Repetitionsblatt ManSec
Governance, Risk & Compliance und ISMS (6 Lektionen)

1. Was versteht man unter (Corporate) Governance?
   Unterschriftenregelung, Umgang mit Daten, Berechtigungen, regulatorische Regelungen, Governance ist ein Framework, um sämtliche Prozesse so zu gestalten dass sie "verthebet" "Bezeichnet den rechtlichen und faktischen Umfangsrahmen für Leitung und Überwachung, der Prozess, nicht die Berechtigungen, werden geregelt"

2. Welche Komponenten benötigt eine funktionierende Governance?
   - Regeln, Ziele und Aktionen (danach Sanktionen)
   - Verantwortlich für Governance: Führung/Management legt Prozesse vor, Mitarbeiter sind für
   - Durchführung verantwortlich und Chief Compliance Officer führt Sanktionen etc. durch
   -

3. Welche Ziele verfolgt Governance?
   - Wettbewerb
   - Arbeitsfortlauf
   -
   -
   -

4. Wie müssen Sie vorgehen, um eine Governance einzuführen?
   a. Plan machen, warum man eine Governance braucht (Framework definieren)
   b. Bestandesaufnahme, wo gibt es Risiken/Breaches
   c. Ziele definieren, welche Ressourcen habe ich, wieviel "Energie" um Governance einzuführen
   d. Root Cause Analysis, warum Events passieren können
   e. Beobachten, messen, schauen was passiert ist
   f. Kontinuierliche Wiederholung des gesamten Prozesses
   g.
   h.

5. Was bedeutet Risiko, Risikomanagement und Risikomanagementprozess?

   Risiko: Mögliche negative Abweichungen von Zielen — Risiko = Eintretenswahrscheinlichkeit (Häufigkeit)
   R-Mgt: Umgang mit Risiko — * Schaden [pro Jahr]
   RM-Prozess: BBCA Prozess, 8 Boxen durchlaufen, den Prozess durchlaufen

6. Wieso spricht man von einem „Risiko-Management-System“?

7. Welche Standards von ISO und BSI beschreiben Risko-Management en detail?

   - ISO 27005
   - BSI 200-3

8. Was verstehen Sie unter Compliance?

   Compliance = Einhaltung/Konsistenz/Erfüllung
   Gesetze, Unternehmensziele, Regulatorisches, ethische/kulturelle Standards, Interessenskonflikte
   Compliance überprüft Governance

9. Erklären Sie die Principal-Agent-Theorie.

10. Was sind die Ziele von Compliance?

    - .
    - .
    - .

11. Was macht ein Information Security Management System und wo steht das?

12. Beschreiben Sie die IS-Pyramide.

Top: Policy, einfach verständlich,

Middle:

Bottom:

13. Wozu dient eine IS-Policy? Was muss beachtet werden?

14. Was bezweckt der IT-Grundschutz nach BSI?

Um zu begründen, dass man so gut wie möglich gehandelt hat, um sich selbst zu schützen.
Ohne aufwändige Risikoanalyse die grösstmöglichen Löcher stopfen können.
Gibt ein gewisses Grundsicherheitsniveau.