Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Personenzertifizierung: Programm IT-Grundschutz-Berater

IT-Grundschutz-Berater

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	22.05.2019	Personenzertifizierungsstelle Ref SZ 12	Erstausgabe
1.1	27.06.2019	Personenzertifizierungsstelle Ref SZ 12	Revision: • Korrektur der Beschreibungen zu Qualifizierungsmaßnahmen und Übergangsregelungen
1.2	16.12.2020	Personenzertifizierungsstelle Ref SZ 12	Revision: • Übergangsregelung entfernt • Änderung in Kapitel 3.2 „Bewertung der Fachkompetenz“: Multiple-Choice-Test ist 90 Minuten lang
1.2.1	13.04.2022	Personenzertifizierungsstelle Ref SZ 12	Revision: • Fehlerhaften Absatz unter Kapitel 2.1.3 gelöscht • Abbildung 1 aktualisiert
2.0	01.11.2024	Personenzertifizierungsstelle S21	Revision: • Umstrukturierung des Dokumentes • Entfernen der Abbildung 1: Dokumentenübersicht (Zertifizierungs- und Anerkennungsprogramm) in Kapitel 1.1 und entsprechende Anpassung im Kapitel • Überarbeitung der Literaturangaben und der Zitate der Rechtsnormen • Redaktionelle und strukturelle Anpassungen • Abschnitt 2.1.2.3 Anforderung geändert: „aus“ den letzten 3 Jahren... • Tabellarische Zusammenfassung der Zulassungsvoraussetzungen eingefügt

Tabelle 1: Änderungshistorie

Inhalt

1 Einleitung

Das vorliegende Dokument beschreibt die Zertifizierung von Personen im Programm IT-Grundschutz-Berater.

1.1 Zielsetzung und Eingliederung des Programms IT-GS-Berater

Dieses Dokument beinhaltet detaillierte Hinweise als Ergänzung zum übergeordneten Dokument „Verfahrensbeschreibung zur Zertifizierung von Personen“ [VB-Personen] für die Situation, in der sich der Antragsteller entschieden hat, sich als IT-GS-Berater zertifizieren zu lassen.

Es werden konkret die Anforderungen und Aufgaben benannt, die ein Antragsteller berücksichtigen muss, um den Regelungen und Anforderungen zum Verfahren gerecht zu werden. An den entsprechenden Stellen im Dokument wird z.B. auf Formulare oder andere Hilfsmittel hingewiesen, die besonders bei einer erstmaligen Zertifizierung 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 IT-GS-Berater

Institutionen, die IT-Grundschutz umsetzen und sich unabhängig von einer Zertifizierung beraten lassen möchten, benötigen qualifizierte IT-Grundschutz-Berater.

Aufgabe des IT-Grundschutz-Beraters ist es, bei der Einführung eines Informationssicherheitsmanagementsystems (ISMS) mitzuwirken, Konzepte zu erstellen und die Institutionen bei der Einführung von Prozessen fachkundig zu unterstützen. Hierbei kann der IT-Grundschutz-Berater seine Erfahrungen bei der Erstellung von benutzerdefinierten Bausteinen oder Profilen zielgerichtet einbringen. Auch die Vorbereitung auf ein Audit kann zu seinen Aufgaben gehören.

2.1 Anforderungen an den IT-GS-Berater

2.1.1 Die persönlichen Eigenschaften eines IT-GS-Beraters

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

2.1.1.1 Managementfähigkeiten

- Überzeugungsfähigkeit
- Flexibilität
- Durchsetzungskraft
- Lösungsorientierung
- Zielorientiertes Denken und Handeln
- Organisatorische Fähigkeiten

2.1.1.2 Kommunikationsfähigkeiten

- Überzeugungsfähigkeit
- Kundenorientierung
- Beherrschung von Moderationstechniken
- Konfliktmanagement

2.1.1.3 Didaktische Fähigkeiten

- Verständliche und nachvollziehbare Erklärung von Sachverhalten
- Objektive Ergebnispräsentation
- Anschauliche Ergebnispräsentation

2.1.1.4 Methodenkompetenz

- Analyse- und Bewertungsmethoden
- Motivationsfähigkeit
- Methoden zur Priorisierung
- Entwicklung von Lösungsstrategien

2.1.1.5 Soziale Kompetenz

- Selbstvertrauen in die eigenen Empfehlungen
- Aufgeschlossenheit und Freundlichkeit
- Schnelle Auffassungsgabe und gesundes Urteilsvermögen
- Analytische Fähigkeiten
- Einfühlungsvermögen/ Empathie
- Kontaktfähigkeit
- Glaubwürdigkeit
- Teamfähigkeit
- Sachlichkeit insbesondere bei heiklen Sachverhalten
- Selbstbewusstsein
- Verschwiegenheit

2.1.2 Zulassungsvoraussetzungen für die Zertifizierung

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

2.1.2.1 Bildungsabschluss

Anforderung

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

Nachweis

Ein Lebenslauf (mit Ausbildungs-und Arbeitshistorie) sowie ein Zeugnis des Ausbildungsabschlusses und ggf. Bescheinigungen der Teilnahme an Fortbildungen bzw. ein Zeugnis/eine Bestätigung eines Dritten (z.B. Arbeitgeber) über die Berufserfahrung muss nachgewiesen werden.

Sollte der Antragsteller 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 Antragsteller die Anforderungen an die 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 acht Jahre im Bereich IT, davon mindestens fünf Jahre im Bereich Informationssicherheit, erworben worden sind.

2.1.2.2 Berufserfahrung

Anforderung

Der Antragsteller muss aus den letzten acht Jahren mindestens fünf Jahre fachspezifische, praktische Berufserfahrung gerechnet auf Vollzeit im Bereich IT, davon mindestens zwei Jahre im Bereich

Informationssicherheit nachweisen. Hierbei finden alle Zeiten Berücksichtigung, die nach Abschluss der entsprechenden Ausbildung (siehe Bildungsabschluss) erbracht wurden.

Des Weiteren muss der Antragsteller umfangreiche (mindestens fünf Jahre) Erfahrung bei der Umsetzung von IT-Grundschutzanforderungen besitzen.

Nachweis

Es muss ein Zeugnis oder eine Bestätigung eines unabhängigen Dritten (z.B. Arbeitgeber oder Auftraggeber) über die Berufserfahrung im Bereich IT und der Umsetzung von IT-Grundschutzanforderungen nachgewiesen werden. Aus dem Zeugnis/der Bestätigung müssen die konkreten Erfahrungen (Art und Umfang) hervorgehen. Dies erfolgt in der Regel durch eine kurze Tätigkeitsbeschreibung.

Hierbei finden nur Zeiten Berücksichtigung, die nach Erlangung der Voraussetzungen im Bereich „Bildungsabschluss“ erbracht wurden.

2.1.2.3 Praxiserfahrung

Anforderung

Der Antragsteller muss aus den zurückliegenden drei Jahren (Stichtag: Antragsdatum) an Beratungsprojekten mit dem Ziel der vollständigen Einführung eines ISMS gemäß BSI-Standard 200-2 [BSI200] oder der Erstellung von IT-Sicherheitskonzepten, Notfallkonzepten oder Risikodokumentation nach IT-Grundschutz als Berater oder Experte mit einem Gesamtumfang von mindestens 40 Personentagen leitend teilgenommen haben. Bei den Projekten muss die Umsetzung des IT-Grundschutzes wesentlicher Bestandteil gewesen sein.

Nachweis

Vom Auftraggeber oder Arbeitgeber bestätigte Kurzberichte über die Durchführung der Beratungstätigkeiten sind vorzulegen.

Anzugeben sind hierbei:

- die wesentlichen Ziele z.B. Auditvorbereitung, Einführung eines ISMS, Erstellung eines benutzerdefinierten Bausteines sowie der Gegenstand der Beratungsaufgabe
- Grundlagen der Beratungstätigkeit (z.B. BSI-Standard 200-1, 200-2, 200-3 oder 100-4)
- die Rollenverteilung im Projekt, insbesondere die Position/Verantwortung des Antragstellers
- der Zeitraum und Umfang (Personentage) des Projektes

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

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

2.1.2.4 Qualifikation als IT-GS-Berater

Anforderung

Der Antragsteller muss

- Basisschulung oder Selbststudium durchgeführt,
- die Prüfung zum IT-Grundschutz-Praktiker bestanden und
- an der Aufbauschulung zum IT-Grundschutz-Berater teilgenommen haben.

Nachweis

Ein Nachweis über die erfolgreiche Teilnahme (z.B. Abschlusstest) am Besuch einer mindestens dreitägigen IT-Grundschutz-Basisschulung (zum IT-Grundschutz-Praktiker) und der Besuch einer mindestens zweitägigen IT-Grundschutz-Aufbauschulung für IT-Grundschutz-Berater bei einem qualifizierten Schulungsanbieter muss vorgelegt werden.

Eine Liste möglicher Schulungsgebote findet sich unter
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/Personenzertifizierung-IT-Grundschutzberater/Schulungen-zum-IT-Grundschutz-Praktiker-und-IT-Grundschutzberater/schulungen-zum-it-grundschutz-praktiker-und-it-grundschutzberater.html

2.1.2.5 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 • mindestens 5 Jahre Erfahrung bei der Umsetzung von IT-Grundschutzanforderungen	• Zeugnis/Bestätigung eines Dritten über die Berufserfahrung mit Übersicht über die durchgeführten Tätigkeiten
Praxiserfahrung	aus den letzten 3 Jahren Beratungsprojekte mit dem Ziel • vollständige Einführung eines ISMS gemäß BSI Standard 200-2 oder • Erstellung IT-Sicherheitskonzepten, Notfallkonzepten oder Risikodokumentation nach IT-Grundschutz als Berater oder Experte leitend • mit einem Gesamtumfang von mindestens 40 Personentagen • Umsetzung IT-Grundschutz als wesentlicher Bestandteil	• vom Auftraggeber/ Arbeitgeber bestätigte Kurzberichte
Qualifikation	• Basisschulung oder Selbststudium • mind. 3-tägige Schulung zum IT-Grundschutz-Praktiker mit bestandener Abschlussprüfung • mind. 2-tägige Aufbauschulung zum IT-Grundschutz-Berater	• Teilnahmebescheinigungen • Prüfungszeugnisse • erlangte Zertifikate

2.1.3 Anforderungen an die Fachkompetenz

2.1.3.1 Basiskenntnisse

Als IT-GS-Berater werden folgende grundlegende Kenntnisse vorausgesetzt:

- Einführung und Grundlagen der IT-Sicherheit und rechtlicher Rahmenbedingungen
- Normen und Standards der IT- und Informationssicherheit
- ISO- und BSI-Ansätze zum Informationssicherheitsmanagement im Überblick
- Relevante ISO-Standards, wie der ISO 27000ff.-Normenreihe (insbesondere der Managementrahmen der ISO/IEC 27001)
- Grundlagen des Anforderungs- und Risikomanagements
- Einführung in IT-Grundschutz (IT-Grundschutz-Kompendium, BSI-Standards, etc.) [IT-Grundschutz] (insbesondere die BSI-Standardreihe 200-1 bis 200-3 und 100-4)
- Umsetzung der IT-Grundschutz-Vorgehensweise
- IT-Grundschutz-Check
- Umsetzungsplanung
- Aufrechterhaltung und kontinuierliche Verbesserung
- Notfallmanagement
- Beratungserfahrung (insbesondere im Bereich IT-Grundschutz).

2.1.3.2 Erweiterte Fachkenntnisse

Als IT-GS-Berater sind folgende Fachkenntnisse aus den folgenden Themenfeldern in einer Prüfung gegenüber dem BSI nachzuweisen:

- Einführung und Grundlagen der IT-Sicherheit und rechtlicher Rahmenbedingungen
- Normen und Standards der Informationssicherheit
  - Weitere system- und produktbezogene Informationssicherheitsstandards
  - Geschichte und Struktur der Normenreihe ISO 27000ff. [ISO 27001]
  - die Maßnahmenkataloge der ISO/IEC 27001 und ISO/IEC 27002
- Einführung IT-Grundschutz
- IT-Grundschutz-Vorgehensweise (Überblick)
- IT-Grundschutz-Kompendium [IT-GS]
  - Aufbau und Inhalt des IT-Grundschutz-Kompendiums [IT-GS]
  - Anwendung und Umsetzung des IT-Grundschutz-Kompendiums inkl. Erstellung benutzerdefinierter Bausteine
- Umsetzung der IT-Grundschutz-Vorgehensweise
- IT-Grundschutz-Check
- Risikoanalyse
  - Kenntnisse der Risikoanalyse auf der Basis von IT-Grundschutz / BSI-Standard 200-3 [BSI200]
  - Durchführung und Auswertung von Risikoanalysen

- Umsetzungsplanung
- Aufrechterhaltung und kontinuierliche Verbesserung
- Erwerb des IT-Grundschutz-Zertifikats auf der Basis von ISO 27001
- Einsatz von IT-Grundschutz-Profilen
- Durchführung der Vorbereitung auf ein Audit
- Einführung eines Notfallmanagementsystems
- Kenntnis aktueller Informationen zum IT-Grundschutz (siehe auch [Curriculum])

2.2 Bewertung der Fachkompetenz

Die Bewertung der Fachkompetenz erfolgt durch einen Multiple-Choice-Test.

Bei Nichtbestehen kann die Wiederholung der Prüfung innerhalb der nächsten sechs Monate erneut als separate Einzelprüfung erfolgen. Eine zweite Wiederholung ist nicht möglich.

3 Aufrechterhaltung der Zertifizierung

3.1 Anforderungen an die Tätigkeiten des IT-GS-Beraters

Der IT-Grundschutz-Berater ist der Vertraulichkeit der ihm bei seinen Tätigkeiten zur Kenntnis gelangten Informationen verpflichtet. Ist der IT-Grundschutz-Berater auch als Auditteamleiter zertifiziert, darf dieser nicht das Audit für die Institution durchführen, die er zuvor entsprechend beraten hat.

Der IT-Grundschutz-Berater wirkt bei der Einführung eines ISMS mit. Er hat die entsprechenden Konzepte zu erstellen und stellt Hilfeleistungen zur Umsetzung von Anforderungen und Durchführung von Maßnahmen, die der Informationssicherheit dienen. Hierbei hat der IT-Grundschutz-Berater seine für die Zertifizierung erforderlichen Erfahrungen entsprechend einzubringen.

Der IT-Grundschutz-Berater hat sich an dem Stand der Technik zu orientieren.

Soll die Beratung der Vorbereitung auf ein Audit dienen, hat der IT-Grundschutz-Berater die erforderlichen Anforderungen an eine Zertifizierung zu kennen und der zu beratenden Institution mitzuteilen und bei der Umsetzung zu unterstützen.

3.2 Kompetenzüberwachung

Das BSI kann stichprobenartig die Tätigkeit des Beraters überwachen, um die Eignung des zertifizierten IT-Grundschutz-Beraters für zukünftige Beratungen festzustellen und eventuell notwendigen Schulungsbedarf zu erkennen.

3.3 Anforderungen zur Rezertifizierung

Strebt der bereits zertifizierte IT-Grundschutz-Berater nach Ablauf der Zertifikatsdauer eine Rezertifizierung an, muss er verschiedene, vom Auftraggeber unterschriebene Tätigkeitsnachweise erbringen und an den Terminen des BSI zum Erfahrungsaustausch teilgenommen haben. Um eine nahtlose Rezertifizierung zu gewährleisten, muss der Antrag rechtzeitig gestellt werden.

Zusammen mit dem Antrag auf Rezertifizierung müssen aktuelle Tätigkeitsnachweise (siehe auch Kapitel 3.1.3 „Nachweis Praxiserfahrung“) beim BSI eingereicht werden.

Die Nachweise müssen aus dem aktuellen 3-jährigen Zertifizierungszeitraum stammen, um anerkannt zu werden.

Der Antragsteller muss nachweisen, federführend an Beratungsprojekten im Umfang von 40 Personentagen teilgenommen zu haben, mit dem Ziel

- der vollständigen Einführung eines ISMS gemäß BSI-Standard 200-2 [BSI200] oder
- der Erstellung von IT-Sicherheitskonzepten, Notfallkonzepten oder Risikoanalyse-Dokumentation nach IT-Grundschutz.

3.4 Veröffentlichung der Zertifizierung

Das BSI veröffentlicht im Internet und in der Publikation <kes> – Die Zeitschrift für Informations-Sicherheit1<KES> die Zertifizierung eines IT-Grundschutz-Beraters unter Angabe der Zertifizierungsnummer, des Namens des IT-Grundschutz-Beraters, der Anschrift sowie des Gültigkeitszeitraums des BSI-Zertifikats, entsprechend § 7 BSIZertV.

Die Datenverarbeitung erfolgt auf Grundlage von Art. 6 Abs. 1 lit. e) i.V.m. § 3 Abs. 1 S. 2 Nr. 4 und 5 BSIG. Bei Antragstellung wird der Antragsteller über die Datenverarbeitung entsprechend der Art. 13, 14 DSGVO informiert.

Eine Weitergabe der Daten an Dritte erfolgt nur nach vorheriger Einwilligung durch den Antragsteller.

4 Spezielle Rahmenbedingungen

Pflichten des IT-GS-Beraters

Der IT-GS-Berater stellt sicher, dass er

- alle Tätigkeiten objektiv und unabhängig sowie entsprechend den geltenden Vorgaben (Richtlinien und Verfahrensbeschreibungen) durchführt,
- die Vorgaben des BSI sowie die in den betreffenden festgelegten Vorgehensweisen beachtet und einhält,
- eventuelle Auflagen erfüllt und Abweichungen umgehend behebt,
- bei signifikanten Änderungen, die sich auf das Programm oder die Arbeitsweise auswirken, die Personenzertifizierungsstelle unverzüglich unterrichtet sowie
- bei der Durchführung von Beratungen jederzeit umfassend Auskunft über Ablauf und Inhalt der Beratung geben kann.

5 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.