

# 1 Einführung in Grundbegriffe

**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-Governance:** Liegt der Verantwortung des Vorstands und des Managements und ist wesentlicher Bestandteil der Unternehmensführung. IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmenstrategie und Ziele unterstützt.

**ISMS = Informationssicherheitsmanagementsystem:** Beschreibt das allgemeine Sicherheitsmanagement speziell im Bereich der Informationssicherheit. ISMS ist ein komplexer Prozess der Steuerung von materiellen, konzeptionellen und menschlichen Ressourcen mit dem Ziel, den Anforderungen an die Aspekte -Auftragserfüllung, Vertraulichkeit, Integrität und Verfügbarkeit einer Organisation angemessen zu entsprechen.

**Bedrohung:** Ereignisse oder Begebenheiten aus denen ein Schaden entstehen kann.

## **Bedrohungskategorie**

höhere Gewalt

elementare Bedrohung

technisches Versagen

vorsätzliches Handeln

menschliche Fehlentscheidung

**Schwachstelle:** Sicherheitsrelevanter 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 Assets anzugreifen. nach BSI:

Infrastruktur: Verschlussene Türen + Videokameras

Hardware und Software: Firewall, Malwarechutz, IDS (Analysiert 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, Übersicht über Verfügbarkeitsanforderungen

Personal: Vertretungsregelung, Awarenessmaßnahmen, Einarbeitung von Mitarbeitern

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

# 2 Einordnung der Managementsysteme

## 2.1 Eine Beschreibung nach COBIT 5

**IT Governance:** Überwacht die IT bezüglich Strategie und Ziele des Unternehmen

**ISMS = Informationssicherheitsmanagementsystem:** Sorgt dafür dass Sicherheit der Schutzziele garantiert ist - steuert die IT um Informationssicherheit zu gewährleisten.

**IT-Risikomanagement:** Der Teil des ISMS der sich mit der IT beschäftigt (Berichtet an Risikomanagement)

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

# 3 ISO-Standard

**27000** Enthält Überblick und verwendete Definitionen

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

#### **27001** Voraussetzungen

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 Assessment 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)

Angestellte sollten Informationssicherheitspolicy kennen (Awareness) und sich ihres Beitrags zur Sicherheit bewusst sein

Kommunikation 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 Konsequenzen behandeln  
Ursachen herausfinden und beseitigen  
Gab es da schonmal was ähnliches?