Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Personenzertifizierung: Programm Auditoren bzw. Auditteamleiter

Auditoren

Version 2.0 vom 01.11.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0)800 247-1000
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Änderungshistorie

Version	*Datum*	*Name/Org.-Einheit*	*Beschreibung*
1.0	30.11.2021	Personenzertifizierungsstelle SZ 12	Erstausgabe ersetzt VB-Auditoren
1.1	14.02.2022	Personenzertifizierungsstelle SZ 12	Revision: • Fehlende Zulassungsvoraussetzung bei den Secure CA Operation Auditoren wieder eingefügt (2.4.1 und 2.4.3).
1.2	01.06.2023	Personenzertifizierungsstelle SZ 12	Revision: • Abbildung 1: "Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramme)" entfernt und Kapitel 1.1 und 1.2 zusammengelegt • „Auditor sicherer E-Mail-Transport“ gelöscht • Formatierungsfehler in Punkt 2.2.1.4.2 korrigiert
2.0	01.11.2024	Personenzertifizierungsstelle SZ12	Revision: • Umstrukturierung des Dokumentes • Überarbeitung der Literaturangaben und der Zitate der Rechtsnormen • Redaktionelle und strukturelle Anpassungen • Entfall der Anforderung zur DAkkS-Akkreditierung • IT-GS-Berater als Alternative zur IT-GS-Schulung (2.2.1.3.) • Tabellarische Zusammenfassung der Zulassungsvoraussetzungen eingefügt

Tabelle 1: Änderungshistorie

Inhalt

1 Einleitung

Die Zertifizierung eines Auditors kann auf Antrag einer natürlichen Person durchgeführt werden.

1.1 Zielsetzung und Eingliederung des Dokuments Auditoren

Dieses Dokument beinhaltet verpflichtende Anforderungen und weitere wichtige Informationen und Regelungen als Ergänzung zur übergeordneten „Verfahrensbeschreibung zur Zertifizierung von Personen“ [VB-Personen]. Es richtet sich insbesondere an die Antragsteller, die sich dafür entschieden haben, eine Zertifizierung als Auditor durchführen zu lassen.

Es werden die speziellen Anforderungen mit detaillierten Hinweisen zu Verfahrensabläufen benannt, die ein Antragsteller berücksichtigen muss. An den entsprechenden Stellen im Dokument wird z. B. auf Formulare oder weitere Hilfsmittel hingewiesen, die insbesondere bei einer Erstzertifizierung hilfreich sind.

Die Beschreibung der verschiedenen Dokumentenkategorien befindet sich in der übergeordneten [VB-Personen].

Das Dokument „Verzeichnisse“ [Verzeichnisse] gibt einen Überblick über alle benötigten Hilfs- und Informationsquellen (Literaturverzeichnis) und enthält ein Stichwort- und Abkürzungsverzeichnis (Glossar).

2 Zertifizierungsprogramm Auditoren

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

Das vorliegende Zertifizierungsprogramm beschreibt die verschiedenen Auditorengruppen sowie die Kompetenzanforderungen in diesen Geltungsbereichen.

Eine ***Zertifizierung von Auditoren*** wird für folgende Auditorengruppen durchgeführt:

- **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.
- **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.
- **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.
- **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.
- **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.

2.1 Persönliche Eigenschaften eines Auditors bzw. Auditteamleiters

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

2.1.1 Managementfähigkeiten

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

2.1.2 Kommunikationsfähigkeiten

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

2.1.3 Didaktische Fähigkeiten

- Objektive Ergebnispräsentation

2.1.4 Methodenkompetenz

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

2.1.5 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

2.1.6 Unabhängigkeit

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

2.2 Zertifizierung als Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz

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-Zertifizierungs- und Anerkennungsverordnung – BSIZertV [BSI-ZertV]) vom 17. Dezember 2014 sowie die ISO/IEC 27006 [ISO 27006], eine Norm für Stellen, die Audits und Zertifizierungen von Informationssicherheitsmanagementsystemen (ISMS) anbieten.

2.2.1 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft. Ein Lebenslauf mit Ausbildungs-und Arbeitshistorie, sowie eine aktuelle Arbeitgeberbescheinigung mit Angabe der Art und des Umfanges (Voll-/Teilzeit in %) der Beschäftigung sind vorzulegen.

2.2.1.1 Bildungsabschluss

Anforderung

Der Antragsteller 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 Antragsteller 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 Antragsteller 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 bzw. Auftraggeber) über die Berufserfahrung sind vorzulegen.

2.2.1.2 Berufserfahrung

Anforderung

Der Antragsteller 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.

Nachweis

Ein Zeugnis oder eine unterschriebene Bestätigung eines unabhängigen Dritten (z.B. Arbeitgeber bzw. Auftraggeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Zulassung sowie Beschäftigung als Auditor bzw. Auditteamleiter sind vorzulegen.

Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung.

2.2.1.3 Qualifikation als Auditor

Anforderung

Der Antragsteller muss

- in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum) an einer mindestens 3-tägigen IT-Grundschutzschulung (nach BSI-Standard 200 [BSI200]) mit bestandener Abschlussprüfung teilgenommen haben
  oder alternativ ein aktuell gültiges IT-Grundschutz-Berater-Zertifikat vorweisen können
  und
- eine mindestens 5-tägige Ausbildung zum Auditor für ISO 27001 mit bestandener Abschlussprüfung vorweisen.

Nachweis

Teilnahmebescheinigungen, Prüfungszeugnisse, Zertifikate sind vorzulegen.

2.2.1.4 Praxiserfahrung

Anforderung

Zum Nachweis der Praxiserfahrung stehen 2 alternative Varianten zur Verfügung:

2.2.1.4.1 Variante I

Der Antragsteller muss in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum), an 4 Zertifizierungsaudits (Drittparteien-Audits) im Bereich Informationssicherheit mit mindestens je 3 Personentagen teilgenommen haben, davon:

- mindestens 1 Audit durchgängig nach BSI-Standard 200-2 [BSI200] und
- mindestens 1 ISO 27001-Zertifizierungsaudit als leitender Auditor.

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.

Der Antragsteller muss als Auditor, Auditor-Trainee oder technischer Experte, mit einem Gesamtumfang von mindestens 20 Personentagen teilgenommen haben.

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

2.2.1.4.2 Variante II

Der Antragsteller muss in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum) an 6 Zweitparteien-Audits im Bereich Informationssicherheit mit mindestens je 3 Personentagen teilgenommen haben, davon

- mindestens 1 Audit durchgängig nach BSI-Standard 200-2[BSI200] und
- zusätzlich mindestens 1 ISO 27001-Zertifizierungsaudit leitend.

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.

Der Antragsteller muss als verantwortlicher Auditor, mit einem Gesamtumfang von mindestens 20 Personentagen teilgenommen haben.

Bei allen 6 Audits muss der Antragsteller am gesamten Audit beteiligt gewesen sein.

Nachweis

Gefordert sind vom Auftraggeber oder Arbeitgeber bestätigte und unterschriebene Kurzberichte über die Durchführung der Audits bzw. bei Zertifizierungsaudits die Vorlage der erlangten Zertifikate mit einer Bestätigung des zertifizierten Unternehmens über die Dauer des Audits und dass der Antragsteller der verantwortliche Auditor bzw. Auditteamleiter gewesen 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 Antragstellers,
- der Zeitraum und Umfang (Personentage) des Audits.

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

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

Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Art	***Anforderung***	***Nachweis***
Bildungsabschluss	• Lebenslauf mit Ausbildungs-und Arbeitshistorie • 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	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Beschäftigung als Auditor

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 200-2 „IT-Grundschutz-Vorgehensweise“
	  • mindestens 1 ISO 27001-Zertifizierungsaudit als leitender Auditor
	• 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 Zweitparteien-Audits im Bereich Informationssicherheit mit mindestens je 3 Personentagen, davon
	  • mindestens 1 Audit durchgängig nach BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“
	  • zusätzlich mindestens 1 ISO 27001-Zertifizierungsaudit leitend
	• 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 200-2 alternativ • vom BSI aktuell zertifizierter IT-Grundschutz-Berater • mind. 5-tägige Ausbildung zum Auditor für ISO 27001	• Teilnahmebescheinigungen • Prüfungszeugnisse • erlangte Zertifikate

2.2.2 Anforderungen an die Fachkompetenz

2.2.2.1 Basiskenntnisse

Es werden die folgenden grundlegenden 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 200-1 bis 200-3 und 200-4 im Überblick, IT-Grundschutz nach BSI-Standard 200-2 [BSI200]),
- 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).

2.2.2.2 Erweiterte Fachkenntnisse

- Weitere system- und produktbezogene Informationssicherheitsstandards,
- 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 200-3 [BSI200],
- 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/erweiterte Fachkenntnisse).

2.2.3 Qualifizierungsmaßnahme

Eine Qualifizierungsmaßnahme wird vom BSI nicht angeboten.

2.2.4 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung

Es werden anhand von Fragen die Kenntnisse des Kandidaten in den geforderten Bereichen beurteilt.

Es wird eine 90-minütige schriftliche Prüfung (Multiple-Choice-Test) durchgeführt.

2.2.5 Aufrechterhaltung der Zertifizierung

2.2.5.1 Anforderungen an die Durchführung der Audits

Alle Audits müssen durch die zertifizierte Person gemäß [ISO 17021-1] bzw. [ISO 19011] durchgeführt werden. Dabei sind insbesondere die jeweiligen Regelungen zur Durchführung der Audits in den jeweiligen Programmen zu berücksichtigen und einzuhalten (z. B. das Auditierungsschema im IT-Grundschutz).

2.2.5.2 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 (sofern angeboten) 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 Antragsteller Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

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

Punkteskala zur Rezertifizierung

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 200-2 [BSI200] 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.

Tätigkeiten	*Bewertung (P= Punktzahl)*	
Audits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Auditteamleiter durchgeführt	35 P	2 Audits aus diesem Bereich sind zwingend erforderlich
Audit für ISO 27001-Zertifikate leitend durchgeführt (für in diesem Bereich von der DAkkS akkreditierten Zertifizierungsstelle), max. 2 Audits werden gewertet	25 P	
Audits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Co-Auditor/begleitender Auditor durchgeführt	15 P	
Überwachungsaudits für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Auditteamleiter durchgeführt (auch außerplanmäßige Überwachungsaudits)	10 P	
Audits mit Auditor-Testat (BSI-Standard 200-2 [BSI200]) als Auditteamleiter durchgeführt	10 P	
Projekt mit Zielsetzung der Umsetzung eines Sicherheitskonzeptes nach der Vorgehensweise gemäß BSI-Standard 200-2 [BSI200] abgeschlossen	10 P	
Grundschutz-Beratungsprojekt mit Zertifikatsziel abgeschlossen (mindestens 20 Tage)	10 P	
Schulung über IT-Grundschutz gehalten (mindestens 2-tägig)	10 P	
Entwicklung eines IT-Grundschutz-Bausteines (nur veröffentlichte Bausteine)	10 P	

2.3 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.

Diese Zertifizierung setzt auf der Personenzertifizierung als „**Auditteamleiter** für die Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz“ auf.

2.3.1 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

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

Der Auditor „De-Mail" muss zur Aufnahme in das Zertifizierungsverfahren ein gültiges Auditteamleiter-Zertifikat nachweisen.

2.3.1.1 Bildungsabschluss

Die Anforderungen an den Bildungsabschluss entsprechen denen, die an Auditteamleiter (2.2.1.1) gestellt werden und muss in diesem Zertifizierungsverfahren nicht mehr nachgewiesen werden.

2.3.1.2 Berufserfahrung

Die Anforderungen an die Berufserfahrung entsprechen denen, die an Auditteamleiter (2.2.1.2) gestellt werden und muss in diesem Zertifizierungsverfahren nicht mehr nachgewiesen werden.

2.3.1.3 Qualifikation als Auditor

Die Anforderungen an die Qualifikation als Auditor entsprechen denen, die an Auditteamleiter (2.2.1.2) gestellt werden und muss in diesem Zertifizierungsverfahren nicht mehr nachgewiesen.

2.3.1.4 Praxiserfahrung

Anforderung

Der Auditor „De-Mail“ für BSI TR-01201 muss in den vergangenen 3 Jahren (Stichtag: Antragseingang) mindestens 3 vollständige Zertifizierungsaudits im Bereich ISO 27001 auf der Basis von IT-Grundschutz (keine Überwachungsaudits) als Auditteamleiter durchgeführt haben.

Nachweis

Angabe der Zertifikatsnummern der Zertifizierungsaudits bei Antragstellung.

2.3.1.5 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

• *Art*	• ***Anforderung***	• ***Nachweis***
Bildungsabschluss/ Berufserfahrung	• vom BSI zertifizierter Auditteamleiter auf Basis von IT-Grundschutz	Zertifikat
Praxiserfahrung/ Auditerfahrung	In den letzten 3 Jahren 3 Zertifizierungsaudits im Bereich ISO 2700 auf Basis von IT-Grundschutz	Angabe der Zertifizierungsnummern

2.3.2 Qualifizierungsmaßnahme

Das BSI bietet keine Qualifizierungsmaßnahme an.

2.3.3 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung

Es wird keine Prüfung durchgeführt.

2.3.4 Aufrechterhaltung der Zertifizierung

2.3.4.1 Anforderungen an die Durchführung der Audits

Alle Audits müssen durch die zertifizierte Person gemäß [ISO 17021-1] bzw. [ISO 19011] durchgeführt werden. Dabei sind insbesondere die jeweiligen Regelungen zur Durchführung der Audits in den jeweiligen Programmen zu berücksichtigen und einzuhalten (z. B. das Auditierungsschema im IT-Grundschutz).

2.3.4.2 Kompetenzüberwachung

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

2.3.4.3 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene, vom Auftraggeber unterschriebene Tätigkeitsnachweise erbringen und an den Erfahrungsaustauschterminen des BSI (sofern angeboten) 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 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 Antragsteller Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

Sind die Nachweise für die 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.

Punkteskala zur Rezertifizierung

Tätigkeiten	*Bewertung (P = Punktzahl)*
Audit für ISO 27001-Zertifikate auf der Basis von IT-Grundschutz als Auditteamleiter durchgeführt	20 P
De-Mail-Audit durchgeführt	50 P

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

Nur eine sichere Certification Authority kann in einer Public Key Infrastruktur für die Sicherung von Vertraulichkeit oder auch Authentizität und Integrität von Informationen dienen.

Die Grundlage von Public Key Infrastrukturen (PKI) ist Vertrauen. Daher muss eine Certification Authority (CA) 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 eindeutigen und dokumentierten Anforderungen.

Die [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.

2.4.1 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft. Ein Lebenslauf mit Ausbildungs-und Arbeitshistorie, sowie eine aktuelle Arbeitgeberbescheinigung mit Angabe der Art und des Umfanges (Voll-/Teilzeit in %) der Beschäftigung sind vorzulegen.

2.4.1.1 Bildungsabschluss

Anforderung

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

Sollte der Antragsteller 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 Antragsteller 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 bzw. Auftraggeber) über die Berufserfahrung sind vorzulegen.

2.4.1.2 Berufserfahrung

Anforderung

Der Antragsteller 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.

Nachweis

Ein Zeugnis oder eine unterschriebene Bestätigung eines unabhängigen Dritten (z.B. Arbeitgeber bzw. Auftraggeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Zulassung sowie Beschäftigung als Auditor bzw. Auditteamleiter sind vorzulegen.

Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung

Darüber hinaus 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.

2.4.1.3 Qualifikation als Auditor

Anforderung

Der Antragsteller muss

- in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum) an einer mindestens 3-tägigen IT-Grundschutzschulung (nach BSI-Standard 200 [BSI200]) mit bestandener Abschlussprüfung teilgenommen haben
  oder alternativ ein aktuell gültiges IT-Grundschutz-Berater-Zertifikat vorweisen können
  und
- eine mindestens 5-tägige Ausbildung zum Auditor für ISO 27001 mit bestandener Abschlussprüfung vorweisen.

Nachweis

Teilnahmebescheinigungen, Prüfungszeugnisse, Zertifikate sind vorzulegen

2.4.1.4 Praxiserfahrung

Anforderung

Innerhalb der letzten 3 Jahre muss der Kandidat mindestens an einem ISO 27001-Zertifizierungsaudit als Auditor teilgenommen haben. Dies schließt eine Beschäftigung als externer Auditor (nach ISO/IEC 27006-2011 Abschnitt 7.3 [ISO 27006]) ein.

Nachweis

Gefordert ist bei dem Zertifizierungsaudit die Vorlage des erlangten Zertifikats mit einer Bestätigung des zertifizierten Unternehmens, dass der Antragsteller der verantwortliche Auditor bzw. Auditteamleiter gewesen ist.

2.4.1.5 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Art	***Anforderung***	***Nachweis***
Bildungsabschluss	• Lebenslauf mit Ausbildungs-und Arbeitshistorie • 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	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Beschäftigung als Auditor
Qualifikation als Auditor	• in den letzten 3 Jahren Teilnahme mind. 3 tägiger IT-Grundschutz-Schulung (BSI-Standard 200-2 alternativ vom BSI aktuell zertifizierter IT-Grundschutz-Berater • mind. 5 tägige Ausbildung zum Auditor für ISO 27001	• Teilnahmebescheinigungen • Prüfungszeugnisse • erlangte Zertifikate
Praxiserfahrung/ Auditerfahrung	• in den letzten 3 Jahren ein ISO 27001-Zertifizierungsaudit als leitender Auditor	• vom Auftraggeber/Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate

2.4.2 Anforderungen an die Fachkompetenz

2.4.2.1 Basiskenntnisse

Es werden die folgenden grundlegenden 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.

2.4.2.2 Erweiterte Fachkenntnisse

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

2.4.3 Qualifizierungsmaßnahme

Das BSI bietet keine Qualifizierungsmaßnahme an.

2.4.4 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung

Es werden anhand von Fragen die Kenntnisse des Kandidaten in den geforderten Bereichen beurteilt.

Es wird eine 45-minütige schriftliche Prüfung durchgeführt.

2.4.5 Aufrechterhaltung der Zertifizierung

2.4.5.1 Anforderungen an die Durchführung der Audits

Alle Audits müssen durch die zertifizierte Person gemäß [ISO 17021-1] bzw. [ISO 19011] durchgeführt werden. Dabei sind insbesondere die jeweiligen Regelungen zur Durchführung der Audits in den jeweiligen Programmen zu berücksichtigen und einzuhalten (z. B. das Auditierungsschema im IT-Grundschutz).

2.4.5.2 Kompetenzüberwachung

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

2.4.5.3 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene, vom Auftraggeber unterschriebene Tätigkeitsnachweise erbringen und an den Erfahrungsaustauschterminen des BSI (sofern angeboten) 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 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 Antragsteller Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

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

Punkteskala zur Rezertifizierung

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 leitend 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
Audits für ISO 27001-Zertifikate als Co-Auditor/begleitender Auditor im Bereich PKI durchgeführt	25 P
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)

Tätigkeiten	*Bewertung (P = Punktzahl)*
Projekt mit Zielsetzung der Umsetzung eines Sicherheitskonzeptes im Bereich PKI nach der Vorgehensweise gemäß [ISO 27001] abgeschlossen	15 P (max. 3x)

2.5 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 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.

2.5.1 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft. Ein Lebenslauf mit Ausbildungs-und Arbeitshistorie, sowie eine aktuelle Arbeitgeberbescheinigung mit Angabe der Art und des Umfanges (Voll-/Teilzeit in %) der Beschäftigung sind vorzulegen.

2.5.1.1 Bildungsabschluss

Anforderung

Der Antragsteller 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 Antragsteller 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 Antragsteller 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 bzw. Auftraggeber) über die Berufserfahrung sind vorzulegen.

2.5.1.2 Berufserfahrung

Anforderung

Der Antragsteller 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.

Nachweis

Ein Zeugnis oder eine unterschriebene Bestätigung eines unabhängigen Dritten (z.B. Arbeitgeber bzw. Auftraggeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Zulassung sowie Beschäftigung als Auditor bzw. Auditteamleiter sind vorzulegen.

Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung.

2.5.1.3 Qualifikation als Auditor

Anforderung

Der Antragsteller muss

- in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum) an einer mindestens 3-tägigen IT-Grundschutzschulung (nach BSI-Standard 200 [BSI200]) mit bestandener Abschlussprüfung teilgenommen haben
  oder alternativ ein aktuell gültiges IT-Grundschutz-Berater-Zertifikat vorweisen können
  und
- eine mindestens 5-tägige Ausbildung zum Auditor für ISO 27001 mit bestandener Abschlussprüfung vorweisen.

Nachweis

Teilnahmebescheinigungen, Prüfungszeugnisse, Zertifikate sind vorzulegen.

2.5.1.4 Praxiserfahrung

Anforderung

Bei der Praxiserfahrung stehen 2 alternative Varianten zur Verfügung:

2.5.1.4.1 Variante I

Der Antragsteller muss in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum), an 4 Zertifizierungsaudits (Drittparteien-Audits) im Bereich Informationssicherheit mit mindestens je 3 Personentagen teilgenommen haben, davon:

- mindestens 1 Audit durchgängig nach BSI-Standard 200-2 [BSI200] und
- mindestens 1 ISO 27001-Zertifizierungsaudit als leitender Auditor.

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.

Der Antragsteller muss als Auditor, Auditor-Trainee oder technischer Experte, mit einem Gesamtumfang von mindestens 20 Personentagen teilgenommen haben.

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

2.5.1.4.2 Variante II

Der Antragsteller muss in den zurückliegenden 3 Jahren (Stichtag: Antragsdatum) an 6 Zweitparteien-Audits im Bereich Informationssicherheit mit mindestens je 3 Personentagen teilgenommen haben, davon

- mindestens 1 Audit durchgängig nach BSI-Standard 200-2[BSI200] und
- zusätzlich mindestens 1 ISO 27001-Zertifizierungsaudit leitend.

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.

Der Antragsteller muss als verantwortlicher Auditor, mit einem Gesamtumfang von mindestens 20 Personentagen teilgenommen haben.

Bei allen 6 Audits muss der Antragsteller am gesamten Audit beteiligt gewesen sein.

Nachweis

Gefordert sind vom Auftraggeber oder Arbeitgeber bestätigte und unterschriebene Kurzberichte über die Durchführung der Audits bzw. bei Zertifizierungsaudits die Vorlage der erlangten Zertifikate mit einer Bestätigung des zertifizierten Unternehmens über die Dauer des Audits und dass der Antragsteller der verantwortliche Auditor bzw. Auditteamleiter gewesen 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 Antragstellers,
- der Zeitraum und Umfang (Personentage) des Audits.

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

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

Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Art	*Anforderung*	*Nachweis*
• Bildungsabschluss	• Lebenslauf mit Ausbildungs-und Arbeitshistorie • 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	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten sowie der Beschäftigung als Auditor
• 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 200-2 „IT-Grundschutz-Vorgehensweise“ • mindestens 1 ISO 27001-Zertifizierungsaudit als leitender Auditor • 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 Zweitparteien-Audits im Bereich Informationssicherheit mit mindestens je 3 Personentagen, davon • mindestens 1 Audit durchgängig nach BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“ • zusätzlich mindestens 1 ISO 27001-Zertifizierungsaudit leitend • 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 200-2, alternativ • vom BSI aktuell zertifizierter IT-Grundschutz-Berater • mind. 5-tägige Ausbildung zum Auditor für ISO 27001	• Teilnahmebescheinigungen • Prüfungszeugnisse • erlangte Zertifikate

2.5.2 Anforderungen an die Fachkompetenz

2.5.2.1 Basiskenntnisse

- 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.

2.5.2.2 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.

2.5.3 Qualifizierungsmaßnahme

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

2.5.4 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung

Es werden anhand von Fragen die Kenntnisse des Kandidaten in den geforderten Bereichen beurteilt.

Es wird eine 60-minütige Prüfung durchgeführt (schriftlich oder mündlich als Prüfungs-Interview).

2.5.5 Aufrechterhaltung der Zertifizierung

2.5.5.1 Anforderungen an die Durchführung der Audits

Alle Audits müssen durch die zertifizierte Person gemäß [ISO 17021-1] bzw. [ISO 19011] durchgeführt werden. Dabei sind insbesondere die jeweiligen Regelungen zur Durchführung der Audits in den jeweiligen Programmen zu berücksichtigen und einzuhalten (z. B. das Auditierungsschema im IT-Grundschutz).

2.5.5.2 Kompetenzüberwachung

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

2.5.5.3 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene, vom Auftraggeber unterschriebene Tätigkeitsnachweise erbringen und an den Erfahrungsaustauschterminen des BSI (sofern angeboten) 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 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 Antragsteller Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

Sind die Nachweise für die 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.

Punkteskala zur Rezertifizierung

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
• ISMS-Audit bei einer Sub-CA im Smart Metering Umfeld	• 10 P
• ISMS-Audit im Bereich des KRITIS-Sektors Energiebranche (z.B. bei einem Netzbetreiber)	• 10 P
• ISMS-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 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.

2.6.1 Zulassungsvoraussetzungen für die Teilnahme am Zertifizierungsverfahren

Die Zulassungsvoraussetzungen zur Zertifizierung werden in der Antragsphase durch Vorlage externer Fachkundenachweise überprüft. Ein Lebenslauf mit Ausbildungs-und Arbeitshistorie, sowie eine aktuelle Arbeitgeberbescheinigung mit Angabe der Art und des Umfanges (Voll-/Teilzeit in %) der Beschäftigung sind vorzulegen.

2.6.1.1 Bildungsabschluss

Anforderung

Der Antragsteller 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 Antragsteller 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 Antragsteller 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 unterschriebene Bestätigung eines Dritten (z.B. Arbeitgeber bzw. Auftraggeber) über die Berufserfahrung sind vorzulegen.

2.6.1.2 Berufserfahrung

Anforderung

Der Antragsteller 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.

Nachweis

Ein Zeugnis oder eine unterschriebene Bestätigung eines unabhängigen Dritten (z.B. Arbeitgeber bzw. Auftraggeber) über die Berufserfahrung im Bereich IT sowie im Bereich Informationssicherheit und die Zulassung sowie Beschäftigung als Auditor sind vorzulegen.

Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung.

2.6.1.3 Praxiserfahrung

Anforderung

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

Nachweis

Gefordert sind vom Auftraggeber oder Arbeitgeber bestätigte und unterschriebene Kurzberichte über die Durchführung der Audits bzw. bei Zertifizierungsaudits die Vorlage der erlangten Zertifikate mit einer Bestätigung des zertifizierten Unternehmens, dass der Antragsteller der verantwortliche Auditor bzw. Auditteamleiter gewesen 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 Antragstellers,
- der Zeitraum und Umfang (Personentage) des Audits.[1]

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

2.6.1.4 Tabellarische Zusammenfassung der Zulassungsvoraussetzungen

Art	***Anforderung***	***Nachweis***
Bildungsabschluss	• Lebenslauf mit Ausbildungs-und Arbeitshistorie • 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

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

Art	***Anforderung***	***Nachweis***
Berufserfahrung	• aus den letzten 5 Jahren mindestens 3 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 Beschäftigung als Auditor
Praxiserfahrung/ Auditerfahrung	• in den letzten 3 Jahren ein ISO 27001-Zertifizierungsaudit als Auditteamleiter oder • in den letzten 3 Jahren ein Zertifizierungsaudit nach BSI TR-03138 als verantwortlicher Auditor	• vom Auftraggeber/Arbeitgeber bestätigte Kurzberichte oder erlangte Zertifikate

2.6.2 Anforderungen an die Fachkompetenz

2.6.2.1 Basiskenntnisse

Es werden die folgenden grundlegenden 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

2.6.2.2 Erweiterte Fachkenntnisse

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

2.6.3 Qualifizierungsmaßnahme

Das BSI bietet keine Qualifizierungsmaßnahme an.

2.6.4 Bewertung der nachzuweisenden Fachkompetenz durch eine Prüfung

Es werden anhand von Fragen die Kenntnisse des Kandidaten in den geforderten Bereichen beurteilt.

Es wird eine 60-minütige schriftliche Prüfung (Multiple-Choice-Test) durchgeführt.

2.6.5 Aufrechterhaltung der Zertifizierung

2.6.5.1 Anforderungen an die Durchführung der Audits

Alle Audits müssen durch die zertifizierte Person gemäß [ISO 17021-1] bzw. [ISO 19011] durchgeführt werden. Dabei sind insbesondere die jeweiligen Regelungen zur Durchführung der Audits in den jeweiligen Programmen zu berücksichtigen und einzuhalten (z. B. das Auditierungsschema im IT-Grundschutz).

2.6.5.2 Kompetenzüberwachung

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

2.6.5.3 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte Auditor nach Ablauf der Zertifizierungsdauer eine Rezertifizierung an, muss er verschiedene, vom Auftraggeber unterschriebene Tätigkeitsnachweise erbringen und an den Erfahrungsaustauschterminen des BSI (sofern angeboten) 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 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 Antragsteller Tätigkeitsnachweise in ausreichendem Umfang erbracht hat.

Sind die Nachweise für die 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.

Punkteskala zur Rezertifizierung

Tätigkeiten	*Bewertung (P = Punktzahl)*
Audits für eine Zertifizierung nach BSI [TR-03138] durchgeführt	50 P

3 Spezielle Rahmenbedingungen

3.1 Pflichten des zertifizierten Auditors bzw. Auditteamleiters

Der zertifizierte Auditor bzw. Auditteamleiter verpflichtet sich bei seinen Tätigkeiten im Programm 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 und, falls dies nicht gewährleistet werden könnte, auf das Audit zu verzichten.

Bei der Durchführung von Audits stellt der zertifizierte Auditteamleiter bzw. Auditor 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, Audits zu begleiten. Kosten für diese Begleitung entstehen nicht.

3.2 Arbeitstreffen mit den Auditoren bzw. Auditteamleitern

Bei Bedarf können Arbeitstreffen mit den Auditoren bzw. Auditteamleitern angesetzt werden.

3.3 Verfahren bei Mängeln in der Konformitätsprüfung

Die Verfahrensweise bei Mängeln in der Konformitätsprüfung sind dem Kapitel 5.4 des Dokuments [VB-Personen] zu entnehmen.

4 Referenzen und Glossar [Verzeichnisse]

Das Dokument Verzeichnisse als Nachschlagewerk für Interessenten und Beteiligte an Zertifizierungs- und Anerkennungsverfahren [Verzeichnisse] gibt einen Überblick über alle benötigten Anforderungen, Quellen und Hilfsmittel mit einem Glossar- und Abkürzungsverzeichnis.

Die Listen im Bereich der Anforderungen, Quellen und Hilfsmittel sind als Stammliste zu verstehen und decken für sämtliche Anforderungen und Dokumente die Information über aktuelle Quellenhinweise ab.