

99109029001000

Zertifizierung von Personen

Erteilung

Heruntergeladen am 03.07.2025

<https://fimpportal.de/xzufi-services/102789963/B100019>

Modul	Sachverhalt
Leistungsschlüssel	99109029001000
Leistungsbezeichnung I	Zertifizierung von Personen Erteilung
Leistungsbezeichnung II	IT security: Apply for certification of persons
Typisierung	1 - Bund: Regelung und Vollzug
Quellredaktion	Bund
Freigabestatus Katalog	fachlich freigegeben (gold)
Freigabestatus Bibliothek	unbestimmter Freigabestatus
Begriffe im Kontext	
Leistungstyp	Leistungsobjekt mit Verrichtung
Leistungsgruppierung	
Verrichtungskennung	Erteilung (1)
SDG-Informationsbereich	Erlangung von Lizenzen, Genehmigungen oder Zulassungen im Hinblick auf die Gründung und Führung eines Unternehmens
Lagen Portalverbund	Befähigungs- und Sachkundenachweise (2010200), Erlaubnisse und Genehmigungen (2010400)

Modul	Sachverhalt
Einheitlicher Ansprechpartner	Nein
Fachlich freigegeben am	26.05.2021
Fachlich freigegeben durch	Federal Ministry of the Interior, for Construction and Home Affairs (BMI)
Handlungsgrundlage	https://www.gesetze-im-internet.de/bsig_2009/_9.html https://www.gesetze-im-internet.de/bmibgebv/ https://www.gesetze-im-internet.de/bsizertv_2014/BJNR223100014.html https://www.gesetze-im-internet.de/agebv/BJNR013000015.html
Teaser	If you would like to qualify in the field of IT security and prove your expertise, you can apply for certification under certain conditions.
Volltext	<p>As the central certification body for IT security in Germany, the Federal Office for Information Security (BSI) currently offers you 9 certifications that prove your expertise around the BSI Technical Guidelines. The certifications are generally aimed at employees of IT security service providers.</p> <ul style="list-style-type: none"> • Audit team leader for ISO 27001 audits based on IT-Grundschutz As the holder of this certificate, you audit the technical and organizational measures of public authorities or companies. You create audit reports that form the basis for the certification of authorities or companies by the BSI. Certification as an audit team leader is aimed at employees of accredited bodies. • Auditor De-Mail Messages and documents are sent electronically via De-Mail reliably and protected against changes. With your status as a certified person, you check, among other things, whether De-Mail service providers are complying with the security requirements. You must already be certified as an audit team leader to receive certification for De-Mail audits. • Information Security Auditor (IS Auditor) You will assist organizations in creating and implementing security policies and conducting IS audits.

Modul

Sachverhalt

- Auditor Secure CA Operation: Among other things, they audit security measures for managing and issuing digital certificates (Certification Authority - CA). These are a central basis for secure electronic exchange of encrypted documents.
- Auditor Smart Meter Gateway Administration They audit the operation and administration of intelligent information networks in energy supply and work on a central component of the energy transition.
- Auditor Secure E-Mail Transport Among other things, they check how e-mail service providers have implemented the corresponding BSI Technical Guideline.
- Auditor RESISCAN With replacement scanning (RESISCAN), the judiciary, public authorities or business digitise documents such as files. The aim is that these no longer have to be kept on paper. Among other things, they check scanning processes and prepare reports on compliance with the BSI Technical Guideline.
- IS penetration tester IS penetration tests examine paths and interfaces through which hacking attacks into IT systems could occur. As the holder of this certificate, you identify configuration errors as well as vulnerabilities that have not yet been remedied.
- IT basic protection consultant You advise and support companies or public authorities in securing information and setting up an information security management system (ISMS). Tasks within the scope of IT-Grundschutz are, for example, security concepts or the introduction of processes.

You must submit your application for certification online or in writing to the BSI.

Erforderliche Unterlagen

When applying must achieve:

- Audit team leader: Certificate of your training qualification in the field of IT or information security or. Certificate of your training qualification and certificates of participation in further training courses or Testimonial or confirmation from a third party (for example your employer) about your professional experience The certificate or confirmation must show the type and scope of the activities you have

Modul

Sachverhalt

performed (for example, by means of a brief description of your activities) Certificates obtained from your certification audits or Brief reports confirmed by the client or employer on your practical experience The summary reports must show: the essential objectives as well as the subject of the audit, the audit procedure (document review, on-site review, audit report), the distribution of roles in the audit, in particular your position/responsibilities, the period and scope (person days) of the audit. Confirmation of your employment as an auditor Proof of DAkkS accreditation of your employer or the commissioning certification body (e.g. copy of the accreditation certificate) Certificates of attendance, examination certificates or obtained certificates IT basic protection training and auditor training for ISO 27001

- Auditor De-Mail: Documents as for certification as an audit team leader additionally: valid audit team leader certificate

- IS Auditor: Certificate of your training qualification and certificates of attendance of further training courses or Certificate of your training qualification in the field of IT or information security or A certificate or signed confirmation from a third party (e.g. your employer) about your professional and auditing experience. Your certificates or evidence must show the nature and scope of the activities you have performed (e.g. by means of a brief description of your activities). Brief reports confirmed by the client or employer on your audit experience The summary reports must show: the main objectives and subject matter of your audits the audit procedure the distribution of roles in the audit your position/responsibility in the audit the period and scope (person days) of the audit if available: valid audit team management certificate
- Auditor Secure CA Operation: Certificate of your training qualification in the field of IT or information security or Certificate of your training qualification and certificates of attendance of further training courses or A certificate or signed confirmation from a third party (e.g. your employer) about your professional experience in the field of IT and information security. The type and scope of your activities must be evident

Modul

Sachverhalt

from the certificate or confirmation (e.g. by means of a brief description of your activities). Proof of the DAkkS accreditation of your employer or the commissioning certification body (e.g. copy of the accreditation certificate). Proof of your accreditation as an auditor or valid audit team management certificate

- Auditor Smart Meter Gateway Administration:

Certificate of your training qualification in the field of IT or information security or Certificate of your training qualification and certificates of attendance of further training courses or A certificate or signed confirmation from a third party (e.g. your employer) about your professional experience. The certificate or confirmation must show the type and scope of the activities you have performed (e.g. by means of a brief description of the activities). Certificates obtained from your certification audits or brief reports confirmed by the client or employer on your practical experience The summary reports must show: the essential objectives as well as the subject of the audit, the audit procedure (document review, on-site review, audit report), the distribution of roles in the audit, in particular your position/responsibilities, the period and scope (person days) of the audit. Confirmation of your employment as an auditor Proof of DAkkS accreditation of your employer or the commissioning certification body (e.g. copy of the accreditation certificate) Certificates of attendance, examination certificates or obtained certificates IT basic protection training and auditor training for ISO 27001

- Auditor Secure Email Transport: Certificate of your training qualification in the field of IT or information security or Certificate of your training qualification and certificates of participation in further training courses Certificate or confirmation from a third party (e.g. your employer) about your professional experience with an overview of the activities performed Proof of your accreditation as an auditor

- Auditor RESISCAN: Certificate of your training qualification in the field of IT or information security or Certificate of your training qualification and certificates of attendance of further training courses Testimonial or confirmation from a third party (e.g. your employer) about your work experience The certificate or confirmation must indicate the type and scope of the

Modul

Sachverhalt

activities you have performed (e.g. by means of a brief description of the activities). Certificates obtained and short reports confirmed by the client or employer

Proof of the DAkkS accreditation of your employer or the commissioning certification body (e.g. copy of the accreditation certificate) Proof of your accreditation as an auditor or valid audit team management certificate

- Penetration tester: Certificate or confirmation from a third party (e.g. your employer) and/or further evidence of your professional, practical and project experience as well as your special knowledge in the field of penetration testing (e.g. training certificates) the supporting documents must show Type and scope of your specific experience (for example, a brief description of your activities) Evidence of certification from your employer: BSI certificate of the IT security service provider (copy) or Copy of the application for certification as an IT security service provider
- Basic IT protection consultant: Curriculum vitae (education, work and project history) Certificate of the last educational qualification Certificate or confirmation from a third party (e.g. your employer) about your professional experience in the field of IT, in the area of information security and the implementation of IT baseline protection requirements Brief reports confirmed by the principal or employer on your practical experience. The documents must show the main objectives of your consulting activities the basics of your consulting activities (e.g. the respective BSI standards) the distribution of roles in the project, in particular your position and responsibilities the period and scope (person days) of the project Proof that you have passed the examination as an IT-Grundschutz practitioner (e.g. final test) Certificate of participation in the advanced training course to become an IT baseline protection consultant.

Notice: For the current and legally binding details of the evidence to be provided, please refer to the procedure description and programme on the BSI website.

Voraussetzungen

Applications may be submitted by

Modul

Sachverhalt

- natural persons

Further requirements:

- Audit team leader: You have Completed a relevant professional training (for example, studies in the field of IT or information security) and/or comparable in-service training, or at least 8 years of professional experience in the field of IT, of which at least 5 years in the field of information security. You are working as an auditor at an accredited certification body in the field of ISO 27001 and have led at least 1 ISO 27001 certification audit within the last 3 years. You can demonstrate the following practical experience:
Variant 1: You have in the past 3 years Accompanied 4 certification audits in the area of information security with at least 3 person days each as an auditor, trainee or technical expert under the following conditions: At least 1 audit has been conducted consistently in accordance with BSI Standard 200-2 "IT-Grundschatz Procedure". The total scope of your practical or audit experience comprises at least 20 person days. In at least 3 of the audits you were involved in the entire audit. Variant 2: You have in the past 3 years Conducted at least 6 first-party audits or second-party audits in the area of information security with at least 3 person-days each under the following prerequisites: At least 1 audit for which you were responsible was carried out consistently in accordance with BSI Standard 200-2 "Basic IT Security Procedure". The total scope of your practical or audit experience comprises at least 20 person days. You have been involved in the entire audit in all audits. You have successfully participated in a 3-day training course on IT-Grundschatz within the last 3 years. You have successfully completed at least 5 days of auditor training for ISO 27001. You have passed the written examination for audit team management (90-minute test).
- Auditor De-Mail: You are already certified as an audit team leader. You have carried out at least 3 complete certification audits in the area of ISO 27001 on the basis of IT-Grundschatz in the past 3 years.
- IS Auditor: You are already certified as an audit team leader. You have deepened your expertise (one-day BSI

Modul

Sachverhalt

training) and passed a written and oral examination as part of the training.

- Auditor Secure CA Operation: Requirements as for certification as an audit team leader additionally: You have passed a written test of the BSI.
- Auditor Smart Meter Gateway Administration
Prerequisites as for certification as an audit team leader additionally: You have passed a written test of the BSI (60-minute test).
- Auditor Secure e-mail transport: You have completed a relevant professional training (for example, studies in the field of IT or information security) and/or appropriate in-service training. You have at least 4 years of professional experience in the field of IT in the past 8 years, of which at least 2 years in the field of information security. If education or training does not apply to you, you may also demonstrate the following: You have at least 6 years of professional experience in IT, including at least 4 years in information security. You have passed a two-part BSI examination (60-minute multiple-choice test, 120-minute practical test using a test system).
- Auditor RESISCAN: You have completed a relevant vocational training (for example, studies in the field of IT or information security) and/or corresponding in-service training. You have at least 3 years of professional experience in the field of IT in the past 5 years, of which at least 2 years in the field of information security. If education or training does not apply to you, you may also provide evidence of the following: You have at least 5 years of professional experience in the field of IT, of which at least 3 years in the field of information security. You have a licence as an auditor with an accredited certification body in the field of ISO 27001 or You are already certified as an audit team leader. You have conducted at least 1 ISO 27001 certification audit or 1 certification audit in the area of BSI TR03138 within the past 3 years. You have passed a BSI written examination (multiple choice test). If you have already performed certification audits in the area of RESISCAN, BSI may waive the written test.
- Penetration tester: You have specialist, practical work experience in the field of IT or information security. System Administration, network protocols, programming languages, IT security products (for

Modul

Sachverhalt

example firewalls, intrusion detection systems), application systems. You are employed by a BSI-certified IT security service provider in the field of penetration testing. Your practical expertise and personal requirements were tested during a project day at the BSI. For example Your special knowledge, the handling of tools and vulnerability scanners as well as the creative approach to penetration testing.

- Basic IT protection consultant You have already successfully qualified as a basic IT protection practitioner (at least 3 days basic IT protection training followed by an examination at a training provider). You have at least 5 years of specialist, practical work experience in IT within the last 8 years, of which at least 2 years must have been in the field of information security. You have at least 5 years of experience in the implementation of IT-Grundschutz requirements. You have worked in a leading role on consulting projects in the past 3 years. In doing so the implementation of IT-Grundschutz was an essential part and the total scope of the applicant's services amounted to at least 40 person days. The goals of your consulting projects were the complete implementation of an information security management system (ISMS) according to BSI standard 200-2 or the creation of IT security concepts, emergency concepts or risk documentation according to IT-Grundschutz. You have participated in an advanced training course to become an IT-Grundschutz consultant at a training provider. You have passed the examination for basic IT protection consultant at the BSI.

Kosten

- The certifications are charged according to time and effort. For exact details, please refer to the Fee Ordinance.

Verfahrensablauf

You can submit the application for certification of a person as well as recertification in the online procedure or in writing to the Federal Office for Information Security (BSI).

Online procedure

- Call up the online application wizard.
- The online application wizard will guide you step by

Modul

Sachverhalt

step through the application and the respective information and documents for your desired certification.

- Upload the necessary documents (e.g. certificates or external certificates) as a file (PDF, maximum 5 megabytes per document).
- After logging into your citizen account and confirming with the online ID function of your identity card, you can send the application to the BSI.
- The BSI will check whether you meet the admission requirements and whether your certificates of professional competence meet the requirements.
- If there are any questions or doubts, the BSI will contact you. You can then submit supplementary or further evidence.
- If you meet the admission requirements, the BSI will invite you to a workshop and examination as part of the so-called competence assessment, depending on the certification you are aiming for. The appointments usually take place on site at the BSI.
- You will be informed of the results of the examination in a timely manner. If you do not meet the requirements, you can repeat the examination once. If you still do not meet the requirements after repeating the test or if you cancel your participation 3 times without good reason, the procedure will be terminated. If the result of the examination is positive, you will receive a certificate and a fee notice from the BSI.
- Unless you object, the BSI will publish your certification, the period of validity, your name and your professional or private address on its website.
- The 3-year validity period of your certification starts. During this period, please have your services confirmed by your clients via activity certificates.
- For recertification, you then submit proof of activities to the BSI, which are weighted according to a point system.
- Alternatively, you can go through the initial certification process again.
- You will also need to demonstrate to BSI that you are continually developing professionally and taking account of changes in practice, relevant standards and other requirements. BSI may additionally assess your work (for example, by accompanying you on an audit

Modul

Sachverhalt

day).

In writing by post

- Download and print out the application for the certification you are seeking from the BSI in Information Technology website.
- Send the completed and signed application together with the necessary documents (for example, certificates and external proof of expertise as copies) to the BSI.
- The BSI will check whether you meet the admission requirements and whether your certificates of professional competence meet the requirements.
- If there are any questions or doubts, the BSI will contact you. You can then submit additional or further evidence.
- If you meet the admission requirements, the BSI will invite you to a workshop and examination as part of the so-called competence assessment, depending on the certification you are aiming for. The appointments usually take place on site at the BSI.
- You will be informed of the results of the examination in a timely manner. If you do not meet the requirements, you can repeat the examination once. If you still do not meet the requirements after repeating the test or if you cancel your participation 3 times without good reason, the procedure will be terminated. You will then receive a fee notice for the costs incurred up to that point.
- If the result of the examination is positive, you will receive a certificate and a fee notice from the BSI.
- Unless you object, the BSI will publish your certification, the period of validity, your name and your professional or private address on its website.
- The 3-year validity period of your certification starts. During this period, please have your services confirmed by your clients via activity certificates.
- For recertification, you then submit proof of activities to the BSI, which are weighted according to a point system.
- Alternatively, you can go through the initial certification process again.
- You will also need to demonstrate to BSI that you are continually developing professionally and taking

Modul	Sachverhalt
	<p>account of changes in practice, relevant standards and other requirements. The BSI may additionally assess your work (for example, by accompanying you on an audit day).</p> <ul style="list-style-type: none"> • for processing the application: usually about 3 months from application to certificate issuance.
Bearbeitungsdauer	<ul style="list-style-type: none"> • for the processing of the application: usually about 3 months from the submission of the application to the granting of the certificate.
Frist	<ul style="list-style-type: none"> • for the application for personal certification: none • for the application for recertification: received at the earliest 6 months before expiry of the 3-year validity period and at the latest 6 weeks before expiry of your certification complete with supporting documents
weiterführende Informationen	<p>https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Personen/zertifizierung-von-personen_node.html</p> <p>https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/VB-Personen.html#download=1</p>
Hinweise	
Rechtsbehelf	<ul style="list-style-type: none"> • Contradiction
Kurztext	<ul style="list-style-type: none"> • Certification of individuals Granting • Application for various certifications for natural persons • Certifications are aimed at IT security specialists (usually employed by IT security service providers or self-employed) • Certification of persons for the implementation of: audits, IS audits, IS penetration tests as well as consulting on basic IT protection possible • Requirements are different for each certification • Certification is valid for 3 years • Recertification is possible on application, in particular proof of activities must be provided. • The certification procedure is subject to a fee • Information provided by: Federal Office for Information Security (BSI) • Application via: Application must be made online or in writing to the Federal Office for Information Security

Modul	Sachverhalt
	(BSI). • responsible: Federal Office for Information Security (BSI).
Ansprechpunkt	
Zuständige Stelle	
Formulare	Forms: yes Online procedure possible: yes Written form required: yes Personal appearance required: yes https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung_Auditteamleiter.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung-DE-Mail_Auditor.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung_IS-Revisor.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung_Auditor_Secure-CA-Operation.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Antrag_AuditorSmartMeterGateway.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Antrag_Auditor_sicherer_E-Mail_Transport.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung_Auditor_RESISCAN.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung_Penetrationstester.pdf https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/Veroeffentl/Antrag_Zertifizierung_Rezertifizierung-IT-GS-Berater.pdf
Ursprungsportal	Zertifizierung von Personen Erteilung, Zertifizierung von Personen Erteilung