

Modulbeschreibung „Qualifizierung zum KRITIS-Auditor“

Modultitel	Qualifizierung von Personen zur Prüfkompetenz als KRITIS-Auditor (§ 39 Abs. 2 BSIg)
Kürzel/Modulnummer	KRITIS-AUD
Fachbereich	Informationssicherheit & Compliance
Modulverantwortlicher	Herr Prof. Dr. Matthias Mehrrens
Dozent	Herr Prof. Dr. Matthias Mehrrens, Herr Prof. Dr.-Ing. René Treibert
Modultyp	Zulassungsvoraussetzung für die Personenzertifizierung zum KRITIS-Auditor durch das BSI (§ 39 Abs. 2 BSIg); auch offen für KRITIS-Betreiber, KRITIS-Verantwortliche, Berater und Neueinsteiger ohne Zertifizierungsabsicht
Dauer	3 Tage, mindestens 24 Unterrichtseinheiten (UE) à 60 Minuten
Häufigkeit des Angebotes	mehrmals jährlich, Termine nach Bedarf
Zielgruppe(n)	Auditierende, KRITIS-Betreiber und dortige KRITIS-Verantwortliche, KRITIS-Berater sowie KRITIS-Neueinsteiger. Es bestehen keine formalen Zulassungsvoraussetzungen; Grundkenntnisse in Auditierung, Informationssicherheit und der Regulierung kritischer Anlagen sind von Vorteil. Für die anschließende Personenzertifizierung zum KRITIS-Auditor durch das BSI sind zusätzlich Anforderungen an Berufserfahrung und Ausbildung zu erfüllen.
Angestrebte Lernergebnisse/ Learning outcomes	Diese Schulung basiert auf dem verbindlichen Curriculum des BSI zum Schulungskonzept KRITIS-Auditor (Qualifizierung von Personen zur Prüfkompetenz nach § 39 Abs. 2 BSIg). Sie dient der Vorbereitung auf und ist Zulassungsvoraussetzung für die Personenzertifizierung zum KRITIS-Auditor durch das BSI. Nach Abschluss der Schulung können die Teilnehmenden KRITIS-Prüfungen nach einer einheitlichen Methodik und einem Mindeststandard planen, durchführen und dokumentieren. Der Schulungsleitfaden und die vom BSI bereitgestellten Schulungsfolien konkretisieren die Inhalte und sichern ein einheitliches Vorgehen sowie eine gleichbleibende Qualität der Qualifikation.
Inhalte	• Modul 1: Kritische Infrastrukturen und gesetzliche Grundlagen (2 UE) 1. Definition kritischer Dienstleistungen und kritischer Anlagen (KRITISDachG) 2. Bedeutung von KRITIS für die Versorgungssicherheit in Deutschland 3. Überblick über die KRITIS-Regulierung und relevante Normen (u. a. B3S) 4. Europäischer Kontext: NIS-2-Richtlinie und CER-Richtlinie 5. Anforderungen an Informationssicherheit und Prüfwesen (§§ 30, 31, 38, 39, 61 BSIg; §§ 12, 13, 16, 18 KRITISDachG) 6. Systeme zur Angriffserkennung und Stand der Technik 7. Informations- und Meldewesen nach dem BSIg • Modul 2: Betroffenheit und Rechtsverordnung (2 UE) 1. Betroffenheitsanalyse 2. Grundlagen der Rechtsverordnung (BSI-KritisV) 3. Aufbau des KRITISDachG 4. Durchführung einer KRITIS-Schwellenwertanalyse 5. Informationsquellen für Betreiber und Prüfer • Modul 3: Die Prüfungsvorbereitung (3 UE) 1. Rollen und Verantwortlichkeiten in der KRITIS-Prüfung 2. Prüfgrundlage mit und ohne B3S 3. Einführung in das Phasenmodell einer KRITIS-Prüfung 4. Übungsaufgabe: Gruppendiskussion zum Phasenmodell und zu Risiken bei dessen Missachtung • Modul 4: Die Grundlagenprüfung (4 UE) 1. Validierung der Prüfgrundlage 2. Validierung des Geltungsbereichs 3. Validierung des KRITIS-Risikomanagements 4. Idealisertes Beispiel einer Asset-basierten Risikoanalyse 5. Erstellung eines Prüfplans 6. Übungsaufgabe: Validierung eines beispielhaften Geltungsbereichs 7. Übungsaufgabe: Evaluierung und Validierung einer beispielhaften Risikoanalyse • Modul 5: Angemessenheits- und Wirksamkeitsprüfung (7 UE)

	1. Vertiefung des Phasenmodells (Phase 2 und 3) 2. Mehrjahresplanung der KRITIS-Prüfung 3. Auswahl von Grundgesamtheiten und Stichproben 4. Herleitung der mindestens abzudeckenden Themenfelder 5. Beispielhafte Prüfhandlungen: Sicherheitsorganisation und Asset-Management 6. Beispielhafte Prüfhandlungen: Aufrechterhaltung des Betriebs 7. Beispielhafte Prüfhandlungen: Informationssicherheitsvorfallmanagement 8. Beispielhafte Prüfhandlungen: Angriffserkennung und Protokollierung 9. Beispielhafte Prüfhandlungen: Dienstleistersteuerung, Schulungen und OT 10. Dokumentation in einer KRITIS-Prüfung • Modul 6: Prüfbericht und Nachweise (3 UE) 1. Grundlagen der Nachweiseinreichung nach § 39 BSIG 2. Verwendung von Nachweisen aus anderen Prüfungen (z. B. ISO/IEC 27001, SOC-Berichte) 3. Anforderungen an Mängelliste und Umsetzungsplan 4. Anforderungen an den Prüfbericht 5. Prüfung der Nachweise durch das BSI und mögliche Nachforderungen 6. Übungsaufgabe: Gruppenarbeit zur Bewertung von Prüfbericht-Ausschnitten
Lehrformen	Interaktives Seminar (Verhältnis Theorie zu interaktivem Anteil 40 % zu 60 %) mit Gruppenarbeiten, Diskussionen und Übungsaufgaben; mindestens der interaktive Anteil in Präsenz
Unterrichtssprache	Deutsch
Voraussetzungen zur Weiterbildung	Keine formalen Zulassungsvoraussetzungen. Grundkenntnisse in Auditierung, Informationssicherheit und der Regulierung kritischer Anlagen sind vorteilhaft, um den Inhalten folgen zu können und dem straffen Zeitplan der Schulung nicht unnötig zu unterliegen.
Prüfungsleistung(en)	Eine Prüfungsleistung im Rahmen der Schulung ist nicht vorgesehen. Der Nachweis der Schulung erfolgt durch eine individuelle Teilnahmebescheinigung, die je Modul den geschulten Zeitumfang (Anzahl UE) eindeutig ausweist; eine bloße Bestätigung der Gesamtteilnahme genügt nicht. Werden wesentliche Anteile der Schulung entschuldigt oder unentschuldigt versäumt, darf keine Teilnahmebescheinigung ausgestellt werden. Die eigentliche Personenzertifizierung zum KRITIS-Auditor erfolgt separat durch das BSI und setzt zusätzlich Berufserfahrung und Ausbildung gemäß den BSI-Vorgaben voraus.
Workload / Arbeitsaufwand	mind. 21 h (entspricht 21 UE à 60 Minuten)
Kontaktzeit	21 UE Präsenz (empfohlen verteilt auf 3 Tage à 7 UE)
Selbststudium	optional: Lektüre des Schulungsleitfadens sowie Vor-/Nachbereitung der Übungsaufgaben
Geplante Gruppengröße	max. 12 Personen (empfohlene Teilnehmerzahl gemäß BSI-Curriculum)
Verwendbarkeit des Moduls	Zulassungsvoraussetzung für die Personenzertifizierung zum KRITIS-Auditor durch das BSI; einzelne Module (z. B. Modul 5) können bei homogenem Teilnehmerkreis, etwa ausschließlich KRITIS-Betreibern, angepasst oder ausgelassen werden.
Literatur	Bundesamt für Sicherheit in der Informationstechnik (BSI): Curriculum zum Schulungskonzept KRITIS-Auditor – Qualifizierung von Personen zur Prüfkompentenz nach § 39 Absatz 2 BSIG, Version 1.0, 31.08.2026; Schulungsleitfaden für die Schulung von Personen zur Prüfkompentenz nach § 39 BSIG, Version 1.0, 31.08.2026; BSI-Gesetz (BSIG), insbesondere §§ 30, 31, 38, 39, 61; KRITIS-Dachgesetz (KRITISDachG), insbesondere §§ 12, 13, 16, 18.