1) Welche der folgenden Themen sind Inhalte der Unternehmensleitlinie?

a) Organisationsstruktur für die Umsetzung des Informationssicherheitsprozesses (100%)
b) Leitaussagen zur Durchsetzung und Erfolgskontrolle (100%)
c) Unternehmensspezifische Sicherheitsziele (100%)
d) Prozessbeschreibung zur Änderung (0%)

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

a) IT-Struktur analysieren (100%)
b) Kritische Applikationen identifizieren (100%)
c) Bericht erstellen (0%)
d) Revision (100%)

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

a) Untersuchung, welche Sicherheitsmaßnahmen aus dem ISIS12-Katalog bezogen auf die IT-Zielobjekte noch nicht oder nur teilweise wirksam umgesetzt wurden (0%)
b) Modellierung von Sicherheitsmaßnahmen für Applikationen (0%)
c) Zuordnung von IT-Systemen zu Applikationen (100%)
d) Modellierung von Sicherheitsmaßnahmen für IT-Systeme (0%)

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

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

5) 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) 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%)
c) Der Auditor muss nach Wichtigkeit entscheiden, welcher Standort von Bedeutung ist und somit bei der Planung Vorrang hat. (100%)
d) Das Erstzertifizierungs-Audit erfolgt in einer einzigen Phase. Ein Vor-Audit ist nicht vorgesehen. (100%)

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

a) Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen gegenüber unbefugten Personen (100%)
b) Vertraulichkeit und Integrität sind Synonyme (0%)
c) Ein angemessenes Niveau an Vertraulichkeit und Integrität lässt sich nur durch den Einsatz von Verschlüsselung und durch digitale Signaturen erreichen (0%)
d) Integrität bedeutet Schutz vor Manipulation der Richtigkeit oder Vollständigkeit von Informationen (100%)

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

a) Das Maximumprinzip wird für die Ableitung des Schutzbedarfs verwendet (100%)
b) Jeweils der höchste Schutzbedarf eines Objektes bezüglich Vertraulichkeit, Integrität und Verfügbarkeit wird auf das übergeordnete Objekt übertragen (100%)
c) Nach dem Maximumprinzip müssen alle IT-Systeme immer maximal geschützt werden (0%)
d) Aufgrund des Maximumprinzips kann ein ISIS12-Zertifikat nur erteilt werden, wenn maximal möglicher Schutz der Informationssicherheit vorhanden ist (0%)

8) 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%)

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

a) ein Mitglied aus der Geschäftsführung (0%)
b) Informationssicherheitsbeauftragter (ISB) (100%)
c) Vertreter der Arbeitnehmer (0%)
d) Vertreter der Lieferanten (0%)

10) Welche Aussagen zu ISIS12 treffen zu?

a) ISIS12 gibt dem Anwender die 12 wichtigsten Sicherheitsmaßnahmen an die Hand (0%)
b) Ein Informationssicherheitsmanagement nach ISIS12 muss zertifiziert werden (0%)
c) ISIS12 ist ein zertifizierungsfähiges Managementsystem für Informationssicherheit (100%)
d) Ein Informationssicherheitsmanagementsystem nach ISIS12 endet mit Schritt 12 (0%)

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

a) TK-Komponenten (100%)
b) Softwarestände (0%)
c) Alle Anwendungen (Applikationen) (0%)
d) Gebäude (100%)

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

a) Setzen eines Revisionstermins (100%)
b) Zuordnung der Objekte aus der Strukturanalyse zu Sicherheitsmaßnahmen (100%)
c) Prüfung der Strukturanalyse auf Plausibilität (100%)
d) Ermittlung des Umsetzungsgrades der Sicherheitsmaßnahmen (0%)

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

a) Vertraulichkeit (100%)
b) Stabilität (0%)
c) Souveränität (0%)
d) Integrität (100%)

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

a) Das IT-Betriebshandbuch muss in Papierform vorliegen (0%)
b) Das IT-Betriebshandbuch gehört zu den Rahmendokumenten von ISIS12 (100%)
c) Das IT-Betriebshandbuch ist vertraulich (100%)
d) Verantwortlichkeiten für Aktualität und Freigabe des IT-Betriebshandbuchs müssen klar geregelt sein (100%)

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

a) Die Unternehmensrichtlinie wurde an alle Kunden verteilt. (0%)
b) Wurde der Stellenwert der Informationssicherheit bezogen auf die spezifischen Unternehmensziele dargestellt? (100%)
c) Die Unternehmensrichtlinie wurde vom IT-Sicherheitsteam bestätigt. (0%)
d) Hat die Unternehmensleitung die Leitlinie unterzeichnet? (100%)

16) Was ist bezüglich des ISIS12-Zertifikats korrekt?

a) Die Gültigkeit des Zertifikats beträgt 1 Jahr (0%)
b) Der Geltungsbereich des Informationssicherheits-Managementsystems ist auf dem Zertifikat angegeben (100%)
c) Das Zertifikat wird vom Bayerischen IT-Sicherheitscluster ausgestellt (0%)
d) Die Gültigkeit des Zertifikats beträgt 2 Jahre (0%)

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

a) Überwachungsaudits müssen von ISIS12-lizenzierten Auditoren durchgeführt werden (100%)
b) Überwachungsaudits sind unabhängig vom Zertifizierungsprozess (0%)
c) Die Anzahl der Überwachungsaudits wird im Auditbericht der Erstzertifizierung festgelegt (0%)
d) Es findet ein Überwachungsaudit pro Jahr statt (100%)

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

a) Zuverlässigkeit (100%)
b) Governance (0%)
c) Verbindlichkeit (100%)
d) Authentizität (100%)

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

a) Wurde der aktuelle ISIS12-Katalog zur Modellierung verwendet? (100%)
b) Wurden die Bausteine der Schicht 1 dem Prüfplan komplett zugeordnet? (100%)
c) Wurde der „Baustein B 1.12 Mobile Datenträger“ berücksichtigt? (100%)
d) Wurden die gefundenen IT-Objekte hinreichend mit den entsprechenden Bausteinen aus den Schichten 2-4 modelliert? (100%)

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

a) Ein Grund, ein Notfallhandbuch anzupassen ist,wenn sich gesetzliche und andere Vorschriften sowie Verträge mit Kunden ändern. (100%)
b) Notfallhandbücher sind mindestens halbjährlich einem Review zu unterziehen, und dieser Vorgang ist entsprechend zu dokumentieren. (0%)
c) Das Notfallhandbuch muss nur nach einem fehlgeschlagenen Notfalltest akutalisiert werden. (0%)
d) Das Notfallhandbuch darf nur in Papierform vorliegen (0%)

21) Was trifft auf den PDCA-Zyklus zu?

a) PDCA beschreibt die Eigenschaften von Information, die im Rahmen der Informationssicherheit aufrechterhalten werden sollen (0%)
b) Die Struktur von ISIS12 ist, zumindest in Teilen, an dem PDCA-Ansatz ausgerichtet (100%)
c) PDCA ist ein grundlegender Ansatz zur kontinuierlichen Verbesserung (100%)
d) PDCA beschreibt die Prinzipien der Informationssicherheit (0%)

22) 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 15408 (Common Criteria) (100%)
b) ISO/IEC 27000 (100%)
c) BSI IT-Grundschutz (100%)
d) ISO 9000 (0%)

23) 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 2 wählen. (0%)
b) Der Auditor hat die wirksame Umsetzung von Sicherheitsmaßnahmen aus 2 Bausteinen zu prüfen. (100%)
c) Der Auditor muss einen Baustein aus Schicht 1 wählen. (100%)
d) Der Auditor muss einen Baustein aus Schicht 3 oder 4 wählen. (100%)

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

a) Die Mitarbeiter müssen die Unternehmensleitung zur Einhaltung der Leitlinie motivieren (0%)
b) Die Unternehmensleitlinie definiert die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (0%)
c) Die Unternehmensleitlinie ist das zentrale Strategiepapier zum Thema Informationssicherheit (100%)
d) Die Unternehmensleitlinie beschreibt die Sicherheitsziele der Organisation (100%)

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

a) Zuerst die Sicherheitsmaßnahmen modellieren und dann die IT-Service-Mananagement-Prozesse einführen (0%)
b) Zuerst die IT-Dokumentationsstruktur festlegen und dann den IT-Service-Management-Prozesse einführen (100%)
c) Zuerst die IT-Service-Management-Prozesse einführen und dann die Mitarbeiter instruieren (0%)
d) Zuerst das Informationssicherheitsteam aufbauen und dann die IT-Dokumentationsstruktur festlegen (100%)

26) 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 empfohlene Sicherheitsmaßnahmen für Infrastruktur, IT-Systeme, Netze und Anwendungen (100%)
d) Der ISIS12-Katalog enthält universale Aspekte, die unabhängig von der Strukturanalyse anzuwenden sind (100%)

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

a) Mitarbeiter sensibilisieren (0%)
b) Umsetzen (0%)
c) Leitlinie erstellen (0%)
d) IT-Service-Management-Prozesse einführen (100%)

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

a) Einem Dokument wurden unberechtigterweise weitere Informationen hinzugefügt. (100%)
b) Informationen in einem Dokument wurden unberechtigterweise umgeordnet, also in ihrer Reihenfolge verändert. (100%)
c) Zu einem Dokument liegt keine Datensicherung vor. (0%)
d) Auf ein Dokument wurde unberechtigterweise zugegriffen. (0%)

29) Welche der folgenden Aussagen sind bezüglich der Phase Dokumentenprüfung bei der Zertifizierung von Unternehmen richtig?

a) Bei der Dokumentenprüfung prüft der Auditor, ob die Zertifizierungsfähigkeit des Antragstellers prinzipiell gegeben ist. (100%)
b) Bei der Dokumentenprüfung werden dem Auditor die im Anhang A2 aufgeführten Referenzdokumente zur Verfügung gestellt. (100%)
c) Bei der Dokumentenprüfung prüft der Auditor den eingereichten Antrag auf Vollständigkeit und Konsistenz. (0%)
d) Die Einsicht in die Dokumente bei der Dokumentenprüfung erfolgt vor Ort. (100%)

30) Welche der folgenden Aussagen sind bezüglich der Phase "Umsetzungsprüfung – ISIS12-Sicherheitsmaßnahmen" und der Auswahl der Bausteinen bei einem Erst- oder Re-Zertifizierungsaudit richtig?

a) Die geprüften Bausteine und die Prüfungsergebnisse werden vom Auditor im Audit-Bericht dokumentiert. (100%)

b) Der zertifiziete Berater erklärt per Unterschrift im Audit-Bericht, dass die modellierten ISIS12-Sicherheitsmaßnahmen, die nicht geprüft worden sind, wirksam umgesetzt wurden. (0%)

c) Der Auditor hat die wirksame Umsetzung von Sicherheitsmaßnahmen aus acht Bausteinen (2 pro Schicht 1-4) zu prüfen. (0%)

d) Der Auditor muss aus Schicht 2 den Baustein 2.3 und drei weitere Bausteine auswählen. (0%)