Inhaltsverzeichnis

1. Geltungsbereich

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

- Information Security Officer (ISO)
- Information Security Officer^{Plus} (inkl. BSI IT-Grundschutz) (ISO^{Plus})
- 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 DEKRA Certification GmbH.

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

Aus Vereinfachungsgründen wurde für Bezeichnungen durchgängig die männliche Form gewählt. Damit soll keine Benachteiligung eines Geschlechts verbunden sein; die Bezeichnungen erfassen die jeweilige weibliche Form ebenso.

2. Anmeldung und Zulassung zur Prüfung

Die Anmeldung zu einer Prüfung und Zertifizierung erfolgt schriftlich anhand des Antrags zur Zertifizierung für ISMS-Fachpersonal (F-03S-48) und Bestätigung der PZO, AZB und AGB der DEKRA Certification GmbH. Die Antragstellung muss spätestens 1 Woche vor dem geplanten Prüfungstermin erfolgen.

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

Die Nachweispflicht liegt beim Teilnehmer. Die Zertifizierungsstelle prüft die Vollständigkeit und formale Richtigkeit der Anmeldeunterlagen sowie das Vorliegen der Zulassungsvoraussetzungen und entscheidet über die Zulassung zur Prüfung.

3. Durchführung der Prüfung

Die Prüfung bezieht sich auf die Wissensbereiche und Lerninhalte gemäß der **Anlage 2** dieser Prüfungs- und Zertifizierungsordnung (PZO).

Die Prüfungsaufgaben werden von der Zertifizierungsstelle aus dem Aufgabenpool ausgewählt.

Die Prüfung erfolgt grundsätzlich in deutscher Sprache. Die Organisation der Prüfung liegt in der Verantwortung der Zertifizierungsstelle. Die Prüfung führt ein zugelassener und von der DEKRA Certification GmbH für diese Durchführung beauftragter Prüfer durch. Die Organisation der Prüfung vor Ort obliegt dem eingesetzten Prüfer.

3.1. Durchführung der Prüfung ISO

Die Prüfung erfolgt schriftlich und besteht aus 40 Multiple-Choice-Fragen (MC-Fragen). Die Dauer der Prüfung beträgt 60 Minuten. Die mögliche Höchstpunktzahl beträgt 40 Punkte.

Die Prüfung wird von einem Prüfer abgenommen. Als Hilfsmittel sind die Normenreihe ISO 27000 ff. sowie die von der DEKRA Certification GmbH zugelassenen Schulungsunterlagen zugelassen.

3.2. Durchführung der Prüfung ISO^{Plus}

Die Prüfung erfolgt schriftlich und besteht aus 50 Multiple-Choice-Fragen (MC-Fragen). Die Dauer der Prüfung beträgt 75 Minuten. Die mögliche Höchstpunktzahl beträgt 50 Punkte.

Die Prüfung wird von einem Prüfer abgenommen. Als Hilfsmittel sind die Normenreihe ISO 27000 ff., BSI-Standards sowie die von der DEKRA Certification GmbH zugelassenen Schulungsunterlagen zugelassen.

3.3. Durchführung der Prüfung CISO

Die Prüfung erfolgt schriftlich und besteht aus 30 Multiple-Choice-Fragen (MC-Fragen) und 5 offenen Fragen. Die mögliche Höchstpunktzahl beträgt 55 Punkte. Die Dauer der Prüfung beträgt 90 Minuten.

Die Prüfung wird von einem Prüfer abgenommen. Als Hilfsmittel sind die Normenreihe ISO 27000 ff. sowie die von der DEKRA Certification GmbH zugelassenen Schulungsunterlagen zugelassen.

3.4. Durchführung der Prüfung ISA

Die Prüfung erfolgt schriftlich und besteht aus 20 Multiple-Choice-Fragen (MC-Fragen), 2 offenen Fragen und 4 Auditsituationen. Die Dauer der Prüfung beträgt 120 Minuten. Die mögliche Höchstpunktzahl beträgt 70 Punkte.

Die Prüfung wird von einem Prüfer abgenommen. Als Hilfsmittel sind die Normenreihe ISO 27000 ff., die Norm 19011 sowie die von der DEKRA Certification GmbH zugelassenen Schulungsunterlagen zugelassen.

4. Bewertung

Die Auswertung der Prüfung erfolgt durch den beauftragten Prüfer.

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 MC-Frage werden vier Antwortmöglichkeiten vorgegeben, wobei immer eine oder mehrere Antworten richtig sein können. Jede vollständig richtig beantwortete MC-Frage wird mit einem Punkt gewertet. Jede vollständig richtig beantwortete offene Frage wird mit höchstens 5 Punkten gewertet bzw. anteilig nach Erfüllungsgrad. Jede vollständig richtig beantwortete Auditsituation wird mit höchstens 10 Punkten gewertet bzw. anteilig nach Erfüllungsgrad.

Das Prüfungsergebnis und die Prüfungsunterlagen werden der Zertifizierungsstelle übermittelt und gegen geprüft.

5. Wiederholung der Prüfung

Eine nicht bestandene Prüfung kann einmal 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 DEKRA Certification GmbH.

Die Wiederholungsprüfung muss im Regelfall innerhalb von 60 Tagen nach der Zertifizierungsentscheidung (Datum des Entscheides) beantragt werden. Der Termin der Wiederholungsprüfung wird von der DEKRA Certification GmbH festgelegt.

In Ausnahmen kann eine 2. Wiederholungsprüfung innerhalb von 30 Tagen nach der Zertifizierungsentscheidung (Datum des Entscheides) beantragt werden. Die Entscheidung über die Sonderzulassung zur 2. Wiederholungsprüfung obliegt dem Industry Expert Personnel Certification.

6. Zertifizierungsentscheidung

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

Bei bestandener Prüfung und erfolgreicher Zertifizierung wird das DEKRA Zertifikat in der Regel 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 werden in das zur Veröffentlichung für berechtigte Personen bestimmte Verzeichnis der zertifizierten Personen der DEKRA Certification GmbH aufgenommen. Das Zertifikat bleibt das Eigentum der DEKRA Certification GmbH. Die Nutzungsbedingungen für das Zertifikat sind in den AZB geregelt.

7. Überwachung

Die zertifizierte Person hat eigenverantwortlich ihren Kompetenzerhalt sicherzustellen. Die DEKRA Certification GmbH 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 vom Zertifikatsinhaber spätestens bis zu 3 Monaten nach dem Ablauf der Gültigkeit des aktuellen Zertifikates unter Verwendung des Antrags zur Rezertifizierung (F-03S-17) schriftlich bei DEKRA Certification GmbH beantragt werden. Dabei sind die in der **Anlage 1** geforderten Nachweise mit einzureichen. Später eingereichte Anträge werden nicht akzeptiert.

Voraussetzung für eine Rezertifizierung sind ein vollständiger und korrekter Antrag und die positive Bewertung der eingereichten Nachweise. Das Ergebnis der Dokumentenprüfung wird dem Antragsteller 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 oder in Papierform archiviert aufbewahrt. 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} (ISO^{Plus})	300,00 EUR	357,00 EUR
Chief Information Security Officer (CISO)	350,00 EUR	416,50 EUR
Information Security Auditor (ISA)	410,00 EUR	487,90 EUR
Rezertifizierung	**Preis zzgl. MwSt.**	**Preis inkl. MwSt.**
alle Abschlüsse (Preis pro Abschluss)	175,00 EUR	208,25 EUR

Abweichend von diesen Regelpreisen kann für Gruppenprüfungen eine angemessene Rabattierung vereinbart werden. Die Zustimmung dazu obliegt dem Industry Expert Personnel Certification.

11. Änderungsdienst

Der Teilnehmer 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 DEKRA Certification GmbH erhältlich.

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

Erstzertifizierung				
Anforderung	**ISO**	**ISO^{Plus}**	**CISO**	**ISA**
Abschluss			Zertifikat Information Security Officer oder Information Security Officer^{Plus} (DEKRA) bzw. gleichwertiger Nachweis	Zertifikat Information Security Officer oder Information Security Officer^{Plus} oder Chief Information Security Officer (DEKRA) bzw. gleichwertiger Nachweis
Schulung	Erfolgreiche Teilnahme am ISO-Lehrgang bei einem von DEKRA Certification GmbH anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis	Erfolgreiche Teilnahme am ISO^{Plus}-Lehrgang bei einem von DEKRA Certification GmbH anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis	Erfolgreiche Teilnahme am CISO-Lehrgang bei einem von DEKRA Certification GmbH anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis	Erfolgreiche Teilnahme am ISA-Lehrgang bei einem von DEKRA Certification GmbH anerkannten Bildungsdienstleister bzw. gleichwertiger Nachweis
Rezertifizierung				
Anforderung	**ISO**	**ISO^{Plus}**	**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. 1-tägige Auffrischungs-/Fortbildungs-schulung zum Thema ISMS	mind. 1-tägige Auffrischungs-/Fortbildungs-schulung zum Thema ISMS	mind. 1-tägige Auffrischungs-/Fortbildungs-schulung zum Thema ISMS	mind. 1-tägige 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:

- 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 DEKRA Certification GmbH 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. Eine 1-tägige Auffrischungsschulung dauert mind. 8 U-Std. (1 U-Std. = 45 Min.).
- Die eigenständige Durchführung der internen bzw. externen Audits ist bzgl. Datum, Dauer, Art des Audit, 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} (ISO^{Plus})

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

Anlage 3 - Dokumentenmatrix

Dokument/Formblatt	Nr.	Teilnehmer			Prüfer			DEKRA Certification		
		EZ		RZ	EZ		RZ	EZ		RZ
Prüfungs- und Zertifizierungsordnung (PZO) ISMS-Fachpersonal	D-03S-27	x		x	x		x	x		x
Allgemeine Zertifizierungsbedingungen (AZB) Personenzertifizierung	D-030-19	x		x	x		x	x		x
Allgemeine Geschäftsbedingungen (AGB) Personenzertifizierung	D-030-18	x		x	x		x	x		x
Ablauf des Zertifizierungsverfahrens Personenzertifizierung	V-09S-01				x		x	x		x
Antrag zur Zertifizierung ISMS-Fachpersonal	F-03S-48	x						x		
Antrag zur Rezertifizierung	F-03S-17			x						x
Bestätigung der Auditerfahrung	F-03S-51			x						x
Checkliste zur Prüfungsdurchführung ISMS-Fachpersonal	C-06S-30				x		o	x		o
Fragebogen inkl. Antwortblatt	-	x		o	x		o	x		o
Lösungsmatrix	-				x		o	x		o
Antrag zur Wiederholungsprüfung	F-03S-09	o		o				o		o
Kandidatenliste/ Zertifizierungsentscheidung	F-09S-24	x		x	x		x	x		x
Zertifikat*	-	x		x				x		x
Entscheid zum Zertifizierungsverfahren	-	x		x				x		x
Prüferbeauftragung	F-06S-03				x		o	x		o
Rechnung und Reisekostenbelege des Prüfers	-				x		x	x		x
DIN EN ISO 17024	-				x			x		

Erklärungen:

EZ = Erstzertifizierung
RZ = Rezertifizierung
o = bei Bedarf (optional)
x = zwingend erforderlich
*Zertifikat nur bei erfolgreicher Zertifizierung