DIM
Deutsches Institut für
Managementmethoden

Vorbereitungshandbuch – Informationssicherheits-beauftragter ISB (DIM®)

1. Überblick

Die Zertifizierung Informationssicherheitsbeauftragter ISB (DIM®) vermittelt tiefgehende Kenntnisse zur Planung, Umsetzung und Überwachung von IT-Sicherheitsstrategien nach internationalen Standards wie ISO 27001.

Zielgruppe

Diese Zertifizierung richtet sich an:

- IT-Sicherheitsbeauftragte
- Compliance- und Risikomanager
- IT-Administratoren und Datenschutzbeauftragte

2. Prüfungsanforderungen

Die Prüfung bewertet Kenntnisse und Fähigkeiten zur Implementierung von IT-Sicherheitsmaßnahmen.

Prüfungsdetails:

Prüfungsart: Multiple-Choice

Anzahl der Fragen: 40

Mindestpunktzahl: 65 % (26 von 40 Fragen)

Prüfungsdauer: 60 Minuten

Einsicht in Dokumentation erlaubt: Nein

Hilfsmittel erlaubt: Nein

Prüfungsinhalte und Gewichtung

Prüfungsbereiche	Themen	Gewichtung
1. Grundlagen der IT-Sicherheit	IT-Sicherheitsstrategien, Bedrohungen	20 %
2. Sicherheitsstandards & Compliance	ISO 27001, BSI IT-Grundschutz	25 %
3. Risikomanagement	Identifikation, Analyse, Maßnahmen	20 %
4. Incident Management & Response	Erkennung & Behandlung von Sicherheitsvorfällen	15 %
5. Datenschutz & rechtliche Anforderungen	DSGVO, Unternehmensrichtlinien	20 %

3. Liste der Grundbegriffe

Informationssicherheits-Managementsystem (ISMS):
Ein systematischer Ansatz zur Verwaltung aller Aspekte der Informationssicherheit innerhalb einer Organisation.

Informationssicherheit:
Der Schutz von Informationen vor unbefugtem Zugriff, Veränderung oder Zerstörung zur Sicherstellung von Vertraulichkeit, Integrität und Verfügbarkeit.

Risiko:
Die Kombination aus der Wahrscheinlichkeit eines Sicherheitsvorfalls und den potenziellen Auswirkungen auf die Organisation.

Risikobewertung:
Der Prozess der Identifikation, Analyse und Bewertung von Risiken, die die Informationssicherheit betreffen.

Risikobehandlung:
Maßnahmen zur Reduzierung, Akzeptanz, Übertragung oder Vermeidung identifizierter Risiken durch geeignete Sicherheitskontrollen.

Vertraulichkeit:
Das Prinzip, sicherzustellen, dass Informationen nur für autorisierte Personen zugänglich sind.

Integrität:
Der Schutz der Richtigkeit, Vollständigkeit und Vertrauenswürdigkeit von Informationen und Systemen.

Verfügbarkeit:
Die Gewährleistung, dass autorisierte Benutzer bei Bedarf jederzeit auf Informationen und Systeme zugreifen können.

Schwachstelle (Vulnerability):
Eine Schwäche in einem System oder Prozess, die ausgenutzt werden kann, um unbefugten Zugriff oder Schaden zu verursachen.

Bedrohung:
Jede potenzielle Gefahr, die zu einem Sicherheitsvorfall führen kann und die Informationssicherheit beeinträchtigt.

Sicherheitskontrolle (Control):
Maßnahmen, die implementiert werden, um identifizierte Risiken zu mindern und die Informationssicherheit zu gewährleisten.

Erklärung zur Anwendbarkeit (SoA):
Ein Dokument, das darlegt, welche Sicherheitskontrollen ausgewählt und implementiert wurden und begründet, warum bestimmte Kontrollen nicht angewendet wurden.

Interne Audit:
Systematische Überprüfungen des ISMS, um dessen Wirksamkeit und die Einhaltung der Anforderungen sicherzustellen.

Kontinuierliche Verbesserung:
Der fortlaufende Prozess, das ISMS durch Überwachung, Audits und Bewertungen zu optimieren und an neue Herausforderungen anzupassen.

Nichtkonformität:
Ein Abweichen von den festgelegten Anforderungen oder Standards innerhalb des ISMS, das einer Korrektur bedarf.

Korrekturmaßnahme:
Maßnahmen zur Behebung der Ursachen einer Nichtkonformität, um deren Wiederauftreten zu verhindern.

Informationsvermögenswert:
Jede Information oder jedes Datenobjekt, das für die Organisation von Wert ist und geschützt werden muss.

Business Continuity Management (BCM):
Strategien und Prozesse, die sicherstellen, dass kritische Geschäftsprozesse auch bei Störungen oder Krisensituationen fortgeführt werden können.

Sicherheitsvorfall:
Ein Ereignis, das die Informationssicherheit beeinträchtigt, wie z. B. ein Datenleck, ein Cyberangriff oder ein Systemausfall.

Zugriffskontrolle:
Mechanismen und Richtlinien, die den Zugang zu Informationen und Systemen regeln, um unbefugte Zugriffe zu verhindern.

Lieferantenmanagement:
Prozesse zur Bewertung und Überwachung der Sicherheitspraktiken von Drittanbietern, um sicherzustellen, dass diese den Anforderungen der Informationssicherheit entsprechen.

4. Empfohlene Literatur & Vorbereitung

Empfohlene Schulungszeit

Präsenz-/Online-Kurs: ca. 20 Stunden

Selbststudium: ca. 40 Stunden

Literatur

ISO 27001 Standardwerke

BSI IT-Grundschutz-Kompendium

Zusätzliche Ressourcen und Beispielprüfungen sind über Ihre Akkreditierte Trainingsorganisation oder das Deutsche Institut für Managementmethoden (DIM) erhältlich.

5. Anmeldung zur Prüfung

Die Prüfung kann online oder vor Ort abgelegt werden.

Anmeldung über Ihre Akkreditierte Trainingsorganisation

Kontaktieren Sie uns für weitere Informationen!