Repetitionsfragen Frameworks

Begriffe:

- CISO: Chief Information Security Officer
- ISMS: Information Security Management System
- ISP: Information Security Policy
- QMS: Quality Management System

1. Weshalb ist es nicht genügend, heuristisch vorzugehen, bzw. weshalb braucht es ein ISMS?

- das heuristische Vorgehen ist in einer grossen Organisation kaum handhabbar

2. Welche Frameworks kennen Sie? Sagen Sie bei jedem Framework, welche Organisation dahinter steht!

- ISO 27001/27002 (ISO)
- Grundschutzhandbuch (BSI)
- COBIT (ISACA: Information System Audtitors and Control Association)

3. Weshalb sind Frameworks für den CISO wertvoll?

- Frameworks dienen dem CISO als Nachschlage- und Hilfswerk
- Rahmenwerke definieren Bereiche, die abgedeckt/geprüft werden müssen/sollten

4. Erklären Sie die Grundidee von QMS und ISMS. Inwiefern sind diese beiden Systeme vergleichbar, inwiefern sind sie unterschiedlich?

- Zweck des QMS: ständige Verbesserung der Qualität
- Zweck des ISMS:
  - kontinuierliche Verbesserung
  - permanente (automatisierte) Überprüfung
  - auf etablierte Standards verweisen
  - Berechtigung von Sicherheitsanliegen unterstreichen

Ein ISMS bezieht sich konkret auf die Sicherheit, ein QMS auf Qualität im Allgemeinen.

5. Wie drücken Sie (z.B. als CISO) aus, welche Controls (Prüfpunkte von Massnahmen) Sie berücksichtigen wollen?

- Mit einem Statement of Applicability (SoA)

  - was ist wichtig?
  - was ist nicht wichtig?

6. Wer ist für die Informationssicherheit, das ISMS und für Schäden verantwortlich?

- Informationssicherheit: CISO
- ISMS: Ausführungsverantwortung bei CISO
- Schäden: Besitzer bzw. Vertreter der Besitzer (CEO)

7. Wer entscheidet über die Implementierung einer Massnahme?

- derjenige, der die Budgetkontrolle hat

8. Welche Rolle hat die Information Security Policy?

- interne „Gesetzgebung“, wie Sicherheit in der Firma gelebt wird
- verbindliche Vorschriften
- muss top-down unterstützt und „gelebt“ werden

9. Was ist Baseline Security? Braucht es eine Risikoanalyse?

- Baseline-Security: man tut das, was alle machen → Anwendung von Best Practices
  - Backup
  - Updates
  - Passwörter
- Eine Risikoanalyse ist für unternehmensspezifische Gegebenheiten sinnvoll.