Vorbereitungshandbuch

Ausgabe 202305

Inhalt

1. Überblick

EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.DE)

Anwendungsbereich

Die Zertifizierung EXIN Information Security Foundation based on ISO/IEC 27001 validiert, dass Professionals die Prinzipien und Begriffe der Informationssicherheit in der Arbeitsumgebung verstehen und wissen, wie Risiken reduziert werden können.

Die Zertifizierung deckt folgende Aspekte ab:

- Informationen und Sicherheit
- Bedrohungen und Risiken
- Sicherheitsmaßnahmen
- Gesetzgebung, Vorschriften und Normen

Zusammenfassung

Die Globalisierung der Wirtschaft geht mit einem stetig wachsenden Austausch von Informationen einher. Der Informationsaustausch überschreitet dabei nicht nur nationale Grenzen, sondern auch den schmalen Grat zwischen privat und geschäftlich. Mit der Menge an zu verwaltenden Informationen wächst auch die Verantwortlichkeit. Die allgemein anerkannte und referenzierte internationale Norm ISO/IEC 27001 für Informationssicherheitsmanagement bietet ein Framework für die Organisation und das Management von Informationssicherheitsprogrammen.

Das Programm EXIN Information Security Management based on ISO/IEC 27001 nutzt die folgende Definition: Informationssicherheit ist die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Die Zertifizierung EXIN Information Security Foundation based on ISO/IEC 27001 prüft die Grundbegriffe der Informationssicherheit und wie diese zueinander in Beziehung stehen. Diese Zertifizierung möchte das Bewusstsein für den Wert und die Schwachstellen von Informationen stärken und vermitteln, welche Sicherheitsmaßnahmen für den Schutz von Informationen erforderlich sind.

Kontext

Die EXIN Information Security Foundation based on ISO/IEC 27001-Zertifizierung ist Teil des EXIN EXIN Information Security Management based on ISO/IEC 27001-Qualifizierungsprogramms.

Zielgruppe

Die Zertifizierung EXIN Information Security Foundation ISO/IEC 27001 richtet sich an alle Fachkräfte, die in der Datenverarbeitung tätig sind und eignet sich auch für Klein- und Mittelstandsunternehmer:innen, die ein gewisses Grundwissen auf dem Gebiet der Informationssicherheit benötigen. Für alle Professionals, die neu auf dem Gebiet der Informationssicherheit sind, ist diese Zertifizierung ein guter erster Schritt.

Zertifizierungsvoraussetzungen

- Erfolgreicher Abschluss der Prüfung EXIN Information Security Foundation based on ISO/IEC 27001.

Einzelheiten zur Prüfung

Art der Prüfung:	Multiple-Choice-Fragen
Anzahl der Fragen:	40
Mindestpunktzahl:	65% (26/40 Fragen)
Einsicht in Dokumentation:	Nein
Notizen machen:	Nein
Elektronische Geräte/Hilfsmittel erlaubt:	Nein
Prüfungsdauer:	60 Minuten

Es gilt die Prüfungsordnung von EXIN.

Bloom Level

Die EXIN Information Security Foundation based on ISO/IEC 27001-Zertifizierung testet Kandidatinnen und Kandidaten auf Bloom Level 1 und Level 2 nach der überarbeiteten Taxonomie von Bloom:

- Bloom Level 1: Wissen – basiert auf dem Wiederabrufen von Informationen. Kandidatinnen und Kandidaten müssen aufnehmen, merken, erkennen und wiedergeben.
- Bloom Level 2: Verstehen - ein Schritt über das Wissen hinaus. Verstehen zeigt, dass Kandidatinnen und Kandidaten begreifen, was präsentiert wird und bewerten können, wie der Unterrichtsstoff in ihrem eigenen Umfeld angewendet werden kann. Diese Art von Fragen soll zeigen, dass die Kandidatin oder der Kandidat in der Lage ist, die richtige Beschreibung von Fakten und Ideen zu organisieren, zu vergleichen, zu interpretieren und auszuwählen.

Schulung

Präsenzstunden

Für diesen Kurs werden 14 Präsenzstunden empfohlen. Darin enthalten sind Gruppenarbeiten, Prüfungsvorbereitung und kurze Pausen. Nicht enthalten sind: Mittagspausen, Hausaufgaben und die Prüfung.

Regelstudiendauer

56 Stunden (2 ECTS), je nach Vorwissen.

Schulungsanbieter

Eine Liste mit unseren akkreditierten Schulungsanbietern finden Sie unter www.exin.com.

2. Prüfungsanforderungen

Die Prüfungsanforderungen sind im Einzelnen in den Prüfungsspezifikationen erläutert. In der unten dargestellten Tabelle finden Sie eine Liste mit den Themen (Prüfungsanforderungen) und Unterthemen (Prüfungsspezifikationen) des Moduls.

Prüfungsan-forderungen	Prüfungsspezifikationen	Gewichtung
1. Informationen und Sicherheit		**27,5%**
	1.1 Begriffe zum Thema Informationen	10%
	1.2 Aspekte der Zuverlässigkeit	7,5%
	1.3 Schutz von Informationen in der Organisation	10%
2. Bedrohungen und Risiken		**12,5%**
	2.1 Bedrohungen und Risiken	12,5%
3. Sicherheitsmaßnahmen		**52,5%**
	3.1 Darlegung von Sicherheitsmaßnahmen	2,5%
	3.2 Organisatorische Sicherheitsmaßnahmen	15%
	3.3 Personelle Sicherheitsmaßnahmen	7,5%
	3.4 Physische Sicherheitsmaßnahmen	10%
	3.5 Technische Sicherheitsmaßnahmen	17,5%
4. Gesetzgebung, Vorschriften und Normen		**7,5%**
	4.1 Gesetze und Vorschriften	2,5%
	4.2 Normen	5%
	Total	**100%**

Prüfungsspezifikationen

1 Informationen und Sicherheit

1.1 Begriffe zum Thema Informationen

Die Kandidatin oder der Kandidat ist in der Lage…

1.1.1 den Unterschied zwischen Daten und Informationen zu erklären.

1.1.2 die Begriffe des Informationssicherheitsmanagements zu erklären.

1.2 Aspekte der Zuverlässigkeit

Die Kandidatin oder der Kandidat ist in der Lage…

1.2.1 den Wert der CIA-Triade zu erklären.

1.2.2 die Begriffe Verantwortlichkeit und Auditierbarkeit zu beschreiben.

1.3 Schutz von Informationen in der Organisation

Die Kandidatin oder der Kandidat ist in der Lage…

1.3.1 den Zweck und den Inhalt einer Informationssicherheitsrichtlinie darzulegen.

1.3.2 zu erklären, wie Informationssicherheit bei der Arbeit mit Lieferanten sichergestellt werden kann.

1.3.3 die Rollen und Zuständigkeiten bezüglich der Informationssicherheit darzulegen.

2 Bedrohungen und Risiken

2.1 Bedrohungen und Risiken

Die Kandidatin oder der Kandidat ist in der Lage…

2.1.1 die Begriffe Bedrohung, Risiko und Risikomanagement zu erklären.

2.1.2 Schadenstypen zu beschreiben.

2.1.3 Risikostrategien zu beschreiben.

2.1.4 eine Risikoanalyse zu beschreiben.

3 Sicherheitsmaßnahmen

3.1 Darlegung von Sicherheitsmaßnahmen

Die Kandidatin oder der Kandidat ist in der Lage…

3.1.1 für jeden Typ von Sicherheitsmaßnahme Beispiele zu nennen.

3.2 Organisatorische Sicherheitsmaßnahmen

Die Kandidatin oder der Kandidat ist in der Lage…

3.2.1 zu erklären, wie Werte (Assets) im Bereich der Informationen klassifiziert werden.

3.2.2 Sicherheitsmaßnahmen für das Zugangs- und Zugriffsmanagement von Informationen zu beschreiben.

3.2.3 Bedrohungs- und Schwachstellenmanagement, Projektmanagement und Incident Management in der Informationssicherheit zu erklären.

3.2.4 den Wert von Business Continuity zu erklären.

3.2.5 den Wert von Audits und Reviews zu beschreiben.

3.3 Personelle Sicherheitsmaßnahmen

Die Kandidatin oder der Kandidat ist in der Lage…

3.3.1 zu erklären, wie sich Informationssicherheit mit Hilfe von Verträgen und Vereinbarungen verbessern lässt.

3.3.2 zu erklären, wie sich Bewusstsein für Informationssicherheit schaffen lässt.

3.4 Physische Sicherheitsmaßnahmen

Die Kandidatin oder der Kandidat ist in der Lage…

3.4.1 physische Zutrittskontrollen zu beschreiben.

3.4.2 zu beschreiben, wie Informationen in Sicherheitsbereichen geschützt werden.

3.4.3 zu erläutern, wie Sicherheitsringe (Protection Rings) funktionieren.

3.5 Technische Sicherheitsmaßnahmen
Die Kandidatin oder der Kandidat ist in der Lage…
3.5.1 darzulegen, wie man Informationswerte (Information Assets) managt.
3.5.2 zu beschreiben, wie man Systeme unter Berücksichtigung von Informationssicherheit entwickelt.
3.5.3 Sicherheitsmaßnahmen zu benennen, um die Netzwerksicherheit zu gewährleisten.
3.5.4 technische Sicherheitsmaßnahmen für das Zugangs- und Zugriffsmanagement zu beschreiben.
3.5.5 zu beschreiben, wie Informationssysteme vor Schadprogrammen, Phishing und Spam geschützt werden.
3.5.6 zu erklären, wie Aufzeichnung und Überwachung zur Informationssicherheit beitragen.

4 Gesetzgebung, Vorschriften und Normen

4.1 Gesetze und Vorschriften
Die Kandidatin oder der Kandidat ist in der Lage…
4.1.1 Beispiele für Gesetze und Vorschriften zur Informationssicherheit zu nennen.

4.2 Normen
Die Kandidatin oder der Kandidat ist in der Lage…
4.2.1 die Normen ISO/IEC 27000, ISO/IEC 27001 und ISO/IEC 27002 darzulegen.
4.2.2 weitere Normen zum Thema Informationssicherheit darzulegen.

3. Liste der Grundbegriffe

Dieses Glossar enthält Begriffe und Abkürzungen, mit denen die Kandidatinnen und Kandidaten vertraut sein sollten.

Bitte beachten Sie, dass die Kenntnis dieser Begriffe alleine nicht ausreicht. Die Kandidatin oder der Kandidat muss diese Begriffe auch verstehen und mit Beispielen belegen können.

Englisch	Deutsch
access control	Zugangssteuerung/Zugriffssteuerung
accountability	Verantwortlichkeit
annualized loss expectancy (ALE)	annualisierte Verlusterwartung (ALE)
annualized rate of occurrence (ARO)	annualisierte Häufigkeitsrate (ARO)
asset	Wert (Asset)
auditability	Auditierbarkeit
authentication	Authentifizierung
authorization	Autorisierung
availability	Verfügbarkeit
backup	Backup
biometrics	Biometrik
business continuity management (BCM)	Business Continuity Management (BCM)
certificate	Zertifikat
change management	Change Management
chief information security officer (CISO)	Chief Information Security Officer (CISO)
classification	Klassifizierung
code of conduct	Verhaltenskodex
compliance	Einhaltung von Vorgaben (Compliance)
confidentiality	Vertraulichkeit
controls • corrective • detective • insurance • preventive • reductive • repressive (suppressive)	Sicherheitsmaßnahmen • korrigierend • erkennend • abgesichert (über Versicherung) • präventiv • reduzierend • unterdrückend
cryptography	Kryptographie
cyber crime	Cyberkriminalität
damage • direct damage • indirect damage	Schaden • direkter Schaden • indirekter Schaden
data	Daten
digital signature	digitale Signatur
due care	Due Care
due diligence	Due Diligence
escalation	Eskalation
exposure	Anfälligkeit
(business) impact	Auswirkung (auf das Geschäft)
incident cycle	Lebenszyklus der Incidents (Incident Cycle)
information	Informationen
information analysis	Informationsanalyse
information management	Informationsmanagement

information security management system (ISMS)	Informationssicherheitsmanagementsystem (ISMS)
information security manager (ISM)	Information Security Manager (ISM)
information security officer (ISO)	Information Security Officer (ISO)
information security policy	Informationssicherheitsrichtlinie
information security strategy	Informationssicherheitsstrategie
information system	Informationssystem
integrity	Integrität
likelihood	Eintrittswahrscheinlichkeit
non-disclosure agreement (NDA)	Vertraulichkeitsvereinbarung (NDA)
Plan, Do, Check, Act (PDCA)	Planen, Umsetzen, Überprüfen, Handeln (Plan, Do, Check, Act; PDCA)
personally identifiable information (PII)	Persönlich identifizierbare Informationen (PII)
phishing	Phishing
privacy	Privatsphäre
protection ring	Sicherheitsring (Protection Ring)
public key infrastructure (PKI)	Infrastruktur mit öffentlichem Schlüssel (PKI)
reliability	Zuverlässigkeit
risk	Risiko
risk analysis • qualitative risk analysis • quantitative risk analysis	Risikoanalyse • qualitative Risikoanalyse • quantitative Risikoanalyse
risk assessment	Risikobewertung
risk management	Risikomanagement
risk strategy • risk avoiding • risk bearing (risk acceptance) • risk neutral	Risikostrategie • risikovermeidend/Risikovermeidung • Risikotragfähigkeit (Risikoakzeptanz) • risikoneutral/Risikoneutralität
risk treatment	Risikobehandlung
security incident	Sicherheitsincident
segregation of duties	Trennung der Verantwortlichkeit
single loss expectancy (SLE)	Einzelverlusterwartung (SLE)
stand-by arrangement	Stand-by-Regelung
threat • human threat • non-human threat	Bedrohung • menschliche Bedrohung • nicht-menschliche Bedrohung
threat agent	Threat Agent (Bedrohungsakteur)
validation	Validierung
verification	Verifizierung
virtual private network (VPN)	virtuelles privates Netzwerk (VPN)
vulnerability	Schwachstelle

4. Literatur

Prüfungsliteratur

Das für die Prüfung benötigte Wissen wird durch folgende Literatur abgedeckt:

A. Baars, H., Hintzbergen, J., and Hintzbergen, K.
Foundations of Information Security – Based on ISO 27001 and ISO 27002
Van Haren Publishing: 4. vollständig überarbeitete Ausgabe, 2023
ISBN: 978 94 018 0958 0 (Papierausgabe)
ISBN: 978 94 018 0959 7 (eBook)
ISBN: 978 94 018 0960 3 (ePub)

Literaturmatrix

Prüfungsan-forderungen	Prüfungsspezifikationen	Literaturverweis
1. Informationen und Sicherheit		
	1.1 Begriffe zum Thema Informationen	Kapitel 3.1 - 3.3, 4.7 - 4.9
	1.2 Aspekte der Zuverlässigkeit	Kapitel 3.4, 4.4 - 4.6
	1.3 Schutz von Informationen in der Organisation	Kapitel 4.2, 4.3, 4.11 - 4.14, 5.1 - 5.6, 5.14, 5.19 - 5.23, 5.35, 7.7, 7.9, 7.10, 8.30
2. Bedrohungen und Risiken		
	2.1 Bedrohungen und Risiken	Kapitel 3.5, 3.7, 3.9 – 3.11
3. Sicherheitsmaßnahmen		
	3.1 Darlegung von Sicherheitsmaßnahmen	Kapitel 3.8
	3.2 Organisatorische Sicherheitsmaßnahmen	Kapitel 3.6.2, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8
	3.3 Personelle Sicherheitsmaßnahmen	Kapitel 6
	3.4 Physische Sicherheitsmaßnahmen	Kapitel 7
	3.5 Technische Sicherheitsmaßnahmen	Kapitel 4.10, 8
4. Gesetzgebung, Vorschriften und Normen		
	4.1 Gesetze und Vorschriften	Kapitel 5.31 – 5.34
	4.2 Normen	Kapitel 1, 3.6, 3.12, 4.1, 4.12, 5.36

Kontakt EXIN

www.exin.com