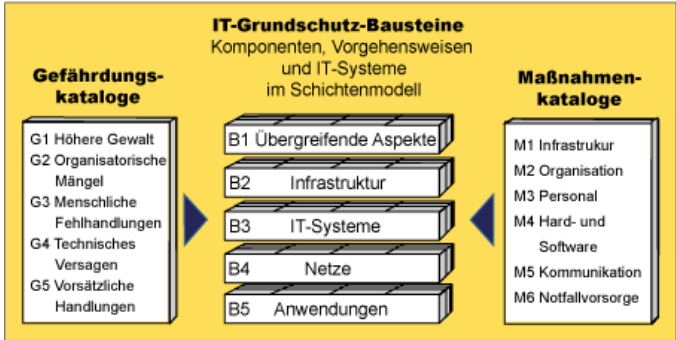





Nr	Frage	Antwort
1	Nenne die drei Schutzziele des IT-Grundschatzes:	Verfügbarkeit Vertraulichkeit Integrität (= die Korrektheit der Informationen)
2	Erkläre die Verletzung der 3 Schutzziele der Informationssicherheit mithilfe eines Beispiels:	<ul style="list-style-type: none"> <li>• Wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (→ Verletzung der Vertraulichkeit),</li> <li>• Wenn die Korrektheit der Informationen und der Funktionsweise von Systemen nicht mehr gegeben ist (→ Verletzung der Integrität),</li> <li>• Wenn autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (→ Verletzung der Verfügbarkeit).</li> </ul>
3	Erklären Sie die 7 Schutzziele der Informationssicherheit aus ISO 2700-0	<p><b>Verfügbarkeit</b>→ bedeutet dass ein berechtigtes Objekt auf verlangen die Nutzbarkeit und die Zugänglichkeit erhält.</p> <p><b>Vertraulichkeit</b>→ Bedeutet dass Informationen unberechtigten Objekten nicht verfügbar gemacht werden.</p> <p><b>Integrität</b>→ Informationen müssen richtig und vollständig sein.</p> <p><b>Authentizität</b>→ gewährleistet die Echtheit von Information und Identität. Es wird unterschieden:</p> <ul style="list-style-type: none"> <li>• Authentifizierung: Ich selbst weise mich aus(durch Wissen, Besitz etc.)</li> <li>• Authentisierend: Ein dritter weißt mich aus</li> </ul> <p><b>Zurechenbarkeit</b>→ Ich trage die Verantwortung und Haftung der Informationswerte</p> <p><b>Nicht-Abstreitbarkeit</b>→ bedeutet dass das senden/empfangen von Daten nicht abgestritten werden kann(proof of delivery-proof of origins)</p> <p><b>Verlässlichkeit</b>→ es wird wirklich immer gemacht</p> <p>Die 7 Punkte müssen aufrecht erhalten werden!</p>

4	was ist der Unterschied zwischen Informativ und Normativ?	Informativ ist eine Art „good practise“ und Normativ ist eine Richtlinie an die ich mich halten muss
5	Erkläre Informationssicherheitsmanagement	In diesem werden die notwendigen Planungs und Lenkungsarbeiten beschrieben welche erforderlich sind um einen durchdachten und planmäßigen Informationssicherheitsprozess aufzubauen. Dieser wird im BSI-Standard 100-1 beschrieben. Besser: Ist ein Regelwerk und den damit verbundenen Ressourcen um einen oder mehreren prozess zu implementieren(das ist recursiv) Sammlung von Prozessen und metaprozessen + ressourcen ist ein managementsystem.
6	Nenne die 5 Gefährdungskataloge	G1: höhere Gewalten G2: Organisatorische Mängel G3: Menschliche Fehlerhandlungen G4: Technisches versagen G5: Vorsätzliche Handlungen

7	Nenne die 6 Maßnahmenkataloge und beschreibe sie in einem kurzen Satz:	M1: Infrastruktur: M2: Organisation: M3: Personal M4: Hard-Software M5 Kommunikation M6: Notfallversorgung
8	Nenne die Phasen des Sicherheitsprozesses	1.) Initiierung des Sicherheitsprozesses a.) Verantwortung der Leitungsebene b.) Konzept und Planung c.) Erstellung einer Leitlinie zur Informationssicherheit d.)Aufbau einer Organisationssicherheit e.) Bereitstellung von Ressourcen f.) Einbindung aller Mitarbeiter 2.) Erstellung einer Sicherheitskonzeption → Nach der Erstellung dieses Konzepts sollte es nochmals geprüft werden und durch schritt 1.) durchlaufen- erst wenn es zufriedenstellend ist wird fortgeführt. 3.) Umsetzung der Sicherheitskonzeption 4.) Aufrechterhaltung der Verbesserung
9	Nenne die 2 wesentlichen Bestandteile des IT-Grundschutzes:	<ul style="list-style-type: none"> <li>• BSI-Standards zum IT-Grundschutz→ enthalten Empfehlungen für Organisatorisches und methodisches Vorgehen</li> </ul>

		<ul style="list-style-type: none"> <li>IT-Grundschutzkataloge- mit ihrer Hilfe können die in den BSI-Standards formulierten Empfehlungen konkretisiert und umgesetzt werden. (<i>Gefährdungskataloge, IT-Grundschutz-Baustein-Kataloge, Maßnahmenkataloge</i>)</li> </ul> 
10	Erkläre die Gefährdungskataloge:	In den Gefährdungs-Katalogen sind wesentliche Gefährdungen für die Informationssicherheit zusammengestellt und entlang der möglichen Ursachen "Höhere Gewalt", "Organisatorische Mängel", "Menschliche Fehlhandlungen", "Technisches Versagen" und "Vorsätzliche Handlungen" gegliedert.
11	Erkläre die Maßnahmenkataloge	<p>Die Maßnahmen-Kataloge enthalten detailliert beschriebene, in der Praxis bewährte und meist kostengünstige Maßnahmen, mit denen Sie den möglichen Gefährdungen für die Informationssicherheit wirksam begegnen können.</p> <p>Sie sind in die Bereiche "Infrastruktur", "Organisation", "Personal", "Hardware und Software", "Kommunikation" und "Notfallvorsorge" gegliedert.</p>
12	Erkläre die Bausteinkataloge	<p>Die Baustein-Kataloge bilden die Klammer zwischen Gefährdungs- und Maßnahmen-Katalogen. Sie sind in die Schichten "Übergreifende Aspekte", "Infrastruktur", "IT-Systeme", "Netze" und "Anwendungen" sortiert. Ein Baustein beschreibt jeweils einen bestimmten Teilaspekt der Informationssicherheit. Dies kann ein technisches System, ein zu regelnder organisatorischer Sachverhalt oder eine Anwendung sein. Jeder Baustein enthält neben einer kurzen Darstellung seines Anwendungsgebiets Zusammenstellungen der für den beschriebenen Sachverhalt relevanten Gefährdungen und empfohlenen Schutzmaßnahmen.</p> <p>Achtung: Bausteine gelten nur dann wenn ich sie in einem standardisierten Betrieb betreibe</p>
13	Was beschreibt die 2700-1 oder :der BSI-Standard 100-1: Management für	Dieser Standard beschreibt, welche grundlegenden Anforderungen ein Managementsystem für Informationssicherheit (ISMS) erfüllen muss sowie

	Informationssicherheit:	welche Komponenten es enthält und welche Aufgaben zu bewältigen sind. Die Darstellung orientiert sich an den Vorgaben der Norm ISO 27001 und weiterer aktueller internationaler Standards zur Informationssicherheit.
14	Was steht im iso-2700-2 oder : der BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise:	<p>Dieses Dokument konkretisiert die Darstellung eines ISMS im BSI-Standard 100-1 und beschreibt mit der IT-Grundschutz-Vorgehensweise einen effizienten Weg, die allgemeinen Anforderungen dieses Standards und der zugrunde liegenden Norm ISO 27001 umzusetzen</p>  <pre> graph TD     A[BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise] --&gt; B[Sicherheitsmanagement]     B --&gt; C[Initiierung Sicherheitsprozess]     C --&gt; D[Sicherheitsleitlinie und -konzeption]     D --&gt; E[Strukturanalyse]     E --&gt; F[Schutzbedarfsfeststellung]     F --&gt; G[Modellierung]     G --&gt; H[Basis-Sicherheitscheck]     H --&gt; I[Risikoanalyse]     I --&gt; J[Realisierung]     J --&gt; K[Aufrechterhaltung und Verbesserung] </pre>
15	der BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz:	<p>In diesem Standard ist ein gegenüber anderen Methoden vereinfachtes Verfahren zur Risikoanalyse beschrieben. Diese Methode ist immer dann wichtig und hilfreich, wenn Sie Komponenten absichern wollen, für die unter Umständen die IT-Grundschutz-Maßnahmen alleine keine ausreichende Sicherheit bieten. (CD-Anmerkung: „Ziehen sie einen Experten zu“→nicht sehr nützlich weil was ist ein Experte?)</p>  <pre> graph TD     A[BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz] --&gt; B[Erhöhter Schutzbedarf oder zusätzlicher Analysebedarf?]     B --&gt; C[Gefährdungsübersicht]     C --&gt; D[Zusätzliche Gefährdungen]     D --&gt; E[Bewertung]     E --&gt; F[Behandlung und Maßnahmen]     F --&gt; G[Konsolidierung: Sicherheitskonzept] </pre>
16	der BSI-Standard 100-4: Notfallmanagement:	Hier wird ein systematischer Weg aufgezeigt, ein Notfallmanagement in einer Behörde oder einem Unternehmen aufzubauen, zu überprüfen und weiterzuentwickeln. Die an einem Lebenszyklus-Modell ausgerichteten Konzepte zielen darauf ab, die

		<p>Widerstandsfähigkeit einer Institution zu erhöhen und die Kontinuität zumindest der wichtigsten Geschäftsprozesse und Fachaufgaben bei Krisen und Notfällen zu sichern.</p> 
17	Welches Modell liegt fast bei allen Prozessmanagementsystemen ,unter anderem dem in BSI-Standard 100-1 beschriebenen Sicherheitsprozessen zugrunde?	<p>Dem PDCA-Modell = Ein Zyklus aus Plan,(→Plan schreiben) Do, (→Plan umsetzen) check (→macht es sinn?-überprüfung)und Act(→Durchführen)</p> <p>Achtung wird auch Deming_Zyklus oder Demingkreis, Deming-Rad...etc. genannt!</p>
18	Was sollte eine Leitlinie zur Informationssicherheit enthalten	<ul style="list-style-type: none"> <li>• Aussagen zur Bedeutung der Informationssicherheit für die betroffene Institution</li> <li>• Und grundlegende Regelungen zur Organisation der Informationssicherheit</li> <li>• Scoping?+Rahmenbedingungen (rechtlich..)</li> </ul>
19	was versteht man unter einer Leitlinie?	Ist Normativ
20	Sie sind ein IT-Sicherheitsbeauftragter(der prozessowner)- welche Aufgaben haben sie üblicherweise?	<ul style="list-style-type: none"> <li>• Untersuchen von Sicherheitsvorfällen</li> <li>• Koordination der Entwicklung von Sicherheitskonzepten</li> <li>• Bericht über den Stand der Informationssicherheit für die Leitungsebene erstellen</li> </ul>
21	Wer ist für die Bekanntgabe der Leitlinie zur Informationssicherheit verantwortlich?	Die Unternehmens-oder BehördenLEITUNG
23	was ist ein Informationsverbund?	Unter „Informationsverbund“ versteht man die Gesamtheit der infrastrukturellen, organisatorischen, personellen und technischen Objekten die in einem bestimmten Anwendungsbereich der

		Informationsverarbeitung arbeiten. →kurz: der Geltungsbereich den das Sicherheitskonzept betrifft.
24	beschreibe kurz die „Strukturanalyse“	Zunächst ist der Informationsverbund zu definieren→ anschließend werden alle Objekte aus diesem Verbund strukturiert erfasst Organisation-Anwendung laufen auf Computersystemen und diese stehen in Gebäuden – diese haben Netzwerke(-wer-wo-wie) so sieht die strukturierung aus
25	Sie wollen einen Informationsverbund festlegen. Auf was müssen sie achten?	<ul style="list-style-type: none"> <li>• Er muss eindeutig und einfach gegen die anderen Bereiche(welche nicht einbezogen werden sollen) der Institution abgegrenzt werden können.</li> <li>• Es muss vollständig (mit allen externen Schnittstellen!) beschrieben werden.</li> <li>• Es muss eine sinnvolle Mindestgröße haben.</li> </ul>
26	welche Ziele verfolgt die Strukturanalyse im Rahmen der IT-Grundschutz-Vorgehensweise?	Die Ermittlung aller Objekte die einem Sicherheitskonzept zu berücksichtigen sind Und die Zusammenfassung von Objekten für die die gleichen Sicherheitsmaßnahmen angewendet werden können
27	wann bietet es sich an IT-Systeme bei der Strukturanalyse zu gruppieren?	Wenn diese den gleichen Schutzbedarf und ähnliche Eigenschaften (betriebssysteme, Netzanbindung, unterstützte Anwendung...) haben.
28	Welche Aufgaben gehören gemäß BSI-Standard 100-2 zur Strukturanalyse?	Die angemessene Gruppierung der Objekte die ein Sicherheitskonzept unterschieden werden müssen. Die Erhebung der : <ul style="list-style-type: none"> <li>• Informationen,</li> <li>• Geschäftsprozesse,</li> <li>• Anwendungen, IT-Systeme,</li> <li>• Kommunikationsverbindungen</li> <li>• räumliche Gegebenheiten eines Informationsverbundes</li> </ul>
29	müssen die Verwendungen von Datenträgern bei der Strukturanalyse beachtet werden?	Wenn diese Schutzbedürftige Informationen enthalten
30	Müssen sie Datenträger die fest mit einem IT-System verknüpft sind in der Strukturanalyse erfassen?	Nein
31	was muss ein Netzplan im Rahmen einer Strukturanalyse beinhalten?	Die in das Netz eingebundenen IT-Systeme- die Verbindung dieser Systeme- die Außenverbindung dieser IT-Systeme.

32	Was sollten sie bei der Erstellung eines Netzplanes im Rahmen einer Strukturanalyse beachten?	<p>Es sollte ein „bereinigter Netzplan“ erstellt werden. Das heißt, dass gleiche/ ähnliche Komponenten zusammengefasst werden → Komponenten welche:</p> <ul style="list-style-type: none"> <li>• vom gleichen Typ sind</li> <li>• nahezu gleich konfiguriert sind</li> <li>• (nahezu) gleiche Netzeinbindung besitzen</li> <li>• Den gleichen Rahmenbedingungen unterliegen(administrativ und infrastrukturell)</li> <li>• Gleichen Anwendungen bedienen.</li> </ul> <p>Wichtig: die zusammengefassten Gruppen(und „deren Inhalt“) müssen den gleichen Schutzbedarf haben- da sonst Sicherheitslücken entstehen</p>
33	Welches Kriterium beachten Sie bei der Bestimmung des Bedarfs an Verfügbarkeit eines IT-Systems?	Die maximale tolerierbare Ausfallzeit des IT-Systems
34	Was müssen Sie beachten wenn sie den Schutzbedarf einer Anwendung bestimmen?	<p>Die Information, die im Zusammenhang mit der Anwendung verwendet werden</p> <p>Die Bedeutung der Anwendung für die Geschäftsprozesse oder Fachaufgaben</p>
35	Unter welchen Bedingungen kann der Schutzbedarf eines IT-Systems bezüglich Verfügbarkeit geringer sein als derjenige der Anwendungen, für die es eingesetzt wird ?	<p>Wenn das IT-System nur unwesentliche Teile der Anwendung bedient</p> <p>Wenn ein redundantes ausgelegtes weiteres IT-System vorhanden ist welche die benötigten Anwendungen ebenfalls zur Verfügung stellen</p>
36	was bedeutet es wenn bei einer Schutzbedarfsfeststellung für ein IT-System Kumulationseffekte berücksichtigt werden?	<p>Es bedeutet dass sich der Schutzbedarf dieses IT-Systems erhöht weil sich Einzelschäden zu einem insgesamt höheren Gesamtschaden addieren.</p> <p>(zb.: wenn auf einem PC 2 wichtige anwendungen laufen.-dann ist dieser doppelt so wichtig)</p>
37	Nennen Sie die 3 Schutzbedarfskategorien:	<p>normal: Die Schadensauswirkungen sind begrenzt und überschaubar.</p> <p>hoch: Die Schadensauswirkungen können beträchtlich sein.</p> <p>sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.</p>
38	Was geschieht bei der Modellierung?	<p>Bei der <b>Modellierung</b> bilden Sie den Informationsverbund und seine einzelnen Komponenten mithilfe der Bausteine nach. Das Ergebnis ist ein <b>IT-Grundschutz-Modell</b>. Dafür greifen Sie auf die Ergebnisse der beiden vorangegangenen Schritte zurück: <b>Strukturanalyse und Schutzbedarfsfeststellung</b> . Und Abschätzung von</p>

		Kostenhöhe und Wahrscheinlichkeit eines Schadens zu errechnen-danach werden passende Bausteine assoziiert. (es sollte Konsistent, nachvollziehbar, ..sein)
39	Was machen Sie wenn die IT-Grundschutz-Kataloge keinen passenden Baustein enthalten?	In diesem Fall müssen neue benutzerdefinierte Bausteine angelegt werden dafür brauchen wir bedrohungs und gefährdungsanalyse
40	Welche Aufgaben stellen sich bei der Modellierung gemäß IT-Grundschutz?	<ul style="list-style-type: none"> <li>• Abbilden von dem (vorher in der Strukturanalyse dokumentierten) Informationsverbund mithilfe der IT-Grundschutz-Bausteine</li> <li>• Zusätzliche individuelle Bausteine entwickeln – wenn diese benötigt aber nicht vorhanden sind.</li> <li>• PRÜFEN welche Bausteine für den betrachteten Informationsverbund relevant sind</li> </ul>
41	Welche der folgenden Änderungen an den IT-Grundschutz-Bausteinen sind gemäß IT-Grundschutz-Vorgehensweise unter bestimmten Umständen im Rahmen der Modellierung zulässig	<ul style="list-style-type: none"> <li>• Die Konkretisierung von Maßnahmen um technische Details</li> <li>• Die Anpassung von Bezeichnungen (zb.: für Rollen) an die Konventionen der betrachteten Institution</li> <li>• Ergänzung eines Bausteines um zusätzliche Maßnahmen</li> </ul>
42	Worauf sollte bei der Erstellung eines neuen Bausteines geachtet werden?	<b>Wirtschaftlichkeit</b> der Maßnahmen <b>Wirksamkeit</b> der Maßnahmen <b>Benutzerfreundlichkeit</b> der Maßnahmen
43	Was ist das Ziel bei der Modellierung?	Ziel der Modellierung ist eine möglichst vollständige Abbildung des betrachteten Informationsverbundes auf die Bausteine der IT-Grundschutz-Kataloge: Jeder Baustein sollte auf alle Zielobjekte (IT-Systeme, Räume usw.) angewandt werden, für die er relevant ist.(Risikoreichweite, wahrscheinlichkeit..etc)

44	Nennen Sie die 6 Prüfpunkte welche nach der Modellierung erfüllt sein sollten:	<ul style="list-style-type: none"> <li>• alle übergeordneten Aspekte sind korrekt modelliert</li> <li>• alle beteiligten Gebäude, Räume, Schutzschränke und die Verkabelung im Hinblick auf die infrastrukturelle Sicherheit sind berücksichtigt</li> <li>• alle erfassten IT-Systeme sind abgedeckt</li> <li>• die netztechnischen Sicherheitsaspekte durch die zugehörigen Bausteine korrekt sind modelliert</li> <li>• diejenigen Anwendungen sind berücksichtigt für die es IT-Grundschutz-Bausteine gibt,</li> <li>• diejenigen Objekte, für die keine unmittelbar passenden Bausteine vorhanden sind, angemessen durch andere geeignete Bausteine sind modelliert</li> </ul>
45	Beschreiben Sie das Schichtenmodell der Modellierung des IT-Grundschuttsverfahrens	Die Bausteine sind in den IT-Grundschutz-Katalogen in fünf Schichten gruppiert:



		<p><b>B1:Übergreifende Aspekte:</b> Die hier zugeordneten Bausteine betreffen grundsätzliche organisatorische Aspekte der Informationssicherheit und gelten in der Regel für den gesamten Informationsverbund.</p> <p><b>B2: Infrastruktur:</b> Diese Bausteine behandeln die baulich-technische Fragen und dienen insbesondere dem physischen Schutz etwa vor Feuer, Wasser oder Diebstahl.</p> <p><b>B3: IT-Systeme:</b> Diese Bausteine beschreiben die Sicherheitsaspekte von IT-Systemen</p> <p><b>B4: Netze:</b> Hier finden Sie Bausteine für Netzaspekte</p> <p><b>B5: Anwendungen:</b> Zur Sicherheit ausgewählter Anwendungen gibt es hier Bausteine</p>
46	Wenn sie bei der Modellierung einen Baustein selber erstellen wollen, wie müssen sie diesen aufbauen?	<p><b>Kurzbeschreibung</b> Jeder Baustein beginnt mit einer kurzen Beschreibung und Abgrenzung des betrachteten Gegenstands.</p> <p><b>Gefährdungslage</b> Dieser Abschnitt zeigt auf, welchen Gefährdungen die im Baustein beschriebenen Objekte ausgesetzt sein können. Die Gefährdungslage wird pauschal betrachtet, also ohne Berücksichtigung von Eintrittswahrscheinlichkeiten. Die Gefährdungen werden als Referenzen auf ihre ausführliche Beschreibung in den Gefährdungskatalogen angeführt und sind gegliedert in die möglichen Ursachen "Höhere Gewalt", "Organisatorische Mängel", "Menschliche Fehlhandlungen", "Technisches Versagen" und "Vorsätzliche Handlungen".</p> <p><b>Maßnahmenempfehlungen</b> Danach folgen die Maßnahmenempfehlungen, die mit kurzen Erläuterungen zum jeweiligen Maßnahmenbündel eingeleitet werden, z. B. Hinweisen zu einer sinnvollen Umsetzungsreihenfolge. Die Maßnahmen sind als Referenzen auf die ausführliche Beschreibung in den Maßnahmenkatalogen angeführt und in Anlehnung an ein Lebenszyklusmodell gegliedert in die Rubriken "Planung und Konzeption", "Beschaffung", "Umsetzung", "Betrieb", "Aussonderung" und die Querschnittsaufgabe "Notfallvorsorge".</p>
47	Wofür mache ich einen Basis-Sicherheitscheck	<p>Um Defizite bei der Umsetzung von Sicherheitsmaßnahmen zu ermitteln</p> <p>Um einen Soll-Ist-Vergleich zwischen den erforderlichen</p>

		und tatsächlichen umgesetzten Sicherheitsmaßnahmen zu erhalten. Um eine Anforderungsliste zu erhalten.
48	Nenne die 3 Voraussetzungen für einen Basis-Sicherheitscheck	Festlegung eines Zeitplanes  Auswahl von geeigneten Gesprächspartnern  Zusammenstellung der vorhandenen Dokumente zur Informationssicherheit in dem betrachteten Informationsverbund
49	Welche Verfahren nutzen Sie, um in einem Basis-Sicherheitscheck zu prüfen, wie gut eine Gruppe von Clients geschützt ist?	Interviews mit zuständigen Systembetreuern führen  Stichprobenartig und vor Ort Clients auf ihre Konfiguration testen  Vorhandene Dokumentation der Clients lesen. (hier gäbe es noch mehr möglichkeiten!)
50	Wann beurteilen Sie eine Maßnahme zu Schutz eines IT-Systems in einem Basis-Sicherheitscheck als umgesetzt?	Wenn alle wesentlichen Empfehlungen der zugehörigen Maßnahmenbeschreibung umgesetzt sind  wenn sowohl im Interview mit einem für das IT-System Zuständigen als auch bei einer stichprobenartigen Überprüfung keine Sicherheitsmängel festgestellt wurden
51	Erklären sie die Kennzeichnungen „W“, und „Z“ der Maßnahmen im Basis-Sicherheitscheck:	W: Hier muss die Umsetzung nicht geprüft werden da diese nur Hintergrundwissen enthalten  Z: Diese geben Sicherheitsempfehlungen, die über den normalen Schutzbedarf oder typische Informationsverbünde hinausführen. Falls solche Maßnahmen umgesetzt wurden, sollten sie auch in Prüfungen einbezogen werden
52	Sie stellen fest, dass eine wichtige IT-Grundschutz-Maßnahme für ein IT-System nicht umgesetzt ist, das nur noch kurze Zeit in Betrieb ist. Wie behandeln Sie diese Maßnahme beim Basis-Sicherheitscheck	Es wird als „nicht umgesetzt“ dokumentiert und angemerkt dass 2 Prüfungen notwendig sind. 1.) Eine Prüfung soll feststellen ob eine nachträgliche Umsetzung, trotz der kurzen Einsatzzeit des IT-Systems, notwendig ist. 2.) Die zweite Prüfung soll feststellen ob die daraus resultierenden Risiken in der Restlaufzeit des IT-Systems noch tragbar sind.
53	Was ist die Aufgabe einer ergänzenden Sicherheitsanalyse?	Es wird festgestellt für welche Objekte eines Informationsverbundes eine Risikoanalyse durchgeführt wird.

		<div><div>Strukturanalyse des Informationsverbundes</div><div>Schutzbedarfsfeststellung</div><div>Modellierung</div><div>Basis-Sicherheitscheck I</div><div>Ergänzende Sicherheitsanalyse</div><div>Risikoanalyse</div><div>Erstellung einer Gefährdungsübersicht Ermittlung zusätzlicher Gefährdungen Bewertung der Gefährdungen Behandlung der Risiken und Maßnahmenauswahl Konsolidierung des Sicherheitskonzepts</div><div>Basis-Sicherheitscheck II</div><div>Umsetzung des Sicherheitskonzepts</div></div>
54	Wer trägt die Verantwortung bei der Entscheidung einer ergänzenden Sicherheitsanalyse?	Die Leitung der Institution
55	Welche Gefährdungen sind Ausgangspunkt bei einer Risikoanalyse auf Basis von IT-Grundschutz	Die für die betrachteten Objekte relevanten Gefährdungen aus dem IT-Grundschutz-Katalogen
56	Was wird bei der Gefährdungsbewertung geprüft?	Die Wirksamkeit der umgesetzten/ geplanten Maßnahmen gegen eine Gefährdung
57	Wodurch kann ein Risiko verlagert werden	Durch den Abschluss einer Versicherung Durch Outsourcing
58	Wann werden zusätzliche/ergänzende Sicherheitsmaßnahmen benötigt?	Beim fehlenden geeigneter IT-Grundschutz-Maßnahmen Für hoch-Schutz-bedürftige Objekte
59	Wie ist ein Risiko definiert?	$R = \sum(p \cdot S)$ (Risiko = Summe aus (Wahrscheinlichkeit* Schaden)) Also die Summe aus der Wahrscheinlichkeit dass es eintritt (p) mal dem Schaden den es anrichten kann(S)
60	Wann kann ich ein Risiko akzeptieren?	<ul style="list-style-type: none"><li>• Wenn der Aufwand für die möglichen Schutzmaßnahmen unangemessen hoch sind</li><li>• Wenn die möglichen Schutzmaßnahmen verhindern dass die Geschäftsprozesse hinreichend effizient durchgeführt werden können</li></ul>
61	Auf welche 2 Arten können sie ein Risiko bekämpfen- Orientieren Sie sich dabei an der Formel $R = \sum(p \cdot S)$	Entweder man senkt die Wahrscheinlichkeit(p) dass es eintritt oder man überträgt die Kosten für den Schaden(S)
62	Nennen und beschreiben Sie die 6 Schritte des Realisierungsplanes	<b>1. Ergebnisse sichten</b> Sichten Sie zunächst die Ergebnisse des Basis-Sicherheitschecks und gegebenenfalls durchgeführter Risikoanalysen und stellen Sie die noch nicht oder nur

		<p>teilweise umgesetzten Sicherheitsmaßnahmen tabellarisch zusammen.</p> <p><b>2. Maßnahmen konsolidieren</b> Prüfen und konkretisieren Sie die Maßnahmen im Zusammenhang. Dies reduziert gegebenenfalls die Anzahl der umzusetzenden Maßnahmen.</p> <p><b>3. Aufwand schätzen</b> Schätzen Sie den finanziellen und personellen Aufwand, der mit der Umsetzung der einzelnen Maßnahmen verbunden ist. Unterscheiden Sie dabei zwischen dem einmaligen Aufwand bei der Einführung einer Maßnahme und dem wiederkehrenden Aufwand im laufenden Betrieb.</p> <p><b>4. Umsetzungsreihenfolge festlegen</b> Legen Sie eine sinnvolle Umsetzungsreihenfolge fest. Berücksichtigen Sie dabei sowohl die sachlogischen Zusammenhänge der einzelnen Maßnahmen als auch deren Wirkung auf das Sicherheitsniveau des Informationsverbundes.</p> <p><b>5. Verantwortliche bestimmen</b> Entscheiden Sie, bis zu welchem Termin eine Maßnahme umzusetzen ist und wer für die Realisierung und deren Überwachung zuständig sein soll.</p> <p><b>6. Begleitende Maßnahmen festlegen</b> Die praktische Wirksamkeit der Sicherheitsmaßnahmen hängt von der Akzeptanz und dem Verhalten der betroffenen Mitarbeiter ab. Planen Sie daher Schritte zu ihrer Sensibilisierung und Schulung ein.</p>
63	Welche Kriterien sollten Sie bei der Überprüfung Ihres Sicherheitskonzepts berücksichtigen?	<p>Die Aktualität des Sicherheitskonzepts</p> <p>Die Vollständigkeit des Sicherheitskonzepts</p>
64	Erkläre „Cross Site Scripting“ und wie man dieses verhindern kann	<p>Wird auch als XSS bezeichnet.(das X-steht im englischen für „Cross“ ;P)</p> <p>Cross-Site-Scripting ist eine Art der HTML Injection. Cross-Site-Scripting tritt dann auf, wenn eine Webanwendung Daten annimmt, die von einem Nutzer stammen, und diese Daten dann an einen Browser weitersendet, ohne den Inhalt zu überprüfen. Damit ist es einem Angreifer möglich, auch Skripte indirekt an den Browser des Opfers zu senden und damit Schadcode auf der Seite des Clients auszuführen.</p> <p>Ein klassisches Beispiel für Cross-Site-Scripting ist die Übergabe von Parametern an ein serverseitiges Skript, das eine dynamische Webseite erzeugt. Dies kann etwa das Eingabeformular einer Webseite sein, wie in Webshops, Foren, Blogs und Wikis üblich. Die eingegebenen Daten werden auf der Webseite wieder</p>

		<p>als Seiteninhalt ausgegeben, wenn die Seite von Benutzern aufgerufen wird. So ist es möglich, manipulierte Daten an alle Benutzer zu senden, sofern das Serverskript dies nicht verhindert. Diese Daten sind oft Code einer clientseitigen Skriptsprache (meist JavaScript).</p> <p>Verhindert werden kann es dadurch dass man den Input „escaped“ (also zb.: um /n zu verhindern vor / noch ein / einfügen um die ausführung von /n zu verhindern).</p> <p>Oder verhindern dass es überhaupt eingegeben werden kann</p> <p>Um durch eine Webanwendung keine Basis für XSS-Angriffe zu bieten, müssen alle eingehenden Eingabewerte als unsicher betrachtet und vor der weiteren Verarbeitung auf der Serverseite geprüft werden.</p>
65	Was ist „Broken Authentication and Session Management“?	<p>Problem: http ist zustandslos, Schutzziel Vertraulichkeit ist gebrochen. Weil vorher die Authentizität des Users oder des Browsers gebrochen wurde!</p> <p>Beispiel: Benutzer befindet sich auf „vertrauenswürdiger Seite“ und will sich anmelden. Benutzer sendet credentials (Benutzername, Passwort)→ Seite speichert Session in URL→ nun bewegt sich der Benutzer in der Seite und klickt auf einen anderen Link (von dem Angreifer)-dadurch dass nun meine SessionID in der URL weitergeleitet wird erhält der Angreifer( durch checken von referer logs!) meine SessionID und folglich meinen Account.</p> <p>Einschränken durch: keine eindeutigen Dinge in bezug auf die Session(!) in die URL speichern. Einschränken dadurch dass Authentifizierung immer einfach, zentral und standardisiert ist! Die Vertraulichkeit ist verletzt</p>
66	Wie kann „Insecure Cryptographic Storage“ verhindert werden?	<p>Die Vertraulichkeit ist verletzt weil vertrauenswürdige Daten den Bereich verlassen und diese verschlüsselt werden sollen (probleme-verschlüsselung findet zu spät statt, garnicht verschlüsselt, daten werden verschlüsselt aber nicht sehr gut) ACHTUNG: ist nicht beschränkt auf passwörter</p> <ul style="list-style-type: none"> <li>• Passwörter nie in log-Files speichern.</li> <li>• Auf Einwegverschlüsselung achten</li> </ul>

		<ul style="list-style-type: none"> <li>• Speicher löschen/überschreiben nach einer Passwortbearbeitung bevor er wieder freigegeben wird</li> </ul>
67	Erkläre „Insufficient Transport Layer Protection“	<p>Annahme- App sind die Guten, und in der Datenbank sind die Guten-nur alles außerhalb ist böse und dadurch ergibt sich das Problem dass Daten zwischen diesen Beiden ausgetauscht werden müssen→ wir brauchen einen schützengraben→ kommunikationsleitung muss geschützt werden-wir nehmen richtigen Tunnel. In dem Moment wo dieser Übertragungsweg nicht geschützt ist habe ich alle angreifmöglichkeiten wie Man-In-the-Middle...etc (vertraulichkeit oder integrität gefährdet) Kann durch SSL-Verschlüsselung verhindert werden</p>
68	Wie funktioniert „SQL Injection“? Und wie kann es verhindert werden?	<p>Diese Technik nützt den ungeschützten Zugang zur Datenbank aus. Der Benutzer wird aufgefordert Informationen (meist Benutzername oder Passwort) einzugeben. Der Benutzer kann nun SQL- Befehle in die Eingabefelder einfüllen welche zur Datenbank gesendet werden und ausgeführt werden. Dadurch kann Beispielsweise die Eingabe eines Passwortes umgangen werden.</p> <p>Verhindern kann man dies durch:  Benutzereingaben validieren→ im Code!  Erlaubten Zeichensatz des Formulars einschränken→ Im GUI(zb.: Regex)  (SQL-Statements vorbereiten)BESSER AUF ENGLISCH: Prepare Statements</p> <p>Wesentlich: Daten werden als Befehle interpretiert→ immer wenn ich einen Interpreter habe habe ich dieses Problem!</p>
69	Erkläre „Security Misconfiguration“ und wie diese verhindert werden kann.	<p>Entweder es ist garnichts das was ich konfigur Integrität und/oder vertraulichkeit- weil entweder die Konfiguration nicht sauber stattgefunden hat oder weil sie garnicht stattfinden können(hardcodierung)</p>
70	Was steht in den ISO 27 000, ISO27001, und ISO27002 und deren Geltungsbereich?	<p>Ich kann die ISO27000 auf alles was mit Information zu tun hat anwenden.  ISO 27 000 →Dient als „Wörterbuch“  ISO 27 001 →Betrifft Managementsysteme  ISO 27 002 →Erklärt Maßnahmen</p>
71	Wozu dient eine Firewall	<p>sie setzt eine Politik durch = sie erhöht die Sicherheit nicht dadurch ihr Vorhandensein.</p>
72	Welche Aussagen treffen auf einen transparenten Proxy zu?	<p>A: .) Standardport auf der anderen Seite notwendig</p> <p>.) Alle Anfragen werden anhand es Ports auf den transparenten Proxy umgeleitet</p>

		.) --falsche Antwort: der Client muss kooperieren --falsche Antwort ENDE
73	Worin besteht die Schutzwirkung der "Demilitarisierten Zone"?	Durch Isolation eines Systems gegenüber zwei oder mehr Netzen.
74	Warum kann eine TCP Verbindung in einem SSH Tunnel zu Problemen führen?	Sowohl SSH als auch TCP benötigen einen Timer, da der SSH Timer und der TCP Timer anders takten, kann es zu gegenseitigen Verzögerungen führen.
75	Nenne die 5 Hauptstufen des Security Development Lifecycle	1(Training) 2Requirements 3Design 4Implementation 5Verification 6Release 7(Response)
76	Wie werden die einzelnen Phasen des MS Security Development Lifecycles verbunden?	^Sie werden durch „Gates“ verbunden → diese sind Meilensteine und werden durch den „Deming Zyklus“(siehe frage 17) geprüft. Wichtig ist, dass wenn ich weiß das Fehler in einer Stufe vorhanden sind es nicht zu der nächsten Phase kommen darf-erst nach Test und sicherstellung kann es weitergehen.
77	An was kann ich mich halten wenn ich die Requirements des MS Security Development Lifecycle aufstelle?	An den BSI Grundschutz
78	Was geschieht beim „Threat Modeling“ bei der Stufe des Designs in dem MS Security Development Lifecycle?	„Threat Modeling“ wird in Umgebungen verwendet bei denen es schwerwiegende Risiken geben könnte. Die Aufgabe liegt darin MÖGLICHE (!Aber auch realistische) Gefahren zu erkennen , analysieren und für diese Maßnahmen festsetze.--> Ich mache die Wahrscheinlichkeit kleiner dass Fehler ausgenutzt werden können.
79	Welche 3 Punkte kommen in „Requirements“ in dem MS Security Development Lifecycle vor?	Security Requirements, Quality Gates & Bug Bars, Security and Privacy Risk Assessment
80	Für was werden “Bug Bars” eingesetzt?	Sie sind ein Teil von „Requirements“ in dem MS Security Development LifeCycle. Es wird verwendet, um starke Schwellen von Sicherheitsschwachstellen zu definieren.
81	Welchen Zweck erfüllt das “Security and Privacy Risk Assessment” in dem MS Security Development Lifecycle?	Es handelt sich hierbei um einen ausschlaggebenden Prozess welcher die funktionalen Aspekte der zu betrachtenden Software analysiert.

83	Welche 3 Stufen kommen in dem „Design“ in dem MS Security Development Lifecycle vor?	Design Requirements Threat Modeling Attack Surface Reduction
84	Erklär kurz „Attak Surface Reduction“ aus dem MS Security Development Lifecycle?	Es ist ähnlich wie Threat Modeling- nur die Ansicht erfolgt aus einem anderen Blickwinkel. Hierbei wird versucht den Angreifern weniger Angriffsfläche zu bieten.--> Schwächen und Verwundbarkeit reduzieren. → Den Zugang zu System Services zu begrenzen → Anwendung des Prinzips der geringsten Rechte → Einsatz von geschichteter Verteidigung wo immer möglich
85	Welche 3 Stufen gehören zu der „Implementation“ aus dem MS Security Development Lifecycle?	Use approved tools Static Analysis Deprecate Unsafe funktions
86	Von wo weiß ich welche Tools ich bei dem Schritt „Implementation“ aus dem MS Security Development Lifecycle verwenden darf?	Es gibt ein sogenanntes „Blue Book“ in dem alle erlaubten Tools genannt werden.
87	Was ist ein“ Fuzz Test“?	Es ist bestandteil aus dem Schritt „Verification“ aus dem MS Security Development Lifecycle. Es ist eine spezielle Anwendung der dynamischen Analyse. Es werden absichtlich fewhlerhafte oder statische Daten in die Anwendung induziert.

#### CD-Informationen:

(Informationssicherheit ist die Erklärung von Schutzziele-Es gibt aber auch andere Modelle Der IT-Grundschutz als solches hat im prinzip ebenfalls schutzziele und versucht mit einem Vorgehensmodell(hat prüfziele) und kirtereien eine Reihung zu erstellen)

Grundschutz-bedrohung der schutzziele:

Missachtung in die Informelle selbstbestimmtheit

...das sind kriterien die Schutzziele sind aber gleich...

Leitlinie ist im Rahmen einer Norm= Leitlinie ist Normativ!!!

Scoping= auswahl eines Bereichs/Gültigkeitsrahmen

Wann muss ich gefährdungs und bedrohungsanalyse machen: wenn ich gefährdungen hab die nicht vorkommen-wenn ich eine hohe schutzbedürftigketi habe- wenn ich den baustein dort betreibe die nicht üblich ist

Organisation-Anwendung laufen auf Computersystemen und diese stehen in Gebäuden –diese haben Netzwerke(-wer-wo-wie) so sieht die strukturierung aus

Quellen die verwendet wurden:	<ul style="list-style-type: none"> <li>• <a href="https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project">https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project</a></li> <li>• <a href="https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursITGrundschutz/webkursitgrundschutz_node.html">https://www.bsi.bund.de/DE/Themen/weitereThemen/WebkursITGrundschutz/webkursitgrundschutz_node.html</a></li> <li>• <a href="http://de.wikipedia.org/wiki/Cross-Site-Scripting">http://de.wikipedia.org/wiki/Cross-Site-Scripting</a></li> <li>• Dokument: „Simplified Implementation of the SDL“→ für MS Security Development Lifecycle</li> </ul>
-------------------------------	--