Repetitionsblatt W1 ManSec: GRC

1) Was versteht man unter (Corporate) Governance?

> Unternehmensführung & -lenkung, ein Set von Verantwortungen und Massnahmen des Managements zur Festlegung der *strategischen Ausrichtung*, Sicherstellung der *Zielerreichung*, *Risikomanagement* und *Ressourcenverwaltung*.
>
> Framework zur Gestaltung von Prozessen, Beschreibung des rechtlichen und faktischen Umfangs der Leitung, Überwachung.

2) Welche Komponenten benötigt eine funktionierende Governance?

> - Ziele und Regeln, Aktionen und Sanktionen.
> - Verantwortlichkeiten: Management legt Prozesse vor, Mitarbeiter führen durch, der *Chief Compliance Officer* bestraft

3) Welche Ziele verfolgt Governance?

> - Wettbewerbsfähigkeit
> - Arbeitsfortlauf
> - ...

4) Wie müssen Sie vorgehen, um eine Governance einzuführen?

> - Plan machen, warum man eine Governance braucht (Framework definieren)
> - Bestandesaufnahme, wo gibt es Risiken/Breaches
> - Ziele definieren, welche Ressourcen habe ich, wieviel "Energie" um Governance einzuführen
> - Root Cause Analysis, warum Events passieren können
> - Beobachten, messen, schauen was passiert ist
> - Kontinuierliche Wiederholung des gesamten Prozesses

5) Was bedeutet Risiko, Risikomanagement und Risikomanagementprozess?

> - Risiko: *Potentielles Abweichen von Zielen,* `Risiko = Eintretenswahrscheinlichkeit * Schaden`
> - Risikomanagement: *Umgang mit Risiken*
> - RM-Prozess: TODO

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

> TODO

7) Welche Standards von ISO und BSI beschreiben Risiko-Management en detail?

> - ISO 27005
> - BSI 200-3

8) Was verstehen Sie unter Compliance?

> Compliance bedeutet *Einhaltung, Konsistenz, Erfüllung* und bezieht sich auf Gesetze, Unternehmensziele, Regeln, Standards, kulturelle Normen, Ethik, Interessenskonflikte etc.
>
> Compliance überprüft Governance

9) Erklären Sie die Principal-Agent-Theorie.

> TODO

10) Was sind die Ziele von Compliance?

> TODO

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

> TODO

12. Beschreiben Sie die IS-Pyramide.

> TODO
>
> - Top: *Policies, einfach verständlich*
> - Middle:
> - Bottom:

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

> TODO

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.