**1.1**

1. Bitte wählen Sie die richtige(n) Aussage(n) aus.

* Risiken sollten entsprechend ihrer Auswirkung und einem Priorisierungsplan behandelt werden.
* Risiken, bei denen die Kosten für die Minderung gering sind, sollten zuerst behandelt werden, auch wenn schwerwiegendere Risiken vorhanden sind.
* Risiken mit einer geringen Eintrittswahrscheinlichkeit können ignoriert werden.

1. Bitte vervollständigen Sie den folgenden Satz:

Es lohnt sich in der Regel, ein Risiko zu mindern, wenn die Kosten für die Behandlung des Risikos niedriger sind als die mit dem Risiko verbundenen Kosten.

**1.2**

1. Beschreiben Sie, was ein Datenexfiltrationsangriff ist.

*Ein Datenexfiltrationsangriff ist ein Angriff, bei dem sich böswillige Akteure Zugang zu einem System verschaffen und Daten exfiltrieren. Es handelt sich dabei meist um sensible oder vertrauliche Daten.*

1. Bitte erklären Sie, warum Datenexfiltrationsangriffe Teil des Risikomanagementprozesses sein sollten.

*Datenexfiltrationsangriffe sind für ein Unternehmen sehr kostspielig. Das Risikomanagement muss die potenziellen Kosten senken. Dazu gehört auch die Verringerung des Risikos eines Datenexfiltrationsangriffes.*

**1.3**

1. Bitte markieren Sie die richtige(n) Aussage(n).

* Katastrophen *haben schwerwiegende Auswirkungen*.
* Die Eintrittswahrscheinlichkeit von Katastrophen ist hoch.
* Für das Risikomanagement sind die Auswirkungen einer Katastrophe nicht relevant.

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Die Quelle eines Ereignisses ist für die Einstufung als Cyber-Katastrophe irrelevant*.
* Cyber-Katastrophen haben nur nicht-menschliche Ursachen.
* Cyber-Katastrophen sind immer das Ergebnis einer böswilligen Handlung.

**1.4**

1. Beschreiben Sie den Unterschied zwischen einem Risiko und einem Cyber-Risiko.

*Cyber-Risiken beschränken sich nur auf Bedrohungen, die im Cyber-Raum auftreten. Ein Risiko, das seinen Ursprung außerhalb des Cyber-Raums hat, ist kein Cyber-Risiko. Alle Cyber-Risiken sind Risiken, aber nicht andersherum.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Es ist möglich, dass eine Bedrohung kein Risiko für eine Organisation darstellt*.
* Ein Risiko kann keine Bedrohung für eine Organisation sein.
* *Ein Risiko hat immer eine Eintrittswahrscheinlichkeit.*

**2.1**

1. Beschreiben Sie, was es bedeutet, das Risiko zu vermeiden.

*Die Vermeidung des Risikos bedeutet, dass Maßnahmen oder Prozesse implementiert werden, damit das Risiko nicht eintreten kann.*

1. Bitte markieren Sie die richtigen Aussagen.

* *Für ein angemessenes Risikomanagement muss das Risiko quantifizierbar sein*.
* Das Risiko ist das Vielfache der Eintrittswahrscheinlichkeit und der Auswirkungen.
* Die Beschreibung des Risikos in quantifizierbarer Form ist für die Entscheidung zur Risikominderung nicht erforderlich.

1. Bitte vervollständigen Sie den folgenden Satz:

Ein Risiko zu mindern oder zu reduzieren bedeutet, die Eintrittswahrscheinlichkeit der Bedrohung zu verringern.

**2.2**

1. Bitte nennen Sie die Komponenten der Auswirkungen und der Eintrittswahrscheinlichkeit.

*Eintrittswahrscheinlichkeit: Bedrohungsakteur, Schwachstelle*

*Auswirkungen: technische Auswirkungen, geschäftliche Auswirkungen*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Der Verlust der Vertraulichkeit ist eine technische Auswirkung*.
* Die Ausnutzbarkeit ist eine technische Auswirkung.
* Das Bewusstsein ist eine geschäftliche Auswirkung.

1. Bitte vervollständigen Sie den folgenden Satz.

Ein Risiko, das als finanzieller Schaden zum Bankrott führen kann, ist schlimmer als ein Risiko, das den Datenschutz von Hunderten von Menschen verletzt.

**2.3**

1. Die Faktoren eines Risikos haben folgende Werte. Bitte berechnen Sie das daraus resultierende Risiko.
   * Faktor Bedrohungsakteur: 6
   * Faktor Schwachstelle: 3,5
   * Technische Auswirkungen: 6,25
   * Geschäftliche Auswirkungen: 5

*Eintrittswahrscheinlichkeit = (6 + 3,5) / 2 = 4,75 -> Mittel*

*Auswirkungen = (6,25 + 5) / 2 = 5,625 -> Mittel*

*-> Risiko = Mittel + Mittel = Mittel*

*Das daraus resultierende Risiko ist mittel.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Die Gesamtauswirkung ist der Durchschnitt der beiden Auswirkungsfaktoren.*
* Die Gesamtauswirkung ist die Summe der beiden Auswirkungsfaktoren.
* Die Gesamtauswirkung ist das Produkt der beiden Auswirkungsfaktoren.

1. Beschreiben Sie, wie die Berechnung der Auswirkungen angepasst werden kann und warum?

*Der Faktor der geschäftlichen Auswirkungen kann stärker gewichtet werden, so dass er mehr zählt. Dies ist möglich, weil die technischen Auswirkungen meist wichtiger sind als die technischen Auswirkungen.*

**2.4**

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Die Motivation für einen Angriff kann durch die finanziellen Vorteile eines erfolgreichen Angriffs beschrieben werden*.
* Die Größe der möglichen Bedrohungsakteure ist nicht relevant.
* Wenn eine Schwachstelle leicht zu entdecken ist, werden die Auswirkungen zunehmen.

**2.5**

1. Beschreiben Sie die Unterschiede zwischen einem Black-Swan-Ereignis und einer Cyber-Katastrophe.

*Beide Ereignisse haben verheerende Auswirkungen für die Betroffenen. Der Unterschied liegt darin, dass die Eintrittswahrscheinlichkeit eines Black-Swan-Ereignisses gegen Null geht. Eine Cyber-Katastrophe ist demgegenüber wahrscheinlicher. Im Risikomanagement ist es einfacher, eine Cyber-Katastrophe zu behandeln, da die Eintrittswahrscheinlichkeit und das Ereignis bekannt sind. Ein Black-Swan-Ereignis ist eine Überraschung.*

1. Bitte vervollständigen Sie den folgenden Satz:

Ein Black-Swan-Ereignis hat verheerende *Auswirkungen*. Im Risikomanagement ist es *schwierig*, für solche Ereignisse zu planen und sich darauf vorzubereiten, denn sie treten meist *überraschend* auf.

**3.1**

1. Bitte beschreiben Sie, warum Attack-Trees zur Modellierung von Bedrohungen verwendet werden.

*Attack-Trees bieten eine formale Möglichkeit, Bedrohungen für ein bestimmtes Szenario mit hierarchischen Angriffsdarstellungsmodellen zu modellieren.*

1. Bitte markieren Sie die richtigen Aussagen.

* *Attack-Trees sind vollständig, wenn sie für den gegebenen Anwendungsfall repräsentativ sind*.
* Attack-Trees sind vollständig, wenn sie 50 Knoten erreichen.
* Attack-Trees sind vollständig, wenn sie die gesamte Organisation abbilden.

1. Bitte vervollständigen Sie den folgenden Satz:

Attack-Trees sind eine ausführliche Methode des Threat Modelings. Sie haben in der Regel die Form einer Liste oder eines Graphen.

**3.2**

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *STRIDE ist eine Merkhilfe zur Modellierung von Bedrohungen.*
* STRIDE ist ein Framework für das Risikomanagement.
* STRIDE ist eine Richtlinie für das Threat Modeling.

1. Bitte beschreiben Sie ein DFD.

Ein DFD oder Datenflussdiagramm ist ein Diagramm, das logische Dateneinheiten und den Datenfluss zwischen ihnen darstellt. Ein DFD erklärt, wie ein System funktioniert und interagiert.

1. Bitte beschreiben Sie, warum STRIDE zur Modellierung von Bedrohungen verwendet wird.

Das Ziel von STRIDE ist es, Bedrohungen für ein System zu identifizieren und sie mit Hilfe der STRIDE-Merkhilfe zu klassifizieren.

**3.3**

1. Bitte beschreiben Sie den Unterschied zwischen der Modellierung von Datenschutz- und Sicherheitsbedrohungen.

*Sicherheitsbedrohungsmodelle konzentrieren sich auf die Assets und wie diese vor (externen) Bedrohungen geschützt werden können. Die Datenschutzbedrohungsmodelle verfolgen jedoch einen anderen Ansatz. Anstatt sich auf die Assets des Systems zu konzentrieren, konzentrieren sich die Datenschutzbedrohungsmodelle auf die Daten der betroffenen Personen, um die Objekte von Interesse (IOI) und nicht das System zu schützen.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *LINDDUN ist ein Threat-Modeling-Framework.*
* LINDDUN ist ein Risikomanagement-Framework für Datenschutzrisiken.
* LINDDUN wird zur Bewertung von Datenschutzrisiken verwendet.

1. Bitte vervollständigen Sie den folgenden Satz:

Die drei Hauptschritte der LINDDUN-Methode des Threat Modelings sind Systemmodellierung, Bedrohungsermittlung und Bedrohungsmanagement.

**4.1**

1. Bitte beschreiben Sie den Zweck der NIST Special Publication 800-37.

*Der Zweck dieser Publikation ist es, einen praktischen Leitfaden für das Risikomanagement in Organisationen bereitzustellen. Das Framework enthält grundlegende Informationen über den Aufbau eines Risikomanagement-Frameworks (RMF) und eines Prozesses für das Risikomanagement.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Sicherheitsmaßnahmen sollten bewertet werden, nachdem das System kategorisiert wurde.*
* Sicherheitsmaßnahmen sollten bewertet werden, bevor das System kategorisiert wird.
* Sicherheitsmaßnahmen sollten implementiert werden, nachdem das System und die zugehörigen Maßnahmen überwacht wurden.

1. Bitte vervollständigen Sie den folgenden Satz:

Der NIST-Risikomanagementprozess besteht aus sieben Schritten.

**4.2**

1. Bitte nennen Sie die grundlegenden Kriterien für den Prozess des Sicherheitsrisikomanagements.

* *Kriterien für die Risikobewertung*
* *Kriterien für die Auswirkungen*
* *Kriterien für die Risikoakzeptanz*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *ISO/IEC 27005 ist Teil eines ISMS*.
* ISO/IEC 27005 ersetzt ein ISMS.
* ISO/IEC 27005 ersetzt den SDLC.

1. Bitte vervollständigen Sie den folgenden Satz:

ISO/IEC 27005 ist Teil der *ISO/IEC 2700*-Familie von Standards und beschreibt das *Informationssicherheitsrisiko*-Management.

**4.3**

1. Bitte führen Sie die Strategien für den Umgang mit Risiken im BSI-Standard 100-3 auf.

* *Risikoreduzierung durch zusätzliche Sicherheitsmaßnahmen*
* *Risikovermeidung durch Umstrukturierung*
* *Risikoakzeptanz*
* *Risikotransfer*

1. Bitte vervollständigen Sie den folgenden Satz.

Der BSI-Standard 100-3 ist ein vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichter Standard zur Risikobewertung.

**5.1**

1. Beschreiben Sie, warum Diagramme für das Threat Modeling nützlich sind.

*Diagramme helfen Analysten dabei, die Datenflüsse und die Prozesse des Geltungsbereichs besser zu verstehen.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Der Prozess der Risikobewertung sollte einer definierten Methodik folgen*.
* Risikobewertungen können auch ohne Methodik durchgeführt werden.
* Es gibt keine definierten Methoden für Risikobewertungen.

1. Bitte vervollständigen Sie den folgenden Satz.

Server sind unterstützende Assets. Die gespeicherten Daten sind primäre Assets.

**5.2**

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Black-Swan-Ereignisse haben schwerwiegende Auswirkungen.*
* Black-Swan-Ereignisse haben eine hohe Eintrittswahrscheinlichkeit.
* Black-Swan-Ereignisse haben eine hohe Eintrittswahrscheinlichkeit und schwerwiegende Auswirkungen.

1. Bitte vervollständigen Sie den folgenden Satz.

In den meisten Fällen senkt eine Risikominderungsmaßnahme für Black-Swan-Ereignisse die *Auswirkungen* des Risikos.

**5.3**

1. Erklären Sie, warum eine kontinuierliche Neubewertung wichtig ist.

*Eine kontinuierliche Neubewertung ist notwendig, um mit der sich verändernden Risikolandschaft des Unternehmens Schritt zu halten.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Kommunikation ist Teil jedes Schrittes im SEI-Paradigma*.
* Kommunikation ist nur am Ende erforderlich, um den erfolgreichen Prozess zu vermitteln.
* Kommunikation ist nur bei kritischen Ereignissen notwendig.

**6.1**

1. Beschreiben Sie den Begriff Security Champion.

*Ein Security Champion ist Teil eines Entwicklungsteams, z. B. als Entwickler:in, Produktmanager:in oder Tester:in. Champions helfen bei der Implementierung und Verbesserung der Sicherheit in ihrem Team.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Der Risikomanagementprozess muss für agile Umgebungen geändert werden*.
* Risikomanagement ist in einer agilen Umgebung nicht erforderlich.
* Das Risikomanagement ist in einer traditionellen Umgebung immer besser als in einer agilen Umgebung.

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Security Champions müssen Freiwillige sein*.
* Security Champions müssen ernannt werden.
* Es spielt keine Rolle, ob ein Security Champion sich freiwillig meldet oder als solcher ernannt wird.

**6.2**

*Eine Krise kann ein Sicherheitsvorfall oder eine andere Situation sein, die eine große Gefahr für die Organisation darstellt.*

1. Bitte markieren Sie die richtige(n) Aussage(n).

* *Eine ordnungsgemäße Dokumentation des Vorfalls kann für weitere Vorfälle hilfreich sein*.
* Die Dokumentation von Vorfällen ist ein optionaler Schritt in der Nachbearbeitungsphase.
* Die Dokumentation von Vorfällen erfolgt in der technischen Vorbereitung.

1. Bitte vervollständigen Sie den folgenden Satz.

Die aus dem Vorfall gewonnenen Erkenntnisse können genutzt werden, um die Organisation durch Empfehlungen und Richtlinien zu verbessern

**6.3**

1. Beschreiben Sie, wann eine Cyber-Versicherung sinnvoll ist.

*Eine Cyber-Versicherung ist sinnvoll, um potenzielle Schäden abzudecken, die auch dann auftreten können, wenn alle anderen Maßnahmen zur Schadensbegrenzung und Sicherheitskontrolle getroffen sind*