**LMS Questions for [Information Security Standards and DLBCSEISS01\_E]**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 1/1 | 1.1 | ISO/IEC 27005:2011, die ISO-Norm für das Risikomanagement im Bereich der Informationssicherheit, verwendet den Begriff, um das Risikomanagement insgesamt zu beschreiben, während die Elemente innerhalb des Risikomanagementprozesses als \_\_\_\_\_\_\_\_\_ bezeichnet werden. | Prozess und Aktivitäten | Risiken und Prozesse | Risiken und Aktivitäten | Risiken und Pläne |
| 1/2 | 1.1 | Eine deutsche Chiffriermaschine wurde von welchem Land in welchem Jahr geknackt? | Polen in den 1930er Jahren | Russland in den 1930er Jahren | England in den 1930er Jahren | China in den 1930er Jahren |
| 1/3 | 1.2 | Normen und Standards sind \_\_\_\_\_\_\_\_\_\_, während die regulatorischen Rahmenbedingungen \_\_\_\_\_\_\_\_\_\_\_\_\_\_ sind. | Empfehlungen, obligatorisch | Obligatorisch, zwingend | Empfehlungen, Anforderungen  | Obligatorisch, optional |
| 1/4 | 1.1 | Welcher der folgenden Punkte wird in den ISO-Normen als Auswirkung der Unsicherheit auf die Ziele definiert? | Risiko | Risikobeurteilung | Risikobewertung | Risikomanagement |
| 1/5 | 1.1 | Was ist ein Zusammenschluss von Politiken, Prozessen, Verfahren, Organisationsstrukturen, Software und Hardware, die zum Schutz von Informationswerten eingesetzt werden? | Informationssicherheitsmanagementsystem | Informationssicherheitskontrollsystem | Informationssicherheitsworkflowsystem | Informationssicherheitsdatenbanksystem |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 2/1 | 2.2 | Warum sollte die Definition des ISMS-Anwendungsbereichs in den ersten Phasen der Implementierung nicht übersprungen werden? | Es ist schwierig, die Probleme des Anwendungsbereichs später zu lösen. | Es ist schwierig, den Anwendungsbereich zu entwickeln.  | Es ist schwierig, den Anwendungsbereich zu ändern. | Es ist schwierig, den Anwendungsbereich zu kontrollieren. |
| 2/2 | 2.2 | Auf welchen der folgenden Bereiche konzentriert sich die ISO 31000? | Risikomanagement | Ressourcenmanagement | Systemmanagement | Sicherheitsmanagement |
| 2/3 | 2.2 | Ein verbreitetes Framework für das Management von Sicherheitsrisiken ist TARA. Was bedeutet TARA? | Transfer, Avoid, Reduce, Accept | Transfer, Allow, Redo, Accept | Transfer, Agree, Repeat, Accept | Transfer, Action, React, Accept  |
| 2/4 | 2.2 | Welche der folgenden Klauseln der ISO 27001 spezifiziert die Informationssicherheitsrisikobeurteilung? | Klausel 6.1.2 | Klausel 6.2.2 | Klausel 6.3.2 | Klausel 6.4.2 |
| 2/5 | 2.3 | Welches der folgenden Attribute ist gemäß der Charakterisierung des Informationssicherheitsreifegradmodells ein Attribut der Stufe 5? | Vollständige Implementierung von Sicherheitsmaßnahmen und -verfahren | Physische Sicherheit | Sicherheitsarchitektur | Sicherheitstests |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 3/1 | 3.1 | Mathematisch gesehen, sind Risiken gleich\_\_\_\_\_\_\_\_\_ | Bedrohungen multipliziert mit Schwachstellen. | Bedrohungen multipliziert mit Defekten. | Bedrohungen multipliziert mit Fehlern. | Defekte multipliziert mit Schwachstellen. |
| 3/2 | 3.2 | Welches der folgenden Dokumente ist eines der wichtigsten für Organisationen, die eine Zertifizierung nach ISO 27001 anstreben? |  SoA | SoE | SoI | SoU |
| 3/3 | 3.4 | Schritt 5 bei der Entwicklung eines Kommunikationsplans als Teil des ISMS ist\_\_\_\_\_\_ | Kommunikationsziele definieren. | Kommunikationsplan definieren. | Kommunikationslücke definieren. | Kommunikationsort definieren. |
| 3/4 | 3.1 | Welche der folgenden ISOs spezifiziert und bezieht sich auf das Risikomanagement? | ISO 31000 | ISO 31001 | ISO 27006 | ISO 27009 |
| 3/5 | 3.5 | Eine Reihe von Maßnahmen, die nach der Auswahl der Risikobehandlungsoptionen durchgeführt werden müssen, sind in welchem Dokument beschrieben? | Anhang A der ISO 27001:2013 | Anhang B der ISO 27001:2013 | Anhang C der ISO 27001:2013 | Anhang D der ISO 27001:2013 |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 4/1 | 4.1 | Welcher der folgenden Indikatoren könnte als Leistungsindikator für die Messung der Informationssicherheit in einer Organisation verwendet werden? | COBIT 5 für Informationssicherheit | COBIT 5 für Informationsentwicklung | HIPAA | DSGVO |
| 4/2 | 4.2 | Die Konformitätskontrolle gemäß ISO/IEC 27001 ist\_\_\_\_\_\_\_\_\_\_\_\_ | eine wichtige Kontrollaktivität. | eine wichtige Risikoaktivität. | eine wichtige Überprüfungsaktivität. | eine wichtige Entwicklungsaktivität. |
| 4/3 | 4.2 | Es wird erwartet, dass interne Audits des ISMS mindestens \_\_\_\_\_\_\_\_\_ durchgeführt werden. | einmal in drei Jahren | zweimal in drei Jahren | dreimal in drei Jahren | jährlich in drei Jahren |
| 4/4 | 4.2 | Ein organisatorisches internes Kontrollsystem (IKS) ist \_\_\_\_\_\_\_\_ | ein breiter angelegtes Kontrollsystem. | Teil des ISMS. | ein breiter angelegtes System der Verwaltung.  | Teil der Schritte der internen Revision. |
| 4/5 | 4.3 | Welcher der folgenden Punkte wird in Klausel 9.3 der ISO 27001 gefordert? | Managementbewertung des ISMS | Managementausführung des ISMS | Managementplanung des ISMS | Managementwechsel des ISMS |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 5/1 | 5.1 | Welcher der folgenden Punkte ist eine Folge der Nichterfüllung der Anforderungen der ISO 27001-Normen? | Nichtkonformität | Nichterfüllung | Nichtautorisierung | Nichteffizienz |
| 5/2 | 5.1 | Die in den Normen aufgeführten obligatorischen Anforderungen heißen wie? | „Muss“-Anforderungen | „Kann“-Anforderungen | „Soll“-Anforderungen | „Sollte nicht“-Anforderungen |
| 5/3 | 5.2 | Ein nützliches Modell zur Gewährleistung der fortlaufenden Verbesserung des ISMS ist der \_\_\_\_\_\_\_\_ | PCDA-Zyklus. | PCDE-Zyklus. | PBDA-Zyklus. | PUDA-Zyklus. |
| 5/4 | 5.3 | Um geeignete Abhilfemaßnahmen zu ergreifen, ist es wichtig, die Ursache eines Problems oder einer Anomalie zu ermitteln. Dies ist bekannt als\_\_\_\_\_\_\_\_\_\_ | Ursachenanalyse. | Hauptsituationsanalyse. | Systemanalyse. | Hauptfehleranalyse. |
| 5/5 | 5.3 | Welche der folgenden Maßnahmen gehen normalerweise mit Präventivmaßnahmen einher? | Korrektive Maßnahmen | Korrekte Maßnahmen | Neue Maßnahmen | Korrektive Analyse |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 6/1 | 6.1 | Was enthält der Anhang A der ISO 27001? | Eine Reihe von Maßnahmen | Eine Reihe von Gesetzen | Eine Reihe von Richtlinien | Eine Reihe von Vorschriften |
| 6/2 | 6.1 | Welche der folgenden Angaben ist eine detaillierte Erklärung der in Anhang A der Normen aufgeführten Maßnahmen? | ISO 27002 | ISO 27003 | ISO 27004 | ISO 27005 |
| 6/3 | 6.1 | Wie viele organisatorische Maßnahmen und technologische Maßnahmen gibt es laut den Normen in der aktualisierten Version ISO 27001:2022? | 37 und 14 | 8 und 14 | 17 und 14 | 37 und 8 |
| 6/4 | 6.2 | In wie viele Gruppierungen sind die Maßnahmenkategorien unterteilt? | 14 | 40 | 8 | 9 |
| 6/5 | 6.1 | Was ist der Unterschied zwischen ISO 27001 und ISO 27002? | Anhang A der ISO 27001 listet die Maßnahmen auf, während die ISO 27002 eine detaillierte Erläuterung enthält. | Anhang B der ISO 27001 listet die Maßnahmen auf, während die ISO 27002 eine detaillierte Erläuterung enthält. | Anhang B der ISO 27002 listet die Maßnahmen auf, während die ISO 27001 eine detaillierte Erläuterung enthält. | Anhang A der ISO 27002 listet die Maßnahmen auf, während die ISO 27001 eine detaillierte Erläuterung enthält. |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 7/1 |  |  |  |  |  |  |
| 7/2 |  |  |  |  |  |  |
| 7/3 |  |  |  |  |  |  |
| 7/4 |  |  |  |  |  |  |
| 7/5 |  |  |  |  |  |  |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 8/1 |  |  |  |  |  |  |
| 8/2 |  |  |  |  |  |  |
| 8/3 |  |  |  |  |  |  |
| 8/4 |  |  |  |  |  |  |
| 8/5 |  |  |  |  |  |  |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 9/1 |  |  |  |  |  |  |
| 9/2 |  |  |  |  |  |  |
| 9/3 |  |  |  |  |  |  |
| 9/4 |  |  |  |  |  |  |
| 9/5 |  |  |  |  |  |  |
| **Unit/****Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 10/1 |  |  |  |  |  |  |
| 10/2 |  |  |  |  |  |  |
| 10/3 |  |  |  |  |  |  |
| 10/4 |  |  |  |  |  |  |
| 10/5 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |