Sana Management Service GmbH

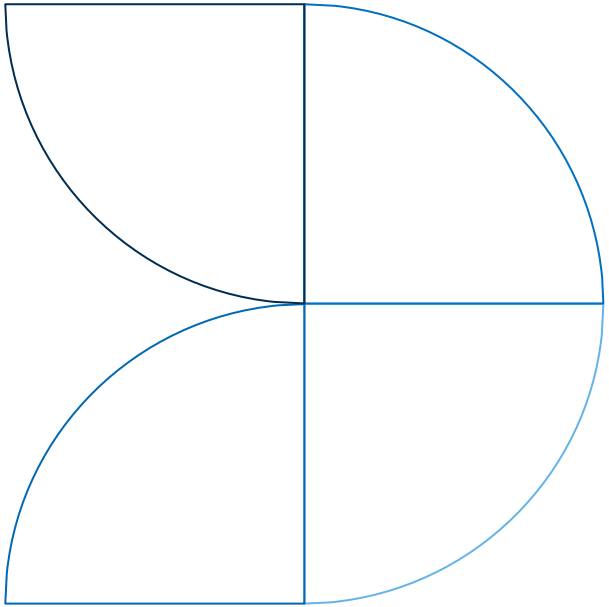
KRITIS CARE Klinik-Kompetenz macht den Unterschied.

Krankenhäuser im Spannungsfeld zwischen biologischen und technischen Viren

Dr. Christian Mayr,
Robert Färberböck,
Uwe Kauntz
Sana Management Service – KRITIS CARE

Agenda

1. Kurzvorstellung der Referenten
2. Realitätsszenario
3. Handlungsdruck „Zwischen biologischen und technischen Viren
4. ISMS Systeme „Zwischen Theorie und Praxis“
5. Integrierte Managementsysteme



Kurzvorstellung Referenten

Kritiscare Team

Uwe Kauntz

- zwanzig Jahre IT-Erfahrung IT Security in der Healthcare Branche
- Senior Berater im Bereich Informationssicherheit
- Risikomanager (CRISC)
- zertifizierter Lead Auditor (ISO27001, §8a BSIG)
- aktives Mitglied des Branchen-arbeitskreises Gesundheit
- aktiv an der Erstellung des B3S (Branchenspezifischer Sicherheits-standard) für die Gesundheitsversorgung im Krankenhaus beteiligt

Dr. Christian Mayr

- 25 Jahre Erfahrung als IT-Auditor und Datenschutzexperte
- promovierter Naturwissenschaftler
- 12 Jahre IT-Management und Audit Know-how (CISA / CISM / ISO 9001) bei international tätigen Prüfungs- und Beratungsgesellschaften
- 11 Jahre tiefreichende Expertise in allen Stufen von Risiko-Auditierung,
- Bereichsleiter Governance, Risk & Compliance
- Datenschutzbeauftragter für 9 Unternehmen des Sana-Konzerns

Robert Färberböck

- 12 Jahre IT-Berater bei WP Gesellschaft
- Verantwortet komplexe technische IT-Architekturen im SANA Konzern
- zertifizierter CISO
- Experte für Informationssicherheit
- IT-Auditor

Das Krankenhaus im Fadenkreuz

Düsseldorfer Uniklinikum mit Hilfe der „Citrix-Sicherheitslücke“ angegriffen

Hacker erpressen Klinikum Wolfenbüttel

Nach einem Hackerangriff vor gut zwei Monaten auf Kliniken des "Medizin Campus Bodensee" (MCB) im Bodenseekreis, läuft die IT immer noch nicht einwandfrei.

Cyberangriff auf das SRH Klinikums in Langensteinbach

…

Chronologie eines echten Cyberangriffes

- **Donnerstag, 03:00 Uhr Nachts:** Cyberangriff mittels der Ransomware „DoppelPaymer“ mit einem weitreichenden IT-Ausfall, Verschlüsselung der Daten
- **Donnerstag, 07:00 Uhr Morgens**: Information der Behörden und Inkrafttreten des KEP (Krankenhaus Einsatz Planes)
- **Donnerstag, 12:00 Uhr Mittags:** Mitarbeiter der Polizei mit Cyber-Security-Spezialisten im KH vor Ort im Einsatz sowie in den Folgetagen weitere externe IT-Experten, die die IT-Fachkräfte des KH unterstützten.
- **Freitag, 23:00 Uhr**: Freischaltung der verschlüsselten Daten
- **Eine Woche nach dem Angriff**: Teilöffnung der Fachambulanzen
- **Zwei Wochen nach dem Angriff**: Wiederaufnahme des vollen KH-Services

Die Folgen von Cyberangriffen auf Krankenäuser

Krankenhausbetrieb und die Patientenbehandlung schwer gestört

Finanzielle Verluste

Verluste der Datenvertraulichkeit

Verlust der Datenverfügbarkeit

Verlust der Datenintegrität

Negative Presse und Vertrauensverlust

Strafzahlungen

Die Gründe für Angriffe auf Krankenhäuser

Finanzielle Gründe

„Versehen“

Politische Gründe

Niedrigere Hürden durch immer stärkere Vernetzung von IT- und Medizingeräten

Steigende Kosten für hoch qualifiziertes IT-Personal

Gezielter Versuch des Datendiebstahls

Die harte Realität

Derzeitige Bedrohungen für Krankenhäuser:

- COVID19 Pandemie
- Cyberangriffe
  - politisch motiviert
  - wirtschaftlich motiviert

Daraus erwachsene Herausforderungen:

- Gesetzlicher Druck zum Schutz der Infrastruktur und Daten
  - DSGVO
  - BSIG
  - §75c SGB V
  - …

Fazit

- „*Krankenhäuser stehen im Spannungsfeld zwischen technischen und biologischen Viren*“

Der Druck auf das Krankenhaus steigt!

Steigender, gesetzlicher Handlungsdruck auf das Management,

die IT- und

Medizintechnik Fachabteilungen,

Verpflichtung zur Einhaltung eines hohen Versorgungsniveaus für die Bevölkerung

Gesetzlich bindende Regelungen bedeuten für Entscheider im Ernstfall massive rechtliche Folgen mit potentiellen Strafzahlungen

Damoklesschwert der Strafzahlungen

Datenschutzverstöße: Bußgelder von bis zu 20 Millionen Euro oder für Unternehmen von bis zu vier Prozent des weltweiten Jahresumsatzes (je nachdem, welcher Betrag am Ende höher ist)

Verstoß gegen das BSI-Gesetz (§14 V BSIG): Die Ordnungswidrigkeit kann ….. mit einer Geldbuße bis zu zwei Millionen Euro sowie in den Fällen …. mit einer Geldbuße bis zu einer Million Euro geahndet werden. (Genauere und weitere Informationen unter https://www.openkritis.de/betreiber/bussgelder-kritis-bsig.html)

Die wichtigsten Gesetze

Artikel 32 DSGVO

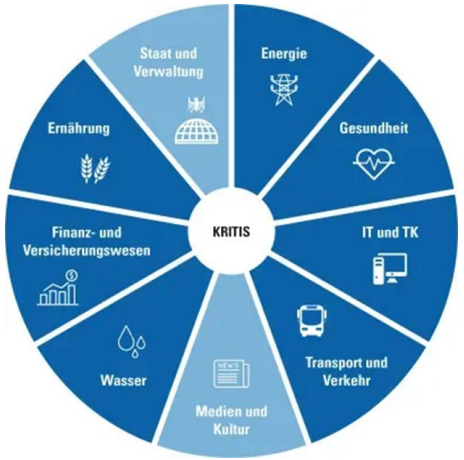
„***Unter Berücksichtigung des Stands der Technik***, ……. *treffen der Verantwortliche und der Auftragsverarbeiter* ***geeignete technische und organisatorische Maßnahmen***, *um ein dem Risiko angemessenes Schutzniveau zu gewährleisten…….“*

§75c SGB V

„Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, ***nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen,*** *die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.“*

§8a BSIG

„*Betreiber Kritischer Infrastrukturen sind verpflichtet, …….****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****……“*



ISMS Systeme

„Zwischen Theorie und Praxis“

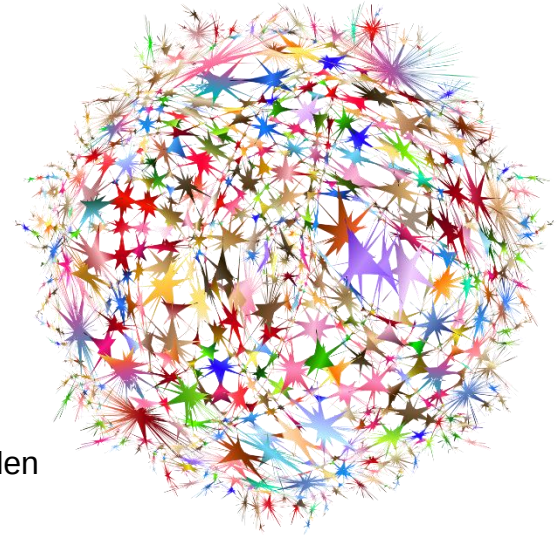
„Soll trifft auf Ist“

Das „Soll“

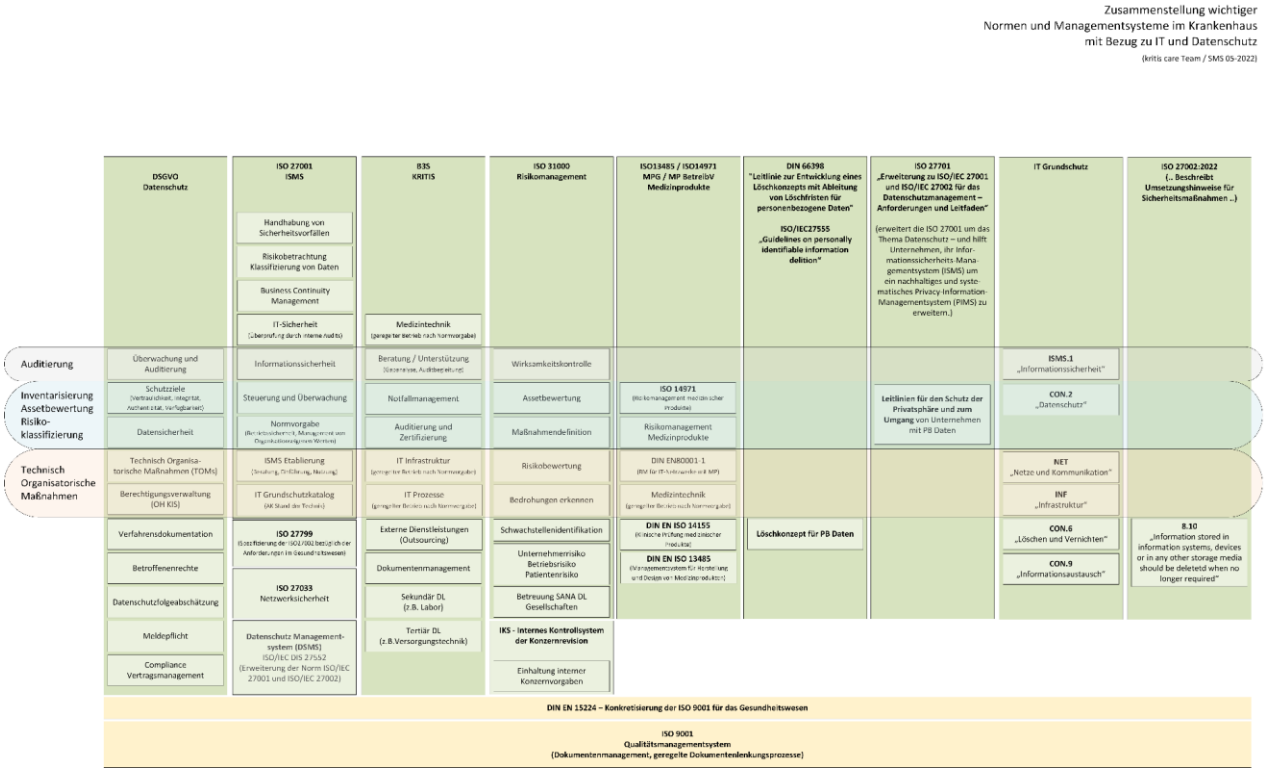
Steigende Risiken erfordern funktionierende Prozesse, eine effiziente Organisation und strukturierte Maßnahmen für einen sicheren Betrieb von Informationsverarbeitenden Systemen im Krankenhausumfeld.

Die Wirklichkeit

- Kein Managementsystem vorhanden
- Kaum Dokumentation vorhanden
- Ressourcenengpässe (vor allem bei IT-Mitarbeitern)
- Wenig Erfahrung mit Informationssicherheitsmanagement
- Inselwissen
- Starker Arbeitsdruck
- Kreativität von Cyberkriminellen beim Finden neuer Schwachstellen
- COVID19



Ein Wald aus „hilfreichen“ Gesetzen, Normen und Katalogen



ISMS als Weg zu mehr Sicherheit

Die Stärke eines Information Security Management Systems ist dessen ganzheitliche Auslegung.

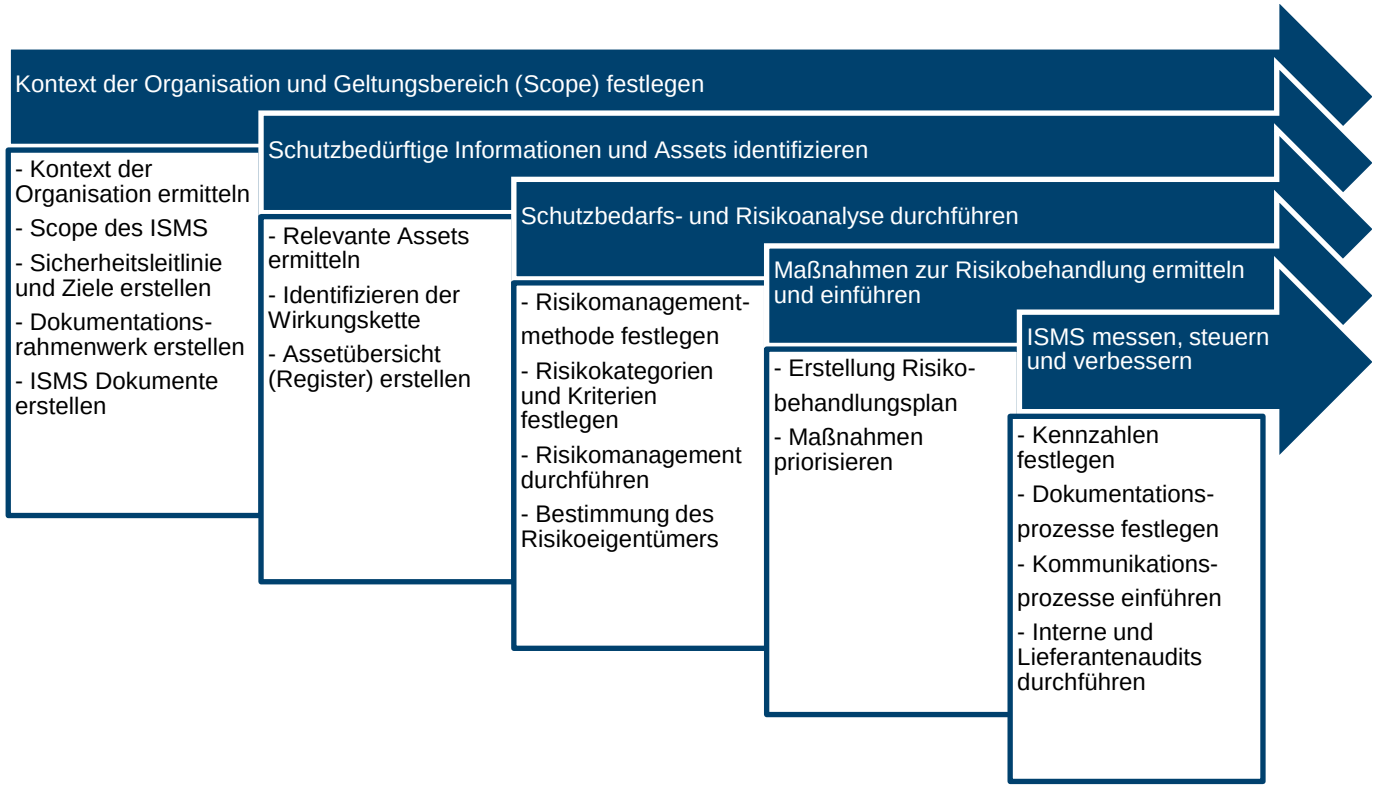
Definition von Prozessen
Es werden Abläufe entwickelt, die die Erreichung eines festgelegten Niveaus an IT-Sicherheit versprechen. Das erreichte Sicherheitsniveau wird in einem ISMS ständig weiter optimiert.

Aufbau und Ausbau der IT
ISMS berücksichtigt nicht nur vorhandene IT-Systeme, sondern ebenso deren Erweiterung und Anpassung. Es leistet Unterstützung bei Auswahl neuer Komponenten (Hardware und Software), damit bereits in dieser frühen Stufe die richtigen Entscheidungen getroffen werden.

Laufender Betrieb
Eine der wichtigsten Maßnahmen im Feld der Informationssicherheit ist die Wartung der Unternehmens-IT. Es werden interne Prozesse geschaffen, die u.a. ein zeitnahes Einspielen von Patches und Software-Updates gewährleisten.

Berücksichtigung der Mitarbeiter
Sobald es um Daten und IT-Systeme geht, stellen Mitarbeiter eine der größten Gefahrenquellen dar. Cyberkriminelle haben dies längst erkannt und setzen lieber auf Social Engineering als auf klassisches Hacking. Ebenso sind Mitarbeiter, die das Unternehmen verlassen, zu berücksichtigen.

Die ISMS Einführung

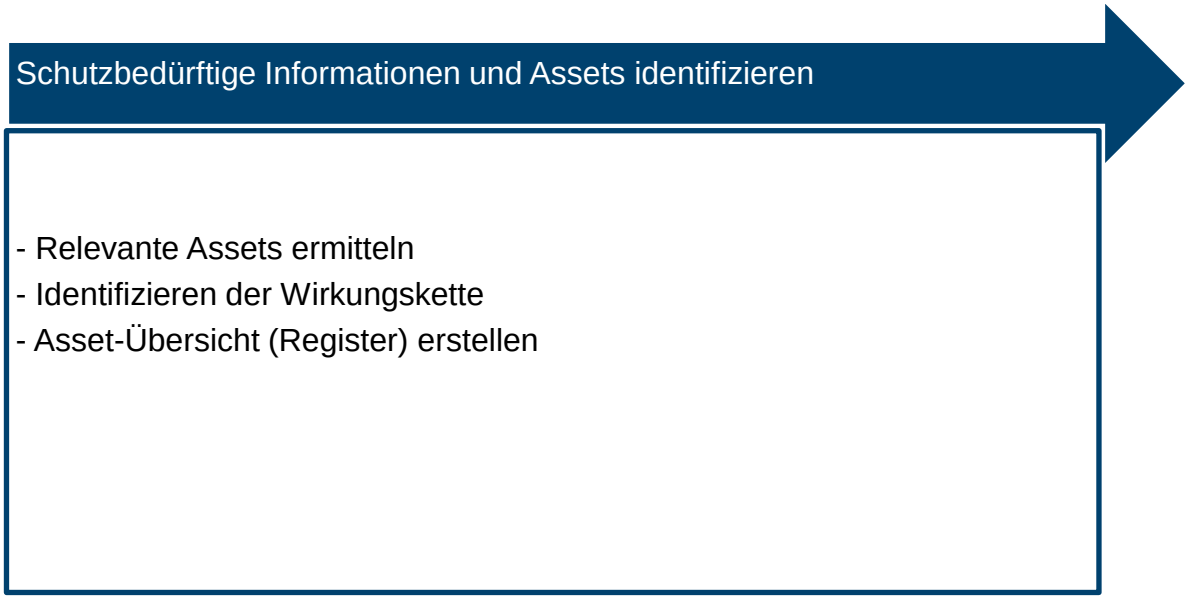


Kontext der Organisation und Scope festlegen

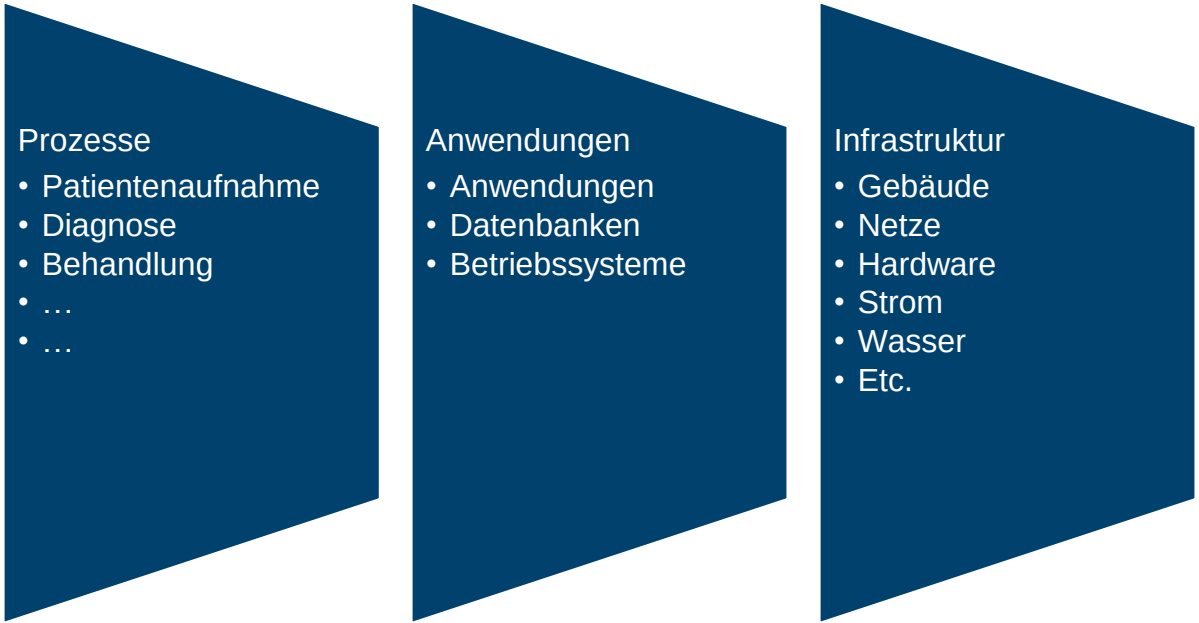
Kontext der Organisation und Geltungsbereich (Scope) festlegen

- Kontext der Organisation ermitteln
- Scope des ISMS
- Sicherheitsleitlinie und Ziele erstellen
- Dokumentations-rahmenwerk erstellen
- ISMS Dokumente erstellen

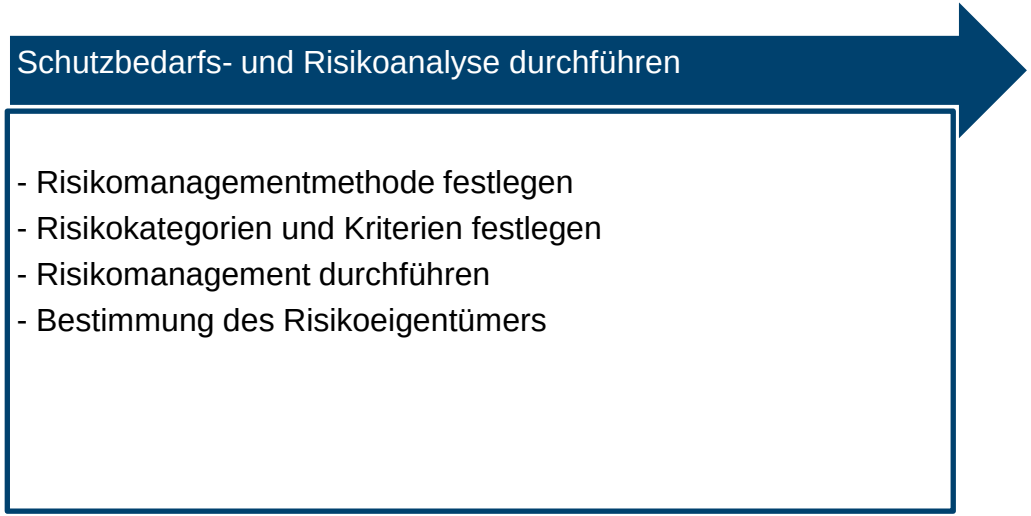
Schutzbedürftige Informationen und Assets identifizieren



Schichtenmodell



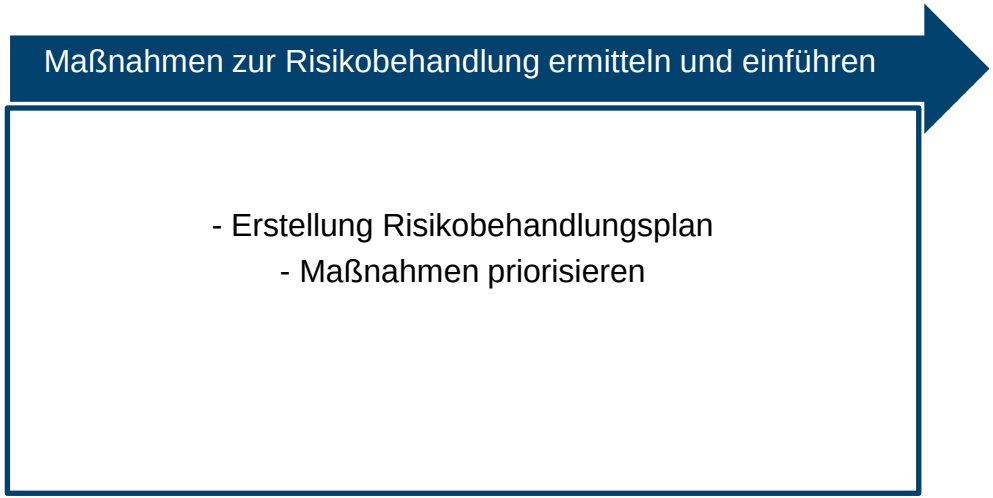
Schutzbedarfs- und Risikoanalyse durchführen



Schutzbedarfsanalyse – Kurz und knapp

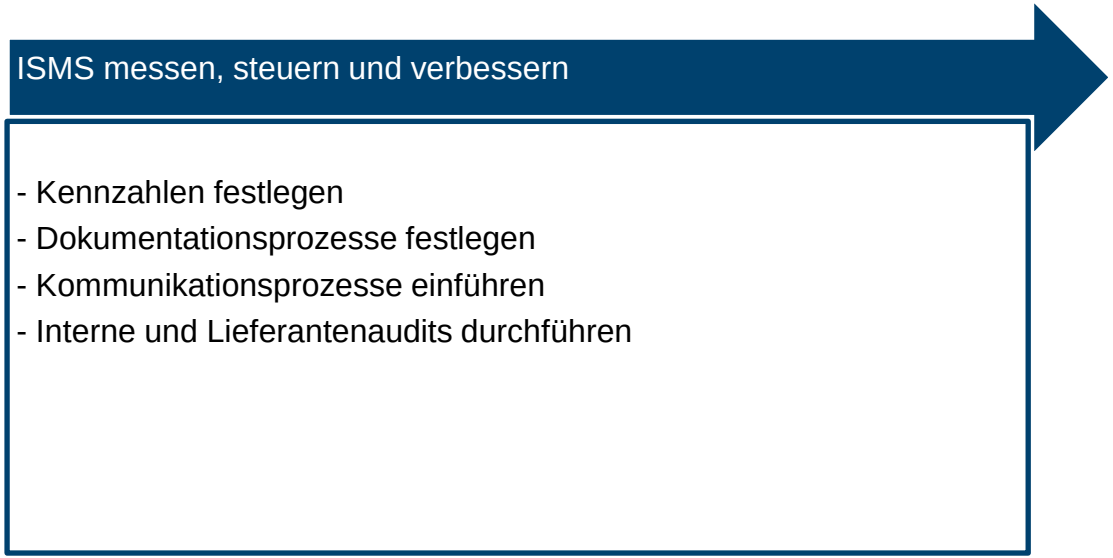
Asset-Beschreibung				Schutzbedarfsanalyse						
Asset	Kundenprozess	Typ	Priorität	Verfügbarkeit	Beschreibung	Vertraulichkeit	Beschreibung	Integrität	Beschreibung	Einstufung
Citrix	Terminalserver-Betrieb	Dienste	1	H	bedrohlich	H	bedrohlich	H	bedrohlich	kritisch
Klimaanlage	Physische- u.	physische Werte	1	H	bedrohlich	G	begrenzt	G	begrenzt	kritisch
Netzwerk	LAN-Betrieb	Dienste	1	H	bedrohlich	H	bedrohlich	H	bedrohlich	kritisch
MS Office	Betrieb Sonstige	Anwendung	2	M	beträchtlich	G	begrenzt	G	begrenzt	unkritisch
KIS Anwendung	Betrieb Klinische Informationssysteme	Anwendung	1	H	bedrohlich	H	bedrohlich	H	bedrohlich	kritisch

Maßnahmen zur Risikobehandlung ermitteln und durchführen



Risikoanalyse in der Praxis – Ein Beispiel

ISMS messen, steuern und verbessern



Die häufigsten Stolperfallen bei der ISMS Einführung

Unklare Rolle und Umfang der ISB-Rolle

Keine klare Definition der Rolle, der Kompetenzen und des Zeitbedarfs des ISB

Ressourcenknappheit in IT-Abteilungen

IT-Abteilungen wurden in der Vergangenheit so lange „optimiert“, dass Mitarbeiterressourcen fehlen. Neue IT-Mitarbeiter zu finden ist schwer, denn es herrscht Arbeitskräfteknappheit in der Branche.

Fehlende Dokumentationen

In organisch gewachsenen IT-Abteilungen wurde von langjährigen Mitarbeitern ein Inselwissen aufgebaut ohne Dokumentationen.

Ungeregelte Beschaffung

Beschaffung nur analog Budget und ohne Absprache zwischen den Fachabteilungen

Integrierte Managementsysteme aus einer Effizienzbetrachtung

Vorteile eines integrierten Managementsystems

Ressourcen sparen

Durch die Nutzung von Synergien können personelle, zeitliche und finanzielle Ressourcen gebündelt und effizient eingesetzt werden

Weniger Dokumente, mehr Transparenz

Mit der Kombination mehrerer Managementsysteme reduziert sich die Dokumentation, da nur noch ein Handbuch geschrieben wird bzw. zwischen den Handbüchern einfach verlinkt werden kann.

Zeitaufwand reduzieren

Audits und Schulungen können gebündelt für alle Managementsysteme stattfinden.

Effizienter Personaleinsatz

Zur Steuerung eines integrierten Managementsystems benötigt eine Organisation in der Regel erheblich weniger Manpower.

Ganzheitliche Betrachtung von Unternehmensprozessen:

Prozesse und Aufgaben können ganzheitlich im Unternehmen analysiert und optimiert werden.

Fazit

- Integrierte Managementsysteme führen in einem Krankenhaus zu einem höheren Sicherheitsniveau bei größtmöglicher Effizienz
- Um valide Ergebnisse zu erhalten muss auf die gleiche Datenbasis zugegriffen werden
- Eine zentrale Dokumentation schafft Transparenz für alle Beteiligten
- Bewertungen müssen harmonisiert und zu standardisiert werden, damit Vergleiche zu vergangenen Zeiträumen zuverlässig und aussagekräftig gemacht werden können und notwendige Maßnahmen getroffen werden können.
- Mit zunehmendem Reifegrad des Managementsystems empfehlen wir eine Standardisierung und Automatisierung von Datenimportstellen.
- In einem integrierten Managementsystem bilden die Technisch- Organisatorischen Maßnahmen (TOM´s) die datenschutzrechtliche Vorgabe und Ergebnis aus den beteiligten Managementsystemen.

Ansprechpartner

Uwe Kauntz
Tel.: 089 / 678204 – 498
Email: uwe.kauntz@sana.de
Website: https://kritiscare.com/

Dr. Christian Mayr
Tel.: 089 / 678204 – 493
Email: christian.mayr@sana.de
Website: https://kritiscare.com/

Robert Färberböck
Tel.: 089 / 678204 – 245
Email: roberg.faerberboeck@sana.de
Website: https://kritiscare.com/

Vielen Dank!

Sana Management Service GmbH

Bereich „KRITIS Care“