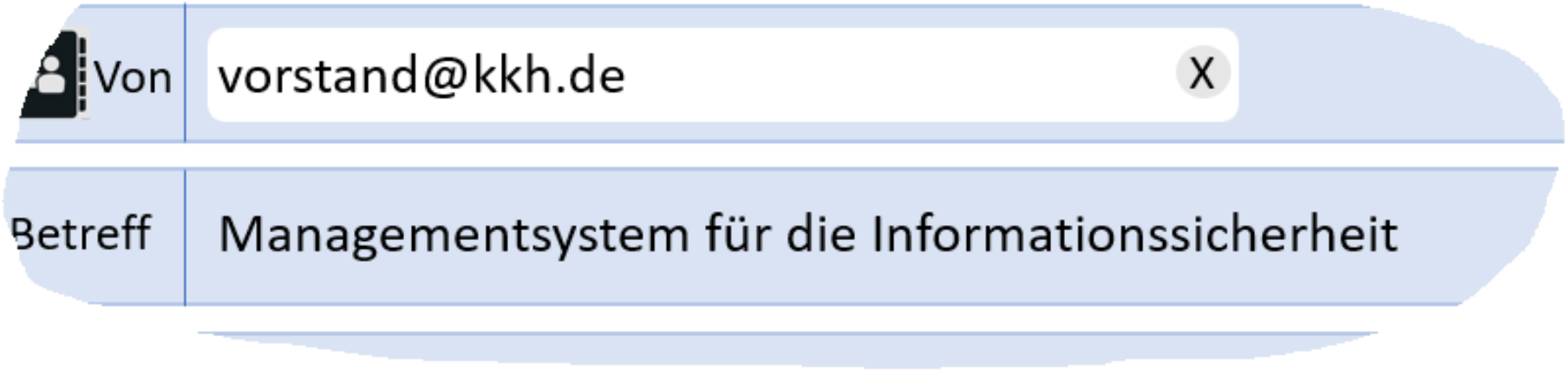
Einführung eines ISMS

Merkur.de

Erneuter Cyberangriff auf die Klinik

Innerhalb von 3 Monaten wurde die Kreisklinik das zweite Mal Opfer eines Cyberangriffes.



Von vorstand@kkh.de X

Betreff Beginn mit der Einführung des ISMS

docx Sicherheitsprozess.docx X

Antworten

Archivieren

Hallo IT-Klasse,

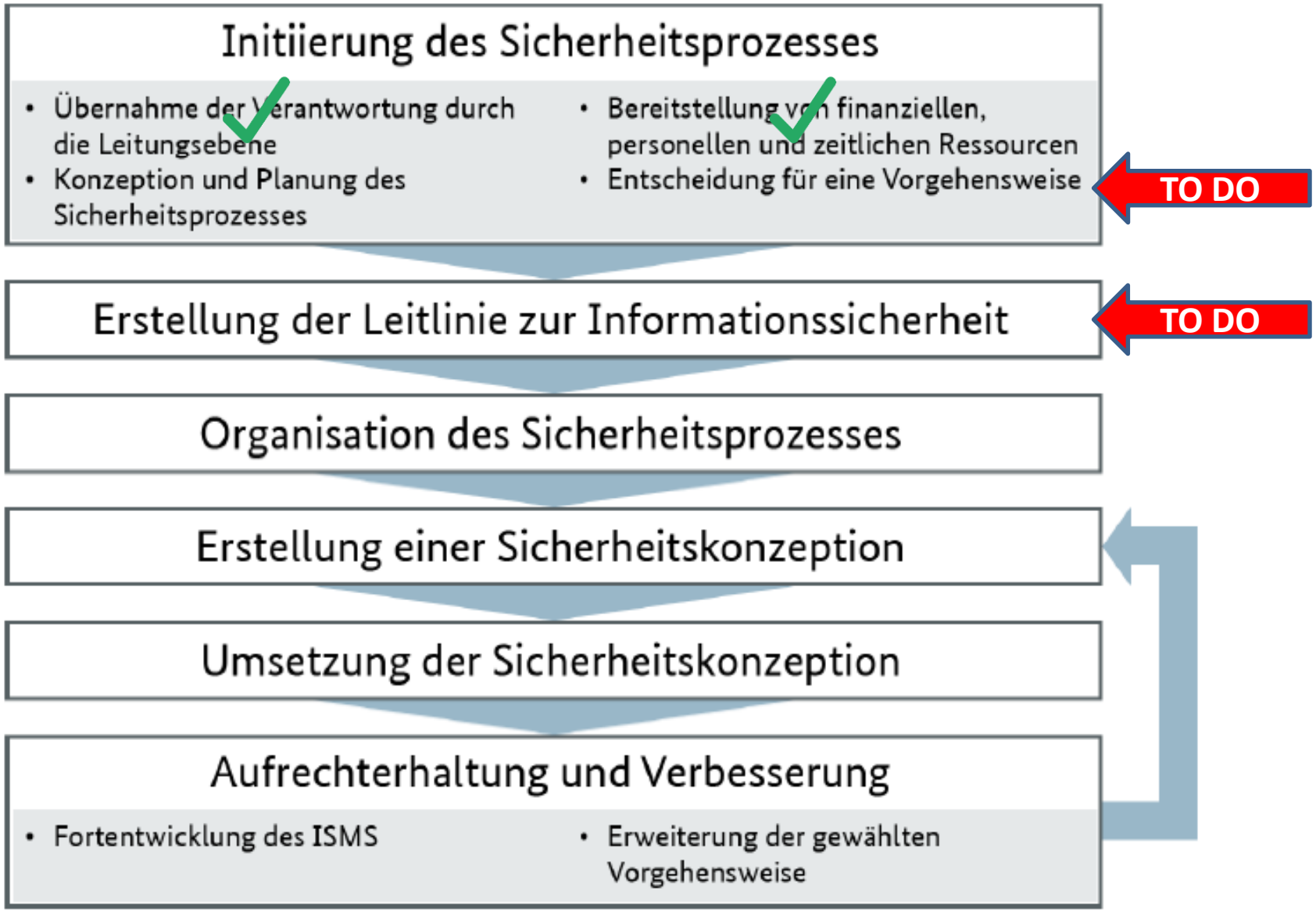
wir haben uns in der letzten IT-Sitzung dazu entschieden, das wir das ISMS als **erstes** in der **Abrechnungsabteilung** einführen möchten, da die Abteilung in beiden Fällen der Angriffspunkt der Täter war.
Die Geschäftsführung übernimmt die Verantwortung und sichert eine angemessene Bereitstellung von finanziellen, zeitlichen und personellen Ressourcen zu!

Laut BSI-Standard müssen wir uns im IT-Grundschutz für eine **Vorgehensweise zur Absicherung** der Geschäftsprozesse und Ressourcen entscheiden.
Bitte unterstützen Sie uns deshalb bei der **Initiierung** des **Sicherheitsprozesses** und der **Auswahl der Vorgehensweise**.

PS: Wir möchten bereits in der nächsten IT-Sitzung die **Leitlinie zur Informationssicherheit** präsentieren.

Beste Grüße
E. Neuwirth
Geschäftsführung

Der Sicherheitsprozess



Entscheidung für eine Vorgehensweise

Aufgabenstellung

- **Informieren** Sie sich über die **möglichen Vorgehensweisen** zur **Absicherung der Geschäftsprozesse und Ressourcen** des Krankenhauses mithilfe des **Informationstextes** *„IT10_LF4_Vorgehensweisen_Absicherung…“***!**

- **Bearbeiten** Sie die **Aufgabenstellung** auf Seite 2!

- **Präsentieren** Sie nach der Bearbeitungszeit Ihre Ergebnisse vor der Klasse!

Bearbeitungszeit: **10 Minuten!**

Besprechung Arbeitsauftrag

Beschreiben Sie, was unter dem IT-Grundschutz zu verstehen ist!

umfangreiche Dokumentensammlung, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird

Welche Bestandteile bilden den Kern des BSI-Grundschutzes?

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS)
- BSI-Standard 200-2: IT-Grundschutz-Methodik
- BSI-Standard 200-3: Risikomanagement
- BSI-Standard 100-4/200-4: Notfallmanagement

+ IT-Grundschutz-Kompendium mit Umsetzungsbeispielen

Besprechung Arbeitsauftrag

Was ist ein "BSI-Grundschutz Baustein"?

- alle Bereiche des ISMS sind in Bausteine untergliedert (übersichtlich).

- beinhalten konkrete Maßnahmen und Umsatzhilfen

prozessorientiert:	ORP: Organisation und Personal
	CON: Konzeption und Vorgehensweise
	OPS: Betrieb
systemorientiert:	DER: Detektion und Reaktion
	APP: Anwendungen
	SYS: IT-Systeme
	IND: Industrielle IT
	NET: Netze und Kommunikation
	INF: Infrastruktur

Besprechung Arbeitsauftrag

Beschreiben Sie kurz die drei Varianten der Absicherung nach dem BSI IT-Grundschutz-Verfahren!

Basisabsicherung:

- Erst-Absicherung, senkt die größten Risiken

Kernabsicherung:

- Focus ist wichtigster Teil des Unternehmens (Kronjuwelen)
- gründliche Absicherung notwendig

Standardabsicherung

- angemessene, ausreichende Absicherung aller Prozesse und Bereiche mit normalen Schutzbedarf als Ziel
- empfohlene IT-Grundschutz-Vorgehensweise

Im Rahmen der Kernabsicherung wird von "Kronjuwelen" gesprochen. Was heißt das?

wichtigster Teil (Prozess, Produkt, Abteilung usw.) des Unternehmens (der Kern)

Besprechung Arbeitsauftrag

Vorgehensweisen
Basis-Absicherung

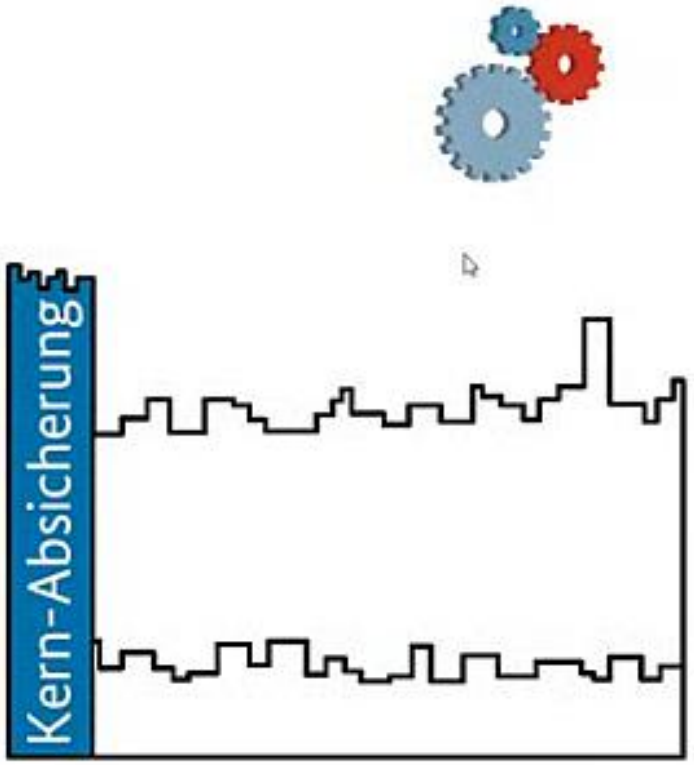
- Vereinfachter Einstieg in das Sicherheitsmanagement
- Grundlegende Erstabsicherung der Geschäftsprozesse und Ressourcen
  - Erstabsicherung in der Breite
  - Umsetzung essentieller Anforderungen
- Auf die Bedürfnisse von KMUs zugeschnitten
- Auch für kleine Institutionen geeignet

Besprechung Arbeitsauftrag

Vorgehensweisen
Kern-Absicherung

- Schutz herausragender, besonders gefährdeter Geschäftsprozesse und Ressourcen (Kronjuwelen)
- Unterschied zu IT-Grundschutz Classic: Fokussierung auf einen kleinen, aber sehr wichtigen Informationsverbund

- Zeitersparnis im Vorgehen
- beschleunigte Absicherung dieser Ressourcen in der Tiefe

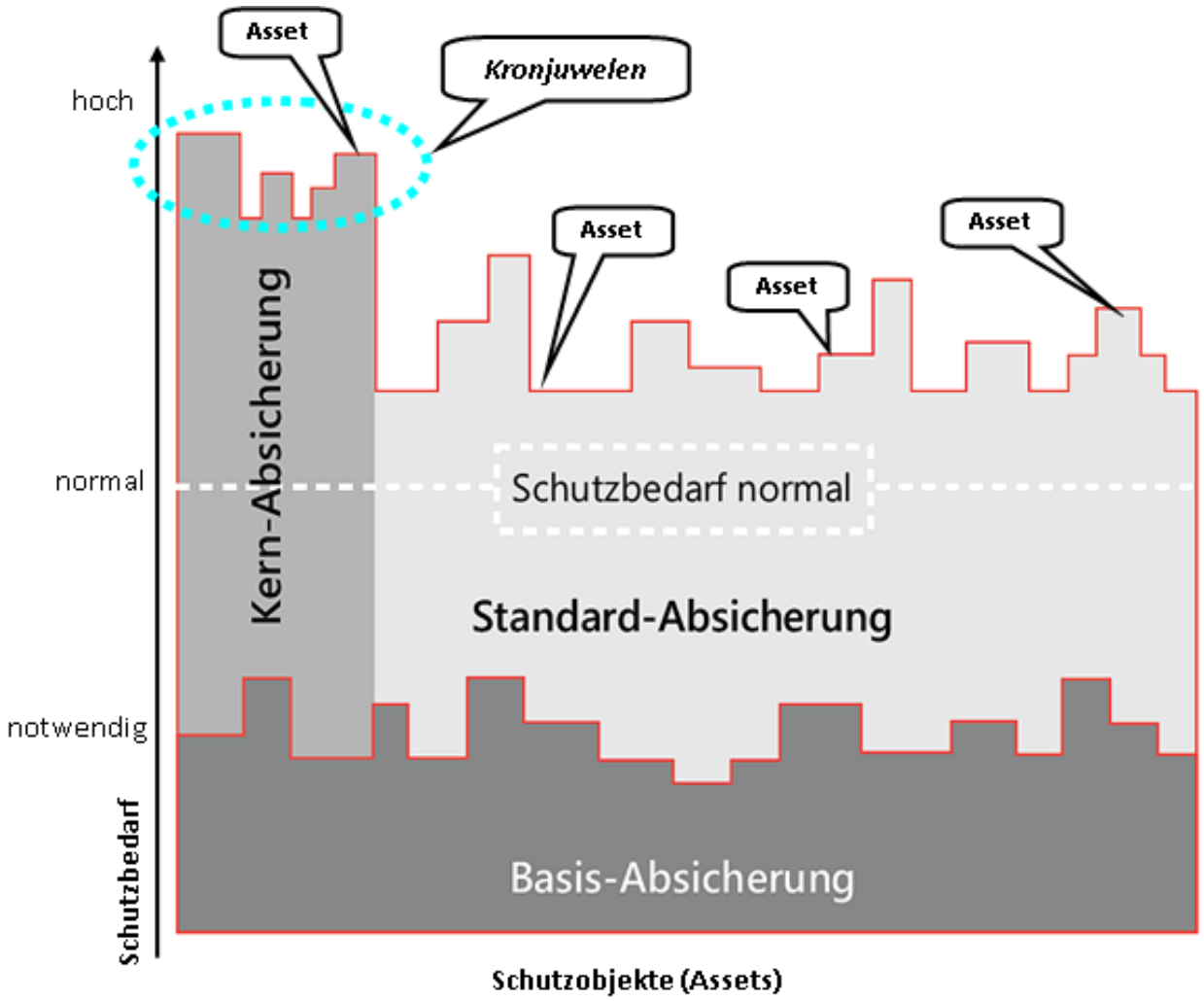


Besprechung Arbeitsauftrag

Vorgehensweisen
Standard-Absicherung

- Die Methode bleibt in den Grundzügen unverändert
- Implementierung eines vollumfänglichen Sicherheitsprozesses nach (jetzigem) BSI-Standard 100-2
- Weiterhin ISO 27001 Zertifizierung auf der Basis von IT-Grundschutz vorgesehen

Besprechung Arbeitsauftrag



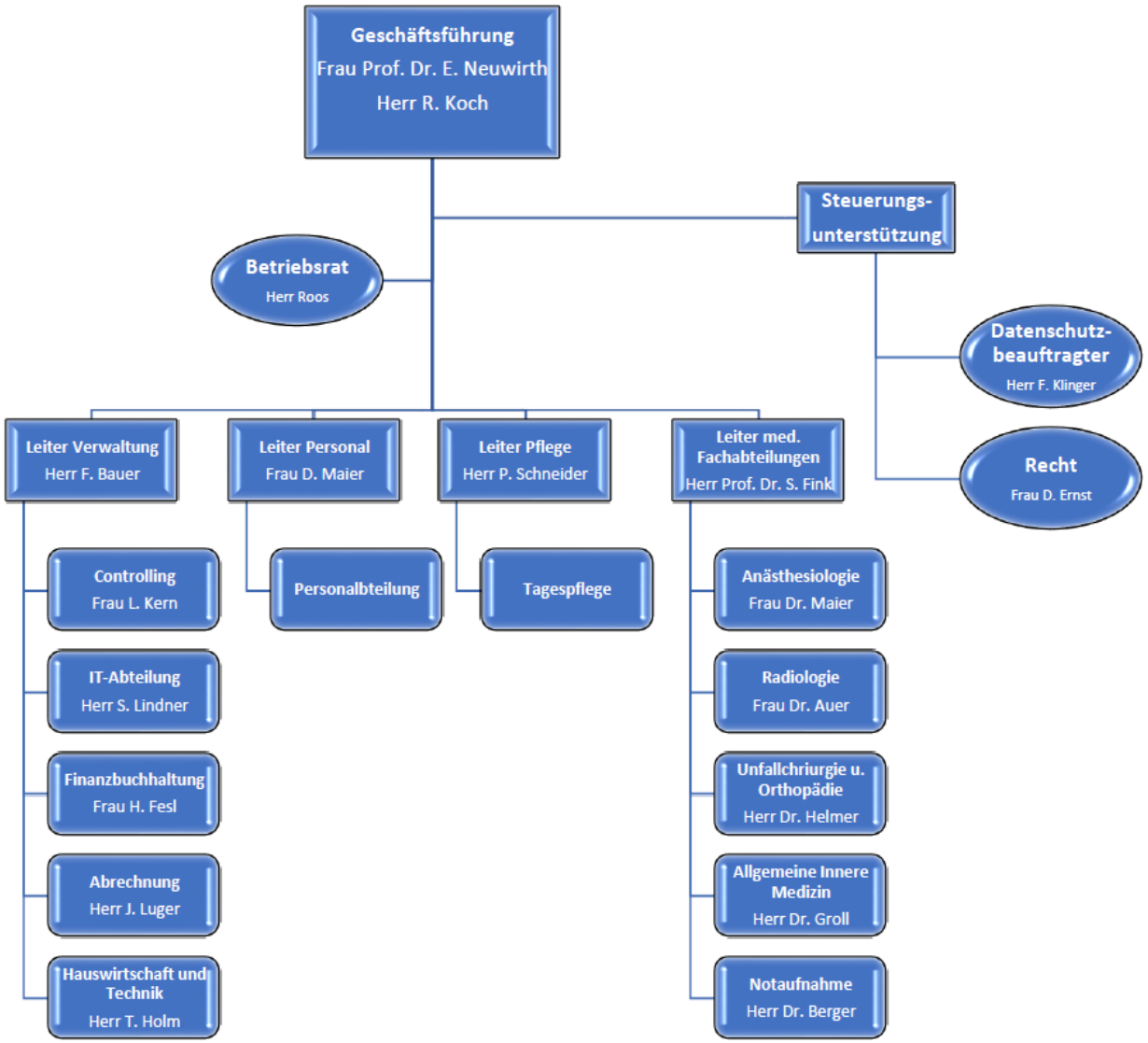
Aufbau des Krankenhauses

Aufgabenstellung

- **Informieren** Sie sich über den **organisatorischen Aufbau** des Krankenhauses mithilfe folgender Dokumente:
  - Organigramm KH
  - Situationsbeschreibung KH

Bearbeitungszeit: **5 Minuten!**

Organigramm KH



ISB im Sicherheitsprozess

Aufgabenstellung

- **Informieren** Sie sich mit Hilfe des **Informationstextes „ISBeauftragter“** über den **Informationssicherheitsbeauftragen (ISB)**!

- **Bearbeiten** Sie die **Aufgabenstellung** auf Seite 2!

- **Präsentieren** Sie nach der Bearbeitungszeit Ihre Ergebnisse vor der Klasse!

Bearbeitungszeit: **10 Minuten!**

Besprechung Arbeitsauftrag

Eigenschaften eines ISB

- Erfahrung und Wissen in der
  - Informationssicherheit
  - allgemeinen IT

- fundamentale Kenntnisse über Geschäftsprozesse der Institution

Besprechung Arbeitsauftrag

Aufgaben des ISB

Ein Informationssicherheitsbeauftragter ist für alle Fragen rund um die Informationssicherheit in der Institution zuständig.

Zu seinen Aufgaben gehört es,

- den Sicherheitsprozess zu steuern und zu koordinieren,
- die Leitung bei der Erstellung der Sicherheitsleitlinie zu unterstützen,
- die Erstellung des Sicherheitskonzepts und zugehöriger Teilkonzepte und Richtlinien zu koordinieren,
- Realisierungspläne für Sicherheitsmaßnahmen anzufertigen sowie ihre Umsetzung zu initiieren und zu überprüfen,
- der Leitungsebene und anderen Sicherheitsverantwortlichen über den Status der Informationssicherheit zu berichten,
- sicherheitsrelevante Projekte zu koordinieren,
- sicherheitsrelevante Vorfälle zu untersuchen sowie
- Sensibilisierungen und Schulungen zur Informationssicherheit zu initiieren und zu koordinieren

Besprechung Arbeitsauftrag

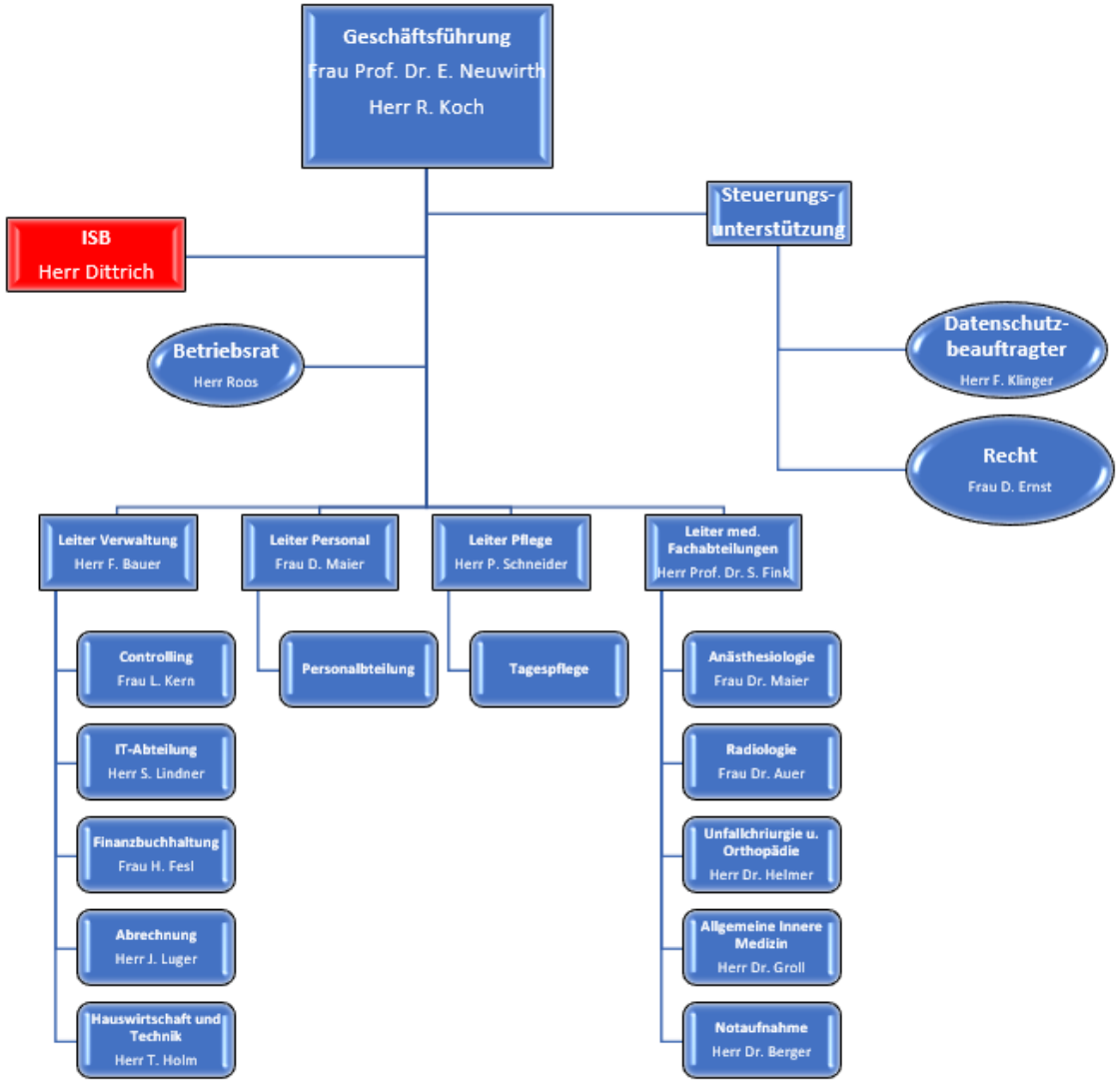
Der geeignete ISB im Krankenhaus

- Herr Dittrich
- lange genug im Unternehmen
- gute Kenntnisse in der IT-Sicherheit
- hat bereits Erfahrung in anderem Unternehmen gesammelt
- hat keine andere (konfliktbehaftete) Rolle (z.B. Datenschutzbeauftragter)

Einordnung in das Organigramm

- als Stabstelle direkt der Geschäftsführung zugeordnet
- dadurch ist direkte Kommunikation gewährleistet

Organigramm KH



IS-Management-Team

Aufgabenstellung

- **Informieren** Sie sich mit Hilfe des **Informationstextes „ISM_Team“** über das **IS-Management-Team**!

- **Bearbeiten** Sie die **Aufgabenstellung** auf Seite 2!

- **Präsentieren** Sie nach der Bearbeitungszeit Ihre Ergebnisse vor der Klasse!

Bearbeitungszeit: **10 Minuten!**

Besprechung Arbeitsauftrag

Personengruppen die Mitglied im IS-Management-Team sein sollten

- Herr Dittrich (ISB)
- Herr Klinger (Datenschutzbeauftragter)
- Frau Ernst (Juristin)
- IT-Abteilung
- Herr Bauer (Leiter Verwaltung)
- Herr Luger (Teamleiter Abrechnung)

Besprechung Arbeitsauftrag

Aufgaben des IS-Management-Team

- die Sicherheitsziele und -strategien festlegen sowie die Leitlinie zur Informationssicherheit entwickeln,
- die Umsetzung der Sicherheitsleitlinie überprüfen,
- den Sicherheitsprozess initiieren, steuern und kontrollieren,
- bei der Entwicklung des Sicherheitskonzepts mitwirken,
- überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen geeignet und wirksam sind und wie beabsichtigt funktionieren,
- Schulungs- und Sensibilisierungsprogramme für Informationssicherheit konzipieren sowie
- die Fachverantwortlichen, den IT-Betrieb, eventuell die ISB für einzelne Bereiche und den ICS-ISB sowie die Leitungsebene beraten.

Besprechung Arbeitsauftrag

Entscheiden Sie, ob das Krankenhaus ein IS-Management-Team aufbauen oder mehrere ISBs bestimmen sollte!

- IS-Management-Team
- nur Einführung in der Abrechnungsabteilung
- nur ein Standort

Erstellen einer Sicherheitsleitlinie

Aufgabenstellung für die einzelnen Gruppen!

- **Bilden** Sie **3er** Gruppen!
- **Informieren** Sie sich über den Aufbau einer **Sicherheitsleitlinie**!

- **Verwenden** Sie dazu den **Informationstext** in **„IT10_LF4_Leitlinie“**!
- **Bearbeiten** Sie den **Arbeitsauftrag** (Seite 2) auf dem **Informationstext**!
  - **Tipp:** Das Dokument **„IT10_LF4_Beispiel_Leitlinie“** hilft Ihnen dabei!

- **Laden** Sie Ihr Dokument in den **Ordner** „06_Ergebnisse_Leitlinie“ hoch!

- **Präsentieren** Sie nach der Bearbeitungszeit Ihre Ergebnisse!

Bearbeitungszeit: **30 Minuten!**

An vorstand@kkh.de X

Senden

Betreff AW: Beginn mit der Einführung des ISMS

Von/CC/BCC

Sicherheitsleitlinie.docx X

B I U Mehr

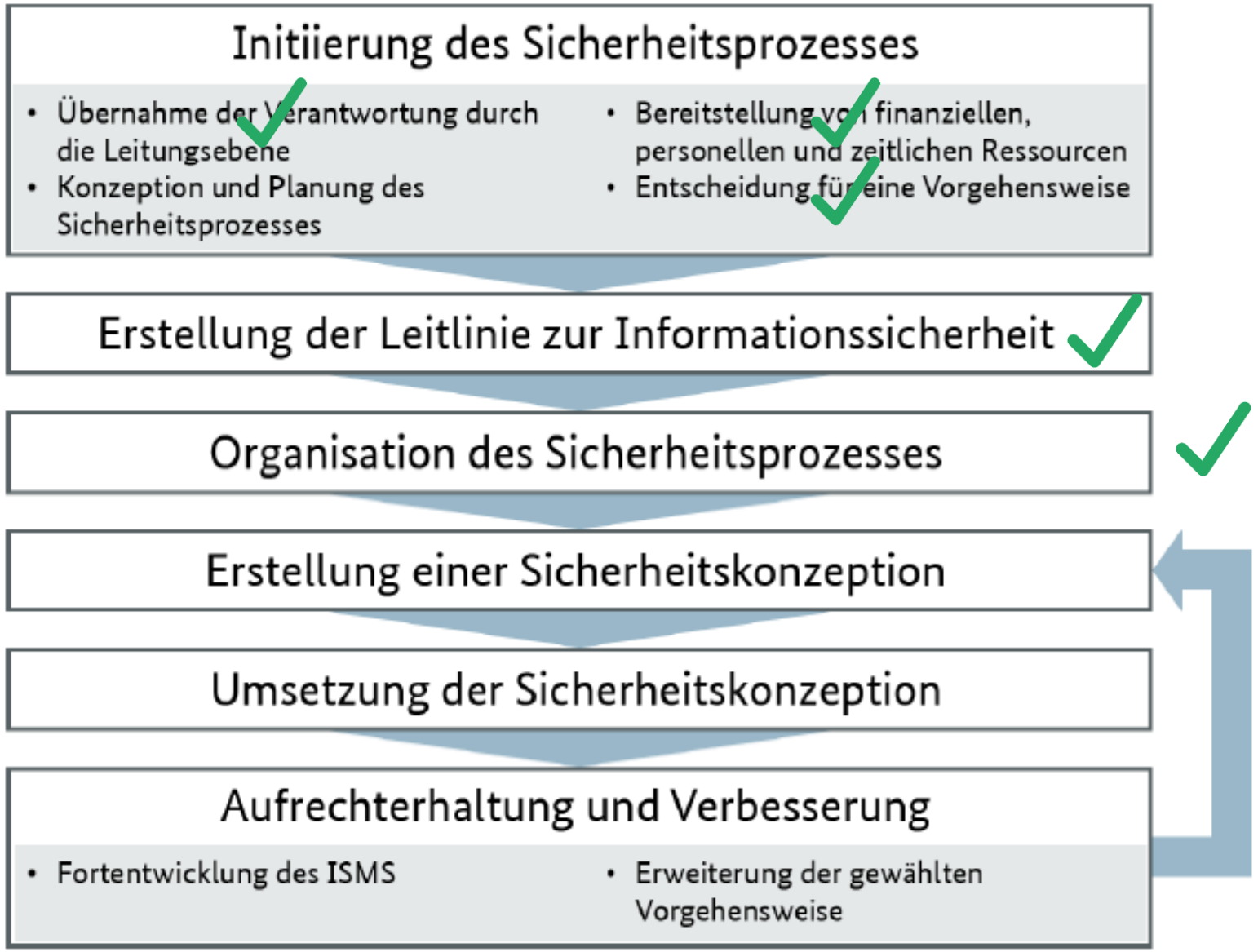
Sehr geehrte Frau Neuwirth,

anbei finden Sie die Leitlinie zur Informationssicherheit.

Viel Erfolg in der nächsten IT-Sitzung.

Beste Grüße
IT´ler

Fortschritt im Sicherheitsprozess



Fragenkatalog

- Welches Modell liegt dem in BSI-Standard 200-1 beschriebenen Sicherheitsprozess zugrunde?

- Was sollte eine Leitlinie zur Informationssicherheit enthalten?

- Beschreiben Sie die Aufgaben des Informationssicherheitsbeauftragten!
- Wie setzt sich ein IS-Management-Team geeignet zusammen?
- Wer ist für die Freigabe der Leitlinie zur Informationssicherheit verantwortlich?

- Nennen Sie die drei möglichen Vorgehensweisen zur Absicherung der Informationssicherheit!
- Welches Absicherungskonzept schützt die Kronjuwelen des Unternehmens?
- Warum kann es sinnvoll sein, sich für die Basis-Absicherung zu entscheiden?
- Was versteht man unter einem BSI Grundschutzbaustein?