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)

3 ISO-Standard

27000 Enthält Überblick und verwendete Definitionen
Enthält einen Überblick über die Familie des ISMS-Standards. Sowie eine Einfühung was ein ISMS (Information Management System) überhaupt ist. Eine kurze Beschreibunb von Plan-Do-Check-Act (PDCA). Sowie die Therme und Definitionen die benötigt werden.

27001 Vorraussetzungen
Enthält Informationen über den Aufbau, Betrieb, Verbesserungen, Einschätzungen und Behandlung von Risiken eines ISMS.
27002 Verfahrensregeln für die Informationssicherheit
Enthält Sicherheitsmaßnahmen die in 13 unterschiedliche Domänen geteilt werden - Hinweise zum Organisationsaufbau wie man Richtlinien und Policyerstellung und technische Maßnahmen.
27003 Umsetzungs-Leitfaden
Wie man Projekte aufsetzt - zuerst Management-Zustimmung, ISMS Scope und Richtlinien, Analyse der Organisation, Risikomanagementprozess, Design des ISMS **27004** Überprüfen der Wirksamkeit
Wirksamkeit des ISMS und der Sicherheitsmaßnahmen
27005 Informationssicherheit Risikomanagement
1. Den Kontext feststellen
2. Risiko Einschätzung
3. Risiko Behandlung
4. Risiko Akzeptanz
5. Risiko Kommunikation
6. Risiko monitoring und Rezension

4 27001

7 Schritte:
1. Kontext der Organisation
2. Leitung
3. Planung
4. Support
5. Betrieb
6. Leistungsauswertung
7. Verbesserung

1.
Für den Kontext der Organisation was sind die Hauptziele der Organisation und wie kann die IT dabei helfen? - Was ist absolut nötig damit der Laden läuft?
Welche Anforderungen stellt das Unternehmen deshalb an die IT.
Welche Anforderungsgruppen gibt es und welche Anforderungen haben sie (IT-Compliance).
2.
Management soll Leitung und Bekenntnis zum ISMS zeigen. Viel Bla bla bla was Management machen soll - Policy - Integrierung des ISMS in Geschäftsprozesse - Förderung und Verbesserung des ISMS - Unterstützen der anderen re... Management
3.
Unter berücksichtigung der Kontextfeststellung, insbesondere der Anforderungsfeststellung:
-Information Security Risk Assement nach Iso 27005: Risiko-Identifizierung, Risiko-Abschätzung, Risiko-Bewertung
-Information Security Risk Treatment nach Iso 27005 4.
Ressourcen bereitstellen
Identifizierung der nötigen Kompetenz
Dokumentation zur Feststellung der Kompetenz (Test wäre viel besser)
Angstellte sollten Informationssicherheitspolicy kennen (Awareness) und sich ihres Beitrags zur Sicherheit bewusst sein
Komunikation muss klar geregelt werden
Dokumentation
5.
Planen + umsetzen und dokumentieren der Prozesse
Umsetzen der Maßnahmen die identifiziert worden
Änderungsmanagement bei jedem change
ausgelagerte Prozesse müssen auch kontrolliert werden

Planung Support und Betrieb im Kreislaufen lassen plötzliche Änderung des Bildes -.-
6.
Ziel: Bewerten der Effektivität des ISMS Was gemessen Wie Wann Wer - Wann auswertung - Wer soll analysieren?

In Betracht ziehen für ob geeignet effektive und angemessenheit: Status vergangener Beschlüsse
Ergebnisse interner Audits
Feedback von Beteiligten
Ergebnisse Risikoanalyse und deren Status
Gelegenheiten für Verbesserungen
7.
Bei nicht Konformität Maßnahmen kontrollieren und korregieren und Konesequenzen behandln
Ursachen herausfinden und beseitigen
Gab es da schonmal was ähnliches?