

- 1) Welche der folgenden Aussagen sind bezüglich der Phase "Umsetzungsprüfung – ISIS12-Sicherheitsmaßnahmen" und der Auswahl der Bausteine bei einem Überwachungsaudit richtig?
 - a) **Der Auditor muss einen Baustein aus Schicht 1 wählen. (100%)**
 - b) **Der Auditor muss einen Baustein aus Schicht 3 oder 4 wählen. (100%)**
 - c) **Der Auditor hat die wirksame Umsetzung von Sicherheitsmaßnahmen aus 2 Bausteinen zu prüfen. (100%)**
 - d) Der Auditor muss einen Baustein aus Schicht 2 wählen. (0%)

- 2) Welche der folgenden Aktivitäten gehören zum Schritt "Sicherheitsmaßnahmen modellieren"?
 - a) **Zuordnung der Objekte aus der Strukturanalyse zu Sicherheitsmaßnahmen (100%)**
 - b) **Setzen eines Revisionstermins (100%)**
 - c) **Prüfung der Strukturanalyse auf Plausibilität (100%)**
 - d) Ermittlung des Umsetzungsgrades der Sicherheitsmaßnahmen (0%)

- 3) Welche Objekte werden im Schritt "IT Struktur analysieren" erfasst?
 - a) **TK-Komponenten (100%)**
 - b) **Gebäude (100%)**
 - c) Softwarestände (0%)
 - d) Alle Anwendungen (Applikationen) (0%)

- 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 (100%)**
 - b) **Das Maximumprinzip wird für die Ableitung des Schutzbedarfs verwendet (100%)**
 - c) Aufgrund des Maximumprinzips kann ein ISIS12-Zertifikat nur erteilt werden, wenn maximal möglicher Schutz der Informationssicherheit vorhanden ist (0%)
 - d) Nach dem Maximumprinzip müssen alle IT-Systeme immer maximal geschützt werden (0%)

- 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? (100%)**
 - b) **Wurde der aktuelle ISIS12-Katalog zur Modellierung verwendet? (100%)**
 - c) **Wurde der „Baustein B 1.12 Mobile Datenträger“ berücksichtigt? (100%)**
 - d) **Wurden die Bausteine der Schicht 1 dem Prüfplan komplett zugeordnet? (100%)**

- 6) Welche der folgenden Servicemanagement-Prozesse werden in Schritt 5 eingeführt?
 - a) **Wartungsprozess (100%)**
 - b) **Störungsbeseitigungsprozess (100%)**
 - c) **Änderungsprozess (100%)**
 - d) Abnahmeprozess (0%)

- 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. (100%)**
 - b) **Die ISIS12-Software ist eine Web-Applikation. (100%)**
 - c) Die ISIS12-Software ist ein Open Source Produkt und kann jederzeit von jedem heruntergeladen und verwendet werden. (0%)
 - d) Die ISIS12-Software ist eine Software, die Auditoren dabei hilft, bei einer Zertifizierungsprüfung die notwendigen Dokumentationen zu erstellen. (0%)
- 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. (0%)
 - b) **Das Erstzertifizierungs-Audit erfolgt in einer einzigen Phase. Ein Vor-Audit ist nicht vorgesehen. (100%)**
 - c) **Der Auditor muss nach Wichtigkeit entscheiden, welcher Standort von Bedeutung ist und somit bei der Planung Vorrang hat. (100%)**
 - 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. (0%)
- 9) Welche der folgenden Schritte gehören zur Phase "Entwicklung und Umsetzung ISIS12-Konzept"?
- a) **IT-Struktur analysieren (100%)**
 - b) **Kritische Applikationen identifizieren (100%)**
 - c) **Revision (100%)**
 - d) Bericht erstellen (0%)
- 10) Was gilt für den ISIS12-Katalog?
- a) **Der ISIS12-Katalog wurde auf Basis der IT-Grundschutzkataloge des BSI erstellt (100%)**
 - b) **Der ISIS12-Katalog wurde auf Basis des internationalen Standards ISO/IEC 27001 erstellt (100%)**
 - c) **Der ISIS12-Katalog enthält universale Aspekte, die unabhängig von der Strukturanalyse anzuwenden sind (100%)**
 - d) **Der ISIS12-Katalog enthält empfohlene Sicherheitsmaßnahmen für Infrastruktur, IT-Systeme, Netze und Anwendungen (100%)**
- 11) In welchen der folgenden Fälle liegt eine Verletzung der Integrität vor?
- a) Auf ein Dokument wurde unberechtigterweise zugegriffen. (0%)
 - b) **Einem Dokument wurden unberechtigterweise weitere Informationen hinzugefügt. (100%)**
 - c) **Informationen in einem Dokument wurden unberechtigterweise umgeordnet, also in ihrer Reihenfolge verändert. (100%)**
 - d) Zu einem Dokument liegt keine Datensicherung vor. (0%)

- 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 (100%)**
 - b) **Zuerst das Informationssicherheitsteam aufbauen und dann die IT-Dokumentationsstruktur festlegen (100%)**
 - c) Zuerst die Sicherheitsmaßnahmen modellieren und dann die IT-Service-Management-Prozesse einführen (0%)
 - d) Zuerst die IT-Service-Management-Prozesse einführen und dann die Mitarbeiter instruieren (0%)
- 13) Welche der folgenden Aussagen sind hinsichtlich des Notfallhandbuches richtig?
- a) Das Notfallhandbuch muss nur nach einem fehlgeschlagenen Notfalltest aktualisiert werden. (0%)
 - b) Das Notfallhandbuch darf nur in Papierform vorliegen (0%)
 - c) Notfallhandbücher sind mindestens halbjährlich einem Review zu unterziehen, und dieser Vorgang ist entsprechend zu dokumentieren. (0%)
 - d) **Ein Grund, ein Notfallhandbuch anzupassen ist, wenn sich gesetzliche und andere Vorschriften sowie Verträge mit Kunden ändern. (100%)**
- 14) Welche Eigenschaften von Informationen sollen im Rahmen der Informationssicherheit aufrechterhalten werden?
- a) **Integrität (100%)**
 - b) Stabilität (0%)
 - c) **Vertraulichkeit (100%)**
 - d) Souveränität (0%)
- 15) Was trifft auf den PDCA-Zyklus zu?
- a) **PDCA ist ein grundlegender Ansatz zur kontinuierlichen Verbesserung (100%)**
 - b) PDCA beschreibt die Eigenschaften von Information, die im Rahmen der Informationssicherheit aufrechterhalten werden sollen (0%)
 - c) **Die Struktur von ISIS12 ist, zumindest in Teilen, an dem PDCA-Ansatz ausgerichtet (100%)**
 - d) PDCA beschreibt die Prinzipien der Informationssicherheit (0%)
- 16) Welche der folgenden Aktivitäten gehören zum Schritt "IT-Struktur analysieren"?
- a) Modellierung von Sicherheitsmaßnahmen für Applikationen (0%)
 - b) **Zuordnung von IT-Systemen zu Applikationen (100%)**
 - c) Untersuchung, welche Sicherheitsmaßnahmen aus dem ISIS12-Katalog bezogen auf die IT-Zielobjekte noch nicht oder nur teilweise wirksam umgesetzt wurden (0%)
 - d) Modellierung von Sicherheitsmaßnahmen für IT-Systeme (0%)
- 17) Was ist bezüglich des ISIS12-Zertifikats korrekt?
- a) **Der Geltungsbereich des Informationssicherheits-Managementsystems ist auf dem Zertifikat angegeben (100%)**
 - b) Die Gültigkeit des Zertifikats beträgt 1 Jahr (0%)
 - c) Das Zertifikat wird vom Bayerischen IT-Sicherheitscluster ausgestellt (0%)
 - d) Die Gültigkeit des Zertifikats beträgt 2 Jahre (0%)

- 18) Welche der folgenden Aussagen sind bzgl. der Unternehmensleitlinie korrekt?
- a) **Die Unternehmensleitlinie beschreibt die Sicherheitsziele der Organisation (100%)**
 - b) Die Unternehmensleitlinie definiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (0%)
 - c) Die Mitarbeiter müssen die Unternehmensleitung zur Einhaltung der Leitlinie motivieren (0%)
 - d) **Die Unternehmensleitlinie ist das zentrale Strategiepapier zum Thema Informationssicherheit (100%)**
- 19) Welche der folgenden Rahmenwerke, Standards oder Standardfamilien befassen sich schwerpunktmäßig mit IT- oder Informationssicherheit (oder werden als Standard für IT- oder Informationssicherheit bezeichnet)?
- a) **ISO/IEC 27000 (100%)**
 - b) **ISO/IEC 15408 (Common Criteria) (100%)**
 - c) **BSI IT-Grundschutz (100%)**
 - d) ISO 9000 (0%)
- 20) Welche Aussagen zu ISIS12 treffen zu?
- a) **ISIS12 ist ein zertifizierungsfähiges Managementsystem für Informationssicherheit (100%)**
 - b) ISIS12 gibt dem Anwender die 12 wichtigsten Sicherheitsmaßnahmen an die Hand (0%)
 - c) Ein Informationssicherheitsmanagement nach ISIS12 muss zertifiziert werden (0%)
 - d) Ein Informationssicherheitsmanagementsystem nach ISIS12 endet mit Schritt 12 (0%)
- 21) Welche Personen müssen laut ISIS12 Standard dem Informationssicherheitsteam (Kern-Team) angehören?
- a) **Informationssicherheitsbeauftragter (ISB) (100%)**
 - b) ein Mitglied aus der Geschäftsführung (0%)
 - c) Vertreter der Lieferanten (0%)
 - d) Vertreter der Arbeitnehmer (0%)
- 22) Welche zusätzlichen generischen Oberbegriffe definiert das Bundesamt für Sicherheit in der Informationstechnik neben den drei Grundwerten Vertraulichkeit, Verfügbarkeit und Integrität?
- a) **Authentizität (100%)**
 - b) **Zuverlässigkeit (100%)**
 - c) **Verbindlichkeit (100%)**
 - d) Governance (0%)
- 23) Was sind die typischen Kontrollfragen für den Schritt "Leitlinie erstellen"?
- a) Die Unternehmensrichtlinie wurde vom IT-Sicherheitsteam bestätigt. (0%)
 - b) **Hat die Unternehmensleitung die Leitlinie unterzeichnet? (100%)**
 - c) Die Unternehmensrichtlinie wurde an alle Kunden verteilt. (0%)
 - d) **Wurde der Stellenwert der Informationssicherheit bezogen auf die spezifischen Unternehmensziele dargestellt? (100%)**

- 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. (0%)
 - b) Vertraulichkeit und Integrität sind Synonyme. (0%)
 - c) Integrität bedeutet Schutz vor Manipulation der Richtigkeit oder Vollständigkeit von Informationen. (100%)**
 - d) Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen gegenüber unbefugten Personen. (100%)**
- 25) Welche Eigenschaften haben Überwachungsaudits bei einem nach ISIS12 zertifizierten Unternehmen?
- a) Es findet ein Überwachungsaudit pro Jahr statt (100%)**
 - b) Überwachungsaudits müssen von ISIS12-lizenzierten Auditoren durchgeführt werden (100%)**
 - c) Überwachungsaudits sind unabhängig vom Zertifizierungsprozess (0%)
 - d) Die Anzahl der Überwachungsaudits wird im Auditbericht der Erstzertifizierung festgelegt (0%)
- 26) Welche der folgenden Aussagen sind hinsichtlich des IT-Betriebshandbuchs richtig?
- a) Das IT-Betriebshandbuch ist vertraulich (100%)**
 - b) Das IT-Betriebshandbuch gehört zu den Rahmendokumenten von ISIS12 (100%)**
 - c) Verantwortlichkeiten für Aktualität und Freigabe des IT-Betriebshandbuchs müssen klar geregelt sein (100%)**
 - d) Das IT-Betriebshandbuch muss in Papierform vorliegen (0%)
- 27) Welche der folgenden Themen sind Inhalte der Unternehmensleitlinie?
- a) Prozessbeschreibung zur Änderung (0%)
 - b) Leitaussagen zur Durchsetzung und Erfolgskontrolle (100%)**
 - c) Unternehmensspezifische Sicherheitsziele (100%)**
 - d) Organisationsstruktur für die Umsetzung des Informationssicherheitsprozesses (100%)**
- 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 (100%)**
 - b) Datenschutz ist kein Bestandteil der IT-Compliance (0%)
 - c) Der Baustein hat keine Relevanz für das ISMS und ist optional. (0%)
 - d) Der Baustein basiert auf Baustein 1.5 Datenschutz des BSI. (0%)
- 29) Welche der folgenden Schritte gehören zur Phase "Festlegung der Aufbau- und Ablauforganisation"?
- a) Umsetzen (0%)
 - b) IT-Service-Management-Prozesse einführen (100%)**
 - c) Mitarbeiter sensibilisieren (0%)
 - d) Leitlinie erstellen (0%)

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

- a) Informationssicherheitsteam aufbauen (0%)
- b) Mitarbeiter instruieren (0%)
- c) Mitarbeiter sensibilisieren (100%)**
- d) Revision einleiten (0%)