# ManSec Repetitionsblatt Inhalte W3

1. Erklären Sie das «Bull Eye» Modell:
   Konzentrische Kreise von aussen nach innen:
   Policies, Networks, Systems, Application

2. Erklären sie die vier Begriffe «Standards, Policies, Procedures, Guidelines» und ordnen Sie diese in eine Pyramide (zuoberst das verbindlichste Element)
   Pyramide: Policies, Standards, Guidelines, Procedures

3. Wie häufig müssen Policies überprüft und erneuert werden, und welche Typen von Policies kennen Sie?
   6-12 Monate. EISP: Enterprise information security program policy; IISP: Issue-specific information security policies; SSISP: Systems-specific policies

4. Wer Unterschreibt die EISP?
   Verwaltungsratspräsident und CEO

5. EISP: An wen richtet sich eine EISP? Und welchen Zweck hat die EISP?
   An alle ICT User: Es soll Rechtssicherheit geben, welche Art von Nutzung erlaubt ist, und wie man sich zu verhalten hat

6. Was sind die wesentlichsten Inhalte?
   Legt Verantwortlichkeiten und ROllen fest. Beschreibt Entwicklung, Implementation und Management des Information Security Programms. Ausserdem werden auch spezifische Sicherheitsfunktionen beschreiben, wie z.B. Incident Reporting Stelle

7. Welchen Bezug hat die Information Securtiy Policy zu Corporate High Level Documents, wie z.B. Mission?
   Die EISP unterstützt die Firma in Ihrer Mission und es wird aufgezeigt, wie wichtig EISP ist, um die Ziele der Mission zu erreichen?

8. Weshalb ist es wichtig, dass die Philosophie der Sicherheit erklärt wird?
   Das gibt eine Selbstbeurteilungsfähigkeit und bleibt den Lesen am Längsten präsent.

9. Nennen Sie je ein Typisches Beispiel für die ISSP und SSISP:
   IISP Email und Application Security Policy; SSISP: Windows Axcess Right Management, Checkpoint FW Policy. Eigentlich für jedes System die generellen Policies und wie diese eingestellt werden.