Leitfaden zum Personenzertifizierungsprogramm

Information Security Personal (TÜV®)

Inhalt

Guideline for the Certification Scheme of Persons

Information Security Personnel (TÜV®)

Content

Herausgeber und Eigentümer:
TÜV NORD CERT GmbH
Zertifizierungsstelle für Personen
Am TÜV 1
45307 Essen
E-Mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 09
Status: freigegeben, BM 19.11.2024
Gültig ab: 19.11.2024

Publisher and owner:
TÜV NORD CERT GmbH
Certification body of persons
Am TÜV 1
45307 Essen
E-Mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 09
Status: freigegeben, BM 19.11.2024
Valid from: 19/11/2024

Leitfaden zum Personenzertifizierungsprogramm
Information Security Personal (TÜV®)

1. Allgemein

Die Informationssicherheit hat zum Ziel die Verarbeitung, Speicherung und Kommunikation von Informationen so zu gestalten, dass die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen und Systeme in ausreichendem Maß sichergestellt werden. Die Herstellung der Informationssicherheit in Unternehmen und Einrichtungen ist Gemeinschaftsaufgabe aller im Betrieb beschäftigten Mitarbeiter. Der Unternehmer bzw. der Leiter einer Organisation trägt jedoch die Verantwortung für die Erfüllung dieser Aufgabe in seinem Bereich. Die vielfältigen und umfangreichen Aufgaben machen es erforderlich, zur Unterstützung der oder des Verantwortlichen innerhalb der Sicherheitsorganisation des Betriebes einen oder mehrere Verantwortliche zu bestellen, dem oder denen diese Aufgaben in wesentlichen Teilen übertragen werden.

Der Information Security Officer (ISO) muss mit den Grundlagen und Normen des Informationssicherheitsmanagements vertraut sein und er muss die Prinzipien, Methoden und Verfahren des Informationssicherheitsmanagements entsprechend den Belangen der Wirtschaft beherrschen. Er muss die Kompetenz besitzen, um beim Aufbau und bei der Aufrechterhaltung eines Informationssicherheitsmanagements Unterstützung zu leisten.

Der Chief Information Security Officer (CISO) muss die Qualifikation des ISO haben und zudem kompetent sein, ein Informationssicherheitsmanagementsystem aufzubauen und anzuwenden. Er kann 1st- und 2nd-Party Audits organisieren und ein Informationssicherheitsmanagementsystem im Rahmen eines Verbesserungsprozesses weiterentwickeln.

Guideline for the Certification Scheme for persons
Information Security Personnel (TÜV®)

1. General information

The purpose of information security is to design the processing, storage and communication of information in a way to ensure the confidentiality, availability and integrity of information and systems to a sufficient extent.

Ensuring information security in companies and institutions is a joint task of all employees working in the company. The entrepreneur or the head of an organization, however, is responsible for the fulfillment of this task in his area.

The many and varied tasks make it necessary to appoint one or more responsible persons to whom these tasks are essentially entrusted, in support of the person responsible within the safety organization of the establishment.

The Information Security Officer must be familiar with the fundamentals and standards of information security management and with the principles, methods and procedures of it in accordance with business concerns. He must have the expertise to assist in building and maintaining information security management.

The Chief Information Security Officer must have the qualification of the Information Security Officer as well as be competent to build and apply an information security management system. He can organize 1st and 2nd party audits and develop an information security management system as part of an improvement process.

2. Anwendungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Zertifikats Information Security Officer (TÜV) bzw. Chief Information Security Officer (TÜV) im Rahmen von anerkannten Lehrgängen. Die Lehrgänge können sowohl als Präsenzschulung, Blended Learning als auch Online anerkannt sein.

2. Scope

This guideline applies to all certification procedures for obtaining the certificate Information Security Officer (TÜV) / Chief Information Security Officer (TÜV) within the scope of recognized training courses. The courses can be recognized as face-to-face training, blended learning or live-online training.

3. Eingangsvoraussetzungen zur Teilnahme an der Prüfung und zur Zertifikatserteilung

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung	Berufserfahrung	fachbezogene Tätigkeit / bestandene Prüfung	Schulung im Zertifizierungsgebiet	praktische Erfahrung oder Auditerfahrung
Information Security Officer (TÜV)	abgeschlossene Berufsausbildung / gleichwertig ersatzweise drei Jahre Berufserfahrung	3 Jahre		fachbezogener Lehrgang mit mind. 32 UE*. und erfolgreichem Abschluss	1 Jahr im Bereich der Informationssicherheit
Chief Information Security Officer (TÜV)	abgeschlossene Berufsausbildung / höherwertig ersatzweise drei Jahre Berufserfahrung	3 Jahre	erfolgreich abgelegte Prüfung zum Information Security Officer	fachbezogener Lehrgang mit mind. 32 UE*. und erfolgreichem Abschluss	1 Jahr im Bereich der Informationssicherheit

Hinweise zur Tabelle:

- 1 UE entspricht einer Unterrichtseinheit von 45 Minuten.
- „Erfolgreicher Abschluss“ bedeutet das Bestehen der zum Lehrgang bzw. zur Zertifizierung gehörenden Abschlussprüfung gemäß diesem Personenqualifizierungsprogramm.

3. Prerequisites for participation in the examination and issuing of the certificate

	training / alternatively work experience for lack of training	Work experience	Specialized activity / successful completion of examination	Training in area of certification	Practical experience or audit experience
Information Security Officer (TÜV)	completed professional training / equivalent alternatively 3 years of work experience	3 years		specialized training with at least 32 TU* and successful completion	1 year in Information Security
Chief Information Security Officer (TÜV)	completed professional training / higher quality alternatively 3 years of work experience	3 years	successful completion of the Information Security Officer examination	successful completion of the Information Security Officer examination / specialized training with at least 32 TU* and successful completion	1 year in Information Security

Notes on the table:

- 1 TU corresponds to a teaching unit of 45 minutes.
- “Successful completion” means passing the final examination associated with the course or certification in accordance with this personal qualification program.

.

4. Prüfungsgegenstand und Prüfungshilfsmittel

Die Präsenzprüfungen nach Präsenzlehrgängen finden in der Regel am letzten Lehrgangstag oder am Tag nach dem letzten Lehrgangstag am Ort des Lehrgangs statt.

Für Online-Prüfungen werden entsprechende separate Termine angeboten.

Aktuelle technische Voraussetzungen finden sich unter folgendem Link:
https://www.tuev-nord.de/de/unternehmen/bildung/personenzertifizierung/pruefungsinformationen-1/

Einige Tage vor der Prüfung bekommen die Kandidatinnen und Kandidaten eine E-Mail mit den Zugangsvoraussetzungen, Links, Installationsanleitungen, der geltenden Prüfungsordnung für Online-Prüfungen und speziellen Informationen zur jeweiligen Prüfung. Darüber hinaus werden mit der Mail die notwendigen Passwörter zur Prüfung mitgeteilt.

Zur schriftlichen/digitalen Prüfung sind keine Unterlagen als Hilfsmittel zugelassen. Bei Bedarf sind Taschenrechner erlaubt, andere elektronische Hilfsmittel sind nicht zulässig.

Zur Bearbeitung der Fallstudie in der praktischen Prüfung Chief Information Security Officer (TÜV) sind als Hilfsmittel Lehrgangsunterlagen, Lehrbücher, die relevanten normativen Dokumente sowie eigene Aufzeichnungen zugelassen.

4. Subject of examination and aids permitted for an exam

The face-to-face examination following face-to-face training usually take place on the last day of the course or on the day after the last day of the course at the location of the course.

Accordingly, individual dates are offered for live-online examinations.

Current technical requirements can be found under the following link:
https://www.tuev-nord.de/de/unternehmen/bildung/personenzertifizierung/pruefungsinformationen-1/

A few days before the examination, candidates receive an e-mail with access requirements, links, installation instructions, the applicable examination regulations for live online exams, and specific information about the respective examination. In addition, the mail includes the necessary passwords for the examination for the candidates.

No documents are permitted as auxiliary means during the written examination. If required, calculators are allowed, other electronic means are not permitted.

For the case study in the practical examination for the Chief Information Security Officer (TÜV) course materials, textbooks, the relevant normative documents, and the candidate's own notes in paper form are permitted as auxiliary means.

5. Prüfungsübersicht

Prüfung Information Security Officer (TÜV)	schriftlich:	praktisch
Dauer:	75 min.	
Anzahl der Prüfungsaufgaben gesamt:	32	
MC-Aufgaben:	30	
Offene Aufgaben:	2	
Höchstpunktzahl:	40	
Mindestpunktzahl:	24 (60 %)	
Prüfung Chief Information Security Officer (TÜV)	**schriftlich:**	**praktisch**
Dauer:	75 min.	4 Wochen
Anzahl der Prüfungsaufgaben gesamt:	32	
MC-Aufgaben:	30	
Offene Aufgaben / Dokumentenprüfung:	2 / 0	
Höchstpunktzahl:	40	50
Mindestpunktzahl:	24 (60 %)	30 (60 %)

Details s. Anlagen

5. Overview of Examination

Examination for Information Security Officer (TÜV)	written	practical
Duration:	75 min.	
Total number of examination questions:	32	
MC questions:	30	
Open questions:	2	
Maximum score:	40	
Minimum score:	24 (60 %)	
Examination for Chief Information Security Officer (TÜV)	**written**	**practical**
Duration:	75 min.	4 weeks
Total number of examination questions:	32	
MC questions:	30	
Open questions	2	
Maximum score	40	50
Minimum score:	24 (60 %)	30 (60 %)

Details see attachment

6. Schriftliche Präsenzprüfung

Die Prüfungsaufgaben werden in einem separaten Aufgabenheft vorgelegt. Die Lösungen zu jeder Prüfungsaufgabe werden auf den Seiten des Einzelberichts eingetragen. Nur die Antworten auf dem Einzelbericht werden gewertet.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Lösungen durch Ankreuzen jede richtige ausgewählt werden. Es sind immer eine, mehrere oder alle richtigen Lösungen zu kennzeichnen. Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Kreuze an den richtigen Stellen der Tabelle gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten.

Bei den offenen Aufgaben formuliert der Kandidat die Antworten in freier, knapper Form und schreibt diese jeweils in das Feld im Einzelbericht. Für jede vollständig und richtig beantwortete Aufgabe gibt es fünf Punkte. Eine teilweise richtige Lösung erhält Teilpunkte im Verhältnis zur richtigen Gesamtlösung. Hierbei ist eine Punktstückelung von halben (½) Punkten möglich.

6. Written face-to-face examination

The examination questions are presented in a separate question booklet. The candidate enters the solutions to each examination question on the pages of the individual report. Only the answers on the individual report will be scored.

The MC questions are formulated in the singular, so it is not possible to infer the number of correct answers. Each correct solution is selected from several given solutions by ticking the appropriate box. One, several or all correct answers must always be marked. One point is awarded for each correctly answered MC question. A question is solved correctly if the crosses are placed in the right places in the table. Questions that are not solved at all or not solved completely receive zero points. There are no fractional points.

As for the open questions, the candidate formulates the answers in a free, concise form and writes them in the respective field in the individual report. Five points are awarded for each question that is answered completely and correctly. A partially correct solution receives partial points in proportion to the correct overall solution. A point division of half (½) points is possible here.

7. Schriftliche Online-Prüfung

Die Prüfungsaufgaben erscheinen einzeln auf dem Bildschirm. Die Lösungen zu jeder Prüfungsaufgabe werden direkt zur Aufgabe eingetragen.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Lösungen durch Anklicken jede richtige markiert werden. Es sind immer eine, mehrere oder alle richtigen Lösungen zu kennzeichnen. Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Markierungen an den richtigen Stellen gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten. Die Aufgaben werden automatisch gewertet.

Bei den offenen Aufgaben formuliert der Kandidat die Antworten in freier, knapper Form und schreibt diese jeweils in das Feld unter der Aufgabenstellung. Für jede vollständig und richtig beantwortete Aufgabe gibt es fünf Punkte. Eine teilweise richtige Lösung erhält Teilpunkte im Verhältnis zur richtigen Gesamtlösung. Hierbei ist eine Punktstückelung von halben (½) Punkten möglich. Die Aufgaben werden im Anschluss an die Prüfung durch einen Prüfer bewertet.

7. Written live-online examination

The examination questions appear individually on the screen. The candidate enters solutions to each examination question directly in the question.

The MC questions are formulated in the singular, so it is not possible to infer the number of correct answers. Each correct solution is selected from several given solutions by ticking the appropriate box. One, several or all correct answers must always be marked. One point is awarded for each correctly answered MC question. A question is solved correctly if the crosses are placed in the right places in the table. Questions that are not solved at all or not solved completely receive zero points. There are no fractional points.

For the open questions, the candidate formulates the answers in a free, concise form and writes them in the respective field below the question. Five points are awarded for each complete and correct answer. A partially correct solution receives partial points in proportion to the correct overall solution. A point division of half (½) points is possible here. The questions are evaluated by an examiner after the examination.

8. Praktische Prüfung

Die praktische Prüfung erfolgt in Form der Erstellung einer Fallstudie. Die Aufgabenstellung für die praktische Prüfung wird direkt im Anschluss der schriftlichen Prüfung ausgegeben. Für die Erstellung der Fallstudie hat der Kandidat vier Wochen Zeit (24 Werktage). Details s. Anlage 2b.

Eine Nachbesserung der Fallstudie ist bei Nichtbestehen mit einer Bearbeitungsfrist von einer Woche (6 Werktagen) Tagen gegen Gebühr möglich.

9. Gesamtbewertung

Die Prüfung Information Security Officer (TÜV) ist bestanden, wenn die schriftliche Prüfung bestanden ist.

Die Prüfung Chief Information Security Officer (TÜV) ist bestanden, wenn die schriftliche und praktische Prüfung bestanden sind.

Es erfolgt keine Mitteilung über Einzelergebnisse oder Punktzahlen.

Maßgeblich für die Bewertung sind bei nachträglichen Korrekturen, die erreichten 60 %, nicht die auf- oder abgerundete Punktzahl.

8. Practical examination

The practical examination takes the form of the preparation of a case study. The assignment for the practical examination is handed out directly after the written examination. The candidate has 4 weeks (24 working days) to work on the case study. See annex 2b for details.

If the case study is not passed, a revision can be made within a period of one week (6 working days) for a fee.

9. Overall evaluation

The examination Information Security Officer (TÜV) is passed when the written examination has been passed.

The examination Chief Information Security Officer (TÜV) is passed when the written and the practical examination have been passed.

There will be no notification of individual or point results.

The 60 % achieved is decisive for the assessment, not the number of points rounded up or down.

10. Zertifizierungsentscheidung und Zertifikatserteilung

Bei bestandener Prüfung wird durch die TÜV NORD CERT ein Zertifikat ausgestellt.

Das Zertifikat enthält folgende Angaben:

a) Personalien der zertifizierten Person (Titel, Vorname, Name, Geburtsdatum)
b) Bezeichnung der Qualifikation
c) Prüfungsinhalte
d) Unterschrift der Fachleitung Personenzertifizierung
e) Ausstellungsdatum
f) Ausbildungsträger

Jedes Zertifikat erhält eine eindeutige Nummer:

44-01-10201105-tt.mm.jjjj-DE02-32157 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
02	Zertifikat
10201105	Kurzkennzeichnung des Zertifizierungsgebietes
tt.mm.jjjj	Tag der Prüfung
DE02	Kennzahl des Prüfungszentrums
32157	Prüfungszentrumsspezifische Kandidatenidentifikationsnummer

Das Zertifikat darf nur in der zur Verfügung gestellten Form verwendet werden. Es darf nicht nur teil- oder auszugsweise benutzt werden. Änderungen des Zertifikats dürfen nicht vorgenommen werden. Das Zertifikat darf nicht irreführend verwendet werden.

10. Certification and issuance of the certificate

The candidate will be issued a certificate by TÜV NORD CERT when the examination is passed.

The certificate contains the following information:

a) Personal information of the candidate (title, first name, last name, date of birth)
b) Designation of the qualification
c) Contents of the examination
d) Signature of the person in charge of personal certification
e) Date of issue
f) Training provider

Each certificate is assigned a unique number:

44-02-10201105-dd.mm.yyyy-DE02-32157 (example)

The number is composed as follows:

44	TÜV NORD CERT GmbH-Personenzertifizierung
02	certificate
10201105	Product number
dd.mm.yyyy	Examination day
DE002	Code of the examination center
32157	Specific examination center candidate identification number

The certificate may only be used in the form issued. It may not be used only in part or in extracts. Changes to the certificate may not be made. The certificate may not be used in a misleading manner.

11. Gültigkeit der Zertifikate

Die Bescheinigung der bestandenen Prüfung ist unbegrenzt gültig.

12. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

11. Validity of certificates of achievement

Certificates of achievement have no limitations of the validity.

12. Applicable documents

General examination regulation (TÜV®)

Fee schedule for examinations (TÜV®)

13. Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Information Security Officer (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Grundlagen der Informationssicherheit (IM) • Informationssicherheit: Begriffe, Spektrum, Abgrenzung Notwendigkeit und strategische Bedeutung von IS Anforderungen an IS IS-Strategie Standards der Informationssicherheit • Aktuelle Themen und Gefährdungslage Gefahrenpotential Bedrohungen und ihre Einschätzung Angriffe, Angriffsziele und -methoden Schwachstellen • Anforderungs- und Risikomanagement Grundbegriffe und Klassifizierung Typische IT-Sicherheitsrisiken Risikoanalyse und -strategien Der Prozess „Risikomanagement“ • Schutzbedarfsfeststellung	**5 UE**	**5 MC**

2. Informationssicherheitsmanagement (IS) • Aufgaben und Rollen in der Sicherheitsorganisation Ebenen der Sicherheitsorganisation Projekt- und Konfliktmanagement • Der Information Security Officer Notwendigkeit des ISO • Stellung und Aufgaben des ISO Anforderungsprofil	**3 UE**	**4 MC**
3. IS-Management nach ISO 27001 (ISO) • Einführung in die ISO 27001 • Aufbau, Inhalt und Methodik • Umsetzungshilfen	**6 UE**	**6 MC**
4. IS-Management nach BSI IT-Grundschutz (GS) Vorgehensweisen nach BSI 200-x Strukturanalyse Schutzbedarfsfeststellung Risikoanalyse nach BSI 200-3 Auswertung der Ergebnisse Schichtenmodell und Bausteine IT-GS-Kompendium • Realisierungsplanung	**6 UE**	**6 MC**
5. Übergreifende Informationssicherheitskonzepte (KON) • Aufbau der ISMS Dokumentation • Basis-Sicherheitskonzepte Datensicherung und Archivierung Schutz vor Schadprogrammen Incident Management User- und Berechtigungsmanagement • Infrastruktursicherheit Zutrittskontrollen, Sicherheitszonen, bauliche Sicherheit, Schutz vor Brand, Wasser, Einbruch etc. Überblick: IT-GS Maßnahmen in der Schicht „Sicherheit der Infrastruktur“	**5 UE**	**5 MC**

6. Kryptographische Verfahren, Sicherheit im Netzwerk, System- und Anwendungssicherheit (IT) • Systemsicherheit Server-Sicherheit Client-Sicherheit Speichersysteme und Speichernetze Virtualisierung • Kryptographische Verfahren Grundlagen der Verschlüsselung Signaturen und Hash-Funktionen Key Management und Zertifikate Public Key Infrastructure (PKI) • Sicherheitsaspekte der TCP/IP-Kommunikation ISO/OSI-Referenzmodell IP-Protokollsuite Sicherheitslecks der IP-Protokolle IP-Netzdienste und Sicherheit Analysemethoden und -tools • Anwendungssicherheit E-Mail	**7 UE**	**4 MC**
Themenübergreifendes Verständnis		**2 o**
6. Abschlussprüfung		**30 MC /2 o**
schriftlich	**75 min.**	

*

UE: Unterrichtseinheit à 45 Minuten
MC: Multiple-Choice-Aufgaben
o: offene Aufgaben

In der Tabelle „Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung“ handelt es sich bei den Angaben der Unterrichtseinheiten um Richtwerte, die in Einzelfällen bedingt durch Zusammensetzung der Teilnehmenden, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.

13. Annex 1: Topics of the course and examination modalities of the written examination Information Security Officer (TÜV®)

Topics and learning content	Number of TU*	Number of questions MC*/o*
1. Basics of information security (IM) • Information security: Terms, spectrum, demarcation Necessity and strategic importance of information security Information security requirements Information security strategy Information security standards • Current topics and danger situation Risk potential Threads and their assessment Attacks, targets and methods of attack Weaknesses • Requirements and risk management Basic concepts and classification Typical IT-Security risks Risk analysis and strategies The process „Risk Management“ • Protection requirements	**5 TU**	**5 MC**

2. Information security management (IS) • Tasks and roles in the security organization Levels of security organization Project- and conflictmanagement • Information Security Officer Need of the ISO Position and tasks of the ISO • Requirements	**3 TU**	**4 MC**
3. ISO 27001 (ISO) • Introduction to ISO 27001 • Structure, content and methodology • Implementation assistance	**6 TU**	**6 MC**
4. BSI IT-Grundschutz (GS) Proceeding to BSI 200-x Structural analysis Protection requirements Risk analysis according to BSI 200-3 Evaluation of results Layer model and building blocks IT-GS-Compendium • Implementation planning	**6 TU**	**6 MC**
5. Information security concepts (KON) • Structure of the ISMS documentation • Basic safety concepts Data backup and archiving Protection against malicious programs Incident Management User- and authorization management • Infrastructure Security Access controls, security zones, structural safety, protection against fire, water, burglary etc. • Overwiew: IT-GS measures in the „Infrastructure Security” layer	**5 TU**	**5 MC**

6. Cryptographic methods, security in the network, system and application security (IT) • System Security Server Security Client Security Storage systems and storage networks Virtualization • Cryptographic methods Basics of encryption Signatures and hash functions Key Management and certificates Public Key Infrastructure (PKI) • Security aspects of TCP / IP communication ISO/OSI reference model IP Protocol Suite Security leaks of the IP protocols IP network services and security Analysis methods and tools • Application Security E-Mail	**7 TU**	**4 MC**
6. Cross-topic understanding		**2 o**
7. Final exam		**30 MC/2 o**
written	**75 min.**	

*

TU: 1 TU corresponds to a teaching unit of 45 minutes.
MC: Multiple Choice questions
o: open question

In the table "Topics of the course and examination modalities of the written examination", the details of the teaching units are approximate values which may deviate slightly in individual cases due to the composition of the participants, previous knowledge and number of participants. The order of the topics presented here does not necessarily correspond to the order of the topics of the course.

14. Anlage 2a: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Chief Information Security Officer (TÜV®)

Themenbereich und Lerninhalte	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
1. Management und Steuerung der Informationssicherheit (SIS) • Die Rolle des CISO im IS-Management • Zielsetzung • Steuerungsinstrumente • Indikatoren • Kontrolle, Überwachung • Management-Bewertung des ISMS und kontinuierliche Verbesserung (KVP) • Sicherheitsvorfallbehandlung im Rahmen der kontinuierlichen Verbesserung	**4 UE**	**4 MC**
2. Sicherheitsvorfälle und Sicherheitslücken inkl. persönlicher Aspekte (SSP) • Prozess für die Reaktion auf Sicherheitsvorfälle • Grundlagen der Forensik • Krisenmanagement und Kommunikation • Prozess für den Umgang mit Sicherheitslücken Personelle Aspekte der Informationssicherheit	**4 UE**	**4 MC**
3. Sicherheitsprojekte und Sicherheitsanalysen (SSA) • Informationssicherheitsprogramme und -projekte • Entscheidungen vorbereiten • Sicherheitsanalyse	**4 UE**	**4 MC**

4. Risikomanagement (RM) • Standards und Methoden 1. ISO 27005 2. ISO31000 3. BSI 100-3 4. FMEA • Einbindung in das unternehmensweite Risikomanagement • Übung zur Erstellung einer Risikoanalyse: 1. Ermittlung von Bedrohungsszenarien und Schwachstellen für ein gegebenes Asset (Informationswert) 2. Bewertung des Risikos für: 1. Vertraulichkeit 2. Verfügbarkeit und 3. Integrität des Assets 3. Ermittlung eines Risikowertes unter Anwendung der ISO 27005 • Ableitung von Handlungsempfehlungen zur Risikobehandlung	**4 UE**	**4 MC**
5. Business Continuity Management (BCM) • Grundlagen des Notfallmanagements • BCM als Organisationsaufgabe, Verzahnung mit dem Informationssicherheitsmanagement • Relevante Standards des Notfallmanagements 1. ISO 22301 2. BSI 200-4 • Notfallorganisation Testen von Notfallplänen	**4 UE**	**4 MC**

6. Nachweis, Auditierung & Zertifizierung (AUD) • Planung eines internen Auditprogramms (ISO 19011) 1. Methoden der internen Auditierung 2. Risikoorientierung 3. Dokumentation und Aufzeichnungen • Organisation externer Audits • Die Rolle des CISO bei der Organisation und Durchführung externer Audits Anforderungen des Auditteams und organisatorische	**4 UE**	**4 MC**
7. Compliance Aspekte der Informationssicherheit (CIS) • Rechtsgrundlagen der Informationssicherheit und Compliance • Verantwortung für die IS: 1. Pflichten und Haftung der Geschäftsleitung • Der Chief Information Security Officer: 1. Rolle, Anforderungen, Haftung und Pflichten • Datenschutz • IS-Management • Compliance-Management Anforderungsmanagement	**8 UE**	**6 MC**
Themenübergreifendes Verständnis		**2 o**
6. Abschlussprüfung		**30 MC /2 o**
schriftlich	**75 min.**	

*

UE: Unterrichtseinheit à 45 Minuten
MC: Multiple-Choice-Aufgaben
o: offene Aufgaben

In der Tabelle „Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung“ handelt es sich bei den Angaben der Unterrichtseinheiten um Richtwerte, die in Einzelfällen bedingt durch Zusammensetzung der Teilnehmenden, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.

14. Annex 2a: Topics of the course and examination modalities of the written examination Chief Information Security Officer (TÜV®)

Topics and learning content	Number of TU*	Number of questions MC*/o*
1. Information security management and control (SIS). • The role of the CISO in IS management • Objective • Management tools • Indicators • Control, monitoring • Management evaluation of the ISMS and continuous improvement (CIP) • Security incident handling in the context of continuous improvement	**4 TU**	**4 MC**
2. Security incidents and security gaps incl. personal aspects (SSP). • Security incident response process • Basics of forensics • Crisis management and communication • Process for dealing with security breaches • Personal aspects of information security	**4 TU**	**4 MC**
3. Security projects and security analyses (SSA) • Information security programs and projects • Prepare decisions Security analysis	**4 TU**	**4 MC**

4. Risk management (RM) • Standards and methods 1. ISO 27005 2. ISO31000 3. BSI 100-3 4. FMEA • Integration into the company-wide risk management • Exercise to create a risk analysis: 1. Identify threat scenarios and vulnerabilities for a given asset (information value). 2. Assessing the risk to: 1. Confidentiality 2. Availability and 3. Integrity of the asset 3. Determination of a risk value using the ISO 27005 4. Derivation of recommended actions for risk treatment	**4 TU**	**4 MC**
5. Business continuity management (BCM) • Basics of emergency management • BCM as an organizational task, dovetailing with information security management • Relevant standards of emergency management 1. ISO 22301 2. BSI 200-4 • Emergency organization Testing of emergency plans	**4 TU**	**4 MC**
6. Verification, auditing & certification (AUD) • Planning an internal audit program (ISO 19011) 1. Methods of internal auditing 2. Risk orientation 3. Documentation and records • Organization of external audits • The role of the CISO in organizing and conducting external audits Requirements of the audit team and organizational	**4 TU**	**4 MC**
7. Compliance aspects of information security (CIS)	**8 TU**	**6 MC**

• Legal basis of information security and compliance • Responsibility for IS: 1. Duties and liability of senior management • The Chief Information Security Officer: 1. Role, requirements, liability and duties • Data Protection • IS Management • Compliance Management Requirements Management		
6. Cross-topic understanding		**2 o**
7. Final exam		**30 MC/2 o**
written	**75 min.**	
practical	**4 weeks**	

*

TU: 1 TU corresponds to a teaching unit of 45 minutes.
MC: Multiple Choice questions
o: open question

In the table "Topics of the course and examination modalities of the written examination", the details of the teaching units are approximate values which may deviate slightly in individual cases due to the composition of the participants, previous knowledge and number of participants. The order of the topics presented here does not necessarily correspond to the order of the topics of the course.

15. Anlage 2b: Themen und Prüfungsmodalitäten für die praktische Prüfung Chief Information Security Officer (TÜV®)

In der praktischen Prüfung stellt der Kandidat sein Fachwissen und seine Methodik in Form einer schriftlichen Fallstudie dar. Hierbei sind konkrete Aufgabestellungen aus dem Arbeitsumfeld des Kandidaten zu bearbeiten. Die Bearbeitungszeit beträgt vier Wochen (24 Werktage). Der Umfang der eingereichten Arbeit sollte ca. 15 Seiten umfassen, jedoch 20 Seiten nicht überschreiten.

Dem Kandidaten wird eine Aufgabestellung zu den Themen

- Informationssicherheit im Unternehmen
- Übergreifende IT-Sicherheitskonzeption
- Sicherheit von IT-Systemen und Anwendungen

vorgelegt, die von ihm eigenständig zu bearbeiten ist.

Es werden bei der Prüfung der Fallstudie die Kriterien

- Beantwortung der Aufgabestellung und Erreichung der sicherheitstechnischen Zielstellung mit maximal 15 Punkten (30 %),
- Inhaltliche Richtigkeit der Aussagen bezüglich formaler Regelungen, Themenbezug und logische Stringenz, Darstellung des Sachverhalts mit maximal 15 Punkten (30 %),
- Fachliche Schlüssigkeit und Struktur mit maximal 10 Punkten (20 %) und
- Niveau und Anschaulichkeit der Darstellung (Grammatik, Grafiken, Tabellen, Verweise, Zitate) mit maximal 10 Punkten (20 %) bewertet.

15. Annex 2b: Topics of the course and examination modalities of the practical examination Chief Information Security Officer (TÜV®)

In the practical exam, the candidate presents his or her knowledge and methodology in the form of a written case study. The candidate works on a concrete task from his or her work environment. The candidate has four weeks (24 working days) to complete the case study. The case study should be around 15 pages long but should not exceed 20 pages.

The candidate receives a task on the topics

- Information security in the company
- Comprehensive IT security concept
- Security of IT systems and applications

which is to be worked on independently by him or her.

The following criteria are evaluated when examining the case study:

- Answering the task and achieving the security-related objective
  with a maximum of 15 points (30 %)
- Content correctness of the statements regarding formal regulations, topic reference and logical stringency, representation of the facts with a maximum of 15 points (30 %)
- Professional consistency and structure with a maximum of 10 points (20 %)
- Level and clarity of presentation (grammar, graphics, tables, references, quotes)
  with a maximum of 10 points (20 %).