Die iterative Implementierung eines ISMS

- Fallbeispiel eines KRITIS-Hauses

Katholisches Klinikum Lünen/Werne

Ralf Plomann
IT-Leiter

plomann.ralf@klinikum-luenen.de * 02306 / 775 775

Klinikum Lünen St.-Marien-Hospital

Katholisches Klinikum Lünen/Werne GmbH

ST. CHRISTOPHORUS-KRANKENHAUS WERNE

KKLW Kurzvorstellung

Klinikum Lünen
St.-Marien-Hospital

ST. CHRISTOPHORUS-
KRANKENHAUS WERNE

Schwerpunktversorgung
16 Fachabteilungen
592 Planbetten

akademisches Lehrkrankenhaus

Grund- und Regelversorgung
216 Planbetten

Ein Krankenhaus / zwei Betriebsstätten
Gemeinsame Leitung / Geschäftsführung

ca. 34.000 vollstationäre Fälle pro Jahr
ca. 1.500 Mitarbeiter

Klinikum Lünen
St.-Marien-Hospital

Katholisches Klinikum
Lünen/Werne GmbH

ST. CHRISTOPHORUS-
KRANKENHAUS WERNE

Unsere „Motivation“

2014 / 2015 erster Kontakt zum Thema

KGNW
Krankenhausgesellschaft Nordrhein-Westfalen e. V.

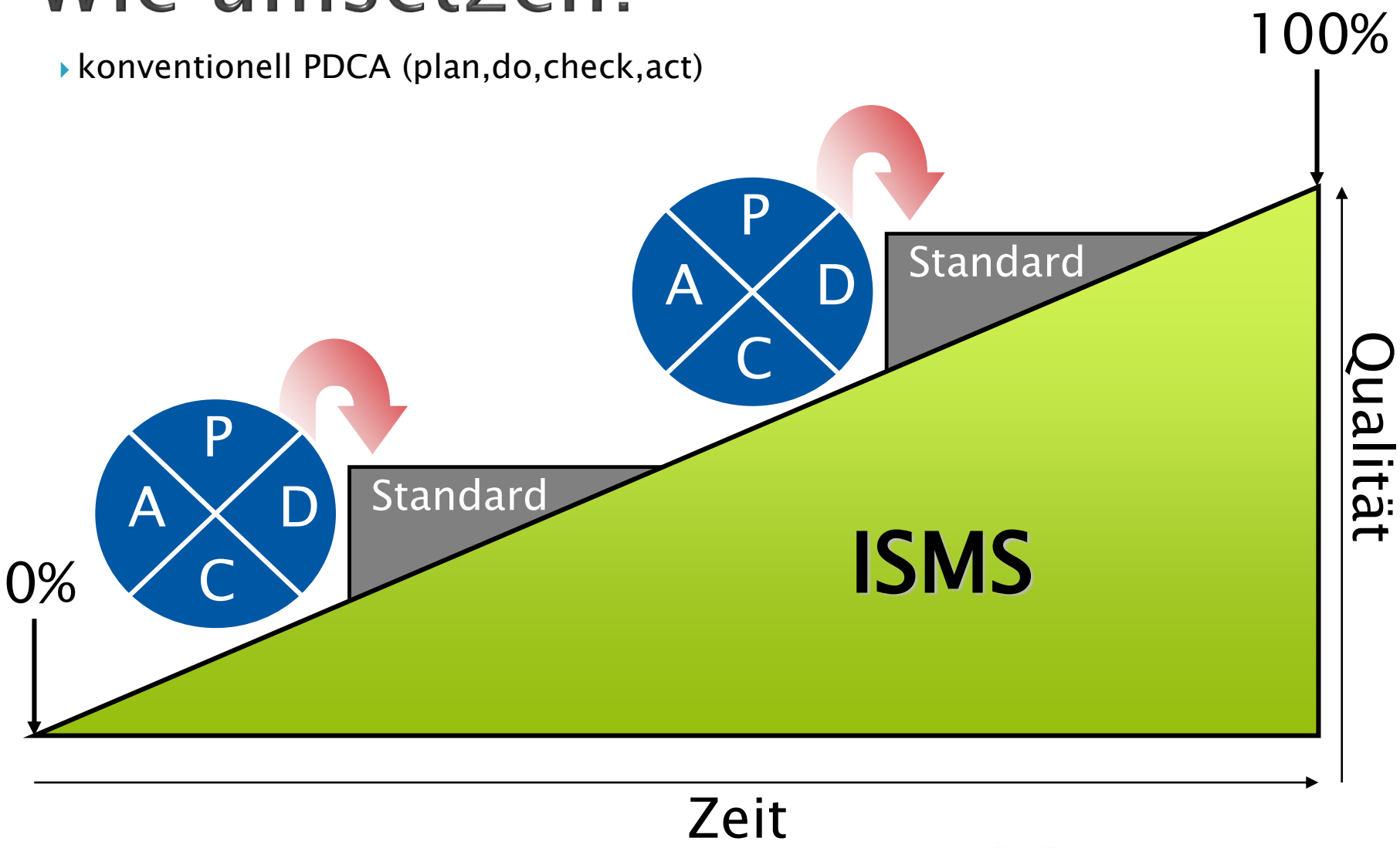
13.11.2014 Rundschreiben Nr. 477/2014
Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz (ITSiG))
zum Dokument im Archiv >>

- „§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

- (1) Betreiber Kritischer Infrastrukturen sind **verpflichtet**, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 **angemessene** organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der **Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der **Stand der Technik** eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche **Aufwand nicht außer Verhältnis** zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

Wie umsetzen?

- konventionell PDCA (plan,do,check,act)



Phase: Analyse

- Definition des Scope
  (Geltungsbereich / Anwendungsbereich des ISMS)

- d.h. IT / Medizintechnik / Haustechnik

Wo kommt „IT“ überhaupt zur Anwendung?

Prozess  **Informationstechnologie!**

- Beispiel Prozess: Patientenaufnahme
- PC/Drucker/LAN/KVK/
- Telefon
- Energie, Klima, Beleuchtung, Aufzug,…

WICHTIG: Den Kontext verstehen!

(vgl. §4 ISO 27001)

Phase: Design

- Ziele (passend zum Scope)
- Priorisierung (ggf. nach Risiko)
- Zeitrahmen (>12 Monate)

- Risiko Analysen (nach BSI Grundschutz)
- Dokumentationsstruktur des ISMS
- Definition von Regeln des ISMS

Phase: Umsetzung 1

- Schwachstellen beseitigen
- -Technisch
- -Organisatorisch

- Umsetzen von Maßnahmen

Phase: Umsetzung 2

- Monitoring / „Überwachung“
  - „Compliance“
    - –Technisch
    - –Organisatorisch

- Selbstkontrolle

Phase: Umsetzung 3

- Maßnahmen zur Awareness / Bewusstsein
  - proaktive Informationen (Security Newsletter)
  - Einzelgespräche (Anlassbezogen)
  - IT Sicherheit präsent halten (Konferenzen)

Beispiele…

Phase: Umsetzung 4

- [illegible]

IT-Sicherheitsmeeting
Teilnehmer
IT-Leiter
IT-Sicherheitsmanager

Frequenz 14 Tägig
Dauer 60 min
Wochentag Mittwochs 13 Uhr

Gesprächsinhalte:
- Sicherheitslage
- Strategien
- Aktivitätenbericht

Protokoll
ja
Gesprächsnotizen der Beteiligten
für die jeweilige Weiterbearbeitung

Fachgespräche Medizintechnik IT
Teilnehmer
IT-Leiter, Mitarbeiter IT(Msc. Medizininformatik)
und/oder Fachinformatiker für Systemintegration
Medizintechnik 2 Personen

Frequenz wöchentlich
Dauer 30-45 min
Wochentag Dienstags 10:30 Uhr

Gesprächsinhalte:
- Projekte
- Strategien
- Ablauforganisation
- Probleme, Vorfälle, Beschaffung

Protokoll
ja, Aktivitäten, Stand und Zuständigkeiten
Gesprächsnotizen der Beteiligten
für die jeweilige Weiterbearbeitung

Fe[illegible]

In[illegible]

Phase: Umsetzung Dokumente

- Beispiele für essentielle Dokumente:
  - Risikobewertung
  - Assetverwaltung (Produkte)
  - Lieferanten Abfragen
  - Gesprächsprotokolle

Empfehlung:
Alle Informationen zum ISMS an einer Stelle sammeln.
ISMS „Cockpit/Dashboard“

z.B. via Sharepoint / Alferesco..etc

Phase: Überprüfung

- micro Audit (RSA) [200 x pro Jahr)
- alle 2 Jahre via KRITIS Audit
- alle 14 Tage mit „CIO“ und „CISO“

Wer?

Wer behält den Überblick,
wer arbeitet aus,
wer lebt die PDCA Zyklen operativ?

- Rolle IT-Sicherheitsmanager

„Unser“ Fazit

- von 0% auf xx% geht!
- „Kunst der kleinen Schritte“
- Anfangen ist besser als abwarten
- Digitalisierungsgrad – Zeitpunkt
- Sicherheit by Design
- Synergien entstehen schnell
- wenige „Player“
- Erwecken! Nicht drohen!
- **Wir tragen Verantwortung!**

Danke für Ihre
Aufmerksamkeit!

Fragen?