Fragebogen

Name: _____

Matrikelnummer: _____

Unterschrift: _____

Für den Erhalt des ISIS 12 Prüfungszertifikates muss die im Multiple-Choice-Verfahren gehaltene Prüfung erfolgreich bestanden werden.

Sprache: Deutsch

Dauer: 60 Minuten

Format: 30 Multiple-Choice-Fragen; mit vier Antwortmöglichkeiten, von denen eine, oder auch alle Antworten korrekt sein können.

min. Punkte: 20 von 30
Jede komplett richtig beantwortete Frage gibt einen Punkt. Bei falsch beantworteten Fragen gibt es 0 Punkte (aber keinen Punktabzug). Als falsch beantwortet gilt eine Frage, wenn eine falsche Antwort markiert ist, oder nicht alle richtigen angekreuzt wurden.

AUSFÜLLHILFE FÜR DEN ANTWORTBOGEN

Wie markiere ich richtig?
Für diese Prüfung erhalten Sie einen Fragebogen und einen Antwortbogen. Die Antworten sind durch entsprechende Markierungen auf dem Antwortbogen vorzunehmen. Dieser wird maschinell ausgewertet, handschriftliche Anmerkungen werden nicht berücksichtigt. Ankreuzungen auf dem Fragebogen werden nicht ausgewertet! Verwenden Sie für Ihre Markierungen ausschließlich einen schwarzen oder blauen Kugelschreiber von normaler Schriftstärke. Die Markierungen müssen deutlich und positionsgenau durch ein Kreuz erfolgen. Wenn Sie eine Ankreuzung korrigieren möchten, füllen Sie das Kästchen vollkommen aus, dadurch wird diese Markierung wie ein leeres Kästchen gewertet. Eine neuerliche Korrektur ist dann nicht mehr möglich!

Ausfüllen der Matrikelnummer:
Tragen Sie zu Beginn der Prüfung Ihre 9-stellige Matrikelnummer auf dem Antwortbogen in das dafür vorgesehene Feld ein. Übertragen Sie dann Ihre Matrikelnummer mit Kreuzen in die darunter befindlichen Kästchen, die von 0 bis 9 nummeriert sind. Die erste Spalte entspricht der 1. Ziffer Ihrer Matrikelnummer, die zweite Spalte entspricht der 2. Ziffer Ihrer Matrikelnummer usw.

Übertragen der richtigen Gruppe:
Bitte übertragen Sie die Gruppe, die Sie in der Kopfzeile des Fragebogens finden, in das entsprechende Feld auf dem Antwortbogen.

Viel Erfolg bei der Prüfung!

1) Welche der folgenden Aussagen sind bezüglich der Phase "Umsetzungsprüfung – ISIS12-Sicherheitsmaßnahmen" und der Auswahl der Bausteinen bei einem Überwachungsaudit richtig?

a) Der Auditor muss einen Baustein aus Schicht 1 wählen.
b) Der Auditor muss einen Baustein aus Schicht 3 oder 4 wählen.
c) Der Auditor hat die wirksame Umsetzung von Sicherheitsmaßnahmen aus 2 Bausteinen zu prüfen.
d) Der Auditor muss einen Baustein aus Schicht 2 wählen.

2) Welche der folgenden Aktivitäten gehören zum Schritt "Sicherheitsmaßnahmen modellieren"?

a) Zuordnung der Objekte aus der Strukturanalyse zu Sicherheitsmaßnahmen
b) Setzen eines Revisionstermins
c) Prüfung der Strukturanalyse auf Plausibilität
d) Ermittlung des Umsetzungsgrades der Sicherheitsmaßnahmen

3) Welche Objekte werden im Schritt "IT Struktur analysieren" erfasst?

a) TK-Komponenten
b) Gebäude
c) Softwarestände
d) Alle Anwendungen (Applikationen)

4) Was sagt das Maximumprinzip in der IT-Sicherheit aus?

a) Jeweils der höchste Schutzbedarf eines Objektes bezüglich Vertraulichkeit, Integrität und Verfügbarkeit wird auf das übergeordnete Objekt übertragen
b) Das Maximumprinzip wird für die Ableitung des Schutzbedarfs verwendet
c) Aufgrund des Maximumprinzips kann ein ISIS12-Zertifikat nur erteilt werden, wenn maximal möglicher Schutz der Informationssicherheit vorhanden ist
d) Nach dem Maximumprinzip müssen alle IT-Systeme immer maximal geschützt werden

5) Was sind typische Kontrollfragen zum Schritt "Sicherheitsmaßnahmen modellieren"?

a) Wurden die gefundenen IT-Objekte hinreichend mit den entsprechenden Bausteinen aus den Schichten 2-4 modelliert?
b) Wurde der aktuelle ISIS12-Katalog zur Modellierung verwendet?
c) Wurde der „Baustein B 1.12 Mobile Datenträger“ berücksichtigt?
d) Wurden die Bausteine der Schicht 1 dem Prüfplan komplett zugeordnet?

6) Welche der folgenden Servicemanagement-Prozesse werden in Schritt 5 eingeführt?

a) Wartungsprozess
b) Störungsbeseitigungsprozess
c) Änderungsprozess
d) Abnahmeprozess

7) Welche der folgenden Aussagen sind bezüglich der ISIS12-Software richtig?

a) Die ISIS12-Software richtet sich an Unternehmen, die ISIS12 einführen wollen und wird für eine schlanke und effiziente Einführung dringend empfohlen.
b) Die ISIS12-Software ist eine Web-Applikation.
c) Die ISIS12-Software ist ein Open Source Produkt und kann jederzeit von jedem heruntergeladen und verwendet werden.
d) Die ISIS12-Software ist eine Software, die Auditoren dabei hilft, bei einer Zertifizierungsprüfung die notwendigen Dokumentationen zu erstellen.

8) Welche der folgenden Aussagen bezüglich der Zertifizierung von Unternehmen sind richtig?

a) Empfehlungen des Auditors, die im Rahmen der kontinuierlichen Verbesserung geprüft wurden, aber nicht umgesetzt sind, führen im Folgeaudit immer zu einer geringfügigen Abweichung.
b) Das Erstzertifizierungs-Audit erfolgt in einer einzigen Phase. Ein Vor-Audit ist nicht vorgesehen.
c) Der Auditor muss nach Wichtigkeit entscheiden, welcher Standort von Bedeutung ist und somit bei der Planung Vorrang hat.
d) Bei Vorliegen einer schwerwiegenden Abweichung ist die Ausstellung eines ISIS12-Zertifikats möglich, wenn diese bis zum nächsten Überwachungsaudit ausgebessert wird. Ab zwei schwerwiegenden Abweichungen ist die Ausstellung nicht möglich.

9) Welche der folgenden Schritte gehören zur Phase "Entwicklung und Umsetzung ISIS12-Konzept"?

a) IT-Struktur analysieren
b) Kritische Applikationen identifizieren
c) Revision
d) Bericht erstellen

10) Was gilt für den ISIS12-Katalog?

a) Der ISIS12-Katalog wurde auf Basis der IT-Grundschutzkataloge des BSI erstellt
b) Der ISIS12-Katalog wurde auf Basis des internationalen Standards ISO/IEC 27001 erstellt
c) Der ISIS12-Katalog enthält universale Aspekte, die unabhängig von der Strukturanalyse anzuwenden sind
d) Der ISIS12-Katalog enthält empfohlene Sicherheitsmaßnahmen für Infrastruktur, IT-Systeme, Netze und Anwendungen

11) In welchen der folgenden Fälle liegt eine Verletzung der Integrität vor?

a) Auf ein Dokument wurde unberechtigterweise zugegriffen.
b) Einem Dokument wurden unberechtigterweise weitere Informationen hinzugefügt.
c) Informationen in einem Dokument wurden unberechtigterweise umgeordnet, also in ihrer Reihenfolge verändert.
d) Zu einem Dokument liegt keine Datensicherung vor.

12) Welche der folgenden Schritte sind laut ISIS12 direkte Vorgänger und Nachfolger?

a) Zuerst die IT-Dokumentationsstruktur festlegen und dann den IT-Service-Management-Prozesse einführen
b) Zuerst das Informationssicherheitsteam aufbauen und dann die IT-Dokumentationsstruktur festlegen
c) Zuerst die Sicherheitsmaßnahmen modellieren und dann die IT-Service-Mananagement-Prozesse einführen
d) Zuerst die IT-Service-Management-Prozesse einführen und dann die Mitarbeiter instruieren

13) Welche der folgenden Aussagen sind hinsichtlich des Notfallhandbuches richtig?

a) Das Notfallhandbuch muss nur nach einem fehlgeschlagenen Notfalltest akutalisiert werden.
b) Das Notfallhandbuch darf nur in Papierform vorliegen
c) Notfallhandbücher sind mindestens halbjährlich einem Review zu unterziehen, und dieser Vorgang ist entsprechend zu dokumentieren.
d) Ein Grund, ein Notfallhandbuch anzupassen ist,wenn sich gesetzliche und andere Vorschriften sowie Verträge mit Kunden ändern.

14) Welche Eigenschaften von Informationen sollen im Rahmen der Informationssicherheit aufrechterhalten werden?

a) Integrität
b) Stabilität
c) Vertraulichkeit
d) Souveränität

15) Was trifft auf den PDCA-Zyklus zu?

a) PDCA ist ein grundlegender Ansatz zur kontinuierlichen Verbesserung
b) PDCA beschreibt die Eigenschaften von Information, die im Rahmen der Informationssicherheit aufrechterhalten werden sollen
c) Die Struktur von ISIS12 ist, zumindest in Teilen, an dem PDCA-Ansatz ausgerichtet
d) PDCA beschreibt die Prinzipien der Informationssicherheit

16) Welche der folgenden Aktivitäten gehören zum Schritt "IT-Struktur analysieren"?

a) Modellierung von Sicherheitsmaßnahmen für Applikationen
b) Zuordnung von IT-Systemen zu Applikationen
c) Untersuchung, welche Sicherheitsmaßnahmen aus dem ISIS12-Katalog bezogen auf die IT-Zielobjekte noch nicht oder nur teilweise wirksam umgesetzt wurden
d) Modellierung von Sicherheitsmaßnahmen für IT-Systeme

17) Was ist bezüglich des ISIS12-Zertifikats korrekt?

a) Der Geltungsbereich des Informationssicherheits-Managementsystems ist auf dem Zertifikat angegeben
b) Die Gültigkeit des Zertifikats beträgt 1 Jahr
c) Das Zertifikat wird vom Bayerischen IT-Sicherheitscluster ausgestellt
d) Die Gültigkeit des Zertifikats beträgt 2 Jahre

18) Welche der folgenden Aussagen sind bzgl. der Unternehmensleitlinie korrekt?

a) Die Unternehmensleitlinie beschreibt die Sicherheitsziele der Organisation
b) Die Unternehmensleitlinie definiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit
c) Die Mitarbeiter müssen die Unternehmensleitung zur Einhaltung der Leitlinie motivieren
d) Die Unternehmensleitlinie ist das zentrale Strategiepapier zum Thema Informationssicherheit

19) Welche der folgenden Rahmenwerke, Standards oder Standardfamilen befassen sich schwerpunktmäßig mit IT- oder Informationssicherheit (oder werden als Standard für IT- oder Informationssicherheit bezeichnet)?

a) ISO/IEC 27000
b) ISO/IEC 15408 (Common Criteria)
c) BSI IT-Grundschutz
d) ISO 9000

20) Welche Aussagen zu ISIS12 treffen zu?

a) ISIS12 ist ein zertifizierungsfähiges Managementsystem für Informationssicherheit
b) ISIS12 gibt dem Anwender die 12 wichtigsten Sicherheitsmaßnahmen an die Hand
c) Ein Informationssicherheitsmanagement nach ISIS12 muss zertifiziert werden
d) Ein Informationssicherheitsmanagementsystem nach ISIS12 endet mit Schritt 12

21) Welche Personen müssen laut ISIS12 Standard dem Informationssicherheitsteam (Kern-Team) angehören?

a) Informationssicherheitsbeauftragter (ISB)
b) ein Mitglied aus der Geschäftsführung
c) Vertreter der Lieferanten
d) Vertreter der Arbeitnehmer

22) Welche zusätzlichen generischen Oberbegriffe definiert das Bundesamt für Sicherheit in der Informationstechnik neben den drei Grundwerten Vertraulichkeit, Verfügbarkeit und Integrität?

a) Authentizität
b) Zuverlässigkeit
c) Verbindlichkeit
d) Governance

23) Was sind die typischen Kontrollfragen für den Schritt "Leitlinie erstellen"?

a) Die Unternehmensrichtlinie wurde vom IT-Sicherheitsteam bestätigt.
b) Hat die Unternehmensleitung die Leitlinie unterzeichnet?
c) Die Unternehmensrichtlinie wurde an alle Kunden verteilt.
d) Wurde der Stellenwert der Informationssicherheit bezogen auf die spezifischen Unternehmensziele dargestellt?

24) Welche der folgenden Aussagen im Zusammenhang mit Vertraulichkeit und Integrität von Informationen sind korrekt?

a) Ein angemessenes Niveau an Vertraulichkeit und Integrität lässt sich nur durch den Einsatz von Verschlüsselung und durch digitale Signaturen erreichen.
b) Vertraulichkeit und Integrität sind Synonyme.
c) Integrität bedeutet Schutz vor Manipulation der Richtigkeit oder Vollständigkeit von Informationen.
d) Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen gegenüber unbefugten Personen.

25) Welche Eigenschaften haben Überwachungsaudits bei einem nach ISIS12 zertifizierten Unternehmen?

a) Es findet ein Überwachungsaudit pro Jahr statt
b) Überwachungsaudits müssen von ISIS12-lizenzierten Auditoren durchgeführt werden
c) Überwachungsaudits sind unabhängig vom Zertifizierungsprozess
d) Die Anzahl der Überwachungsaudits wird im Auditbericht der Erstzertifizierung festgelegt

26) Welche der folgenden Aussagen sind hinsichtlich des IT-Betriebshandbuchs richtig?

a) Das IT-Betriebshandbuch ist vertraulich
b) Das IT-Betriebshandbuch gehört zu den Rahmendokumenten von ISIS12
c) Verantwortlichkeiten für Aktualität und Freigabe des IT-Betriebshandbuchs müssen klar geregelt sein
d) Das IT-Betriebshandbuch muss in Papierform vorliegen

27) Welche der folgenden Themen sind Inhalte der Unternehmensleitlinie?

a) Prozessbeschreibung zur Änderung
b) Leitaussagen zur Durchsetzung und Erfolgskontrolle
c) Unternehmensspezifische Sicherheitsziele
d) Organisationsstruktur für die Umsetzung des Informationssicherheitsprozesses

28) Welche Aussagen treffen auf Baustein 1.5 Datenschutz zu?:

a) Der Baustein basiert auf Regelungen der DS-GVO, des BDSG und Checklisten der Aufsichtsbehörden
b) Datenschutz ist kein Bestandteil der IT-Compliance
c) Der Baustein hat keine Relevanz für das ISMS und ist optional.
d) Der Baustein basiert auf Baustein 1.5 Datenschutz des BSI.

29) Welche der folgenden Schritte gehören zur Phase "Festlegung der Aufbau- und Ablauforganisation"?

a) Umsetzen
b) IT-Service-Management-Prozesse einführen
c) Mitarbeiter sensibilisieren
d) Leitlinie erstellen

30) Welche der folgenden Schritte gehören zur "Initialisierungsphase"?

a) Informationssicherheitsteam aufbauen
b) Mitarbeiter instruieren
c) Mitarbeiter sensibilisieren
d) Revision einleiten