Inhaltsverzeichnis

1. Geltungsbereich 1
2. Anmeldung und Zulassung zur Prüfung 1
3. Durchführung der Prüfung 2
3.1. Durchführung der Prüfung ISO 2
3.2. Durchführung der Prüfung ISOPlus 2
3.3. Durchführung der Prüfung CISO 2
3.4. Durchführung der Prüfung ISA 2
4. Bewertung 2
5. Wiederholung der Prüfung 3
6. Zertifizierungsentscheidung 3
7. Überwachung 3
8. Rezertifizierung 3
9. Prüfungsunterlagen 3
10. Kosten 4
11. Änderungsdienst 4
Anlage 1 - Formale Zulassungsvoraussetzungen zur Teilnahme an der Prüfung und Zertifizierung 5
Anlage 2 - Prüfungsinhalte 7

1. Geltungsbereich

Diese Prüfungs- und Zertifizierungsordnung (PZO) gilt für das Zertifizierungsverfahren für Informationssicherheitsmanagement-Fachpersonal entsprechend dem Programm zur Zertifizierung von Personen der DEKRA Certification GmbH (DCG) und auf der Grundlage der DIN EN ISO 17024 in der jeweils gültigen Fassung und für die folgenden Abschlüsse:

- Information Security Officer (ISO)
- Information Security OfficerPlus (ISOPlus)
- Chief Information Security Officer (CISO)
- Information Security Auditor (ISA)

Zusätzlich gelten die Allgemeinen Geschäftsbedingungen (AGB) (D-030-18) und die Allgemeinen Zertifizierungsbedingungen (AZB) (D-030-19) der DCG.

Die Dienstleistungen der Zertifizierungsstelle stehen allen interessierten Personen offen und die DCG garantiert die Gleichbehandlung aller Antragsteller:innen durch die Festlegung objektiver Kriterien für die Zulassung, die Prüfung und die Zertifizierung.

2. Anmeldung und Zulassung zur Prüfung

Die Anmeldung zu einer Prüfung und Zertifizierung erfolgt schriftlich anhand des Antrags zur Zertifizierung als Informationssicherheitsmanagement-Fachpersonal (F-03S-48) und Bestätigung der PZO, AZB und AGB der DCG. Die Antragstellung muss spätestens 10 Werktage vor dem geplanten Prüfungstermin erfolgen.

Die Teilnahme an den unter **Punkt 1** genannten Prüfungen unterliegt den in **Anlage 1** entsprechend genannten Zulassungsvoraussetzungen.

Die in der **Anlage 1** geforderten Nachweise sind dem Antrag zur Zertifizierung beizufügen. Die Nachweispflicht liegt bei der zu prüfenden Person.

Bei nicht erfüllten Zulassungsvoraussetzungen wird die zu prüfende Person von der Prüfung ausgeschlossen oder nimmt an der Prüfung teil und reicht die fehlenden Nachweise innerhalb von 10 Werktagen nach. Sollten die Zulassungsvoraussetzungen nicht innerhalb von 10 Werktagen nach dem Prüfungstermin erfüllt worden sein,

wird eine durchgeführte Prüfung ohne weiteres als nicht bestanden gewertet und der Prüfungspreis ist in voller Höhe zu entrichten. Bei Unklarheiten ist die Zertifizierungsstelle berechtigt, weitere Nachweise anzufordern.

Alle Nachweise müssen in deutscher Sprache verfasst sein. Ausländische Nachweise müssen über eine:n öffentlich bestellte:n und allgemein beeidigte:n Übersetzer:in durch den/die Antragsteller:in übersetzt sein.

Die Zertifizierungsstelle prüft die Vollständigkeit und formale Richtigkeit der Anmeldeunterlagen und entscheidet über die Zulassung zur Prüfung.

3. Durchführung der Prüfung

Die Prüfungsaufgaben sind von der Zertifizierungsstelle erstellt und aus dem aktuellen Prüfungsfragenpool ausgewählt. Die Prüfung erfolgt grundsätzlich in deutscher Sprache, schriftlich und besteht aus Multiple-Choice-Fragen (MCF), offenen Fragen (OF) sowie Auditsituationen (AS). Die Prüfungsfragen spiegeln hierbei repräsentativ die vermittelten Lerninhalte wider.

Die Organisation der Prüfung liegt in der Verantwortung der Zertifizierungsstelle. Präsenz-Prüfungen führen zugelassene und von der DCG für diese Durchführung beauftragte Prüfer:innen oder eine Prüfungsaufsicht durch. Die Durchführung der Prüfung vor Ort obliegt dem/der eingesetzten Prüfer:in / Prüfungsaufsicht. Remote-Prüfungen werden über das von der DCG bereitgestellte Prüfungstool durchgeführt.

3.1. Durchführung der Prüfung ISO

Die Prüfung erfolgt schriftlich und besteht aus 40 MCF. Die Dauer der Prüfung beträgt 60 Minuten. Die mögliche Höchstpunktzahl beträgt 40 Punkte.

Als Hilfsmittel ist die Normenreihe ISO 27000 ff zugelassen.

3.2. Durchführung der Prüfung ISOPlus

Die Prüfung erfolgt schriftlich und besteht aus 50 MCF. Die Dauer der Prüfung beträgt 75 Minuten. Die mögliche Höchstpunktzahl beträgt 50 Punkte.

Als Hilfsmittel ist die Normenreihe ISO 27000 ff zugelassen.

3.3. Durchführung der Prüfung CISO

Die Prüfung erfolgt schriftlich und besteht aus 30 MCF und 5 offenen Fragen. Die Dauer der Prüfung beträgt 90 Minuten. Die mögliche Höchstpunktzahl beträgt 55 Punkte.

Als Hilfsmittel ist die Normenreihe ISO 27000 ff zugelassen.

3.4. Durchführung der Prüfung ISA

Die Prüfung erfolgt schriftlich und besteht aus 20 MCF, 2 offenen Fragen und 4 Auditsituationen. Die Dauer der Prüfung beträgt 120 Minuten. Die mögliche Höchstpunktzahl beträgt 70 Punkte.

Als Hilfsmittel sind die Normenreihe ISO 27000 ff sowie die Norm 19011 zugelassen.

4. Bewertung

Die Auswertung der Prüfung erfolgt durch den/die beauftragte:n und zugelassene:n Prüfer:in.

Die Prüfung gilt als bestanden, wenn mindestens 60 % der möglichen Höchstpunktzahl erreicht wird. Bei weniger als 60 % gilt die Prüfung als nicht bestanden.

Bei jeder MCF werden vier Antwortmöglichkeiten vorgegeben, wobei immer eine oder zwei oder drei Antworten richtig sind, jedoch nie alle vier Antworten. Jede vollständig richtig beantwortete MCF wird mit einem Punkt gewertet. Jede vollständig richtig beantwortete OF wird mit höchstens 5 Punkten gewertet bzw. anteilig nach Erfüllungsgrad. Jede vollständig richtig beantwortete AS wird mit höchstens 10 Punkten gewertet bzw. anteilig nach Erfüllungsgrad.

Das Prüfungsergebnis und die Prüfungsunterlagen werden der Zertifizierungsstelle übermittelt und gegengeprüft.

5. Wiederholung der Prüfung

Eine nicht bestandene Prüfung kann zweimal wiederholt werden. Die Anmeldung zu einer Wiederholungsprüfung erfolgt schriftlich anhand des Antrags zur Wiederholungsprüfung (F-03S-09) und Bestätigung der PZO, AZB und AGB der DCG.

Die Wiederholungsprüfung muss im Regelfall innerhalb von 60 Tagen nach der Zertifizierungsentscheidung (Datum des Informationsscheibens) beantragt werden. Der Termin der Wiederholungsprüfung wird von der DCG festgelegt.

6. Zertifizierungsentscheidung

Das Zertifizierungsgremium trifft die Zertifizierungsentscheidung innerhalb von ca. 3 Wochen nach dem Prüfungstermin. Weicht das Zertifizierungsgremium vom Votum des Prüfers oder der Prüferin ab, ist dies schriftlich zu begründen.

Bei bestandener Prüfung und erfolgreicher Zertifizierung wird das DEKRA Zertifikat in deutscher Sprache für die Laufzeit von max. 3 Jahren erteilt. Das Zertifikat beinhaltet die folgenden Angaben: vollständiger Name, Geburtsdatum und Titel (falls vorhanden) der zertifizierten Person, die erworbene Qualifikationsstufe, der Hinweis auf das Zertifizierungsprogramm, nachgewiesene Kenntnisse und Kompetenzen, DEKRA Logo, DEKRA Zeichen, Angaben zur Zertifizierungsstelle, Prüfungsdatum, Prüfungsort, Ausstellungsdatum, Ausstellungsort, Ablaufdatum des Zertifikates, eindeutige Zertifikatsnummer sowie die Unterschrift der verantwortlichen Person.

Die Zertifikatsinhaber:innen werden in das zur Veröffentlichung für berechtigte Personen bestimmte Verzeichnis der zertifizierten Personen der DCG aufgenommen. Das Zertifikat bleibt das Eigentum der DCG. Die Nutzungsbedingungen für das Zertifikat sind in den AZB geregelt.

7. Überwachung

Die zertifizierte Person hat eigenverantwortlich ihren Kompetenzerhalt sicherzustellen. Die DCG überwacht die Einhaltung der Nutzungsbedingungen für das Zertifikat. Dazu gehören – sofern im Gültigkeitszeitraum des Zertifikats eintretend – die Auswertung von Informationen von Aufsichtsbehörden, die Bewertung von Beschwerden und Informationen von interessierten Kreisen sowie von eingeleiteten rechtlichen Schritten in Bezug auf die zertifizierte Person.

8. Rezertifizierung

Eine Rezertifizierung kann von Zertifikatsinhaber:innen spätestens bis zu 3 Monaten nach dem Ablauf der Gültigkeit des aktuellen Zertifikates unter Verwendung des Antrags zur Rezertifizierung (F-03S-17) schriftlich bei DCG beantragt werden.

Dabei sind die in der **Anlage 1** geforderten Nachweise mit einzureichen.

Später eingereichte Anträge werden nicht akzeptiert. Alle Anforderungen für die Rezertifizierung müssen im Zeitraum der Zertifikatsgültigkeit erfüllt worden sein.

Voraussetzung für eine Rezertifizierung sind ein vollständiger und korrekter Antrag und die positive Bewertung der eingereichten Nachweise. Das Ergebnis der Dokumentenprüfung wird dem/der Antragsteller:in mitgeteilt. Bei erfolgreicher Dokumentenprüfung wird ein neues Zertifikat für weitere max. 3 Jahre ausgestellt. Das bisherige Zertifikat verliert seine Gültigkeit.

9. Prüfungsunterlagen

Alle Unterlagen zur Prüfung werden von der Zertifizierungsstelle elektronisch archiviert. Die Aufbewahrungsfrist beträgt 10 Jahre.

10. Kosten

Erstprüfung/ Wiederholungsprüfung (inkl. Zertifizierung)	**Preis zzgl. MwSt.**	**Preis inkl. MwSt.**
Information Security Officer (ISO)	250,00 EUR	297,50 EUR
Information Security Officer^{Plus} (ISOPlus)	300,00 EUR	357,00 EUR
Chief Information Security Officer (CISO)	350,00 EUR	416,50 EUR
Information Security Auditor (ISA)	450,00 EUR	535,50 EUR
Rezertifizierung	**Preis zzgl. MwSt.**	**Preis inkl. MwSt.**
Information Security Officer (ISO)	175,00 EUR	208,25 EUR
Information Security Officer^{Plus} (ISOPlus)	175,00 EUR	208,25 EUR
Chief Information Security Officer (CISO)	175,00 EUR	208,25 EUR
Information Security Auditor (ISA)	195,00 EUR	232,05 EUR

11. Änderungsdienst

Der/Die Teilnehmende bzw. die zertifizierte Person hat sich laufend eigenverantwortlich über Änderungen an den für den Zertifizierungsprozess relevanten Verfahren, Beschreibungen, Dokumenten und Formularen zu informieren. Die aktuellen Unterlagen sind auf der Website der DCG erhältlich.

Anlage 1 - Formale Zulassungsvoraussetzungen zur Teilnahme an der Prüfung und Zertifizierung

Erstzertifizierung				
Anforderung	**ISO**	**ISOPlus**	**CISO**	**ISA**
Abschluss			Zertifikat ISO oder ISOPlus (DEKRA) bzw. gleichwertiger Nachweis	Zertifikat ISO oder ISOPlus oder CISO (DEKRA) bzw. gleichwertiger Nachweis
Schulung	Erfolgreiche Teilnahme am ISO-Lehrgang bei einem von DCG anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis	Erfolgreiche Teilnahme am ISOPlus-Lehrgang bei einem von DCG anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis	Erfolgreiche Teilnahme am CISO-Lehrgang bei einem von DCG anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis	Erfolgreiche Teilnahme am ISA-Lehrgang bei einem von DCG anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis
Rezertifizierung				
Anforderung	**ISO**	**ISOPlus**	**CISO**	**ISA**
ISMS-bezogene Tätigkeiten	mind. 1 Jahr der Berufserfahrung in Vollzeit	mind. 1 Jahr der Berufserfahrung in Vollzeit	mind. 1 Jahr der Berufserfahrung in Vollzeit	
Auffrischungs-schulung	mind. 8 LE Auffrischungs-/ Fortbildungs-schulung zum Thema ISMS	mind. 8 LE Auffrischungs-/ Fortbildungs-schulung zum Thema ISMS	mind. 8 LE Auffrischungs-/ Fortbildungs-schulung zum Thema ISMS	mind. 8 LE Auffrischungs-/ Fortbildungs-schulung zum Thema ISMS
Audit-erfahrung				mind. 3 externe ISMS-Audits mit mind. 6 Audittagen vor Ort **oder** mind. 6 interne ISMS-Audits mit mind. 12 Audittagen vor Ort

Bitte beachten Sie unbedingt die folgenden Hinweise:

- 1 Lehreinheit (LE) entspricht 45 Minuten
- Eine Tätigkeit wird als ISMS-bezogen betrachtet, wenn diese in Eigenverantwortung ausgeübt wird und in der Regel auf die Umsetzung wesentlicher Forderungen von ISMS-Normen (z. B. ISO 27001) oder entsprechenden normativen Dokumenten gerichtet ist. Die Tätigkeiten sind aufzulisten bzw. zu beschreiben und von dem Arbeitgeber zu bestätigen.

- Schulung bedeutet den Besuch des geforderten Lehrgangs bei einem von der DCG anerkannten Bildungsdienstleister (80 % Anwesenheitspflicht).
- Alle Anforderungen für die Rezertifizierung müssen im Zeitraum der Zertifikatsgültigkeit erfüllt worden sein.
- Auffrischungsschulung bedeutet den Besuch einer Weiterbildungs-/Fortbildungsschulung bzw. einer Schulung, in der Neuerungen im ISMS-Bereich behandelt wurden. Die Auffrischungsschulung sowie der Bildungsdienstleister sind frei wählbar.
- Die eigenständige Durchführung der internen bzw. externen Audits ist bzgl. Datum, Dauer, Art des Audits, Funktion des Antragstellers im Audit (Lead- oder Co-Auditor), auditierte Norm und Name der auditierten Organisation durch den Arbeitgeber oder Auditauftraggeber schriftlich zu bestätigen. Das DEKRA-Formular „Bestätigung der Auditerfahrung“ (F-03S-51) kann optional dafür verwendet werden.
- Audits über einzelne Anforderungen bzw. Unterabschnitte der Norm können nicht als vollständiges Audit anerkannt werden. Ein Audittag entspricht 8 Stunden.
- Bei der Rezertifizierung können nur Standards bestätigt werden, die bereits bei der Erstzertifizierung bestätigt wurden. Soll bei der Rezertifizierung ein neuer Standard bestätigt werden (z. B. neue Version der ISO 27001), so ist dies nur möglich, wenn entsprechende Schulungsnachweise vorgelegt werden.

Anlage 2 - Prüfungsinhalte

Information Security Officer (ISO)

- Grundlagen der Informationssicherheit
- Informationssicherheitsmanagementsystem (ISMS)
- Informationssicherheitsmanagementsystem vs. IT-Servicemanagement
- Normen und Standards der Informationssicherheit
- Normenreihe ISO/IEC 27000 im Überblick
- Anforderungen der ISO/IEC 27001
- PDCA-Zyklus
- Datenschutzrechtliche Anforderungen
- Rollen und Verantwortlichkeiten im ISMS
- Sicherheitstechnologien
- Kryptographie
- Assets
- SoA und Scope
- Maßnahmenziele und Maßnahmen (Anhang A der ISO/IEC 27001; ISO/IEC 27002)
- Risikoanalyse und -bewertung

Information Security Officer^{Plus} (ISOPlus)

Zusätzlich zu den ISO-Inhalten:

- BSI IT-Grundschutz
- Vergleich mit ISO/IEC 27001
- BSI-Standards
- Notfallmanagement
- IT-Grundschutz-Methodik
- Umsetzungshinweise

Chief Information Security Officer (CISO)

- Management und Steuerung der Informationssicherheit – Bewertung von Nachweisen und Auditierungen
- Strategische Steuerung von PDCA / KVP
- Aktuelle Bedrohungen und Gefährdungen der IT-Sicherheit aus strategischer Sicht
- Sicherheitstechnologien im Überblick
- Informationssicherheitsmanagement vs. IT-Servicemanagement – Managemententscheidungen
- Sicherheitsorganisation und Verantwortlichkeiten – strategische Rollen im ISMS
- Verantwortung und Aufgaben des CISO im Unternehmen
- Rechtliche Aspekte der Informationssicherheit
- Rechtsgrundlagen – Datenschutz – Compliance
- Asset Register – Werte und Bewertung
- SoA und Scope aus Sicht des CISO
- Steuerungselemente des ISMS einsetzen
- Security Incident Management in der Verantwortung des CISO
- Bewerten und Lenken des ISMS anhand von KPIs und internen Kontrollprozessen/Systemen
- Risikoanalyse und -bewertung, BSI Standard 200-3 Zusammenfassung für den CISO
- Abgrenzung ISO vs. CISO

Information Security Auditor (ISA)

- Grundlagen der Auditierung
- Normative Anforderungen (ISO 19011)
- Steuerung eines Auditprogramms
- Vorbereitung von Audits
- Durchführung von Audits
- Kommunikation / Gesprächsführung im Audit
- Umgang mit besonderen Auditsituationen
- Nachbereitung von Audits
- Folgemaßnahmen
- Anforderungen an Auditoren
- Überblick über die Rechtsgrundlagen Datenschutz und Compliance