Bundesministerium
des Innern

Leitfaden

IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung

Fortbildungsgang der BAköV und Zertifikat
in Zusammenarbeit mit dem BSI

BAKöV

BSI Bundesamt für Sicherheit in der Informationstechnik

Leitfaden

IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung

Fortbildungsgang der BAköV und Zertifizierung in Zusammenarbeit mit dem BSI

Brühl / Rheinland Januar 2009
Version 5.0

Hinweis:

Wird im Text die männliche Form verwendet, geschieht dies ausschließlich aus Gründen der leichteren Lesbarkeit.

Dieser Leitfaden wurde erstellt von der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV) und 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
Willy-Brandt-Str. 1
50321 Brühl

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

Telefax: **0228 / 99 629-5555**
02232 / 929-5555

E-Mail: **poststelle@bakoev.bund.de**

Internet: **http://www.bakoev.bund.de**
http://www.ifos-bund.de
https://www.lernplattform-bakoev.bund.de

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

Druck: **Statistisches Bundesamt – Zweigstelle Bonn**
Fachhochschule des Bundes

Vorwort

Die Modernisierung in unserer Gesellschaft und ebenso in der Bundesverwaltung ist ohne den Einsatz moderner Informationstechnik nicht mehr denkbar. Nahezu alle Geschäftsprozesse und Fachaufgaben sind von einem sicheren und einwandfreien Betrieb der Informationstechnik abhängig. Diese Abhängigkeit wird in Zukunft noch zunehmen und stellt alle Behörden vor große Herausforderungen.
Der IT-Fortbildung fällt die Aufgabe zu, die Bediensteten ganzheitlich in allen Kompetenzfeldern zu fördern, die für eine effektive und effiziente Nutzung der IT-Potenziale in der Verwaltungsarbeit erforderlich sind. Dies schließt die Förderung und Herstellung eines Informationssicherheitsbewußtseins und einer umfassenden Informationssicherheitskompetenz ein. Die Bandbreite der Informationssicherheitsfragen ist weit gespannt. Nicht nur technische Probleme sind zu klären, sondern auch juristische, wirtschaftliche und gesellschaftliche Antworten zu finden. In diesem Prozess der Entwicklung der Informationssicherheit in der Kommunikation der Behörden und dem IT-Betrieb gewinnt die Tätigkeit und Kompetenz des IT-Sicherheitsbeauftragten und des gesamten Informationssicherheits-Teams eine herausragende Bedeutung.
Ihre Aufgaben reichen von der Risikoanalyse über die Erstellung und Umsetzung eines Sicherheitskonzeptes bis zur Sensibilisierung 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. Daher müssen sie umfassend für ihre Arbeit qualifiziert werden.
Gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik hat die Bundesakademie für öffentliche Verwaltung einen neuen Fortbildungsgang “IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ mit der Möglichkeit des Zertifikaterwerbs entwickelt. Damit erhält die Fortbildung zu IT-Sicherheitsbeauftragten eine neue Qualität. Das Vorliegen der Kompetenzen für die Aufgabenwahrnehmung wird in einer Prüfung nachgewiesen. Für die Ausübung der Tätigkeit wird ein einheitlicher Qualitätsstandard gesetzt. Auf diese Weise wird die Fortbildung zu IT-Sicherheitsbeauftragten Bestandteil der Sicherheitsstrategie des Bundes und trägt entscheidend dazu bei, dass die Stellung der IT-Sicherheitsbeauftragten in ihren Behörden gestärkt wird.
Wir wünschen den Teilnehmerinnen und Teilnehmern an dieser Fortbildung ein gutes Gelingen und im Interesse der gesamten Bundesverwaltung viel Erfolg in ihrer Tätigkeit.

Günther Wurster
Präsident der Bundesakademie für öffentliche Verwaltung

Inhaltsverzeichnis

1 Vorbemerkung

Die Bundesregierung hat mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ eine IT-Sicherheitsstrategie vorgelegt. Mit dem Umsetzungsplan Bund (UP Bund) soll IT-Sicherheit mittel- und langfristig auf hohem Niveau in der gesamten Bundesverwaltung gewährleistet werden.

Die ständig wachsenden Sicherheitsrisiken beim Einsatz der Informationstechnik erfordern die Vermittlung von Wissen über Bedrohungen und Schutzmöglichkeiten, die Regelung der Sicherheitsverantwortlichkeiten, die Konzeption, Umsetzung und Kontrolle von Sicherheitsmaßnahmen. Der umfassende Schutz in allen sicherheitsrelevanten Bereichen erfordert ein qualifiziertes Sicherheitsmanagement. Zur Gewährleistung des Sicherheitsniveaus wächst die Bedeutung der guten und umfassenden Qualifikation des 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“ (IT-SiBöV) mit Zertifikatserwerb 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 herzustellen. Mit diesem Angebot ist die Möglichkeit der behörden- und aufgabenangepassten Fortbildung verbunden.

Die Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern 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 ist als unabhängige und neutrale Stelle für die IT-Sicherheit in Deutschland verantwortlich. Es ist operativ für den Bund, kooperativ für die Wirtschaft und informativ für den Bürger tätig. Neben den strategischen Zielen Prävention, Reaktion und Nachhaltigkeit wird als oberstes Ziel der Schutz von Information und Kommunikation verfolgt.

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, Bedienstete für die Tätigkeit des IT-Sicherheitsbeauftragten bzw. im Sicherheitsmanagement zu befähigen, zu zertifizieren und permanent fortzubilden.

Der Fortbildungsgang wendet sich an Verantwortliche des Sicherheitsmanagements und jene, die die Funktion 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 eigenes 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 für den Einzelnen 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 unterstützt der Fachliche Berater den Praktischen Teil (eine Projektarbeit) der Fortbildung. Die fachliche Beratung, von Seiten des BSI oder der abordnenden Behörde, unterstützt die Festlegung der Projektaufgabe, begleitet beratend den Prozess, die Dokumentation und 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 I - Basis“, je nach Bedarf bzw. Aufgabengebiet zu besuchende Aufbauseminare „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung II - Aufbau“ und eine behördenangepasste Spezialisierung „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung III - Aufbau“ nach Absolvierung der Stufen I und II. Jede Stufe ist mit der Möglichkeit des Erwerbs eines Zertifikats verbunden.

Die Teilnahme an den Seminaren 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 „Grundlagen in der Informationstechnik und Informationssicherheit“ angeboten.
- Der Basislehrgang ist modular aufgebaut, d.h. in einzelne Abschnitte gegliedert. Die Entscheidung für den Besuch einzelner Abschnitte, das vollständige Basisseminar oder das 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 Beratung (aus dem BSI oder der delegierenden Behörde) wird ein Projekt innerhalb der Behörde bzw. dem Aufgabenbereich erarbeitet. Dieses Projekt wird im Rahmen eines Workshops präsentiert und ist grundsätzlich Bedingung für die Prüfung.
- Die Zertifizierung „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I – Basis“ schließt mit einer theoretischen Prüfung ab. Die Prüfung (der Abschlusstest) erfolgt in Form eines elektronischen Multiple Choice Tests.
- Die Abschnitte des Aufbauseminars „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung II - Aufbau“ ergänzen zu ausgewählten Schwerpunkten das Seminar „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I – Basis“. Für den Zertifikatserwerb erfolgt eine Prüfung in Form eines elektronischen Multiple Choice Tests.
- Die erworbenen Zertifikate der Stufen I und II sind 5 Jahre gültig. Die Verlängerung des Zertifikats der Stufe I ist nur über eine vorgegebene zu erreichende Punktzahl möglich. Für den Erhalt des Zertifikats der Stufe II ist eine erneute Prüfung erforderlich.
- Nach Erlangung der Zertifikate der Stufen I und II kann der IT-Sicherheitsbeauftragte in einer dritten Stufe eine tiefergehende behördenangepasste Spezialisierung seiner Ausbildung erlangen.
  Im Rahmen dieser dritten Stufe wird eine Studie unter Anleitung und Begleitung des BSI entwickelt. Auch hier ist der Erwerb eines Zertifikates vorgesehen, das 7 Jahre gültig ist.

Grundlagen der Informationstechnik und Informationssicherheit	**(IT 485)**	**Dauer**
Die Teilnahme ist fakultativ und hängt von den individuellen Kenntnissen ab ▪ Grundlagen der Informationstechnik und Informationssicherheit		5 Tage

IT-Sicherheitsbeauftragte I – Basis (IT 486)	Dauer
Der Besuch der nachfolgenden Abschnitte hängt von den individuellen Vorkenntnissen (individueller Lernpfad) des Teilnehmenden ab.	15 Tage
a) Informationssicherheit – warum?	1 Tag
b) Informationssicherheit – Rechtliche und organisatorische Rahmenbedingungen	1 Tag
c) Informationssicherheit – zentrale Maßnahmen	3 Tage
d) Informationssicherheit am Arbeitsplatz	2 Tage
e) Verschlüsselungsverfahren und elektronische Signatur	1 Tag
f) Sicherheitsmanagement – Standards und Erstellen einer Leitlinie zur Informationssicherheit	2 Tage
g) Entwurf eines Sicherheitskonzepts nach IT-Grundschutz	5 Tage

IT-Sicherheitsbeauftragte I - Basis – Kompakt (IT 487)	Dauer
Vorausgesetzt werden der Inhalt des Handbuches sowie Kenntnisse in Sicherheitsmaßnahmen am Arbeitsplatz und in Netzen (z.B. Firewall, VPN, Verschlüsselung), die in den Abschnitten c) „Informationssicherheit – zentrale Maßnahmen“, d) „Informationssicherheit am Arbeitsplatz“ und e) „Verschlüsselungsverfahren“ des Basisseminars erworben werden können.	5 Tage
▪ IT-Grundschutz und den BSI-Standards 100-01 und 100-02	

Projektarbeit	Dauer
Auf der Grundlage der Inhalte des Basisseminars und der Anforderungen an den Aufgabenbereich ist ein überschaubares Projekt innerhalb der Behörde zu absolvieren (in Zusammenarbeit mit dem BSI).	ca. 20 Stunden

Präsentationsworkshop (IT 488)	Dauer
Die Teilnahme am Workshop ist Voraussetzung für die Prüfung / Zertifizierung.	1 Tag
▪ Vorstellung der Projektarbeit	
▪ Erfahrungsaustausch	

Zertifizierung (IT 491)	Dauer
▪ Abschlusstest (Multiple Choice)	1 Tag
▪ Verleihung des Zertifikats nach bestandenem Abschlusstest	

IT-Sicherheitsbeauftragte II – Aufbau (IT 489)	Dauer
Themen, die für die Erweiterung der Kenntnisse und Erfahrungen je nach Bedarf bzw. Aufgabengebiet benötigt werden. Ein Zertifikat mit einer Gültigkeit von 5 Jahren wird nach erfolgreicher Prüfung eines Abschnitts (a oder b) erteilt.	
a) IT Continuity und Notfallmanagement, Hochverfügbarkeit von Systemen, Anlagen und Prozessen	5 Tage

b) Qualitätssicherung und Schwachstellenanalyse, Kryptokonzeption und Aufbau einer PKI	5 Tage

IT-Sicherheitsbeauftragte III – Aufbau (IT 490)

Im Rahmen dieser Stufe wird eine Studie unter Anleitung und Begleitung des BSI entwickelt. Diese Anwenderstudie soll einen Best Practice Charakter für ein anspruchsvolles Thema haben und nach Fertigstellung gezielt publiziert werden können.
Nach dem Erstellungszeitraum von ca. 6 Monaten ist die Studie vor dem Prüfungsausschuss der BAköV und des BSI in einem 60 minütigen Vortrag zu präsentieren.

2 Sicherheitsmanagement

Der Umfang des Sicherheitsmanagements, der Tätigkeit des IT-Sicherheitsbeauftragten und des Informationssicherheits-Teams ist in den BSI-Standards umfassend beschrieben und dient als Orientierung für die Konzeption der Fortbildung. (BSI-Standard 100-2. IT-Grundschutz - Vorgehensweise. Standards zur IT-Sicherheit. Bonn 2008, S. 26 ff)

2.1 Anforderungsprofil

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.

Die genannten Fachkompetenzen bzw. Inhalte finden sich in den Seminaren bzw. Stufen des Gesamtfortbildungskonzeptes wieder. So entsprechen die

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

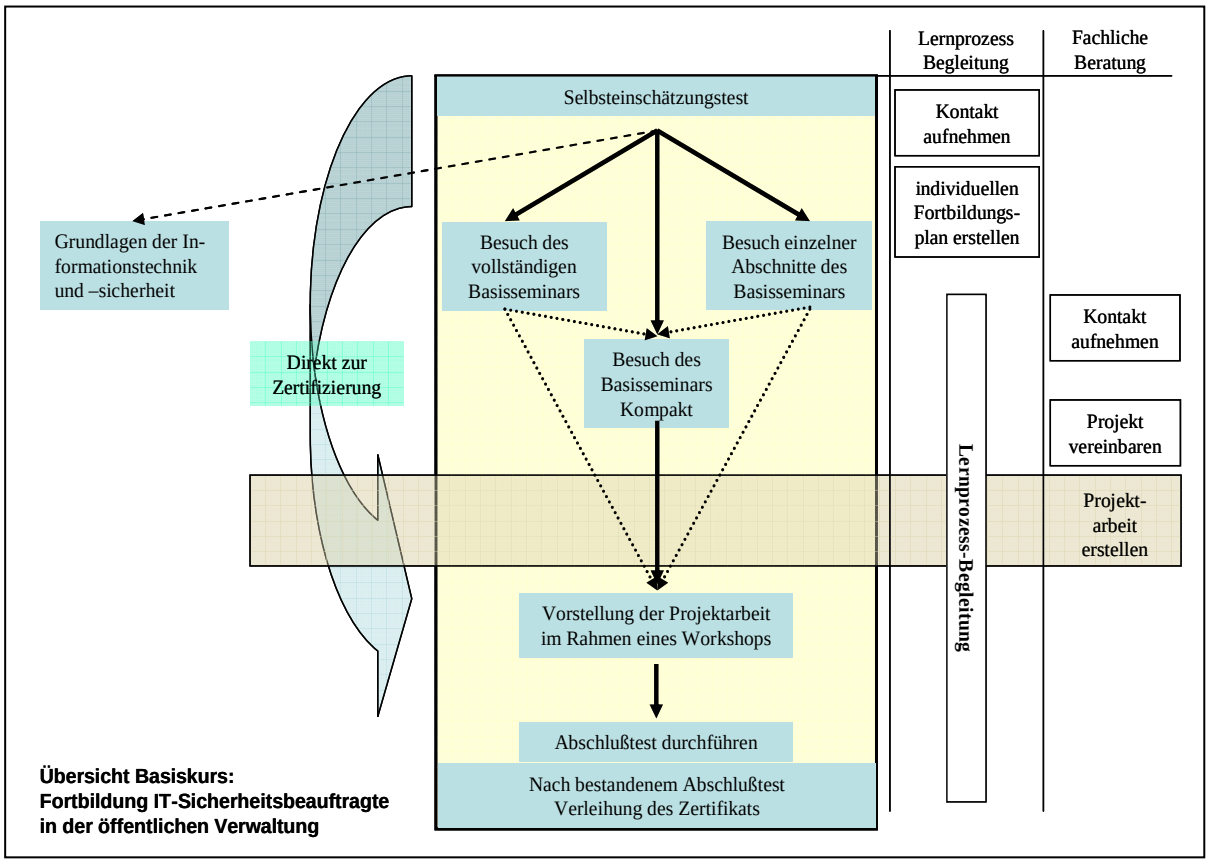
3 Fortbildung in der öffentlichen Verwaltung

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

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

Jeder in der Zielgruppe genannte Angehörige der Bundesverwaltung ist nach vorheriger Anmeldung der Behörde und Vereinbarung des Fortbildungsganges (Fortbildungsplan) zur Teilnahme berechtigt.

Der Fortbildungsgang und die Zertifizierung sind für Bundesbedienstete kostenfrei.



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 möglich.

Der Selbsteinschätzungstest umfasst insgesamt 80 Fragen und erfordert eine Bearbeitungszeit von etwa 2 Stunden. Er unterstützt die Beurteilung der Vorkenntnisse und verdeutlicht die Prüfungsanforderungen und damit die Einschätzung des individuellen Fortbildungsbedarfs. Der Aufbau des Tests spiegelt die im Fortbildungskonzept entwickelte modulare Gliederung wider. Die Fragen veranschaulichen, welches Wissen in den einzelnen Arbeitsbereichen eines IT-Sicherheitsbeauftragten erforderlich ist sowie fachliche Anforderungen für die Prüfung.

Dieser Test ist ein Hilfsmittel zur eigenen Orientierung und sollte unbedingt durch das Gespräch mit dem Lernprozessbegleiter ergänzt werden.

3.2 Fortbildungsantrag

Neben dem Selbsteinschätzungstest und dem Anforderungsprofil unterstützt der Lernprozessbegleiter den 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.

Der Fortbildungsantrag gibt im Wesentlichen Auskunft über die Erfahrungen, den Verantwortungsbereich und die Erreichbarkeit des Antragstellers.

Kern des Dokumentes bildet der Fortbildungsplan. Diesen bespricht der Antragsteller zuerst mit dem Fortbildungsbeauftragten und wenn erforderlich, mit dem 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 den Fortbildungsbeauftragten erfolgt eine Rückmeldung, welche Teilnahme zu welchem Zeitpunkt ermöglicht wird. Mit der Bestätigung des Lernprozessbegleiters erfolgt eine verbindliche Zusage der Teilnahme. Die Anmeldung an den Seminaren bzw. Abschnitten muss durch den Fortbildungsbeauftragten in IFOS-BUND zusätzlich erfolgen.

Die abschließende Erklärung des Antragstellers enthält die Kenntnisnahme der Prüfungsordnung und die Datenschutzerklärung.

Das Thema der Projektarbeit für die Zertifizierung wird mit dem Fachlichen Berater besprochen.

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 und Fachliche Beratung

Zur Unterstützung der Antragstellung und Begleitung der Umsetzung des individuellen Fortbildungsplanes steht von Seiten der Bundesakademie eine Lernprozessbegleitung zur Verfügung. Aufgabe des Fachlichen Beraters ist es, die Auswahl und Durchführung des Projektes fachlich zu unterstützen.

3.3.1 Lernprozessbegleitung

Der Lernprozessbegleiter 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 werden von dieser Stelle auch entsprechende Anfragen und Kontakte mit der Fachlichen Beratung im BSI weitergeleitet und vermittelt.

Die Bundesakademie sichert die notwendige Dokumentation entsprechend der rechtlichen Grundlagen.

3.3.2 Fachliche Beratung

Der Fachliche Berater begleitet das Projekt. Seine Aufgabe ist es, die Auswahl und Durchführung des Projektes fachlich zu unterstützen. Die Fachliche Beratung von Seiten des BSI unterstützt bei der Festlegung der Projektaufgabe, begleitet den Prozess, die Dokumentation und Präsentation und bestätigt die Themenwahl. Der Fachliche Berater kann auch bei der entsendenden Behörde beschäftigt sein. Die Entscheidung darüber wird vom Kandidaten getroffen.

3.4 Stufen der Fortbildung und Zertifizierung

Das Gesamtkonzept der Fortbildung zum IT-Sicherheitsbeauftragten in der öffentlichen Verwaltung (IT-SiBöV) beinhaltet

- das Seminar „IT-Sicherheitsbeauftragte I Basis“ –als modular aufgebautes Seminar oder Kompaktseminar,
- nach Bedarf bzw. Aufgabengebiet zu besuchende Aufbauseminare zum Erreichen der Stufe „IT-Sicherheitsbeauftragte II“ und
- eine behördenangepasste Spezialisierung „IT-Sicherheitsbeauftragte III“ nach Absolvierung der vorherigen Stufen. Im Rahmen dieser dritten Stufe wird eine Studie unter Anleitung und Begleitung des BSI entwickelt.

Für jede Stufe (Stufe I und II nach erfolgreicher Prüfung) wird ein Zertifikat ausgehändigt. Zum Erhalt oder zur Verlängerung der Zertifikate sind verschiedene Fortbildungsmaßnahmen bzw. erneute Prüfungen erforderlich. Diese sind in der Übersicht des Anforderungsprofils enthalten.

4 Grundlagen

Grundlagenwissen zur Informationstechnik und Informationssicherheit kann in einem gesonderten Kurs erworben werden. Dieses Seminar hat für Teilnehmende, welche über geringe Kenntnisse in diesem Bereich verfügen, den Charakter eines Vorkurses. Die Durchführung des Selbsteinschätzungstests erübrigt sich in diesem Falle.

Grundlagen der Informationstechnik und Informationssicherheit	**IT 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 Basiskurses Kompakt.
4. Die direkte Anmeldung, nach Absolvierung der Projektarbeit und deren Präsentation in einem Workshop, zur Prüfung für den Zertifikatserwerb ist ebenfalls möglich.

Die Teilnahme an den Abschnitten des Seminars, welche einzeln gebucht werden können, wird ebenfalls bestätigt.

IT-Sicherheitsbeauftragte I – Basis	IT 486	Dauer
a) Informationssicherheit – warum?		1 Tag
b) Informationssicherheit– Rechtliche und organisatorische Rahmenbedingungen		1 Tag
c) Informationssicherheit– zentrale Maßnahmen		3 Tage
d) Informationssicherheit am Arbeitsplatz		2 Tage
e) Verschlüsselungsverfahren und elektronische Signatur		1 Tag
f) Sicherheitsmanagement – Standards und Erstellen einer Leitlinie zur Informationssicherheit		2 Tage
g) Entwurf eines Sicherheitskonzepts nach IT-Grundschutz		5 Tage

5.1 Theoretischer Teil

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

IT 486	**IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I – 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 I – Basis Kompakt

Das fünftägige Seminar „IT-Sicherheitsbeauftragte I - Basis - Kompakt“ ermöglicht, vorhandene Kenntnisse besonders im Bereich IT-Grundschutz zu aktualisieren. Den Teilnehmenden des Basisseminars steht dieses ebenfalls offen. Vorausgesetzt werden der Inhalt des Handbuches „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“ sowie Kenntnisse in technischen Sicherheitsmaßnahmen am Arbeitsplatz und in Netzen (z.B. Firewall, VPN, Verschlüsselung), die in den Abschnitten (c) „Informationsicherheit – zentrale Maßnahmen“, (d) „Informationssicherheit am Arbeitsplatz“ und (e) „Verschlüsselungsverfahren und elektronische Signatur“ des Basisseminars erworben werden können.

IT-Sicherheitsbeauftragte I - Basis – Kompakt IT 487	Dauer
▪ Informationssicherheit- Anforderungen ▪ Rechtliche und organisatorische Rahmenbedingungen für Informationssicherheit ▪ Standards und Zertifizierung ▪ Sicherheitsmanagement und Leitlinie zur Informationssicherheit ▪ Informationssicherheit nach IT-Grundschutz ▪ Sensibilisierungs- und Schulungskonzept ▪ Behandlung von Sicherheitsvorfällen und Notfallvorsorge ▪ Aufrechterhaltung der Informationssicherheit und Revision	5 Tage

5.1.3 Bereitstellung eines Handbuches

Ein Handbuch für den Basislehrgang „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I - Basis“ wird jedem Teilnehmer ausgehändigt. Dieses ist inhaltlich den Schwerpunkten des Basislehrganges angepasst und dient der grundlegenden Orientierung. Es enthält kurze Erörterungen, Verweise auf weiterführende Literatur und Links 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 I – Basis soll ein Projekt in der jeweiligen Behörde bearbeitet werden. Begleitet wird der Praktische Teil – abgestimmt mit der Lernprozessbegleitung - von einem Fachlichen Berater (BSI oder behördenintern). Das Thema sollte, wenn möglich, den eigenen 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 „Plan der Projektarbeit“ über die Bundesakademie an das BSI gesandt und von dort beschieden. Der Zeitaufwand des Projektes sollte mindestens 20 Stunden (ohne Vorbereitung der Präsentation) umfassen. Der Umfang des Projektes wird mit dem Fachlichen Berater besprochen und die Dokumentation (siehe 9.5 des Leitfadens) sollte max. 20 Seiten umfassen.

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

Projektarbeit	Dauer
Auf der Grundlage der Inhalte des Basisseminars und den Anforderungen aus dem Aufgabenbereich ist ein überschaubares Projekt innerhalb der Behörde zu absolvieren (in Zusammenarbeit mit dem Fachlichen Berater des BSI oder der eigenen Behörde).	mindestens 20 Stunden

5.3 Workshop Projektpräsentation

Die Präsentation der Projektarbeit erfolgt in einem Workshop (IT 488) der Bundesakademie. Die Abgabe der Arbeit muss **ausnahmslos** spätestens zwei Wochen vor dem Workshop erfolgen. Eine elektronische Abgabe (sibe-lg5@bakoev.bund.de) ist möglich. Die Papierform muss zum Workshoptermin vorliegen. Alle Teilnehmenden präsentieren ihre Projektarbeit und führen ein Gespräch darüber. Dieses Gespräch wird - die Präsentation eingeschlossen - jeweils einen Zeitraum von etwa 30 Minuten beanspruchen. Der Workshop wird von der BAköV und dem BSI moderiert.

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 Schwie-

rigkeitsgrad der Testfragen orientieren sich an den inhaltlichen Schwerpunkten des Basislehrganges. Die Auswahl der Fragen für die Prüfung erfolgt automatisch aus einem Fragenpool.

Nach bestandener Prüfung wird das Zertifikat: „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I – 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 möglich. Hierfür werden mit dem Blick auf einen Kompetenzerhalt Seminare und Veranstaltungen (mit Erfahrungsaustausch) von der BAköV angeboten (siehe 9.1 Anforderungsprofil und 7. Zertifikatserhalt).

6 Behördenangepasste Fortbildung

Der Zertifikatserwerb „IT-Sicherheitsbeauftragte II“ und „IT-Sicherheitsbeauftragte III“ ist darauf ausgerichtet, eine weitere behördenangepasste Fortbildung, dem besonderen Verantwortungsbereich entsprechend, anzubieten.

Der jeweilige Antrag für diese Fortbildung muss mit den Verantwortlichen abgesprochen und bei der BAköV eingereicht werden. In Absprache mit dem BSI wird dem Antrag entsprochen.

6.1 IT-Sicherheitsbeauftragte II – Aufbau

Die Abschnitte des Aufbauseminars „IT-Sicherheitsbeauftragte II – Aufbau“ setzen inhaltlich auf entsprechende Abschnitte des Basisseminars „IT-Sicherheitsbeauftragte I – Basis“ auf. Es wird die Möglichkeit eröffnet, Wissen für die Tätigkeiten als IT-Sicherheitsbeauftragte zu speziellen Themen der IT-Sicherheit und -Organisation zu erwerben.

Die Vorlage des Zertifikats Stufe I oder vergleichbarer Fortbildungsprogramme ist Voraussetzung für die Teilnahme.

IT-Sicherheitsbeauftragte II – Aufbau	**IT 489**	**Dauer**
Die Abschnitte des Aufbauseminars behandeln Themen, die für die Erweiterung der Kenntnisse und Erfahrungen je nach Bedarf bzw. Aufgabengebiet benötigt werden. Ein Zertifikat mit einer Gültigkeit von 5 Jahren wird nach erfolgreicher Prüfung eines Abschnitts (a oder b) erteilt.		
c) IT Continuity und Notfallmanagement, Hochverfügbarkeit von Systemen, Anlagen und Prozessen		5 Tage
a) Qualitätssicherung und Schwachstellenanalyse, Kryptokonzeption und Aufbau einer PKI		5 Tage

Die Abschnitte des Aufbauseminars haben eigenständige Inhalte (siehe. 9.1 Anforderungsprofil). Für jeden Abschnitt wird eine Seminarunterlage zur Verfügung gestellt, welche zur Prüfungsvorbereitung genutzt wird.

Für die Erreichung des Zertifikats ist das Bestehen der Prüfung eines Abschnitts (a oder b) erforderlich. Auch dieses Zertifikat soll 5 Jahre gültig sein. Der Erhalt bzw. die Verlängerung des Zertifikats ist nur über eine erneute Prüfung möglich.

Fachkompetenz	**BAköV Angebot**
▶ IT Continuity und Notfallmanagement o Business Continuity aus Informationssicherheitssicht o Notfallmanagement nach BSI Standard 100-4 o Der Notfallmanagement Prozess o Analysen o Notfallvorsorgekonzept o IT-Krisenmanagement ▶ Hochverfügbarkeit von Systemen, Anlagen und Prozessen o Grundlagen von Hochverfügbarkeit o Kennzahlen und Berechnungen o Ausfallkosten und Aufwand o Methodisches Vorgehen o Beispiele für hochverfügbare Architekturen	IT 489 a)
▶ Qualitätssicherung und Schwachstellenanalyse o IT- Revision planen und durchführen o Penetrationstest o IT-Sicherheitsvorfälle erkennen und bewerten, kommunizieren und behandeln o Sicherheitskonzepte für neue Verfahren – generelle Vorgehensweise ▶ Kryptokonzeption und Aufbau einer PKI o Kryptokonzeption o Aufbau einer PKI und PKI-1-Verwaltung	IT 489 b)

6.2 IT-Sicherheitsbeauftragte III – Aufbau

Je nach Aufgabengebiet und Erfordernis kann in einer dritten Stufe nach Absolvierung der Stufen I und II eine behördenangepasste Spezialisierung erfolgen. Der Umfang und das Thema des Projektes werden mit der Fachlichen Beratung im BSI abgestimmt. Es soll eine Anwenderstudie mit Best Practice Charakter für

ein anspruchsvolles Thema erarbeitet werden. Auch hier ist der Erwerb eines Zertifikats vorgesehen. Der Antrag der Stufe III erfolgt über die BAköV.

IT-Sicherheitsbeauftragte III – Aufbau	**IT 490**

Vorgehensweise für die Absolvierung der Stufe III:

1) Interesse bekunden

Formlose Anfrage bei der BAköV (sibe-lg5@bakoev.bund.de). Der Antragsteller muss über die Zertifikate der Stufen I und II (Basis und Aufbau) verfügen. Die Interessenbekundung wird an das BSI weitergeleitet. Es wird empfohlen, das Vorhaben und dessen Umfang vorab mit dem Fortbildungsbeauftragten der Behörde zu besprechen.

2) Projektantrag

Das BSI nimmt mit dem/der Antragsteller/in Kontakt auf. Es werden folgende Punkte besprochen: Festlegung des Projektthemas, der Ansprechpersonen, Zeitraum der Fertigstellung, inhaltlicher Umfang.

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

3) Projekt / Studie

Erarbeitung der Studie im festgelegten Zeitraum unter Betreuung / Beratung des BSI.

4) Präsentation und Veröffentlichung

Das Projekt wird dem BSI und der BAköV in einer Veranstaltung präsentiert und diskutiert. In Abstimmung mit der Behörde wird die Veröffentlichung vorbereitet und das Projekt auf der folgenden Jahrestagung vorgestellt.

6.3 Jahrestagung für IT-Sicherheitsbeauftragte

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

Die Jahrestagung wird jährlich durchgeführt und spricht alle IT-Sicherheitsbeauftragten in der Bundesverwaltung an. Diese Veranstaltung bildet den Mittelpunkt eines Forums für IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung. Deren Besuch ist gleichzeitig Schwerpunkt des Zertifikatserhalts.

Jahrestagung: IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung	**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 breite Basis für den Erfahrungsaustausch gewährleistet.

7 Zertifikatserhalt und ergänzende Fortbildung

Informationstechnik, Anwendungen, Bedrohungsszenarien und Sicherheitstechnik unterliegen einem ständigen Wandel, ebenso das rechtliche und organisatorische Umfeld, 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 der BAköV ermöglicht.

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

Für den Zertifikatserhalt der Bediensteten der Länder und Kommunen gilt nachstehende Punktetabelle mit der Maßgabe, dass an Stelle der Teilnahme an der Jahrestagung für IT-Sicherheitsbeauftragte der Besuch von zwei Grundschutztagen des BSI im Jahr gewertet wird. Eine nochmalige Prüfung zum Zertifikatserhalt ist möglich.

Punktesystem für den Werterhalt des Zertifikats der Stufe I

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

Die Punkte sind über folgende Maßnahmen zu erreichen	Punkte
Teilnahme an der jährlich stattfindenden „Jahrestagung für IT-Sicherheitsbeauftragte“	15
Teilnahme an IT - Seminaren der BAköV aus dem Bereich IT-Sicherheit (siehe Überblick – Aufbau)	13

Teilnahme an anderen Seminaren der BAköV (siehe Überblick – Ergänzend)	12
Teilnahme an IT-Seminaren von externen Anbietern und Kongressen im Bereich IT-Sicherheit (Anerkennung nur nach Absprache mit der BAköV)	8
Teilnahme an anderen Seminaren von externen Anbietern (Anerkennung nur nach Absprache mit der BAköV)	5
Teilnahme an 2 Grundschutztagen im Jahr (nur für Länder)	15

Das Zertifikat der Stufe II kann nur über den Besuch eines Abschnitts des Aufbauseminars mit anschließender Prüfung verlängert werden.

Die Verlängerung des Zertifikats der Stufe III wird durch die Erstellung einer weiteren Studie erreicht.

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

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

Im Rahmen einer "Sommerakademie für IT-Sicherheit" wird ein Fortbildungsgang "IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I - 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 100-01 und 100-02 und den Anforderungen aus dem Aufgabenbereich IT-Sicherheit ist ein überschaubares Projekt innerhalb der eigenen Behörde in Zusammenarbeit mit einem Fachlichen Berater aus der eigenen Behörde oder einer externen Firma zu absolvieren (vgl. LEITFADEN 5.2). Die Themenvorschläge aus dem LEITFADEN können für die Arbeit herangezogen werden. Zur Bestätigung des Projektthemas wird der „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 des BSI teilnehmen. Die Abgabe der Arbeit muss **ausnahmslos** spätestens zwei 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 I – Basis“ vergeben.

Das Zertifikat ist 5 Jahre gültig.

9 ANHANG

9.1 Anhang zu 2.1 (Anforderungsprofil)

9.2 Anhang zu 5.1 (Theoretischer Teil)

9.3 Prüfungsordnung

9.4 Themenvorschläge für die praktische Arbeit

9.5 Empfehlungen zur Anfertigung der Projektarbeit

9.6 Empfehlungen zur Vorbereitung der Präsentation

9.7 Formulare für IT-SiBöV

9.7.1 Fortbildungsantrag I – Basis

9.7.2 Plan der Projektarbeit

9.7.3 Änderungs- / Ergänzungsmitteilung

9.7.4 Fortbildungsantrag II - Aufbau

9.7.5 Fortbildungsantrag III - Aufbau

9.7.6 Antrag: Zertifikatsverlängerung

10 Muster Zertifikat

9.1 Anhang zu 2.1 (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. Stufen des Gesamtfortbildungskonzeptes wieder. So entsprechen die

- **Basiskompetenzen** - den fachlichen Anforderungen (Seminarinhalte) „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung I – Basis“,
- **Aufbaukompetenzen** - den fachlichen Anforderungen (Seminarinhalte) „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung II – 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.ifos-bund.de) in Fettdruck betreffen ausschließlich Seminare des Fortbildungsganges „IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung“

Fachkompetenzen	**Basis**	**Aufbau**	**Ergänzend**	**BAköV Angebot**
		behördenangepasst		
Grundlagen Informationstechnik und Informationssicherheit				**IT 485**
IT-Systeme – Grundlagen und Arbeitsplatzrechner	**X**			**IT 485**
IT-Systeme – Netze und Server	**X**			**IT 485**
Internet und lokale Netze	**X**			**IT 485**
IT-Anwendungen in der öffentlichen Verwaltung	**X**			**IT 485**
Informationssicherheit				**IT 486 a)**
Gefährdungen und Risiken (in Behörden)	**X**			**IT 486 a)**

Fachkompetenzen	**Basis**	**Aufbau**	**Ergän-zend**	**BAköV Angebot**
		behördenangepasst		
Ganzheitliche Informationssicher-heit	**X**			**IT 486 a)**
Informationssicherheit - Recht-liche und organisatorische Rah-menbedingungen				**IT 486 b)**
Aktuelle Entwicklungen zur IT-Strategie und Informationssicher-heit IT-Sicherheit in der Bundes-verwaltung - Standards und Archi-tekturen	**X**		**X**	**IT 486 b)**
			X	**SO 505**
Sicherheitsanforderungen im Be-hördennetz	**X**			**IT 486 b)**
Rechtliche Rahmenbedingungen und relevante gesetzliche Regel-ungen	**X**			**IT 486 b)**
Sicherheitsanforderungen an E-Government-Anwendungen	**X**			**IT 486 b)**
Verantwortung und Haftung der Zuständigen für Informationssi-cherheit (Leitung, IT-Sicherheitsbeauftragte, IT-Administration)	**X**			**IT 486 b)**
Informationssicherheit - Zentra-le Maßnahmen				**IT 486 c)**
Datensicherungskonzept	**X**			**IT 486 c)**
Softwaremanagement	**X**			**IT 486 c)**
Schutz vor Schadsoftware	**X**			**IT 486 c)**
			X	IT 435
			X	IT 436
E-Mail- und Internetsicherheit	**X**			**IT 486 c)**
			X	IT 435
Sicherheitsaspekte im Bereich der Vernetzung und beim Anschluss ans Internet		**X**		IT 455
Virtual Private Network (VPN)	**X**			**IT 486 c)**

Fachkompetenzen	**Basis**	**Aufbau**	**Ergän-zend**	**BAköV Angebot**
		behördenangepasst		
Sicherheitsmaßnahmen für ausgesuchte Techniken	**X**			**IT 486 c)**
Protokollierung und Kontrolle	**X**			**IT 486 c)**
Physische Sicherheitsmaßnahmen	**X**			**IT 486 c)**
Personelle Sicherheitsmaßnahmen	**X**			**IT 486 c)**
Behandlung von IT-Sicherheitsvorfällen	**X**			**IT 486 c)**
Computer-Notfallteam	**X**			**IT 486 c)**
Informationssicherheit am Arbeitsplatz				**IT 486 d)**
Informationssicherheit am Arbeitsplatz	**X**			**IT 486 d)**
			X	IT 435
Mobile IT-Geräte	**X**			**IT 486 d)**
Telearbeitsplatz: Aktenverwahrung, Zutritts- und Zugriffsschutz, Dienstvereinbarung, Handhabung, Transport, ...	**X**			**IT 486 d)**
Zugangs- und Zugriffsschutz am behördlichen Arbeitsplatz	**X**			**IT 486 d)**
Dienstanweisungen erstellen	**X**			**IT 486 d)**
Schulungs- und Sensibilisierungsmaßnahmen	**X**			**IT 486 d)**
			X	IT 410
Verschlüsselungsverfahren und elektronische Signatur				**IT 486 e)**
Grundlagen der Kryptographie	**X**			**IT 486 e)**
Grundlegende Verfahren der Verschlüsselung	**X**			
			X	IT 430
Anwendungen der Verschlüsselung	**X**			**IT 486 e)**
Anwendungsszenarien von Verschlüsselung in der öffentlichen Verwaltung	**X**			**IT 486 e)**
			X	IT 430
Verfahren der elektronischen Signatur mit Bezug zur Verschlüsselung	**X**			**IT 486 e)**
			X **X**	IT 430 IT 434

Fachkompetenzen	**Basis**	**Aufbau**	**Ergänzend**	**BAköV Angebot**
		behördenangepasst		
Public Key Infrastruktur	**X**			**IT 486 e)**
				IT 430
Virtuelle Poststelle	**X**		**X**	**IT 486 e)** IT 434
Der rechtliche Rahmen von Verschlüsselung und elektronischer Signatur	**X**			**IT 486 e)**
Relevante Benutzungs- und Sicherheitsmaßnahmen / Identitäts- und Berechtigungsmanagement	**X**			**IT 486 e)**
Rechtliche Anforderungen und Datenschutzaspekte	**X**			**IT 486 e)**
			X	IT 430
Kriterien für eine Produktauswahl	**X**			**IT 486 e)**
Sicherheitsmanagement: Standards und Erstellen einer Leitlinie zur Informationssicherheit (BSI-Standard 100-1)				**IT 486 f)**
Nationale und internationale Standards im Überblick	**X**			**IT 486 f)**
Organisation eines Informationssicherheitsprozesses und Planung von Beiträgen von IT-Sicherheitsverantwortlichen zur Leitlinie	**X**			**IT 486 f)**
Mitwirkung an einer Leitlinie zur Informationssicherheit mit Entscheidungen für Sicherheitsziele im Hinblick auf Schadensszenarien	**X**			**IT 486 f)**
Erstellen einer Leitlinie zur Informationssicherheit	**X**			**IT 486 f)**
System- und anwendungsspezifische Leitlinie zur Informationssicherheit	**X**			**IT 486 f)**
Betriebswirtschaftliche Aspekte der IT-Sicherheit	**X**			**IT 486 f)**

Fachkompetenzen	**Basis**	**Aufbau**	**Ergän-zend**	**BAköV Angebot**
		behördenangepasst		
Erarbeitung eines Sicherheits-konzepts nach IT-Grundschutz (BSI-Standard 100-2)				**IT 486 g)**
Einführung in die Vorgehensweise	**X**			**IT 486 g)**
IT-Strukturanalyse	**X**			**IT 486 g)**
Schutzbedarfsfeststellung	**X**			**IT 486 g)**
Modellierung	**X**			**IT 486 g)**
Überblick: Ergänzende Sicher-heitsanalyse inkl. Restrisikobe-trachtung	**X**			**IT 486 g)**
Basis-Sicherheitscheck	**X**			**IT 486 g)**
Realisierung / Aufrechterhaltung von Informationssicherheit	**X**			**IT 486 g)**
Zertifizierung	**X**			**IT 486 g)**
Risiken- und Schwachstellen-Analyse		**X**		**IT 489 a)**
Business Continuity Management und Notfallplanung		**X**		**IT 489 b)**
Hochverfügbarkeit von Systemen, Anlagen und Prozessen		**X**		**IT 489 c)**
IT-Sicherheitskonzept für neue Verfahren / Qualitätssicherung von Anwendungen		**X**		**IT 489 d)**
Audit und Zertifizierung / Revisi-on von IT-Verfahren / Basis-Sicherheitscheck und Penetrations-test		**X**		**IT 489 e)**
Kryptokonzeption / Aufbau einer PKI		**X**		**IT 489 f)**
Virenschutz in Bundesbehörden			**X**	IT 436
IT-Sicherheit in heterogenen Net-zen			**X**	IT 440
IT-Sicherheit im Bereich der Ver-netzung			**X**	IT 455
Sichere Client-Server Architek-turen			**X**	IT 455

Fachkompetenzen	Basis	Aufbau	Ergän-zend	BAköV Angebot
		behördenangepasst		
GSTOOL – Arbeiten mit dem IT-Grundschutztool			**X**	IT 465
Datenschutz und Datensicherheit			**X**	BF 210
IT Service Management – unter Nutzung von ITIL / Einführung in Behörden			**X**	IT 250
			X	IT 255
Standards und Architekturen für E-Government Anwendungen - SAGA 4.0			**X**	IT 240
V-Modell XT		**X**		IT 230
IT-Projekte in der öffentlichen Verwaltung		**X**		IT 210
Projektmanagement		**X**		OR 500
Kommunizieren und kooperieren		**X**		KO 110
Konflikte erkennen und konstruktiv bewältigen		**X**		KO 210
Veränderungsprozesse aktiv mitgestalten		**X**		KO 240
Betreuung der Anwender in der IT			**X**	IT 510
Besprechungen leiten		**X**		KO 303
Präsentationstechnik		**X**		IT 550
Arbeitsgruppen zielorientiert leiten		**X**		FÜ 210
Methodik und Didaktik von Schulungen in der Informationstechnik		**X**		IT 520

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

9.2 Anhang zu 5.1 (Theoretischer Teil)

IT 486 **Abschnitt a**	**Informationssicherheit – warum?**
Ziel	Die Teilnehmenden sollen • Informationssicherheit im Prinzip erklären: Ziele, Werte, Anforderungen an Informationssicherheit erkennen, • Gefährdungen der Informationstechnik durch typische Schwachstellen, Benutzer und Bedrohungen der behördlichen IT von außen und von innen charakterisieren, • vielfältige Sicherheitsanforderungen in den Behörden feststellen und • die für ihre Arbeit relevanten Rollen, Aufgaben und Informationsleistungen der auf Informationssicherheit spezialisierten Bundeseinrichtungen Bundesamt für Sicherheit in der Informationstechnik und CERT-Bund kennen.
Inhalt	Informationssicherheit wird in diesem Seminar in 2 Teilen über folgende Begriffsklärungen anhand von Beispielen anschaulich und verständlich: • Gefährdungen und Risiken der Informationssicherheit (in Behörden) o Bedrohungen für IT und Informationen von innen und außen: Gefahren und Risiken beim IT-Einsatz im Behördennetz und am Arbeitsplatz: Abhängigkeit von IT-Anwendungen, Fachaufgaben und Organisationseinheiten; Sensibilisierung und Endanwendersicherheit o Informationen über Gefährdungen für IT und ihre Schwachstellen o Unterschiedliche Sicherheitsanforderungen und Schutzbedarf bezüglich Informationstechnik in Behörden: Lehr- und Rundgespräch zu E-Government-Verfahren • Ganzheitliche Informationssicherheit o Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit, Integrität, Au-

	thentizität, Verbindlichkeit o Informationssicherheit und IT-Sicherheit: Vorstellung und Diskussion unterschiedlicher Definitionen nach IT-Grundschutz des BSI (auch aus Sicherheitsschulungen bzw. Webkursen) und von Datenschutzbeauftragten o Definition und Abgrenzung von Datensicherheit, -sicherung, Authentisierung, Autorisierung, Datenschutz u.a. o Übersicht, auf welchen Ebenen Sicherheitsmaßnahmen durchgeführt werden sollten: zentral, dezentral; Infrastruktur, IT-Systeme, Netze, Anwendungen o IT-Sicherheitsstrategie des Bundes (UP Bund) o Rollen, Aufgaben und Dienstleistungen von Einrichtungen des Bundes für IT-Sicherheit: BSI und CERT-Bund o Anforderungen an IT-Sicherheitsbeauftragte

IT 486 Abschnitt b	**Informationssicherheit - Rechtliche und organisatorische Rahmenbedingungen**
Ziel	Die Teilnehmenden sollen • rechtliche Vorgaben aus Gesetzen und Regelwerken und • Verantwortung und Haftung der Zuständigen für Informationssicherheit kennen.
Inhalt	• Relevante Vorgaben aus Gesetzen wie o Bundesdatenschutzgesetz; Strafgesetzbuch; Telekommunikationsgesetz; Domänen-Recht; Signaturgesetz; Urhebergesetz u.a. • Verantwortung und Haftung der Zuständigen für Informationssicherheit (Leitung, IT-Sicherheitsbeauftragte, IT-Administration)

IT 486 Abschnitt c **IT 487**	**Informationssicherheit - Zentrale Maßnahmen**
Ziel	Die Teilnehmenden sollen • für die spätere Überprüfung von Sicherheitsmaßnahmen in einem „Basis-Sicherheitscheck“, Kenntnisse über erforderliche zentral durchgeführte Sicherheitsmaßnahmen erwerben, • die wichtigsten organisatorischen, personellen und technischen Sicherheitsmaßnahmen kennen und • Sicherheitsmaßnahmen zum Umgang mit bestimmten Techniken beurteilen.
Inhalt	Dieses Seminar ist auf wichtige Sicherheitsmaßnahmen im Netz nach IT-Grundschutz ausgerichtet: • Datensicherungskonzept o Art, Häufigkeit und Zeitpunkt o Medium und Aufbewahrungsort für Datenträger o Verantwortlichkeiten o Rekonstruktion o Anforderungen an Vertraulichkeit und Verfügbarkeit • Softwaremanagement o Einspielen von Updates und Patchmanagement • Schutz vor Schadsoftware o Definition und Wirkungsweise: Viren, Würmer, Trojaner o Wirkungsweise von Virenschutzsoftware o Automatische Update-Routinen o Virenschutzkonzept • E-Mail- und Internetsicherheit o Virenüberprüfung o Spamfilter o Phishing, Pharming o HTML-Mail o Funktionen von Proxyservern

	○ Aktive Inhalte ○ SQL-Injektion ○ zentrale Sicherheitseinstellungen • Sicherheits-Gateway (Firewall) ○ Zweck einer Firewall ○ Firewall-Architekturen ○ Firewall-Komponenten: Paketfilter, Circuit-Level Gateway, Application-Level Gateway, Stateful Inspection Gateway ○ Kriterien zur Auswahl von Firewalls ○ Personal Firewalls • Virtual Private Network (VPN) ○ Zweck und Wirkungsweise eines VPN ○ Komponenten eines VPN ○ Protokolle: L2TP, PPTP, SSL, IPsec ○ Das IVBB-Netz als Anwendungsbeispiel eines VPN: Geschlossenes Netz, Einstellungen • Sicherheitsmaßnahmen für ausgesuchte Techniken ○ WLAN ○ Bluetooth ○ Netzsegmentierung (z. B. bei hoher Vertraulichkeit, mobilen Geräten, Internet-PC) ○ Treiber • Protokollierung und Kontrolle • Physische Sicherheitsmaßnahmen ○ Objektschutz ○ Zutrittskontrolle ○ Stromversorgung ○ Brandschutz ○ Klimatisierung ○ Schutz gegen Wasser • Personelle Sicherheitsmaßnahmen ○ Funktionsbezogene Zugriffsberechtigungen ○ Regelungen bei Einstellung, Versetzung und Ausscheiden von Mitarbeitern ○ Vertretungsregelungen ○ Verpflichtung der Mitarbeiter auf Gesetze und

	andere Vorgaben • Behandlung von Sicherheitsvorfällen o Verantwortlichkeiten o Verhaltensregeln und Meldewege o Eskalationsstrategie o Prioritätenklassifizierung o Umsetzung von Maßnahmen zur Behebung von Sicherheitsvorfällen o Nachbearbeitung o Notfallhandbuch • Computer-Notfallteam • Sicherheit bei der IT-Beschaffung (Hard- und Software, zertifizierte Produkte, BSI-Zertifizierungen), Beschaffungsleitfaden

IT 486 **Abschnitt d**	**Informationssicherheit am Arbeitsplatz**
Ziel	Die Teilnehmenden sollen noch vor der Erstellung der Leitlinie zur Informationssicherheit und des Sicherheitskonzepts notwendige Grundkenntnisse über Informationssicherheit am Arbeitsplatz erwerben. Dieses Wissen können sie dann bei den Übungen zum Sicherheitskonzept anwenden. Die Teilnehmenden sollen die wichtigsten Funktionen der organisatorischen, personellen und technischen Sicherheitsmaßnahmen für Arbeitsplatzgeräte erklären, • Möglichkeiten der Sensibilisierung und Motivierung für Informationssicherheitsbelange am Arbeitplatz beurteilen • Sensibilisierungs- und Schulungskonzepte inklusive Dienstanweisung zuordnen • Quellen für Hilfsmittel kennen. Vorausgesetzt werden Grundkenntnisse über IT-Anwendungen.
Inhalt	Dieses Seminar ist auf ausgewählte Sicherheitsmaßnahmen nach IT-Grundschutz ausgerichtet: • Informationssicherheit am Arbeitsplatz: o Sichere Passwörter o Sicheres Surfen im Internet (Browser-Einstellungen, Cookies, Vermeidung aktiver Inhalte) o Herunterladen von Dateien oder Programmen aus dem Internet o Umgang mit E-Mail und -Anhängen (auch Spam, Phishing, HTML-E-Mail) o Update von Virenschutz-Software und Patches einspielen o Maßnahmen bei kurzfristiger Abwesenheit (z. B. Bildschirmschoner mit Passwortschutz) o Regelungen für Urlaub, Dienstreisen u.a. o Vertrauliche Daten

	○ Der aufgeräumte Arbeitplatz • Mobile IT-Geräte ○ Laptop, Smartphones, Blackberry, PDAs • Telearbeitsplatz: Aktenverwahrung, Zutritts- und Zugriffsschutz, Dienstvereinbarung, Handhabung, Transport, ... • Zugangs- und Zugriffsschutz am behördlichen Arbeitsplatz • Dienstanweisungen erstellen • Schulungs- und Sensibilisierungsmaßnahmen ○ Hindernisse für die Informationssicherheit, Sicherheitsfaktor Mitarbeiter ○ Sicherheitsbewusstsein, –wissen und übergeordnete Ziele ○ Warum Sensibilisierungs- und Schulungsmaßnahmen? ○ Analyse, was fehlt, Ursachen, Lösungsansätze ○ Konzeption und Planung für verschiedene Zielgruppen ○ Zielgruppen, Zuständigkeiten und Rollen, Ziele, Stufenkonzept ○ Sensibilisierung von Mitarbeitern und Vorgesetzten ○ Sensibilisierungs-Kampagnen: Beispiele, Phasen, Schritte, Methoden und Medienauswahl, Erfolgsfaktoren ○ Schulungsmaßnahmen nach BSI: Organisation, Inhalte, Planung ○ Durchführung und Materialien für Sensibilisierung und Schulung • Übung: Entwurf eines Sensibilisierungs- und Schulungskonzepts für eine Beispielbehörde, inklusive Identifikation von Zielgruppen, Inhalten und Maßnahmen im Sicherheitsprozess

IT 486 Abschnitt e	**Verschlüsselungsverfahren und elektronische Signatur**
Ziel	Die Teilnehmenden sollen • rechtliche, technische und organisatorische Grundlagen des Einsatzes von Verschlüsselungsverfahren kennen lernen, • über Aufgaben und Probleme bei der Einführung der Elektronischen Signatur und deren Einbindung in den Geschäftsprozess informiert werden und • und relevante Sicherheitsmaßnahmen wie auch das Identitäts- und Berechtigungsmanagement kennen lernen.
Inhalt	• Grundlagen der Kryptographie o Kryptologie = Kryptoanalyse + Kryptographie Abgrenzung zur Steganographie; Historischer Rückblick o Sicherheit bei Verschlüsselung o Anwendungsgebiete der Kryptographie • Grundlegende Verfahren der Verschlüsselung o Symmetrische und Asymmetrische Verschlüsselung o Vor- und Nachteile von symmetrischer und asymmetrischer Verschlüsselung o Schlüsselgrößen o Hybride Verschlüsselung • Anwendungen der Verschlüsselung o SSL-Verschlüsselung (https) o Festplattenverschlüsselung o Dateiverschlüsselung (PGP, Chiasmus) o E-Mail Verschlüsselung o Anwendungsszenarien von Verschlüsselung in der öffentlichen Verwaltung • Verfahren der elektronischen Signatur mit Bezug zur Verschlüsselung • Public Key Infrastruktur o Zertifikate

	○ Formen der Zertifizierung: Hierarchie oder Vertrauensnetze ○ Begriff der PKI ○ Signaturgesetzkonforme PKI ○ PKI des Bundes ○ Technische Lösungen ○ Bridge-CA • Virtuelle Poststelle • Überblick über rechtlichen Rahmen von Verschlüsselung und elektronischer Signatur ○ Signaturgesetz, Formanpassungsgesetz, Verwaltungsverfahrensgesetz • Relevante Benutzungs- und Sicherheitsmaßnahmen: ○ Benutzungsregeln ○ Passwortschutz, ○ Sicherer Umgang mit Schlüsseln: Hinterlegung und Weitergabe ○ Vertretungsregeln ○ Arbeiten in Gruppen ○ Unterschiedliche Schlüssel für Verschlüsselung und Signatur ○ Notfallvorsorge (Korrumpierung von Zertifikaten, Verlust von Zertifikaten, Änderung von Zertifikaten) ○ Archivierung von verschlüsselten und signierten Dateien • Identitäts- und Berechtigungsmanagement (als Anwendung zu s. o.) ○ Identifizierungs- und Authentifizierungsverfahren inkl. Biometrie ○ Konzepte und Techniken zur Verwaltung von Benutzern und Zugriffsrechten (Rollenkonzept, Verzeichnisdienste, Single-Sign-On, TCG ...) ○ Rechtliche Anforderungen und Datenschutzaspekte ○ Kriterien für eine Produktauswahl ○ Anwendungsszenarien und Übungen

IT 486 **Abschnitt f**	**Sicherheitsmanagement:** **Standards und Erstellen einer Leitlinie zur Informationssicherheit**
Ziel	Die Teilnehmenden sollen • nationale und internationale Standards benennen und einordnen können und • nach IT-Grundschutz eine Leitlinie zur Informationssicherheit für eine Behörde entwerfen.
Inhalt	• Nationale und internationale Standards im Überblick o ISO 17799 und ISO 27001 o ISO 13335 o ISO 15000 - ITIL o BSI 100-1, 100-2, 100-3 • Einführung in die Konzeption und Anwendung von IT-Grundschutz: o Sicherheitsorganisation in der Verwaltung mit IT-Zuständigen und Datenschutzbeauftragten o Sicherheitsmanagement und Kataloge mit Bausteinen, Gefährdungen und Sicherheitsmaßnahmen im IT-Grundschutz o Überblick über Analysen, Konzepte, Audit und Revision, • Sicherheitsprozess und -management nach IT-Grundschutz o Einführung von Sicherheitsmanagement in der öffentlichen Verwaltung o Verteilte Verantwortlichkeiten, Zuständigkeiten und Aufgaben für Informationssicherheit: Leitung, Sicherheitsmanagement-Team, IT-Sicherheitsbeauftragte, IT-Administratoren, Datenschutzbeauftragte, Geheimschutzbeauftragte, Anwenderbetreuer, IT-Anwender nach Vorgaben aus: BSI-Standard 100-1 • betriebswirtschaftliche Aspekte der Informationssicherheit o Abwägen von Kosten und Nutzen einer Sicherheitsmaßnahme z. B. im Hinblick auf Beschaffung

	○ Kalkulation bei Erreichen und Nicht-Erreichen von Informationssicherheit ○ Sicherheitsrisiken und Investition ○ Outsourcing von IT-Dienstleistungen • Sicherheitsaufgaben von IT-Sicherheitsbeauftragten in Organigrammen bzw. Strukturdarstellungen • IT-Sicherheitsbeauftragte im Sicherheitsmanagement-Kommunikation und Kooperation

IT 486 Abschnitt g	**Entwurf eines Sicherheitskonzepts nach IT-Grundschutz**
Ziel	Die Teilnehmenden sollen für ihre neuen Aufgaben als IT-Sicherheitsbeauftragte • Inhalt und Aufbau eines Sicherheitskonzepts kennen, • ein Sicherheitskonzept durchgängig mit der IT-Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basis-Sicherheitscheck bis zur Realisierungsplanung erarbeiten, • erworbenes organisatorisches, technisches und methodisches Wissen in Übungen zu einem durchgängigen Fallbeispiel anwenden, • soweit erforderlich, Stammdaten recherchieren und erfassen, Schutzbedarf feststellen und die Modellierung überprüfen, den Basis-Sicherheitscheck durchführen und Realisierungen von Sicherheitsmaßnahmen planen, • Maßnahmen zur Aufrechterhaltung wie Aktualisierungsüberprüfung, Sicherheitsberichte und Audits zur Revision kennen, • Möglichkeiten der Zertifizierung kennen und • trainieren, diese Aufgaben zu organisieren und zu gemeinsam abgestimmten Ergebnissen zu kommen. Voraussetzung sind Kenntnisse über Sicherheitsmanagement inklusive Leitlinie zur Informationssicherheit (Abschnitt f).
Inhalt	1) Einführung in die Vorgehensweise • Vorstellung der Vorgehensweise • Ziele, Inhalt, Aufbau • Erstellung eines Sicherheitskonzepts nach IT-Grundschutz • Was das GSTOOL unterstützen kann • Festlegen des IT-Verbundes 2) IT-Strukturanalyse • Erhebung des Netzplans: exemplarische Demonstration

	• Gruppieren von Komponenten • Übung Gruppen: Bereinigung des vorgegebenen Netzplans • Auswertung der Ergebnisse und Diskussion der Regeln • Erhebung der IT-Systeme: exemplarische Demonstration • Einführung in die Benutzungsoberfläche des GSTOOL für die Strukturanalyse • Beispielhafte Eingabe von zwei Anwendungen, einem Serverraum, einem Server, einem Client und zwei Netzkomponenten 3) Schutzbedarfsfeststellung • Vorgehen gemäß IT-Grundschutz • Die Bedeutung der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit für die Schutzbedarfsfeststellung • Definition der Schutzbedarfskategorien mit Hilfe von Schadensszenarien • Einführung in die Benutzungsoberfläche (GSHB benutzerdefiniert) für die Konkretisierung der Schutzbedarfskategorien und Hinweis, wo der Schutzbedarf eingetragen wird • Übung in Gruppen: Formulierung von Schadensszenarien aus Anwendersicht und Konkretisierung der Schutzbedarfskategorien • Vorgehensweise bei der Festlegung des Schutzbedarfs (Vererbung) • Übung: Festlegen des Schutzbedarfs für die eingegebenen IT-Anwendungen mit Hilfe von Fragen aus den Schadensszenarien und Eingabe in die Datenbank des GSTOOL. • Regeln zur Festlegung des Schutzbedarfs für IT-Systeme • Übung: Festlegen des Schutzbedarfs für die eingegebenen IT-Anwendungen und Eingabe in die Datenbank • Regeln zur Festlegung des Schutzbedarfs für Räume • Vervollständigung des Schutzbedarfsfestlegung

	in der Datenbank • Kritische Kommunikationsverbindungen • Übung: Einzeichnen der kritischen Kommunikationsverbindungen in den bereinigten Netzplan • Was ist mit der Behördenleitung abzustimmen? • Zusammenfassung Schutzbedarfsfeststellung 4) Modellierung • Überblick über vorhandene Bausteine • Aufbau der Bausteine: Gefährdungen und Maßnahmen • Überblick über die Maßnahmen: organisatorische, technische und personelle Maßnahmen • Überblick über das Schichtenmodell • Vorgehensweise, Zuordnung der IT-Komponenten zu Bausteinen der fünf Schichten • Übung: Anwendung von Bausteinen auf ausgewählte Objekte des IT-Verbundes und Ergebnisdiskussion • Einfügen und Weglassen von Maßnahmen • Modellierung zusätzlicher Komponenten • Prüfung auf Vollständigkeit und Dokumentation • Einführung in die Oberfläche „Modellierung“ und Modellierung des eingegebenen IT-Verbundes mit dem GSTOOL durchführen 5) Überblick: Ergänzende Sicherheitsanalyse inkl. Restrisikobetrachtung • Weitere Vorgehensweise nach IT-Grundschutz • Warum ist eine ergänzende Sicherheitsanalyse notwendig? • Für welche Komponenten ist eine ergänzende Sicherheitsanalyse notwendig? • Kurze Erläuterung der Vorgehensweise 6) Basis-Sicherheitscheck • Überblick: Soll-Ist-Vergleich zwischen empfohlenen und umgesetzten Maßnahmen • Hinweise zu den unterschiedlichen Maßnahmen, u.a. Grundschutz und optionale Maßnahmen, Zertifizierung

	• Vorgehensweise im Soll-Ist-Vergleich • Entscheidungsprozess beim Basis-Sicherheitscheck • Übung: Eingabe in das GSTOOL unter Einsatz von Checklisten des IT-Grundschutz an Hand der eingegebenen Beispiele 7) Realisierungsplanung • Vorgehensweise bei der Realisierungsplanung • Sichtung der Ergebnisse, Konsolidierung der Maßnahmen • Kosten- und Aufwandschätzung, Umsetzungs-reihenfolge, Verantwortliche • Einplanen von Schulungs- und Sensibilisie-rungsmaßnahmen • Berichte erstellen und Abschluss der Fallstudie o Berichte erstellen mit dem GSTOOL: Die Anwenderoberfläche, Arten von Berichten, Filter setzen o Übung: Erstellen einiger Berichte, z. B.: Grundschutzerhebung, noch nicht realisierte Maßnahmen, oder Kosten von Maßnahmen • Kurzer Überblick über weitere Funktionen des GSTOOL: o Export- und Importfunktionen, Vergabe von Berechtigungen, GSTOOL benutzerdefiniert 8) Aufrechterhaltung von Informationssicherheit • Aufgaben zur Aufrechterhaltung der Informati-onssicherheit • Überwachung und Kontrolle • Überprüfung des Sicherheitskonzepts • Audit und Change Management • IT-Krisenmanagement in der Bundesverwaltung 9) Zertifizierung • Motivation • Zertifizierungsprozess • Zertifizierungsstufen • Dokumente für das Audit

9.3 Prüfungsordnung (vom 01.01.2007; geändert am 12.09.2007und 16.10.2008)

I. Allgemeines

§ 1: Geltungsbereich

(1) Diese Prüfungsordnung gilt für die Fortbildungsmaßnahme zum IT-Sicherheitsbeauftragten in der öffentlichen Verwaltung im Sinne des Nationalen Plans zum Schutz der Informationsinfrastrukturen (NPSI). Sie regelt die Zertifizierung der Abschlüsse dieser Fortbildungsmaßnahme.

(2) Die Fortbildungsmaßnahme gliedert sich in folgende Teile

a) IT-Sicherheitsbeauftragter I - Basis

b) IT-Sicherheitsbeauftragter II - Aufbau

§ 2: Zweck der Prüfung, Zertifizierung

Die Abschlussprüfungen bilden die Abschlüsse der in § 1 dieser Prüfungsordnung genannten Fortbildungsmaßnahme. Nach erfolgreicher Absolvierung jeder Prüfung erhalten die Absolventinnen bzw. Absolventen ein Zertifikat, durch das bescheinigt wird,

a) dass sie aus Sicht des Prüfungsausschusses i. S. d. § 8 dieser Prüfungsordnung die notwendigen Kenntnisse und Fähigkeiten besitzen, um die Tätigkeit eines bzw. einer IT-Sicherheitsbeauftragten auszuüben (nach Basislehrgang)

b) dass sie aus Sicht des Prüfungsausschusses i. S. d. § 8 dieser Prüfungsordnung vertiefende Kenntnisse für die Tätigkeiten des IT-Sicherheitsbeauftragten zu speziellen Themen (der jeweiligen Abschnitte) besitzen und anwenden können. (Nach Teilnahme an einem Abschnitt des Aufbaulehrgang.)

II. IT-Sicherheitsbeauftragter I - 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 muss sich um Verantwortliche oder Beteiligte des Sicherheitsmanagements 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 lit. a dieser Prüfungsordnung genannte Prüfung können die Teilnehmenden folgende Fortbildungsmaßnahmen alternativ oder kumulativ absolvieren.

a) Ein eintägiges Seminar zu den Grundlagen der Informationssicherheit,

b) ein eintägiges Seminar zu den rechtlichen und organisatorischen Rahmenbedingungen der Informationssicherheit,

c) ein dreitägiges Seminar zu zentralen Maßnahmen in der Informationssicherheit,

d) ein zweitägiges Seminar zum Thema Informationssicherheit am Arbeitsplatz,

e) ein eintägiges Seminar zu Verschlüsselungsverfahren und zur digitalen Signatur,

f) ein zweitägiges Seminar zum Thema Sicherheitsmanagement – Standards, Leitlinie,

g) 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 bis b und f bis g aufgeführten Seminare vermittelt.

(4) Schließlich ist Teil der Fortbildungsmaßnahme auch ein eintägiger Workshop (vgl. § 5 Abs. 3). Die Teilnahme hieran ist zwingend.

§ 5: Projektarbeit und Abschlussprüfung

(1) Zur Abschlussprüfung i. S. v. § 2 lit. a zugelassen werden alle Angehörigen des in § 3 dieser Prüfungsordnung genannten Personenkreises.

(2) Die Absolventinnen und Absolventen müssen eine Projektarbeit zu einem Sicherheitsthema erstellen. Dabei können sie sich vom BSI oder/ und einer vom BSI akzeptierten Person aus ihrer Behörde beraten 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 Bestand-

teile des Projekts enthält, und bestätigt gegenüber dem Prüfungsausschuss i. S. d. § 8 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.

(3) Voraussetzung für den Erhalt des Zertifikats nach § 12 dieser Prüfungsordnung ist eine etwa 20 Minuten umfassende Präsentation der Projektarbeit gem. Absatz 2. Diese erfolgt grundsätzlich im Rahmen des Workshops nach § 4 Abs. 4 dieser Prüfungsordnung.

III. IT-Sicherheitsbeauftragter II - Aufbau

§ 6: 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 Abschlussprüfung i. S. d. § 2 lit. a) dieser Prüfungsordnung absolviert haben.

§ 7: Lehrgangsinhalt und –dauer

Die Abschnitte des Aufbauseminars zum IT-Sicherheitsbeauftragten II – Aufbau - behandeln Themen, die für die Erweiterung der Kenntnisse und Erfahrungen je nach Bedarf bzw. Aufgabengebiet benötigt werden. Hierbei werden zwei Abschnitte unterschieden:

a) IT Continuity und Notfallmanagement;
   Hochverfügbarkeit von Systemen, Anlagen und Prozessen.

b) Qualitätssicherung und Schwachstellenanalyse;
   Kryptokonzeption, Aufbau einer PKI.

Die Abschnitte dauern jeweils fünf Tage einschließlich der Abschlussprüfung.

IV. Die Abschlussprüfungen

§ 8: Umfang und Inhalt der Abschlussprüfungen

(1) Die Abschlussprüfungen sind eintägig.

(2) Gegenstand der Prüfungen i. S. d. § 2 lit. a) sind Inhalte aus den in § 4 Abs. 2 lit. a) bis g) dieser Prüfungsordnung aufgeführten Themen. Die konkreten Inhalte ergeben sich aus der aktuellen Fassung des „Handbuch IT-Sicher-

heitsbeauftragter in der öffentlichen Verwaltung“, das zur Vorbereitung auf die Prüfung zur Verfügung gestellt wird.

(3) Gegenstand der Prüfungen i. S. d. § 2 lit. b) sind Inhalte aus den in § 7 dieser Prüfungsordnung aufgeführten Themen. Dabei können die Prüflinge den Prüfungsgegenstand alternativ auf die Themen nach § 7 lit. a oder § 7 lit. b beschränken.

§ 9: Form und Durchführung der Abschlussprüfungen

(1) Die Abschlussprüfungen finden in Form von schriftlichen Multiple Choice Verfahren statt (Abschlusstest).

(2) Die Abschlussprüfungen sind nicht öffentlich.

§ 10: Verantwortliche für die Auswertung der Abschlussprüfungen

Verantwortlich für die Auswertung der Abschlussprüfungen ist der Prüfungsausschuss. Der Prüfungsausschuss wird von je einem Mitarbeiter bzw. je einer Mitarbeiterin der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern und des Bundesamtes für Sicherheit in der Informationstechnik gebildet.

§ 11: Bewertung der Prüfungsleistung

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

(2) Die Abschlussprüfungen gem. § 9 Abs. 1 dieser Prüfungsordnung gelten jeweils als bestanden, wenn mindestens 75 Prozent der möglichen Punktzahl erreicht werden.

§ 12: Wiederholungsmöglichkeiten

Die Abschlussprüfungen können jeweils einmal wiederholt werden. Die Wiederholung soll in der Regel innerhalb von zwölf Monaten nach dem erfolglosen Versuch stattfinden.

§ 13: Versäumnis, Rücktritt, Täuschung, Ordnungsverstoß

(1) Eine 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 seiner 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 einer Prüfungsleistung, kann verlangt werden, dass diese Entscheidung vom Prüfungsausschuss überprüft wird. Dies gilt entsprechend bei Feststellungen gemäß Satz 1.

§ 14: Zertifikat, Gesamtnote

(1) Über die bestandene Abschlussprüfung wird unverzüglich, möglichst innerhalb von zwei Wochen nach der Prüfung, ein Zertifikat ausgestellt.

(2) Das Zertifikat ist vom Präsidenten der Bundesakademie oder seinem Vertreter zu unterzeichnen. Das Zertifikat trägt das Datum des Tages, an dem die Prüfung bestanden worden ist.

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

§ 15: Ungültigkeit von Prüfungen

(1) Hat der Prüfling im Rahmen einer Abschlussprüfung gem. § 9 Abs. 1 dieser Prüfungsordnung getäuscht und wird diese Tatsache erst nach der Aushändigung des Zertifikats nach § 14 dieser Prüfungsordnung bekannt, so kann der Prüfungsausschuss nachträglich die Abschlussprüfung für nicht bestanden erklären.

(2) Das unrichtige Zertifikat nach § 14 dieser Prüfungsordnung ist einzuziehen und gegebenenfalls neu zu erteilen.

§ 16: 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.

V. Abschlussvorschriften

§ 17 Datenschutzerklärung

(1) Die von den Angehörigen des in § 3 dieser Prüfungsordnung genannten Personenkreises 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.

(3) Die personenbezogenen Daten werden bei der Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern aufbewahrt. 10 Jahre nach der Entscheidung über das Bestehen oder Nichtbestehen der Prüfung werden die Daten vernichtet. Personenbezogene Daten von Angehörigen des in § 3 dieser Prüfungsordnung genannten Personenkreises, die sich nicht zur Prüfung anmelden, werden 10 Jahre nach der letzten Teilnahme an einer Fortbildungsmaßnahme i. S. d. § 4 Absätze 2 oder 4 dieser Prüfungsordnung vernichtet. Personenbezogene Daten von Angehörigen des in § 6 dieser Prüfungsordnung genannten Personenkreises, die sich nicht zur Prüfung anmelden, werden 10 Jahre nach der letzten Teilnahme an einer Fortbildungsmaßnahme i. S. d. § 7 dieser Prüfungsordnung vernichtet.

§ 18: Inkrafttreten und Veröffentlichung

Diese Prüfungsordnung tritt am 1. Januar 2007 in Kraft.

9.4 Themenvorschläge für die praktische Arbeit

Aus allen Gebieten, mit denen sich IT-Sicherheitsbeauftragte beschäftigen, können Themen für Projektarbeiten formuliert und den Teilnehmern zur Ausarbeitung (und späteren Präsentation) gestellt werden:

Themenvorschlag 1:

Passen Sie die vom BSI vorgegebenen 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 Formulierung an die Belange der Behörde
- Befragen von weiteren für die Informationssicherheit Zuständigen, Abstimmen mit der Leitung, den Fachabteilungen und IT-Referaten.
- Vorstellung der zwei ausgewählten Beispiele (mit unterschiedlichem Schutzbedarf)
- schlüssige, an den eigenen Definitionen orientierte Begründung der Schutzbedarfsfeststellungen

Themenvorschlag 2:

Stellen Sie für Ihre Behörde ein Sensibilisierungs- und Schulungsprogramm zusammen.

Die Projektarbeit sollte die folgenden Aspekte berücksichtigen:

- Welche Zielgruppen müssen sensibilisiert werden?
- Welche Schulungen sind für welche Zielgruppe notwendig (sowohl Sicherheitsschulungen als auch Anwenderschulungen)?
- Welche Schulungen sind für wen in welchem Zeitraum verpflichtend?
- Wie soll die Sensibilisierung geschehen (Vorträge, Web-based Training, Intranet-Inhalte, Sensibilisierungskampagnen)? Beschreiben Sie das Vorgehen in Ihrer Behörde.
- Wie wird Sensibilisierung aufgefrischt (Intranet)?
- Welche (möglichen) Sicherheitsvorfälle sollen behandelt werden?
- Wie und von wem (extern, intern) soll die Schulung durchgeführt werden?

Themenvorschlag 3:

Stellen Sie die organisatorischen, technischen und personellen Voraussetzungen für den Einsatz eines Intrusion Detection Systems aus der Sicht des IT-Sicherheitsbeauftragten zusammen.

Die Lösung sollte 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 ein IDS arbeitet, welche Arten von IDS es gibt und wofür (wogegen) sie sinnvoll eingesetzt werden können.
- Als nächstes sind die Anwendungen und IT-Systeme zu identifizieren, die mit einem IDS überwacht werden sollen. Begründen Sie die Auswahl.
- Allerdings ist es nicht ausreichend, ein IDS zu implementieren, es muss auch das Wissen vorhanden sein, um die notwendigen Einstellungen vorzunehmen (Schulung, Einbindung von Externen).
- Außerdem fällt zusätzliche Arbeit für die IT-Gruppe an, um die Logfiles und mögliche Sicherheitsvorfälle zu untersuchen.
- Datenschutzrechtliche Aspekte, die eine Beratung mit dem Datenschutzbeauftragten und dem Personalrat erfordern.

Themenvorschlag 4:

Welche Maßnahmen sind einzuplanen, wenn in Ihrer Behörde Verschlüsselung und elektronische Signatur eingesetzt werden sollen?

Die Erarbeitung eines vollständigen Konzepts würde den Rahmen der Arbeit sprengen. Daher soll hier nur dargelegt werden, welche Vorgehensweise und Maßnahmen erforderlich sind.

Folgende Themen müssten bearbeitet werden:

- Welche Daten (E-Mails, Dokumente) sollen verschlüsselt bzw. signiert werden?
- Wo werden die öffentlichen Schlüssel gespeichert?
- Verfügbarkeitsanforderungen an den Schlüsselserver
- Wie wird der Schlüsselserver vor Missbrauch geschützt?
- Kriterien für die Auswahl eines Produkts
- Ablaufprozedur, wie die Schlüsselpaare generiert und den einzelnen Personen zugewiesen werden
- Ein Schlüsselpaar oder zwei (eines für Verschlüsselung und eines für elektronische Signatur)?
- Benennung von Verantwortlichen
- Schulungskonzept
- Wann müssen die Schlüssel gewechselt werden?

- Wie werden die persönlichen Schlüssel gespeichert?
- Datensicherung der Schlüssel und verschlüsselten Daten
- Regelungen für den Umgang mit Verschlüsselung und Signatur, zum Beispiel Vertretungsregelung, Schlüsselhinterlegung und Vorsorge für unvorsehbare Ereignisse (Krankheit, Verlust des Schlüssels)

Themenvorschlag 5:

Erstellen Sie ein Datensicherungskonzept für Ihre Behörde.

Festzulegen sind:
- Welche Daten müssen gesichert werden?
- Art der Datensicherung
- Wo werden zu sichernde Daten hinterlegt (Server)?
- Zeitpunkt und Häufigkeit
- Vorgehensweise und Speichermedium (z.B. Band, Ausweichserver in anderem RZ)
- Aufbewahrung der Datensicherungsmedien (inkl. Schutz)
- Fristen für die Aufbewahrung und Anzahl der Generationen
- Festlegen der Verantwortlichkeiten
- Übungen zur Datenrekonstruktion
- Verpflichtung der Mitarbeiter zur Datensicherung

Themenvorschlag 6:

Erarbeiten Sie eine Dienstanweisung, in der Mitarbeiter, denen ein Gerät zur mobilen Kommunikation, z.B. ein Laptop anvertraut wird, auf einen angemessenen Umgang mit diesen Geräten hingewiesen werden. Skizzieren Sie ferner technische Maßnahmen für die Sicherheit der auf den mobilen Geräten gespeicherten Daten.

Festzulegen sind:
- Konfiguration der Laptops
- Umgang mit dem Laptop unterwegs (Diebstahlsicherung)
- Schutz des Laptops (Passwort, Bios Passwort, biometrische Sicherung)
- Einwahl ins behördeninterne Netz
- Einwahl ins Internet von unterwegs oder zu Hause
- Anschluss ins Netz in der Behörde
- Virenschutzregelungen
- Verschlüsselung

Themenvorschlag 7:

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

- 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 Plugins
- Erlaubte aktive Inhalte
- Umgang mit Cookies
- Proxy-Einstellungen, Filter (Welche Seiten sind gesperrt)
- Unterschiedliche Sicherheitseinstellungen im Internet und Intranet und bei den verwendeten Browsern?

Themenvorschlag 8:

Prüfen Sie die Maßnahmen, mit denen die Serverräume Ihrer Behörde physisch 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 Maßnahmen des IT-Grundschutzes für den Serverraum beschäftigen und diese verstehen. Anschließend müssen Sie den IT-Administrator interviewen und ggf. zumindest stichprobenartig die Maßnahmen überprüfen.
In der Ausarbeitung sollten zu allen im IT-Grundschutz angegebenen Maßnahmen Erläuterungen enthalten sein.

Themenvorschlag 9:

Erstellen Sie einen Netzplan über die logische Struktur des Netzes Ihrer Behörde.
Gruppieren Sie dabei die IT-Systeme soweit wie dies sinnvoll möglich ist. Begründen Sie die vorgenommenen Gruppierungen. Stellen Sie außerdem fest, welche Kommunikationsverbindungen besonders abgesichert werden sollten. Die Einschränkung auf einen Teilbereich ist möglich.
Diese Aufgaben müssen IT-Sicherheitsbeauftragte zu Beginn der IT-Strukturanalyse und bei der Schutzbedarfsfeststellung vornehmen.

Themenvorschlag 10:

Entwerfen Sie eine Leitlinie zur Informationssicherheit für Ihre Behörde, die alle gemäß IT-Grundschutzmethodik vorgegebenen Inhalte enthält. Gehen Sie in Ihrer Skizze insbesondere auch auf die Struktur der Verantwortlichkeiten im Infomationssicherheitsprozess ein.

In der Projektarbeit sollten folgende Aspekte erläutert werden:

- Stellen Sie ein Modell des Informationssicherheitsprozesses 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
- Zeigen Sie in Schritten auf, wie Ihre Behörde zu einer wirksamen IT-Sicherheitsleitlinie kommt
- Erläutern Sie im Entwurf der Leitlinie zur Informationssicherheit Ihre Formulierung für die Bedeutung der IT für Ihre Behörde, wie wichtig die IT 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
- Erklären Sie, wie die Beschäftigten über diese Leitlinie informiert werden sollten

Themenvorschlag 11:

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 zu allen im IT-Grundschutz Baustein Computer-Virenschutzkonzept enthaltenen Maßnahmen Aussagen zu Ihrer Behörde getroffen werden.

Themenvorschlag 12:

Erarbeiten Sie eine Vorlage zur Entscheidung für die Behördenleitung, in der Sie verschiedene Firewallkonzepte sowie deren Vor- und Nachteile skizzieren und begründen Sie, welches das geeignete Konzept für Ihre Behörde ist.

Sinn dieser Aufgabe ist, die verschiedenen Firewallkonzepte zu verstehen und eine Auswahl und ihren Einsatz in der Behörde zu begründen.

Themenvorschlag 13:

Entwerfen Sie einen Fragebogen, mit dessen Hilfe Sie die Akzeptanz verschiedener einschränkender Sicherheitsmaßnahmen bei den Benutzern testen:

a) der Verschluss von Laufwerken an den Clients,
b) das Verbot, eigenmächtig Programme zu installieren
c) Internetfilter
d) Passwortregelungen (Anforderung an die Güte und Länge der Passwörter, regelmäßiger Passwortwechsel, Umgang mit dem Passwort)
e) das Verbot, Brandschutztüren offen zu halten

f) Sperrung des APC bei Verlassen des Raumes, Einsatz von Bildschirmschonern

Entwerfen Sie ferner kurze Erläuterungstexte, in denen Sie den Benutzern den Sinn der jeweiligen Maßnahmen begründen.

Themenvorschlag 14:

Angenommen, es wird von Ihrer Behördenleitung erwogen, die beiden Aufgaben Administration der Firewall und Durchführung der Datensicherung für einen Standort der Behörde an ein externes Dienstleistungsunternehmen zu vergeben.
Erstellen Sie eine Präsentation, in der Sie der Behördenleitung die Vor- und Nachteile einer solchen Lösung darstellen und Anforderungen formulieren, die ein Dienstleistungsunternehmen für diese Aufgaben 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, Hackereinbruch, Systemzusammenbruch durch technisches Verfahren).
Allgemein beschrieben sind die Maßnahmen bei Sicherheitsvorfällen im IT-Grundschutz M 6.60.
Diese und insbesondere die Meldewege sind auf die Behörde angepasst in der Ausarbeitung zu spezifizieren.

Themenvorschlag 16:

Stellen Sie die wesentlichen Anwendungen zusammen, die in Ihrer Behörde eingesetzt werden. Bestimmen Sie für jede Anwendung anhand zuvor festgelegter Kriterien, welchen Bedarf an Verfügbarkeit sie hat, und beschreiben Sie für zwei bis drei Anwendungen mit höheren Verfügbarkeitsanforderungen, mit welchen Maßnahmen Sie diese Anforderungen gewährleisten wollen.

Die Ausarbeitung sollte enthalten:

- Spezifikation für normale, hohe und sehr hohe Verfügbarkeit
- Begründung für die Verfügbarkeitsanforderungen von ca. 10 Anwendungen
- Maßnahmen für zwei bis drei Anwendungen, die zu einer hohen Verfügbarkeit der Anwendungen beitragen

Themenvorschlag 17:

Ihre IT-Administration schlägt den Einsatz von Security Scannern vor. Informieren Sie sich über Arten und Leistungen von Security Scannern auf dem Markt.

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 sollte.

Themenvorschlag 18:

Entwerfen Sie eine Struktur (Gliederung) mit allen wesentlichen Inhalten zur Informationssicherheit, die von unterschiedlichen Benutzergruppen aus Ihrem (Behörden) Intranet abgerufen werden können.
Schlagen Sie eine sinnvolle Struktur vor und ordnen Sie Themen zu und erläutern Sie das Informationsangebot (inklusive Aktualisierung).

Themenvorschlag 19:

Ihre Behörde plant die Einführung eines chipkartengestützten Zeiterfassungssystems. Eine wesentliche Komponente soll ein zentraler Server sein, auf dem die Zeitdaten aller Beschäftigten gespeichert sind, zusammen mit allen anderen Daten, die für die Lohn- und Gehaltsabrechnung bedeutsam sind.
Stellen Sie die wichtigen Sicherheitsanforderungen an die Anwendung und an den Server zusammen.

Themenvorschlag 20:

In einer Behörde ist ein homogenes Windows XP-Netz mit entsprechenden Clients und Servern eingerichtet.
Entwerfen Sie eine Sicherheitsrichtlinie für die Clients, die ausschließlich für übliche Büroanwendungen und E-Mail benutzt werden.
Begründen Sie Ihre Entscheidungen.

Themenvorschlag 21:

In Ihrer Behörde ergibt sich die Notwendigkeit funkgebundener Kommunikation, 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 22:

Ihre Behörde plant eine Zertifizierung nach ISO 27001 auf Basis von IT Grundschutz. Erstellen Sie hierfür einen Projektplan.
Berücksichtigen Sie dabei maßgebliche Komponenten, wie

- Initiierung des Informationssicherheitsprozesses

- Definition des betrachteten IT-Verbundes, der Leitlinie zur Informationssicherheit und die Einrichtung des Sicherheitsmanagements.

- Durchführung einer IT-Strukturanalyse
  - Erfassung Komponenten des IT Verbundes IT-Anwendung, IT-System, Raum und Kommunikationsverbindung
- Durchführung einer Schutzbedarfsfeststellung
  - Festlegen mit einer auf den IT-Verbund angepassten Definition der Schutzbedarfskategorien, die in der Institution abgestimmt ist.
- Modellierung nach IT-Grundschutz
  - Modellierung nach IT-Grundschutz (Phase 4) unter Zuhilfenahme des GSTOOL
- Durchführung des Basis-Sicherheitsscheck
  - Durchführung des Basis-Sicherheitsscheck unter Verwendung des GSTOOL

Themenvorschlag 23:

In Ihrer Behörde fallen Daten an, die bezüglich der Grundwerte Vertraulichkeit, Integrität und Authentizität einen höheren Schutzbedarf benötigen. Zum Schutz der genannten Grundwerte sollen kryptographische Verfahren eingesetzt werden.
Entwickeln Sie zum Schutz dieser Daten ein Kryptokonzept unter Berücksichtigung des BSI Kryptoleitfadens und der BSI Arbeitshilfe zur Erstellung von Kryptokonzepten.

Themenvorschlag 24a:

In Ihrer Behörde steht eine Migration von Clients an. Evaluieren Sie aus Sicht des IT-Sicherheitsbeauftragten, welche Auswirkungen diese geplante Migration auf Sicherheitsaspekte hat. Entwickeln Sie eine Entscheidungsvorlage für ihre Behördenleitung zur Migration der Clients. Begründen Sie ihre Entscheidung, indem Sie auf technische und organisatorische Maßnahmen eingehen.

Themenvorschlag 24b:

In Ihrer Behörde steht eine Migration der Serverumgebung an. Evaluieren Sie aus Sicht des IT-Sicherheitsbeauftragten, welche Auswirkungen diese geplante Migration auf Sicherheitsaspekte hat. Entwickeln Sie eine Entscheidungsvorlage für ihre Behördenleitung zur Migration der Umgebung. Begründen Sie ihre Entscheidung, indem Sie auf technische und organisatorische Maßnahmen eingehen.

Anm.: Themen 24a und 24b können auch zusammengelegt werden. Hier ist jedoch der Aufwand zu beachten

Themenvorschlag 25:

In Ihrem IT-Umfeld wird bei der Schutzbedarfsanalyse ein höherer Schutzbedarf identifiziert. Im Rahmen der IT-Grundschutz-Vorgehensweise wird zunächst in einer ergänzenden Sicherheitsanalyse untersucht, welche Zielobjekte mit Hilfe einer Risikoanalyse genauer untersucht werden müssen.
Berücksichtigen Sie dabei maßgebliche Komponenten, wie

- Erstellung einer Gefährdungsübersicht
- Ermittlung zusätzlicher Gefährdungen
- Bewertung der Gefährdungen
- Behandlung der Risiken und Maßnahmenauswahl
- Konsolidierung des Sicherheitskonzepts

Themenvorschlag 26:

In Ihrer Behörde ist ein Geschäftsprozess besonders wichtig. Analysieren Sie die Verfügbarkeitsanforderungen dieses Prozesses und die Auswirkungen, die der Ausfall dieses Prozesses auf Ihre Behörde hätte. Entwerfen Sie Maßnahmen, bezogen auf

- Infrastruktur
- Organisation
- Personal
- Technik
- Kommunikation

die für die Aufrechterhaltung (und Wiederanlauf) des Prozesses notwendig sind. Beachten Sie auch sog. Sofortmaßnahmen.

Themenvorschlag 27:

In Ihrem Hause steht mittelfristig eine Informationssicherheitsrevision auf Basis von IT-Grundschutz an. Entwickeln Sie einen Maßnahmenplan oder Projekt-plan, um sich einen Überblick über das Thema „IS-Revision“ zu verschaffen. Machen Sie sich durch Ihren Maßnahmenplan mit den Voraussetzungen und dem Ablauf einer IS-Revision vertraut.

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 kann, erfolgt eine Begründung durch den Prüfungsausschuss.
- Der Betreuer hat die Möglichkeit bei der Präsentation der Arbeit anwesend zu sein. Eine Teilnahme ist jedoch nicht erforderlich.

Zielsetzung

- Der Kandidat soll mit der Projektarbeit dokumentieren,
  - dass er im Tätigkeitsbereich eines 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 IT-Sicherheitsbeauftragten.

  Nach der Benennung des Betreuers der Projektarbeit soll die Initiative bei der Erstellung der Projektarbeit **immer** vom Kandidaten ausgehen. Der Betreuer sollte hinzugezogen werden, wenn fachliche Fragestellungen oder Unsicherheiten auftreten. Insbesondere, wenn der Kandidat noch keine größere Erfahrung als IT-Sicherheitsbeauftragter 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 dem Betreuer 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 dem Betreuer) im Vorfeld abzuschätzen und evtl. zu prüfen, ob der Aufwand (auch für den Betreuer) vertretbar ist.
- Für die Aufwendungen der Betreuer 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 des 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 Fachlicher Berater (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 schnelle Entscheidung für ein Thema zu treffen. Der Beratungswunsch wird über die BAköV an das BSI weitergegeben.
- Besprechung der Arbeit mit dem Fachlichen Berater.
- Vorlage der Arbeit spätestens **2 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 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, wie Beamer oder Overhead-Projektor 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 der Zuhörer kennt	je Aufzählungspunkt maximal zwei Zeilen

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

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 Teilnehmer der Veranstaltung weitergegeben.

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

9.7 Formulare

9.7.1 Fortbildungsantrag I –Basis

9.7.2 Plan der Projektarbeit

9.7.3 Änderungs-/Ergänzungsmitteilung

9.7.4 Fortbildungsantrag II- Aufbau

9.7.5 Fortbildungsantrag III- Aufbau

9.7.6 Antrag: Zertifikatsverlängerung

9.7.1 Fortbildungsantrag I – Basis

Bundesministerium
des Innern

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.

Wurden Sie bereits bei einer anderen Stelle zertifiziert?

☐ nein ☐ ja Bezeichnung der Stelle, Zertifikat u. Zeitpunkt:

A. Informationen zum Antragsteller

(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:

Fortbildungsbeauftragter:
Telefon:

(3) Informationen zur Berufserfahrung und Tätigkeit

Aktuelle Tätigkeit:

Arbeitszeit:	☐ Vollzeit	☐ Teilzeit	Umfang .....Std.
Tätigkeit als IT-Sicherheitsbeauftragte:	☐ Vollzeit	☐ Teilzeit	Umfang .....%

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):

B. 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
☐ Grundlagen der Informationstechnik und Informationssicherheit		IT 485.___	
☐ Abschnitt a – Informationssicherheit – warum?		IT 486.___a	
☐ Abschnitt b – Informationssicherheit – Rechtliche und organisatorische Rahmenbedingungen		IT 486.___b	
☐ Abschnitt c – Informationssicherheit – zentrale Maßnahmen		IT 486.___c	
☐ Abschnitt d – Informationssicherheit am Arbeitsplatz		IT 486.___d	
☐ Abschnitt e – Verschlüsselungsverfahren und elektronische Signatur		IT 486.___e	
☐ Abschnitt f – Informationssicherheitsmanagement – Standards, Leitlinien		IT 486.___f	
☐ Abschnitt g – Entwurf eines Sicherheitskonzepts nach IT-Grundschutz		IT 486.___g	
☐ Basisseminar Kompakt		IT 487.___	

Für das Thema der Projektarbeit (Vorschlag) verwenden Sie bitte das Formblatt „Plan der Projektarbeit“ (9.7.2). Bitte geben Sie an, ob Sie einen Fachlichen Berater aus der eigenen Behörde oder des BSI (BSI-Berater nur für Bundesbedienstete) in Anspruch nehmen wollen.	

☐	Fachlicher Berater des BSI	☐ Fachlicher Berater in der Behörde (Eintrag unter C 2b.)

☐ Projektpräsentation – Workshop		IT 488.___	
☐ Prüfung		IT 491.___	

Ort, Datum Unterschrift/Stempel Lernprozessbegleiter

C. Informationen zum Betreuungssystem / Unterstützungssystem

(1) Lernprozessbegleiter der BAköV*

Name: Vorname:

Bundesakademie für öffentliche Verwaltung – Lehrgruppe 5

Willy-Brandt Straße 1

50321 Brühl

Telefon: 0228 / 99629 - 0 Fax: 0228 / 99629 - 5555

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

(2) a. Fachlicher Berater des BSI *

Name: Vorname:

Organisationseinheit:

Godesberger Allee 185 -189

53175 Bonn

Telefon: Fax:

E-Mail:

b. Fachlicher Berater in der eigenen Behörde

Name: Vorname:

Behörde/Institution:

Straße / Postfach:

PLZ: Ort:

Organisationseinheit / Tätigkeit:

Telefon: Fax:

E-Mail:

* Wird von der BAköV ergänzt.

D. Erklärung des Antragstellers

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. Der Lernprozessbegleiter nimmt eine beratende Funktion ein.

Ich erkläre mein Einverständnis, dass vorstehende Daten unter Beachtung der Vorschriften des Bundesdatenschutzgesetzes (BDSG) mittels EDV verarbeitet und gespeichert werden. Ich versichere mit meiner Unterschrift die Richtigkeit der in diesem Antrag von mir getätigten Angaben.

_____

Ort, Datum

_____

Unterschrift Antragsteller

Ich bestätige die vorstehend gemachten Angaben zum Fortbildungsplan.

_____

Ort, Datum

_____

Unterschrift Fortbildungsbeauftragter

9.7.2 Plan der Projektarbeit

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 Unterschrift/Stempel Fachlicher Berater

9.7.3 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

9.7.4 Fortbildungsantrag II - Aufbau

Grundlage für den Fortbildungsplan II-Aufbau sind die Vorgaben und Bedürfnisse der Behörde des Kandidaten. Die Abschnitte der Aufbauseminare haben eigenständige Inhalte. Um das Zertifikat zu erwerben, ist der Besuch mindestens eines Abschnitts (a oder b) und das Bestehen der jeweiligen Prüfung notwendig.

Die Termine für die einzelnen Fortbildungsabschnitte werden 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:

Fortbildungsbedarf	Wunschtermin	BAköV Veranstaltung	Bestätigung / Änderung
☐ **Abschnitt a** IT Continuity und Notfallmanagement; Hochverfügbarkeit von Systemen, Anlagen und Prozessen;		IT 489.___a	
☐ **Abschnitt b** Qualitätssicherung und Schwachstellenanalyse; Kryptokonzeption und Aufbau einer PKI;		IT 489.___b	

Ort, Datum Unterschrift Antragsteller

Ort, Datum Unterschrift Lernprozessbegleiter

9.7.5 Fortbildungsantrag III - Aufbau

Nach Erwerb der Zertifikate der Stufe I und II kann der IT-Sicherheitsbeauftragte in einer dritten Stufe eine tiefergehende behördenangepasste Spezialisierung seiner Ausbildung erlangen. Der Antrag der Stufe III wird nach Abstimmung mit allen Beteiligten der BAköV vorgelegt.

Name: Vorname:

Behörde:

Zertifikatsnummer Stufe I: Zertifikatsnummer Stufe II:

Thema und Beschreibung der Studie (wird in Absprache mit dem BSI festgelegt)
Erstellungszeitraum der Studie:

Von: bis:

Bezeichnung der Studie

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

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

Ort, Datum Unterschrift Antragsteller

Ort, Datum Unterschrift Fortbildungsbeauftragter

Ort, Datum Unterschrift/Stempel Fachlicher Berater

9.7.6 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

Bestätigung des zuständigen Fortbildungsbeauftragten über die besuchten Seminare.

Ort, Datum

Unterschrift Fortbildungsbeauftragter

Ort, Datum

Unterschrift/Stempel Lernprozessbegleiter

10 Muster Zertifikat

Bundesministerium
des Innern

Zertifikat

Herr Max Mustermann,
geboren am 01.02.1955,

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 I

gemäß Prüfungsordnung vom 01.01.2007 erlangt.
Das Zertifikat basiert auf den BSI Standards 100-1 bis 100-3.

Zertifikatsnummer:	30042007-A001
Zeitpunkt der Prüfung:	30.04.2007
Ablauf der Gültigkeit des Zertifikats:	29.04.2012

Bundesministerium des Innern 20

Brühl, den 30.04.2007

Günther Wurster, Präsident der BAköV

BAköV

BSI Bundesamt für Sicherheit in der Informationstechnik

Ihre Ansprechpartner

Für die BAköV:

BAköV - Lehrgruppe 5
Tel.: 0228 / 99629 - 0
Fax: 0228 / 99629 - 5555
sibe-lg5@bakoev.bund.de
http://www.bakoev.bund.de

Für das BSI:

BSI - Referat 113
Tel.: 0228 / 999582 - 5220
Fax: 0228 / 99109582 - 5220
sibeforum@bsi.bund.de
http://www.bsi.bund.de

Bundesakademie für öffentliche Verwaltung
im Bundesministerium des Innern

Willy-Brandt Straße 1
50321 Brühl

Tel.: 0228 / 99629 - 0
Fax: 0228 / 99629 - 5555

http://www.bakoev.bund.de
https://www.lernplattform-bakoev.bund.de
http://www.ifos-bund.de