Bundesamt
für Sicherheit in der
Informationstechnik

Anlage 1 zur Verfahrensbeschreibung zur
Kompetenzfeststellung und Zertifizierung von Personen (VB-Personen):

Programm zur Kompetenzfeststellung und Zertifizierung von Personen

Prog-Personen

Version	3.5
Stand	02.02.2018

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

Tel.: +49 22899 9582-0
E-Mail: auditor@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik führt im Bereich der Konformitätsbewertung Zertifizierungen von Personen auf Grundlage des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz, [BSIG]) vom 14. August 2009 durch.

Zur Durchführung von Evaluierungen und Prüfungen zum Zwecke der Zertifizierung von Produkten und Managementsystemen sowie zur Unterstützung des BSI im Bereich IT-Sicherheitsdienstleistungen werden qualifizierte Personen benötigt.

Das vorliegende Dokument beschreibt das Programm zur Kompetenzfeststellung und Zertifizierung von Personen (kurz: **Programm**, [Prog-Personen]). Es beschreibt die verschiedenen Personengruppen sowie die Kompetenzanforderungen an diese Personengruppen.

Aus Gründen der Lesbarkeit wurde in diesem Dokument nur die männliche Form für die Bezeichnung der Personengruppe gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige beider Geschlechter.

Eine ***Zertifizierung von Personen*** wird für folgende Personengruppen durchgeführt:

1. **Zertifizierung als Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz** (kurz: **Auditteamleiter**) - für die Durchführung von Audits für Organisationen, die ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz [IT-GS] erhalten und aufrechterhalten wollen.
2. **Zertifizierung als Auditor „De-Mail“**- für die Durchführung von Audits für Organisationen, die ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz [IT-GS] (aufrecht) erhalten wollen und eine Akkreditierung als De-Mail-Diensteanbieter anstreben.
3. **Zertifizierung als Auditor „Secure CA Operation“** - für die Durchführung von Audits für Organisationen, die eine Zertifizierung nach BSI [TR-03145] inklusive eines Zertifikats nach ISO 27001 für den Betrieb einer Certification Authority anstreben.
4. **Zertifizierung als IS-Revisions- und IS-Beratungs-Experten** (kurz: **IS-Revisor**) - für die Unterstützung von Bundesbehörden bei der Erstellung und Umsetzung von Sicherheitskonzepten sowie die regelmäßige Durchführung von IS-Revisionen gemäß “Leitfaden für die Informationssicherheitsrevision auf der Basis von IT-Grundschutz” [REV].
5. **Zertifizierung als Penetrationstester** - für die Unterstützung von Bundesbehörden bei der Durchführung von Penetrationstests.
6. **Zertifizierung als Auditor „Smart Meter Gateway Administration“** für TR-03109-6 – für die Durchführung von Audits des IT-Betriebs beim Smart Meter Gateway Administrator gemäß Messstellenbetriebsgesetz.
7. **Zertifizierung als Auditor „Sicherer E-Mail Transport“** - für die Durchführung von Audits für Organisationen, die eine Zertifizierung nach [BSI TR-03108] für den Betrieb eines E-Mail Dienstes anstreben.
8. **Zertifizierung als Auditor RESISCAN** - für die Durchführung von Audits für Organisationen, die eine Zertifizierung nach [BSI TR-03138] „Ersetzendes Scannen“ zur sicheren Gestaltung ihrer Prozesse für das ersetzende Scannen anstreben.

Eine ***Kompetenzfeststellung*** von Personen im Rahmen der ***Anerkennung von Stellen und Zertifizierung von IT-Sicherheitsdienstleistern*** wird für folgende Personengruppen durchgeführt: [1]

.

1. **BOS-Interoperabilitätsprüfer** für die Durchführung von IOP-Prüfungen, die ein Zertifikat nach den Interoperabilitätsrichtlinien der BDBOS [BOS-IOP-Richtlinien] erhalten.
   Die Kompetenzfeststellung wird in folgenden Geltungsbereichen durchgeführt:
   - Durchführung von IOP-Prüfungen für Endgeräte im Digitalfunk BOS,
   - Durchführung von IOP-Prüfungen für Leitstellen im Digitalfunk BOS.
2. **ZPL-Mitarbeiter** für die Konfiguration und Bereitstellung eines Zertifizierungsprüflabors (ZPL) für den Digitalfunk BOS.
3. **CC-Evaluatoren** für die Durchführung von Zertifizierungsverfahren im Bereich der Common Criteria (CC - Kriterien zur Prüfung und Bewertung der Sicherheit von IT-Produkten).[2]

1 Die Anforderungen zur Kompetenzfeststellung von TR-Prüfern sind dem Dokument „Kompetenzfeststellung als Prüfer im Bereich Technischer Richtlinien“ zu entnehmen. [TR-Prüfer]

2 Das Dokument zu Punkt 3 befindet sich noch in der Entwicklung und ist nicht Bestandteil dieses Dokuments.

2 Zertifizierung von Personen

Neben der ***Grundpauschale*** sowie den Kosten für eine ***Vor-Ort-Begutachtung*** werden weitere Pauschalen für die Qualifizierungsmaßnahmen in Rechnung gestellt. Die Höhe dieser Kosten können dem jeweiligen Antrag entnommen werden.

2.1 Zertifizierung als Auditteamleiter

Vor der Erteilung eines „ISO 27001-Zertifikats auf der Basis von IT-Grundschutz“ [IT-GS] ist ein Audit des betrachteten Informationsverbundes gemäß der aktuellen Fassung der Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Auditierungsschema“ durchzuführen.

Dieses Audit wird von Auditteamleitern durchgeführt, die in einem Personenzertifizierungsverfahren als Person ihre Fachkenntnisse im Bereich Informationssicherheit und IT-Grundschutz sowie ihre Befähigung zur Durchführung dieser Audits vorab ausreichend nachgewiesen haben und somit vom BSI zertifiziert wurden.

Grundlage des Zertifizierungsverfahrens bilden hierbei das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz [BSIG]) vom 14. August 2009, die Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung – BSIZertV [BSIZertV]) vom 07. Juli 1992 sowie die ISO/IEC 27006 [ISO 27006], eine Norm für Stellen, die Audits und Zertifizierungen von Informationssicherheitsmanagementsystemen (ISMS) anbieten.

2.1.1 Die persönlichen Eigenschaften eines Auditteamleiters

Im Folgenden sind die persönlichen Eigenschaften eines Auditteamleiters dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills" nur eingeschränkt im Rahmen eines Zertifizierungsverfahrens bewertet werden können.

2.1.1.1 Managementfähigkeiten

- Praktische Führungsfähigkeiten
- Organisatorische Fähigkeiten
- Unternehmerisches Denken
- Durchsetzungsstärke
- Zielorientiertes Denken und Handeln

2.1.1.2 Kommunikationsfähigkeiten

- Umfassende und sachliche Berichterstattung
- Behandlung von Einwänden
- Beherrschung von Moderations- und Audittechniken
- Managen von Konflikten
- Überzeugungsfähigkeit

2.1.1.3 Didaktische Fähigkeiten

- Objektive Ergebnispräsentation

2.1.1.4 Methodenkompetenz

- Motivationsfähigkeit
- Schaffung eines angenehmen Gesprächsklimas
- Konzentration auf das Wesentliche
- Kreativität

2.1.1.5 Soziale Kompetenz

- Aufgeschlossenheit und Freundlichkeit
- Schnelle Auffassungsgabe
- Gesundes Urteilsvermögen
- Analytische Fähigkeiten
- Beharrlichkeit
- Fachliche und persönliche Reife
- Bereitschaft zur Weiterbildung
- Psychologisches Einfühlungsvermögen/Empathie
- Kontaktfähigkeit
- Gewissenhaftes Handeln
- Konstruktiver Umgang mit Kritik und Lob
- Glaubwürdigkeit
- Teamfähigkeit
- Partnerschaftliches Verhalten
- Optimismus
- Belastbarkeit
- Sachlichkeit insbesondere bei heiklen Sachverhalten
- Selbstbewusstsein

2.1.1.6 Unabhängigkeit

- Unabhängigkeit vom Auditierten
- Unbeeinflussbarkeit und Unvoreingenommenheit
- Unbedingte Verschwiegenheit
- Unbestechlichkeit
- Fähigkeit zur Argumentation auf Basis objektiver Nachweise

2.1.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise geprüft (siehe „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“).

2.1.2.1 Bildungsabschluss

Anforderung

Der Kandidat muss eine Ausbildung abgeschlossen haben, in der er grundlegende Kenntnisse und Fähigkeiten für seine spätere Tätigkeit als Auditteamleiter erlangt hat. Hierzu zählt beispielsweise ein(e) abgeschlossene(s) Ausbildung oder Studium im Bereich IT und/oder Informationssicherheit.

Sollte der Kandidat mit der abgeschlossenen Ausbildung bzw. dem Tätigkeitsfeld, in dem die Ausbildung abgeschlossen wurde, nicht die erforderlichen Kenntnisse und Fähigkeiten (im Bereich IT und/oder Informationssicherheit sowie Auditierung) erlangt haben, so muss ein Nachweis erbracht werden, dass diese über vergleichbare berufsbegleitende Fortbildungen (z.B. Fortbildungen im Bereich IT und/oder Informationssicherheit) erworben worden sind.

Falls der Kandidat die Anforderungen an Ausbildung und vergleichbare Fortbildungen nicht nachweisen kann, so muss alternativ ein Nachweis erbracht werden, dass die erforderlichen Kenntnisse und Fähigkeiten durch einschlägige Berufserfahrung über mindestens 8 Jahre im Bereich IT, davon mindestens 5 Jahre im Bereich Informationssicherheit erworben worden sind.

Nachweis

Ein Zeugnis des Ausbildungsabschlusses und gegebenenfalls Bescheinigungen der Teilnahme an Fortbildungsveranstaltungen oder ein Zeugnis/eine unterschriebene Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung ist vorzulegen.

2.1.2.2 Berufserfahrung

Anforderung

Der Kandidat muss aus den letzten 8 Jahren mindestens 5 Jahre fachspezifische, praktische Berufserfahrung gerechnet auf Vollzeit im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit nachweisen. Hierbei finden alle Zeiten Berücksichtigung, die nach Abschluss der entsprechenden Ausbildung (siehe Bildungsabschluss) erbracht wurden.

Des Weiteren muss der Kandidat bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 [ISO 27006] akkreditierten Zertifizierungsstelle im Bereich ISO 27001 als Auditor beschäftigt sein und innerhalb der letzten 3 Jahre mindestens ein ISO 27001-Zertifizierungsaudit geleitet haben. Dies schließt eine Beschäftigung als externer Auditor (nach ISO/IEC 27006 Abschnitt 7.3 [ISO 27006]) ein.

Nachweis

Ein Zeugnis oder eine unterschriebene Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Beschäftigung als Auditor. Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung. Des Weiteren muss ein Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle bspw. in Form der Kopie der Akkreditierungsurkunde vorgelegt werden.

2.1.2.3 Praxiserfahrung

Anforderung

Der Kandidat muss

- in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum),
- an 4 Zertifizierungsaudits (Drittparteien-Audits) im Bereich Informationssicherheit mit mindestens je 3 Personentagen (davon mindestens 1 Audit durchgängig nach BSI-Standard 100-2 [BSI100]),

  Hinweis:
  Hierzu zählen alle externen, unabhängig durchgeführten Audits, die im Bereich Informationssicherheit zu Zertifikaten oder vergleichbaren Abschlüssen geführt haben. Diese Zertifikate müssen nicht vom BSI ausgestellt worden sein.
- als Auditor, Auditor-Trainee oder technischer Experte,
- mit einem Gesamtumfang von mindestens 20 Personentagen

teilgenommen haben.

Bei mindestens 3 dieser Audits muss der Kandidat am gesamten Audit beteiligt gewesen sein.

Alternativ muss der Kandidat

- in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum),
- an 6 *Erstparteien-Audits* oder *Zweitparteien-Audits* im Bereich Informationssicherheit mit mindestens je 3 Personentagen (davon mindestens 1 Audit durchgängig nach BSI-Standard 100-2 [BSI100]),
- als verantwortlicher Auditor,
- mit einem Gesamtumfang von mindestens 20 Personentagen

teilgenommen haben.

Bei allen 6 Audits muss der Kandidat am gesamten Audit teilgenommen haben.

Nachweis

Vom Auftraggeber oder Arbeitgeber bestätigte und unterschriebene Kurzberichte über die Durchführung der Audits bzw. bei Zertifizierungsaudits die Vorlage der erlangten Zertifikate, falls die Teilnahme des Kandidaten und die Dauer des Audits daraus ersichtlich ist. Im Kurzbericht sind anzugeben:

- die wesentlichen Ziele sowie der Gegenstand des Audits,
- die Audit-Vorgehensweise (Dokumentenprüfung, Vor-Ort-Prüfung, Auditbericht, etc.),
- die Rollenverteilung im Audit, insbesondere die Position/Verantwortung des Kandidaten,
- der Zeitraum und Umfang (Personentage) des Audits[3].

Die Angaben im Kurzbericht können (zum Beispiel bei Projekten mit Dritten) auch anonymisiert erfolgen.

3 Falls mehrere Personen am Audit beteiligt waren oder der Kandidat neben dem Audit noch andere Tätigkeiten vorgenommen hat (beispielsweise Beratung) so ist nur die Anzahl der Personentage anzugeben, die der Kandidat für den Auditanteil aufgewandt hat.

2.1.2.4 Qualifizierungsmaßnahmen

Anforderung

Der Kandidat muss

- in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum), an einer mindestens 3-tägigen IT-Grundschutzschulung (nach BSI-Standard 100 [BSI100]) mit bestandener Abschlussprüfung teilgenommen haben und
- eine mindestens 5-tägige Ausbildung zum Auditor für ISO 27001 mit bestandener Abschlussprüfung vorweisen.

Nachweis

- Teilnahmebescheinigungen,
- Prüfungszeugnisse,
- Zertifikate.

2.1.2.5 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Anforderung	*Erläuterung*	*Nachweis*
Bildungsabschluss	• abgeschlossene Berufsausbildung • ggf. Fortbildungen • oder mindestens 8 Jahre Berufserfahrung im Bereich IT, davon mindestens 5 Jahre im Bereich Informationssicherheit	• Zeugnis Ausbildungsabschluss oder • Zeugnis Ausbildungsabschluss und Bescheinigung der Teilnahme an Fortbildungen oder Zeugnis/Bestätigung eines Dritten über die Berufserfahrung
Berufserfahrung	• In den letzten 8 Jahren mindestens 5 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit • Beschäftigung als Auditor bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 akkreditierten Zertifizierungsstelle im Bereich ISO 27001 und innerhalb der letzten 3 Jahre Leitung von mind. 1 ISO 27001-Zertifizierungsaudit[4]	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Beschäftigung als Auditor • Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle, z.B. durch Kopie der Akkreditierungsurkunde

4 Dies schließt eine Beschäftigung als externer Auditor (nach ISO/IEC 27006 Abschnitt 7.3 [ISO/IEC 27006] ein.

Anforderung	*Erläuterung*	*Nachweis*
Praxiserfahrung/Auditerfahrung Alternative I	• In den letzten 3 Jahren • 4 Zertifizierungsaudits im Bereich Informationssicherheit mit mindestens je 3 Personentagen, davon mindestens 1 Audit durchgängig nach BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ [BSI100] • als Auditor, Auditor-Trainee oder technischer Experte • Gesamtumfang mindestens 20 Personentage • bei mindestens 3 der Audits Beteiligung am gesamten Audit	• Vom Auftraggeber/Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate
Praxiserfahrung/Auditerfahrung Alternative II	• In den letzten 3 Jahren • 6 Erstparteien-Audits oder Zweitparteien-Audits im Bereich Informationssicherheit mit mindestens je 3 Personentagen, davon mindestens 1 Audit durchgängig nach BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ [BSI100] • als verantwortlicher Auditor (und damit am gesamten Audit beteiligt) • Gesamtumfang mindestens 20 Personentage • bei allen Audits Beteiligung am gesamten Audit	• Vom Auftraggeber/Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate
Qualifikation	• in den letzten 3 Jahren Teilnahme mind. 3-tägiger IT-Grundschutz-Schulung (BSI-Standard 100 [BSI100]) • mind. 5-tägige Ausbildung zum Auditor für ISO 27001	• Teilnahmebescheinigungen, • Prüfungszeugnisse, erlangte Zertifikate

2.1.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

2.1.3.1 Basiskenntnisse („kleine Fachkunde“)

Es werden grundlegende Kenntnisse vorausgesetzt:

- IT- und Informationssicherheit,
- ISO- und BSI-Ansätze zum Informationssicherheitsmanagement im Überblick,
- IT-Grundschutz (IT-Grundschutz-Kataloge , BSI-Standards, etc.) [IT-GS]

(insbesondere die BSI-Standardreihe 100-1 bis 100-4 im Überblick, IT-Grundschutz nach BSI-Standard 100-2 [BSI100]),

- relevante ISO-Standards, wie der ISO 27000ff.-Normenreihe (insbesondere der Managementrahmen der ISO 27001 [ISO 27001]),
- Grundlagen des Anforderungs- und Risikomanagements und
- Auditerfahrung (insbesondere im Bereich IT-Grundschutz).

2.1.3.2 Erweiterte Fachkenntnisse

- Weitere system- und produktbezogene Informationssicherheitsstandards,
- Geschichte und Struktur der Normenreihe ISO 27000ff. [ISO 27001],
- die Maßnahmenkataloge der ISO 27001 und ISO 27002,
- Aufbau und Inhalt der IT-Grundschutz-Kataloge [IT-GS],
- Kenntnisse der Risikoanalyse auf der Basis von IT-Grundschutz / BSI-Standard 100-3 [BSI100],
- Kenntnisse des Prüfschemas nach ISO 27001 auf der Basis von IT-Grundschutz [Schema],
- Kenntnisse des Zertifizierungsverfahrens nach ISO 27001 auf der Basis von IT-Grundschutz sowie
- aktuelle Informationen zum IT-Grundschutz.

2.1.3.3 Bewertung der nachzuweisenden Fachkompetenz

Die schriftliche Prüfung für Auditteamleiter erfolgt in Form eines 90-minütigen Tests.

Bei Nichtbestehen kann die Wiederholung der Prüfung zeitnah separat als Einzelprüfung erfolgen. Eine zweite Wiederholung ist nicht möglich – der Antrag auf Zertifizierung wird dann abgelehnt.

2.1.4 Kompetenzüberwachung

Um die Eignung des zertifizierten Auditteamleiters für zukünftige Audits sicherzustellen und eventuell notwendigen Schulungsbedarf zu erkennen, wird nach Abschluss eines Zertifizierungsverfahrens beim BSI die Leistung des Auditors beurteilt und schriftlich fixiert. In diese Beurteilung fließen sämtliche Kontakte der Zertifizierungsstelle mit dem Auditor im Rahmen des Zertifizierungsverfahrens, wie z.B. Treffen, Telefonate und der Auditbericht ein.

Um die eigentliche Audittätigkeit des Auditteamleiters zu beurteilen, wird zudem einmal während der Vertragslaufzeit, in Anlehnung an die zugrunde liegende Norm ISO/IEC 27006 [ISO 27006], ein Audittag (vor Ort) im Rahmen eines ISO 27001-Audits auf der Basis von IT-Grundschutz vom BSI begleitet (Vor-Ort-Beobachtung). Hierfür wählt das BSI ein Audit des Auditors stichprobenartig aus und vereinbart den Termin nach Vorliegen des Auditplans.

2.1.5 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditteamleiter nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene, vom Auftraggeber unterschriebene Tätigkeitsnachweise erbringen und an den Erfahrungsaustauschterminen des BSI teilgenommen haben. Zusammen mit dem Antrag auf Rezertifizierung müssen die erforderlichen Tätigkeitsnachweise beim BSI eingereicht werden. Die Nachweise müssen aus dem aktuellen 3-jährigen Zertifizierungszeitraum stammen. Diese werden verschieden gewichtet und mit Punktzahlen unterschiedlich hoch bewertet, wobei insgesamt eine Summe von 60 Punkten erreicht werden muss. Wird eine Tätigkeit nur teilweise ausgeführt, dann wird diese Tätigkeit mit entsprechend prozentualer Punktezahl bewertet. Das BSI prüft,

ob der Kandidat Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

Punkteskala zur Rezertifizierung ab dem 01.01.2016 (Ablaufdatum der aktuellen Personenzertifizierung):

Für die Rezertifizierung als Auditteamleiter muss der Antragsteller Tätigkeiten nachweisen, deren Gesamtbewertung mindestens 60 Punkte erreicht. Dabei ist es zwingend erforderlich, dass zu diesen Tätigkeiten mindestens zwei vom Antragsteller als Auditteamleiter durchgeführte Audits für ISO 27001-Zertifikate gehören. Diese Audits müssen entweder auf der Basis von IT-Grundschutz oder für eine in diesem Bereich von der DAkkS akkreditierten Zertifizierungsstelle (natives ISO 27001 Audit) durchgeführt worden sein. Dabei ist zu beachten, dass ein Audit nach ISO 27001 auf der Basis von IT-Grundschutz mit 35 Punkten bewertet wird, ein natives ISO 27001 Audit hingegen mit 25 Punkten. Die für eine Rezertifizierung erforderlichen 60 Punkte können somit nicht allein durch zwei native ISO 27001 Audits erreicht werden. In dem Fall sind zusätzliche Nachweise über eine Beschäftigung mit dem IT-Grundschutz bzw. dem BSI-Standard 100-2 [BSI100] erforderlich (s. nachfolgende Tabelle). Hierdurch soll gewährleistet werden, dass der Antragsteller Audits für ISO 27001-Zertifikate auch auf der Basis von IT-Grundschutz durchführen kann.

<table>
<tr><th>Tätigkeiten</th><th colspan="2">Bewertung (P= Punktzahl)</th></tr>
<tr><td>Audits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Auditteamleiter durchgeführt</td><td>35 P</td><td rowspan="2">2 Audits aus diesem Bereich sind zwingend erforderlich</td></tr>
<tr><td>Audit für ISO 27001-Zertifikate durchgeführt (für in diesem Bereich von der DAkkS akkreditierten Zertifizierungsstelle), max. 2 Audits werden gewertet</td><td>25 P</td></tr>
<tr><td>Audits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Co-Auditor/begleitender Auditor durchgeführt</td><td colspan="2">15 P</td></tr>
<tr><td>Überwachungsaudits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz durchgeführt (auch außerplanmäßige Überwachungsaudits)</td><td colspan="2">10 P</td></tr>
<tr><td>Audits mit Auditor-Testat (BSI-Standard 100-2 [BSI100]) durchgeführt</td><td colspan="2">10 P</td></tr>
<tr><td>Projekt mit Zielsetzung der Umsetzung eines Sicherheitskonzeptes nach der Vorgehensweise gemäß BSI-Standard 100-2 [BSI100] abgeschlossen</td><td colspan="2">10 P</td></tr>
<tr><td>Grundschutz-Beratungsprojekt mit Zertifikatsziel abgeschlossen (mindestens 20 Tage)</td><td colspan="2">10 P</td></tr>
<tr><td>Schulung über IT-Grundschutz gehalten (mindestens 2-tägig)</td><td colspan="2">10 P</td></tr>
<tr><td>Entwicklung eines IT-Grundschutz-Bausteines (nur veröffentlichte Bausteine)</td><td colspan="2">10 P</td></tr>
</table>

Sind die Nachweise für de Rezertifizierung nicht ausreichend bzw. wird die verlangte Punktezahl nicht erreicht, so kann der Antragsteller nicht rezertifiziert werden. In dem Fall kann die Personenzertifizierung nur wie bei der Erstzertifizierung erlangt werden.

2.1.6 Pflichten des zertifizierten Auditteamleiters

Der zertifizierte Auditteamleiter verpflichtet sich bei seinen Tätigkeiten im Geltungsbereich der Zertifizierung, die Vorgaben der Personenzertifizierungsstelle sowie die in dem betreffenden Prüfschema festgelegte Vorgehensweise zu beachten und einzuhalten.

Darüber hinaus erklärt er, die Vertraulichkeit der ihm bei seinen Tätigkeiten zur Kenntnis gelangten Informationen zu wahren sowie bei Prüftätigkeiten Bewertungen objektiv und unabhängig durchzuführen und, falls dies nicht gewährleistet werden könnte, auf das Audit zu verzichten.

Bei der Durchführung von ISO 27001-Audits auf der Basis von IT-Grundschutz stellt der zertifizierte Auditteamleiter sicher, dass er dem BSI jederzeit auf Verlangen umfassend Auskunft über Ablauf und Inhalt der Audits geben kann.

Das BSI behält sich vor, bei Vorliegen eines öffentlichen Interesses, Zertifizierungs- oder Überwachungsaudits gemäß Auditierungsschema [Auditierungsschema], zu begleiten. Kosten für diese Begleitung entstehen nicht.

2.1.7 Registrierung des zertifizierten Auditteamleiters

Alle vom BSI zertifizierten Auditteamleiter erhalten eine Registrierungsnummer, die wie folgt aufgebaut ist:

BSI-ZIG-XXXX-JJJJ.

2.1.8 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines Auditteamleiters unter Angabe der Zertifizierungsnummer, des Namens des Auditteamleiters, gegebenenfalls der Anschrift (beruflich und/oder privat) sowie dem Gültigkeitszeitraum des Zertifikats vom BSI im Internet und in der Publikation <KES>. Für die Veröffentlichung der Anschrift(en) holt es die Einwilligung des Auditteamleiters ein.

2.2 Zertifizierung als Auditor „De-Mail" für BSI TR-01201

Unter dem Begriff „De-Mail“ wurde in Deutschland eine sichere und vertrauenswürdige Kommunikationsinfrastruktur aufgebaut. Per „De-Mail“ werden Nachrichten und Dokumente zuverlässig und vor Veränderungen geschützt in einem sicheren Kommunikationsraum versendet. Hinter allen De-Mail-Adressen stehen zweifelsfrei identifizierte Kommunikationspartner. Der Betrieb dieser Infrastruktur in einem gesicherten Informationsverbund wird von De-Mail-Diensteanbietern (DMDA) übernommen.

Für den funktionsfähigen und sicheren Betrieb von De-Mail ist es unerlässlich, dass alle DMDAs definierte Anforderungen an die Sicherheit erfüllen und daher bestimmte, vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegebene Leistungsmerkmale erfüllen. Die Prüfung der Sicherheitsvorgaben erfolgt im Rahmen einer Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz.

Das Audit wird durch einen zertifizierten Auditor „De-Mail“ durchgeführt und findet vor Ort bei dem zu prüfenden DMDA statt.

2.2.1 Die persönlichen Eigenschaften eines Auditors „De-Mail"

Im Folgenden sind die persönlichen Eigenschaften eines Auditors „De-Mail" dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills" nur eingeschränkt im Rahmen des Zertifizierungsverfahrens bewertet werden können:

- alle Eigenschaften des Auditteamleiters (siehe Kapitel 2.1.1).

2.2.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise geprüft (siehe „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“).

Diese Zertifizierung setzt auf der Personenzertifizierung als „**Auditteamleiter** für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz“ auf. Dies bedeutet, dass jeder Auditor „De-Mail" zur Aufnahme in das Zertifizierungsverfahren ein gültiges Auditteamleiter-Zertifikat nachweisen und in den vergangenen 3 Jahren (Stichtag: Antragsdatum) mindestens 3 vollständige Zertifizierungsaudits im Bereich ISO 27001 auf der Basis von IT-Grundschutz (keine Überwachungsaudits) durchgeführt haben muss.

2.2.2.1 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Anforderung	***Erläuterung***	***Nachweis***
Bildungsabschluss, Berufserfahrung, Praxiserfahrung/Auditerfahrung	• Vgl. Voraussetzungen Auditteamleiter • in den vergangenen 3 Jahren (Stichtag: Antragsdatum) mind. 3 vollständige Zertifizierungsaudits im Bereich ISO 27001 auf der Basis von IT-Grundschutz	• Gültiges Auditteamleiter-Zertifikat

2.2.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

Im Zertifizierungsverfahren muss der Kandidat keine weitere Fachkompetenz nachweisen.

2.2.4 Kompetenzüberwachung

Um die Eignung des zertifizierten Auditors „De-Mail“ bzw. Auditteamleiters für zukünftige Audits sicherzustellen und eventuell notwendigen Schulungsbedarf zu erkennen, wird nach Abschluss eines Zertifizierungsverfahrens die Leistung des Auditors beurteilt und schriftlich fixiert. In diese Beurteilung fließen sämtliche Kontakte der Zertifizierungsstelle mit dem Auditor im Rahmen des Zertifizierungsverfahrens, wie z.B. Treffen, Telefonate und der Auditbericht ein.

2.2.5 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor „De-Mail“ nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er Tätigkeitsnachweise analog zur Erstzertifzierung erbringen oder ein De-Mail-Audit durchgeführt, sowie an den jährlichen Erfahrungsaustauschterminen der Auditteamleiter teilgenommen haben. Er muss nachweisen, dass er sich ständig fachlich weitergebildet hat und Änderungen der Auditpraxis, einschlägiger Normen und anderer Anforderungen berücksichtigt. Dabei steht die Aufrechterhaltung der Fähigkeiten, ein Audit auf Grundlage des aktuellen Standes der Technik und der neuesten Version der IT-Grundschutz-Kataloge [IT-GS] und der BSI-Standards [BSI100] sowie der Norm ISO 27001 [ISO 27001] durchzuführen, im Vordergrund.

2.2.6 Pflichten des zertifizierten Auditors „De-Mail"

Der zertifizierte Auditor „De-Mail“ verpflichtet sich bei seinen Tätigkeiten im Geltungsbereich der Zertifizierung, die Vorgaben der Personenzertifizierungsstelle sowie die in den betreffenden Verfahrensbeschreibungen festgelegten Vorgehensweisen zu beachten und einzuhalten.

Darüber hinaus erklärt er, die Vertraulichkeit der ihm bei seinen Tätigkeiten zur Kenntnis gelangten Informationen zu wahren sowie bei Prüftätigkeiten Bewertungen objektiv und unabhängig durchzuführen.

Bei der Durchführung von 27001-Audits auf der Basis von IT-Grundschutz stellt der zertifizierte Auditteamleiter bzw. Auditor „De-Mail“ sicher, dass er dem BSI jederzeit auf Verlangen umfassend Auskunft über Ablauf und Inhalt der Audits geben kann.

Das BSI behält sich vor, bei Vorliegen eines öffentlichen Interesses De-Mail-Audits nach ISO 27001 auf der Basis von IT-Grundschutz zu begleiten. Kosten für diese Begleitung entstehen nicht.

2.2.7 Registrierung des zertifizierten Auditors „De-Mail“

Alle vom BSI zertifizierten Auditoren „De-Mail“ erhalten eine Registrierungsnummer, die wie folgt aufgebaut ist:

BSI-ZADE-XXXX-JJJJ.

2.2.8 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines Auditors „De-Mail“ unter Angabe der Zertifizierungsnummer, des Namens des Auditors „De-Mail“, gegebenenfalls der Anschrift (beruflich und/oder privat) sowie dem Gültigkeitszeitraum des Zertifikats im Internet und der Publikation (<KES>). Für die Veröffentlichung der Anschrift(en) holt es die Einwilligung des De-Mail-Auditors ein.

2.3 Zertifizierung als Auditor „Secure CA Operation“ für BSI TR-03145

Nur eine sichere Certification Authority kann als Wurzel für eine Public Key Infrastruktur dienen, welche für die Sicherung von Vertraulichkeit oder auch Authentizität/Integrität von Informationen genutzt wird.

Die Grundlage von Public Key Infrastrukturen (PKI) ist Vertrauen. Daher muss eine Certification Authoritiy (CA), welche die PKI betreibt, zum einen vertrauenswürdig sein und zum anderen Vertrauen von Dritten erhalten.

Um dieses Vertrauen herzustellen, müssen zwei Bedingungen erfüllt sein:

- Erstens muss es eine Basis für Vertrauenswürdigkeit geben, d.h. die CA muss auf einem angemessenen Sicherheitsniveau organisatorische und technische Maßnahmen implementieren und Regeln für alle PKI-Teilnehmer aufstellen.
- Zweitens müssen diese Sicherheitsmaßnahmen, transparent dokumentiert werden. Hierzu dient ein (bestandenes) Audit basierend auf klaren und dokumentierten Anforderungen.

Die BSI [TR-03145] hat zum Ziel, CAs bei beiden Schritten zu unterstützen. Es werden Anforderungen an die zu implementierenden Sicherheitsmaßnahmen gestellt, und die Technische Richtlinie dient als Grundlage für einen Audit- und Zertifizierungsprozess. Die Anforderungen der [TR-03145] beinhalten u.a. ein Audit nach ISO/IEC 27001 in dessen Rahmen alle in der TR benannten Prozesse und Bereiche der CA berücksichtigt werden müssen.

Das Audit wird durch einen zertifizierten Auditor „Secure CA Operation“ durchgeführt und findet vor Ort bei der zu prüfenden CA statt.

Die persönlichen Eigenschaften eines Auditors „Secure CA Operation“

Im Folgenden sind die persönlichen Eigenschaften eines Auditors „Secure CA Operation“ dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills“ nur eingeschränkt im Rahmen des Zertifizierungsverfahrens bewertet werden können:

- alle Eigenschaften des Auditteamleiters (siehe Kapitel 2.1.1).

2.3.1 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft.

2.3.1.1 Bildungsabschluss

Anforderung

Der Kandidat muss eine Ausbildung abgeschlossen haben, in der er grundlegende Kenntnisse und Fähigkeiten für seine spätere Tätigkeit als Auditor erlangt hat. Hierzu zählt beispielsweise ein(e) abgeschlossene(s) Ausbildung oder Studium im Bereich IT und/oder Informationssicherheit.

Sollte der Kandidat mit der abgeschlossenen Ausbildung bzw. dem Tätigkeitsfeld, in dem die Ausbildung abgeschlossen wurde, nicht die erforderlichen Kenntnisse und Fähigkeiten (im Bereich IT und/oder Informationssicherheit sowie Auditierung) erlangt haben, so muss ein Nachweis erbracht werden, dass diese über vergleichbare berufsbegleitende Fortbildungen (z.B. Fortbildungen im Bereich IT und/oder Informationssicherheit) erworben worden sind.

Falls der Kandidat die Anforderungen an Ausbildung und vergleichbare Fortbildungen nicht nachweisen kann, so muss alternativ ein Nachweis erbracht werden, dass die erforderlichen Kenntnisse und Fähigkeiten durch einschlägige Berufserfahrung über mindestens 8 Jahre im Bereich IT, davon mindestens 5 Jahre im Bereich Informationssicherheit erworben worden sind.

Nachweis

Ein Zeugnis des Ausbildungsabschlusses und gegebenenfalls Bescheinigungen der Teilnahme an Fortbildungsveranstaltungen oder ein Zeugnis/eine Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung ist vorzulegen.

2.3.1.2 Berufserfahrung

Anforderung

Der Kandidat muss aus den letzten 8 Jahren mindestens 5 Jahre fachspezifische, praktische Berufserfahrung gerechnet auf Vollzeit im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit nachweisen. Hierbei finden alle Zeiten Berücksichtigung, die nach Abschluss der entsprechenden Ausbildung (siehe Bildungsabschluss) erbracht wurden.

Des Weiteren muss der Kandidat bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 [ISO 27006] akkreditierten Zertifizierungsstelle im Bereich ISO 27001 als Auditor zugelassen sein. Alternativ wird die Personenzertifizierung des BSI als Auditteamleiter im Bereich ISO 27001 auf der Basis von IT-Grundschutz akzeptiert. Innerhalb der letzten 3 Jahre muss der Kandidat mindestens an einem ISO 27001-Zertifizierungsaudit als Auditor teilgenommen haben. Dies schließt eine Zulassung als externer Auditor (nach ISO/IEC 27006-2011 Abschnitt 7.3 [ISO 27006]) ein.

Hinweis: Es ist zu beachten, dass für eine Zertifizierung nach [TR-03145] ein ISO 27001-Zertifikat über denselben Prüfbereich vorliegen muss, wofür ein Audit durch einen Auditteamleiter vorausgesetzt wird.

Nachweis

Ein Zeugnis oder eine Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Zulassung als Auditor. Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung. Des Weiteren muss ein Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle bspw. in Form der Kopie der Akkreditierungsurkunde vorgelegt werden.

2.3.1.3 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Anforderung	***Erläuterung***	***Nachweis***
Bildungsabschluss	• abgeschlossene Berufsausbildung • ggf. Fortbildungen • oder mindestens 8 Jahre Berufserfahrung im Bereich IT, davon mindestens 5 Jahre im Bereich Informationssicherheit	• Zeugnis Ausbildungsabschluss oder • Zeugnis Ausbildungsabschluss und Bescheinigung der Teilnahme an Fortbildungen oder • Zeugnis/Bestätigung eines Dritten über die Berufserfahrung

Anforderung	*Erläuterung*	*Nachweis*
Berufserfahrung	• In den letzten 8 Jahren mindestens 5 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit • Zulassung als Auditor bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 akkreditierten Zertifizierungsstelle im Bereich ISO 27001. Alternativ Zertifizierung als Auditteamleiter im Bereich ISO 27001 auf der Basis von IT-Grundschutz. Innerhalb der letzten 3 Jahre Durchführung von mind. 1 ISO 27001-Zertifizierungsaudit[5]	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Zulassung als Auditor Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle, z.B. durch Kopie der Akkreditierungsurkunde

2.3.2 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

Die Fachbegutachtung des Kandidaten im BSI stellt das zentrale Instrument zur Bewertung der Fachkompetenz dar. Diese wird in Form eines schriftlichen Tests beim BSI überprüft.

2.3.2.1 Basiskenntnisse („kleine Fachkunde“)

Es werden grundlegende Kenntnisse vorausgesetzt:

- IT- und Informationssicherheit,
- ISO- und BSI-Ansätze zum Informationssicherheitsmanagement im Überblick,
- relevante ISO-Standards, wie der ISO 27000ff.-Normenreihe (insbesondere der Managementrahmen der [ISO 27001]),
- die Maßnahmenkataloge der ISO 27001 und ISO 27002,
- Grundlagen des Anforderungs- und Risikomanagements und
- Auditerfahrung (insbesondere im Bereich [ISO 27001]).

Der Auditor “Secure CA Operation“ muss zusätzlich Fachwissen im Rahmen einer Fachbegutachtung durch das BSI in den folgenden Teilbereichen nachweisen:

- Public Key Infrastrukturen,
- Kryptografie,
- Schlüsselmanagement,
- Rollenkonzepte und Rollentrennung im Bereich PKI,
- Registrierungsprozesse,
- Zertifikatsmanagement (Erstellen, Verteilen, Verwalten und Zurückrufen von Zertifikaten),
- Datensicherung.

5 Dies schließt eine Beschäftigung als externer Auditor (nach ISO/IEC 27006 Abschnitt 7.3 [ISO/IEC 27006] ein.

2.3.2.2 Erweiterte Fachkenntnisse

- Weitere system- und produktbezogene Informationssicherheitsstandards,
- Geschichte und Struktur der Normenreihe ISO 27000ff. [ISO 27001],
- die Maßnahmenkataloge der ISO 27001 und ISO 27002,
- BSI [TR-03145].

2.3.3 Kompetenzüberwachung

Um die Eignung des zertifizierten Auditors „Secure CA Operation“ für zukünftige Audits sicherzustellen und eventuell notwendigen Schulungsbedarf zu erkennen, wird nach Abschluss eines Zertifizierungsverfahrens beim BSI die Leistung des Auditors beurteilt und schriftlich fixiert. In diese Beurteilung fließen sämtliche Kontakte der Zertifizierungsstelle mit dem Auditor im Rahmen des Zertifizierungsverfahrens, wie z.B. Treffen, Telefonate und der Auditbericht ein.

Um die eigentliche Audittätigkeit des Auditors „Secure CA Operation“ zu beurteilen, wird zudem einmal während der Vertragslaufzeit, in Anlehnung an die zugrunde liegende Norm ISO/IEC 27006 [ISO 27006], ein Audittag (vor Ort) im Rahmen eines „Secure CA Operation“-Audits vom BSI begleitet (Vor-Ort-Beobachtung). Hierfür wählt das BSI ein Audit des Auditors stichprobenartig aus und vereinbart den Termin nach Vorliegen des Auditplans.

2.3.4 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor „Secure CA Operation“ nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene Tätigkeitsnachweise erbringen. Zusammen mit dem Antrag auf Rezertifizierung müssen die erforderlichen Tätigkeitsnachweise beim BSI eingereicht werden. Diese werden verschieden gewichtet und mit Punktzahlen unterschiedlich hoch bewertet, wobei insgesamt eine Summe von 50 Punkten erreicht werden muss. Wird eine Tätigkeit nur teilweise ausgeführt, dann wird diese Tätigkeit mit entsprechend prozentualer Punktezahl bewertet. Das BSI prüft, ob der Kandidat Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

Tätigkeiten	***Bewertung (P = Punktzahl)***
Audits für eine Zertifizierung nach BSI [TR-03145] inklusive eines Zertifikats nach ISO 27001 für den Betrieb einer Certification Authority durchgeführt	50 P
Audits für ISO 27001-Zertifikate im Bereich PKI durchgeführt	35 P
Audits für eine Zertifizierung nach BSI [TR-03145] inklusive eines Zertifikats nach ISO 27001 für den Betrieb einer Certification Authority als Co-Auditor/begleitender Auditor durchgeführt	30 P
Ergänzende Audits für eine Zertifizierung nach BSI [TR-03145] für den Betrieb einer Certification Authority durchgeführt	25 P
Ergänzende Audits für eine Zertifizierung nach BSI [TR-03145] für den Betrieb einer Certification Authority als Co-Auditor/begleitender Auditor durchgeführt	20 P
Audits für ISO 27001-Zertifikate als Co-Auditor/begleitender Auditor im Bereich PKI durchgeführt	25 P

Tätigkeiten	*Bewertung (P = Punktzahl)*
Überwachungsaudits für ISO 27001-Zertifikate im Bereich PKI durchgeführt	10 P
Audits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Auditteamleiter durchgeführt	20P (max. 1x)
Erst- oder Zweitparteienaudits im Bereich Informationssicherheit und PKI durchgeführt	15 P (max. 3x)
Projekt mit Zielsetzung der Umsetzung eines Sicherheitskonzeptes im Bereich PKI nach der Vorgehensweise gemäß [ISO 27001] abgeschlossen	15 P (max. 3x)

Des Weiteren muss der Kandidat bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 [ISO 27006] akkreditierten Zertifizierungsstelle im Bereich ISO 27001 als Auditor zugelassen sein. Alternativ wird die Personenzertifizierung des BSI als Auditteamleiter im Bereich ISO 27001 auf der Basis von IT-Grundschutz akzeptiert.

Sind die Nachweise für de Rezertifizierung nicht ausreichend bzw. wird die verlangte Punktezahl nicht erreicht, so kann der Antragsteller nicht rezertifiziert werden. In dem Fall kann die Personenzertifizierung nur wie bei der Erstzertifizierung erlangt werden.

2.3.5 Pflichten des zertifizierten Auditors „Secure CA Operation“

Der zertifizierte Auditor „Secure CA Operation“ verpflichtet sich bei seinen Tätigkeiten im Geltungsbereich der Zertifizierung, die Vorgaben der Personenzertifizierungsstelle sowie die in dem betreffenden Prüfschema festgelegte Vorgehensweise zu beachten und einzuhalten.

2.3.6 Registrierung des zertifizierten Auditors „Secure CA Operation“

Alle vom BSI zertifizierten Auditoren „Secure CA Operation“ erhalten eine Registrierungsnummer, die wie folgt aufgebaut ist:

BSI-ZACA-XXXX-JJJJ.

2.3.7 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines Auditors „Secure CA Operation“ unter Angabe der Zertifizierungsnummer, des Namens des Auditors „Secure CA Operation“, gegebenenfalls der Anschrift (beruflich und/oder privat) sowie dem Gültigkeitszeitraum des Zertifikats im Internet. Für die Veröffentlichung der Anschrift(en) holt es die Einwilligung des „Secure CA Operation“-Auditors ein.

2.4 Zertifizierung als IS-Revisor

Um Bundesbehörden oder interessierte Stellen bei der Auswahl von IT-Sicherheitsdienstleistern zu unterstützen, hat das BSI als neutrale staatliche Stelle ein Zertifizierungsverfahren für IT-Sicherheitsdienstleister im Geltungsbereich „IS-Revision und -Beratung“ entwickelt. Insbesondere bei Bundesbehörden mit sicherheitssensiblen Bereichen müssen sich die beauftragten IT-Sicherheitsdienstleister durch Unabhängigkeit, Fachkompetenz und Qualität der Dienstleistung auszeichnen. Ziel der Zertifizierung des IT-Sicherheitsdienstleisters ist somit die Sicherstellung der Vertrauenswürdigkeit und Kompetenz.

Eine Grundlage jeder Dienstleistung in diesem Geltungsbereich sind qualifizierte und kompetente Mitarbeiter.

Aufgabe des IS-Revisions- und IS-Beratungs-Experten (kurz: IS-Revisor) ist es, Bundesbehörden oder interessierte Stellen bei der Erstellung und Umsetzung von Sicherheitskonzepten sowie bei der regelmäßigen Durchführung von IS-Revisionen gemäß “Leitfaden für die Informationssicherheitsrevision auf Basis von IT-Grundschutz” [REV] zu unterstützen.

2.4.1 Die persönlichen Eigenschaften eines IS-Revisors

Im Folgenden sind die persönlichen Eigenschaften eines IS-Revisors dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills“ nur eingeschränkt im Rahmen des Zertifizierungsverfahrens bewertet werden können.

- Fähigkeit zum „Hineindenken“ in Behördenstrukturen und -abläufe,
- Beherrschen der Behördensprache sowie
- alle Eigenschaften des Auditteamleiters (siehe Kapitel 2.1.1).

2.4.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft (siehe [VB-Personen]).

Diese Zertifizierung setzt auf der Personenzertifizierung als „**Auditteamleiter** für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz“ (s. Kapitel 2.1.1) auf. Dies bedeutet, dass jeder IS-Revisor zur Aufnahme in das Zertifizierungsverfahren ein gültiges Auditteamleiter-Zertifikat nachweisen muss.

2.4.2.1 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Anforderung	***Erläuterung***	***Nachweis***
Bildungsabschluss, Berufserfahrung, Praxiserfahrung / Auditerfahrung	• Vgl. Voraussetzungen Auditteamleiter	• Gültiges Auditteamleiter-Zertifikat

2.4.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

2.4.3.1 Basiskenntnisse („kleine Fachkunde“)

Es werden grundlegende Kenntnisse vorausgesetzt:

- zum IS-Revisionsleitfaden [REV] sowie
- alle Basiskenntnisse des Auditteamleiters.

2.4.3.2 Erweiterte Fachkenntnisse

Folgende Fachkenntnisse werden zur Erlangung des Zertifikats als IS-Revisor vorausgesetzt:

- Überblick über Inhalte und Ziele einer IS-Revision.
- Abgrenzung der IS-Revision zu
    - IT-Revision und
    - ISO 27001-Audits auf Basis von IT-Grundschutz.
- Integration der IS-Revision in den ISMS-Prozess.
- Grundsätze der Revision.
- Überblick über die Phasen der IS-Revision aus Sicht einer Behörde.
- Unterschiedliche Arten der IS-Revision:
    - IS-Querschnittsrevision,
    - IS-Partialrevision,
    - IS-Kurzrevision.
- Planung von IS-Revisionen in der Institution:
    - Grobplanung,
    - Jahresplanung,
    - IS-Revisionszyklen,
    - Zusammenstellung des IS-Revisionsteams.
- Überblick über das IS-Revisionsprüfverfahren.
- Vorstellung der unterschiedlichen Prüfmethoden, wie z.B.
    - Dokumentenprüfung,
    - Interview,
    - Inaugenscheinnahme,
    - Beobachtung,
    - Datenanalyse.
- Anwendung der Prüfmethoden.
- Erläuterung der Bewertung von Prüfergebnissen.
- Rechte und Pflichten des IS-Revisionsteams.

- Erstellung des Prüfplans:
    - Auswahl der Baustein-Zielobjekte,
    - Auswahl der IT-Grundschutz-Maßnahmen.
- Ablauf einer Vor-Ort-Prüfung.
- Durchführung von Eröffnungsgesprächen.
- Methoden und Verfahren zur Auswertung der Ergebnisse aus der Vor-Ort-Prüfung.
- Erstellung von Berichten:
    - Dokumentationsprinzipien,
    - Form und Inhalt von Revisionsberichten.
- Aufbewahrung und Archivierung.

2.4.3.3 Qualifizierungsmaßnahmen

Der Kandidat hat die nachzuweisende Fachkompetenz (insbesondere die Grundlagen der IS-Revision gemäß „Leitfaden für Informationssicherheitsrevisionen auf Basis von IT-Grundschutz“ [REV]) in einer eintägigen Schulung beim BSI zu vertiefen und nachzuweisen.

Sollte ein Kandidat bei mehrmaliger (maximal 3) Einladung seine Schulungsteilnahme absagen, so wird davon ausgegangen, dass der Kandidat nicht weiter an einer Zertifizierung interessiert ist. Der Antrag auf Zertifizierung wird dann abgelehnt.

Schulungsabsagen, die nicht durch Verschulden des Kandidaten (z.B. wegen Krankheit) erfolgen, führen nicht zu einer Einstellung des Verfahrens. Absagen sind jedoch grundsätzlich zu begründen und zu belegen.

2.4.3.4 Bewertung der nachzuweisenden Fachkompetenz

Die Fachkompetenz des Kandidaten wird anhand einer schriftlichen und mündlichen Prüfungsaufgabe (Prüfungsmodul/Fallbeispiele) geprüft.

Bei Nichtbestehen der Prüfung, kann diese einmalig wiederholt werden. Eine Wiederholung kann in der nächsten Schulung erfolgen. Eine zweite Wiederholung ist nicht möglich – der Antrag auf Zertifizierung wird dann abgelehnt.

2.4.4 Kompetenzüberwachung

Nach jeder durchgeführten IS-Beratung oder IS-Revision werden von den beauftragten Bundesbehörden Bewertungsbögen eingefordert. Anhand dessen wird die Durchführung der Dienstleistung bewertet.

2.4.5 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte IS-Revisor nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er Tätigkeitsnachweise als IS-Revisor erbringen und am jährlichen Erfahrungsaustausch teilgenommen haben. Der IS-Revisor muss nachweisen, dass er sich ständig fachlich weiterentwickelt hat und Änderungen der Audit- und Revisionspraxis, einschlägiger Normen und anderer Anforderungen berücksichtigt. Dabei steht die Fähigkeit IS-Revisionen auf Grundlage des aktuellen Standes der Technik und der neuesten Version der IT-Grundschutz-Kataloge [IT-GS] durchzuführen, im Vordergrund.

Der IS-Revisor muss nachweisen, dass er in den letzten 3 Jahren mindesten 3 IS-Revisionen bzw. IS-Beratungen durchgeführt hat.

Ein gültiges Auditteamleiter-Zertifikat ist für die Rezertifizierung nicht erforderlich.

2.4.6 Pflichten des zertifizierten IS-Revisors

Vor jeder Durchführung einer IS-Beratung oder einer IS-Revision bei einer Bundesbehörde muss der IS-Revisor die Sicherheitsberatung des BSI über die Durchführung des Projekts informieren. Hierbei muss eine Kurzbeschreibung des Inhalts und des zeitlichen Ablaufs des Projekts mitgeteilt werden.

2.4.7 Registrierung des zertifizierten IS-Revisors

Alle vom BSI zertifizierten IS-Revisoren erhalten eine Registrierungsnummer, die wie folgt aufgebaut ist:

BSI-ZISR-XXXX-JJJJ.

2.4.8 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines IS-Revisors unter Angabe der Zertifizierungsnummer, des Namens des IS-Revisors, gegebenenfalls der Anschrift (beruflich und/oder privat) sowie des Gültigkeitszeitraums des Zertifikats im Internet und in der Publikation (<KES>). Zur Veröffentlichung der Anschrift(en) holt es die Einwilligung des IS-Revisors ein.

2.5 Zertifizierung als Penetrationstester

Um Bundesbehörden oder interessierte Stellen bei der Auswahl von IT-Sicherheitsdienstleistern zu unterstützen, hat das BSI als neutrale staatliche Stelle ein Zertifizierungsverfahren für IT-Sicherheitsdienstleister im Geltungsbereich „Penetrationstests“ entwickelt. Insbesondere bei interessierten Stellen oder Bundesbehörden mit sicherheitssensiblen Bereichen müssen sich die beauftragten IT-Sicherheitsdienstleister durch Unabhängigkeit, Fachkompetenz und Qualität der Dienstleistung auszeichnen. Ziel der Zertifizierung des IT-Sicherheitsdienstleisters ist somit die Sicherstellung der Vertrauenswürdigkeit und Kompetenz. Die Grundlage jeder Dienstleistung sind qualifizierte und kompetente Mitarbeiter.

Penetrationstests sind auf die individuelle Situation der Behörde bzw. der interessierten Stelle abzustimmen und somit nur in begrenztem Umfang standardisierbar. Bei einem Penetrationstest kann deshalb nur bis zu einem gewissen Grad nach einem starren Muster vorgegangen werden. Deshalb sollte die Durchführung von Penetrationstests von Experten vorgenommen werden, die über langjährige Erfahrung im Bereich der IT-Sicherheit und als Penetrationstester verfügen.

2.5.1 Die persönlichen Eigenschaften eines Penetrationstesters

Im Folgenden sind die persönlichen Eigenschaften eines Penetrationstesters dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills“ nur eingeschränkt im Rahmen des Zertifizierungsverfahrens bewertet werden können.

2.5.1.1 Organisatorische Fähigkeiten

- Ergebnispräsentation

2.5.1.2 Kommunikationsfähigkeiten

- Umfassende und sachliche Berichterstattung
- Didaktische Fähigkeiten

2.5.1.3 Soziale Kompetenz

- Analytische Fähigkeiten
- Wille zur Weiterentwicklung von Fähigkeiten
- Verantwortungsbewusstes Handeln
- Teamfähigkeit

2.5.1.4 Unabhängigkeit

- Fachliche und sachliche Unabhängigkeit
- Unbeeinflussbarkeit und Unvoreingenommenheit
- Verschwiegenheit und Unbestechlichkeit

2.5.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

2.5.2.1 Berufserfahrung

Anforderung

Der Kandidat muss fachspezifische, praktische Berufserfahrung im Bereich IT/Informationssicherheit auf den Gebieten

1. Systemadministration,
2. Netzwerkprotokolle,
3. Programmiersprachen,
4. IT-Sicherheitsprodukten (Firewalls, Intrusion-Detection-Sytemen, etc.) und
5. Anwendungssystemen

haben.

2.5.2.2 Praxiserfahrung

Anforderung

Der Kandidat muss

- Penetrationstests organisatorisch und technisch vorbereiten,
- Penetrationstests fachlich kompetent durchführen,
- Ergebnisse analysieren und präsentieren können.

2.5.2.3 Anstellung bei einem zertifizierten IT-Sicherheitsdienstleister

Ein Penetrationstester kann nur im Rahmen seiner Anstellung bei einem vom BSI zertifizierten IT-Sicherheitsdienstleister im Geltungsbereich Penetrationstests (s. [VB-Stellen]) die Personenzertifizierung erlangen[6].

Nachweis

Bei in Zertifizierung befindlichem IT-Sicherheitsdienstleister: Kopie des Antrags auf Zertifizierung als IT-Sicherheitsdienstleister.

Bei bereits zertifiziertem IT-Sicherheitsdienstleister: Kopie des Zertifikats des IT-Sicherheitsdienstleisters.

2.5.2.4 Spezialkenntnisse

Anforderung

Im Einzelnen sind insbesondere folgende Spezialkenntnisse zur qualifizierten Durchführung von Penetrationstests notwendig:

1. Kenntnisse im Bereich der Systemadministration: Kenntnisse bei der Systemadministration bzw. Administration von Betriebssystemen sind zur Beurteilung von Schwächen in den Betriebssystemen der Zielsysteme notwendig. Zusätzlich erleichtern sie auch die Handhabung der für den Penetrationstest eingesetzten Systeme.
2. Kenntnisse im Bereich Netzwerkprotokolle: Da der Datenverkehr im Internet über TCP/IP abgewickelt

6 Bei Erstzertifizierung erfolgt die Zertifizierung der Person und des IT-Sicherheitsdienstleisters zeitgleich.

wird und sich auch im LAN TCP/IP als der Standard durchgesetzt hat, ist ein tiefgreifendes Wissen über dieses Protokoll unerlässlich. Daher sind Kenntnisse in TCP/IP sowie weitere Netzwerkkenntnisse und Kenntnisse über das OSI-Referenzmodell erforderlich.

3. Kenntnisse im Bereich Programmiersprachen: Um in der Lage zu sein, Schwachstellen in Anwendungen und Systemen auszunutzen, sind Kenntnisse in einer Programmiersprache erforderlich. Zwar existieren eine Reihe von vorgefertigten Werkzeugen als Skripte oder mit graphischer Benutzeroberfläche. Oft können Sicherheitslücken wie Pufferüberläufe o. Ä. jedoch nur dann wirksam ausgenutzt werden, wenn der Penetrationstester über die notwendigen Programmierkenntnisse verfügt.
4. Kenntnisse im Bereich von IT-Sicherheitsprodukten (z.B. Firewalls, IDS, usw.): Da mittlerweile Sicherheitsvorkehrungen wie Firewalls oder Intrusion-Detection-Systeme einen sehr hohen Verbreitungsgrad haben, muss der Penetrationstester die Funktionsweise dieser Sicherheitsvorkehrungen kennen und auch aktuelle Meldungen im Bereich der Sicherheitslücken von IT-Sicherheitsprodukten verfolgen können. Einen Überblick über die marktgängigen Produkte im Bereich der IT-Sicherheit ist unerlässlich.
5. Kenntnisse im Bereich Anwendungssystemen: Viele Schwachstellen liegen nicht im Bereich der Betriebssystemsoftware, sondern in den Anwendungen. Dies umfasst von z. B. unzureichend abgesicherten Makro-Funktionen in Textverarbeitungsprogrammen, über Verwundbarkeiten von Internet-Browsern mittels „Scripting“ bis hin zu sog. Pufferüberlauffehlern in großen Datenbanksystemen die gesamte Bandbreite von Anwendungssystemen. Der Penetrationstester muss daher über möglichst breite Kenntnisse von Anwendungen aller Art verfügen. Besonders wichtig sind detaillierte Kenntnisse über weit verbreitete Anwendungen, da hier die Gefährdungen durch Hacker/Cracker im Allgemeinen besonders groß sind.

Nachweis

Die Spezialkenntnisse in den o.g. Bereichen sind durch Zeugnisse, Berufserfahrung, Projekterfahrung oder Schulungsnachweise zu belegen.

2.5.3 Zusammenfassung der in der Kompetenzfeststellung nachzuweisenden Fachkompetenz

2.5.3.1 Basiskenntnisse („kleine Fachkunde“)

Es werden grundlegende Kenntnisse vorausgesetzt:

- zu IT und Informationssicherheit und
- zu IT-Grundschutz (IT-Grundschutz-Kataloge und BSI-Standards [BSI100]).

2.5.3.2 Erweiterte Fachkenntnisse

Es werden erweiterte Fachkenntnisse vorausgesetzt:

- zum IT-Grundschutz (Aktualität),
- zur Systemadministration,
- zu Netzwerkprotokollen,
- zu Programmiersprachen,
- zu IT-Sicherheitsprodukten (z.B. Firewalls, Intrusion-Detection-Systemen),
- zu Anwendungssystemen und
- Kenntnisse in der Handhabung von Werkzeugen und Schwachstellen-Scannern.

Zur Durchführung von Penetrationstests ist neben dem erforderlichen Grundlagenwissen auch Erfahrung in der Handhabung von Werkzeugen und Schwachstellen-Scannern notwendig. Kenntnisse im Umgang mit diesen Tools sollten in der Praxis erworben worden sein. Aus der Vielzahl der verfügbaren Tools haben im Laufe der Zeit einige Produkte eine weite Verbreitung gefunden. Sowohl kostenpflichtige als auch frei verfügbare Werkzeuge können für die Durchführung einer effizienten Prüfung und Demonstration der relativ einfachen Durchführbarkeit des Angriffs zum Einsatz kommen. Die Effizienz des Penetrationstests hängt aber wesentlich davon ab, wie erfahren der Penetrationstester im Umgang mit diesen Tools ist.

2.5.3.3 Qualifizierungsmaßnahmen

Für Penetrationstester wird kein Ausbildungsgang angeboten.

2.5.3.4 Bewertung der nachzuweisenden Fachkompetenz

Im Rahmen eines Projekttages im BSI, werden die praktische Fachkompetenz und die persönlichen Voraussetzungen des Penetrationstesters geprüft. Hierbei wird das Spezialwissen, die Handhabung von Tools und Schwachstellen-Scannern sowie die kreative Vorgehensweise bei der Durchführung von Penetrationstests überprüft.

Bei Nichtbestehen kann einmalig wiederholt werden. Eine zweite Wiederholung ist nicht möglich – der Antrag auf Zertifizierung wird abgelehnt.

2.5.4 Pflichten des zertifizierten Penetrationstesters

Vor jeder Durchführung eines Penetrationstests bei einer Bundesbehörde muss der Penetrationstester die Sicherheitsberatung des BSI über die Durchführung des Projekts informieren. Hierbei muss eine Kurzbeschreibung des Inhalts und des zeitlichen Ablaufs des Projektes mitgeteilt werden.

2.5.5 Anforderung zur Rezertifizierung

Strebt der bereits zertifizierte Penetrationstester nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, so muss er die von ihm in den letzten 3 Jahren durchgeführten Penetrationstests geeignet nachweisen (bspw. in Form von vom Auftraggeber oder Arbeitgeber bestätigten Kurzberichten über die Durchführung der Penetrationstests). Sollte ein Nachweis (z.B. mangels Aufträgen) nicht erbracht werden, muss eine erneute *Kompetenzfeststellung* – auch mit dem Risiko des Nicht-Bestehens – durchlaufen werden.

2.5.6 Registrierung des zertifizierten Penetrationstesters

Alle vom BSI zertifizierten Penetrationstester erhalten eine Registrierungsnummer, die wie folgt aufgebaut ist:

BSI-ZPT-XXXX-JJJJ.

2.5.7 Veröffentlichung der Zertifizierung

1. Die vom zertifizierten Penetrationstester zur Verfügung gestellten personenbezogenen Daten, die zur Durchführung des Zertifizierungsverfahrens notwendig sind, werden ausschließlich zum Zweck der Zertifizierung im BSI elektronisch gespeichert und verarbeitet.
2. Der zertifizierte Penetrationstester erklärt sich mit der Veröffentlichung der Tatsache der Zertifizierung[7] unter Angabe der Zertifizierungsnummer und des Gültigkeitszeitraums des Zertifikats, des Namens und

7 Hinweis: Die Zertifizierung als Penetrationstester ist nur im Rahmen seiner Anstellung bei einem vom BSI zertifizierten IT-Sicherheitsdienstleister im Geltungsbereich Penetrationstest gültig.

der Anschrift im Internet und in der Publikation „KES“ einverstanden.

2.6 Zertifizierung als Auditor „Smart Meter Gateway Administration“

In Deutschland wird im Rahmen der Ausgestaltung der Energiewende und der Umsetzung der entsprechenden EU-Verordnungen die Einführung von intelligenten Messsystemen betrieben. Hierbei sieht der derzeitige nationale gesetzliche Rahmen (§ 25 Messstellenbetriebsgesetz) u.a. die Zertifizierung des IT-Betriebs beim Smart Meter Gateway Administrators (SMGW-Admin) vor, der für die Aufgaben rund um das intelligente Messsystem verantwortlich ist.

Die Notwendigkeit der Zertifizierung des IT-Betriebs beim SMGW Admin lässt sich nachvollziehen, wenn man sich das Aufgabenportfolio und die Anwendungsfälle des SMGW Admin (beschrieben in der TR-03109-6) vor Augen führt.

Die [BSI TR-03109-6] definiert Anforderungen an die zu implementierenden Mindestmaßnahmen und dient als Grundlage für einen Audit- und Zertifizierungsprozess. Die Anforderungen der [BSI TR-03109-6] beinhalten u.a. ein Audit nach ISO/IEC 27001 [ISO 27001] oder nach ISO 27001 auf Basis von IT-Grundschutz, in dessen Rahmen alle in der Technischen Richtlinie benannten Prozesse und Bereiche des SMGW-Admin berücksichtigt werden müssen.

Mit dem Betrieb beim SMGW-Admin existiert offensichtlich ein Bereich mit kritischen Anwendungen, so dass bei der Prüfung der Umsetzung des konkreten ISMS sowie der vorgegebenen Mindestmaßnahmen eine entsprechende Sorgsamkeit und Verantwortung notwendig ist. Deshalb sind in den folgenden Absätzen besondere Anforderungen für Auditoren aufgeführt, die in diesem Bereich Audits durchführen wollen.

Das Audit wird durch einen zertifizierten Auditor „Smart Meter Gateway Administration“ durchgeführt und findet vor Ort bei dem zu prüfenden SMGW-Admin statt.

2.6.1 Die persönlichen Eigenschaften

Es gelten alle Eigenschaften des Auditteamleiters (siehe Kapitel 2.1.1).

2.6.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise geprüft (siehe „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“).

2.6.2.1 Bildungsabschluss

Es gelten alle Anforderungen des Auditeamleiters (siehe Kapitel 2.1.2.1).

2.6.2.2 Berufserfahrung

Es gelten alle Anforderungen des Auditteamleiters (siehe Kapitel 2.1.2.2).

2.6.2.3 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Anforderung	*Erläuterung*	*Nachweis*
Bildungsabschluss	• abgeschlossene Berufsausbildung • ggf. Fortbildungen • oder mindestens 8 Jahre Berufserfahrung im Bereich IT, davon mindestens 5 Jahre im Bereich Informationssicherheit	• Zeugnis Ausbildungsabschluss oder • Zeugnis Ausbildungsabschluss und Bescheinigung der Teilnahme an Fortbildungen oder • Zeugnis/Bestätigung eines Dritten über die Berufserfahrung
Berufserfahrung	• Zulassung als Auditor bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 akkreditierten Zertifizierungsstelle im Bereich ISO 27001. Alternativ Zertifizierung als Auditteamleiter im Bereich ISO 27001 auf der Basis von IT-Grundschutz. • In den zurückliegenden 3 Jahren (Stichtag: Antragsdatum) mindestens 1 vollständiges Zertifizierungsaudit im Bereich der ISO/IEC 27001 („native“ oder auf Basis von IT-Grundschutz)	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Zulassung als Auditor • Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle, z.B. durch Kopie der Akkreditierungsurkunde • Vom Auftraggeber/Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate

2.6.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

2.6.3.1 Basiskenntnisse („kleine Fachkunde“)

- IT- und Informationssicherheit,
- BSI-Ansatz zum ISMS im Überblick,
- Normenreihe ISO/IEC 27001[ISO 27001],
- Grundlagen des Anforderungs- und Risikomanagements,
- Auditerfahrung im Bereich ISO/IEC 27001 oder im Bereich IT-Grundschutz.

2.6.3.2 Erweiterte Fachkenntnisse

- Inhalte der BSI TR-03109[BSI TR-03109]
- Inhalte und Regelungsbereich der BSI TR-03109-6[BSI TR-03109-6]
- Regelungsbereiche des IT-Sicherheitsgesetzes[IT-Sicherheitsgesetz] und des Sicherheitskatalogs der Bundesnetzagentur[BNetzA-Katalog] sowie mögliche Schnittpunkte mit der TR-03109-6

2.6.3.3 Überprüfung der Fachkompetenz

Die schriftliche Prüfung für den Auditor „Smart Meter Gateway Administration“ besteht aus einem 60-minütigem Test.

Bei Nichtbestehen kann die Wiederholung der Prüfung zeitnah separat als Einzelprüfung erfolgen. Eine zweite Wiederholung ist nicht möglich – der Antrag auf Zertifizierung wird dann abgelehnt.

2.6.4 Qualifizierungsmaßnahme

Der Kandidat kann die nachzuweisende Fachkompetenz im Rahmen eines Workshops beim BSI oder bei einer sonstigen externen Organisation vertiefen.

2.6.5 Kompetenzüberwachung

Um die Eignung des zertifizierten Auditors „Smart Meter Gateway Administration“ für zukünftige Audits sicherzustellen und eventuell notwendigen Schulungsbedarf zu erkennen, kann in begründetem Einzelfall nach Abschluss eines Audits auf Grundlage der Auditberichte beim BSI die Leistung des Auditors beurteilt werden.

Um die eigentliche Audittätigkeit des Auditors „Smart Meter Gateway Administration“ zu beurteilen, wird zudem einmal während der Vertragslaufzeit, in Anlehnung an die zugrunde liegende Norm ISO/IEC 27006 [ISO 27006], ein Audittag (vor Ort) im Rahmen eines „Smart Meter Gateway Administration“-Audits vom BSI begleitet (Vor-Ort-Beobachtung). Hierfür wählt das BSI ein Audit des Auditors stichprobenartig aus und vereinbart den Termin nach Vorliegen des Auditplans.

2.6.6 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor „Smart Meter Gateway Administration“ nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene Tätigkeitsnachweise erbringen. Zusammen mit dem Antrag auf Rezertifizierung müssen die erforderlichen Tätigkeitsnachweise beim BSI eingereicht werden. Diese werden verschieden gewichtet und mit Punktzahlen unterschiedlich hoch bewertet, wobei insgesamt eine Summe von 50 Punkten erreicht werden muss. Wird eine Tätigkeit nur teilweise ausgeführt, dann wird diese Tätigkeit mit entsprechend prozentualer Punktezahl bewertet. Das BSI prüft, ob der Kandidat Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

Tätigkeiten	*Bewertung (P = Punktzahl)*
Audit für ein Zertifikat nach ISO/IEC 27001 für den Betrieb eines SMGW-Admin durchgeführt	50 P
Audit für ein ISO 27001-Zertifikat auf Basis von IT-Grundschutz im Bereich SMGW-Admin durchgeführt	50 P
Audits für ISO 27001-Zertifikate (auf Basis von IT-Grundschutz oder gemäß ISO/IEC 27001) als Co-Auditor/begleitender Auditor im Bereich SMGW-Admin durchgeführt	25 P
Überwachungsaudit im Bereich SMGW-Admin durchgeführt	10 P
Audit aus besonderem Anlass / außerplanmäßiges Audit	10 P
Projekt mit Zielsetzung der Umsetzung eines Sicherheitskonzeptes im Bereich SMGW-Admin nach Vorgaben der TR-03109-6 und gemäß der Vorgehensweise [ISO 27001] oder IT-Grundschutz abgeschlossen	15 P (max. 3x)

2.6.7 Pflichten des zertifizierten Auditors „Smart Meter Gateway Administration“

Der zertifizierte Auditor „Smart Meter Gateway Administration“ verpflichtet sich, bei seinen Tätigkeiten im Geltungsbereich der Zertifizierung die Vorgaben der Personenzertifizierungsstelle sowie die in dem betreffenden Prüfschema festgelegte Vorgehensweise zu beachten und einzuhalten.

2.6.8 Registrierung des zertifizierten Auditors „Smart Meter Gateway Administration“

Alle vom BSI zertifizierten Auditoren „Smart Meter Gateway Administration“ erhalten eine Zertifizierungsnummer, die wie folgt aufgebaut ist:

BSI-ZASM-XXXX-JJJJ

2.6.9 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines Auditors „Smart Meter Gateway Administration“ unter Angabe der Zertifizierungsnummer, des Namens des Auditors „Smart Meter Gateway Administration“, gegebenenfalls der Anschrift (beruflich/privat) sowie dem Gültigkeitszeitraum des Zertifikats im Internet. Für die Veröffentlichung der Anschrift(en) holt es die Einwilligung des „Smart Meter Gateway Administration“-Auditors ein.

2.7 Zertifizierung als Auditor „Sicherer E-Mail Transport“

Die E-Mail hat sich als wichtiges Medium zum Austausch von Nachrichten etabliert, wobei nachweislich die konsequente Anwendung von IT-Sicherheitsmaßnahmen häufig vernachlässigt wird.

Die Technische Richtlinie BSI TR-03108 Secure E-Mail Transport [TR-03108] adressiert die Transportsicherheit von E-Mails und zeigt einen Lösungsansatz, wie die Anzahl an sicher versendeten E-Mails ohne Mehraufwand für den Nutzer erhöht werden kann. Überdies wird die Vergleichbarkeit der Sicherheit von E-Mail-Diensten ermöglicht.

Die TR enthält technische und organisatorische Anforderungen an den Betrieb eines sicheren E-Mail-Dienstes, die modular strukturiert sind.

Als Grundlage für den sicheren Betrieb wird ein geprüftes Sicherheitskonzept im Rahmen des Telekommunikationsgesetzes (oder ein vergleichbares Sicherheitskonzept für interne E-Mail Dienste) oder wie empfohlen ein zertifiziertes ISMS nach ISO/IEC 27001 [ISO 27001] gefordert.

Bei der Zertifizierung „Sicherer E-Mail Transport“ wird kein Audit eines ISMS durchgeführt. Es wird geprüft, dass die in der TR aufgeführten Prozesse und Bereiche mit dem Geltungsbereich (Scope) des Sicherheitskonzepts des E-Mail-Dienstes übereinstimmen. Hierzu enthält die Prüfspezifikation eine Checkliste, welche die Inhalte definiert, die im Sicherheitskonzept berücksichtigt sein müssen.

Den Schwerpunkt der Prüfung nach der TR bildet die Konformitätsprüfung, bei der festgestellt werden soll, dass die technischen Maßnahmen für die sichere Kommunikation vollständig und korrekt umgesetzt wurden. Diese Maßnahmen beziehen sich auf den Einsatz und die Konfiguration von etablierten Sicherheitstechnologien.

Als Grundlage für die Schnittstellentests muss vor dem Beginn der Tests ein Implementation Conformance Statement (ICT) erstellt werden. Dieses Dokument bildet die Grundlage für die Testdurchführung und definiert, welche Funktionalität von den Tests adressiert wird und welche Testfälle hierauf angewendet werden. Die Schnittstellentests können abhängig vom Aufbau des E-Mail-Dienstes auch via Fernzugriff durchgeführt werden.

Letztlich wird durch die Tests insbesondere nachgewiesen, dass die für eine sichere Kommunikation erforderlichen Schnittstellen vorhanden und korrekt konfiguriert sind. Somit ist der E-Mail-Dienst vorbereitet, um mit anderen E-Mail-Diensten sicher zu kommunizieren.

Das Audit wird durch einen zertifizierten Auditor „Sicherer E-Mail Transport“ durchgeführt.

2.7.1 Die persönlichen Eigenschaften

Im Folgenden sind die persönlichen Eigenschaften eines Auditors „Sicherer E-Mail Transport“ dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills“ nur eingeschränkt im Rahmen des Zertifizierungsverfahrens bewertet werden können.

2.7.1.1 Organisatorische Fähigkeiten

- Ergebnispräsentation

2.7.1.2 Kommunikationsfähigkeiten

- Umfassende und sachliche Berichterstattung
- Didaktische Fähigkeiten

2.7.1.3 Soziale Kompetenz

- Schnelle Auffassungsgabe
- Analytische Fähigkeiten
- Wille zur Weiterentwicklung von Fähigkeiten
- Verantwortungsbewusstes Handeln
- Teamfähigkeit

2.7.1.4 Unabhängigkeit

- Fachliche und sachliche Unabhängigkeit
- Unbeeinflussbarkeit und Unvoreingenommenheit
- Verschwiegenheit und Unbestechlichkeit

2.7.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise geprüft (siehe „Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen“).

2.7.2.1 Bildungsabschluss und Berufserfahrung

Es sind die folgenden Zulassungsvoraussetzungen für Auditoren „Sicherer E-Mail Transport" gefordert:

Anforderung	***Erläuterung***	***Nachweis***
Bildungsabschluss	• abgeschlossene Berufsausbildung • ggf. Fortbildungen • oder mindestens 6 Jahre Berufserfahrung im Bereich IT, davon mindestens 4 Jahre im Bereich Informationssicherheit	• Zeugnis Ausbildungsabschluss oder • Zeugnis Ausbildungsabschluss und Bescheinigung der Teilnahme an Fortbildungen oder • Zeugnis/Bestätigung eines Dritten über die Berufserfahrung
Berufserfahrung	• In den letzten 8 Jahren mindestens 4 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Zulassung als Auditor

2.7.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

2.7.3.1 Basiskenntnisse („kleine Fachkunde“)

- IT- und Informationssicherheit
- Internet Kommunikationsprotokolle, speziell im Bereich E-Mail

- ISO/IEC 27001 zum Informationssicherheitsmanagement im Überblick
- Programmiersprachen / Werkzeuge / Skripting
- Angewandte Kryptografie

2.7.3.2 Erweiterte Fachkenntnisse

- Inhalte der BSI TR-03108
- Inhalte der TR-03116-4 und TR-2102-2
- Transport Layer Security (TLS) - RFC 5246
- DNS-based Authentication of Named Entities (DANE) - RFC 6698
- Domain Name System Security Extensions (DNSSEC) - RFC 4033

2.7.3.3 Überprüfung der Fachkompetenz

Die Fachkompetenz wird durch eine Prüfung festgestellt. Die Prüfung besteht aus zwei Teilen:

- 60-minütiger schriftlicher Test (Multiple-Choice)
- 120-minütiger praktischer Test (Test-System)
  - Im Rahmen des praktischen Tests wird dem Auditor ein Zugang zu einem Testsystem (Test-E-Mail-Dienst) zur Verfügung gestellt. Auf dem Testsystem muss der Auditor vorgegebene Schnittstellen anhand der Testfälle aus der Prüfspezifikation zur TR-03108 untersuchen. Voraussetzung für den praktischen Test ist, dass der Auditor seine eigenen Testwerkzeuge mitbringt und sich dann vor Ort mit dem Testsystem verbindet. Wenn ein Testfall fehlschlägt muss die Art des Fehlers schriftlich dokumentiert werden. Nach Abschluss des praktischen Tests bildet die Dokumentation die Grundlage für die Bewertung.

Bei Nichtbestehen kann die Wiederholung der Prüfung zeitnah erfolgen. Wurde einer beiden Teile erfolgreich abgeschlossen, muss nur der nicht bestandene Teil wiederholt werden. Eine zweite Wiederholung ist erst nach einer Wartezeit von 6 Monaten möglich – der Antrag auf Zertifizierung wird bis dahin abgelehnt. Bei der zweiten Wiederholung muss wieder eine vollständige Prüfung abgelegt werden. Bei einer dritten oder mehr Wiederholungen ist jeweils ein Wartezeit von 12 Monaten einzuhalten und die Prüfung muss immer vollständig abgelegt werden.

2.7.4 Kompetenzüberwachung

Um die eigentliche Audittätigkeit des Auditors „Sicherer E-Mail Transport“ zu beurteilen, wird im Regelfall einmal während der Vertragslaufzeit, in Anlehnung an die zugrunde liegende Norm ISO/IEC 27006 [ISO 27006], ein Audittag (vor Ort) im Rahmen eines „Sicherer E-Mail Transport“-Audits vom BSI begleitet (Vor-Ort-Beobachtung). Der Auditor hat daher die Durchführung von Audits nach BSI TR-03108 mindestens 4 Wochen vor Durchführung der Personenzertifizierungsstelle des BSI zu melden.Das BSI wählt dann ein Audit des Auditors stichprobenartig aus und vereinbart den Termin nach Vorliegen des Auditplans.

2.7.5 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor „Sicherer E-Mail Transport“ nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene Tätigkeitsnachweise erbringen. Zusammen mit dem Antrag auf Rezertifizierung müssen die erforderlichen Tätigkeitsnachweise beim BSI eingereicht werden. Diese werden verschieden gewichtet und mit Punktzahlen unterschiedlich hoch bewertet, wobei insgesamt eine Summe von 50 Punkten erreicht werden muss. Wird eine Tätigkeit nur teilweise ausgeführt, dann wird diese Tätigkeit mit entsprechend prozentualer Punktezahl bewertet. Das BSI prüft, ob der Kandidat Tätigkeitsnachweise in ausreichendem Umfang

erbracht hat.

Tätigkeiten	*Bewertung (P = Punktzahl)*
Audits für eine Zertifizierung eines E-Mail Dienstes nach BSI [TR-03108] durchgeführt	50 P
Projekt, mit dem Ziel der Umsetzung eines E-Mail-Dienstes der konform zu BSI [TR-03108] ist verantwortlich durchgeführt.	30 P
Audits für ein ISO 27001-Zertifikat für einen E-Mail-Dienst durchgeführt	30 P
Audits für eine Zertifizierung nach BSI [TR-03108] als Co-Auditor/begleitender Auditor durchgeführt	30 P
Sicherheitskonzept für einen E-Mail-Dienst erstellt, das gemäß Telekommunikationsgesetz erfolgreich geprüft wurde oder die Basis für ein ISO 27001 zertifiziertes ISMS bildet.	20 P
Penetrationstests an einem E-Mail-Dienst als zertifizierter Penetrationstester durchgeführt	20 P
Projekt mit Zielsetzung der technischen Umsetzung eines eines E-Mail-Dienstes durchgeführt	15 P (max. 2x)
Überwachungsaudit für ISO 27001-Zertifikate im Bereich E-Mail-Dienst durchgeführt	10 P
Die vollständige technische Konfiguration eines E-Mail-Dienstes anhand der Vorgaben aus [TR-03108] durchgeführt	10 P (max. 2x)

2.7.6 Pflichten des zertifizierten Auditors „Sicherer E-Mail Transport“

Der zertifizierte Auditor „Sicherer E-Mail Transport“ verpflichtet sich, bei seinen Tätigkeiten im Geltungsbereich der Zertifizierung die Vorgaben der Personenzertifizierungsstelle sowie die in dem betreffenden Prüfschema festgelegte Vorgehensweise zu beachten und einzuhalten.

2.7.7 Registrierung des zertifizierten Auditors „Sicherer E-Mail Transport“

Alle vom BSI zertifizierten Auditoren „Sicherer E-Mail Transport“ erhalten eine Zertifizierungsnummer, die wie folgt aufgebaut ist:

BSI-ZAMT-XXXX-JJJJ

2.7.8 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines Auditors „Sicherer E-Mail Transport“ unter Angabe der Zertifizierungsnummer, des Namens des Auditors „Sicherer E-Mail Transport“, gegebenenfalls der Anschrift (beruflich und/oder privat) sowie dem Gültigkeitszeitraum des Zertifikats im Internet. Für die Veröffentlichung der Anschrift(en) holt es die Einwilligung des Auditor „Sicherer E-Mail Transport“ ein.

2.8 Zertifizierung als Auditor RESISCAN für BSI TR-03138

Das Thema der Digitalisierung und des ersetzenden Scannens hält stetig Einzug in alle Bereiche von Wirtschaft, Verwaltung und Politik. Damit wird es zu einem immer wichtigeren Baustein der Umsetzung der nationalen und europäischen eGoverment Strategien. Um den damit verbundenen Herausforderungen – insbesondere dem Erhalt der Beweiskraft des Digitalisats im Vergleich zum Papieroriginal der digitalisierten Dokumente – Rechnung zu tragen, hat das BSI bereits im Jahr 2013 eine Technische Richtlinie mit dem Titel „Ersetzendes Scannen“ (RESISCAN) herausgegeben. Die Technische Richtlinie bietet dabei Anwendern aus Verwaltung, Justiz, Wirtschaft und Gesundheitswesen einen praxisorientierten Handlungsleitfaden zur sicheren Gestaltung ihrer Prozesse für das ersetzende Scannen.

Das Audit wird durch einen zertifizierten Auditor RESISCAN durchgeführt und findet vor Ort bei dem zu prüfenden Scanprozess statt.

2.8.1 Die persönlichen Eigenschaften eines Auditors RESISCAN

Im Folgenden sind die persönlichen Eigenschaften eines Auditors RESISCAN dargestellt, die für die Tätigkeiten im Geltungsbereich der Zertifizierung notwendig sind, jedoch als „Soft Skills" nur eingeschränkt im Rahmen des Zertifizierungsverfahrens bewertet werden können:

- alle Eigenschaften des Auditteamleiters (siehe Kapitel 2.1.1).

2.8.2 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft.

2.8.2.1 Bildungsabschluss

Anforderung

Der Kandidat muss eine Ausbildung abgeschlossen haben, in der er grundlegende Kenntnisse und Fähigkeiten für seine spätere Tätigkeit als Auditor erlangt hat. Hierzu zählt beispielsweise ein(e) abgeschlossene(s) Ausbildung oder Studium im Bereich IT und/oder Informationssicherheit.

Sollte der Kandidat mit der abgeschlossenen Ausbildung bzw. dem Tätigkeitsfeld, in dem die Ausbildung abgeschlossen wurde, nicht die erforderlichen Kenntnisse und Fähigkeiten (im Bereich IT und/oder Informationssicherheit sowie Auditierung) erlangt haben, so muss ein Nachweis erbracht werden, dass diese über vergleichbare berufsbegleitende Fortbildungen (z.B. Fortbildungen im Bereich IT und/oder Informationssicherheit) erworben worden sind.

Falls der Kandidat die Anforderungen an Ausbildung und vergleichbare Fortbildungen nicht nachweisen kann, so muss alternativ ein Nachweis erbracht werden, dass die erforderlichen Kenntnisse und Fähigkeiten durch einschlägige Berufserfahrung über mindestens 5 Jahre im Bereich IT, davon mindestens 3 Jahre im Bereich Informationssicherheit erworben worden sind.

Nachweis

Ein Zeugnis des Ausbildungsabschlusses und gegebenenfalls Bescheinigungen der Teilnahme an Fortbildungsveranstaltungen oder ein Zeugnis/eine Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung ist vorzulegen.

2.8.2.2 Berufserfahrung

Anforderung

Der Kandidat muss aus den letzten 5 Jahren mindestens 3 Jahre fachspezifische, praktische Berufserfahrung gerechnet auf Vollzeit im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit nachweisen. Hierbei finden alle Zeiten Berücksichtigung, die nach Abschluss der entsprechenden Ausbildung (siehe Bildungsabschluss) erbracht wurden.

Des Weiteren muss der Kandidat bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 [ISO 27006] akkreditierten Zertifizierungsstelle im Bereich ISO 27001 als Auditor zugelassen sein. Dies schließt eine Zulassung als externer Auditor (nach ISO/IEC 27006-2011 Abschnitt 7.3 [ISO 27006]) ein. Alternativ wird die Personenzertifizierung des BSI als Auditteamleiter im Bereich ISO 27001 auf der Basis von IT-Grundschutz akzeptiert.

Innerhalb der letzten 3 Jahre muss der Kandidat mindestens ein ISO 27001-Zertifizierungsaudit als Auditteamleiter durchgeführt haben. Alternativ muss der Kandidat innerhalb der letzten 3 Jahre ein Zertifizierungsaudit nach BSI TR-03138 als verantwortlicher Auditor durchgeführt haben.

Nachweis

Ein Zeugnis oder eine Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Zulassung als Auditor. Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung. Des Weiteren muss ein Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle bspw. in Form der Kopie der Akkreditierungsurkunde vorgelegt werden.

2.8.2.3 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Anforderung	***Erläuterung***	***Nachweis***
Bildungsabschluss	• abgeschlossene Berufsausbildung ggf. Fortbildungen oder mindestens 5 Jahre Berufserfahrung im Bereich IT, davon mindestens 3 Jahre im Bereich Informationssicherheit	• Zeugnis Ausbildungsabschluss oder Zeugnis Ausbildungsabschluss und Bescheinigung der Teilnahme an Fortbildungen oder Zeugnis/Bestätigung eines Dritten über die Berufserfahrung

Anforderung	*Erläuterung*	*Nachweis*
Berufserfahrung/ Auditerfahrung	• In den letzten 5 Jahren mindestens 3 Jahre Berufserfahrung im Bereich IT, davon mindestens 2 Jahre im Bereich Informationssicherheit Zulassung als Auditor bei einer von der DAkkS (oder vergleichbaren nationalen Akkreditierungsstelle im europäischen Ausland) gem. ISO/IEC 27006 akkreditierten Zertifizierungsstelle im Bereich ISO 27001; alternativ Zertifizierung als Auditteamleiter im Bereich ISO 27001 auf der Basis von IT-Grundschutz. Innerhalb der letzten 3 Jahre Durchführung von mindestens einem ISO 27001-Zertifizierungsaudit[8] **oder** einem Zertifizierungsaudits im Bereich BSI TR 03138.	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Zulassung als Auditor Nachweis über die Akkreditierung des Arbeitgebers bzw. der beauftragenden Zertifizierungsstelle, z.B. durch Kopie der Akkreditierungsurkunde Vom Auftraggeber / Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate.

2.8.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

Die Fachbegutachtung des Kandidaten im BSI stellt das zentrale Instrument zur Bewertung der Fachkompetenz dar.

2.8.3.1 Basiskenntnisse („kleine Fachkunde“)

Es werden grundlegende Kenntnisse vorausgesetzt:

- IT- und Informationssicherheit,
- ISO- und BSI-Ansätze zum Informationssicherheitsmanagement im Überblick,
- BSI IT-Grundschutz
- die Maßnahmenkataloge der ISO 27001 und ISO 27002 und
- Auditerfahrung (insbesondere im Bereich IT-Grundschutz / [ISO 27001]).

Der Auditor “RESISCAN“ muss zusätzlich Fachwissen im Rahmen einer Fachbegutachtung durch das BSI in den folgenden Teilbereichen nachweisen:

- BSI TR 03138 und ihrer Anlagen, speziell der Verfahrensanweisung und der Prüfspezifikation BSI TR 03138-P

2.8.3.2 Erweiterte Fachkenntnisse

- Erfahrung aus einem Projekt im Bereich des Scannens allgemein oder
- Erfahrungen aus der Konzipierung und Umsetzung eines Scanverfahrens.

2.8.3.3 Überprüfung der Fachkompetenz

Die schriftliche Prüfung für den Auditor „RESISCAN“ besteht aus einem schriftlichen Test (Multiple-Choice).

8 Dies schließt eine Beschäftigung als externer Auditor (nach ISO/IEC 27006 Abschnitt 7.3 [ISO/IEC 27006] ein.

Bei Nichtbestehen kann die Wiederholung der Prüfung zeitnah separat als Einzelprüfung erfolgen. Eine zweite Wiederholung ist nicht möglich – der Antrag auf Zertifizierung wird dann abgelehnt.

Sollte der Auditor bereits Zertifizierungsaudits im Bereich RESISCAN durchgeführt haben, kann auf eine schriftliche Prüfung im BSI verzichtet werden.

2.8.4 Kompetenzüberwachung

Um die Eignung des zertifizierten Auditors RESISCAN bzw. Auditteamleiters für zukünftige Audits sicherzustellen und eventuell notwendigen Schulungsbedarf zu erkennen, wird nach Abschluss eines Zertifizierungsverfahrens die Leistung des Auditors beurteilt und schriftlich fixiert. In diese Beurteilung fließen sämtliche Kontakte der Zertifizierungsstelle mit dem Auditor im Rahmen des Zertifizierungsverfahrens, wie z.B. Treffen, Telefonate und der Auditbericht ein.

Um die eigentliche Audittätigkeit des Auditors „RESISCAN“ zu beurteilen, wird zudem einmal während der Vertragslaufzeit, in Anlehnung an die zugrunde liegende Norm ISO/IEC 27006 [ISO 27006], ein Audittag (vor Ort) im Rahmen eines „RESISCAN“-Audits vom BSI begleitet (Vor-Ort-Beobachtung). Hierfür wählt das BSI ein Audit des Auditors stichprobenartig aus und vereinbart den Termin nach Vorliegen des Auditplans.

2.8.5 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor RESISCAN nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er mindestens ein Zertifizierungsaudit nach BSI TR-03138 als verantwortlicher Auditor durchgeführt, sowie an den, in der Regel jährlichen Erfahrungsaustauschterminen der Resiscan-Auditoren teilgenommen haben. Er muss nachweisen, dass er sich ständig fachlich weitergebildet hat und Änderungen der Auditpraxis, einschlägiger Normen und anderer Anforderungen berücksichtigt. Dabei steht die Aufrechterhaltung der Fähigkeiten, ein Audit auf Grundlage des aktuellen Standes der Technik und der neuesten Version der IT-Grundschutz-Kataloge [IT-GS] und der BSI-Standards [BSI100] sowie der Norm ISO 27001 [ISO 27001] durchzuführen, im Vordergrund.

2.8.6 Pflichten des zertifizierten Auditors RESISCAN

Der zertifizierte Auditor RESISCAN verpflichtet sich bei seinen Tätigkeiten im Geltungsbereich der Zertifizierung, die Vorgaben der Personenzertifizierungsstelle sowie die in den betreffenden Verfahrensbeschreibungen festgelegten Vorgehensweisen zu beachten und einzuhalten.

Darüber hinaus erklärt er, die Vertraulichkeit der ihm bei seinen Tätigkeiten zur Kenntnis gelangten Informationen zu wahren sowie bei Prüftätigkeiten Bewertungen objektiv und unabhängig durchzuführen.

Bei der Durchführung von 27001-Audits auf der Basis von IT-Grundschutz stellt der zertifizierte Auditteamleiter bzw. Auditor RESISCAN sicher, dass er dem BSI jederzeit auf Verlangen umfassend Auskunft über Ablauf und Inhalt der Audits geben kann.

Das BSI behält sich vor, bei Vorliegen eines öffentlichen Interesses Resiscan-Audits nach ISO 27001 auf der Basis von IT-Grundschutz zu begleiten. Kosten für diese Begleitung entstehen nicht.

2.8.7 Registrierung des zertifizierten Auditors RESISCAN

Alle vom BSI zertifizierten Auditoren RESISCAN erhalten eine Registrierungsnummer, die wie folgt aufgebaut ist:

BSI-ZARS-XXXX-JJJJ.

2.8.8 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht die Tatsache der Zertifizierung eines Auditors RESISCAN unter Angabe der Zertifizierungs-

nummer, des Namens des Auditors RESISCAN, gegebenenfalls der Anschrift (beruflich und/oder privat) sowie dem Gültigkeitszeitraum des Zertifikats im Internet. Für die Veröffentlichung der Anschrift(en) holt es die Einwilligung des Auditors RESISCAN ein.

2.9 Kompetenzfeststellung bei BOS-Interoperabilitätsprüfern bzw. ZPL-Mitarbeitern

In Deutschland wird gegenwärtig ein bundesweit einheitliches digitales Sprech- und Datenfunksystem für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) aufgebaut. Für den funktionsfähigen Betrieb des Digitalfunk BOS ist es unerlässlich, dass sämtliche für die Nutzung im Digitalfunk BOS bestimmten Endgeräte störungsfrei mit allen anderen Komponenten des Digitalfunks BOS zusammenwirken und bestimmte, von der Bundesanstalt für den Digitalfunk der BOS (BDBOS) vorgegebene Leistungsmerkmale erfüllen.

Daher dürfen nur solche Endgeräte im Digitalfunk BOS eingesetzt werden, die entsprechend geprüft worden sind. Die Prüfung erfolgt durch sachverständige Prüfstellen und dort angestellte Prüfer. Die Prüfungen finden hierbei in einem Zertifizierungsprüflabor (ZPL) auf der Testplattform der BDBOS statt, das für den Geltungsbereich „Bereitstellung eines Zertifizierungsprüflabors für Interoperabilitätsprüfungen mit Wirknetzrelevanz für den Digitalfunk BOS“ zertifiziert ist.

Zur Zeit werden IT-Sicherheitsdienstleister für nachfolgende Geltungsbereiche zertifiziert:

- Durchführung von Interoperabilitätsprüfungen für Funkgeräte im Digitalfunk BOS,
- Durchführung von Interoperabilitätsprüfungen für Leitstellen im Digitalfunk BOS,
- Bereitstellung eines Zertifizierungsprüflabors für Interoperabilitätsprüfungen mit Wirknetzrelevanz für den Digitalfunk BOS (ZPL).

In diesen Geltungsbereichen müssen kompetente BOS-Interoperabilitätsprüfer bzw. ZPL-Mitarbeiter beschäftigt sein, deren Kompetenz durch die Personenzertifizierungsstelle des BSI festgestellt wurde.

Nachfolgende Kompetenzbereiche werden unterschieden:

- TETRA-Standard und TETRA-Funksystemtechnik,
- Labor- und Feldtests von Funkgeräten,
- Labortests von Leitstellen,
- Spezifikation und Validierung von IOP-Richtlinien und Testumgebungen,
- Bereitstellung und Konfiguration des ZPL sowie
- Kryptographische Verfahren (BOS-Kryptosystem).

2.9.1 Die persönlichen Eigenschaften eines BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters

Im Folgenden sind die persönlichen Eigenschaften eines BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters dargestellt, die für die Tätigkeiten im Geltungsbereich notwendig sind, jedoch als „Soft Skills" nur eingeschränkt im Rahmen einer Kompetenzfeststellung bewertet werden können.

2.9.1.1 Managementfähigkeiten

- Organisatorische Fähigkeiten.
- Zielorientiertes Denken und Handeln.

2.9.1.2 Kommunikationsfähigkeiten

- Umfassende und sachliche Berichterstattung.
- Behandlung von Einwänden.
- Managen von Konflikten.
- Überzeugungsfähigkeit.

2.9.1.3 Soziale Kompetenz

- Aufgeschlossenheit und Freundlichkeit.
- Schnelle Auffassungsgabe.
- Gesundes Urteilsvermögen.
- Analytische Fähigkeiten.
- Fachliche und persönliche Reife.
- Wille zur Weiterentwicklung von Fähigkeiten.
- Kontaktfähigkeit.
- Gewissenhaftes Handeln.
- Konstruktiver Umgang mit Kritik und Lob.
- Glaubwürdigkeit.
- Teamfähigkeit.
- Partnerschaftliches Verhalten.
- Belastbarkeit.
- Sachlichkeit insbesondere bei heiklen Sachverhalten.
- Selbstbewusstsein.

2.9.1.4 Unabhängigkeit

- Unbeeinflussbarkeit und Unvoreingenommenheit.
- Unbedingte Verschwiegenheit.
- Unbestechlichkeit.
- Argumentation auf Basis objektiver Nachweise.

2.9.2 Mindestvoraussetzungen für einen BOS-Interoperabilitätsprüfer bzw. ZPL-Mitarbeiter

Die Mindestvoraussetzungen werden durch Vorlage externer Fachkundenachweise, Lebensläufe und Mitarbeiterprofile durch die BDBOS überprüft (siehe [VB-Personen]).

2.9.2.1 Bildungsabschluss

Anforderung

Der Kandidat muss eine Ausbildung abgeschlossen haben, in der er grundlegende Kenntnisse und Fähigkeiten für seine spätere Tätigkeit als BOS-Interoperabilitätsprüfer bzw. ZPL-Mitarbeiter erlangt hat. Hierzu zählt beispielsweise ein(e) abgeschlossene(s) Ausbildung oder Studium im Bereich Elektro- oder Informationstechnik bzw. Informatik.

Sollte der Kandidat mit der abgeschlossenen Ausbildung bzw. dem Tätigkeitsfeld, in dem die Ausbildung abgeschlossen wurde, nicht die erforderlichen Kenntnisse und Fähigkeiten erlangt haben, so muss ein Nachweis erbracht werden, dass diese über vergleichbare berufsbegleitende Fortbildungen (z.B. Fortbildungen im Bereich Elektro- oder Informationstechnik bzw. Informatik) erworben worden sind.

Falls der Kandidat die Anforderungen an Ausbildung und vergleichbare Fortbildungen nicht nachweisen kann, so muss alternativ ein Nachweis erbracht werden, dass die erforderlichen Kenntnisse und Fähigkeiten durch einschlägige Berufserfahrung über mindestens 5 Jahre im Bereich Elektro- oder Informationstechnik bzw. Informatik, davon mindestens 3 Jahre im Bereich Kommunikationsnetze (analog zu „2.9.2.2 Berufserfahrung“) erworben worden sind.

Nachweis

Ein Zeugnis des Ausbildungsabschlusses und ggf. Bescheinigungen der Teilnahme an Fortbildungen oder ein Zeugnis/eine Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung.

2.9.2.2 Berufserfahrung

Anforderung

Der Kandidat muss aus den letzten 8 Jahren mindestens 3 Jahre fachspezifische, praktische Berufserfahrung gerechnet auf eine Vollzeitbeschäftigung im Bereich der Entwicklung und Qualitätssicherung, davon mindestens 1 Jahr im Bereich des Hardware- und/oder Software-Testens nachweisen. Hierbei finden alle Zeiten Berücksichtigung, die nach Abschluss der entsprechenden Ausbildung (siehe Bildungsabschluss) erbracht wurden.

Nachweis

Es muss ein Zeugnis oder eine Bestätigung eines Dritten (zum Beispiel Arbeitgeber) über die Berufserfahrung im Bereich der Entwicklung und Qualitätssicherung sowie im Bereich des Hardware- und/oder Software-Testens vorliegen. Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung.

2.9.2.3 Praxiserfahrung

Anforderung

Der Kandidat muss

- in den zurückliegenden 3 Jahren (Stichtag: Datum der Benennung),
- an 5 Projekten im Bereich der Entwicklung und Qualitätssicherung,
- als technischer Experte im jeweiligen Kompetenzbereich
- mit einem Gesamtumfang von jeweils mindestens 20 Personentagen teilgenommen haben.

Nachweis

Vom Auftraggeber oder Arbeitgeber bestätigte Kurzberichte über die Durchführung der Projekte. Im Kurzbericht

sind anzugeben:

- die wesentlichen Ziele sowie der Gegenstand des Projekts,
- Verantwortung des Kandidaten,
- der Zeitraum und Umfang (Personentage) des Projekts.

Die Angaben im Kurzbericht können (z.B. bei Projekten mit Dritten) auch anonymisiert erfolgen.

2.9.2.4 Tabellarische Zusammenfassung der Mindestvoraussetzungen

Anforderung	***Erläuterung***	***Nachweis***
Bildungsabschluss	• Abgeschlossene Ausbildung • ggf. Fortbildungen • oder mind. 5 Jahre Berufserfahrung im Bereich Elektrotechnik bzw. Informatik/Informationstechnik, davon mind. 3 Jahre im Bereich Kommunikationsnetze	• Zeugnis Ausbildungsabschluss oder • Zeugnis Ausbildungsabschluss und Bescheinigung der Teilnahme an Fortbildungen oder • Zeugnis/Bestätigung eines Dritten über die Berufserfahrung
Berufserfahrung	• In den letzten 8 Jahren mind. 3 Berufserfahrung im Bereich der Entwicklung und Qualitätssicherung, davon mind. 1 Jahr im Bereich des Hardware- und/oder Software-Testens	• Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten
Praxiserfahrung	• In den letzten 3 Jahren mind. 5 Projekte in der Entwicklung und Qualitätssicherung als technischer Experte im jew. Geltungsbereich mit einem Gesamtumfang von jeweils mind. 20 Personentagen	• Vom Auftraggeber/Arbeitgeber bestätigte Kurzberichte

2.9.3 In der Kompetenzfeststellung nachzuweisende Fachkompetenz

Die Fachkompetenz wird in der Evaluierungsphase überprüft (siehe [VB-Personen]).

2.9.3.1 Basiskenntnisse („kleine Fachkunde“)

Als **BOS-Interoperabilitätsprüfer** oder **ZPL-Mitarbeiter** werden folgende grundlegende Kenntnisse vorausgesetzt:

- Abschlussbericht der Expertengruppe aus Bund und Ländern Gruppe „Anforderungen an das Netz“ (GAN) [GAN] (empfohlen),
- BDBOS-Gesetz und der Zertifizierungsverordnung der BDBOS,
- Nutzungsordnung und Satzung der Testplattform,

- TETRA-Standard der ETSI,
- TETRA-Interoperabilitätsprofile (TIP) und TETRA-Testpläne (TP) der TETRA Association,
- BOS-Interoperabilitätsrichtlinien (bestehend aus den Dokumenten [LM-END], [EINF], [MINF], [BIP], [BTP] und [BIZ-AT]),
- EADS-Endgeräteleitfaden für Endgerätehersteller [RTCG] und zur Dokumentation der EADS-Leitstellenschnittstelle [LS1-3] sowie
- BOS-Kryptosystem [KRYPTO].

2.9.3.2 Erweiterte Fachkenntnisse für den Kompetenzbereich „TETRA-Standard und TETRA-Funksystemtechnik“

Als **BOS-Interoperabilitätsprüfer** oder **ZPL-Mitarbeiter** im Kompetenzbereich „TETRA-Standard und TETRA-Funksystemtechnik“ sind folgende Fachkenntnisse in einer Fachbegutachtung nachzuweisen:

- Kommerzielle Mobilfunkstandards (empfohlen),
- Professionelle Mobilfunkstandards (empfohlen),
- TETRA-Mobilfunkstandard,
- TETRA-Funksystemtechnik und
- TETRA-Funksystemtechnik von EADS.

2.9.3.3 Erweiterte Fachkenntnisse für den Kompetenzbereich „Labor- und Feldtests von Funkgeräten“

Als **BOS-Interoperabilitätsprüfer** oder **ZPL-Mitarbeiter** im Kompetenzbereich „Labor- und Feldtests von Funkgeräten“ sind folgende Fachkenntnisse in einer Fachbegutachtung nachzuweisen:

- Testen von Protokollen an Telekommunikationssystemen, insbesondere Funksystemen,
- Funkgeräte-Labortests (Mobilfunk) (empfohlen),
- Funkgeräte-Feldtests (Mobilfunk) (empfohlen),
- Funkgeräte-Labortests (TETRA),
- Funkgeräte-Feldtests (TETRA) und
- Gesundheit und Umwelt.

2.9.3.4 Erweiterte Fachkenntnisse für den Kompetenzbereich „Labortests von Leitstellen“

Als **BOS-Interoperabilitätsprüfer** oder **ZPL-Mitarbeiter** im Kompetenzbereich „Labortests von Leitstellen“ sind folgende Fachkenntnisse in einer Fachbegutachtung nachzuweisen:

- Testen von Protokollen an Telekommunikationssystemen, insbesondere Leitstellensystemen.
    - Labortests von Leitstellen.
    - BOS-Leitstellentechnik und -systeme.
    - EADS-Leitstellenschnittstelle TCS-API.

2.9.3.5 Erweiterte Fachkenntnisse für den Kompetenzbereich „Spezifikation und Validierung von IOP-Richtlinien und Testumgebungen“

Als **BOS-Interoperabilitätsprüfer** im Kompetenzbereich „Spezifikation und Validierung von IOP-Richtlinien und Testumgebungen“ sind folgende Fachkenntnisse in einer Fachbegutachtung nachzuweisen:

- Spezifikation von IOP-Richtlinien.
- Entwicklung und Aufbau von Testumgebungen.
- Anwendung von Mess- und Prüfmitteln.
- Validierung von IOP-Richtlinien und Testumgebungen.
- Durchführung von Fehleranalysen.

2.9.3.6 Erweiterte Fachkenntnisse für den Kompetenzbereich „Bereitstellung und Konfiguration des ZPL“

Als **ZPL-Mitarbeiter** im Kompetenzbereich „Bereitstellung und Konfiguration des ZPL“ sind folgende Fachkenntnisse in einer Fachbegutachtung nachzuweisen:

- Entwicklung und Aufbau von Testumgebungen (einschließlich Spezifikation und Anschluss von Mess- und Prüfmitteln).
- Betreiben einer Interoperabilitätsplattform zur Nutzung für Zertifizierungstests.
- Anwendung, Kalibrierung und Wartung von Mess- und Prüfmitteln.
- Konfiguration von Komponenten der BOS-Systemtechnik.
- Validierung von IOP-Richtlinien und Testumgebungen.
- Protokollierung von Telekommunikationssystemen, insbesondere der BOS-Systemtechnik.
- Durchführung von Fehleranalysen an Telekommunikationssystemen, insbesondere der BOS-Systemtechnik.

2.9.3.7 Erweiterte Fachkenntnisse für den Kompetenzbereich „Kryptographische Verfahren“

Als **BOS-Interoperabilitätsprüfer** oder **ZPL-Mitarbeiter** im Kompetenzbereich „Kryptographische Verfahren“ sind folgende Fachkenntnisse in einer Fachbegutachtung nachzuweisen:

- Kryptographische Verfahren im Mobilfunk.
- BOS-Kryptosystem „Funkgeräte“.
- BOS-Kryptosystem „Leitstellen“.

2.9.3.8 Bewertung der nachzuweisenden Fachkompetenz

Die Fachbegutachtung des Kandidaten in der Prüfstelle stellt das zentrale Instrument zur Bewertung der Fachkompetenz dar.

2.9.4 Kompetenzüberwachung

Um die Eignung eines BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters im betreffenden Bereich sicherzustellen und eventuell notwendigen Qualifizierungsbedarf zu erkennen, wird nach Abschluss von Interoperabilitätsprüfungen die Leistung des BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters beurteilt und schriftlich festgehalten.

2.9.5 Anforderungen bei einer erneuten Kompetenzfeststellung

Zusammen mit der erneuten Benennung des BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters müssen die erforderlichen Tätigkeitsnachweise beim BSI eingereicht werden.

Diese werden verschieden gewichtet und mit Punktzahlen unterschiedlich hoch bewertet (s. Punkteskala bei einer erneuten Kompetenzfeststellung), wobei insgesamt eine Summe von 100 Punkten erreicht werden muss. Werden die aufgelisteten Tätigkeiten nur teilweise (zum Beispiel als Mitglied eines Projektteams) ausgeführt, wird die betreffende Tätigkeit prozentual mit der entsprechenden Punktezahl bewertet.

Punkteskala bei einer erneuten Kompetenzfeststellung

Tätigkeiten	***Bewertung (P = Punktzahl)***
Interoperabilitätsprüfungen	25 P
Bereitstellung und Konfiguration des ZPL	20 P
Entwicklertests	15 P
Schulung zum BOS-Digitalfunknetz bzw. zur EADS TETRA-Systemtechnik *gehalten* (mind. eintägig)	10 P (max. 3x)
Schulung zum BOS-Digitalfunknetz bzw. zur EADS TETRA-Systemtechnik *besucht* (mind. eintägig)	5 P (max. 3x)
Mitwirkung bei der Fortschreibung der IOP-Richtlinien im Rahmen des kontinuierlichen Verbesserungsprozesses:	
• Fortschreibung der IOP-Richtlinien	10 P
• Durchführung von qualifizierter Qualitätssicherung	5 P (max. 4x)

2.9.6 Pflichten eines BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters

Der BOS-Interoperabilitätsprüfer bzw. ZPL-Mitarbeiter stellt sicher, dass er

1. alle Tätigkeiten objektiv und unabhängig sowie entsprechend den geltenden Vorgaben (Richtlinien und Verfahrensbeschreibungen) durchführt,
2. die Vorgaben des BSI und der BDBOS sowie die in den betreffenden Verfahrensbeschreibungen festgelegten Vorgehensweisen beachtet und einhält,
3. eventuelle Auflagen erfüllt und Abweichungen umgehend behebt sowie
4. bei signifikanten Änderungen, die sich auf die festgestellte Kompetenz oder die Arbeitsweise auswirken, die Personenzertifizierungsstelle unverzüglich unterrichtet.

Bei der Durchführung von Interoperabilitätsprüfungen stellt der BOS-Interoperabilitätsprüfer sicher, dass er der BDBOS jederzeit umfassend Auskunft über Ablauf und Inhalt der Interoperabilitätsprüfungen geben kann. Der ZPL-Mitarbeiter stellt bei der Bereitstellung und Konfiguration des ZPL sicher, dass er der BDBOS jederzeit umfassend Auskunft über die Konfigurationsstände des ZPL geben kann.

3 Änderungshistorie

Version	*Datum*	*Durchgeführte Änderungen*
1.0	09.07.2009	Erstausgabe: • Geltungsbereich im Digitalfunk BOS • Geltungsbereich „Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz“
1.1	17.07.2009	Revision: • Änderungen in den Geltungsbereichen im Digitalfunk BOS – Konkretisierung in Kapitel „Pflichten des anerkannten BOS-Interoperabilitätsprüfers bzw. ZPL-Mitarbeiters“
2.0	06.08.2010	Neuausgabe: • Aufnahme neuer Geltungsbereiche (Anerkennungs- und Zertifizierungsbereiche) • Änderungen im Geltungsbereich im Digitalfunk BOS – Konkretisierung in Kapitel „In der Kompetenzfeststellung nachzuweisende Fachkompetenz“
2.1	18.04.2011	Revision: • Aufnahme des neuen Geltungsbereichs „Testierer De-Mail“ • Berufserfahrung – Konkretisierung in den Beschreibungen (anrechenbare Zeiten) • Auditor „De-Mail“ - Konkretisierung in den Zulassungsvoraussetzungen • TR-Prüfer „De-Mail“ - neue Unterteilung in zwei Geltungsbereiche „Funktionalität“ und „Interoperabilität“
2.2	03.09.2013	Revision: • Überarbeitung des gesamten Dokuments • Ergänzungen in Kapitel 1 bis 3 • grundsätzliche Überarbeitung der Erst- und Rezertifizierung von Auditteamleitern • Überarbeitung der Rezertifizierung von Penetrationstestern
2.3	27.11.2013	Revision: • Ergänzung Zulassungsvoraussetzungen De-Mail-Auditor
2.4	10.12.2013	Revision: • neues Kapitel „Kompetenzfeststellung bei TR-Prüfern eID-Clients“ eingefügt

Version	*Datum*	*Durchgeführte Änderungen*
2.5	01.04.2014	Überarbeitung der Anforderungen an die Rezertifizierung der Auditteamleiter (Abschwächung der Anforderungen und Verschiebung um ein Jahr)
2.6	25.06.2014	Revision: • Überarbeitung Kapitel 2.1.2.2 Anforderungen an die Berufserfahrung von Auditteamleitern • Überarbeitung Kapitel 2.1.5 Anforderungen zur Rezertifizierung von Auditteamleitern – Punkteskala ab dem 01.01.2016 • Aufnahme eines neuen Geltungsbereichs der Personenzertifizierung „Zertifizierung als Auditor Secure CA Operation“ für BSI TR-03145 (Kapitel 2.3) • Aufnahme eines neuen Geltungsbereichs der Kompetenzfeststellung von Personen „Kompetenzfeststellung bei TR-Prüfern elektronischer Mitarbeiterausweis“ BSI TR-03126-5 (Kapitel 3.3)
2.7	15.03.2015	Revision: • Aufnahme eines neuen Geltungsbereichs der Kompetenzfeststellung von Personen nach BSI TR-03140 (Kapitel 3.4) • Änderung der Anforderungen an die Zertifizierung von Penetrationstestern (Kapitel 2.5) • Änderung der Anforderungen an die Zertifizierung als Auditor „Secure CA Operation“ (Kapitel 2.3) • Änderungen Glossar
2.8.	18.12.2015	Revisionen im Bereich Zertifzierung Auditteamleiter: • Streichung der BSI-Schulung und ersetzen durch externe Schulung • Punkteschema. Streichen der 2015-er Tabelle • Anpassung der Kostensätze
2.9	08.07.2016	Neuausgabe: • Aufnahme des Geltungsbereichs Smart Meter Gateway Administration
3.0	29.07.2016	Aufnahme des Geltungsbereichs Sicherer E-Mail Transport Ausbau redaktioneller Fehler an anderen Stellen
3.1	15.08.2016	Ausbau redaktioneller Fehler an anderen Stellen
3.2	20.09.2016 25.11.2016	Änderung im Bereich als IS-Revisor Revision: • Aufnahme des Geltungsbereichs der Kompetenzfeststellung von Personen nach BSI TR-03140; Kompetenzfeststellung bei TR-Prüfern „eID-Server“ (Kapitel 3.6)

Version	*Datum*	*Durchgeführte Änderungen*
3.3	29.03.2017	Revision: • Aufnahme des Geltungsbereichs RESISCAN [TR 03138] in der Personenzertifizierung • Entfernen des Geltungsbereichs „Kompetenzfeststellung bei Testierern De-Mail“ • Entfernung der Bezüge zum UP-Bund bei IS-Revisoren und Penetrationstestern
3.4	29.08.2017	Revision: • Entfernen des Geltungsbereichs „Kompetenzfeststellung von Personen“ (TR-Prüfer)
3.5	02.02.2018	Revision: • Einfügen allgemeiner Hinweis zu Kosten der (Re)zertifizierung unter Punkt „2 Zertifizierung von Personen“ • Entfernen der Unterpunkte „Kosten der (Re)zertifzierung“ • Änderungen bei Pflichten des zertifizierten IS-Revisors und Penetrationstesters

4 Glossar

Die im Folgenden verwendeten Begriffe stehen im speziellen Kontext der Anerkennung von Stellen und erheben keinen Anspruch auf Allgemeingültigkeit.

Kursiv gedruckte Begriffe verweisen auf weitere Definitionen in diesem Glossar.

Begriff	***Beschreibung***
Antrag	Formales Schreiben, das die Grundlage zur Aufnahme eines *Personenzertifizierungsverfahrens* bildet.
Auditoren/Auditteamleiter	Personengruppe für die Durchführung von Audits für Organisationen, die ein Zertifikat nach ISO 27001 auf der Basis von IT-Grundschutz erhalten und aufrecht erhalten wollen. (Anmerkung: beide Begriffe werden im Dokument synonym verwendet.)
BDBOS	Bundesanstalt für den Digitalfunk der *BOS*
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BOS-Interoparabilitätsprüfer	Personengruppe für die Durchführung von Evaluierungen für Produkte im Digitalfunk *BOS*, die eine Anerkennung für die Durchführung von Interoperabilitätsprüfungen für Funkgeräte oder Leitstellen im Digitalfunk *BOS* erhalten.
CC	Common Criteria for Information Technology Security Evaluation
DAkkS	Deutsche Akkreditierungsstelle GmbH - nationale Akkreditierungsstelle der Bundesrepublik Deutschland
eID-Infrastruktur	Infrastruktur zur sicheren elektronischen Identifizierung
Evaluierung	Prozess der *Kompetenzfeststellung* zur Bewertung der Erfüllung der Anforderungen des Programms bei einem *Kandidaten*.
Erstparteien-Audit	Hierzu zählen nur Erstparteien-Audits, die im Auftrag einer Organisation und nicht von der Organisation selbst für interne Zwecke durchgeführt wurden (anders als in DIN EN ISO 9000:2005 [DIN 9000], Kapitel 2.8.2).
Geltungsbereich	Der Bereich, für den die *Zertifizierung* oder Anerkennung beantragt bzw. erfolgt ist.
IT-System	Eine spezifische IT-Installation mit einem bestimmten Zweck und einer spezifischen Einsatzumgebung.
Kandidat	Die natürliche Person, bei der eine *Kompetenzfeststellung* durchgeführt wird und die ggf. eine *Personenzertifizierung* beim BSI beantragt hat.
Kriterienwerk	Sammelbezeichnung für Sicherheitskriterien, Evaluationskriterien, Sicherheitsstandards und -normen, o.Ä.; Regelwerke mit (technischen) Anforderungen an einen Evaluationsgegenstand (EVG) und/oder Vorgaben für die Durchführung

Begriff	*Beschreibung*
	der Evaluierung des EVGs (im Sinne der Produktzertifizierung) und Bewertung der Ergebnisse (hier: vom BSI öffentlich bekannt gemacht oder allgemein anerkannt), z.B. *CC* oder *TR*.
Kompetenzfeststellung	*Evaluierung* der Anforderungen an einen *Kandidaten*.
Personenzertifizierung	s. *Zertifizierung*
Prüfstelle	(staatliche oder privatwirtschaftliche) Stelle, die *Evaluierungen* durchführt (hier: eine vom BSI im Sinne der Anerkennung von Stellen anerkannte Prüfstelle bzw. zertifizierter IT-Sicherheitsdienstleister) – wird synonym zum Begriff Prüflaboratorium der DIN EN ISO/IEC 17025 [ISO 17025] verwendet.
Stelle	Kurzbezeichnung für *Prüfstellen*/-labore und IT-Sicherheitsdienstleister
Technische Richtlinie (TR)	*Kriterienwerk* und technische Prüfvorschrift des BSI für Konformitätsprüfungen [TR].
TR-Prüfer	Personengruppe für die Durchführung von Evaluierungen für Produkte, die ein *Zertifikat* nach *Technischen Richtlinien* [TR] erhalten.
Zertifikat	Dokument, das einen erfolgreichen Abschluss einer *Zertifizierung* bescheinigt.
Zertifizierung	Bezeichnung des Gesamtverfahrens, bestehend aus den folgenden Phasen: Antragstellung beim BSI, *Kompetenzfeststellung*, Zertifizierungsentscheidung, Überwachung der Zertifizierung und Rezertifizierung.
Zertifizierungsantrag	Antrag, der die Grundlage zur Aufnahme eines Zertifizierungsverfahrens bildet.
Zertifizierungsstelle	Eine das Verfahren der *Zertifizierung* abwickelnde Stelle.
Zertifizierungsvertrag	Vertrag zwischen dem BSI und einem *Kandidaten* mit dem Ziel der *Personenzertifizierung* für einen speziellen *Geltungsbereich*. Dieser Vertrag regelt Rechte und Pflichten des BSI, des *Kandidaten* bzw. der zertifizierten Person.
ZPL-Mitarbeiter	Personengruppe, deren Kompetenz für die Bereitstellung eines Zertifizierungsprüflabors für Interoperabilität-Prüfungen mit Wirknetzrelevanz für den Digitalfunk *BOS* bestätigt wurde.
Zweitparteien-Audits	Zweitparteien-Audits werden von Parteien, die ein Interesse an der Organisation haben, wie z.B. Kunden oder von Personen in deren Auftrag durchgeführt (vgl. DIN EN ISO 9000:2005 [DIN 9000], Kapitel 3.9.1).

Literaturverzeichnis

[Auditierungsschema] Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Auditierungsschema, Version 1.0, BSI, Bezugsquelle unter: https://bsi.bund.de

[BIP] BOS-Interoperabilitätsprofile 1-20, BDBOS, Version 2009-04, Bezugsquelle unter http://www.bdbos.bund.de

[BIZ-AT] BOS-Interoperabilitätszertifikats-Anforderungstabelle, BDBOS, Version 2009-04, Bezugsquelle unter http://www.bdbos.bund.de

BnetzA-Katalog: IT-Sicherheitskataloggemäß § 11 Absatz 1a Energiewirtschaftsgesetz,

[BOS-IOP-Richtlinien] Interoperabilitäts-Richtlinien der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS), BDBOS, Bezugsquelle unter http://www.bdbos.bund.de/

BSI TR-03109: BSI, Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03109/index_htm.html;jsessionid=D675D38D0C9D0EB337030F041F172B23.2_cid286,

BSI TR-03109-6: Smart Meter Gateway Administration, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/AdministrationBetrieb/TechnRichtlinie/TR_03109-6.html,

[BSI100] IT-Sicherheitsmanagement und IT-Grundschutz - BSI Standards 100-1, 100-2 und 100-3, 2008, BSI, Bezugsquelle unter https://www.bsi.bund.de/IT-Grundschutz

[BSIG] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, (BSI-Gesetz – BSIG), Bezugsquelle: Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 54, ausgegeben zu Bonn am 19. August 2009

[BSIZertV] Verordnung über das Verfahren der Erteilung eines Sicherheitszertifikats durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungsverordnung - BSIZertV), ausgefertigt am 07.07.1992, Bezugsquelle unter: www.gesetze-im-internet.de

[BTP] BOS-Testpläne 01-20, BDBOS, Version 2009-04, Bezugsquelle unter http://www.bdbos.bund.de

[DIN 9000] Qualitätsmanagementsysteme –Grundlagen und Begriffe (ISO 9000:2005), Stand: Dezember 2006,

[EINF] Einführung in die BOS-IOP-Richtlinien für Endgeräte zur Nutzung im Digitalfunk, BOS, BDBOS, Version 2009-04, Bezugsquelle unter http://www.bdbos.bund.de

[GAN] Abschlussbericht der Expertengruppe aus Bund und Ländern Gruppe "Anforderungen an das Netz (GAN) über die Leistungsmerkmale eines Mindeststandards und über die Bewertung der technischen Lösungen, Zentralstelle zur Vorbereitung der Einführung eines bundesweit einheitlichen digitalen Sprech- und Datenfunksystems - Digitalfunk - (ZED), Bezugsquelle unter http://www.bdbos.bund.de

[ISO 17025] Allgemeine Anforderungen an die Kompetenz von Prüf- und Kalibrierlaboratorien (ISO/IEC 17025:2005), Beuth 2005, Bezugsquelle unter http://www.iso.org/

[ISO 27001] Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2005), 2008-09, ISO, , Bezugsquelle unter http://www.iso.org/

[ISO 27006] ISO/IEC 27006:2011 "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems", , Bezugsquelle unter: http://www.iso.org/

[ISO/IEC 27006] ISO/IEC 27006:2011 "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems", , Bezugsquelle unter: http://www.iso.org/

[IT-GS] IT-Grundschutz, BSI, Bezugsquelle unter https://www.bsi.bund.de/IT-Grundschutz

[IT-Sicherheitsgesetz]

[KRYPTO] BOS-Kryptosystem " Herstellerpaket", BSI, Bezugsquelle unter https://www.bsi.bund.de oder http://www.bdbos.bund.de

[LM-END] Endgeräteleistungsmerkmale für Endgeräte zur Nutzung im BOS-Digitalfunknetz, BDBOS, Version 2009-04, Bezugsquelle unter http://www.bdbos.bund.de

[LS1-3] System Interface Specification Leitstellen-Schnittstellen. Release 5.5, EADS Secure Networks GmbH, Version 03, Bezugsquelle unter http://www.eads.net oder http://www.bdbos.bund.de

[MINF] Marktinformation für Endgeräte zur Nutzung im Digitalfunk BOS, BDBOS, Version 2009-04, Bezugsquelle unter http://www.bdbos.bund.de

[Prog-Personen] Programm zur zur Kompetenzfeststellung und Zertifizierung von Personen, V 2.2, Stand 24.07.2013, BSI, Bezugsquelle unter https://www.bsi.bund.de/zertifizierung

[Prog-Stellen] Prgoramm zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern, Version 3.1, 04.04.2013, BSI, Bezugsquelle unter: https://www.bsi.bund.de

[REV] Informationssicherheitsrevision- ein Leitfaden für IS-Revision auf der Basis von IT-Grundschutz, Version 2.0, März 2010, Bezugsquelle unter https://www.bsi.bund.de/is-revision

[RTCG] Radio Terminal Compatibility Guide. Release 5.5, EADS Secure Networks GmbH, Version 04, Bezugsquelle unter http://www.eads.net oder http://www.bdbos.bund.de

[Schema] IT-Sicherheitsmanagement und IT-Grundschutz-Prüfschema für ISO 27001-Audits, Version 2.1, Bezugsquelle unter http://www.iso.org/

[TR] Technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI), BSI, Bezugsquelle unter https://www.bsi.bund.de/

[TR-03124-1] Technical Guideline TR-03124-1eID-Client – Part 1: Specifications, Version 1.2, 2015, Bezugsquelle unter https://www.bsi.bund.de/

[TR-03124-2] Technical Guideline TR-03124-2eID-Client – Part 2: Conformance - Test Specification, Version 1.2, 2015, Bezugsquelle unter https://www.bsi.bund.de

[TR-03130-1] Technical Guideline eID-Server Part 1: Functional Specification, Version 2.0.2, 2016, Bezugsquelle unter https://www.bsi.bund.de

[TR-03130-4] Technical Guideline TR-03130 eID-Server Part 4: Conformance Test Specification, Version 1.0, 2016, Bezugsquelle unter https://www.bsi.bund.de

[TR-03145] Secure CA operation - Generic requirements for Trust Centers instantiating as Certification Authority (CA) in a Public-Key Infrastructure (PKI) with security level 'high', Version 1.0, 2014, Bezugsquelle unter https://www.bsi.bund.de/

[VB-Personen] Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen, Version 2.2, 01.07.2013, BSI, Bezugsquelle unter: https://bsi.bund.de