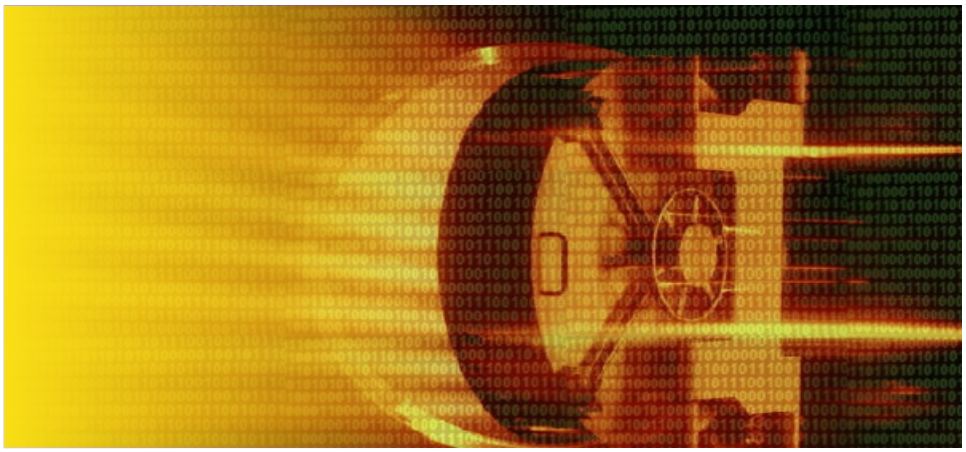
Bundesministerium
des Innern, für Bau
und Heimat

Bundesamt für Sicherheit
in der Informationstechnik

Leitfaden

IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung



Fortbildungsgang der BAköV mit Zertifikat
in Zusammenarbeit mit dem BSI

Leitfaden

IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung

Fortbildungsgang der BAköV mit Zertifikat in Zusammenarbeit mit dem BSI

Brühl / Rheinland Juli 2020
Version 6.4

Dieser Leitfaden wurde erstellt von der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat (BAköV) in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI).
Die Inhalte des Fortbildungsganges 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: http://www.bakoev.bund.de

http://www.ifosbund.de
https://www.lernplattform.intranet.bund.de

Intranet der Bundesregierung (IVBB):
http://www.ivbb.bund.de

Druck: Hochschule des Bundes

Vorwort

Dr. Alexander Eisvogel
Präsident der Bundesakademie

Ein Blick in die Medien zeigt, dass IT-Sicherheit kein Selbstzweck ist. Täglich wird über Ereignisse informiert, welche deutlich machen, dass die Sicherheit der Informationen und Daten zu einem Thema unserer Zeit geworden ist, welches unbedingte Aufmerksamkeit erforderlich macht. Nahezu alle Geschäftsprozesse und Fachaufgaben in der öffentlichen Verwaltung sind von einem sicheren und einwandfreien Betrieb der Informationstechnik abhängig. Diese Abhängigkeit von der Informationssicherheit nimmt weiter zu und stellt die öffentliche Verwaltung vor große Anforderungen.

Neben der Verantwortlichkeit der Behördenleitung für die Informationssicherheit gehört die Festlegung von Verantwortlichkeiten hinsichtlich des Informationssicherheitsmanagements, welche die Benennung von IT-Sicherheitsbeauftragten einschließt.

Der IT-Fortbildung fällt die Aufgabe zu, die Beschäftigten ganzheitlich in allen Kompetenzfeldern zu fördern, die für eine sichere, effektive und effiziente Nutzung der IT-Potenziale in der Verwaltungsarbeit der Bundesbehörden erforderlich sind. Dies schließt die Förderung und Herstellung eines Sicherheitsbewusstseins und einer umfassenden Informationssicherheitskompetenz ein. Die Bandbreite der Informationssicherheitsfragen ist weit gespannt. Nicht nur technische und organisatorische Probleme sind zu klären, sondern es sind auch juristische, wirtschaftliche und gesellschaftliche Antworten zu finden.

In diesem Prozess der Entwicklung der Informationssicherheit in der Bundesverwaltung gewinnt die Tätigkeit und Kompetenz von IT-Sicherheitsbeauftragten und des gesamten IT-Sicherheitsmanagements eine herausragende Bedeutung. Ihre Aufgaben reichen von der Risikoanalyse über die Erstellung und Umsetzung eines Sicherheitskonzeptes bis zur Sensibilisierung und Schulung aller Anwenderinnen und Anwender in Informationssicherheitsfragen. Für ihre Tätigkeit benötigen sie solides Fachwissen, detaillierte Kenntnisse der Strukturen und Abläufe in ihren Behörden sowie ausgeprägte kommunikative Fähigkeiten. Von ihrer Professionalität hängt viel ab.

Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik bietet die Bundesakademie für öffentliche Verwaltung den Fortbildungsgang „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ mit Zertifikat an. Für die Ausübung der Tätigkeit wird ein einheitlicher Qualitätsstandard für den Bund, die Länder und Kommunen gesetzt. Auf diese Weise ist die Fortbildung von IT-Sicherheitsbeauftragten Bestandteil der Sicherheitsstrategie des Bundes und trägt entscheidend dazu bei, dass die Tätigkeit der IT-Sicherheitsbeauftragten in ihren Behörden unterstützt wird.

Wir wünschen den Teilnehmerinnen und Teilnehmern an dieser Fortbildung ein gutes Gelingen und im Interesse der gesamten Bundesverwaltung viel Erfolg in ihrer Tätigkeit.

Dr. Alexander Eisvogel

Präsident der Bundesakademie für öffentliche Verwaltung

Inhaltsverzeichnis

1 Vorbemerkung

Die Bundesregierung hat mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ eine IT-Sicherheitsstrategie vorgelegt. Die Cyber-Sicherheitsstrategie für Deutschland, Kabinettsbeschluss vom Februar 2011, hat den Erfordernissen entsprechend, diese Strategie aktualisiert. Der mit den beiden Beschlüssen verbundene Umsetzungsplan Bund, die Leitlinie für Informationssicherheit in der Bundesverwaltung, (UP Bund) (zuletzt geändert 2017) soll Informationssicherheit mittel- und langfristig auf hohem Niveau in der gesamten Bundesverwaltung gewährleisten.

Der umfassende Schutz in allen sicherheitsrelevanten Bereichen erfordert ein qualifiziertes Sicherheitsmanagement. Zur Gewährleistung des Sicherheitsniveaus wächst die Bedeutung der guten und umfassenden Qualifikation von IT-Sicherheitsbeauftragten und des Informationssicherheits-Teams. Der UP Bund fordert, dass IT-Sicherheitsbeauftragte über ein definiertes Mindestmaß an Fachwissen verfügen und ein Fortbildungsprogramm verpflichtend durchlaufen.

Diesen Anforderungen entsprechend haben die Bundesakademie für öffentliche Verwaltung und das Bundesamt für Sicherheit in der Informationstechnik den Fortbildungsgang „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ und das Angebot des Zertifikatserwerbs entwickelt. Anliegen ist es, auf der Grundlage einer differenzierten Fortbildung eine grundlegende Basis für das Wirken der IT-Sicherheitsbeauftragten und im IT-Sicherheitsmanagement in der Bundesverwaltung und darüber hinaus, herzustellen. Mit diesem Angebot ist die Möglichkeit der behörden- und aufgabenangepassten Fortbildung verbunden.

Die Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat wurde 1969 als zentrale Fortbildungseinrichtung des Bundes gegründet. Sie hat die Aufgabe, in enger Zusammenarbeit mit Verwaltung, Wissenschaft und Wirtschaft Angehörige der Bundesverwaltung praxisnah fortzubilden.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) als die nationale Cyber-Sicherheitsbehörde gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Das BSI ist der zentrale IT-Sicherheitsdienstleister des Bundes.

Mit diesem LEITFADEN werden Informationen und Vorlagen zur Vorbereitung und Durchführung der Fortbildung und Zertifizierung unterbreitet. Die jeweils aktuelle Version des LEITFADEN´s ist unter http://www.bakoev.bund.de/IT-Sicherheitsbeauftragte veröffentlicht.

1.1 Ziel

Anliegen ist es, Beschäftigte für die Tätigkeit der IT-Sicherheitsbeauftragten bzw. im Sicherheitsmanagement zu befähigen, zu zertifizieren und permanent fortzubilden.

Der Fortbildungsgang wendet sich vor allem an Verantwortliche des Sicherheitsmanagements und jene, die die Funktion einer/eines IT-Sicherheitsbeauftragten wahrnehmen oder für die Übernahme dieser Aufgabe vorgesehen sind.

Der Fortbildungsgang richtet sich zunächst an Bedienstete der Bundesverwaltung. Für Bedienstete der Verwaltungen der Bundesländer und Kommunen besteht ein weiteres Angebot (siehe 8. des LEITFADEN´s).

1.2 Überblick

Die Konzeption des Fortbildungsganges geht davon aus, dass die Aufgaben innerhalb der Bundesverwaltung für IT-Sicherheitsbeauftragte vielfältig sind und das Amt laufbahnübergreifend wahrgenommen wird. Ebenfalls wird berücksichtigt, dass hinsichtlich des Wissensstandes, des Aufgabenfeldes bzw. zukünftigen Einsatzgebietes sowie der Erfahrungen, unterschiedliche Voraussetzungen eingebracht werden.

Die Gestaltung der Fortbildung muss flexibel sein und den individuellen Vorkenntnissen, Berufserfahrungen und Aufgabenfeldern Rechnung tragen. Daher ist der Fortbildungsgang modular aufgebaut. Das Erstellen eines Lernpfads (Festlegung der zu besuchenden Seminare) ist im Rahmen eines individuellen Fortbildungsplanes möglich. Neben der Lernprozessbegleitung der BAköV unterstützten fachliche Begleiter den Praktischen Teil (eine Projektarbeit) der Fortbildung. Die fachliche Begleitung, innerhalb der abordnenden Behörde oder bei Bedarf das BSI, unterstützt die Festlegung der Projektaufgabe, begleitet beratend den Erstellungsprozess der Projektarbeit und ggf. die Präsentation des Projektes.

Das Grobkonzept der Fortbildung zum/zur IT-Sicherheitsbeauftragten in der öffentlichen Verwaltung und Zertifizierung umfasst folgende Elemente:

Die Differenzierung in einen Basislehrgang „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Basis“, je nach Bedarf bzw. Aufgabengebiet zu besuchende Aufbauseminare „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Aufbau“ und eine behördenangepasste Spezialisierung „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Expert“ nach Absolvierung der Seminare Basis und Aufbau. Die Teilnahme am Basisseminar erfordert nicht zwingend den Zertifikatserwerb.

- Für die Entscheidung über den individuellen Fortbildungsgang besteht die Möglichkeit, einen Selbsteinschätzungstest (elektronisch, Multiple Choice) durchzuführen.
- Häufig sind IT-Sicherheitsbeauftragte mit der Informationstechnik nicht vertraut. Deshalb wird ein Seminar „Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung – Grundlagen und Anwendung“ zusätzlich angeboten. Dieses Seminar wird auch nur für Frauen angeboten.
- Der Basislehrgang ist modular aufgebaut, d.h. in Abschnitte gegliedert. Die Entscheidung für den Besuch einzelner Abschnitte, das vollständige Basisseminar oder ein Kompaktseminar hängt vom Aufgabenbereich und von den individuellen Vorkenntnissen ab.
- Für den Erwerb des Zertifikats wird die Basisfortbildung ergänzt durch einen praktischen Teil. Mit der Unterstützung der fachlichen Begleitung (aus der abordnenden Behörde oder dem BSI) wird ein Projekt bzw. eine Projektarbeit innerhalb der Behörde bzw. dem Aufgabenbereich erarbeitet. Dieses Projekt wird im Rahmen eines Workshops präsentiert und ist grundsätzlich Voraussetzung für die Prüfung.
- Die Zertifizierung „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis“ schließt mit einer theoretischen Prüfung ab. Die Prüfung (der Abschlusstest) erfolgt in Form eines elektronischen Multiple Choice Tests.
- Aufbauseminare „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Aufbau“ ergänzen zu ausgewählten und aktuellen Schwerpunkten das Seminar „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung –Basis“.
- Das erworbene Basis-Zertifikat ist 5 Jahre gültig. Die Verlängerung des Zertifikats ist nur über eine vorgegebene zu erreichende Punktzahl möglich (siehe 7. des LEITFADEN´s).
- Nach Erlangung des Basis-Zertifikats und Besuch eines Aufbau-Seminars, kann die/der IT-Sicherheitsbeauftragte in einem weiteren Schritt eine tiefergehende behördenangepasste Spezialisierung erlangen. Dafür wird eine weitere qualifizierte Projektarbeit mit „best practice Charakter“ - entwickelt. Auch hier ist der Erwerb eines Zertifikates vorgesehen, das solange gültig ist, wie das Basis-Zertifikat erhalten wird.
- Ab 2021 bietet die BAköV den Basis-Kompaktkurs auch in Form eines **Webinars (IT 497)** an.

Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung – Grundlagen und Anwendung (IT 484 / 485)	Dauer
Die Teilnahme ist fakultativ und hängt von den individuellen Kenntnissen ab (siehe Selbsteinschätzungstest). Dieses Seminar wird auch nur für Frauen angeboten (IT 484). ▪ IT-Systeme – Grundlagen und Arbeitsplatzrechner ▪ IT-Systeme – Netze und Server ▪ Internet und lokale Netze ▪ IT-Anwendungen in der öffentlichen Verwaltung ▪ Informationssicherheit	5 Tage
IT-Sicherheitsbeauftragte – Basis (IT 486)	**Dauer**
Der Besuch der nachfolgenden Abschnitte hängt von den individuellen Vorkenntnissen (individueller Lernpfad) der Teilnehmenden ab.	15 Tage
a) Informationssicherheit – warum? Informationssicherheit – Rechtliche und organisatorische Rahmenbedingungen Sicherheitsmanagement – Standards und Erstellen einer Leitlinie zur Informationssicherheit	5 Tage
b) Maßnahmen für Informationssicherheit Verschlüsselungsverfahren und Elektronische Signatur	5 Tage
c) Entwurf eines Sicherheitskonzepts nach IT-Grundschutz Modernisierung des IT-Grundschutzes und Anwendung Aktuelle Entwicklungen zur Informationssicherheit	5 Tage
IT-Sicherheitsbeauftragte - Basis – Kompakt (IT 487/IT 497)	**Dauer**
Vorausgesetzt werden der Inhalt des Handbuches sowie Kenntnisse in Sicherheitsmaßnahmen am Arbeitsplatz und in Netzen (z.B. Firewall, VPN, Verschlüsselung), die im Abschnitt b erworben werden können. ▪ IT-Grundschutz, bestehend aus den BSI-Standards 200-1, 200-2 und 200-3 und dem IT-Grundschutz-Kompendium	5 Tage
Projektarbeit - Zertifizierung	**Dauer**
Auf der Grundlage der Inhalte des Basisseminars und der Anforderungen an den Aufgabenbereich ist ein überschaubares Projekt innerhalb der Behörde zu absolvieren.	ca. 20 Stunden
Präsentationsworkshop - Zertifizierung (IT 488)	**Dauer**
Die Teilnahme am Workshop ist Voraussetzung für die Prüfung / Zertifizierung. ▪ Vorstellung der Projektarbeit – 30 Minuten Vortrag und Fragen ▪ Erfahrungsaustausch	1 Tag

Test - Zertifizierung (IT 494)	Dauer
▪ Abschlusstest (Multiple Choice) ▪ Verleihung des Zertifikats nach bestandenem Abschlusstest	2,5 Std.
IT-Sicherheitsbeauftragte– Aufbau (IT 489)	**Dauer**
Im Seminar werden Themen behandelt, die u.a. Bestandteil des Basisseminars sind, jedoch im Aufbauseminar vertieft werden, zudem werden neue Inhalte vermittelt. Insbesondere wird im Seminar dem Erfahrungsaustausch, den Übungen und den Gruppenarbeiten ein hohes Gewicht beigemessen. Folgende Inhalte werden im Seminar behandelt: ▪ Informationsquellen und Angebote für IT-Sicherheitsbeauftragte, ▪ Modernisierung des IT-Grundschutzes o Von Maßnahmen zu Anforderungen, o Standards und Verfahren zur Identifikation und Bewertung von Risiken, ▪ Mindeststandards des BSI – Überblick, Umsetzung und Entwicklungen, ▪ Herausforderungen und Lösungen bei IT-Projekten, insbesondere im Kontext von eGovernment-Projekten, ▪ Anforderungen an das Outsourcing und Möglichkeiten der Steuerung externer Dienstleister, o Sicherheitsaspekte bei der Auslagerung von IT-Anwendungen an externe Dienstleister, o Informationssicherheit bei der IT-Konsolidierung des Bundes, o Umgang und Umsetzung von Vereinbarungen (SLAs), o Cloud-Sicherheit – technische und organisatorische Aspekte, ▪ Behandlung von Informationssicherheitsvorfällen (Incident Management), o IT-Sicherheitsmanagement im Incident Management Prozess: Verantwortlichkeiten, Meldepflichten, Meldewege, Schnittstellen, o IT-Forensik - Zusammenhang mit den Aufgaben des IT-Sicherheitsmanagements, o Penetrationstests - rechtliche Rahmenbedingungen, Zielsetzung, Durchführung und Auswertung, ▪ Verfahren und Modelle zum Messen und Bewerten des Reifegrades der Informationssicherheit, o Verfahren zur Effektivitäts- und Effizienzkontrolle des ISMS im Überblick, o IS-Revision – vorbereiten, durchführen, auswerten, Bedeutung in der Bundesverwaltung, o Bewertungskriterien und Kennzahlen für ausgewählte Aspekte	5 Tage

der Informationssicherheit,
    - Einführung in die Arbeitshilfe „Konzeptions- und Auswertungs-Tool für Erhebungen - KATE“,
- wesentliche Aspekte der physischen Absicherung von Infrastrukturen, Betriebsräumen von IT-Systemen und Gebäuden,
- Sensibilisierung für Informationssicherheit als Prozess.

IT-Sicherheitsbeauftragte – Expert (IT 490)

Im Rahmen dieser Fortbildungsmaßnahme wird eine qualifizierte weitere Projektarbeit zu aktuellen Themen der Informationssicherheit, welche nicht schon umfassend im Behördenumfeld behandelt / beschrieben worden sind entwickelt. Diese Themen müssen geeignet sein, als „Best- Practice“ genutzt zu werden. Die Projektarbeit soll vorrangig ohne externe Begleitung selbstständig erstellt werden. Das BSI steht aber gerne im Bedarfsfall als fachliche Ansprechstelle zur Verfügung. Nach der Erstellung ist die Arbeit vor dem Prüfungsausschuss der BAköV und des BSI in einem 30 minütigen Vortrag zu präsentieren. Die Projektarbeit muss innerhalb von zwei Jahren nach Fertigstellung auf der Jahrestagung der IT-Sicherheitsbeauftragten vorgestellt werden.

2 Informationssicherheitsmanagement

Der Umfang des Informationssicherheitsmanagements, der Tätigkeit von IT-Sicherheitsbeauftragten und des Informationssicherheits-Teams ist in den BSI-Standards umfassend beschrieben und dient als Orientierung für die Konzeption der Fortbildung.

Das Anforderungsprofil für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung muss konkret und individuell an die behördenspezifischen Gegebenheiten angepasst werden können. Für die Erledigung der Aufgaben sind sowohl fachliche als auch persönliche Anforderungen zu bewältigen. Dem entsprechend wird eine thematisch breite Fortbildung angeboten.

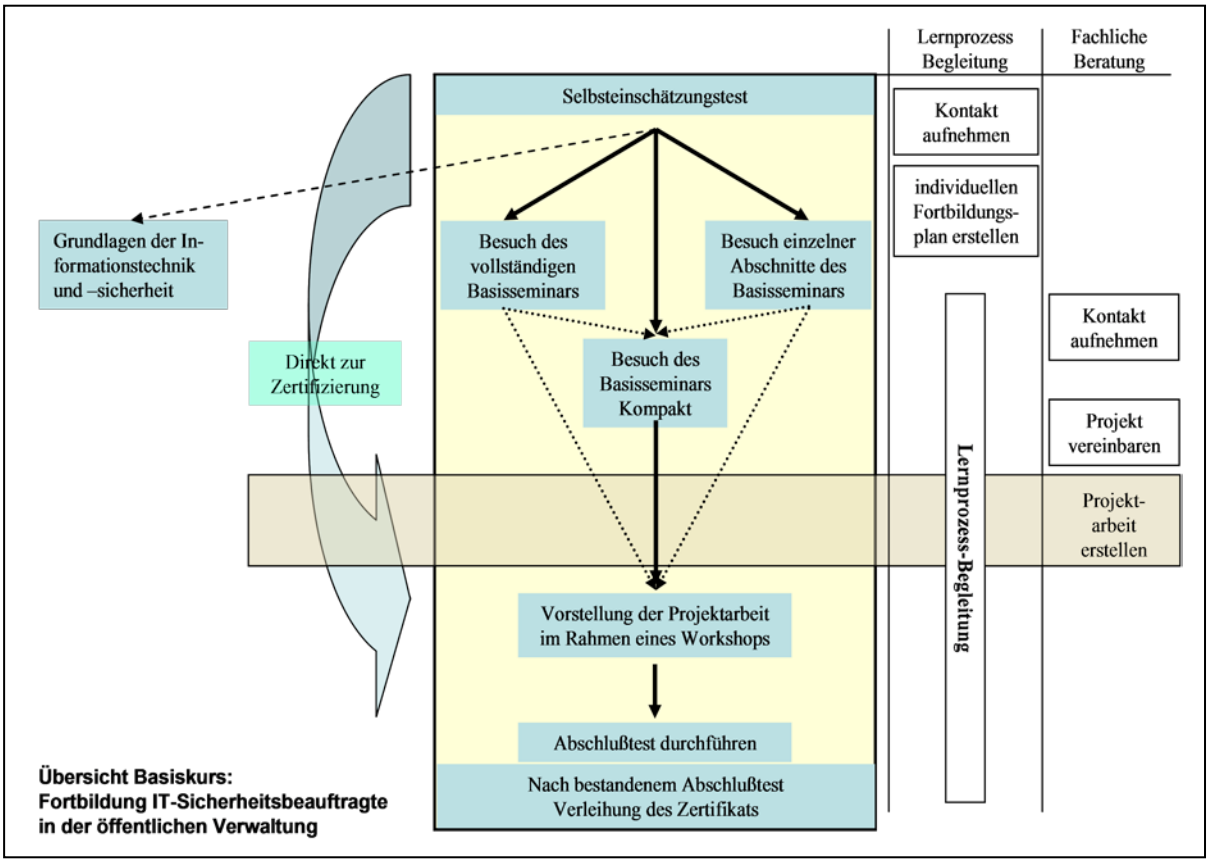
Die Übersicht im Anhang (9.1) gibt einen Überblick über Fachgebiete, welche für die unterschiedlichen Bereiche erforderlich sind, und gleichzeitig die Möglichkeit, die persönliche Kompetenz abzuschätzen. Damit ist eine Ergänzung zum Selbsteinschätzungstest gegeben.

3 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.

Im Rahmen eines **Fortbildungsantrages** ist die Möglichkeit gegeben, selbstständig über den Erwerb des Zertifikats zu entscheiden. Eine **Lernprozessbegleitung** der BAköV, ein **Selbsteinschätzungstest** und die **Seminarübersicht** stehen als Entscheidungshilfe zur Verfügung

Alle in der Zielgruppe genannten Angehörigen der Bundesverwaltung sind nach vorheriger Anmeldung der Behörde und Vereinbarung des Fortbildungsganges (Fortbildungsplan) zur kostenfreien Teilnahme berechtigt.



3.1 Selbsteinschätzungstest

Zur Überprüfung der Kenntnisse besteht die Möglichkeit, einen Selbsteinschätzungstest zu absolvieren. Der Test ist freiwillig, anonym und kann jederzeit wiederholt werden. Der Test wird online unter http://www.bakoev.bund.de/IT-Sicherheitsbeauftragte zur Verfügung gestellt und ist nach Registrierung auf der Lernplattform https://www.lernplattform.intranet.bund.de möglich.

Der Selbsteinschätzungstest unterstützt die Beurteilung der Vorkenntnisse und verdeutlicht die Prüfungsanforderungen und damit die Einschätzung des individuellen Fortbildungsbedarfs. Dieser Test ist ein Hilfsmittel zur eigenen Orientierung und sollte unbedingt durch das Gespräch mit der Lernprozessbegleitung ergänzt werden.

3.2 Fortbildungsantrag

Neben dem Selbsteinschätzungstest und dem Anforderungsprofil unterstützt die Lernprozessbegleitung Interessenten, den individuellen **Fortbildungsplan** festzulegen. Dieser ist Bestandteil des Fortbildungsantrages.

Der Fortbildungsantrag dient der vollständigen Dokumentation des individuellen Fortbildungsganges und wird bei der Zertifizierung herangezogen.

Kern des Dokumentes bildet der Fortbildungsplan. Diesen bespricht der/die Antragsteller/in zuerst mit der Fortbildungsstelle und wenn erforderlich, mit dem/der Vorgesetzten bzw. der Behördenleitung. Dieser Plan entsteht auf der Basis der persönlichen Einschätzung. Es besteht die Möglichkeit, die Lernprozessbegleitung der BAköV in Anspruch zu nehmen.

Der Antrag wird mit dem gewünschten Fortbildungsplan der BAköV zugeleitet. Über die Fortbildungsbeauftragten erfolgt eine Rückmeldung, welche Teilnahme zu welchem Zeitpunkt ermöglicht wird. Mit der Bestätigung der Lernprozessbegleitung erfolgt eine verbindliche Zusage der Teilnahme. Die Anmeldung an den Seminaren bzw. Abschnitten muss durch die Fortbildungsstelle in IFOS-BUND zusätzlich erfolgen.

Die abschließende Erklärung der Antragstellenden enthält die Kenntnisnahme der Prüfungsordnung und die Datenschutzerklärung.

Das Thema und Plan der Projektarbeit für die Zertifizierung wird mit der Fachlichen Begleitung besprochen und vom BSI bestätigt.

Änderungen werden über weitere Formulare mitgeteilt.

Die Formulare sind im Anhang des LEITFADEN´s enthalten und stehen im Internet unter http://www.bakoev.bund.de/IT-Sicherheitsbeauftragte zum Abruf zur Verfügung.

3.3 Lernprozessbegleitung

Die Lernprozessbegleitung der BAköV steht zur Auskunft und Beratung, sowohl für die Fortbildungsbeauftragten als auch die Teilnehmenden zur Verfügung. Die Lernprozessbegleitung berät bei der Erstellung des individuellen Lernplanes, koordiniert, unterstützt den individuell festlegten Fortbildungsgang und steht als Ansprechperson für weitere Qualifizierungen zur Verfügung.

Gleichzeitig vermittelt die Lernprozessbegleitung der BAköV auch Anfragen für eine Begleitung durch das BSI.

Die BAköV sichert die notwendige Dokumentation entsprechend der rechtlichen Grundlagen.

3.4 Fachliche Begleitung

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 der Informationssicherheit und ggf. die Präsentation. Das BSI bestätigt die Themenwahl. Die Begleitung sollte vorzugsweise bei der entsendenden Behörde erfolgen, um im Idealfall eine hohe Nähe der Projektarbeit zum Arbeitsfeld Informationssicherheit herzustellen. Die Entscheidung darüber wird vom Kandidaten bzw. von der Kandidatin getroffen.

3.5 Arten der Fortbildung und Zertifizierung

Das Gesamtkonzept der Fortbildung für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung (IT-SiBöV) beinhaltet

- das Seminar „IT-Sicherheitsbeauftragte Basis“ –als modular aufgebautes Seminar oder Kompaktseminar,
- nach Bedarf bzw. Aufgabengebiet zu besuchende Aufbauseminare „IT-Sicherheitsbeauftragte - Aufbau“ und
- eine behördenangepasste Spezialisierung „IT-Sicherheitsbeauftragte - Expert“ nach Absolvierung der Basis- und Aufbauseminare. Im Rahmen dieser Fortbildungsmaßnahme wird eine weitere qualifizierte Projektarbeit zu aktuellen Themen der Informationssicherheit, welche nicht schon umfassend im Behördenumfeld behandelt / beschrieben worden sind entwickelt.

Für die Basis wird nach erfolgreicher Prüfung ein Zertifikat ausgehändigt. Zum Erhalt bzw. zur Verlängerung des Zertifikats sind verschiedene Fortbildungsmaßnahmen erforderlich. Der Erwerb eines Zertifikats erfolgt nach Erfüllung aller Voraussetzungen. Der Erhalt des Expert-Zertifikats ist an den Erhalt des Basis-Zertifikats gebunden. Die Voraussetzungen für den Zertifikatserwerb sind in der Übersicht des Anforderungsprofils und der Prüfungsordnung enthalten.

4 Grundlagen

Grundlagenwissen zur Informationstechnik und Informationssicherheit kann in einem gesonderten Kurs erworben werden. Dieses Seminar, dass auch nur für Frauen angeboten wird (IT 484), hat für Teilnehmende, welche über geringe Kenntnisse in diesem Bereich verfügen, den Charakter eines Vorkurses. Die Durchführung des Selbsteinschätzungstests erübrigt sich in diesem Fall.

Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung – Grundlagen und Anwendung	IT 484/485	Dauer
▪ IT-Systeme – Grundlagen und Arbeitsplatzrechner ▪ IT-Systeme – Netze und Server ▪ Internet und lokale Netze ▪ IT-Anwendungen in der öffentlichen Verwaltung ▪ Informationssicherheit		5 Tage

5 IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung

Der Besuch der Seminare bzw. Abschnitte hängt von den individuellen Vorkenntnissen ab und wird im persönlichen Fortbildungsplan festgelegt.

Folgende Auswahl steht zur Verfügung:

1. Besuch des gesamten Basisseminars.
2. Besuche einzelner Abschnitte des Basisseminars.
3. Besuch des Basisseminars/Basiswebinars - Kompakt.
4. Im Rahmen der Zertifizierung ist die direkte Anmeldung, nach Absolvierung der Projektarbeit und deren Präsentation in einem Workshop, zur Prüfung für den Zertifikatserwerb möglich.

IT-Sicherheitsbeauftragte – Basis	IT 486	Dauer
a) Informationssicherheit – warum? Informationssicherheit– Rechtliche und organisatorische Rahmenbedingungen Sicherheitsmanagement – Standards und Erstellen einer Leitlinie zur Informationssicherheit		5 Tage
b) Maßnahmen für Informationssicherheit Verschlüsselungsverfahren und Elektronische Signatur		5 Tage
c) Entwurf eines Sicherheitskonzepts nach IT-Grundschutz Modernisierung des IT-Grundschutzes und Anwendung Aktuelle Entwicklungen zur Informationssicherheit		5 Tage

5.1 Theoretischer Teil

Die Inhalte der Seminare /Webinare sind mit dem Handbuch und dem Abschlusstest der Zertifizierung abgestimmt. Damit ist gegeben, dass ein fachliches Wissen vermittelt wird, welches Grundlage und gleichzeitig einheitliche Basis für das Wirken im Informationssicherheitsmanagement ist.

Im Anhang 9.2 sind die Inhalte der Seminare und deren Abschnitte zur Feststellung der eigenen Kenntnisse und Entscheidungsunterstützung aufgeführt. Der zeitliche Umfang der Behandlung der Abschnitte ist in der oben stehenden Übersicht enthalten.

5.1.1 IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis

IT 486	**IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis**
Ziel	Die Teilnehmenden sollen • die Befähigung für ihre Aufgaben als IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung entwickeln, • dazu die erforderlichen organisatorischen und methodischen Qualifikationen aufbauen und • informationstechnisches Wissen und Kenntnisse über Vorgaben aus Gesetzen und Standards erwerben. Die Teilnehmenden lernen • verantwortlich im Informationssicherheitsprozess im Sicherheitsmanagement mitzuwirken, • eine Leitlinie zur Informationssicherheit und ein Sicherheitskonzept zu erstellen, • IT-Sicherheitsmaßnahmen zu überprüfen und • den Umgang mit Störfällen zu planen.

5.1.2 IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis Kompakt

Das fünftägige Seminar/Webinar„IT-Sicherheitsbeauftragte - Basis - Kompakt“ ermög-licht, vorhandene Kenntnisse besonders im Bereich IT-Grundschutz zu aktuali-sieren. Den Teilnehmenden des Basisseminars steht dieses ebenfalls offen. Vorausgesetzt werden der Inhalt des Handbuches „IT-Sicherheits beauftragte in der öffentlichen Verwaltung“ sowie Kenntnisse in technischen Sicherheitsmaßnahmen am Arbeitsplatz und in Netzen, die im Abschnitt b des Basisseminars erworben werden können.

IT-Sicherheitsbeauftragte - Basis – Kompakt IT 487 /IT 497	Dauer
▪ Informationssicherheit - Anforderungen und aktuelle Entwicklungen ▪ Rechtliche und organisatorische Rahmenbedingungen für Informationssicherheit ▪ Datenschutz und Informationssicherheit ▪ Standards und Zertifizierung ▪ Sicherheitsmanagement und Informationssicherheitsleitlinie ▪ Informationssicherheit nach IT-Grundschutz ▪ Sensibilisierungs- und Schulungskonzept ▪ Meldewege, Behandlung von Sicherheitsvorfällen und Notfallvorsorge ▪ Reifegradmessung, Aufrechterhaltung der Informationssicherheit und Revision ▪ IT-Sicherheitsbeauftragte im Sicherheitsmanagement - Kommunikation und Kooperation ▪ Aktuelle Entwicklungen in der Modernisierung des IT-Grundschutzes und deren Anwendung ▪ Berichterstattung und Präsentation von Arbeitsergebnissen	5 Tage

5.1.3 Bereitstellung eines Handbuches

Ein Handbuch für den Basislehrgang „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Basis“ wird jedem Teilnehmenden ausgehändigt. Dieses ist inhaltlich den Schwerpunkten des Basislehrganges angepasst und dient der grundlegenden Orientierung. Es enthält kurze Erörterungen, Verweise auf weiterführende Literatur und Internetlinks und kann als Nachschlagewerk für IT-Sicherheitsbeauftragte genutzt werden.

Gleichzeitig werden für die besuchten Seminare ergänzende Unterlagen zur Verfügung gestellt.

5.2 Projektarbeit

Im praktischen Teil der Zertifizierung IT-Sicherheitsbeauftragte – Basis 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“ über die BAköV an das BSI gesandt und von dort beschieden. Der Zeit-

aufwand des Projektes sollte mindestens 20 Stunden (ohne Vorbereitung der Präsentation) umfassen. Der Umfang des Projektes wird mit der fachlichen Begleitung besprochen und die Dokumentation (siehe 9.5 des Leitfadens) sollte ca. 20 Seiten umfassen.

Im Anhang 9.4 des LEITFADEN´s ist eine Übersicht von Themenvorschlägen enthalten.

Projektarbeit	Dauer
Auf der Grundlage der Inhalte des Basisseminars bzw. Inhalte des Handbuches und den Anforderungen aus dem Aufgabenbereich ist ein überschaubares Projekt innerhalb der Behörde zu absolvieren.	mindestens 20 Stunden

Hinweis:

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

5.3 Workshop Projektpräsentation

Die Präsentation der Projektarbeit erfolgt in einem Workshop (IT 488) der Bundesakademie, der ggf. nach vorheriger Abstimmung auch in Form einer Videokonferenz stattfinden kann. Die Abgabe der Arbeit muss **ausnahmslos** spätestens **drei** Wochen vor dem Workshop erfolgen. Eine elektronische Abgabe an die Mailadresse (sibe-lg5@bakoev.bund.de) ist möglich. Die Papierform muss am Workshoptermin vorliegen. Alle Teilnehmenden präsentieren ihre Projektarbeit und führen ein Gespräch darüber. Dieses Gespräch wird - die Präsentation ein-geschlossen - jeweils einen Zeitraum von etwa 30 Minuten beanspruchen. Der Workshop wird von der BAköV und dem BSI moderiert. **Siehe auch den Hin-weis auf Seite 58.**

Die Teilnahme am Workshop ist verpflichtend und grundsätzlich Voraussetzung der Prüfung zur Zertifizierung.

5.4 Prüfung und Zertifizierung

Im Rahmen der Prüfung wird im Abschlusstest das Verständnis für fachliche Zusammenhänge nachgewiesen. Der Test umfasst insgesamt 120 Fragen und wird in elektronischer Form dargestellt (Multiple Choice). Umfang und Schwierigkeitsgrad der Testfragen orientieren sich an den inhaltlichen Schwerpunkten des Basisseminars bzw. dem Handbuch.

Nach bestandener Prüfung wird das Zertifikat: „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis“ erteilt.

Das mit der Prüfung erworbene Zertifikat ist 5 Jahre gültig. Der Erhalt bzw. die Verlängerung des Zertifikats ist über eine vorgegebene zu erreichende Punktzahl oder alternativ über einer Wiederholung der Prüfung möglich. Hierfür werden mit dem Blick auf einen Kompetenzerhalt Seminare/Webinare und Veranstaltungen (mit Erfahrungsaustausch) von der BAköV angeboten (siehe 9.1 Anforderungsprofil und 7. Zertifikatserhalt).

6 Behördenangepasste Fortbildung

6.1 IT-Sicherheitsbeauftragte – Aufbau

Das Seminar „IT-Sicherheitsbeauftragte – Aufbau“ setzt inhaltlich auf entsprechende Abschnitte des Basisseminars „IT-Sicherheitsbeauftragte – Basis“ auf. Es wird die Möglichkeit eröffnet, Wissen für die Tätigkeiten als IT-Sicherheitsbeauftragte zu speziellen und aktuellen Themen der IT-Sicherheit und -Organisation zu erwerben.

IT-Sicherheitsbeauftragte – Aufbau IT 489	Dauer
Im Seminar werden Themen behandelt, die u.a. Bestandteil des Basiskurses sind, jedoch im Aufbaukurs vertieft werden, zudem werden neue Inhalte vermittelt. Insbesondere wird im Kurs dem Erfahrungsaustausch, den Übungen und den Gruppenarbeiten ein hohes Gewicht beigemessen. Folgende Inhalte werden im Seminar behandelt: ▪ Informationsquellen und Angebote für IT-Sicherheitsbeauftragte, ▪ Modernisierung des IT-Grundschutzes o Von Maßnahmen zu Anforderungen, o Standards und Verfahren zur Identifikation und Bewertung von Risiken, ▪ Mindeststandards des BSI – Überblick, Umsetzung und Entwicklungen, ▪ Herausforderungen und Lösungen bei IT-Projekten, z.B.im Kontext von eGovernment-Projekten, ▪ Anforderungen an das Outsourcing und Möglichkeiten der Steuerung externer Dienstleister, o Sicherheitsaspekte bei der Auslagerung von IT-Anwendungen an externe Dienstleister, o Informationssicherheit bei der IT-Konsolidierung des Bundes, o Umgang und Umsetzung von Vereinbarungen (SLAs), o Cloud-Sicherheit – technische und organisatorische	5 Tage

Aspekte, ▪ Behandlung von Informationssicherheitsvorfällen (Incident Management), o IT-Sicherheitsmanagement im Incident Management Prozess: Verantwortlichkeiten, Meldepflichten, Meldewege, Schnittstellen, o IT-Forensik - Zusammenhang mit den Aufgaben des IT-Sicherheitsmanagements, o Penetrationstests - rechtliche Rahmenbedingungen, Zielsetzung, Durchführung und Auswertung, ▪ Verfahren und Modelle zum Messen und Bewerten des Reifegrades der Informationssicherheit, o Verfahren zur Effektivitäts- und Effizienzkontrolle des ISMS im Überblick, o IS-Revision – vorbereiten, durchführen, auswerten, Bedeutung in der Bundesverwaltung, o Bewertungskriterien und Kennzahlen für ausgewählte Aspekte der Informationssicherheit, o Einführung in die Arbeitshilfe „Konzeptions- und Auswertungs-Tool für Erhebungen - KATE“, ▪ wesentliche Aspekte der physischen Absicherung von Infrastrukturen, Betriebsräumen von IT-Systemen und Gebäuden, ▪ Sensibilisierung für Informationssicherheit als Prozess.	

Das Aufbauseminar hat eigenständige Inhalte (siehe. 9.1 Anforderungsprofil).

6.2 IT-Sicherheitsbeauftragte – Expert

Je nach Aufgabengebiet und Erfordernis kann in einem weiteren Schritt nach Absolvierung der Basis- und Aufbaufortbildung eine behördenangepasste Spezialisierung erfolgen und mit einschlägiger Berufserfahrung einhergehen.

Das Thema muss geeignet sein, als „Best Practice“ genutzt zu werden. Die Projektarbeit soll vorrangig ohne externe Begleitung selbstständig erstellt werden. Das BSI steht aber gerne im Bedarfsfall als fachliche Ansprechstelle zur Verfügung. Nach der Erstellung ist die Arbeit vor dem Prüfungsausschuss der BAköV und des BSI in einem 30 minütigen Vortrag zu präsentieren. Die Projektarbeit muss innerhalb von zwei Jahren nach Fertigstellung auf der Jahrestagung der IT-Sicherheitsbeauftragten vorgestellt werden.
Der Erwerb eines Zertifikats erfolgt nach Erfüllung aller Voraussetzungen. Der Erhalt des Zertifikats ist an den Erhalt des Basis-Zertifikats gebunden. Der Antrag erfolgt über die BAköV.

IT-Sicherheitsbeauftragte – Expert IT 490

Vorgehensweise für die Absolvierung:

1) Interesse bekunden

Formlose Anfrage bei der BAköV (sibe-lg5@bakoev.bund.de). Der/die Antragsteller/in muss an der Basis- und Aufbaufortbildung teilgenommen haben und über das Basis-Zertifikat und über einschlägige Berufserfahrung verfügen. Die Interessenbekundung wird an das BSI weitergeleitet. Es wird empfohlen, das Vorhaben und dessen Umfang vorab mit dem/der Fortbildungsbeauftragten der Behörde und dem (Ressort-) IT-SiBe zu besprechen.

2) Projektantrag

Der ausgefüllte Antrag wird der Fortbildungsstelle vorgelegt. Diese trifft alle notwendigen Absprachen in der Behörde. Zusendung des unterzeichneten Antrages und der Projektbeschreibung an die BAköV-Zertifizierungsstelle.

Die BAköV sendet den Projektantrag an das BSI. Zwischen BAköV und BSI werden u.a. folgende Punkte besprochen: Festlegung des Projektthemas, der Ansprechpersonen, Zeitraum der Fertigstellung, inhaltlicher Umfang. Das BSI bestätigt der BAköV die Themenauswahl und nimmt bei Rücksprachebedarf ggf. mit dem/der Antragsteller/in Kontakt auf.

3) Projektarbeit zu aktuellen Themen der Informationssicherheit, welche nicht schon umfassend im Behördenumfeld behandelt/beschrieben worden sind.

Eigenständige Erarbeitung der Arbeit im festgelegten Zeitraum, ggf. mit dem BSI als fachliche Ansprechstelle und evtl. Unterstützung des (Ressort-) IT-SiBe. Die Arbeit sollte ca. 30 Seiten ohne Deckblatt, Abbildungen und Anhang umfassen.

4) Präsentation und Vortrag auf der Jahrestagung der IT-Sicherheitsbeauftragten

Nach der Erstellung ist die Arbeit vor dem Prüfungsausschuss der BAköV und des BSI in einem 30 minütigen Vortrag zu präsentieren. Anschließend erhält der/die Vortragende eine Rückmeldung, die sich auf die Art und Weise des Vortrags und der Ausarbeitung, sowie auf inhaltliche Fragen beziehen kann. Die Projektarbeit muss innerhalb von zwei Jahren nach Fertigstellung auf der Jahrestagung der IT-Sicherheitsbeauftragten vorgestellt werden.

6.3 Jahrestagung für IT-Sicherheitsbeauftragte

Zusätzlich wird den IT-Sicherheitsbeauftragten eine auf ihr Tätigkeitsfeld zugeschnittene jährliche Veranstaltung angeboten „Jahrestagung für IT-Sicherheitsbeauftragte in der Bundesverwaltung“ (SO 505).

Diese Veranstaltung bildet den Mittelpunkt eines Forums für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung. Deren Besuch ist gleichzeitig Schwerpunkt des Zertifikatserhalts.

Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden	SO 505

Anliegen ist es, den IT-Sicherheitsbeauftragten aktuelle Informationen

- über die Entwicklungen und Trends in der IT-Sicherheit in der Bundesverwaltung,
- darüber hinaus gehende Entwicklungen der Informationssicherheit und
- über Entwicklungen des BSI zu geben.

Des Weiteren ist eine Basis für den Erfahrungsaustausch gewährleistet.

7 Zertifikatserhalt und ergänzende Fortbildung

Informationssicherheit unterliegt einem ständigen Wandel, ebenso das rechtliche und organisatorische Arbeitsumfeld, in dem IT-Sicherheitsbeauftragte tätig sind. Zur Erhaltung der Qualifikation wird daher 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 Seminare/ Webinare der BAköV ermöglicht.

Zum Erhalt oder zur jeweiligen Verlängerung des Basis-Zertifikats werden verschiedene Maßnahmen angeboten.

Das Zertifikat Expert bleibt solange gültig, wie das Basis-Zertifikat erhalten wird.

Eine nochmalige Prüfung zum Erhalt des Basis-Zertifikats ist alternativ möglich, wenn die erforderlichen Punkte nicht erreicht wurden.

Punktesystem für den Werterhalt des Basis-Zertifikats

Innerhalb von 5 Jahren müssen 40 Punkte erreicht werden. Die zweimalige Teilnahme an der „Jahrestagung für IT-Sicherheitsbeauftragte“ ist für Bundesbedienstete und Bedienstete der Länder und Kommunen Bedingung.

Die Punkte sind über folgende Maßnahmen zu erreichen	**Punkte**
Teilnahme an der jährlich stattfindenden „Jahrestagung für IT-Sicherheitsbeauftragte der Bundesbehörden“	15
Teilnahme an Seminaren/Webinaren der BAköV aus dem Bereich Informationssicherheit. Hier wird ebenfalls der Besuch der „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Aufbau“ bewertet.	13
Teilnahme an anderen Seminaren/Webinaren der BAköV	12
Teilnahme an Seminaren /Webinaren von externen Anbietern und Kongressen im Bereich Informationssicherheit, z.B. BSI-Grundschutztag oder BSI-Sicherheitskongress. (Anerkennung nur nach Absprache mit der BAköV)	8
Teilnahme an anderen Seminaren/Webinaren von externen Anbietern (Anerkennung nur nach Absprache mit der BAköV)	5
Zusätzlicher Punkteerhalt für Landes- bzw. Kommunalbedienstete	
Teilnahme an der jährlich stattfindenden „Jahrestagung für IT-Sicherheitsbeauftragte der Landes- und Kommunalbehörden	15

Die Zertifikatsverlängerung ist nur auf schriftlichen Antrag möglich. Der Antrag soll 3 Monate vor Ablauf des Zertifikats vorliegen.

8 Fortbildung / Zertifizierung für IT Sicherheitsbeauftragte in den Ländern und Kommunen

Im Rahmen einer "Sommerakademie IT-Sicherheit" wird ein Fortbildungsgang "IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Basis" für Bedienstete aus den Bundesländern und Kommunen angeboten. Während der insgesamt 3-wöchigen Veranstaltung wird das Basiswissen für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung vermittelt. Für den Zertifikatserwerb ist ein Antrag zu stellen. Es gilt die Prüfungsordnung (siehe 9.3. des LEITFADEN`s).

Ein Besuch einzelner Abschnitte ist ebenfalls möglich, deren Teilnahme bescheinigt wird. Die Fortbildung und Zertifizierung werden von der BAköV durchgeführt und sind kostenpflichtig.

Weitere Informationen sind unter
http://www.bakoev.bund.de/Sommerakademie verfügbar.

Basiskompetenz zur Zertifizierung für Bedienstete in der Verwaltung der Länder und der Kommunen

Auf der Grundlage der BSI-Standards 200-1 bis 200-3 und den Anforderungen aus dem Aufgabenbereich IT-Sicherheit ist ein überschaubares Projekt innerhalb der eigenen Behörde in Zusammenarbeit mit einer fachlichen Begleitung aus der eigenen Behörde oder einer externen Stelle zu absolvieren (vgl. LEITFADEN 5.2 u. 3.4). Die Themenvorschläge aus dem LEITFADEN können für die Arbeit herangezogen werden. Zur Bestätigung des Projektthemas wird der Antrag „**Plan der Projektarbeit**“ über die Bundesakademie an das BSI gesandt und dort beschieden. Die Präsentation der Projektarbeit erfolgt in einem Workshop der Bundesakademie, an dem Vertreter/innen des BSI teilnehmen. Die Abgabe der Arbeit muss **ausnahmslos** spätestens **drei** Wochen vor dem Workshop erfolgen. Eine elektronische Abgabe (sibe-lg5@bakoev.bund.de) ist möglich. Die Papierform muss spätestens zum Workshop vorliegen.

Damit sind die Voraussetzungen für eine Einladung zur Abschlussprüfung/Abschlusstest gegeben, in deren Rahmen das Verständnis für fachliche Zusammenhänge nachzuweisen ist.

Für die Prüfung wird eine Gebühr erhoben.

Nach erfolgreicher Absolvierung der Abschlussprüfung wird das Zertifikat “IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis“ vergeben.

Das Zertifikat ist 5 Jahre gültig.

9 ANHANG

9.1 Anhang zu 2. (Anforderungsprofil)

9.2 Anhang zu 5.1 (Theoretischer Teil)

9.3 Prüfungsordnung

9.4 Themenvorschläge für die Projektarbeit

9.5 Empfehlungen zur Anfertigung der Projektarbeit

9.6 Empfehlungen zur Vorbereitung der Präsentation

9.7 Formulare für IT-SiBöV

Fortbildungsantrag – Basis

Datenschutzerklärung

Plan der Projektarbeit - Antrag

Änderungs- / Ergänzungsmitteilung

Fortbildungsantrag - Aufbau

Fortbildungsantrag - Expert

Antrag: Zertifikatsverlängerung

Muster Zertifikat

9.1 Anhang zu 2. (Anforderungsprofil)

Diese Übersicht soll einen Überblick über Fachgebiete ermöglichen, welche für die unterschiedlichen Bereiche erforderlich sind und gleichzeitig die Möglichkeit geben, die persönliche Kompetenz abzuschätzen. Damit ist eine Ergänzung zum Selbsteinschätzungstest gegeben.

Die genannten Fachkompetenzen bzw. Inhalte finden sich in den Seminaren bzw. im Gesamtfortbildungskonzept wieder. So entsprechen die

- **Basiskompetenzen** - den fachlichen Anforderungen (Seminarinhalte) „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis“,
- **Aufbaukompetenzen** - den fachlichen Anforderungen „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Aufbau“ und die
- **Ergänzenden Kompetenzen** - jenen Anforderungen, welche weitere Qualifikationen umfassen.

Sollte sowohl die Basiskompetenz als auch die Ergänzende Kompetenz angekreuzt sein, ist dies ein Hinweis darauf, dass dieser Inhalt in dem genannten Seminar vertieft wird.

Das Anforderungsprofil findet seinen Niederschlag vor allem in dem Seminarangebot der BAköV. Aus diesem Grunde sind direkt die entsprechenden Jahresarbeitsprogramm-Nummern (JAP-Nummern) eingefügt. Das BAköV Angebot (www.ifosbund.de) in Fettdruck betreffen ausschließlich Seminare des Fortbildungsganges „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“.

Fachkompetenzen	**Basis**	**Aufbau**	**Ergänzend**	**BAköV Angebot**
		behördenangepasst		
Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung – Grundlagen und Anwendung				**IT 484 IT 485**
IT-Systeme – Grundlagen und Arbeitsplatzrechner	**X**			**IT 484 IT 485**
IT-Systeme – Netze und Server	**X**			**IT 484 IT 485**
Internet und lokale Netze	**X**			**IT 484 IT 485**
IT-Anwendungen in der öffentlichen Verwaltung	**X**			**IT 484 IT 485**

Fachkompetenzen	Basis	Aufbau	Ergän-zend	BAköV Angebot
	Stan-dard	behördenangepasst		
Informationssicherheit - warum? (Abschnitt a)				**IT 486a**
Gefährdungen und Risiken der IT	**X**			**IT 486a**
Bedrohungen für IT und Informa-tionen	**X**			**IT 486a**
Gefährdungen und Schwachstellen	**X**			**IT 486a**
Sicherheitsanforderungen und Schutzbedarf	**X**			**IT 486a**
Grundwerte und –begriffe der Informationssicherheit	**X**			**IT 486a**
Definition der Informations-sicherheit	**X**			**IT 486a**
Leitlinien und Dienstanweisungen	**X**			**IT 486a**
IT-Sicherheitsstrategie des Bundes	**X**			**IT 486a**
BSI und CERT-Bund	**X**			**IT 486a**
Anforderungen an IT-Sicherheits-beauftragte	**X**			**IT 486a**
Schulungs- und Sensibilisierungs-maßnahmen	**X**		**X**	**IT 486a IT 410/414**
Erkennen und Behandlung von IT-Sicherheitsvorfällen	**X**			**IT 486a**
Computer-Notfallteam	**X**			**IT 486a**
Anforderungen in den Netzen des Bundes	**X**			**IT 486a**
Anforderungen an ganzheitliche Informationssicherheit	**X**			**IT 486a**
Informationssicherheit - Rechtliche und organisatorische Rahmenbe-dingungen (Abschnitt a)				**IT 486a**
Relevante Vorgaben aus Gesetzen	**X**			**IT 486a**
Verantwortung und Haftung der Zu-ständigen für Informationssicherheit	**X**			**IT 486a**

Fachkompetenzen	Basis	Aufbau	Ergänzend	BAköV Angebot
	Standard	behördenangepasst		
Informationssicherheitsmanagement: Standards und Erstellen einer Leitlinie zur Informationssicherheit (Abschnitt a)				**IT 486a**
Nationale und internationale Standards im Überblick	**X**			**IT 486a**
Einführung in die Konzeption und Anwendung von IT-Grundschutz	**X**			**IT 486a**
Informationssicherheitsprozess und –management nach IT-Grundschutz	**X**			**IT 486a**
Erstellen einer Leitlinie zur Informationssicherheit	**X**			**IT 486a**
Datenschutz und Informationssicherheit	**X**			**IT 486a**
Definition und Festlegung hierarchischer Informationssicherheitsaufgaben und kritischer Geschäftsprozesse	**X**			**IT 486a**
IT-Sicherheitsbeauftragte im Informationssicherheitsmanagement – Kommunikation und Kooperation	**X**			**IT 486a**

Fachkompetenzen	Basis	Aufbau	Ergän-zend	BAköV Angebot
	Standard	behördenangepasst		
Maßnahmen für Informationssi-cherheit (Abschnitt b)				**IT 486b**
Datensicherungskonzept	**X**			**IT 486b**
Softwaremanagement	**X**			**IT 486b**
Sicheres Löschen von Datenträgern	**X**			**IT 486b**
Schutz vor Schadsoftware	**X**			**IT 486b**
			X	**IT 600**
E-Mail- und Internetsicherheit	**X**			**IT 486b**
Sicherheitsaspekte im Bereich der Vernetzung und beim Internet			**X**	**IT 607** **IT 630**
Virtual Private Network (VPN)	**X**			**IT 486b**
Sicherer Betrieb von Netzwerk-koppelelementen	**X**			**IT 486b**
Sicherheits-Gateway	**X**			**IT 486b**
Sicherheitsmaßnahmen für ausge-suchte Techniken – Funknetze und Bluetooth	**X**			**IT 486b**
Mobile Computing	**X**			**IT 486b**
Mindeststandards des BSI	**X**			**IT 486b**
E-Mail und Internetsicherheit	**X**			**IT 486b**
Mobile IT-Computing und Tele-arbeitsplatz	**X**			**IT 486b**
Zugangs- und Zugriffsschutz	**X**			**IT 486b**
Infrastrukturelle Sicherheits-Maßnahmen	**X**	**X**		**IT 486b** **IT 489**
Notfallvorsorge und Behandlung von Sicherheitsvorfällen	**X**			**IT 486b**
Verschlüsselungsverfahren und Elektronische Signatur (Abschnitt b)				**IT 486b**
Grundlagen der Kryptographie	**X**			**IT 486b**
Grundlegende Verfahren der Verschlüsselung	**X**			**IT 486b**
			X	IT 430
Anwendungen der Verschlüsselung	**X**			**IT 486b**

Fachkompetenzen	Basis	Aufbau	Ergän-zend	BAköV Angebot
	Standard	behördenangepasst		
Verfahren der Elektronischen Signatur mit Bezug zur Verschlüsse-lung	**X**			**IT 486b**
			X	**IT 430**
Public Key Infrastruktur	**X**		**X**	**IT 486b** **IT 430**
Der rechtliche Rahmen von Ver-schlüsselung und Elektronischer Signatur	**X**		**X**	**IT 486b** **IT 430**
Identitäts- und Berechtigungsma-nagement	**X**			**IT 486b**
Kryptobedarfserfassung und Erstel-len von Kryptokonzepten	**X**			**IT 486b**

Fachkompetenzen	Basis	Aufbau	Ergän-zend	BAköV Angebot
	Stan-dard	behördenangepasst		
Entwurf eines Informationssicher-heitskonzepts nach IT-Grundschutz (Abschnitt c)				**IT 486c**
Einführung in die Vorgehensweise	**X**			**IT 486c**
IT-Strukturanalyse	**X**			**IT 486c**
Schutzbedarfsfeststellung	**X**			**IT 486c**
Einleitung Modellierung	**X**			**IT 486c**
Überblick: Ergänzende Sicherheitsanalyse inkl. Restrisikobetrachtung	**X**			**IT 486c**
Basis-Sicherheitscheck	**X**			**IT 486c**
Reifegradmessung, Realisierung und Aufrechterhaltung von Informations-sicherheit	**X**			**IT 486c**
Zertifizierung	**X**			**IT 486c**
Modernisierung des IT-Grund-schutzes und Anwendung Aktuelle Entwicklungen zur Infor-mationssicherheit				**IT 486c**
IT-Konsolidierung des Bundes	**X**			**IT 486c**
Vorratsdatenspeicherung	**X**			**IT 486c**
Biometrie	**X**			**IT 486c**
De-Mail	**X**			**IT 486c**
Cloud Computing	**X**			**IT 486c**
Soziale Netze	**X**			**IT 486c**
Serviceorientierte Architekturen	**X**			**IT 486c**
IT-Sicherheit in heterogenen Netzen			**X**	IT 607
IT-Sicherheit im Bereich der Vernet-zung			**X**	IT 607
Sichere Client-Server-Architekturen			**X**	IT 600

Fachkompetenzen	Basis	Aufbau	Ergän-zend	BAköV Angebot
	Stan-dard	behördenangepasst		
Rechtliche Grundlagen des Daten-schutz/Datensicherheit		X		BF 210 BF 214
IT Service Management – unter Nut-zung von ITIL		X		IT 250
V-Modell XT Bund		X		IT 230
IT-Projekte in der öffentlichen Ver-waltung		X		IT 210 IT 205
Kommunizieren und kooperieren		X		KO 100 - 150
Konflikte erkennen und konstruktiv bewältigen		X		KO 210 - 230
Betreuung der Anwender in der IT			X	IT 510
Besprechungen leiten		X		KO 310 - 320
Präsentationstechnik		X		IT 550
Teams zielorientiert leiten		X		FÜ 270

Die vorliegende Übersicht wird den aktuellen Entwicklungen angepasst und ergänzt. Informationen darüber stehen unter http://www.bakoev.bund.de/IT-Sicherheitsbeauftragte bereit. Das Gesamtangebot der BAköV ist auf der Seite http://www.ifosbund.de veröffentlicht.
Auf Nachfrage und Bedarf werden weitere Themen aus dem Angebot aufgenommen.

9.2 Anhang zu 5.1 (Theoretischer Teil)

IT 486	**IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung – Basis**
Ziel	Die Teilnehmenden erwerben • grundlegende Kenntnisse und Fähigkeiten für die Ausführung von Tätigkeiten der IT-Sicherheitsbeauftragten bzw. im IT-Sicherheitsmanagement und • die Voraussetzung für die Absolvierung des Abschlusstestes zum Erwerb des Zertifikats "IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung - Basis".
Abschnitt a	**Informationssicherheit – warum?**
Inhalt	• Gefährdungen, Risiken, Bedrohungen, Schwachstellen für IT und Informationen • Anforderungen an ganzheitliche Informationssicherheit und Datenschutzbedarf • Grundwerte, Grundbegriffe Definitionen der Informationssicherheit • IT-Sicherheitsstrategie des Bundes - Umsetzungsplan des Bundes • Computernotfallteams, BSI und CERT-Bund • Anforderungen an IT-Sicherheitsbeauftragte und Schnittstellen zu anderen Bereichen sowie Beauftragte • Leitlinien und Dienstanweisungen • Schulungs- und Sensibilisierungsmaßnahmen • Übung: Erstellung eines Sensibilisierungskonzeptes und einer Dienstanweisung • Erkennen und Behandlung von IT-Sicherheitsvorfällen • Anforderungen an die Netze des Bundes und aktuelle Entwicklungen

Abschnitt a	**Informationssicherheit - Rechtliche und organisatorische Rahmenbedingungen**
Inhalt	• Relevante Vorgaben aus Gesetzen • Verantwortung und Haftung der Zuständigen für Informationssicherheit
Abschnitt a	**Sicherheitsmanagement – Standards und Erstellen einer Leitlinie zur Informationssicherheit**
Inhalt	• Nationale und internationale Standards im Überblick; ISO27000; COBIT; ITIL; BSI Standards und das Zusammenspiel mit ITIL und ISO • Einführung in die Konzeption und Anwendung von IT-Grundschutz • Sicherheitsprozess und -management nach IT-Grundschutz • Erstellung einer Leitlinie zur Informationssicherheit • Datenschutz und Informationssicherheit • Definition und Festlegung hierarchischer Sicherheitsaufgaben und der Kritischen Geschäftsprozesse • IT-Sicherheitsbeauftragte im Sicherheitsmanagement • Kommunikation und Kooperation, Berichterstattung und Präsentation von Arbeitsergebnissen

Abschnitt b	**Maßnahmen für Informationssicherheit**
Inhalt	• Datensicherungskonzept • Sicheres Löschen von Datenträgern • Softwaremanagement • Schutz vor Schadsoftware • Sicherer Betrieb von Netzkoppelelementen • E-Mail- und Internetsicherheit, Sicherheits-Gateway, Virtual Private Network • Sicherheitsmaßnahmen für ausgesuchte Techniken-Funknetze und Bluetooth • Mobile Computing • E-Mail und Internetsicherheit • Zugangs- und Zugriffsschutz • Mobiler Arbeitsplatz und Telearbeitsplatz • Zugangs- und Zugriffsschutz • Infrastrukturelle Sicherheitsmaßnahmen • Notfallmanagement und Behandlung von Sicherheitsvorfällen • Mindeststandards des BSI
Abschnitt b	**Verschlüsselungsverfahren und Elektronische Signatur**
Inhalt	• Grundlagen der Kryptographie und Grundlegende Verfahren der Verschlüsselung, der Elektronischen Signatur und Anwendungen, sowie Public-Key Infrastruktur • Überblick über den rechtlichen Rahmen von Verschlüsselung und Elektronischer Signatur • Identitäts- und Berechtigungsmanagement • Kryptobedarfserfassung und Erstellung von Kryptokonzepten

Abschnitt c	**Entwurf eines Sicherheitskonzepts nach IT-Grundschutz**
Inhalt	• Einführung in die Vorgehensweise • Strukturanalyse • Schutzbedarfsfeststellung • Modellierung • Risikoanalyse • IT-Grundschutzscheck • Reifegradmessung, Realisierungsplanung und Aufrechterhaltung von Informationssicherheit • Zertifizierung
Abschnitt c	**Modernisierung des IT-Grundschutzes und Anwendung Aktuelle Entwicklungen zur Informationssicherheit**
Inhalt	• IT-Konsolidierung des Bundes • Vorratsdatenspeicherung • Biometrie • De-Mail • Cloud Computing • Soziale Netze • Serviceorientierte Architekturen

9.3 Prüfungsordnung (vom 01.01.07; geändert am 12.09.07, 16.10.08, 31.08.11, 01.06.18 und 21.07.2020)

I. Allgemeines

§ 1: Geltungsbereich

(1) Diese Prüfungsordnung gilt für die Fortbildungsmaßnahme für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung im Sinne des Umsetzungsplan Bund. Sie regelt die Zertifizierung der Abschlüsse dieser Fortbildungsmaßnahme.

(2) Die Fortbildungsmaßnahme gliedert sich in folgende Teile

a) IT-Sicherheitsbeauftragte - Basis

b) IT-Sicherheitsbeauftragte - Aufbau

c) IT-Sicherheitsbeauftragte - Expert

§ 2: Zweck der Prüfung, Zertifizierung

(3) Die Abschlussprüfung bildet den Abschluss der in § 1 Abs. 2, lit a dieser Prüfungsordnung genannten Fortbildungsmaßnahme. Nach erfolgreicher Absolvierung der Prüfung erhalten die Absolventinnen bzw. Absolventen ein Zertifikat, durch das bescheinigt wird, dass sie aus Sicht des Prüfungsausschusses i. S. d. § 9 dieser Prüfungsordnung die notwendigen Kenntnisse und Fähigkeiten besitzen, um die Tätigkeit eines bzw. einer IT-Sicherheitsbeauftragten auszuüben (nach Basisseminar).

II. IT-Sicherheitsbeauftragte - Basis

§ 3: Zulassung zur Fortbildungsmaßnahme

Berechtigt zur Teilnahme an der in § 1 Abs. 2 lit. a dieser Prüfungsordnung genannten Fortbildungsmaßnahme sind Angehörige der öffentlichen Verwaltung aus dem höheren, gehobenen und mittleren Dienst. Es sollte sich um Verantwortliche oder Beteiligte des Informationssicherheitsmanagements einer Behörde handeln oder um Bedienstete bzw. Beschäftigte, welche die Funktion eines/einer IT-Sicherheitsbeauftragten wahrnehmen oder für die Übernahme dieser Aufgabe vorgesehen sind.

§ 4: Lehrgangsinhalt und –dauer

(1) Die in § 1 Abs. 2 lit. a dieser Prüfungsordnung 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 in § 2 dieser Prüfungsordnung genannte Prüfung können die Teilnehmenden folgende Fortbildungsmaßnahmen alternativ oder kumulativ absolvieren.

   a) Ein fünftägiges Seminar zu den Grundlagen der Informationssicherheit, den rechtlichen und organisatorischen Rahmenbedingungen der Informationssicherheit und zum Thema Sicherheitsmanagement – Standards, Leitlinie

   b) ein fünftägiges Seminar zu Maßnahmen in der Informationssicherheit und zu Verschlüsselungsverfahren und zur Elektronischen Signatur,

   c) ein fünftägiges Seminar zum Thema Entwurf eines Sicherheitskonzepts nach IT-Grundschutz.

   Die Teilnahme an allen vorstehend genannten Veranstaltungen ist freiwillig.

(3) Eine weitere Alternative bildet ein fünftägiger Kompaktkurs, der die prüfbaren Inhalte der oben unter den Buchstaben a und c aufgeführten Seminare vermittelt.

(4) Schließlich ist Teil der Fortbildungsmaßnahme auch ein eintägiger Workshop zur Projektpräsentation. Die Teilnahme hieran ist zwingend.

§ 5: Projektarbeit

(1) Die Absolventinnen und Absolventen müssen eine Projektarbeit zu einem für die Informationssicherheit relevanten Thema erstellen. Dabei können sie sich seitens ihrer Behörde, dem BSI oder eine anderen externen Stelle begleiten lassen. Die Projektarbeit sollte einen geschätzten Mindestarbeitsaufwand von etwa zwanzig Stunden erfordern.
   Über die Projektarbeit erstellt die Absolventin bzw. der Absolvent eine schriftliche Dokumentation, die eine Erläuterung aller wesentlichen Bestandteile des Projekts enthält, und bestätigt gegenüber dem Prüfungsausschuss i. S. d. § 9 dieser Prüfungsordnung mit ihrer bzw. seiner Unterschrift unter der Dokumentation, dass die Projektarbeit von ihr bzw. ihm tatsächlich und eigenverantwortlich durchgeführt wurde. Die Dokumentation muss grundsätzlich vor der Anmeldung zur Abschlussprüfung vorgelegt werden, spätestens 3 Wochen vorher.

(2) Voraussetzung für den Erhalt des Zertifikats nach § 13 dieser Prüfungsordnung ist eine etwa 20 Minuten umfassende Präsentation der Projektarbeit gem. Absatz 1. Diese erfolgt grundsätzlich im Rahmen des Workshops nach § 4 Abs. 4 dieser Prüfungsordnung.

§ 6: Abschlussprüfung

Zur Abschlussprüfung i. S. v. § 2 zugelassen werden alle Angehörigen des in § 3 dieser Prüfungsordnung genannten Personenkreises, die ihre Projektarbeit nach § 5 Abs. 2 dieser Prüfungsordnung präsentiert haben.

III. Die Abschlussprüfung Basiszertifikat

§ 7: Umfang und Inhalt der Abschlussprüfung

(1) Die Abschlussprüfung dauert 120 min.

(2) Gegenstand der Prüfungen i. S. d. § 2 sind vermittelte Inhalte aus den in § 4 Abs. 2 lit. a) bis c) dieser Prüfungsordnung aufgeführten Themen. Die konkreten Inhalte ergeben sich aus der aktuellen Fassung des „Handbuch IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“, das zur Vorbereitung auf die Prüfung zur Verfügung gestellt wird.

§ 8: Form und Durchführung der Abschlussprüfung

(1) Die Abschlussprüfung findet in Form eines schriftlichen Multiple Choice Verfahrens statt (Abschlusstest).

(2) Die Abschlussprüfung ist nicht öffentlich.

§ 9: Verantwortliche für die Auswertung der Abschlussprüfung

Verantwortlich für die Auswertung der Abschlussprüfung ist der Prüfungsausschuss. Der Prüfungsausschuss wird von einem Mitarbeiter bzw. einer Mitarbeiterin der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat gebildet.

§ 10: Bewertung der Prüfungsleistung

(1) Eine Differenzierung nach Noten findet bei der Bewertung der Prüfungsleistung nicht statt. Die Prüfung gilt vielmehr nur als „bestanden“ oder „nicht bestanden“.

(2) Die Abschlussprüfung gem. den §§ 7 und 8 dieser Prüfungsordnung gilt als bestanden, wenn mindestens 75 Prozent der möglichen Punktzahl erreicht werden.

§ 11: Wiederholungsmöglichkeiten

Die Abschlussprüfung kann einmal wiederholt werden. Die Wiederholung soll in der Regel innerhalb von zwölf Monaten nach dem erfolglosen Versuch stattfinden.

§ 12: Versäumnis, Rücktritt, Täuschung, Ordnungsverstoß

(1) Die Prüfungsleistung gilt als nicht bestanden, wenn der Prüfling zu einem Prüfungstermin ohne triftige Gründe nicht erscheint oder nach Beginn der Prüfung ohne triftige Gründe von der Prüfung zurücktritt oder die Prüfungsleistung nicht vor Ablauf der Prüfung erbringt.

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

(3) Versucht der Prüfling, das Ergebnis der Prüfungsleistung durch Täuschung oder Benutzung nicht zugelassener Hilfsmittel zu beeinflussen, gilt die betreffende Prüfungsleistung als nicht bestanden. Wer als Prüfling 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.
Erfolgt ein Ausschluss von der weiteren Erbringung der Prüfungsleistung, kann der Prüfling verlangen, dass die Entscheidung des Prüfungsausschuss überprüft wird. Dies gilt entsprechend bei Feststellungen gemäß Satz 1.

§ 13: Zertifikat

(1) Über die bestandene Abschlussprüfung wird möglichst innerhalb von zwei Wochen nach der Prüfung, 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 Abschlussprüfung bestanden worden ist.

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

(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 Zeit einer Betreuung oder Pflege eines pflegebedürftigen sonstigen 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 der/die Zertifikatsinhaber/-in im Zeitraum der Gültigkeitsdauer durch den Besuch einschlägiger Fortbildungsveranstaltungen auf Grundlage der Tabelle auf Seite 25 (Punkt 7.) 40 Punkte erreicht, zweimal die Jahrestagung für IT-Sicherheitsbeauftragte besucht und sie/er im Zeitpunkt der Zertifikatsverlängerung Verantwortliche/-r oder Beteiligte/-r des Informationssicherheitsmanagements einer Behörde ist oder die Funktion als IT-Sicherheitsbauftragte/-r wahrnimmt oder für die Übernahme dieser Aufgabe vorgesehen ist. Wenn die zuvor genannten Mindestpunkte nicht erreicht wurden, kann der/die Zertifikatsinhaber/-in alternativ die Prüfung wiederholen. Die Zertifikatsverlängerung ist nur auf schriftlichen Antrag möglich. Der Antrag soll 3 Monate vor Ablauf des Zertifikats vorliegen.

§ 14: Ungültigkeit von Prüfungen

(1) Hat der Prüfling im Rahmen der Abschlussprüfung gem. den §§ 7 und 8 dieser Prüfungsordnung getäuscht und wird diese Tatsache erst nach der Aushändigung des Zertifikats nach § 13 dieser Prüfungsordnung bekannt, so kann der Prüfungsausschuss nachträglich die Abschlussprüfung für nicht bestanden erklären.

(2) Das unrichtige Zertifikat nach § 13 dieser Prüfungsordnung ist einzuziehen und gegebenenfalls neu zu erteilen.

§ 15: Rechtsmittel

Gegen die Entscheidungen des Prüfungsausschusses ist die Beschwerde möglich. Sie ist innerhalb von vier Wochen nach Bekanntgabe der Entscheidung beim Prüfungsausschuss schriftlich einzureichen. Dieser entscheidet über die Beschwerde.

IV. IT-Sicherheitsbeauftragte - Aufbau

§ 16: Zulassung zur Fortbildungsmaßnahme

Berechtigt zur Teilnahme an der in § 1 Abs. 2 lit. b dieser Prüfungsordnung genannten Fortbildungsmaßnahme sind Angehörige der öffentlichen Verwaltung, die erfolgreich die Prüfung i. S. d. § 2 dieser Prüfungsordnung absolviert haben bzw. über entsprechende Kenntnisse in der Informationssicherheit durch einschlägige Nachweise verfügen.

§ 17: Lehrgangsinhalt und –dauer

Seminare zum IT-Sicherheitsbeauftragten – Aufbau behandeln Themen, die für die Erweiterung der Kenntnisse und Erfahrungen je nach Bedarf bzw. Aufgabengebiet benötigt werden. Das Seminar dauert i.d.R. fünf Tage und beinhaltet nachfolgende Hauptthemen.

- Informationsquellen und Angebote für IT-Sicherheitsbeauftragte,
- Modernisierung des IT-Grundschutzes
- Mindeststandards des BSI – Überblick, Umsetzung und Entwicklungen,
- Herausforderungen und Lösungen bei IT-Projekten, insbesondere im Kontext von eGovernment-Projekten,
- Anforderungen an das Outsourcing und Möglichkeiten der Steuerung externer Dienstleister,
- Behandlung von Informationssicherheitsvorfällen (Incident Management),
- Verfahren und Modelle zum Messen und Bewerten des Reifegrades der Informationssicherheit,
- wesentliche Aspekte der physischen Absicherung von Infrastrukturen, Betriebsräumen von IT-Systemen und Gebäuden,
- Sensibilisierung für Informationssicherheit als Prozess.

V. IT-Sicherheitsbeauftragte - Expert

§ 18: Zulassung zur Fortbildungsmaßnahme

Berechtigt zur Teilnahme sind Angehörige der öffentlichen Verwaltung, die das Basis-Zertifikat besitzen, die Fortbildung zum IT-Sicherheitsbeauftragten-Aufbau absolviert haben und Mitglied des Informationssicherheitsmanagements Ihrer Behörde sind.

§ 19: Projektarbeit

(1) Die Absolventinnen und Absolventen müssen eine Projektarbeit zu einem Thema erstellen, dass für die Informationssicherheit von grundsätzlicher Bedeutung ist und als Best-Practice genutzt werden kann. Die Arbeit ist vorrangig selbstständig oder mit Unterstützung der eigenen Dienststelle zu erstellen. Im Bedarfsfall stellt das BSI nach Ermessensentscheidung eine fachliche Ansprechstelle zur Verfügung. Über die Projektarbeit erstellt die Absolventin bzw. der Absolvent eine schriftliche Dokumentation, die eine Erläuterung aller wesentlichen Bestandteile des Projekts enthält, und bestätigt gegenüber dem Prüfungsausschuss mit ihrer bzw. seiner Unterschrift unter der Dokumentation, dass die Projektarbeit von ihr bzw. ihm tatsächlich und eigenverantwortlich durchgeführt wurde. Die Dokumentation muss grundsätzlich vor der Anmeldung zur Präsentation vorgelegt werden, spätestens 6 Wochen vorher.

(2) Voraussetzung für den Erhalt eines Zertifikats IT-Sicherheitsbeauftragter-Expert ist eine etwa 30 Minuten umfassende Präsentation der Projektarbeit vor dem Prüfungsausschuss. Diese erfolgt grundsätzlich im Rahmen eines Workshops entsprechend § 4 Abs. 4 dieser Prüfungsordnung. Ferner muss die Absolventin bzw. der Absolvent das Thema seiner Projektarbeit innerhalb von zwei Jahren auf der Jahrestagung der IT-Sicherheitsbeauftragten in einem Vortrag vorstellen. Der Erhalt des Zertifikats ist an den Erhalt des Basiszertifikats gebunden. Eine darüber hinaus gehende zeitliche Begrenzung ist nicht gegeben.

Abschlussvorschriften

§ 20: Datenschutzerklärung

(1) Die im Zusammenhang mit dieser Prüfungsordnung zur Verfügung gestellten personenbezogenen Daten werden ausschließlich zum Zweck der Lehrgangsverwaltung einschließlich aller mit der Durchführung der Abschlussprüfung zusammenhängenden Maßnahmen verwendet.

(2) Eine Weitergabe, Verkauf oder sonstige Übermittlung dieser personenbezogenen Daten an Dritte erfolgt nicht. Ausgenommen sind lediglich Mitteilungen an die Entsendungsbehörden über Entscheidungen des Prüfungsausschusses sowie erforderlichenfalls Abstimmungen mit dem Bundesamt für Sicherheit in der Informationstechnik.

(3) Die personenbezogenen Daten werden bei der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat aufbewahrt. 10 Jahre nach der Entscheidung über das Bestehen oder Nichtbestehen der Prüfung werden die Daten vernichtet. Personenbezogene Daten

von Personen, die sich nicht zur Prüfung anmelden, werden 10 Jahre nach der letzten Teilnahme an einer Fortbildungsmaßnahme i. S. d. dieser Prüfungsordnung vernichtet.

§ 21: Inkrafttreten und Veröffentlichung

Diese Prüfungsordnung tritt am 01. Januar 2007 in Kraft.

9.4 Themenvorschläge für die Projektarbeit

Aus allen Aufgabengebieten des/der IT-Sicherheitsbeauftragten können Themen für Projektarbeiten selbstständig formuliert werden. Hier folgt eine Auflistung von möglichen Themen als Hilfestellung, welche durch den Prüfling an seine Behördenspezifika angepasst werden sollten:

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?
* Wann müssen die Schlüssel gewechselt werden?
* Datensicherungskonzept für die Schlüssel (Verlust etc.)
* Wie werden die persönlichen Schlüssel gespeichert?
* Kriterien für die Auswahl eines Produkts
* 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:

* Da beim Einsatz von neuen technischen Sicherheitssystemen auch die IT-Sicherheitsbeauftragten einbezogen werden sollen, müssen Sie sich für eine solche Aufgabe zunächst einmal kundig machen, wie das gewählte „Security Tool“ arbeitet, welche Arten es gibt und wofür (wogegen) sie sinnvoll eingesetzt werden können.
* Als nächstes sind die Anwendungen und IT-Systeme zu identifizieren, die mit einem Security Tool überwacht werden sollen.
  Begründen Sie die Auswahl.
* Datenschutzrechtliche 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.

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:

In Ihrer Behörde fallen Informationen an, die bezüglich der Grundwerte Vertraulichkeit, Integrität und Authentizität einen höheren Schutzbedarf benötigen. Zum Schutz der genannten Grundwerte sollen kryptographische Verfahren (Software- und/oder Hardwarebasierend) eingeführt oder aktualisiert werden.

Entwickeln Sie zum Schutz dieser Daten ein Planungskonzept unter Berücksichtigung des BSI - Kryptoleitfadens und der BSI Arbeitshilfe zur Erstellung von Kryptokonzepten sowie zutreffende Mindeststandards oder Technischen Leitlinien / Richtlinien.

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
* Verpflichtung der Mitarbeiter/in zur Datensicherung
  Berücksichtigen Sie die Schnittstellen zur Notfallvorsorge

Themenvorschlag 7:

Erarbeiten Sie eine Dienstanweisung, für Beschäftigte, denen ein Gerät zur mobilen Kommunikation oder Datenübertragung 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

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 ggf. 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:

* Erläutern Sie Ihre Begründung der Bedeutung der Informationssicherheit für Ihre Behörde und wie wichtig diese für die Geschäftsvorgänge/IT-Anwendungen ist und welches Sicherheitsniveau erreicht werden sollte. Nennen Sie die wichtigsten Sicherheitsziele und was Sie als grobe Sicherheitsmaßnahmen und als organisatorische Regelungen vorschlagen, um diese Ziele zu erreichen.
* Zeigen Sie in Schritten auf, wie Ihre Behörde zu einer wirksamen Leitlinie zur Informationssicherheit kommt
* Stellen Sie ein Modell des Informationssicherheitsprozesses in Ihrer Behörde vor, an dem die Bedeutung der Leitlinie zur Informationssicherheit für weitere Maßnahmen des Sicherheitsmanagements erklärt wird
* Unterscheiden Sie die Verantwortlichkeiten für Informationssicherheit in Ihrer Behörde
* Erläutern Sie an Hand einer Grafik die für Informationssicherheit zuständigen Instanzen, Gremien und ihre Zuordnung zur Leitung
* Erklären Sie, wie die Beschäftigten über diese Leitlinie informiert werden sollten

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. In diesem Falle könnte es sich auch um die Weitergabe einer Aufgabe an ein zentrales Dienstleistungszentrum (IT-Konsolidierung des Bundes) handeln.

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. Nutzen Sie die Bausteine des IT-GS (SYS-Bausteine).

Themenvorschlag 17:

In Ihrer Behörde ergibt sich die Notwendigkeit funkbasierter Kommunikation (WLAN), z.B. weil Kabel nicht über ein dazwischen liegendes Gebiet gezogen werden können.
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 die Zertifizierungsschemas 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 Aufwand zu beachten.

Alternativ 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 Aufwand 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.

Themenvorschlag 22:

In Ihrer Behörde ist ein Geschäftsprozess von hoher Bedeutung (kritische Geschäftsprozesse).
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 Maßnahmenplan mit den Voraussetzungen nach IT-Grundschutz vertraut.

Hinweis:

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

9.5 Hinweise und Empfehlungen zur Durchführung und Betreuung der Projektarbeiten

Allgemein

- Als grundsätzliche Handlungsrichtlinie gelten die Hinweise aus dem LEITFADEN.
- Das Ergebnis der Projektarbeit wird zwischen *erfolgreich* und *nicht erfolgreich* unterschieden. Die Arbeit wird aber nicht benotet. Im Falle, dass die Arbeit nicht erfolgreich bewertet werden muss, erfolgt eine Begründung durch den Prüfungsausschuss.
- Die fachliche Begleitung hat die Möglichkeit bei der Präsentation der Arbeit anwesend zu sein. Eine Teilnahme ist jedoch nicht erforderlich.

Zielsetzung

- Der/die Kandidat/in soll mit der Projektarbeit dokumentieren,
  - dass er/sie im Tätigkeitsbereich eines/einer IT-Sicherheitsbeauftragten selbstständig konzeptionell arbeiten und
  - die Arbeitsergebnisse dann überzeugend vermitteln, bzw. präsentieren kann.

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

  Nach der Benennung der fachlichen Begleitung für die Betreuung der Projektarbeit soll die Initiative bei der Erstellung der Projektarbeit **immer** von dem/der Kandidaten/in ausgehen. Die fachliche Begleitung sollte hinzugezogen werden, wenn fachliche Fragestellungen oder Unsicherheiten auftreten. Insbesondere, wenn der/die Kandidat/in noch keine größere Erfahrung als IT-Sicherheitsbeauftragte oder in dem betreffenden Thema hat.

Inhalt

- Das Thema der Arbeit kann grundsätzlich frei gewählt werden. Es wird empfohlen, ein Thema aus den Vorschlägen des LEITFADEN´s zu wählen. Wenn ein Thema aus dem Leitfaden in Inhalt und Umfang geändert behandelt werden soll, muss dies im Projektantrag dargestellt werden.
- Ob ein Thema für eine Projektarbeit akzeptiert werden kann entscheidet der Prüfungsausschuss nach Eingang des Projektantrages.
- 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

Leitfaden sind Inhalte in Form von Unterpunkten z.T. schon näher spezifiziert.

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

1. **Anliegen / Einleitung**
   z. B. Einordnung der Arbeit in die Tätigkeit der IT – Sicherheitsbeauftragten bzw. des IT - Sicherheitsmanagements; Anlass für die Wahl des Themas; Vorgehensweise bei der Bearbeitung
2. **Gliederung**
3. **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

Form

Inhalt des Deckblattes: Name
Behörde
Thema
fachliche Begleitung
(Nennung nur mit Zustimmung)
Zeitraum der Anfertigung

Umfang: ca. 20 Seiten - Schrift 12 pt (z. B. Times New Roman, Arial)

Termine

- Nach der Anmeldung zur Fortbildung ist eine baldige Entscheidung für ein Thema zu treffen. Der Begleitungswunsch wird über die BAköV an das BSI weitergegeben.
- Besprechung der Arbeit mit der fachlichen Begleitung.
- Vorlage der Arbeit **spätestens 3 Wochen vor dem Workshop** bei der BAköV. Eine elektronische Abgabe ist möglich. Die Papierform muss spätestens zum Workshop vorliegen.
- Vorbereitung der Präsentation und wenn erforderlich Unterlagen für die anderen Teilnehmenden. **Achtung die Präsentationszeit beträgt höchstens 20 Minuten.**

Die Dokumentation muss grundsätzlich vor der Anmeldung zur Abschlussprüfung vorgelegt werden. Empfehlungen zur Vorbereitung der Präsentation sind im LEITFADEN (siehe 9.6 des Leitfadens) und auf der Webseite der BAköV enthalten

9.6 Empfehlungen zur Vorbereitung der Präsentation

Im Rahmen eines Workshops wird die Projektarbeit vorgestellt. An diesem Workshop nehmen Antragsteller/innen teil, welche die Projektarbeit abgeschlossen haben. Neben der Präsentation und dem Gespräch wird 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 Leitlinie zur Informationssicherheit oder Sicherheitskonzept 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 Informationssicherheitsaspekt 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. Am Ende steht die Zulassung zum Abschlusstest.

Hinweise für Präsentationen
Im Rahmen der 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.

Weitere Hinweise sind in der „Handreichung zur Gestaltung von Präsentationen“ - http://www.bakoev.bund.de/IT-Sicherheitsbeauftragte - enthalten.

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

9.7 Formulare

Fortbildungsantrag – Basis

Datenschutzerklärung

Plan der Projektarbeit - Antrag

Änderungs-/Ergänzungsmitteilung

Fortbildungsantrag - Aufbau

Fortbildungsantrag - Expert

Antrag: Zertifikatsverlängerung

Fortbildungsantrag – Basis

Bundesministerium
des Innern, für Bau
und Heimat

IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung mit Zertifikat

Bitte füllen Sie vorliegendes Antragsformular aus und senden Sie dieses der BAköV. Ergänzungen bzw. Änderungen müssen der BAköV (sibe-lg5@bakoev.bund.de) mitgeteilt werden.

A. Informationen zum/zur Antragsteller/in

(1) Persönliche Angaben

Name: Vorname:

Geburtsdatum: Titel, akad. Grad:

Telefonnummer für dringende Fälle (freiwillig):

(2) Dienstliche Angaben

Behörde/Institution:

Organisationseinheit:

Straße bzw. Postfach:

PLZ: Ort:

Telefon: Fax:

E-Mail:

Fortbildungsstelle:
Telefon:

B. Informationen zur Qualifikation, Berufserfahrung und Tätigkeit

Aktuelle Tätigkeit:

Weitere Tätigkeiten/Funktionen (z.B. Datenschutz- /Sicherheitsbeauftragte, etc.):

Einsatz- /Verantwortungsbereich als IT-Sicherheitsbeauftragte:

Berufserfahrung im Bereich IT-Sicherheitsbeauftragte (Angabe von Zeiträumen und Behörden):

Weiterbildungen im Bereich IT-Sicherheit (mit zeitlicher Angabe):

C. Fortbildungsplan Basis

Grundlage für den Fortbildungsplan sind Ihr Ergebnis des Selbsteinschätzungstests und die persönliche Einschätzung Ihrer Kenntnisse bzw. Erfahrungen. Die Termine für die einzelnen Fortbildungsabschnitte werden von der Lernprozessbegleitung bestätigt.

Fortbildungsbedarf	Terminwunsch	BAköV Veranstaltung	Bestätigung / Änderung
☐ Informationstechnik, Informationssicherheit und Internet in der modernen Verwaltung – Grundlagen und Anwendung		IT 485.___	
☐ **für Frauen** – Grundlagen und Anwendung		IT 484.___	
☐ Abschnitt a Informationssicherheit – warum?, Informationssicherheit – Rechtliche und organisatorische Rahmenbedingungen und Informationssicherheitsmanagement – Standards, Leitlinien		IT 486.___a	
☐ Abschnitt b Maßnahmen für Informationssicherheit und Verschlüsselungsverfahren und Elektronische Signatur		IT 486.___b	
☐ Abschnitt c Entwurf eines Sicherheitskonzepts nach IT-Grundschutz		IT 486.___c	
☐ Basisseminar Kompakt		IT 487.___	

Für das Thema der Projektarbeit (Vorschlag) verwenden Sie bitte den Antrag „**Plan der Projektarbeit**“ (9.7.2). Bitte geben Sie an, ob Sie Fachliche Begleitung aus der eigenen Behörde oder des BSI (BSI-Begleitung nur für Bundesbedienstete) in Anspruch nehmen wollen.	

☐	Fachliche Begleitung des BSI	☐ Fachliche Begleitung in der Behörde (Eintrag C 2b.)

☐	Projektpräsentation – Workshop	IT 488.___	
☐	Prüfung	IT 494.___	

Ort, Datum Unterschrift/Stempel Lernprozessbegleitung

D. Informationen zum Betreuungssystem / Unterstützungssystem

(1) Lernprozessbegleitung der BAköV*

Name: Vorname:

Bundesakademie für öffentliche Verwaltung – Lehrgruppe 5

Willy-Brandt Straße 1

50321 Brühl

Telefon: 0228 / 99629 - 0

E-Mail: sibe-lg5@bakoev.bund.de

(2) a. Fachliche Begleitung des BSI *

Name: Vorname:

Organisationseinheit:

Godesberger Allee 185 -189

53175 Bonn

Telefon: Fax:

E-Mail:

b. Fachliche Begleitung (eigene Behörde/Externer)

Name: Vorname:

Behörde/Institution:

Straße / Postfach:

PLZ: Ort:

Organisationseinheit / Tätigkeit:

Telefon: Fax:

E-Mail:

* Wird von der BAköV ergänzt

E. Erklärung des Antragstellers/der Antragstellerin

Hiermit nehme ich die Prüfungsordnung der BAköV zur Kenntnis.

Die vorstehenden Formulare sind Grundlage der individuellen Fortbildung „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ und werden den beteiligten Personen/Behörden zur Verfügung gestellt.

Der vorstehende Fortbildungsplan unterliegt ausschließlich meiner Verantwortung.
Die Lernprozessbegleitung nimmt eine beratende Funktion wahr.

Ich erkläre mein Einverständnis, dass vorstehende Daten unter Beachtung der Vorschriften des geltenden Datenschutzrechts verarbeitet und gespeichert werden. Die beiliegenden Datenschutzhinweise der BAköV habe ich zur Kenntnis genommen. Ich versichere mit meiner Unterschrift die Richtigkeit der in diesem Antrag von mir getätigten Angaben.

_____

Ort, Datum

_____

Unterschrift Antragsteller/-in

Ich bestätige die vorstehend gemachten Angaben zum Fortbildungsplan.

_____

Ort, Datum

_____

Unterschrift Fortbildungsstelle

Datenschutzrecht nach der EU-Datenschutzgrundverordnung (EU-DSGVO) und dem Bundesdatenschutzgesetz (BDSG)

Damit wir Sie für die Teilnahme an Fortbildungsveranstaltungen berücksichtigen können, willigen Sie bitte in die nachstehende Erklärung ein.

Name:

Vorname:

Einwilligungserklärung

Ich willige ein, dass die Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat (BAköV), Willy-Brandt-Straße 1, 50321 Brühl, meine personenbezogenen Daten

- Name, Vorname, akademischer Titel, Anschrift, Telefonnummer(n), E-Mail-Adresse(n), ggf. Homepage(s), ggf. Firmen- oder Behördenzugehörigkeit,

für die Teilnahme an Fortbildungsveranstaltungen verarbeitet.

Ich erkläre mich damit einverstanden, dass diese Daten zur Organisation und Durchführung der Fortbildungsveranstaltung und ggf. Zertifizierung an meinen zuständigen Fortbildungsbeauftragten sowie an die Mitarbeiterinnen und Mitarbeiter der Hochschule des Bundes für öffentliche Verwaltung, mit der die BAköV eine Verwaltungsgemeinschaft bildet, weitergegeben werden.

Einverstanden bin ich auch mit der Weitergabe der aufgeführten Daten, soweit dies zur Durchführung der Veranstaltung erforderlich ist, an die für die Durchführung zuständigen Mitarbeiterinnen und Mitarbeiter in den Veranstaltungsstätten oder des BSI.

Für die Zukunft kann ich meine Einwilligung jederzeit widerrufen.

Die nachstehenden Hinweise zum Datenschutz habe ich zur Kenntnis genommen.

_____ _____

Ort, Datum Unterschrift

Unsere Datenschutzhinweise für Sie!

Die Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat (BAköV) arbeiten mit einigen Hochschulen zusammen, damit diese als Zertifizierungsstellen das BAköV-Zertifikat für "IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung" oder das BAköV-Zertifikat für "Datenschutzbeauftragte in der öffentlichen Verwaltung" für Sie anbieten. Im Rahmen dieser Kooperation verarbeitet die BAköV personenbezogene Daten. Da wir verantwortungsbewusst mit Ihren personenbezogenen Daten umgehen, möchten wir Sie gerne darüber informieren, wie wir Ihre personenbezogenen Daten im Rahmen der Zertifikatsverwaltung verarbeiten und welche Rechte Sie bei dieser Verarbeitung haben. Im Übrigen verweisen wir auf unsere allgemeine Datenschutzerklärung, die Sie auf der Internetseite der BAköV einsehen können (www.bakoev.bund.de).

I. Grundsätzliches zur Datenverarbeitung in der BAköV

1. Wer ist in der BAköV für die Verarbeitung Ihrer Daten verantwortlich?

Verantwortlich für die Datenverarbeitung ist die BAköV selbst, vertreten durch den Präsidenten Herrn Dr. Alexander Eisvogel, dieser vertreten durch den Leiter der Lehrgruppe 1, Herrn Dr. Udo Heyder.
Anschrift:
a.) Standort Brühl: Willy-Brandt-Straße 1, 50321 Brühl
b.) Standort Berlin: Reichpietschufer 86 – 90, 10785 Berlin
Zentrale Telefonnummer: 0228/99629-0
Zentrale Mail-Adresse: poststelle@bakoev.bund.de

2. Wie erreichen Sie unsere Datenschutzbeauftragte?

Unsere Datenschutzbeauftragte ist die Datenschutzbeauftragte des BMI

Bundesministerium des Innern, für Bau und Heimat
Bundesallee 216-218
10719 Berlin
Tel.: 03018681-0
E-Mail: bds@bmi.bund.de

3. Wir verarbeiten Ihre Daten nur, wenn dies erforderlich ist!

Die Verarbeitung von personenbezogenen Daten durch die BAköV steht im unmittelbaren Zusammenhang mit unseren öffentlichen Aufgaben. Personenbezogene Daten werden von der BAköV nur verarbeitet, wenn dies erforderlich ist. Die Erforderlichkeit der Datenverarbeitung wird stets geprüft. Welche Daten zu welchem Zweck und auf welcher Grundlage verarbeitet werden, ist abhängig davon, für welchen Zweck wir Ihre Daten benötigen. Wir haben technische und organisatorische Maßnahmen getroffen, die sicherstellen, dass die Vorschriften zum Datenschutz beachtet werden. Die Verarbeitung personenbezogener Daten in der BAköV erfolgt in Übereinstimmung mit der DSGVO und dem Bundesdatenschutzgesetz (BDSG).

4. Zu welchen Zwecken verarbeitet die BAköV personenbezogene Daten?

Wir verarbeiten personenbezogene Daten im Rahmen unserer Kooperation mit den Zertifizierungsstellen zum Zweck der Zertifikatsverwaltung. Dies ermöglicht uns z.B. im Fall einer Zertifikatsverlängerung eine Prüfung über die Dauer Ihres Zertifikats. Außerdem können sich aus geeigneten Zertifikats-Projekten weitere Fortbildungsmaßnahmen wie z.B. Vorträge auf unseren Veranstaltungen ergeben.

5. Wie lange bewahren wir Ihre Daten auf?

Die BAköV speichert Ihre personenbezogenen Daten im Einklang mit der Richtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien, die gemäß der IT-Richtlinie des Bundesministeriums des Innern, für Bau und Heimat verbindlichen Regelungsgehalt hat und die die Gemeinsame Geschäftsordnung der Bundesministerien (GGO) ergänzt, sowie im Einklang mit der DSGVO und dem BDSG. Nach Ablauf der erforderlichen Aufbewahrungsfristen werden die Akten und erforderliche elektronische Aufbewahrungen vernichtet bzw. gelöscht.

6. Welche Rechtsgrundlagen gelten für die Datenverarbeitung in der BAköV?

Wir verarbeiten Ihre personenbezogenen Daten je nach Verarbeitungszweck aufgrund unserer im öffentlichen Interesse liegenden Aufgabe, Fortbildungen zu organisieren und durchzuführen (Art. 6 Abs. 1 Buchstabe e DSGVO i.V.m. § 3 BDSG) oder aufgrund Ihrer Einwilligung (Art. 6 Abs. 1 Buchstabe a DSGVO).

7. Von wem bekommen wir Ihre personenbezogenen Daten?

Wenn Sie uns Ihre personenbezogenen Daten nicht selbst übermitteln, erhalten wir im Fall der Dritterhebung personenbezogene Daten von der Zertifizierungsstelle, an der Sie das BAKöV-Zertifikat erworben haben oder ggf. von fachlichen Betreuungen für Ihre Projektarbeit.

8. An wen übermitteln wir erforderlichenfalls Ihre personenbezogenen Daten?

Ihre personenbezogenen Daten können durch die BAköV im Rahmen der unter Ziff. 6 genannten Zwecke auf Grundlage des § 25 BDSG insbesondere an folgende Empfängerkategorien übermittelt werden:

Wir bilden mit der Hochschule des Bundes für öffentliche Verwaltung (HS Bund), Willy-Brandt-Straße 1, 50321 Brühl, eine Verwaltungsgemeinschaft. In diesem Zusammenhang ist die HS Bund u.a. für die Geschäftsstelle Fortbildung, für den IT-Betrieb, Registraturtätigkeiten, Versandtätigkeiten und haushaltsrelevante Tätigkeiten der BAköV zuständig. Soweit die HS Bund in diesen Funktionen an der Verarbeitung Ihrer personenbezogenen Daten beteiligt sind, verfahren sie nur gemäß unseren Weisungen und unter unserer Kontrolle und ausschließlich zu den in diesen Datenschutzhinweisen beschriebenen Zwecken.

Außerdem ist es möglich, dass wir Ihre personenbezogenen Daten an Ihre Zertifizierungsstelle in Ihrer Hochschule übermitteln. Sollten Sie eine Projektarbeit angefertigt haben, die sich für weitere Fortbildungsmaßnahmen (z.B. Vorträge) eignet, ist es möglich, dass wir Ihre Daten auf Grundlage Ihrer Einwilligung an kooperierende Behörden (z.B. das Bundesamt für Sicherheit in der Informationstechnik, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) übermitteln sowie den Teilnehmenden unserer Veranstaltungen (z.B. Jahrestagungen) in Form einer Veranstaltungsagenda zur Verfügung stellen.

Dabei prüft die BAköV in jedem Einzelfall, ob eine Datenübermittlung dem Grund nach und in der in der beabsichtigten Art und Weise erforderlich ist.

II. Welche Rechte haben Sie im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten durch die BAköV?

1. Recht auf Information
Gemäß Art. 13, 14 DSGVO ggf. i.V.m. §§ 29, 32, 33 BDSG haben Sie das Recht über die Verarbeitung Ihrer personenbezogenen Daten und Ihre Rechte informiert zu werden. Die BAköV als verantwortliche Stelle erfüllt die ihr obliegende Pflicht zur Bereitstellung dieser Informationen mit diesen Datenschutzhinweisen auf dieser Internetseite.

2. Recht auf Auskunft
Gemäß Art. 15 DSGVO haben Sie das Recht, Auskunft über Ihre von uns gespeicherten personenbezogenen Daten zu verlangen. Insbesondere können Sie Auskunft über die Verarbeitungszwecke, die Kategorie der personenbezogenen Daten, die Kategorien von Empfängern, gegenüber denen Ihre Daten offengelegt wurden oder werden, die geplante Speicherdauer, die Herkunft ihrer Daten, sofern diese nicht bei uns erhoben wurden, sowie über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und ggf. aussagekräftigen Informationen zu deren Einzelheiten verlangen. Es gelten die in § 34 BDSG geregelten Ausnahmen von diesem Recht.

3. Recht auf Berichtigung
Gemäß Art. 16 DSGVO haben Sie das Recht, unverzüglich die Berichtigung unrichtiger oder die Vervollständigung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen.

4. Recht auf Löschung
Gemäß Art. 17 DSGVO haben Sie das Recht, die Löschung Ihrer bei uns gespeicherten personenbezogenen Daten zu verlangen, soweit nicht die Verarbeitung zur Ausübung des Rechts auf freie Meinungsäußerung und Information, zur Erfüllung einer rechtlichen Verpflichtung, aus Gründen des öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Es gelten die in § 35 BDSG geregelten Ausnahmen vom Löschungsrecht.

5. Recht auf Einschränkung
Gemäß Art. 18 DSGVO haben Sie das Recht, die Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen, soweit die Richtigkeit der Daten von Ihnen bestritten wird, die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen und wir die Daten nicht mehr benötigen, Sie diese jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen oder Sie gemäß Art. 21 DSGVO Widerspruch gegen die Verarbeitung eingelegt haben.

6. Recht auf Datenportabilität
Gemäß Art. 20 DSGVO haben Sie das Recht, Ihre personenbezogenen Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten oder die Übermittlung an einen anderen Verantwortlichen zu verlangen.
Recht auf Widerspruch gegen die Erhebung, Verarbeitung und bzw. oder Nutzung

7. Recht auf Widerspruch

Das Recht auf Widerspruch (Art. 21 DSGVO) beinhaltet die Möglichkeit, für Betroffene, in einer besonderen Situation der weiteren Verarbeitung ihrer personenbezogenen Daten zu widersprechen, soweit diese durch die Wahrnehmung öffentlicher Aufgaben oder öffentlicher sowie privater Interessen gerechtfertigt ist. Es gelten die in § 36 BDSG geregelten Ausnahmen von diesem Recht.

8. Recht auf Widerruf Ihrer Einwilligung

Gemäß Art. 7 Abs. 3 DSGVO haben Sie das Recht, Ihre nach Art. 6 Abs. 1 S. 1 a DSGVO erteilte Einwilligung jederzeit gegenüber uns zu widerrufen. Dies hat zur Folge, dass wir die Datenverarbeitung, die auf einer Einwilligung beruhte, für die Zukunft nicht mehr fortführen dürfen. Möchten Sie von Ihrem Widerspruchsrecht Gebrauch machen, genügt eine E-Mail an lg5@bakoev.bund.de

9. Recht auf Beschwerde beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)

Wenn Sie mit der Verarbeitung Ihrer Daten durch die BAköV nicht einverstanden sind, können Sie sich gemäß Art. 77 DSGVO jederzeit beim BfDI über diese Datenverarbeitung beschweren. Den BfDI erreichen Sie wie folgt:

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Anschrift:
Graurheindorferstr. 153, 53117 Bonn
Friedrichstr. 50, 10117 Berlin
Zentrale Telefonnummer: 0228/997799-0
Zentrale Mail-Adresse: poststelle@bfdi.bund.de
Internet-Adresse: www.bfdi.bund.de

10. Recht auf Schadenersatz

Nach Art. 82 DSGVO haben Sie ein Recht auf Schadenersatz, wenn Ihnen durch die Verarbeitung Ihrer personenbezogenen Daten in der BAköV ein Schaden entstanden ist.

Plan der Projektarbeit - Antrag

Name: Vorname:

Behörde:

Projekt-/ Tätigkeitsbeschreibung
Projektlaufzeit:

Von: bis:

Projektbezeichnung

Projektbeschreibung, Arbeitsschritte **(Angaben sind unbedingt erforderlich)**

Sofern zur Erklärung notwendig, fügen Sie bitte ggf. diesem Blatt ergänzende Materialien bei.

Ort, Datum Ort, Datum

Unterschrift Antragsteller/-in Unterschrift/Stempel Fachliche Begleitung

Änderungs- / Ergänzungsmitteilung

In meinem persönlichen bzw. dienstlichen Umfeld haben sich Änderungen (z.B. Name, E-Mail, Telefon, Abbruch der Fortbildung, Projektthema, Fortbildungsplan, etc.) ergeben.

Name: Vorname:

Behörde:

Beschreibung der Änderungen

Sofern zur Erklärung notwendig, fügen Sie bitte ggf. diesem Blatt ergänzende Materialien bei.

Ort, Datum Unterschrift Antragsteller/-in

Fortbildungsantrag - Aufbau

Grundlage für den Fortbildungsplan -Aufbau sind die Vorgaben und Bedürfnisse der Behörde des Kandidaten/der Kandidatin. Das Aufbauseminar hat eigenständige Inhalte.

Der Termin für die Fortbildung wird von der Lernprozessbegleitung bestätigt. Der/Die Teilnehmende versichert mit seiner/ihrer Unterschrift, dass die Voraussetzungen gemäß aktuellem Leitfaden für die Teilnahme am Aufbaukurs erfüllt werden.

Name: Vorname:

Behörde:

Seminarinhalte	Wunschtermin	BAköV Veranstaltung	Bestätigung / Änderung
Informationsquellen und Angebote für IT-Sicherheitsbeauftragte; Modernisierung des IT-Grundschutzes; Mindeststandards des BSI – Überblick, Umsetzung und Entwicklungen; Herausforderungen und Lösungen bei IT-Projekten, insbesondere im Kontext von eGovernment-Projekten; Anforderungen an das Outsourcing und Möglichkeiten der Steuerung externer Dienstleister; Behandlung von Informationssicherheitsvorfällen (Incident Management); Verfahren und Modelle zum Messen und Bewerten des Reifegrades der Informationssicherheit; wesentliche Aspekte der physischen Absicherung von Infrastrukturen, Betriebsräumen von IT-Systemen und Gebäuden; Sensibilisierung für Informationssicherheit als Prozess.		IT 489.___	

Ort, Datum Unterschrift Antragsteller/-in

Ort, Datum Unterschrift Lernprozessbegleitung

Fortbildungsantrag - Expert

Nach Besuch der Seminare Basis und Aufbau kann der/die IT-Sicherheitsbeauftragte durch Erstellung einer Projektarbeit zu aktuellen Themen der Informationssicherheit, welche nicht schon umfassend im Behördenumfeld behandelt/beschrieben worden sind, eine tiefergehende behördenangepasste Spezialisierung seiner/ihrer Ausbildung erlangen. Der Antrag wird nach Abstimmung mit allen Beteiligten der BAköV vorgelegt.

Name: Vorname:

Behörde:

Zertifikatsnummer Basis: Datum Seminarteilnahme Aufbau:

Thema und Beschreibung der Projektarbeit
Erstellungszeitraum der Projektarbeit:

Von: bis:

Bezeichnung der Projektarbeit

Beschreibung der Projektarbeit **(als Anlage ca. eine Seite A4-Format)**

- Anliegen
- Ziele
- Inhalte bzw. Schwerpunkte
- Begründung der Nutzungsmöglichkeiten, bzw. Allgemeingültigkeit des Gegenstandes

Ort, Datum Unterschrift Antragsteller/-in

Ort, Datum Unterschrift Fortbildungsstelle

Antrag Zertifikatsverlängerung

Zur Erhaltung der Qualifikation ist eine kontinuierliche Fortbildung erforderlich. Diese umfasst alle Aspekte des Aufgabenbereichs und soll auf eine Erweiterung der fachlichen und sozialen Kompetenzen abzielen. Die Fortbildung zum Kompetenzerhalt wird überwiegend durch Seminare der BAköV ermöglicht.

Name: Vorname:

Behörde:

Es wurden folgende Veranstaltungen besucht:

VA - Nummer	Datum	VA - Bezeichnung	Punkte

_____

Ort, Datum

_____

Unterschrift Antragsteller/-in

Bestätigung der zuständigen Fortbildungsstelle über die besuchten Seminare.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Fortbildungsstelle	Unterschrift/Stempel Lernprozessbegleitung

Muster Zertifikat

Bundesministerium des Innern, für Bau und Heimat

Bundesamt für Sicherheit in der Informationstechnik

BAköV

Zertifikat

Herr Max Mustermann,

geboren am 01.02.1975,

hat im Rahmen des Fortbildungsgangs 'IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung' die Projektarbeit "Umgang und Entfernen von Risiken – im Speziellen Viren und Würmer" vorgelegt, den Abschlusstest erfolgreich absolviert und damit die Befähigung zum

IT - Sicherheitsbeauftragten Basis

gemäß Prüfungsordnung vom 01.06.2018 erlangt.
Das Zertifikat basiert auf den BSI Standards 200-1 bis 200-3

Zertifikatsnummer:	30042018-A001
Zeitpunkt der Prüfung:	30.04.2018
Ablauf der Gültigkeit des Zertifikats:	29.04.2023

Bundesministerium des Innern 20

Brühl, den 30.04.2018

_____

Dr. Alexander Eisvogel, Präsident der BAköV

Ihre Ansprechpartner

Für die BAköV:

BAköV - Lehrgruppe 5
Tel.: 0228 / 99 629 - 0
sibe-lg5@bakoev.bund.de
https://www.bakoev.bund.de

Für das BSI:

BSI - Informationssicherheitsberatung
Tel.: 0228 / 99 9582 - 333
Fax: 0228 / 99 109582 - 333
Sicherheitsberatung@bsi.bund.de
https://www.bsi.bund.de

Bundesakademie für öffentliche Verwaltung
im Bundesministerium des Innern, für Bau und Heimat

Willy-Brandt Straße 1
50321 Brühl

Tel.: 0228 / 99629 - 0

https://www.bakoev.bund.de
https://www.ifosbund.de