Teilen, die flexibel belegt werden können:

- Webinar: Informationssicherheit in der öffentlichen Verwaltung – Basis kompakt (= IT 497) – Abschnitt a
- Lernprogramme „Informationstechnik“ und „Datenschutz in der öffentlichen Verwaltung - Aufbauprofil für IT-SiBe“ (Fortbildungsportal des Bundes) – Flexible unverbindliche Selbstlernphase
- Informationssicherheitsmanagement in der öffentlichen Verwaltung – Abschnitt b.

Die inhaltlichen Module können Sie der nachstehenden Übersicht entnehmen.

4.3.1 Webinar: Informationssicherheit in der öffentlichen Verwaltung (= IT 497) – Abschnitt a

Zur Vermeidung von Wiederholungen sei an dieser Stelle auf die Inhalte oben zum IT 487/ IT 497 verwiesen. Dieser Kurs wird im ersten Abschnitt des IT 486 inhaltsgleich, allerdings im digitalen Format angeboten. Damit

möchten wir die Attraktivität des Gesamtkurses steigern. Interessierte Beschäftigte müssen nicht – wie noch vor 2022 – drei komplette Wochen vom Dienstort weg. Das digitale Format erhöht an dieser Stelle die Flexibilität wesentlich.

Der Kurs hat das Ziel, Grundlagen zu entwickeln oder vorhandenes Wissen aufzufrischen. Der Kurs bietet sich daher auch für Beschäftigte, die schon vor einigen Jahren mit Themen der Informationssicherheit zu tun hatten, deren Grundkenntnisse aber z.B. nach Rechtsänderungen nicht mehr aktuell sind.

Ziele: Entwicklung von Grundlagen oder Auffrischung vorhandener Kenntnisse

4.3.2 Lernprogramme „Informationstechnik“ und „Datenschutz in der öffentlichen Verwaltung – Aufbau für IT-SiBe“ (Fortbildungsportal des Bundes)

Auch die zweite Woche des IT 486 findet online statt, was die Flexibilität des Gesamtkurses um einen weiteren Baustein erhöht. Diese Woche ist allerdings unverbindlich und kann flexibel zum Selbststudium genutzt werden. Sie kann nicht über IFOS gebucht werden. Interessierte Beschäftigte können in dieser zweiten Woche je nach Lernbedarf zwei Lernprogramme im Fortbildungsportal des Bundes im Rahmen einer freien Selbstlernphase absolvieren. Das Lernprogramm „Informationstechnik“ adressiert Beschäftigte, die bislang über wenig technisches Know-How verfügen. Die Ziele der zweiten Woche sind die Lernvertiefung und Lernergänzung der Grundlagenthemen aus dem ersten Abschnitt. Je nach Bedarf können einzelne Module oder das ganze Programm absolviert werden. Beschäftigten (u.a. aus Ländern und Kommunen), die keinen Zugang zum Fortbildungsportal des Bundes haben, wird das Selbststudium mit dem Handbuch empfohlen. Auch Bundesbeschäftigte können je nach Bedarf hiervon Gebrauch machen.

Ziele: Vertiefung der Lerninhalte (Empfehlung für behördliche IT-Sicherheitsbeauftragte und Beschäftigte im behördlichen Informationssicherheitsmanagement)

Modul	Inhalt	Format	Tag
1	Lernprogramm Grundlagen Informationstechnik	**Online; Selbstlernphase**	**1 – 5, je nach Bedarf**
2	Lernprogramm Datenschutz in der öffentlichen Verwaltung – Aufbaumodul	**Online; Selbstlernphase**	**2**
3	Handbuch	**Selbstlernphase**	**3**

4.3.3 Informationssicherheitsmanagement in der öffentlichen Verwaltung – Abschnitt b

Der dritte Abschnitt (=Abschnitt b in IFOS) stellt einen wichtigen Praxisbaustein dar. Hier geht es darum, dass Ihre theoretischen Kenntnisse in der behördlichen Praxis angewandt werden. Dieser Abschnitt wendet sich in erster Linie an IT-Sicherheitsbeauftragte und Beschäftigte im behördlichen Informationssicherheitsmanagement, die das Zertifikat „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ anstreben. Aber auch Beschäftigte, die dieses Ziel nicht haben, können sich in diesem Abschnitt den „Praxisschliff“ holen. Die Grundlagenkenntnisse werden in jedem Fall vorausgesetzt, damit – von Ausnahmen abgesehen – die Zeit effektiv für die Erarbeitung praxiskonformer Ergebnisse genutzt werden kann. Wir sind der Meinung, dass dieser Abschnitt in Präsenz stattfinden sollte, damit auch der Erfahrungsaustausch neben dem gemeinsamen Entwickeln von Praxishilfen optimiert wird. Die Inhalte dieses Abschnitts können Sie der nachfolgenden Übersicht entnehmen.

Ziele: Praxisvertiefung für behördliche IT-Sicherheitsbeauftragte und Beschäftigte im behördlichen Informationssicherheitsmanagement

Modul	Inhalt	Format	Tag
BSI	Das Bundesamt für Sicherheit in der Informationstechnik – sowie Aufgaben eines IT-SiBe aus dem UP-Bund	**Vortrag**	**1**
1	**Aufrechterhaltung der Informationssicherheit** • Informationssicherheitsrevision, Cyber-Sicherheits-Check, Penetrationstests • Informationsfluss und Wissensmanagement im Informationssicherheitsprozess • Sachstandserhebung nach UP Bund 2017	**Vortrag mit Praxisbeispielen und interaktiven Praxisfragen** **Übung in Gruppen** **Vorstellung/Besprechung**	**1**
BSI	Mindeststandards des BSI (60 Min. inkl. Q&A)	**Vortrag**	**2**
2	**Vertiefung Organisatorische Informationssicherheit** **Schulung und Sensibilisierung, u.a.** • Beispiel einer Sensibilisierungskampagne	**Workshop**	**2**
3	**Vertiefung Zugangs- und Zugriffsschutz** **Organisatorische Informationssicherheit** • Datensicherungskonzept • Sichere Cloud-Nutzung • Software- und APP-Management • Schutz vor Schwachstellen und Schadsoftware	**Übungen in Gruppen** **Vorstellung/Besprechung**	**2**

4	**Vertiefung Organisatorische und technische Informationssicherheit** • Notfallmanagement und Behandeln von Sicherheitsvorfällen • Virtualisierung • Betrieb von Netzkomponenten • Mobile Geräte • Verschlüsselung und Elektronische Signatur	**Workshop**	**3**
5	**Gemeinsame Übung Informationssicherheit/Datenschutz) zur Protokollierung und zur Datensicherung unter ständiger Anleitung**	**Workshop** **Besprechung**	**3** **3**
BSI	IT-Lagezentrum / CERT-Bund – Vorstellung von Aufgaben / Dienstleistungen (60 Min. inkl. Q&A)	**Vortrag**	**4**
BSI	Behördennetze/Sicherheit Netze des Bundes (60 Min. inkl. Q&A)	**Vortrag**	**4**
6	**Entwurf eines Sicherheitskonzepts nach IT-Grundschutz, u.a.** • Einführung in die Methodik • Basis-, Kern-, Standardabsicherung • Aufbau des Kompendiums • Strukturanalyse • Schutzbedarfsfeststellung **Modellierung** • Auswahl der Bausteine • Ermitteln von Anforderungen • Entwickeln von Umsetzungshinweisen **IT- Grundschutz-Check** • Risikoanalyse • Realisierungsplan • Zertifizierung	**Vortrag zum Überblick** **Workshop mit Übungsfall zur Entwicklung einer Sicherheitskonzeption mit dem Schwerpunkt Risikoabwägung** **Vorstellung und Besprechung**	**4** **4** **5**
BSI/LG5	**Hinweise zur Erstellung der Projektarbeit und zur Zertifizierung als Informationssicherheits-Beauftragte/r**	**Online-Vortrag**	**5**

4.4 Follow-Up 1: Nachhaltigkeit des Lernerfolgs

Um die Nachhaltigkeit des Lernerfolgs zu steigern, sieht unser Lernpfad im Anschluss an die Basis-Qualifizierung verschiedene Etappen zur Lernvertiefung, zum Erfahrungsaustausch und dem Ausbau von Basiskompetenzen vor. Diese Etappen sind im Wesentlichen durch verschiedene Erfahrungsaustausche – allen voran jährlich stattfindende Jahrestagung der IT-Sicherheitsbeauftragten in der Bundesverwaltung – sowie die Projektpräsentation und Prüfung zum Erwerb des Zertifikats „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ geprägt. Auch hier gilt das Flexibilisierungsprinzip: Alles kann - nichts muss! Für IT-Sicherheitsbeauftragte ist das Zertifikat zudem ein ausgezeichneter Beleg für das erforderliche

Fachwissen, das der Umsetzungsplan Bund 2017 fordert: (vgl. UP Bund 2017 Kapitel 4.1, S. 14):

„Die mit der Basisfortbildung erreichte Qualifikation soll durch den Erwerb des Zertifikats „IT-Sicherheitsbeauftragte/r in der öffentlichen Verwaltung“ nachgewiesen werden.“

Weitere Bausteine dieses Follow-Ups zur Basisqualifizierung sind anlassbezogene Online-Vorträge, um der thematischen Aktualität Rechnung zu tragen, sowie im IT 489 ein Erfahrungsaustausch für Teilnehmende des IT 486. Dieser Austausch hat das Ziel, dass die Teilnehmenden des IT 486 noch einmal in der gleichen Zusammensetzung zusammenkommen, um sich über ihre praktischen Erfahrungen im Anschluss an die Basisqualifizierung auszutauschen. Hiermit entsprechen wir einem Wunsch aus dem Kreis unserer Teilnehmenden. Freuen Sie sich auf ein Wiedersehen, denn so macht Lernen noch mehr Spaß! Der nachfolgenden Übersicht können Sie noch einmal alle Bausteine dieses ersten Follow-Ups entnehmen.

Modul	Inhalt	Format	Tag
	Erfahrungsaustausch IT 489 (ca. 6 Monate später, nur für TN IT 486) Vertiefungsthemen: Mindeststandards, BSI-Grundschutz, Datensicherheit, Sicherheitskonzeption, Aktuelles, aktiver Austausch zwischen Teilnehmenden	2 Tage in Präsenz	**1-2**
2	**Zertifikat: Projektpräsentation/Prüfung IT 488/IT 494**		**1-2**
3	**Jahrestagung SO 505**	(Präsenz/digital)	**1-2**
4	**Online-Vorträge SO 506** aus dem BSI zu aktuellen Themen	Online 90 Min	

Ausführlichere Hinweise zur Zertifizierung haben wir Ihnen unter Ziff. 6 zusammengestellt.

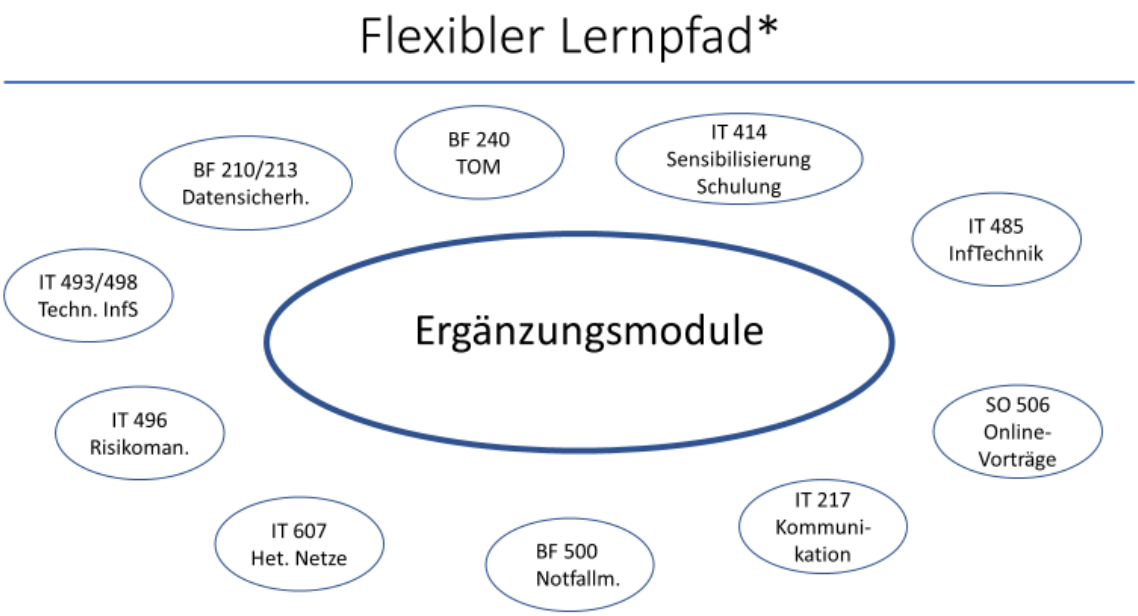
4.5 In Prüfung Follow-Up 2: Spezialfortbildung für Fortgeschrittene

In unseren Kursen haben wir die Erfahrung gemacht, dass Fortgeschrittene ein spezielles Follow-Up benötigen, dem mit den bisherigen Stufen des Lernpfads nicht zufriedenstellend entsprochen werden kann. Hierfür ist ein eigenes Angebot erforderlich, das die Grundlagen voraussetzt und auf einem hohen Wissenstand und sehr ausgeprägten Praxiserfahrungen aufsetzt. Gemeinsam mit dem BSI planen wir aktuell die sog. „Specials“. Dabei handelt es sich um eine Präsenzveranstaltung, die dem erweiterten Erfahrungs- und Wissensaustausch dient. Es sollen dem Bedarf der Teilnehmenden entsprechend Themenkomplexe mit hoher Praxisbedeutung behandelt werden. Eine Übersicht finden Sie hier:

Modul	Inhalt	Format	Tag
1	**Erfahrungsaustausch IT 499 – Für Fortgeschrittene „Specials der Informationssicherheit“** Vertiefungsthemen: Mindeststandards, BSI-Grundschutz, Datensicherheit, Sicherheitskonzeption, Aktuelles, aktiver Austausch zwischen Teilnehmenden	**1 Tag, 2x im Jahr**	**1**

4.6 Flexible Ergänzungsmodule

Die Informationssicherheit in der öffentlichen Verwaltung hat viele Facetten und ist dabei so bunt, wie die verschiedenen Verwaltungsbereiche. Hieraus folgen verschiedene flexible Fortbildungsbedarfe in unterschiedlichen Zielgruppen, für die wir flexible Ergänzungsmodule bereithalten. Eine Übersicht zu diesen flexiblen Ergänzungsmodulen, die im Lernpfad unabhängig von den zuvor vorgestellten Kursen belegt werden können, finden Sie nachstehend.



*Auszug. Eine vollständige Übersicht finden Sie hier im Lernpfad. Diese Kurse werden bei der Zertifikatsverlängerung berücksichtigt

Modul	Inhalt	Format	Tag
1	IT 217 – Kommunikation Fachübergreifende Kommunikation in IT-Projekten - Kommunizieren zwischen IT- und Verwaltungskräften	(Präsenz/digital)	**1 Tag**
2	IT 496 Risikoanalyse für Informationssicherheit • **Einleitung** Die Rolle der Risikoanalyse im Rahmen des IT-Grundschutz kurz darstellen. ○ Warum Risikoanalyse? ○ In welchen Fällen muss eine gemacht werden? ○ Überblick über verschiedene Methoden/Standards und Werkzeuge (z.B. BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz) • **Hauptteil** Übung Beispielhafte Durchführung einer Risikoanalyse nach BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz ○ Voraussetzungen (Systematischer ISMS-prozess, Rollen, Verantwortlichkeiten, Strukturanalyse, Schutzbedarfsfeststellung, Risikoakzeptanzkriterien) ○ Gefährdungsübersicht ○ Einschätzung und Bewertung von Risiken ○ Behandeln von Risiken	(Präsenz) **Workshop**	**2Tage**

	○ Konsolidierung ○ Handlungsanweisungen ableiten (Wer macht Wann Was, um Welchem Risiko zu begegnen) ○ Regelmäßige Reiteration • **Ende** ○ Reflektion Anwendung auf eigenes Arbeitsgebiet und Klärung von Fragen ○ Feedback		
3	IT 493/498 (Präsenz/digital) Technische Informationssicherheit Ziel: Teilnehmende sollen die Grundlagen der u. g. Techniken auf dem aktuellen Stand kennen sowie deren Nutzen und Risiken einschätzen können. Sie sollen beispielsweise anhand eines Schemas erkennen können, ob die verwendete Technik korrekt eingesetzt wurde oder wie verschiedene Techniken sinnvoll miteinander verzahnt werden müssen. Der Bezug zu den aktuell gültigen Standards und Dokumenten des BSI (200-X, MST, …) sowie zum Grundschutzkompendium soll praxisnah hergestellt werden. Inhalte: • Firewall: Definition, Gefährdungen, Aufgaben/Zweck, Aufbau/Komponenten, Architektur • VPN: Definition, VPN-Arten, Gefährdungen, Aufgaben/Zweck • Funknetze: Arten (z. B. NFC, Bluetooth, WLAN), Gefährdungen, Chancen, Funktionsweisen • Mobile Geräte: technische Absicherungsmöglichkeiten, technische Umsetzung von BYOD, COPE, MDM • E-Mail-Sicherheit: Konfiguration und Absicherung von Mailservern/Clients, gängige Gefährdungen, Spamschutz/Phishing/Pharming • Websicherheit: Konfiguration und Absicherung von Webservern und Webbrowsern, Gefährdungen • Infrastruktuelle Sicherheitsmaßnahmen: Stromversorgung, elementare Gefährdungen (wie Wasser, Feuer, Blitz) und Maßnahmen, Zutrittsschutz, häuslicher Arbeitsplatz • Verschlüsselung und elektronische Signatur: Symmetrische/asymmetrische Verschlüsselungsverfahren, Erzeugung/Prüfung von elektronischen Signaturen, digitale Zertifikate, PKI,	**Online-Vortrag mit Praxisbeispielen und interaktiven Praxisfragen, Übungen**	**2 Tage**

	Anwendungsgebiete von Kryptographie in Behörden, Erstellung und Inhalte eines Kryptokonzepts		
3	IT 414 Sensibilisierung Effektiv und fair: Nachhaltig schulen und sensibilisieren im Datenschutz und der Informationssicherheit	Digital	**2 Tage**

Weitere Ergänzungen dieser Module können Sie der nachstehenden Auswahl am BAköV-Angebot zum Kompetenzerwerb in anderen Bereichen entnehmen, die auch für die behördliche Informationssicherheit hilfreich sein können. Ausführlichere Inhalte halten wir für Sie in IFOS-Bund unter ifosbund.de bereit:

- **FP 100 Verständliches Schreiben - Mehr Erfolg durch gute Texte**
- **BF 210/213 Datenschutz und Datensicherheit**
- **BF 240 Technische und organisatorische Maßnahmen nach der DSGVO (TOM)**
- **BF 500 Notfallmanagement etablieren, umsetzen und steuern**
- **FÜ 270 Teams zielorientiert leiten**
- **FÜ 330 Changemanagement: Veränderungsprozesse aktiv gestalten**
- **FÜ 640 Steuerung von Veränderungsprozessen**
- **FÜ 400 Arbeit organisieren und Zeit managen für Führungskräfte**
- **IT 320 Grundlagen Digitales Management in der öffentlichen Verwaltung**
- **IT 205/206 Besondere Rahmenbedingungen für IT-Projekte in der Bundesverwaltung**
- **IT 234/230 Das V-Modell XT Bund – Basis**
- **IT 484/485 Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung - Grundlagen und Anwendung**
- **IT 540 Barrierefreie PDF-Dokumente erstellen - Grundlagen**
- **IT 600 Grundlagenwissen für Systemadministratoren in der öffentlichen Verwaltung**
- **IT 607 IT-Sicherheitsaspekte in heterogenen Netzen**
- **IT 630 Daten- und Informationssicherheit beim Einsatz mobiler Geräte**
- **IT 680 Computer-Forensik in Theorie und Praxis**
- **KO 240/21 Kommunikation mit Vorgesetzten**
- **KO 300 Erfolgreich verhandeln**
- **KO 1XX kommunizieren und kooperieren**
- **KO 340 Argumentieren, überzeugen, Feedback geben**
- **MD 330 Grundlagen- und Aufbauseminar: Lehren lernen**
- **OR 160 Personalbedarfsermittlung**
- **OR 270 Wissensmanagement - Theoretischer Überblick und individuelle Anwendung**
- **OR 520 Risiko- und Krisenmanagement in Projekten**
- **SE 150 Arbeit organisieren und Zeit managen**
- **SE 220 Resilienz - Widerstandskraft und Flexibilität stärken**
- **SE 240 Kreative Problemlösungen im Arbeitsalltag**

Darüber hinaus bietet die BAköV das Thema „Informationssicherheit“ auch als **Querschnittsthema für spezifische Zielgruppen** an (vgl.

hierzu auch Ziff. 3.3, u.a. als integriertes Thema in entsprechenden Grundlagenkursen oder in Form von spezifischen Online-Vorträgen). Dieses Angebot wird z.T. aktuell noch entwickelt und kann daher noch nicht vollständig abgebildet werden. Mit diesem Angebot möchte die BAköV einen Beitrag leisten, um die Informationssicherheit als Querschnittsthema weiter zu entwickeln. Entsprechende Angebote werden in IFOS veröffentlicht.

4.7 Angebote der Digitalakademie des Bundes

Darüber hinaus bietet die Digitalakademie des Bundes als Teil der BAköV weitere Angebote, mit denen Sie sich digital qualifizieren können. Schauen Sie doch einfach mal unter www.digitalakademie.bund.de vorbei und genießen Sie die eine oder andere Lernreise durch die Welt der Digitalisierung. Wir wünschen Ihnen hierbei viel Freude!

4.8 BSI-Grundschutzpraktikerinnen und BSI-Grundschutzpraktiker

BSI und BAköV möchten den Teilnehmenden des IT 486 die Möglichkeit eröffnen, eine Prüfung zur BSI-Grundschutzpraktikerin bzw. zum BSI-Grundschutzpraktiker zu absolvieren. Nach Einschätzung von BSI und BAköV sind die Lerninhalte des IT 486 bis auf wenige Details ausreichend, um die Prüfung bestehen zu können. Allerdings müsste die Prüfung derzeit bei anderen geeigneten Schulungsanbietenden absolviert werden.

Informationen zum IT-Grundschutzpraktiker finden Sie auf der BSI-Webseite:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Personenzertifizierung-IT-Grundschutzberater/Schulungen-zum-IT-Grundschutz-Praktiker-und-IT-Grundschutzberater/schulungen-zum-it-grundschutz-praktiker-und-it-grundschutzberater_node.html

Das Curriculum finden Sie zudem hier: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Berater/curriculum_1_0.pdf?__blob=publicationFile&v=2

5 Fortbildung in der öffentlichen Verwaltung

Die Fortbildung ist modular aufgebaut und beinhaltet die Möglichkeit der individuellen Gestaltung abhängig von dem konkreten Bedarf an Fortbildung der Teilnehmenden.

Alle in der Zielgruppe genannten Beschäftigten der Bundesverwaltung sind nach vorheriger Anmeldung der Behörde zur kostenfreien Teilnahme berechtigt. Die Anmeldung muss durch die Fortbildungsstelle in IFOS-BUND zusätzlich erfolgen.

5.1 Interviewberatung und Selbsteinschätzungstest

Zur Überprüfung Ihrer Kenntnisse im Vorfeld der Fortbildung besteht die Möglichkeit einer Interviewberatung bei der BAköV. Diese ist freiwillig und kann jederzeit wiederholt werden. Zudem bietet die BAköV im Fortbildungsportal des Bundes einen elektronischen Selbsteinschätzungstest für Sie an.

5.2 Lernprozessbegleitung

Sie haben die Möglichkeit, die Lernprozessbegleitung der BAköV in Anspruch zu nehmen. Die Lernprozessbegleitung der BAköV steht zur Auskunft und Beratung, sowohl für die Fortbildungsbeauftragten als auch für die Teilnehmenden zur Verfügung. Die Lernprozessbegleitung berät Sie bei der Erstellung Ihres individuellen Lernpfads, koordiniert und steht Ihnen als Ansprechperson für weitere Qualifizierungen zur Verfügung.

6 Zertifizierung

Für den Erwerb des BAköV-Zertifikats erarbeiten Sie ein Projekt innerhalb ihrer Behörde bzw. dem Aufgabenbereich. Dieses Projekt stellen Sie in einem Präsentationsworkshop vor. Die Zertifizierungen schließen Sie mit einer Prüfung ab. Ihr Zertifikat ist 5 Jahre gültig. Die Verlängerung Ihres Zertifikats ist nur über eine vorgegebene, zu erreichende Punktzahl möglich (siehe unten). Für die Zertifizierung gilt die Zertifizierungsordnung der BAköV.

6.1 Fachliche Begleitung

Das Thema und der Plan der Projektarbeit für die Zertifizierung wird mit der fachlichen Begleitung besprochen und bestätigt. Die Aufgabe der fachlichen Begleitung ist es, die eigenständige Auswahl und Durchführung des Projektes zu unterstützen. Die Begleitung unterstützt bei der Festlegung der Themenauswahl (Projektaufgabe), begleitet den Erstellungsprozess einer konzeptionellen Projektarbeit über ein behördenspezifisches Thema und ggf. die Präsentation. Die Begleitung sollte vorzugsweise bei der eigenen Behörde erfolgen, um im Idealfall eine hohe Nähe der Projektarbeit zum Arbeitsfeld der Nachhaltigkeit herzustellen. In Einzelfällen kann auch eine Begleitung durch das BSI angefragt werden. Die Entscheidung darüber wird vom Kandidaten bzw. von der Kandidatin getroffen.

6.2 Projektarbeit

Im praktischen Teil der Zertifizierung soll ein Projekt in der jeweiligen Behörde bearbeitet werden. Der Praktische Teil sollte begleitend stattfinden (behördenintern oder mit einer externen Unterstützung) und das Thema

sollte den eigenen oder zukünftigen Aufgabenbereich betreffen bzw. daraus hervorgehen. Dies kann sowohl eine Vorlage für Entscheidungen der Hausleitung, die Aufbereitung fachlicher Themen aus dem Bereich Informationssicherheit als auch neue bzw. bevorstehende Projekte umfassen. Anliegen ist es, die Tätigkeit zu unterstützen bzw. die Erstellung von Dokumenten zu begleiten. Zur Bestätigung des Projektthemas wird der Antrag „Plan der Projektarbeit“ von der BAköV genehmigt und mit dem BSI abgestimmt. Der Umfang des Projektes wird mit der fachlichen Begleitung besprochen und die reine Dokumentation sollte ca. 5-10 Seiten (ohne Deckblatt, Inhaltsverzeichnis, Literatur-/Quellenverzeichnis etc.)umfassen. Die Projektarbeit sollte neben der Darstellung eines zu adressierenden Problems und eines möglichen Lösungsansatzes vor allem das Vorgehen beim Erstellen und damit die Eigenleistung des zu Prüfenden darstellen.

Im Anhang dieses Lernpfades ist eine Übersicht von Themenvorschlägen enthalten.

Projektarbeit	Dauer
Auf der Grundlage der modularen Inhalte dieses Konzepts und den Anforderungen aus dem Aufgabenbereich ist ein überschaubares Projekt innerhalb der Behörde zu absolvieren.	Ca. 20 Stunden

Hinweis:

Die positive Beurteilung eines Projekts ersetzt nicht eine vollständige QS, ein (Zertifizierungs-)Audit oder sonstige genaue Überprüfungen des zugehörigen vollständigen Projektes.

6.3 Projektpräsentation

Die Präsentation der Projektarbeit erfolgt in einem behördenübergreifenden Workshop. Die Abgabe der Arbeit muss spätestens **drei Wochen** vor dem Workshop erfolgen. Eine elektronische Abgabe bei der BAköV (lg5@bakoev.bund.de) ist möglich. Alle Teilnehmenden präsentieren ihre Projektarbeit und führen mit dem Teilnehmenden ein Gespräch darüber. Dieses Gespräch wird - die Präsentation eingeschlossen - jeweils einen Zeitraum von etwa 30 Minuten beanspruchen. Der Workshop wird von der BAköV moderiert und vom BSI begleitet.

6.4 Prüfung

Abschließendes Element der Zertifizierung ist die Prüfung. Dieser findet vor Ort bei der BAköV statt (an einer Online-Lösung wird noch gearbeitet).

In 120 Minuten müssen 120 Fragen basierend auf dem Handbuch „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ beantwortet werden. Es handelt sich um einen Multiple-Choice-Test, bei dem mehrere Antworten zu einer Frage richtig sein können. 75 % der Antworten müssen richtig erkannt werden.

6.5 Zertifikatserhalt

Zur Erhaltung der Qualifikation wird eine kontinuierliche Fortbildung benötigt, die alle Aspekte Ihres Aufgabenbereichs umfasst und sowohl auf eine Erweiterung der fachlichen als auch der sozialen Kompetenzen abzielt. Die Fortbildung zum Kompetenzerhalt wird überwiegend durch Veranstaltungen der BAköV ermöglicht. Zum Erhalt oder zur jeweiligen Verlängerung des Zertifikats werden verschiedene Maßnahmen angeboten, die insbesondere im hier vorgestellten Lernpfad beschrieben sind. Auch die flexiblen Ergänzungsmodule zählen hierzu. Zudem besteht die Möglichkeit, eigene Vortrags- oder Dozierendentätigkeit im Bereich der Informationssicherheit anerkennen zu lassen. Über die Geeignetheit der Tätigkeit entscheidet die BAköV in Rücksprache mit dem BSI.

Punktesystem für den Erhalt des Zertifikats

Innerhalb von 5 Jahren müssen 50 Punkte erreicht werden. Die zweimalige Teilnahme an der „Jahrestagung“ in diesem Zeitraum ist Bedingung.

Die Punkte sind über folgende Maßnahmen zu erreichen	**Punkte**
Teilnahme an der Jahrestagung	15
Teilnahme an anderen Veranstaltungen der BAköV aus den Bereichen der Informationssicherheit	13
Teilnahme an anderen Veranstaltungen der BAköV	12
Vortragstätigkeit bzw. Dozierendentätigkeit im Rahmen von Schulungen, Kongressen, usw. (Anerkennung nach Absprache mit der BAköV)	10
Teilnahme an Online-Vorträgen der BAköV	5
Teilnahme an Fortbildungsangeboten von externen Anbietern und Kongressen im Bereich Informationssicherheit (Anerkennung nur nach Absprache mit der BAköV)	8
Teilnahme an anderen Fortbildungsangeboten von externen Anbietern (Anerkennung nur nach Absprache mit der BAköV)	5

Hinweis:

Die Punktetabelle gilt ab dem 1.1.2022. Zertifikate, die in den 5 Jahren vor diesem Stichtag erworben wurden, werden auf der Basis des bis zum 31.12.2021 erforderlichen Werts von 40 Punkten verlängert. Die Übergangszeit geht damit bis zum 31.12.2026. Mit der Punkteerhöhung verfolgen BAköV und BSI das Ziel, die für die Praxis erforderliche Qualifizierung zu intensivieren und nachhaltiger zu gestalten.

Die Zertifikatsverlängerung ist nur auf schriftlichen Antrag möglich. Der Antrag soll drei Monate vor Ablauf des Zertifikats vorliegen.

7 ANHANG

- Zertifizierungsordnung
- Themenvorschläge für die Projektarbeit
- Empfehlungen zur Anfertigung der Projektarbeit
- Empfehlungen zur Vorbereitung der Präsentation
- Formulare
    - Plan der Projektarbeit – Antrag
    - Änderungs- / Ergänzungsmitteilung
    - Antrag: Zertifikatsverlängerung

7.1 Zertifizierungsordnung vom 1. Januar 2022

I. Allgemeines

§ 1: Geltungsbereich

Diese Zertifizierungsordnung gilt für die Qualifizierung von IT-Sicherheitsbeauftragten in der öffentlichen Verwaltung und von Beschäftigten im behördlichen Informationssicherheitsmanagement oder im behördlichen Wissensmanagement (z. B. hauptamtlich Lehrende). Sie regelt die Zertifizierung dieser Zielgruppen.

§ 2: Zweck der Zertifizierung

Die Zertifizierung dient dem Nachweis der erforderlichen Fachkunde für die in § 1 genannten Zielgruppen. Nach erfolgreicher Präsentation des Projekts und der Prüfung erhalten die Absolventinnen bzw. Absolventen ein Zertifikat, durch das bescheinigt wird, dass sie aus Sicht der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat (BAköV) in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) die notwendigen Kenntnisse und Fähigkeiten besitzen, um insbesondere die in § 1 genannten Tätigkeiten auszuüben.

§ 3: Zulassung zur Fortbildungsmaßnahme

Berechtigt zur Teilnahme an der in § 1 dieser Zertifizierungsordnung genannten Fortbildungsmaßnahme und Zielgruppen sind Beschäftigte der öffentlichen Verwaltung aus dem höheren, gehobenen und mittleren Dienst.

§ 4: Fortbildungsinhalt und –dauer

(1) Die in § 1 dieser Zertifizierungsordnung genannte Fortbildungsmaßnahme ist modular aufgebaut und beinhaltet die Möglichkeit der individuellen Gestaltung abhängig von dem konkreten Bedarf an Fortbildung der Teilnehmenden.

(2) Zur Vorbereitung auf die Projektarbeit und die Prüfung sollten die Teilnehmenden grundsätzlich die Fortbildungsmaßnahme IT 486 „Infor-

mationssicherheitsmanagement in der öffentlichen Verwaltung“ gemäß des BAköV-Lernpfades „Informationssicherheitsmanagement in der öffentlichen Verwaltung“ absolvieren.

II. Projektarbeit, Projektpräsentation und Prüfung

§ 5: Projektarbeit

Die Teilnehmenden müssen eine Projektarbeit zu einem für die Informationssicherheit der öffentlichen Verwaltung relevanten Thema erstellen. Dabei können sie sich seitens ihrer Behörde oder einer anderen externen Stelle begleiten lassen. Die Projektarbeit sollte einen geschätzten Mindestarbeitsaufwand von etwa 20 Stunden erfordern. Über die Projektarbeit erstellen die Teilnehmenden eine schriftliche Dokumentation von ca. 5 bis 10 Seiten, die eine Erläuterung aller wesentlichen Bestandteile des Projekts enthält, und bestätigen gegenüber der BAköV mit eigener Unterschrift unter der Dokumentation, dass die Projektarbeit von ihr bzw. ihm tatsächlich und eigenverantwortlich durchgeführt wurde.

§ 6: Projektpräsentation

(1) Voraussetzung für den Erhalt des Zertifikats nach § 9 dieser Zertifizierungsordnung ist eine 20 Minuten umfassende Präsentation der Projektarbeit gem. § 5.

(2) Die BAköV bewertet die Projektarbeit und die Präsentation in Abstimmung mit dem BSI. Die Bewertung kann „bestanden“ oder „nicht bestanden“ lauten. Kriterien für die Bewertung sind neben der Eigenständigkeit der Erarbeitung die überzeugende Anwendung der einschlägigen Vorgaben wie dem BSI-Grundschutz und sonstigen Rechtsnormen sowie die Praxistauglichkeit der Arbeit. Empfehlungen des BSI sind zu berücksichtigen. Zur Praxistauglichkeit der Arbeit zählen die praxiskonforme Ergebnisorientierung für das jeweilige behördliche Umfeld, Nachvollziehbarkeit der Ausführungen, überzeugende Vermittlung der zentralen und wesentlichen Arbeitsergebnisse, die Beachtung von geschlechtergerechter Sprache sowie die Angabe von Quellen und moderne Präsentationstechniken, die auch die Anforderungen aus Behindertengleichstellungsrecht

beachten. Die Arbeit gilt als bestanden, wenn die vorgenannten Kriterien überwiegend erfüllt werden. Hierfür legt die BAköV in Abstimmung mit dem BSI folgende Punktewerte zu Grunde:

5 Punkte: Umfassend erfüllt

4 Punkte: Weit überwiegend erfüllt

3 Punkte: Überwiegend erfüllt

2 Punkte: zum Teil erfüllt

1 Punkt: zu einem geringen Teil erfüllt

0 Punkte: nicht erfüllt

(3) Die BAköV kann die Teilnehmenden in Abstimmung mit dem BSI zur einmaligen Überarbeitung der Projektarbeit in einem angemessenen Zeitraum bitten. Die Prüfungsleistung gilt in diesem Fall als bestanden, wenn für die BAköV und das BSI die Kriterien von § 6 Abs. 2 dieser Zertifizierungsordnung erfüllt sind.

§ 7: Prüfung

(1) Die Abschlussprüfung dauert 120 min.
(2) Gegenstand der Prüfung sind die Inhalte aus der jeweils aktuellen Fassung des „Handbuchs IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“, das zur Vorbereitung auf die Prüfung zur Verfügung gestellt wird.
(3) Die Abschlussprüfung findet in Form eines schriftlichen Multiple Choice Verfahrens statt (Abschlusstest).
(4) Die Abschlussprüfung ist nicht öffentlich.

§ 8: Bewertung

(1) Eine Differenzierung nach Noten findet bei der Bewertung der Prüfungsleistung nicht statt. Die Prüfung gilt vielmehr nur als „bestanden“ oder „nicht bestanden“. Die Prüfung gilt als bestanden, wenn mindestens 75 Prozent der möglichen Punktzahl erreicht werden.
(2) Die Abschlussprüfung kann einmal wiederholt werden. Die Wiederholung soll in der Regel innerhalb von zwölf Monaten nach dem erfolglosen Versuch stattfinden.
(3) Die Prüfungsleistung gilt als nicht bestanden, wenn Teilnehmende zu einem Prüfungstermin ohne triftige Gründe nicht

erscheinen oder nach Beginn der Prüfung ohne triftige Gründe von der Prüfung zurücktreten oder die Prüfungsleistung nicht vor Ablauf der Prüfung erbracht wird.

(4) Die für den Rücktritt oder das Versäumnis geltend gemachten Gründe müssen der BAköV unverzüglich schriftlich angezeigt und glaubhaft gemacht werden. Bei Krankheit kann die Vorlage eines ärztlichen Attestes verlangt werden. Erkennt die BAköV die Gründe an, so kann die Zulassung zu der entsprechenden Prüfungsleistung erneut beantragt werden.

(5) Versuchen Teilnehmende, das Ergebnis der Prüfungsleistung durch Täuschung oder Benutzung nicht zugelassener Hilfsmittel zu beeinflussen, gilt die betreffende Prüfungsleistung als nicht bestanden. Wer den ordnungsgemäßen Ablauf der Prüfung stört, kann von der jeweiligen Aufsicht, in der Regel nach Abmahnung, von der Fortsetzung der Prüfungsleistung ausgeschlossen werden; in diesem Fall gilt die betreffende Prüfungsleistung als nicht bestanden. Die Gründe für den Ausschluss sind aktenkundig zu machen.

(6) Erfolgt ein Ausschluss von der weiteren Erbringung der Prüfungsleistung, können Teilnehmende verlangen, dass die Entscheidung der BAköV überprüft wird. Dies gilt entsprechend bei Feststellungen gemäß Satz 1.

III. Zertifikat

§ 9: Zertifikat

(1) Nach der erfolgreichen Prüfung wird möglichst innerhalb von zwei Wochen ein Zertifikat ausgestellt.

(2) Das Zertifikat ist vom Präsidenten der Bundesakademie oder seiner Vertretung zu unterzeichnen. Das Zertifikat trägt das Datum des Tages, an dem die Prüfung erfolgte.

(3) Das Zertifikat hat eine Gültigkeitsdauer von fünf Jahren, beginnend mit dem Tag der Prüfung.

(4) Die Gültigkeitsdauer verlängert sich auf schriftlichen Antrag für die Zeit einer Inanspruchnahme von Elternzeit nach dem Bundeselterngeld- und Elternzeitgesetz und Zeiten eines Beschäftigungsverbots nach dem Mutterschutzgesetz sowie für Zeiten einer Betreuung oder Pflege eines pflegebedürftigen Angehörigen nach dem Pflegezeitgesetz und dem Familienpflegezeitgesetz in dem Umfang, in dem eine

Erwerbstätigkeit nicht erfolgt ist, höchstens jedoch für die Zeit von fünf Jahren.

(5) Eine Verlängerung des Zertifikats erfolgt, wenn die Zertifikatsinhaberin bzw. Zertifikatsinhaber im Zeitraum der Gültigkeitsdauer durch den Besuch einschlägiger Fortbildungsveranstaltungen auf Grundlage der Tabelle in Ziff. 6.5 des Lernpfads „Informationssicherheitsmanagement in der öffentlichen Verwaltung“ 50 Punkte erreicht, zweimal die Jahrestagung der IT-Sicherheitsbeauftragen in der Bundesverwaltung besucht und sie/er im Zeitpunkt der Zertifikatsverlängerung zur Zielgruppe nach § 1 zählt oder für die Übernahme eine dieser Aufgaben vorgesehen ist. Wenn Teilnehmende die erforderliche Punktzahl nicht erfüllen und auch keine Verlängerung nach Abs. 4 in Betracht kommt, können sie zur Zertifikatsverlängerung die Prüfung erneut ablegen. Die Zertifikatsverlängerung ist nur auf schriftlichen Antrag möglich. Der Antrag soll 3 Monate vor Ablauf des Zertifikats vorliegen.

§ 10: Ungültigkeit von Prüfungen

(1) Haben Teilnehmende im Rahmen der Projektarbeit getäuscht und wird diese Tatsache erst nach der Aushändigung des Zertifikats nach § 9 dieser Zertifizierungsordnung bekannt, so kann die BAköV in Abstimmung mit dem BSI nachträglich die Zertifizierung für nicht bestanden erklären.

(2) Das unrichtige Zertifikat nach § 9 dieser Zertifizierungsordnung ist einzuziehen und gegebenenfalls neu zu erteilen.

§ 11: Rechtsmittel

Gegen die Entscheidungen der BAköV ist der Widerspruch möglich. Er ist innerhalb von vier Wochen nach Bekanntgabe der Entscheidung bei der BAköV schriftlich einzureichen. Diese entscheidet in Abstimmung mit dem BSI über den Widerspruch.

IV. Abschlussvorschriften

§ 12: Datenschutzerklärung

(1) Die im Zusammenhang mit dieser Zertifizierungsordnung zur Verfügung gestellten personenbezogenen Daten werden ausschließlich zum Zweck der erforderlichen Zertifikatsverwaltung einschließlich aller mit der Durchführung der Abschlussprüfung zusammenhängenden erforderlichen Maßnahmen verwendet. Rechtsgrundlage ist Art. 6 Abs. 1 lit.

e EU-DSGVO i.V.m. § 3 BDSG. Im Übrigen gilt die Datenschutzerklärung der BAköV, die unter www.bakoev.bund.de/datenschutz eingesehen werden kann.

(2) Die personenbezogenen Daten werden bei der BAköV aufbewahrt. 10 Jahre nach der letztmaligen Entscheidung über das Bestehen oder Nichtbestehen der Prüfung oder einer Zertifikatsverlängerung werden die Daten vernichtet.

§ 13: Inkrafttreten und Veröffentlichung

Diese Zertifizierungsordnung tritt am 1. Januar 2022 in Kraft.

07.2 Themenvorschläge für die Projektarbeit

Aus allen Aufgabengebieten des behördlichen Informationssicherheitsmanagements können Themen für Projektarbeiten selbstständig formuliert werden. Hier folgt eine Auflistung von möglichen Themen als Hilfestellung, welche an Behördenspezifika angepasst werden sollten. Bitte beachten Sie, dass bei allen Themenvorschlägen die BSI-Veröffentlichungen genutzt werden sollen (z. B. BSI-Standards, Kompendium, usw.)

Themenvorschlag 1:

Passen Sie die in den IT-Grundschutz-Standards vorgeschlagenen Definitionen der Schutzbedarfskategorien an Ihre Behörde an. Beschreiben Sie Ihre Vorgehensweise und zeigen und begründen Sie an zwei Beispielen, wie Sie den Schutzbedarf aufgrund dieser Definitionen festgestellt haben.

Die Projektarbeit sollte die folgenden Aspekte enthalten:

* Aufzeigen der behandelten Schutzbedarfskategorien
* Anpassen der Kategorien an die Belange der Behörde
* Befragen von weiteren für die Informationssicherheit Zuständigen, Abstimmen mit der Leitung, den Fachabteilungen und IT-Referaten (Experteninterview).
* Vorstellung der zwei ausgewählten Beispiele (mit unterschiedlichem Schutzbedarf)
* schlüssige, an den eigenen Definitionen orientierte Begründung der Schutzbedarfsfeststellungen
  (Hinweis: Die hausinterne Abstimmung kann sehr zeitintensiv sein und ggfs. den zeitlichen Rahmen einer Projektarbeit damit vergrößern)

Themenvorschlag 2:

Stellen Sie für Ihre Behörde ein Sensibilisierungs- und Schulungsprogramm zusammen.
Beschreiben Sie, wie Sie zentrale Angebote auf die Bedingungen und Sicherheitskultur Ihrer Behörde anpassen.

Die Projektarbeit sollte die folgenden Aspekte berücksichtigen:

* Beschreiben Sie die Situation und Themen in Ihrem Hause. Definieren Sie die Themen, Ziele, Zielgruppen und das Vorgehen für die Schulung und Sensibilisierung für Ihre Behörde.

* Welche Schulungen sind für welche Zielgruppe notwendig (sowohl Sicherheitsschulungen als auch Anwenderschulungen)?
* Welche Schulungen sind für welche Zielgruppe in welchem Zeitraum durchzuführen?
* Wie soll die Sensibilisierung geschehen (Vorträge, Web-based Training, Intranet-Inhalte, Sensibilisierungskampagnen und andere Maßnahmen)?
* Wie werden die Schulungen und Sensibilisierungen evaluiert und nachhaltig gestaltet?
* Wie und von wem (extern, intern) sollen die Sensibilisierungen und Schulungen durchgeführt werden?

Themenvorschlag 3:

Welche Maßnahmen sind einzuplanen, wenn in Ihrer Behörde E-Mail-Verschlüsselung und die Elektronische Signatur eingesetzt bzw. deren Einsatz erweitert werden soll?

Die Erarbeitung eines vollständigen Konzepts würde den Rahmen der Projektarbeit erfahrungsgemäß übersteigen. Daher könnte hier nur dargelegt werden, welche Vorgehensweise und welche Maßnahmen erforderlich sind.

Folgende Themen müssten bearbeitet werden:

* Welche Daten (E-Mails, Dokumente) sollen verschlüsselt bzw. signiert werden?
* Schlüsselmanagement:
  Wo werden die öffentlichen Schlüssel gespeichert? Verfügbarkeitsanforderungen an den Schlüsselserver? Wie wird der Schlüsselserver vor Missbrauch geschützt?
* Prozesse zur sicheren Generierung der Schlüsselpaare sicheren Zuweisung zu Personen
* Benennung von Verantwortlichen
* Schulungskonzept
* Datensicherungskonzept für die Schlüssel
* Regelungen für den Umgang mit Verschlüsselung und Signatur, zum Beispiel Vertretungsregelung, Schlüsselhinterlegung und Vorsorge für unvorhersehbare Ereignisse (Krankheit, Verlust des Schlüssels)

Themenvorschlag 4:

Stellen Sie die organisatorischen, technischen und personellen Voraussetzungen für den Einsatz eines „Security Tools“ z.B. SIEM, Intrusion Detection System, etc. aus der Sicht des IT-Sicherheitsbeauftragten zusammen. Entwerfen Sie ein Sicherheitskonzept für Ihre Behörde.

Die Lösung sollte u.a. folgende Aspekte umfassen:

* Übersicht zu verschiedenen Arten des ausgewählten Security-Tools sowie der Einsatzszenarien
* Identifikation der Anwendungen/IT-Systeme, die durch das Tool überwacht werden sollen sowie Begründung der Auswahl
* Darstellung der datenschutzrechtlichen Aspekte, die eine Beratung mit dem/der Datenschutzbeauftragten und dem Personalrat erfordern.

Beschreiben Sie die wesentlichen Aufgaben dieser Produkte und stellen Sie Kriterien zusammen, die ein solches Werkzeug erfüllen sollte, damit es in Ihrer Behörde eingesetzt werden kann. Begründen Sie mit Hilfe dieser Kriterien, welches dieser Programme ausgewählt werden könnte.

Alternative: Auch die Konzepterstellung für eine Ergänzung, Aktualisierung oder Migration eines bestehenden Security Tool Konzeptes ist möglich. Berücksichtigen Sie dabei sowohl die zentralen als auch die dezentralen Möglichkeiten.

Es müssen Referenzen zu den im IT-Grundschutz enthaltenen Bausteinen und deren Anforderungen im Kontext Ihrer Behörde getroffen werden, bzw. eine Risikoanalyse stattfinden.

Themenvorschlag 5:

Erstellen Sie ein Kryptokonzept für Ihre Behörde. Legen Sie dar, wie Sie strategisch nach IT-Grundschutz vorgehen und wo die Besonderheiten und spezifischen Schwierigkeiten Ihrer Behörde liegen. Wie setzen Sie theoretische Anforderungen in die konkrete Praxis um? Nachfolgende Stichpunkte bieten Ihnen eine erste Übersicht:

- Auswahl geeigneter Verfahren (Stand der Technik),

- Datensicherung,

- Kommunikationsverbindungen,

- Schlüsselmanagement,

- sicheres Löschen und Vernichten,

- individueller Bedarf für kryptographische Verfahren.

Themenvorschlag 6:

Erstellen Sie ein Datensicherungskonzept nach IT-Grundschutz für Ihre Behörde.

Festzulegen sind:

* Welche Daten müssen gesichert werden?
* Art der Datensicherung
* Wo werden zu sichernde Daten gespeichert?
* Zeitpunkt und Häufigkeit
* Vorgehensweise und Speichermedium (z.B. Band, Ausweichserver in anderem RZ)
* Sichere Aufbewahrung der Sicherungsmedien
* Fristen für die Aufbewahrung und Anzahl der Generationen
* Festlegen der Verantwortlichkeiten
* Übungen zur Datenrekonstruktion
* Welche Vor- und Nachteile hat Verpflichtung der Beschäftigten zur Datensicherung? Wie müsste die Verpflichtung ausgestaltet werden?

Berücksichtigen Sie auch die Schnittstellen zur Notfallvorsorge.

Themenvorschlag 7:

Erarbeiten Sie eine Dienstanweisung für Beschäftigte, denen ein Gerät zur mobilen Kommunikation oder Datenübertragung wie z. B. Laptop, Tablet, USB-Stick, Smartphone, etc. anvertraut wird. Die Dienstanweisung soll Beschäftigte auf einen angemessenen Umgang mit diesen Geräten hinweisen. Skizzieren Sie ferner technische Maßnahmen für die Sicherheit, der auf den mobilen Geräten gespeicherten Daten.

Festzulegen sind:

* Konfiguration
* Umgang (u.a. Diebstahlsicherung)
* Schutz des mobilen Gerätes (u.a. Passwort, Token)

* Verbindungen ins behördeninterne Netz
* Verbindungen ins Internet
* Virenschutzregelungen
* Einsatz Verschlüsselung
* Einsatz von Schnittstellenkontrollen

* Zuständigkeiten

Themenvorschlag 8:

Erarbeiten Sie ein Konzept (Dienstanweisung) für den Umgang mit dem Internet in der Behörde.
Das Konzept sollte unter anderem enthalten:

* den Sinn dieser Regelung
* Ist privates Surfen erlaubt: Wenn ja, in welchem Umfang, wenn nein, welche Kontrollen und Maßnahmen bei Zuwiderhandlung sind möglich?
* Regelungen für Downloads
* Erlaubte bzw. notwendige Erweiterungen des Browsers
* Umgang mit aktiven Inhalten
* Umgang mit Cookies
* Proxy-Einstellungen, Filter (Blacklist/Whitelist)
* Sicherheitseinstellungen bei den verwendeten Browsern

Themenvorschlag 9:

Prüfen Sie die Maßnahmen, mit denen die Serverräume Ihrer Behörde gesichert sind. Dokumentieren Sie Ihre Prüfergebnisse und zeigen Sie ggf. Möglichkeiten auf, mit denen die Sicherheit der dort untergebrachten IT-Systeme den Anforderungen entsprechend angepasst werden können.

Für diese Aufgabe müssen sich IT-Sicherheitsbeauftragte zunächst mit den Anforderungen des IT-Grundschutzes für den Serverraum beschäftigen und diese verstehen. Anschließend müssen Sie den IT-Administrator und weitere Rollen interviewen und zumindest stichprobenartig die Maßnahmen überprüfen. In der Ausarbeitung sollten zu allen im IT-Grundschutz angegebenen Anforderungen Erläuterungen enthalten sein.

Themenvorschlag 10:

Erstellen Sie einen Netzplan über die logische Struktur des Netzes Ihrer Behörde.

Beschreiben Sie dabei die Netzbereiche, soweit wie dies sinnvoll möglich ist und begründen Sie dies. Stellen Sie außerdem fest, welche Kommunikationsverbindungen besonders abgesichert werden sollten und wie dies zu bewerkstelligen ist.
Die Einschränkung auf einen Teilbereich ist im Hinblick auf den Umfang möglich.

Themenvorschlag 11:

Beschreiben Sie Ihr Vorgehen bei der Erstellung der Leitlinie zur Informationssicherheit für Ihre Behörde, die alle gemäß IT-Grundschutzmethodik vorgegebenen Inhalte enthält. Gehen Sie insbesondere auch auf die Struktur der Verantwortlichkeiten im Informationssicherheitsprozess ein.

In der Projektarbeit sollten folgende Aspekte erläutert werden:

* Erläuterung der Begründung der Bedeutung Erläutern Sie Ihre Begründung der Bedeutung der Informationssicherheit für Ihre Behörde,die Wichtigkeit für die Geschäftsvorgänge/IT-Anwendungen sowie das angestrebte Sicherheitsniveau.
* Nennung der wichtigsten Sicherheitsziele sowie der vorgesehenen Maßnahmen und organisatorischen Regelungen, um diese zu erreichen
* Aufzeigen der Schritte zum Erreichen einer wirksamen Leitlinie in Ihrer Behörde
* Vorstellen des Informationssicherheitsprozesses Ihrer Behörden bzw. das geplante Modell mit Erklärung der Bedeutung der Leitlinie für die weiteren Maßnahmen im Sicherheitsmanagement
* Darstellen und Differenzieren der Verantwortlichkeiten für Informationssicherheit in Ihrer Behörde
* Erläuterung an Hand einer Grafik die für Informationssicherheit zuständigen Instanzen, Gremien und ihre Zuordnung zur Leitung
* Darstellen des Veröffentlichungs- und Inkraftsetzungsprozesses mit Augenmerk auf die Information der Beschäftigten

Die Leitlinie (Entwurf) muss im Anhang der Projektarbeit aufgeführt sein.

Themenvorschlag 12:

Entwerfen Sie ein Virenschutzkonzept für Ihre Behörde.
Auch die Konzepterstellung für eine Ergänzung, Aktualisierung oder Migration eines bestehenden Virenschutzkonzeptes ist möglich. Berücksichtigen Sie dabei sowohl die zentralen als auch die dezentralen Möglichkeiten zum Schutz vor Schadsoftware oder Spam.

Es sollten Referenzen zu IT-Grundschutz-Anforderungen im Kontext Ihrer Behörde getroffen werden.

Themenvorschlag 13:

Durch eine Modernisierung steht eine signifikante Änderung der IT-Infrastruktur an.
Erarbeiten Sie ausgehend von der aktuellen Situation und den zukünftigen technischen Erfordernissen eine Vorlage zur Entscheidung für die Behördenleitung, in der Sie verschiedene Konzepte sowie deren Vor- und Nachteile aus Sicht der Informationssicherheit skizzieren und begründen Sie, welches das geeignete Konzept für Ihre Behörde ist.
Sinn dieser Aufgabe ist, das Herangehen zu verdeutlichen und die verschiedenen technischen Konzepte zu verstehen, sowie eine Auswahl und ihren Einsatz in der Behörde zu begründen.

Themenvorschlag 14:

Angenommen, es wird von Ihrer Behördenleitung erwogen, die Aufgaben mit Informationssicherheitsrelevanz für einen Standort der Behörde an einen externen Dienstleiser zu vergeben.
Erstellen Sie ein Konzept, in der Sie der Behördenleitung die Vor- und Nachteile einer solchen Lösung darstellen und vor allem die Anforderungen formulieren, die ein Dienstleister für diese Aufgaben aus Sicht der Informationssicherheit erfüllen muss.

Themenvorschlag 15:

Entwerfen Sie ein Konzept für die Reaktion auf Sicherheitsvorfälle (einschließlich Zuständigkeiten und Meldewegen, Nachbereitung etc.).
Berücksichtigen Sie dabei unterschiedliche Arten von Vorfällen (z.B. Virenbefall, Systemausfall, Informationsabfluss, etc.).

Die internen Meldewege müssen auf die Behörde angepasst in der Ausarbeitung spezifiziert werden. Auch die Ausgestaltung der Meldewege zum BSI müssen enthalten sein.

Themenvorschlag 16:

In einer Behörde ist ein Netz mit entsprechenden Clients und Servern eingerichtet.
Entwerfen Sie eine Sicherheitsrichtlinie für die Clients und/oder Server, entsprechend den vorgegebenen Einsatzszenarien, begründen Sie Ihre Entscheidungen.

Themenvorschlag 17:

In Ihrer Behörde ergibt sich die Notwendigkeit funkbasierter Kommunikation (WLAN).
Entwickeln Sie für Ihre Behördenleitung eine Entscheidungsgrundlage für den Einsatz eines WLAN-Konzeptes. Erarbeiten Sie die dafür notwendigen Sicherheitsmaßnahmen. Stellen Sie sichere Zugangsmöglichkeiten dar. Betrachten und beachten Sie bei der Integration und Nutzung der WLAN-Technik die organisatorischen und technischen Randbedingungen Ihrer Behörde.

Themenvorschlag 18:

Ihre Behörde plant eine Zertifizierung nach ISO 27001 auf Basis von IT–Grundschutz.
Erstellen Sie hierfür einen Projektplan.
Berücksichtigen Sie dabei maßgebliche Komponenten des Informationsverbundes und das Zertifizierungsschema des BSI.

Themenvorschlag 19:

In Ihrer Behörde steht eine Migration von Clientumgebungen an. Evaluieren Sie aus Sicht des/der IT-Sicherheitsbeauftragten, welche Auswirkungen diese geplante Migration auf Informationssicherheitsaspekte hat. Entwickeln Sie eine Entscheidungsvorlage für ihre Behördenleitung zur Migration der Clients. Begründen Sie ihre Entscheidung, indem Sie insbesondere auf IT-GS-Anforderungen und weitere BSI-Veröffentlichungen eingehen.

Anm.: Themen 19 und 20 können auch zusammengelegt werden. Hier ist jedoch der entstehende Aufwand/Umfang zu beachten.

Themenvorschlag 20:

In Ihrer Behörde steht eine Migration von Serverumgebungen an.

Evaluieren Sie aus Sicht des/der IT-Sicherheitsbeauftragten, welche Auswirkungen diese geplante Migration auf Informationssicherheitsaspekte hat. Entwickeln Sie eine Entscheidungsvorlage für ihre Behördenleitung zur Migration der Server. Begründen Sie ihre Entscheidung, indem Sie insbesondere auf IT-GS-Anforderungen und weitere BSI-Veröffentlichungen eingehen.

Anm.: Themen 19 und 20 können auch zusammengelegt werden. Hier ist jedoch der entstehende Aufwand/Umfang zu beachten.

Themenvorschlag 21:

In Ihrer Behörde wird bei der Schutzbedarfsanalyse ein höherer Schutzbedarf für ein Zielobjekt identifiziert.
Im Rahmen der IT-Grundschutz-Vorgehensweise wird daher eine Risikoanalyse durchgeführt.
Berücksichtigen Sie dabei den BSI-Standard 200-3 und führen Sie die Risikoanalyse für das Zielobjekt durch. Legen Sie insbesondere Wert auf eine geeignete Übertragung der beispielhaften Schadensauswirkung sowie Risikobewertung auf Ihre Behörde.

Themenvorschlag 22:

In Ihrer Behörde ist ein Geschäftsprozess von hoher Bedeutung (kritischer Geschäftsprozess).
Analysieren Sie die Anforderungen/Einordnung dieses Prozesses im Hinblick auf die Informationssicherheit (Schutzziele).
Analysieren Sie ebenfalls die Auswirkungen, die der Ausfall dieses Prozesses auf Ihre Schutzziele hat (Risikoanalyse).
Beschreiben Sie, ob für den kritischen Geschäftsprozess zunächst eine Kernabsicherung oder gleich das Standard-Vorgehen nach IT-GS sinnvoll ist.

Themenvorschlag 23:

In Ihrem Hause steht mittelfristig eine Informationssicherheitsrevision auf Basis von IT-Grundschutz an.
Entwickeln Sie einen Projektplan, um sich einen Überblick über das Thema „IS-Revision“ im Kontext ihrer Behörde zu verschaffen.
Anschließend machen Sie sich durch Ihren Maßnahmenplan mit den Voraussetzungen und dem Ablauf einer IS-Revision vertraut.

Themenvorschlag 24:

In Ihrem Hause stehen der Aufbau und die Etablierung eines Informationssicherheitsmanagementsystems (ISMS) an.

Entwickeln Sie einen Projektplan, um sich einen Überblick über das Thema Aufbau und Etablierung eines „ISMS“ im Kontext ihrer Behörde zu verschaffen.
Anschließend machen Sie sich durch Ihren Maßnahmenplanmit

den Voraussetzungen nach IT-Grundschutz vertraut.

Themenvorschlag 25:
In ihrer Behörde steht die Virtualisierung von Servern an. Stellen Sie aus der Sicht des/der IT-Sicherheitsbeauftragten insbesondere die erforderlichen Anpassungen in der Betrachtung der betroffenen Systeme nach BSI-IT Grundschutz dar. Identifizieren Sie die entsprechenden Grundschutzbausteine und skizzieren Sie organisatorische und technische Maßnahmen zur Minderung identifizierter neuer Risiken.

Themenvorschlag 26:
In Ihrer Behörde wird die Einführung einer NAC (Network Access Control) Lösung zu Absicherung des Netzwerkzugriffs erwogen.
Beschreiben Sie die wesentlichen Aufgaben einer derartigen Lösung. Leiten Sie daraus vor dem Hintergrund Ihres Sicherheitskonzeptes am Beispiel konkreter Produkte/Lösungen Auswahlkriterien ab. Prüfen Sie technische, organisatorische und personelle Voraussetzungen und evtl. Anpassungen im Netzwerk / der IT allgemein und Auswirkungen auf das vorhandene Sicherheitskonzept. Betrachten Sie dabei den Kontext Ihrer Behörde, der individuellen Risikoanalyse der Behörde sowie die elementaren Gefährdungen und IT-Grundschutzbausteine gemäß Grundschutz. Berücksichtigen Sie dabei auch Aspekte, die ggf. mit dem/der Datenschutzbeauftragten und dem Personalrat abgestimmt werden müssen.

Themenvorschlag 27:
In Ihrer Behörde wird der Beschaffung einer Sandboxing-Lösung geprüft bzw. es wird erwogen, diese Technologiekomponente bei sich bereits im Einsatz befindlichen Lösungen zu aktivieren.
Betrachten Sie die dabei die insbesondere die Abwägungen bzgl. des Risikos, betrachten Sie dabei auch ggf. neu hinzukommende Risiken auch in organisatorischer Hinsicht unter Beachtung des IT-Grundschutzes.
Berücksichtigen Sie Aspekte, die Sie mit dem/der Datenschutzbeauftragten abstimmen müssen und verweisen Sie dabei auf verschiedene Produktoptionen bzw. Optionen zur Parametrierung, sofern diese vorhanden sind.

Themenvorschlag 28:
Entwerfen Sie im Rahmen des Umfangs Ihrer Projektarbeit ein geeignetes Grundschutz-Profil für einen relevanten Geschäftsprozess Ihrer Behörde. Nennen Sie Gründe für Ihre Auswahl. Beachten Sie dabei insbesondere die Grundstruktur eines Grundschutz-Profils.

Themenvorschlag 29:
Erstellen Sie eine geeignete Sicherheitsrichtlinie zur Informationssicherheit auf Auslandsreisen von Beschäftigten Ihrer Behörde. Gehen Sie neben relevanten Aspekten für Auslandsreisen und problematischen Gegebenheiten auch auf tragbare IT-Systeme ein. Zeigen Sie behördliche Besonderheiten auf und stellen Sie dar, weshalb Sie sich für Ihr Vorgehen entschieden haben. Wie stellen Sie die Einhaltung der Richtlinie sicher? Nennen Sie geeignete Maßnahmen. Folgende Punkte können hilfreich sein:
- Sensibilisierung für Problematiken,
- Identifikation von länderspezifischen Bedingungen,
- technische und analoge Sicherheitsvorkehrungen / Diebstahlsicherung,
- Kryptografie.

Themenvorschlag 30:
Beschäftigen Sie sich mit den Anforderungen zur und mobilen Arbeiten. Stellen Sie allgemeine, aber auch konkrete Problematiken Ihrer Behörde dar und entwickeln Sie Lösungsansätze. Legen Sie die Konzentration auf Ihre Planung und Ihr konkretes Vorgehen nach IT-Grundschutz. Wie wenden Sie theoretische Anforderungen praktisch bei sich an? Nachfolgende Punkte können für Sie hilfreich sein:
- verbindliche Regelungen,
- technische Voraussetzungen,
- Datensicherung,
- Sensibilisierung und Schulung,
- Betreuung und Wartung.

Themenvorschlag 31:
Im Rahmen des Ideenmanagements wurde in Ihrer Behörde vorgeschlagen, dass Mitarbeitende ihre eigenen mobilen Geräte für dienstliche Tätigkeiten nutzen können (BYOD). Die Leitung Ihrer Behörde bittet Sie, diesen Vorschlag aus der Perspektive „Informationssicherheit“ zu betrachten und zu bewerten.
Definieren Sie in Ihrer Darstellung die Vor- und Nachteile von Consumerisation und BYOD aus Sicht eines ISB. Behalten Sie Besonderheiten Ihrer Behörde und rechtliche Vorgaben im Blick. Was können Sie empfehlen, was sollte vermieden werden? Welche konkreten Maßnahmen wä-

ren bei der Umsetzung nötig, wie müssten diese aussehen? Berücksichtigen Sie dabei auch Vorgaben des Geheimschutzes, die mit dem/der Geheimschutzbeauftragten abgestimmt werden müssen.

Themenvorschlag 32:
Werfen Sie einen kritischen Blick auf das Berechtigungsmanagement Ihrer Behörde. Wo sehen Sie (allgemeine) Problematiken? Wie setzen Sie das Berechtigungsmanagement IT-grundschutzkonform um? Auf welche Besonderheiten müssen Sie grundsätzlich achten, welche ergeben sich spezifisch aus Ihrer Behördenstruktur?

Themenvorschlag 33:
Erstellen Sie im Rahmen des Umfangs Ihrer Projektarbeit einen Baustein für einen relevanten Geschäftsprozess bzw. Systems Ihrer Behörde sowie dazu passende Umsetzungshinweise. Nennen Sie Gründe für Ihre Auswahl. Beachten Sie dabei insbesondere die Grundstruktur eines benutzerdefinierten Bausteins und nutzen Sie die BSI-Vorlagen.

Hinweis: Die positive Beurteilung einer Projektarbeit ersetzt nicht eine vollständige QS, ein (Zertifizierungs-)Audit oder sonstige genaue Überprüfungen des zugehörigen vollständigen Projektes.

7.3 Hinweise und Empfehlungen zur Durchführung und Betreuung der Projektarbeiten

Zielsetzung

- Sie sollen mit der Projektarbeit dokumentieren,
  - dass sie im Tätigkeitsbereich des behördlichen Informationssicherheitsmanagements selbstständig konzeptionell arbeiten und
  - die Arbeitsergebnisse dann überzeugend vermitteln, bzw. präsentieren können.

  Eine solche management- und kommunikationsorientierte Aufgabe ist wesentlicher Bestandteil im Aufgabenfeld eines/einer IT-Sicherheitsbeauftragten und im Bereich des behördlichen Informationssicherheitsmanagements.

  Nach der Benennung der fachlichen Begleitung für die Betreuung der Projektarbeit soll die Initiative bei der Erstellung der Projektarbeit immer von der Kandidatin bzw. dem Kandidat ausgehen. Die fachliche Begleitung sollte hinzugezogen werden, wenn fachliche Fragestellungen oder Unsicherheiten auftreten.

Inhalt

- Das Thema der Arbeit kann grundsätzlich frei gewählt werden. Es wird empfohlen, ein Thema aus den Vorschlägen dieses Lernpfades zu wählen. Wenn ein Thema aus diesem Lernpfad in Inhalt und Umfang geändert behandelt werden soll, muss dies im Projektplan dargestellt werden.
- Ob ein Thema für eine Projektarbeit akzeptiert werden kann, entscheidet die BAköV in Abstimmung mit dem BSI nach Eingang des Projektplanes.
- Es empfiehlt sich, die Inhalte der geplanten Arbeit (auch nach Genehmigung des Projektes) am Anfang mit der fachlichen Begleitung abzustimmen. Insbesondere, wenn ein eigenes Thema gewählt wurde, sollte diese Abstimmung erfolgen. Bei den vorgegebenen Themen im Konzept sind Inhalte in Form von Unterpunkten z.T. schon näher spezifiziert.
- In der Arbeit sollte auch sichtbar werden, wie Sie bei der Erstellung vorgegangen sind. Stellen Sie nicht nur eine Lösung vor, sondern beschreiben Sie den Lösungsweg. Welche Probleme hatten Sie bei der Anfertigung und wie haben Sie diese gelöst bzw. wieso waren sie im Rahmen dieser Arbeit nicht lösbar?

Umfang

- Der minimale zeitliche Aufwand der Projektarbeit sollte bei etwa 20 Stunden liegen. Abhängig von der Komplexität des Themas und einer ggfs. vorhandenen Vorarbeit, auf der aufgesetzt wird, kann und darf der Gesamtaufwand höher sein.
- Im Einzelfall sind die Ressourcen (mit der fachlichen Begleitung) im Vorfeld abzuschätzen und evtl. zu prüfen, ob der Aufwand (auch für die fachliche Begleitung) vertretbar ist.
- Für die Aufwendungen der fachlichen Begleitung ist etwa ein Personentag vorgesehen (ohne Teilnahme an der Abschlusspräsentation). Es erscheint sinnvoll, ca. zwei Stunden in die Planung und Abstimmung der Inhalte am Anfang zu investieren. Die weitere Zeit sollte für Rückfragen bzw. Abnahme der Arbeit aufgewendet werden.
- In dem zeitlich begrenzten Rahmen einer solchen Arbeit können nicht immer alle Aspekte eines Themas vollständig bearbeitet werden. In einem solchen Fall sollen nicht behandelte bzw. tangierende Aspekte aufgeführt werden.

Aufbau der Arbeit (ca. 5 bis 10 Seiten, ohne Deckblatt und Verzeichnisse)

1. Anliegen / Einleitung (knappe Beschreibung)
   z. B. Einordnung der Arbeit in das behördliche Informationssicherheitsmanagement; Anlass für die Wahl des Themas; Vorgehensweise bei der Bearbeitung; Abgrenzung des Umfangs
2. Gliederung
3. Hauptteil (Text, Abbildungen, Übersichten etc.)
4. Zusammenfassung
5. Nachweise, Literatur
6. Eidesstattliche Erklärung

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Arbeit tatsächlich, eigenverantwortlich und nur unter Zuhilfenahme der ausgewiesenen Hilfsmittel angefertigt habe. [Ort], den [Datum] [Unterschrift] Vorname Name

Inhalt des Deckblattes

- Name
- Behörde
- Thema
- fachliche Begleitung (Nennung nur mit Zustimmung)
- Zeitraum der Anfertigung

Umfang

ca. 5 - 10 Seiten (exklusive Deckblatt, Inhaltsverzeichnis usw.) - Schrift 12 pt (z. B. Times New Roman, Arial)

Termine

- Nach der Anmeldung zur Fortbildung ist eine baldige Entscheidung für ein Thema zu treffen.
- Besprechung der Arbeit mit der fachlichen Begleitung.
- Vorlage der Arbeit spätestens 3 Wochen vor der Projektpräsentation bei der BAköV. Eine elektronische Abgabe ist möglich.
- Vorbereitung der Präsentation und wenn erforderlich, Unterlagen für die anderen Teilnehmenden. Achtung, die Präsentationszeit beträgt 20 Minuten. Eine zeitliche Überziehung oder eine deutliche Unterschreitung sind zu vermeiden.

7.4 Empfehlungen zur Vorbereitung der Präsentation

Im Rahmen eines Präsentationsworkshops wird die Projektarbeit vorgestellt. An diesem Erfahrungsaustausch nehmen weitere Kandidatinnen und Kandidaten teil, welche die Projektarbeit abgeschlossen haben. Neben der Präsentation und dem Gespräch wird damit eine Plattform für den weiteren Erfahrungsaustausch geöffnet.
Die Projektarbeit wird in einer 20minütigen Präsentation vorgestellt. Zusätzlich sind 10 Minuten für das Gespräch vorgesehen. Eine wesentliche Aufgabe bei der Präsentation besteht darin, die zentralen und wesentlichen Arbeitsergebnisse der Zuhörerschaft überzeugend zu vermitteln.

Die Darstellung sollte sich an folgenden Inhalten orientieren:

- Erläuterung der Projektarbeit und Einordnung in die Agenda/Leitlinie der Behörde.
- Darlegung der Vorgehensweise (fachliches Vorgehen, Absprachen etc.).
- Zusammenfassung der Ergebnisse und wichtige Erfahrungen für die weitere Arbeit.
- Als Modellfall kann man sich z.B. vorstellen, dass man die Aufgabe hat, seiner Behördenleitung in zwanzig Minuten einen Sicherheitsaspekt überzeugend darzustellen, um eine Entscheidung herbeizuführen. (Nicht empfehlenswert wären z. B. weitschweifige oder zu technische Darstellungen in dieser kurzen Zeit.)

Mit der Präsentation und dem Gespräch wird fachliches Wissen, der Lernerfolg und Fähigkeit der Einordnung in die Gesamttätigkeit aufgezeigt.

Hinweise für Präsentationen
Im Rahmen Ihrer Tätigkeit ist immer wieder eine Präsentation von Vorhaben oder Ergebnissen erforderlich. Es empfiehlt sich, für die Präsentation elektronische Medien zu nutzen. Folgende Hinweise haben sich bewährt.

Titel *	**Text**	**Aufzählungstext**
Folientitel auf eine Zeile beschränken	alle Texte sauber formatieren	maximal sechs Aufzählungen pro Folie
Folientitel treffend zum Inhalt wählen	nur Abkürzungen verwenden, die die Zuhörer kennen	je Aufzählungspunkt maximal zwei Zeilen
jeder Folie ihren eigenen aussagekräftigen Titel geben	eine serifenlose Schrift verwenden (20 pt, Überschriften 32 pt, Tabellen 16 pt)	kurze und klare Formulierungen der Aufzählungspunkte mit Hilfe von Verben
auf einen einheitlichen Sprachstil achten	kein Blocksatz, keine Silbentrennung	unnötige Substantive vermeiden

Bilder/Grafiken	**Layout**	**Gliederung**
auf erklärende Funktion achten, keine Dekoration	klare Strukturen schaffen	wiederkehrende Symbole verwenden (Pfeile, Häkchen --)
mit der Farbauswahl harmonisieren	Verwirrendes entfernen oder anpassen	nicht mehr als zwei Gliederungsebenen nutzen
einheitlichen Stil beachten	wichtige Elemente hervorheben	Schrittfolgen deutlich nummerieren
Überzeugungskraft überprüfen	zusammengehörige Elemente gleich gestalten	alle Texte ausreichend gliedern

Die Präsentation bzw. Grundthesen werden an die Teilnehmenden der Veranstaltung weitergegeben. Bei allen Inhalten sind das Urheberrecht und die Barrierefreiheit zu beachten.

* Die vorstehende Übersicht wurde mit freundlicher Genehmigung entnommen: Grundwald, Stefan; Freitag, Thoralf; Witt-Schleuer, Detlef: Zertifizierung im IT-Weiterbildungssystem. Hannover 2005, S. 127

7.5 Formulare (werden online auf der BAköV-Webseite zur Verfügung gestellt)

Plan der Projektarbeit

Änderungs-/Ergänzungsmitteilung

Antrag: Zertifikatsverlängerung