Planung ISMS nach B3S-Systematik (ab EMRAM Stufe 4/5 umsetzbar)

Eine effektive Planung der ISMS Umsetzung nach B3S setzt einen Mindest-Reifegrad der digitalen Organisation und die entsprechenden Kapazitäten in der Einrichtung selbst voraus.
Die Zeitplanung mit einem strukturierten Curriculum hat den aktuellen Digitalisierungsstatus nach EMRAM zu berücksichtigen.

1.1.1.1 Vorbereitung nach B3S

Die Vorbereitungsphase kann mit 3-9 Monaten je nach EMRAM Stufe angesetzt werden:

- Definition der Grundlagen (Kontext), Referenz: B3S Kap. 5
- Identifikation kritischer Dienstleistungen des Krankenhauses
- Dokumentation (Beschreibung kritischer Dienstleistungen)
- Festlegung der Rahmenbedingungen (Budget und Zeitplan)

1.1.1.2 Onboarding nach B3S

Das Onboarding hat große Auswirkungen auf den Erfolg des ISMS-Projekts. Die Orientierung und Synchronisierung im Projektteam kann zeitlich mit 2-3 Monaten veranschlagt werden

- Technische Registrierung und Initialisierung eines digitalen ISMS
- Durchführung von Onboarding Workshops (Präsenz und VC)
- Stammdatenerfassung Krankenhaus und Team
- Definition und Qualifizierung der Projektbeteiligten

1.1.1.3 Umsetzung Phase 1

- Bestandsaufnahme nach EMRAM Reifegradmessung
- Entwicklung des Curriculums mit Einbeziehung aller Kliniken und Beteiligungen
- Definition der Managementstruktur für das ISMS-Projekt, Referenz: B3S Kap. 4&7
- Verabschiedung des Ziele-Katalogs im Kontext der Informationssicherheit und der Entwicklung des digitalen Reifegrads (EMRAM Klassifizierung)
- Erstellung der ISMS Richtlinien für alle Bereiche des Krankenhauses (Grundlagen und Geltungsbereiche)
- Freigabe der Richtlinien durch die Krankenhausleitung
- Bestandsaufnahme Infrastruktur, ISMS-relevante Prozesse, Abteilungs-Teams, Referenz: B3S Kap. 4.2.1
- Festlegung der Kritikalität und Prioritäten, Referenz: B3S Kap. 4.2.2
- Etablierung Risikomanagement für kritische Krankenhausdienstleistungen im Kontext der Informationssicherheit
- Aktualisierung der Risikoeinschätzungen und Definition einer Maßnahme Planung (TOM) für Informationssicherheit und integralen Datenschutz, Referenz: B3S Kap. 4&6

1.1.1.4 Umsetzung Phase 2

- Umsetzung der technischen und organisatorischen Maßnahmen zur Risikominimierung und -vermeidung
- Etablierung eines kontinuierlichen Task-Managements für IS- und DS-Maßnahmen, Referenz: B3S Kap. 4& 7
- Einführung eines Störfalls- und Notfall-Managements mit Integration eines kontinuierlichen Monitorings und Optimierungsmanagements (PDCA)
- Definition und Realisierung des Auditmanagements für alle risikorelevante Prozesse in der Informationssicherheit (und Datenschutz)
- Einführung des internen und externen Berichtswesens (Krankenhausleitung und Aufsichtsbehörden), Referenz: B3S Kap. 4&6

1.1.1.5 Inbetriebnahme des ISMS nach B3S

Der Zeitpunkt für die Inbetriebnahme ist abhängig von der Erreichung der primären Projektziele (siehe 1.4.5.3). Nach QM-Gesichtspunkten empfiehlt sich eine Überprüfung des ISMS-Status vor der Inbetriebnahme

- Durchführung eines internen Reifegrad-Audits des installierten ISMS nach Checklisten für die technischen Prozesse und Maßnahmen
- Durchführung eines internen Reifegrad-Audits des installierten ISMS nach Checklisten für die organisatorischen Prozesse und Maßnahmen
- Organisation von Kick-Off Meetings für alle Beteiligten mit Vorstellung der Systeme, der Ziele und der Leitlinien
- Integration des ISMS in den operativen und administrativen Tagesablauf mit Umsetzung der Richtlinien und Standards, Referenz: Kap. 4&7
- Team Orientierung und Start der Schulungsmaßnahmen nach Curriculum mit der definierten Nachweisdokumentation

1.1.1.6 Einführung des Audit-Managements

- Erstellung des finalen Projektberichts durch das Projektmanagement Team
- Realisierung der technischen Projektabnahme
- Realisierung der organisatorischen Projektabnahme
- Start des integralen PDCA Prozesses mit den relevanten Einweisungen

Das ISMS nach B3S ist mit einem übergreifenden Monitoring für die Informationssicherheit zu unterstützen. Das Monitoring ist Grundlage für die permanente Berichterstattung mit Jahresberichten nach gesetzlichen Normen.