Vorbereitungshandbuch

Ausgabe 202607

Copyright © EXIN Holding B.V. 2026. All rights reserved.
EXIN® is a registered trademark of EXIN.

No part of this publication may be reproduced, stored, utilized or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written permission from EXIN.

Inhalt

1. Überblick

EXIN Information Security Essentials based on ISO/IEC 27001 (ISE.DE)

Anwendungsbereich

Die Zertifizierung EXIN Information Security Essentials 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.

Diese Zertifizierung deckt folgende Themen ab:

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

Zusammenfassung

Da die Welt immer vernetzter wird und sich die Globalisierung der Wirtschaft beschleunigt, tauschen Organisationen und Einzelpersonen mehr Informationen aus als je zuvor. Diese Informationen überschreiten häufig nationale Grenzen und werden zwischen privaten und beruflichen Bereichen ausgetauscht. Sie fließen zudem zwischen Unternehmen, Kunden und Lieferanten. Mit diesem ständigen Austausch wächst die Verantwortung für die Verwaltung und den Schutz von Informationen. 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 Infor mation Security Essentials based on ISO/IEC 27001 führt die Validierung der Schlüsselkonzepte der Informationssicherheit und ihrer Zusammenhänge durch. Sie bestätigt, dass der Kandidat die Grundlagen der Informationssicherheit versteht, und trägt damit dazu bei, die Informationen einer Organisation zu schützen und den täglichen Betrieb sicher, konform und reibungslos zu gestalten. Das Zertifikat bietet zudem einen soliden Ausgangspunkt für das weitere Lernen im Bereich der Informationssicherheit.

Kontext

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

Zielgruppe

Die Zertifizierung EXIN Information Security Essentials based on ISO/IEC 27001, ist für folgende Zwecke bestimmt:

- Alle Mitarbeiter, die mit Informationen umgehen, unabhängig von ihrer Abteilung
- Nicht-IT-Fachkräfte in den Bereichen Personalwesen, Verwaltung, Management oder Betrieb
- Unternehmer und Inhaber kleiner Unternehmen
- Einsteiger im Bereich der Verarbeitung von Informationen
- Einsteiger im Bereich Informationssicherheit

Zertifizierungsvoraussetzungen

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

Einzelheiten zur Prüfung

Art der Prüfung:	Multiple-Choice-Fragen
Anzahl der Fragen:	20
Mindestpunktzahl:	65% (13/20 Fragen)
Einsicht in Dokumentation:	Nein
Notizen machen:	Nein
Elektronische Geräte/Hilfsmittel erlaubt:	Nein
Prüfungsdauer:	30 Minuten

Es gilt die Prüfungsordnung von EXIN.

Bloom Level

Die Zertifizierung EXIN Information Security Essentials based on ISO/IEC 27001 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 7 Präsenzstunden empfohlen. Darin enthalten sind Gruppenarbeiten, Prüfungsvorbereitung und kurze Pausen. Nicht enthalten sind: Mittagspausen, Hausaufgaben und die Prüfung.

Regelstudiendauer

28 Stunden (1 ECTS), je nach Vorwissen.

Akkreditierte Trainingsorganisationen

Eine Liste mit unseren akkreditierten Trainingsorganisationen 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.

Prüfungsanforderungen	Prüfungsspezifikationen	Gewichtung
1. Informationen und Sicherheit		**30%**
	1.1 Begriffe zum Thema das Informationssicherheitsmanagement	5%
	1.2 Aspekte der Zuverlässigkeit	10%
	1.3 Schutz von Informationen in der Organisation	15%
2. Bedrohungen und Risiken		**20%**
	2.1 Bedrohungen und Risiken	20%
3. Sicherheitsmaßnahmen		**45%**
	3.1 Organisatorische Sicherheitsmaßnahmen	17.5%
	3.2 Personelle Sicherheitsmaßnahmen	5%
	3.3 Physische Sicherheitsmaßnahmen	5%
	3.4 Technische Sicherheitsmaßnahmen	17.5%
4. Gesetzgebung, Vorschriften und Normen		**5%**
	4.1 Gesetze und Vorschriften	2.5%
	4.2 Normen	2.5%
	Total	**100%**

Prüfungsspezifikationen

1 Informationen und Sicherheit

1.1 Begriffe zum Thema das Informationssicherheitsmanagement
Die Kandidatin oder der Kandidat ist in der Lage…
1.1.1 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.

1.3 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 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 Organisatorische Sicherheitsmaßnahmen
Die Kandidatin oder der Kandidat ist in der Lage…
3.1.1 zu erklären, wie Werte (Assets) im Bereich der Informationen klassifiziert werden.
3.1.2 Sicherheitsmaßnahmen für das Zugangs- und Zugriffsmanagement von Informationen zu beschreiben.
3.1.3 Bedrohungs- und Schwachstellenmanagement, Projektmanagement und Incident Management in der Informationssicherheit zu erklären.
3.1.4 den Wert von Business Continuity zu erklären.

3.2 Personelle Sicherheitsmaßnahmen
Die Kandidatin oder der Kandidat ist in der Lage…
3.2.1 zu erklären, wie sich Bewusstsein für Informationssicherheit schaffen lässt.

3.3 Physische Sicherheitsmaßnahmen
Die Kandidatin oder der Kandidat ist in der Lage…
3.3.1 physische Zutrittskontrollen zu beschreiben.

3.4 Technische Sicherheitsmaßnahmen
Die Kandidatin oder der Kandidat ist in der Lage…
3.4.1 darzulegen, wie man Informationswerte (Information Assets) managt.
3.4.2 Sicherheitsmaßnahmen zu benennen, um die Netzwerksicherheit zu gewährleisten.
3.4.3 technische Sicherheitsmaßnahmen für das Zugangs- und Zugriffsmanagement zu beschreiben.
3.4.4 zu beschreiben, wie Informationssysteme vor Schadprogrammen, Phishing und Spam geschützt werden.

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.

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)
business continuity plan	Business Continuity Plan
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
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

Prüfungsanforderungen	Prüfungsspezifikationen	Literaturverweis
1. Informationen und Sicherheit		
	1.1 Begriffe zum Thema das Informationssicherheitsmanagement	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 Organisatorische Sicherheitsmaßnahmen	Kapitel 3.6.2, 5.3, 5.7 – 5.18, 5.24 – 5.30, 5.35, 5.36, 6.8
	3.2 Personelle Sicherheitsmaßnahmen	Kapitel 6
	3.3 Physische Sicherheitsmaßnahmen	Kapitel 7
	3.4 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

Certified for what's next

Kontakt EXIN

www.exin.com