

Geprüfter Berufsspezialist für Informationssicherheit
Geprüfte Berufsspezialistin für Informationssicherheit
Rahmenplan mit Lernzielen

Dieses Werk ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechts ist ohne ausdrückliche Zustimmung des Verlages unzulässig; dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Entnahme von Auszügen oder Abbildungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Hinweis

Ist in diesem Rahmenplan von Spezialisten, Teilnehmern und Prüfungsteilnehmern u. Ä. die Rede, sind selbstverständlich auch Spezialistinnen, Teilnehmerinnen und Prüfungsteilnehmerinnen gemeint. Wir gehen davon aus, dass Sie die Verwendung nur einer Geschlechtsform nicht als Benachteiligung empfinden, sondern dass auch Sie zugunsten einer besseren Lesbarkeit diese Formulierungsweise akzeptieren.

Herausgeber

DIHK – Deutsche Industrie- und Handelskammer

Postanschrift: 11052 Berlin | Besucheranschrift: Breite Straße 29 | 10178 Berlin-Mitte | Internet www.dihk.de

Verlag

© DIHK Verlag in der DIHK Service GmbH

Breite Straße 29 | 10178 Berlin

bestellservice@verlag.dihk.de | www.dihk-verlag.de

Stand

Erstauflage November 2024

Druck

dbusiness.de | Eine Marke der MOTIV OFFSET NSK GmbH | Grenzgrabenstraße 4 | 13053 Berlin

Inhaltsverzeichnis

	<u>Seite</u>
Vorwort	III
Taxonomie der Lernziele (Anwendungstaxonomie)	V
Konzeption mit Stundenempfehlung	VII
Lern- und Arbeitsmethodik	1
Informationssicherheit gewährleisten	3
1. Bedrohungs- und Risikoszenarien analysieren	3
2. Sicherheitsmaßnahmen planen	7
3. Sicheren Betrieb gewährleisten	13
4. Sicherheitsmaßnahmen einleiten, dokumentieren und evaluieren	21
5. Organisatorische und rechtliche Vorgaben	25
6. Projektunterstützung und -koordination	31
Anhang	
Verordnung zur Neuordnung der Fortbildungsprüfungen der Geprüften Berufsspezialisten und der Geprüften Berufsspezialistinnen im Bereich der Informations- und Telekommunikationstechnik	37
Abkürzungsverzeichnis	83
Feedbackbogen	85

Vorwort

Die „Verordnung zur Neuordnung der Fortbildungsprüfungen der Geprüften Berufsspezialisten und der Geprüften Berufsspezialistinnen im Bereich der Informations- und Telekommunikationstechnik“ vom 2. Oktober 2024 trat am 1. November 2024 in Kraft. Sie enthält fünf einzelne Artikel mit fünf verschiedenen Fortbildungsprüfungsregelungen zu Geprüften Berufsspezialisten und Geprüften Berufsspezialistinnen im Bereich der Informations- und Telekommunikationstechnik.

Der Artikel 2 regelt die Verordnung über die Prüfung zum anerkannten Fortbildungsabschluss mit der Bezeichnung „Geprüfter Berufsspezialist für Informationssicherheit oder Geprüfte Berufsspezialistin für Informationssicherheit“. Zeitnah zur neuen Fortbildungsprüfungsverordnung liegt nun auch der zugehörige Rahmenplan für diese Berufsspezialisten vor.

Die fortschreitende Digitalisierung und Vernetzung aller Lebens- und Arbeitsbereiche stellt Unternehmen und Organisationen vor neue und zunehmend komplexe Herausforderungen im Bereich der Informationssicherheit. Der Schutz sensibler Daten, die Gewährleistung der IT-Sicherheit sowie die Einhaltung der Datenschutzbestimmungen sind heute nicht nur für große Unternehmen von zentraler Bedeutung, sondern auch für kleine und mittlere Unternehmen, die zunehmend Ziel von Cyberangriffen werden.

In dieser dynamischen und risikobehafteten Umgebung wächst die Nachfrage nach Fachkräften, die in der Lage sind, sowohl eigenständig als auch verantwortlich Maßnahmen zur Gewährleistung der Informationssicherheit zu entwickeln und umzusetzen. Dieser neue Berufsspezialistenabschluss zielt darauf ab, praxisnah und umfassend Kompetenzen zu erwerben, die es ermöglichen, Gefährdungen und Risiken im Bereich der Informationssicherheit zu identifizieren, zu analysieren und passgenaue Schutzmaßnahmen zu implementieren.

Die Absolventinnen und Absolventen dieser neuen Fortbildungsprüfung sollen in der Lage sein, Informationssicherheitsstrategien zu entwickeln, technische und organisatorische Maßnahmen zum Schutz der Datenverfügbarkeit, Vertraulichkeit und Integrität zu implementieren und die relevanten gesetzlichen Anforderungen, insbesondere in Bezug auf den Datenschutz, einzuhalten. Sie sind gefordert, Risiken zu bewerten und Maßnahmen zur Vermeidung, Minimierung oder Bewältigung von Gefahren zu planen und durchzuführen. Dabei sind die kontinuierliche Weiterbildung und der regelmäßige Austausch mit anderen Fachbereichen von zentraler Bedeutung, um den ständig wachsenden und sich wandelnden Bedrohungen in der Informationssicherheit gewachsen zu bleiben.

Der vorliegende Rahmenplan dient als Grundlage für die Qualifizierung von Fachkräften, die einen entscheidenden Beitrag zur Sicherheit und Resilienz der deutschen Wirtschaft leisten. Durch ihre Arbeit tragen die "Geprüften Berufsspezialisten für Informationssicherheit" nicht nur zum Schutz der unternehmerischen Daten bei, sondern stärken auch das Vertrauen von Kunden, Geschäftspartnern und der Öffentlichkeit in die digitale Zukunft.

Der Rahmenplan wurde von Sachverständigen der Unternehmen, der Bildungsträger und der Industrie- und Handelskammern entwickelt. Er folgt der Struktur der Rechtsverordnung und ist in sechs Teile gegliedert. Die Teile mit den Nummern 5 und 6 entsprechen inhaltlich den Teilen der anderen vier neuen Berufsspezialisten im Bereich der Informations- und Telekommunikationstechnik.

Allen, die an diesem Projekt ehrenamtlich mitgearbeitet haben – vielen Dank.
Den Lehrgangs- und Prüfungsteilnehmenden viel Erfolg!

Deutsche Industrie- und Handelskammer

Berlin, November 2024

Taxonomie der Lernziele (Anwendungstaxonomie)

Die Prüfungsanforderungen des Geprüften Berufsspezialisten für Informationssicherheit und der Geprüften Berufsspezialistin für Informationssicherheit sind in der Rechtsverordnung handlungsorientiert formuliert. Sie sind abgeleitet von den Aufgaben, die der Geprüfte Berufsspezialist für Informationssicherheit und die Geprüfte Berufsspezialistin für Informationssicherheit in den verschiedenen Bereichen eines Betriebs wahrzunehmen hat.

Der Rahmenplan ist eine Empfehlung für den Lehrgang, der auf die Prüfung vorbereitet. Er orientiert sich an den Vorgaben der in der Verordnung festgelegten Prüfungsanforderungen. Er beschreibt die Qualifikationsinhalte und deren Bestandteile, die dem Lehrgangsteilnehmenden vermittelt werden sollen, damit er die Anforderungen der Prüfung erfüllen kann.

Die Anwendungstaxonomien beschreiben handlungsorientiert, wie und in welchem Umfang die Bestandteile der Qualifikationsinhalte in die Tätigkeiten des Geprüften Berufsspezialisten für Informationssicherheit und der Geprüften Berufsspezialistin für Informationssicherheit eingehen. Sie sind auf das Ziel hin formuliert, also den Abschluss „Geprüfter Berufsspezialist für Informationssicherheit oder Geprüfte Berufsspezialistin für Informationssicherheit“, und beschreiben nicht den Weg dahin, also den Lehrgang und die Prüfung. Dabei werden – korrespondierend zu herkömmlichen Taxonomien – drei Ebenen unterschieden:

- **WISSEN** beschreibt den Erwerb von Kenntnissen (Daten, Fakten, Sachverhalte), die notwendig sind, um Zusammenhänge zu verstehen.
- **VERSTEHEN** beschreibt das Erkennen und Verinnerlichen von Zusammenhängen, um komplexe Aufgabenstellungen und Problemfälle einer Lösung zuführen zu können.
- **ANWENDEN** beschreibt die aus dem Verstehen der Zusammenhänge resultierende Fähigkeit zu sach- und fachgerechtem Handeln.

Die Zuordnung der Anwendungstaxonomie sieht wie folgt aus:

- **WISSEN:**
kennen, überblicken
- **VERSTEHEN:**
abgleichen, auswerten, erkennen, erläutern, identifizieren, informieren, zusammenstellen
- **ANWENDEN:**
aufbereiten, beachten, beherrschen, berücksichtigen, darstellen, dokumentieren, durchführen, einsetzen, entwickeln, ermitteln, erstellen, festlegen, fördern, mitwirken, planen, prüfen, sicherstellen, überprüfen, überwachen, umsetzen, unterstützen, vorbereiten, vorschlagen,

Konzeption mit Stundenempfehlung

Geprüfter Berufsspezialist für Informationssicherheit/
Geprüfte Berufsspezialistin für Informationssicherheit

Lern- und Arbeitsmethodik	10 UStd.
Informationssicherheit gewährleisten	400 UStd.
1. Bedrohungs- und Risikoszenarien analysieren	90 UStd.
2. Sicherheitsmaßnahmen planen	90 UStd.
3. Sicheren Betrieb gewährleisten	90 UStd.
4. Sicherheitsmaßnahmen einleiten, dokumentieren und evaluieren	40 UStd.
5. Organisatorische und rechtliche Vorgaben	40 UStd.
6. Projektunterstützung und -koordination	50 UStd.
Gesamtstunden	410 UStd.