

4. Informationssicherheits-Managementsystem (ISMS)

4.1 Allgemeine Anforderungen

→ Dokumentiertes ISMS Aufbauen und Leben

4.2 Festlegung und Verwaltung des ISMS

4.2.1 Festlegen des ISMS (**PLAN**)

a) Definition des Anwendungsbereiches und der Grenzen des ISMS, ...

→ Geltungsbereich

b) Definition der ISMS – Leitlinie

→ Analogie QM-Politik. Zielsetzungen / generelle Richtung / gesetzliche Anforderungen / Abstimmung mit Risikomanagement der Organisation / Kriterien für Risikobewertung / Freigabe durch GF

c) Definition der Vorgehensweise für Risikoeinschätzung

→ welche Methode für Risikoeinschätzung / Kriterien für Risikoakzeptanz

d) Identifizierung der Risiken

→ Werte (Assets) identifizieren / Welche Bedrohungen gibt es für diese Assets? / Was kann passieren?

e) Analyse und Bewertung der Risiken

f) Optionen für Risikobehandlung

g) Auswahl Maßnahmenziele und Maßnahmen für Risikobehandlung

→ Siehe Anhang A / Die in Anhang A aufgelisteten Maßnahmen und Maßnahmenziele müssen ausgewählt werden. Diejenigen die nicht angewendet werden müssen begründet werden (Ausschlussverfahren / so wird nichts vergessen)

h) Zustimmung Mgmt zu Restrisiken. → (Sinnvolle Risikovorbeugung)

i) Genehmigung Mgmt für Umsetzung und Durchführung des ISMS

j) Erklärung zur Anwendbarkeit → Zusammenfassung der Entscheidungen zur Risikobehandlung.

4.2.2 Umsetzen und durchführen des ISMS (**DO**)

a-h) → Machen des zuvor festgelegten mit allen Konsequenzen (Verwaltung, Ressourcen, Schulungen, Formulierung Risikobehandlungsplan etc.)

4.2.3 Überwachen und Überprüfen des ISMS (**CHECK**)

a-h) → Methoden und Verfahren zur Erkennung von Fehlern. / Audits / Managementbewertung / Regelmäßiges Überprüfen der Risikoeinschätzung – Maßnahmen.

4.2.4 Instandhalten und Verbessern des ISMS (**ACT**)

a-d) → Umsetzung der Verbesserungen / Korrektur und Vorbeugemaßnahmen etc.

4.3 Dokumentationsanforderungen

4.3.1 Allgemeines

→ Dokumentation muss enthalten: ISMS Leitlinie / Geltungsbereich / Verfahren und Maßnahmen für ISMS / Beschreibung der Methode zur Risikoeinschätzung / Bericht der Risikoeinschätzung / Risikobehandlungsplan / dok.Verfahren (Bsp.Interne Audits) / geforderte Aufzeichnungen(4.3.3) / Erklärung zur Anwendbarkeit.

4.3.2 Lenkung von Dokumenten → Analogie 9001

4.3.3 Lenkung von Aufzeichnungen → Analogie 9001

5. Verantwortung des Managements

5.1 Verpflichtung des Managements

5.2 Management von Ressourcen

5.2.1 Bereitstellung von Ressourcen

5.2.2 Schulung Bewusstsein und Kompetenz

6. Interne ISMS- Audits

7. Managementbewertung des ISMS

7.1 Allgemeines

7.2 Eingaben für die Bewertung

7.3 Ergebnisse für die Bewertung

8. Verbesserung des ISMS

8.1 Ständige Verbesserung → bezogen auf ISMS

8.2 Korrekturmaßnahmen → bezogen auf ISMS

8.3 Vorbeugungsmaßnahmen → bezogen auf ISMS