1 Einführung in Grundbebriffe

IT-Compliance: IT-Compliance bezeichnet die Kenntnis und Einhaltung sämtlicher regulatorischer Vorgaben und Anforderungen an das Unternehmen, die Aufgabe und Einrichtung entsprechender Prozesse und die Schaffung eines Bewusstseins der Mitarbeiter für Regelkonformität, sowie die Kontrolle und Dokumentation der Einhaltung der relevanten Bestimmungen gegenüber internen und externen Adressaten.

IT-Governence: Liegt der Verantwortung des Vorstands und des Managements und ist wesentlicher Bestandsteil der Unternehmungsführung. IT-Governence besteht aus Führung, Organisiationsstrukturen und Prozessen, die sicherstellen, das die IT die Unternehmenstrategie und Ziele unterstüzt.
ISMS = Informationssicherheitsmanagementssystem: Beschreibt das allgemeine Sicherheitsmanagement speziell im Bereich der Informationssicherheit. ISMS es ein komplexer Prozeß der Steuerung von materiellen, konzeptionellen und menschlichen Ressourcen mit dem Ziel, den Anforderungen an die Aspekte -Auftragserfüllung, Vertraulichkeit, Integrität und Verfügbarket einer Organisation angemessen zu entsprechen.

Bedrohung: Ereignisse oder Begebenheiten aus dennen ein Schaden entstehen kann.

Bedrohungskategorie
höhere Gewalt
elementare Bedrohung
techniches Versagen
vorsätzliches Handln
menschliche Fehlentscheidung

Schwachstelle: Sicherheitsrelvanter Fehler eines IT-Systems oder eines Prozesses.

Schutzmaßnahmen: Maßnahmen um einen Zustand von Sicherheit zu erreichen oder zu verbessern.
Begriffe im Zusammenhang: Eine Bedrohung nutzt Schwachstellen aus um Assests anzugreifen. nach BSI:
Infrastruktur: Verschlossene Türen + Videokameras
Hardware und Software: Firewall, Malewareschutz, IDS (Analyisert und schlägt Alarm wenn Angriff stattfindet) - IPS (leitet sogar noch GegenMaßnahmen ein)
Organisation: Verantwortlichkeiten regeln, Nutzungsverbot nicht freigebender Hardware/Software
Kommunikation: Dokumentation der Verkabelung, Regelmäßiger Sicherheitscheck der Netze, restriktive Rechtvergabe
Notfallvorsorge: Regelmäßige Datensicherung, TKA-Basisanschluss für Notrufe, Übersichert über Verfügbarkeitsanforderungen
Personal: Vertretungsregelung, Awarenessmaßnahmen, Einarbeitung von Mitarbeitern

Schutzziele: Generische Sicherheitsziele zur Auswahl von Maßnahmen und Gestaltung eines Sicherheitskonzeptes.

2 Einordnung der Managmentsysteme

2.1 Eine Beschreibung nach COBIT 5

It Governence: Überwacht die IT bezüglich Strategie und Ziele des Unternehmen

ISMS = Informationssicherheitmanagementsystem: Sorgt dafür das Sicherheit der Schutziele garantiert ist - steuert die IT um Informationssicherheit zu gewährleisten.

IT-Risikomanangent: Der Teil des ISMS der sich mit der IT beschäftigt (Berichtet an Riskomanagement)

IT - Compliance: Wird von IT-Risikomanagement überwacht und dient zur Umsetzung aller wichtigen und relavanten Maßnahmen die durch interne so wie externe Anforderungen enstehen (Ist Teil von Compliance)