

99118022074000

Nachweis über die Einhaltung des Standes der Technik für Betreiber Kritischer Infrastrukturen Überprüfung

Heruntergeladen am 06.06.2025

<https://fimportal.de/xzufi-services/103061495/B100019>

Modul	Sachverhalt
Leistungsschlüssel	99118022074000
Leistungsbezeichnung I	Nachweis über die Einhaltung des Standes der Technik für Betreiber Kritischer Infrastrukturen Überprüfung
Leistungsbezeichnung II	Critical infrastructures: demonstrating compliance with the state of the art
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	

Modul	Sachverhalt
Verrichtungskennung	Überprüfung (74)
SDG-Informationsbereich	nicht SDG-relevant
Lagen Portalverbund	Prüfung und Nachweise für Sachkunde und Sicherheit (2120300)
Einheitlicher Ansprechpartner	Nein
Fachlich freigegeben am	11.01.2024
Fachlich freigegeben durch	Federal Ministry of the Interior and for Home Affairs (BMI)
Handlungsgrundlage	https://www.gesetze-im-internet.de/bsig_2009/_8a.html
Teaser	If you operate critical infrastructures, you must prove that the security of your information technology corresponds to the state of the art. You must submit proof to the Federal Office for Information Security (BSI) every two years.
Volltext	Critical infrastructures (KRITIS) are organizations and facilities that are important for the state community. If these facilities fail or are impaired, this can lead to supply bottlenecks, significant disruptions to public safety or other dramatic consequences. Regular proof of compliance with the state of the art is therefore required by law. KRITIS includes the following sectors, for example: • Energy, • health, • information technology and telecommunications, • transportation and traffic, • water, • finance and insurance, • nutrition, • municipal waste disposal. As an operator of critical infrastructures, you must ensure that the security of your information

Modul

Sachverhalt

technology systems, components and processes, which are fundamental to their operation, corresponds to the state of the art. You must prove this to the Federal Office for Information Security (BSI) at least every two years.

To protect your information technology against failure and external attacks, you must take organizational and technical measures and precautions. This also includes the use of attack detection systems.

You can have this documented by security audits, tests or certifications from auditing bodies. In the next step, you submit the results of these audits to the BSI using a verification document, including any security deficiencies discovered.

The BSI then checks whether your precautions and measures meet the legal requirements. The BSI can request the submission of further test documents and, in the event of security deficiencies, the rectification of the security deficiencies.

Erforderliche Unterlagen

- Verification document KI: Information on the operator, the tested critical infrastructure and contact person
- Verification document P: Information on the inspection.
 - must be signed by an employee of the verifying body who is authorized to sign.
 - must contain the following information:
 - Section PD: Information on the performance of the test
 - Appendix PD.A: Description and graphic representation of the scope of the inspection
 - Annex PD.B: Information on the test procedure
 - Appendix PD.C: Description of the test basis
 - Section PE: Information on the test result and the safety deficiencies detected
 - Appendix PE.A: List of safety deficiencies including implementation plan
 - Section PS: Information on the suitability of the inspecting body and the inspection team
 - Annex PS.A: Proof or evidence of qualification additional test procedure competence for § 8a BSIG or equivalent proof of competence

Modul	Sachverhalt
Voraussetzungen	• You operate critical infrastructure • You are registered with the BSI • You have a corresponding operator ID/institution ID
Kosten	There are no costs for you for submitting the certificates to the BSI.
Verfahrensablauf	You can submit your evidence via the online service, by encrypted e-mail or by post. If you submit evidence via the online service: • To use the online service, you need an ELSTER organization certificate and ELSTER company account. • Go to the federal portal verwaltung.bund.de and complete the online application. • You can upload your documents directly. • The KRITIS office of the Federal Office for Information Security (BSI) will check your details. • If the KRITIS office has any questions for you during the review or requests additional documents, it will contact you by email. • After the formal check, the KRITIS office will send you a confirmation by e-mail and inform you of the new deadline for your next proof. If you submit evidence by encrypted e-mail: • Download the proof document KI from the BSI website. • Fill out the form. • You can either complete the form digitally • or print it out first and then fill it in. • Sign the form. • Send the form and your verification documents by email to the BSI's KRITIS office. • The KRITIS Office will accept your verification documents by encrypted e-mail. • For encryption, use the S/MIME certificate of the KRITIS office on the BSI website. • The next steps are the same as for the online service.

Modul
Sachverhalt

If you are submitting evidence by post:

- Download the KI verification document from the website of the Federal Office for Information Security.
- You can either fill out the form digitally and print it out,
- or print it out first and then fill it in.
- Sign the form and add the necessary verification documents.
- Send your proof to the BSI's KRITIS office.
- All further steps correspond to the procedure of the online service.

Bearbeitungsdauer

1 - 2 Woche(n)

The processing time is usually around 10 days from receipt of the supporting documents until confirmation is issued - provided that all the necessary documents have been submitted and the information is complete.

Frist

2 Jahr(e)

You must provide proof of compliance with the state of the art to the Federal Office for Information Security (BSI) at least every 2 years. You can also submit your verification documents at any time before the verification deadline. The calculation of the deadlines depends on the time of the previous submission of the documents. If a proof proves to be incomplete in the course of the inspection, so that subsequent deliveries have to be made, this does not affect the deadline for the subsequent proof once it has been calculated. For critical infrastructures that fall under the regulations of the BSI Act for the first time, proof must be provided within 2 years. If you register new systems in addition to already registered systems through the annual inspection, you can combine all systems in one verification, provided that the respective verification deadlines are not exceeded.

weiterführende Informationen

<https://www.bsi.bund.de/nachweise>
<https://www.bsi.bund.de/kritis-downloads>
<https://www.bsi.bund.de/OHNachweise>
<https://www.bsi.bund.de/dok/faq-nachweise-kritis>
<https://www.bsi.bund.de/dok/kritis-faq-iso27001>

Modul	Sachverhalt
	https://www.bsi.bund.de/dok/906288
Hinweise	There are no indications or special features.
Rechtsbehelf	There are no legal remedies.
Kurztext	• Proof of compliance with the state of the art for operators of critical infrastructures Verification • Critical infrastructure operators must continuously take measures and precautions to ensure the security and functionality of their facilities • Critical infrastructure operators must prove every 2 years that they have taken sufficient measures to protect the information technology of their facilities in accordance with the state of the art • Operators can have the state of the art of the systems checked and documented by • an independent audit • as a supplement to another audit • ISO 27001 certification based on IT baseline protection • ISO 27001 certification process (native) • Internal company security audit • Audit • Audit teams prepare and sign the verification document P, which they hand over to the operator • Operators send the verification document together with other documents to the Federal Office for Information Security (BSI) • The verification documents can be sent via • the online service, • an encrypted e-mail or • by post • responsible: Federal Office for Information Security
Ansprechpunkt	
Zuständige Stelle	
Formulare	Forms available: Yes Written form required: Yes Informal application possible: No Personal appearance necessary: No Online services available: Yes

Modul	Sachverhalt
Ursprungsportal	Nachweis über die Einhaltung des Standes der Technik für Betreiber Kritischer Infrastrukturen Überprüfung, Nachweis über die Einhaltung des Standes der Technik für Betreiber Kritischer Infrastrukturen Überprüfung