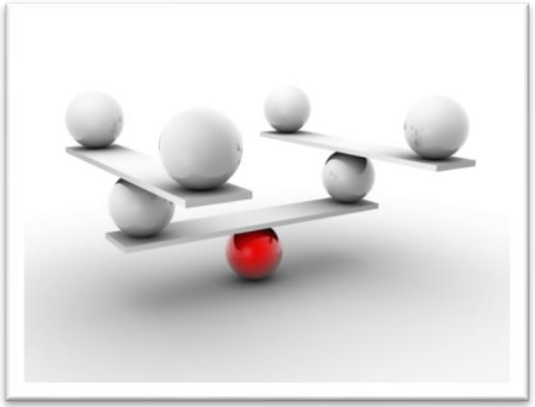
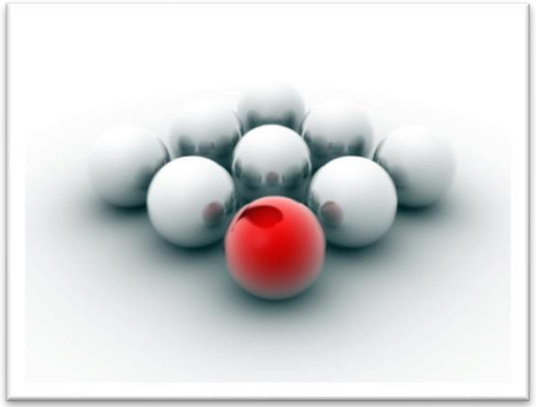
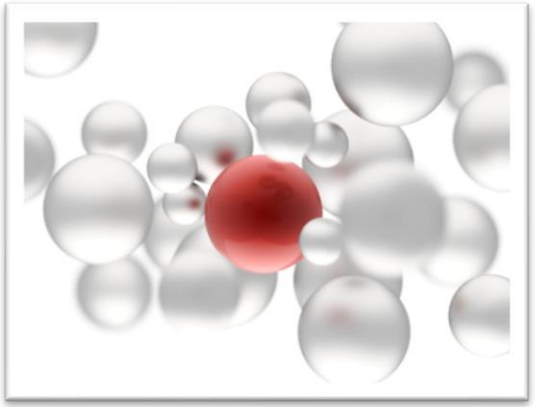
CETUS
Health · IT · Leadership







Risikoanalyse Krankenhaus IT – gepr. IT-Sicherheitsmanager med IT Netze

Risiken ohne Nebenwirkungen.

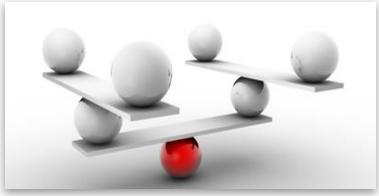
- ✓ Begrüßung und Vorstellung / Zielsetzung
- ✓ Der RiKrIT Leitfaden – und jetzt?
- ✓ Risikoanalyse IT – Voraussetzungen und Methode
  … was will das BSI von Ihnen?
- ✓ Risikoanalyse am Beispiel einer Notaufnahme
  … so sieht das in der Praxis aus!
- ✓ RiKrIT Schnittstellen
  … das haben andere von RiKrIT!

RIKRIT GESCHICHTE

RiKrIT - Ausgangslage

2005

- Etablierung des NPSI
- Analyse kritischer Infrastrukturen
- Aufbau einer nationalen Strategie mit Umsetzungsplan



2008

- Untersuchungen durch das BMI
- Ergebnis: Gefährdungslage ist durch zunehmende Abhängigkeit von der IT erhöht.
- Aufträge an das BSI, nach Lösungen zu suchen

2009

- Untersuchungen des BBK
- Ergebnis: Fokussierung auf IT-Notfälle ist notwendig
- Rettungs- und Notfallinfrastruktur ist abhängig von IT-Nutzung

RiKrIT Ziele

Eine relativ neue Form von Risiken wird in bisherigen Leitfäden jedoch nicht in aller Tiefe betrachtet: **der Ausfall oder die Störung von wichtigen IT-Systemen im Krankenhaus**

Ziel 1: Detaillierung des Risiko- und Krisenmanagements der Krankenhäuser **im Bereich IT** durch einen eigenen Leitfaden

Ziel 2: Erfassung **von IT-Abhängigkeiten** und die sich dabei ergebenden Risiken

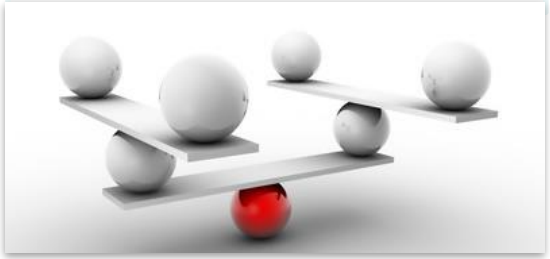
Ziel 3: Forderung eines **Risikomanagements** der IT im Krankenhaus

Methodik: vorherrschend BSI-Standards und ISO/IEC 27001:2008 ff.

RiKrIT Projektziele

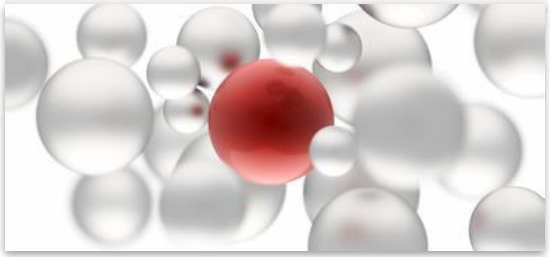
Methodik

- Vorgehensweise für die Erhebung von Prozessen
- Erfassen der beteiligten IT-Komponenten
- Definition der Schutzziele für den Krankenhausbetrieb (Krisenfall)



Werkzeuge

- Fragenkatalog für Krankenhäuser
- Vorgehensmodell für eine Risikoanalyse der Krankenhausinfrastruktur
- Maßnahmenkatalog mit Handlungsempfehlungen



Ergebnisse

- Leitfaden mit Praxisbeispielen
- Typische IT-Risiken und Maßnahmen

RIKRIT – SO STARTEN SIE!

Wer benötigt RiKrIT überhaupt?

- Krankenhäuser, die zu den Kritischen Infrastrukturen zählen – aber nicht zwingend alle!
- Alle Krankenhäuser haben die Verpflichtung, die Verfügbarkeit ihrer Dienste und der Prozesse sicherzustellen
- Die Unterstützung aller Geschäftsprozesse und Kernprozesse in der medizinischen & pflegerischen Patientenversorgung durch (IT) wird immer stärker
- Ausfälle beeinträchtigen im Extremfall die Patientenversorgung ganzer Regionen

Was leistet RiKrIT?

- Integration der IT-Risikoanalyse in das Informationssicherheits- oder Notfallmanagement (falls vorhanden!)
- Die IT-Risikoanalyse ist ein wichtiges Instrument im Risikomanagement eines Krankenhauses!
- Aufgabe IT-Risikoanalyse ist Identifizierung & Bewertung der Ausfallrisiken aufgrund kritischer IT-Abhängigkeiten
- Nach IT-Risikoanalyse hat das Risikomanagement die Aufgabe, identifizierte Risiken zu behandeln und risikomindernde Maßnahmen zu planen und umzusetzen
- RiKrIT bietet dafür die Arbeitsgrundlage!

Was ist die Motivation für RiKrIT

CETUS
Health · IT · Leadership

- ✓ Falls die Krankenhausleitung nicht weiß, wie wichtig die IT-Unterstützung der Prozesse ist rechnen Sie es einfach vor:

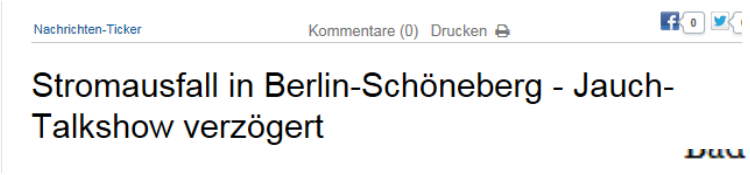
- ✓ 90 Elektivaufnahmen je Tag x 3.035,50 EUR
  = 273.195,00 EUR Umsatz pro Tag

- ✓ Fallpauschalenfaktor, z.B. 1,267 = 273.195,00 EUR x 1,267
  = **346.138,07 EUR pro Tag**

- ✓ **Falls Ihr Krankenhaus es schafft, ohne IT-Unterstützung und nur „zu Fuß“ diese Fallzahl pro Tag zu bewältigen, zu versorgen und dabei noch effizient zu sein, vergessen Sie RiKrIT – falls nicht, sollte Ihr Geschäftsführer nachdenken!**

Die Motivation geht weiter…

- ✓ Das IT-Sicherheitsgesetz fordert IT-Sicherheitskonzepte – RiKrIT bietet hier eine gute Methode
- ✓ Krankenhäuser sind verpflichtet, im Großschadensfall eine Versorgung sicherzustellen – wer kann das wirklich?


Nachrichten-Ticker Kommentare (0) Drucken

Stromausfall in Berlin-Schöneberg - Jauch-Talkshow verzögert


Wegen zwei defekter Starkstromkabel

Wieder Stromausfall in Bad Nauheim

traf mehrere zehntausend Menschen. Die Kliniken in Bad Nauheim und Friedberg aktivierten ihre Notversorgung und Geschäfte mussten schließen.


Patient stirbt nach Stromausfall in Schweriner Krankenhaus

Mittwoch, 30.10.2013, 13:24


Schumachers Krankenakte gestohlen

Größtmögliche Verletzung der Privatsphäre droht

Der richtige Start – Motivation der Leitung

	Ja	Nein
Können Sie ausschließen, dass Patienten durch nicht berücksichtigte Risiken zu Schaden kommen?		
Können Sie uneingeschränkt bestätigen, dass Ihre Medizintechnik und die IT-Infrastruktur jederzeit verfügbar, sicher und ohne unbekannte Lücken betrieben werden?		
Können Sie bestätigen, dass die Abteilungen Medizintechnik und IT gemeinsam an einem Strang ziehen?		
Können Sie ausschließen, dass lebenswichtige Netzwerke nicht überraschend ausfallen können?		
Werden Sie von IT und Medizintechnik regelmäßig über alle Risiken der eingesetzten Infrastruktur informiert?		
Verfügt Ihr Krankenhaus über ein IT- und Medizintechnik Notfallmanagement?		
Können Sie bestätigen, dass Sie über alle Risiken und Veränderungen an der Infrastruktur von IT und Medizintechnik informiert werden?		
Treffen Sie als Geschäftsführer die Entscheidungen, wie mit Risiken umgegangen wird?		
Können Sie ausschließen, dass Sie durch nicht berücksichtigte Risiken Sicherheitslücken in der Infrastruktur haben?		

- ✓ Falls ein Geschäftsführer nur eine der nebenstehenden Fragen mit „Nein“ beantwortet, hat er Handlungsbedarf!
- ✓ Klären Sie auf, Sie benötigen die Unterstützung „von oben“.

Was will das BSI von Ihnen?

RIKRIT – VORAUSSETZUNGEN UND METHODE

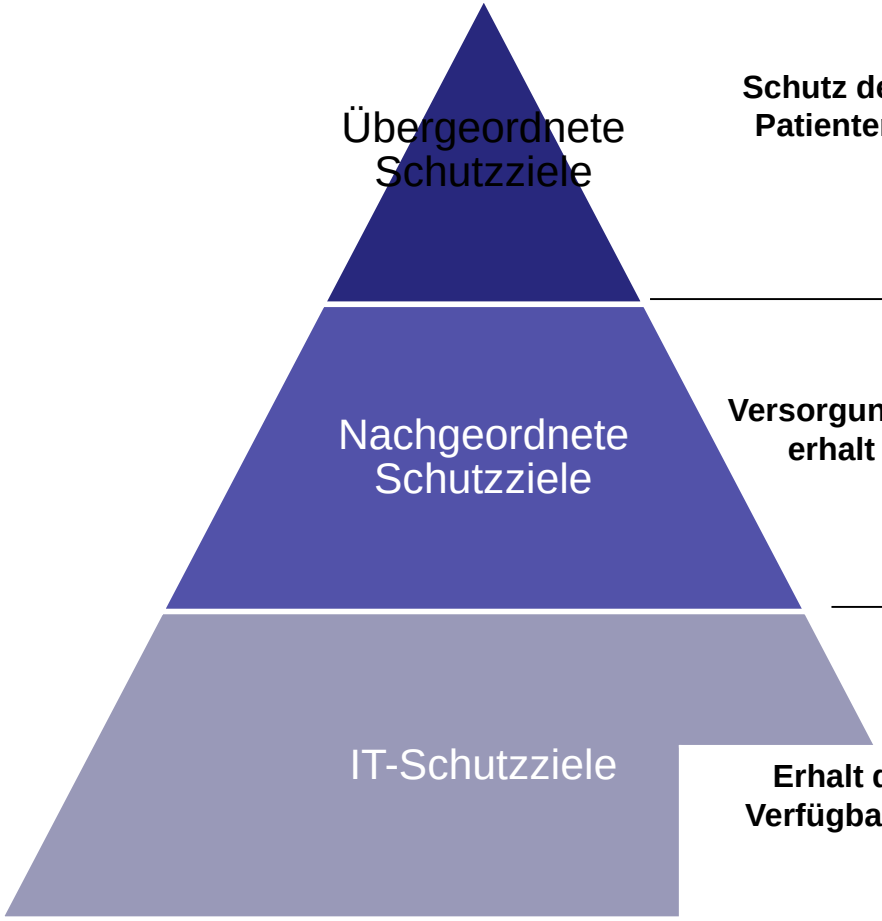
Der Startpunkt – ein Projektplan

Phase	Aktivitäten
Vorbereitende Aktivitäten	1. IT-Risikoanalyse als Projekt initialisieren 2. Schutzziele festlegen (Schutz der Patienten & der Einrichtung) 3. Untersuchungsbereich abgrenzen 4. Prozesse (Kern- und Unterstützungsprozesse) erheben
Kritikalität analysieren	5. Kritische Prozesse ermitteln 6. IT-Unterstützung ermitteln (Anwendersicht & IT-Sicht) 7. Kritikalität der IT-Unterstützung bestimmen 8. Kritische IT-Komponenten ermitteln
Risiken identifizieren & bewerten	9. Risikoszenarien ermitteln 10. Eintrittswahrscheinlichkeiten abschätzen 11. Auswirkungen bewerten 12. Risikowert ermitteln 13. Bestehende Maßnahmen berücksichtigen
Risiken behandeln	14. Behandlung der Risiken entscheiden 15. Präventive Maßnahmen bestimmen & Ersatzverfahren vorsehen

Welche Rollen können sind beteiligt?

Phase	Aktivitäten
Vorbereitende Aktivitäten	1. IT-Risikoanalyse als Projekt initialisieren 2. Schutzziele festlegen (Schutz der Patienten & der Einrichtung) 3. Untersuchungsbereich abgrenzen 4. Prozesse (Kern- und Unterstützungsprozesse) erheben **Beteiligte:** Geschäftsführung, medizinische Leitung, IT-Leitung, Prozessmanagement, Qualitäts- und Risikomanagement
Kritikalität analysieren	5. Kritische Prozesse ermitteln 6. IT-Unterstützung ermitteln (Anwendersicht & IT-Sicht) 7. Kritikalität der IT-Unterstützung bestimmen 8. Kritische IT-Komponenten ermitteln **Beteiligte:** IT-Leitung, Prozessmanagement, Qualitäts- und Risikomanagement
Risiken identifizieren & bewerten	9. Risikoszenarien ermitteln 10. Eintrittswahrscheinlichkeiten abschätzen 11. Auswirkungen bewerten 12. Risikowert ermitteln 13. Bestehende Maßnahmen berücksichtigen **Beteiligte:** IT-Leitung, Qualitäts- und Risikomanagement, Anwendervertreter
Risiken behandeln	14. Behandlung der Risiken entscheiden 15. Präventive Maßnahmen bestimmen & Ersatzverfahren vorsehen **Beteiligte:** Krankenhausleitung, Risikomanagement, Prozessverantwortliche

Festlegen der Schutzziele



Schutz des Patienten

Gesundheitliche Zustand des Patienten darf sich nicht aufgrund unterbleibender oder qualitativ/quantitativ eingeschränkter Behandlung bedingt durch Ausfälle oder Störungen der IT im Krankenhaus verschlechtern

Versorgungs-erhalt

Aufgrund von Ausfällen der IT-Infrastruktur ist es nicht tolerierbar, dass Speisen-, Wasser- sowie Medikamentenver- und entsorgung beeinträchtigt werden.

Erhalt der Verfügbarkeit

IT-Störungen dürfen nicht dazu führen, dass die medizinischen Versorgungskapazitäten nicht mehr in angemessener Qualität und Quantität aufrecht erhalten werden können.

Beispielhafte Dokumentation

Übergeordnetes Schutzziel	Definition
Schutz des Patienten	Gesundheitliche Zustand des Patienten darf sich nicht aufgrund unterbleibender oder qualitativ/quantitativ eingeschränkter Behandlung bedingt durch Ausfälle oder Störungen der IT im Krankenhaus verschlechtern

IT-Schutzziele	Übergeordnetes Schutzziel: Schutz der Patienten
Verfügbarkeit	IT-Störungen dürfen nicht dazu führen, dass die medizinische Versorgungskapazitäten nicht mehr in angemessener Qualität und Quantität aufrechterhalten werden können
Integrität	IT-Störungen dürfen nicht dazu führen, dass Daten verfälscht werden, deren Richtigkeit für die Versorgung des Patienten unbedingt erforderlich ist
Vertraulichkeit	IT-Störungen dürfen nicht dazu führen, dass Daten • Deren Bekanntwerden sekundär zu einer Beeinträchtigung der Verfügbarkeit oder Integrität von Systemen und/oder Daten führt oder • Die für die sichere Versorgung des Patienten nur einem berechtigten Personenkreis bekannt sein dürfen, unberechtigten Dritten zugänglich werden.

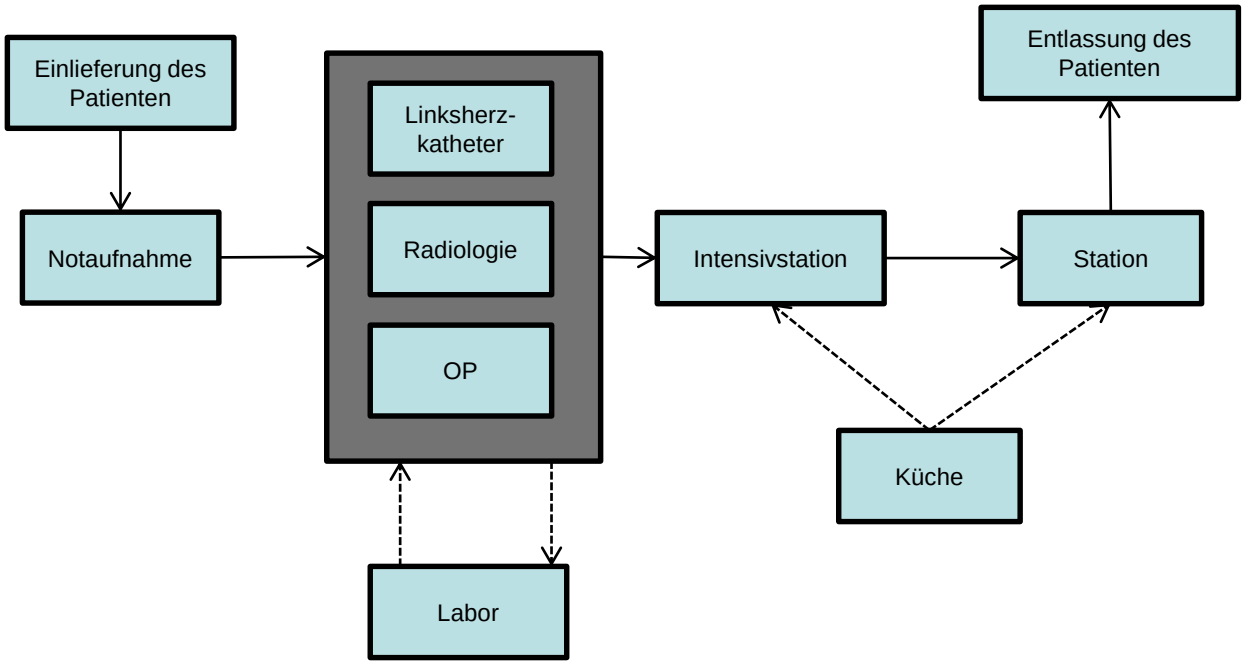
Untersuchungsbereich abgrenzen

- ✓ Nur ein Teil oder alles – was soll betrachtet werden?
- ✓ Keine Pauschalantwort möglich, hängt von den Gegebenheiten ab.
- ✓ Empfehlung: Identifizieren Sie die wirklich kritischen Bereiche in Ihrem Krankenhaus!

Kriterien (Beispiel):

- ✓ Relevanz der IT-Unterstützung für die Patientenversorgung.
- ✓ Relevanz für das Funktionieren des Gesamtbetriebes.
- ✓ Relevanz der IT-Verfügbarkeit für den Behandlungserfolg?
- ✓ usw.

Beispiel aus RiKrIT – Abbildung 1



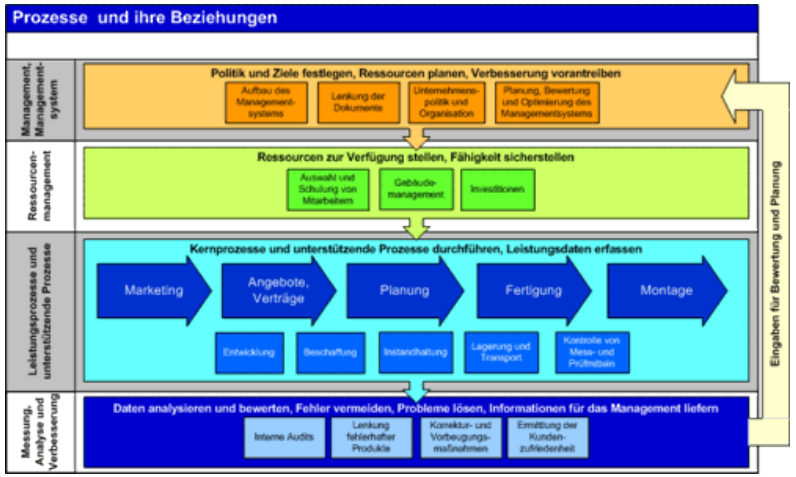
- ✓ Abgrenzung durch Prozessdefinition
- ✓ Setzt Prozessmodelle voraus
- ✓ Benötigt Unterstützung aus dem Prozessmanagement oder QM

Prozesse im Untersuchungsbereich erheben

Organisationseinheit	Prozess
Intensivstation	Aufnahme, Behandlung, Dokumentation, Verlegung / Entlassung, Abrechnung, …
Radiologie	Radiologische Diagnostik, Radiologische Befundung, Abrechnung, DICOM-Datenübertragung, …
Chirurgische Station	Stationäre Behandlung, Pflegedokumentation, Speisenanforderung, …
Notaufnahme	Aufnahme, Anamnese, Diagnostik, Therapie, Betreuung, …
Labor	Probenbestätigung, Probenverteilung, Befundrückmeldung Blutkonservenbereitstellung, …
Küche	Verpflegung, Speisendokumentation, Rückverfolgung, Hygienedokumentation, …

Hilfsmittel zur Prozessanalyse

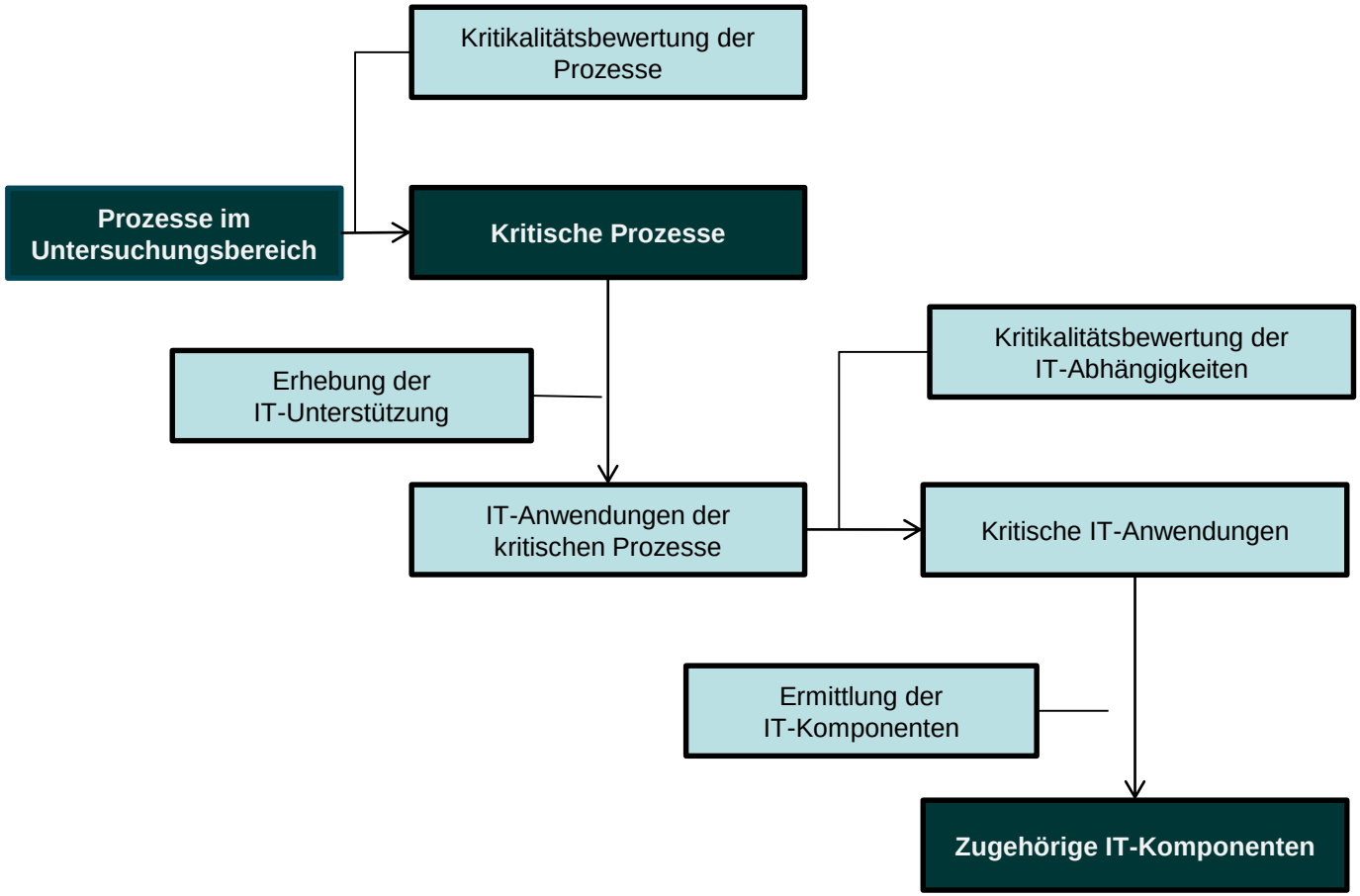
- ✓ Prozessdiagramme
- ✓ Big-Picture – Prozesslandkarte
- ✓ Qualitätsmanagementdokumentation
- ✓ Anwenderinterviews



Zwischenstand – was ist erledigt?

Phase	Aktivitäten
Vorbereitende Aktivitäten	1. IT-Risikoanalyse als Projekt initialisieren 2. Schutzziele festlegen (Schutz der Patienten & der Einrichtung) 3. Untersuchungsbereich abgrenzen 4. Prozesse (Kern- und Unterstützungsprozesse) erheben
Kritikalität analysieren	5. Kritische Prozesse ermitteln 6. IT-Unterstützung ermitteln (Anwendersicht & IT-Sicht) 7. Kritikalität der IT-Unterstützung bestimmen 8. Kritische IT-Komponenten ermitteln
Risiken identifizieren & bewerten	9. Risikoszenarien ermitteln 10. Eintrittswahrscheinlichkeiten abschätzen 11. Auswirkungen bewerten 12. Risikowert ermitteln 13. Bestehende Maßnahmen berücksichtigen
Risiken behandeln	14. Behandlung der Risiken entscheiden 15. Präventive Maßnahmen bestimmen & Ersatzverfahren vorsehen

Kritikalität analysieren



Kriterien formulieren

- ✓ Welche Auswirkungen hat ein Ausfall des Prozesses auf die Patientensicherheit?
- ✓ Wann ist der Ausfall eines Prozesses kritisch für klinische Abläufe?
- ✓ Hat der Ausfall eines Prozess vertragliche oder kaufmännische Folgen?
- ✓ Welche Umweltschäden können bei Ausfall eines Prozesses drohen?

Beispielhafte Kriterien

Kategorie	Verfügbarkeit (MTA)	Integrität	Vertraulichkeit
Sehr hoch	Weniger als 4 Std	Kompromittierung betrifft behandlungs- und lebensnotwendige Daten und/oder IT-Systeme	Vertraulichkeitsverluste betreffen behandlungs- und lebensnotwendige Daten und/oder IT-Systeme
Hoch	Zwischen 4 und 24 Std	Kompromittierung betrifft behandlungs- aber nicht lebensnotwendige Daten und/oder IT-Systeme	Vertraulichkeitsverluste betreffen behandlungs- aber nicht lebensnotwendige Daten und/oder IT-Systeme
Normal	Mehr als 24 Std	Kompromittierung betrifft allgemeine, nicht behandlungs- oder lebensnotwendige Daten und/oder IT-Systems	Vertraulichkeitsverluste betreffen allgemeine, nicht behandlungs- oder lebensnotwendige Daten und/oder IT-Systeme

Beispielhafte Dokumentation

Organisations-einheit	Prozess	Kritikalität (ja / nein)	Begründung
Intensivstation	Aufnahme	Ja	Verzögerungen können sich gravierend auf die Gesundheit des Patienten auswirken
	Behandlung	Ja	Verzögerungen können sich gravierend auf die Gesundheit des Patienten auswirken
	Verpflegung / Entlassung	Nein	Verzögerungen im Rahmen des festgelegten Kriteriums wirken sich nicht kritisch auf die Gesundheit des Patienten aus
Radiologie	Radiologische Diagnostik	Ja	Verzögerungen können sich gravierend auf die Gesundheit des Patienten auswirken
Chirurgische Station	Stationäre Behandlung	Ja	Verzögerungen können sich gravierend auf die Gesundheit des Patienten auswirken

IT-Unterstützung dokumentieren

Organisations-einheit	Prozess	IT-Unterstützung	MTA	Begründung
Intensivstation	Aufnahme	KIS, PDMS	2	Die Aufnahme eines Patienten auf die innere Intensiv ist auch ohne IT Unterstützung möglich. Die Nacharbeiten nach mehr als zwei Stunden Ausfall sind jedoch gravierend.
	Behandlung	PDMS	2	Die lebenserhaltende Behandlung ist möglich. Nach zwei Stunden ist jedoch eine Einsichtnahme in die Krankengeschichte unabdingbar.
Radiologie	Radiologische Diagnostik	KIS, RIS, PDMS	6	Das Klinikum verfügt nicht über einen CT-Arbeitsplatz. Ein Ausfall der radiologischen Diagnostik bis zu sechs Stunden hat keine gravierenden Auswirkungen auf die Notfallversorgung der Region.
Labor	Probenbestätigung	KIS, LIS	4	Kreuzblut und Notfalllabor sind auch ohne IT-Unterstützung möglich.

Kritikalität dokumentieren.

Organisations-einheit	Prozess	IT-Unterstützung	MTA in Std	Kritikalität
Intensivstation	Aufnahme	KIS, PDMS	2	Sehr hoch
	Behandlung	PDMS	2	Sehr hoch
Radiologie	Radiologische Diagnostik	KIS, RIS, PDMS	6	Hoch
Labor	Probenbestäti-gung	KIS, LIS	4	Hoch
	Probenverteilung	LIS	4	Hoch
	Befundrück-meldung	LIS	4	Hoch
	Blutkonserven-bereitstellung	LIS	0,5	Sehr hoch

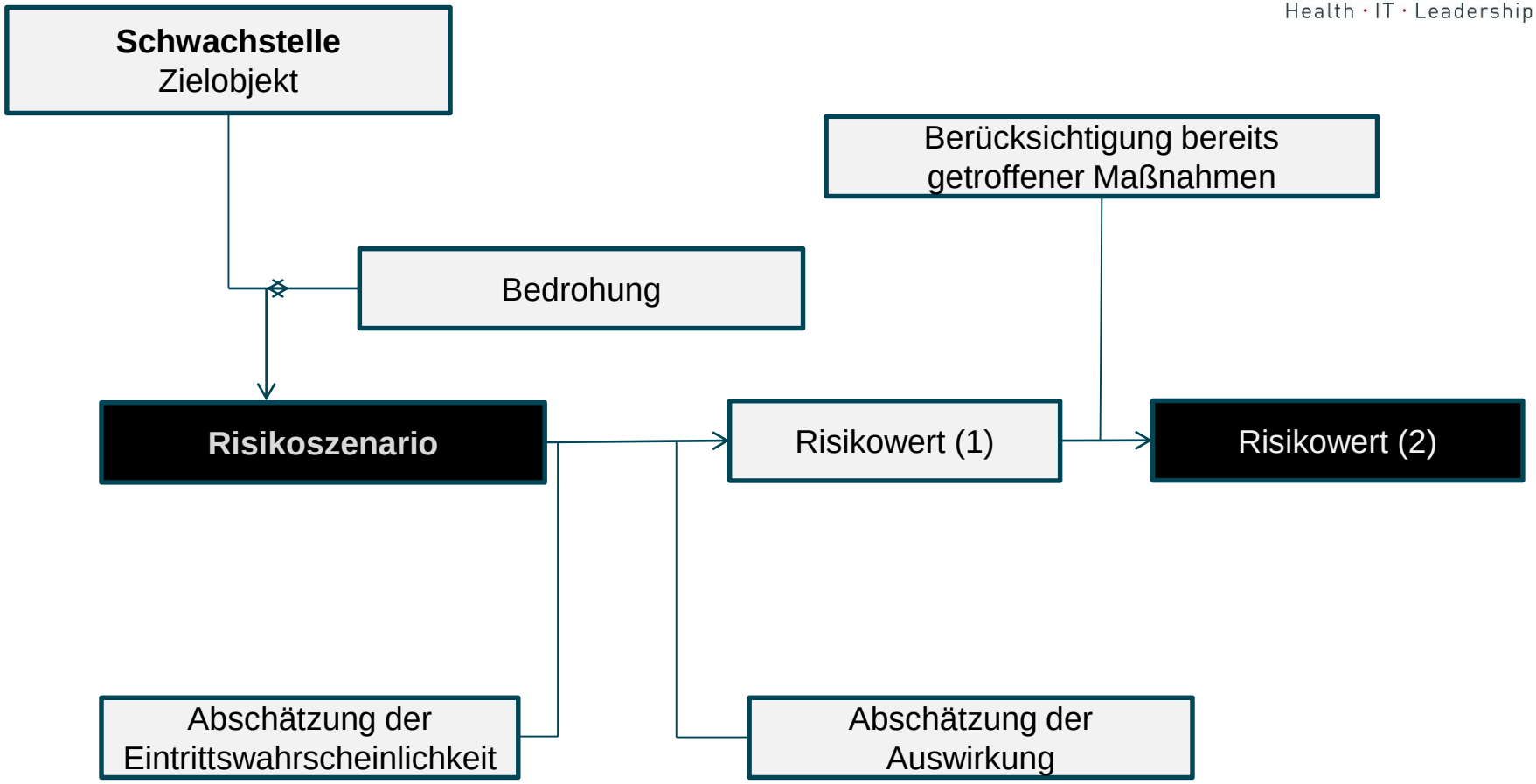
Kritikalität dokumentieren.

Organisations-einheit	Prozess	IT-Unterstützung	Kritische Komponenten
Intensivstation	Aufnahme	KIS, PDMS	DB-Server, KIS-Applikationsserver, SAN, Clientsysteme, PDMS-Applikationsserver, Netzwerk
	Behandlung	PDMS	
Radiologie	Radiologische Diagnostik	KIS, RIS, PDMS	DB-Server RIS, DICOM Middleware, Radiologische Medizintechnik, KIS-Komponenten, PDMS-Komponenten, SAN, Netzwerk
Labor	Probenbestätigung	KIS, LIS	Schnittstellenserver (z.B. MIRTH), LIS-Applikation, Laborclients, KIS-Applikation, KIS-Clients, etc.
	Probenverteilung	LIS	LIS-Applikation, Laborsysteme, DB-Server, SAN, Schnittstellenserver, Laborstraße, Patientenstammdaten, etc.
	Befundrück-meldung	LIS	

Zwischenstand – was ist erledigt?

Phase	Aktivitäten
Vorbereitende Aktivitäten	1. IT-Risikoanalyse als Projekt initialisieren 2. Schutzziele festlegen (Schutz der Patienten & der Einrichtung) 3. Untersuchungsbereich abgrenzen 4. Prozesse (Kern- und Unterstützungsprozesse) erheben
Kritikalität analysieren	5. Kritische Prozesse ermitteln 6. IT-Unterstützung ermitteln (Anwendersicht & IT-Sicht) 7. Kritikalität der IT-Unterstützung bestimmen 8. Kritische IT-Komponenten ermitteln
Risiken identifizieren & bewerten	9. Risikoszenarien ermitteln 10. Eintrittswahrscheinlichkeiten abschätzen 11. Auswirkungen bewerten 12. Risikowert ermitteln 13. Bestehende Maßnahmen berücksichtigen
Risiken behandeln	14. Behandlung der Risiken entscheiden 15. Präventive Maßnahmen bestimmen & Ersatzverfahren vorsehen

Risiken identifizieren und bewerten



Risikoszenarien ermitteln

- ✓ Zur Identifikation der Risikoszenarien sind erst die Bedrohungen zu bestimmen, denen ein Zielobjekt ausgesetzt ist und anschließend zu prüfen, welche Schwachstellen es gegen diese Bedrohungen verwundbar machen.
- ✓ Bei der Identifikation von Bedrohung und Schwachstelle ist es sinnvoll, vom Allgemeinen zum Besonderen vorzugehen.
- ✓ Ergänzend zu Schwachstellen kann es sinnvoll sein, auch noch die klinischen Situationen eines Ausfall mit einzubeziehen.
- ✓ RiKrIT basiert auf den Gefährdungsszenarien des IT-Grundschutz – denken in Situationen geht weiter und berücksichtigt klinische Besonderheiten.

Unterschiedliche Schwachstellenarten

- ✓ Hardware (Server, Medizingeräte)
- ✓ Software (Betriebssysteme, Applikationen, Datenbanken, etc.)
- ✓ Netz (Netzkomponenten, QoS, DoS, etc.)
- ✓ Personal
- ✓ Infrastruktur
- ✓ Organisation (Personalschlüssel, etc.)

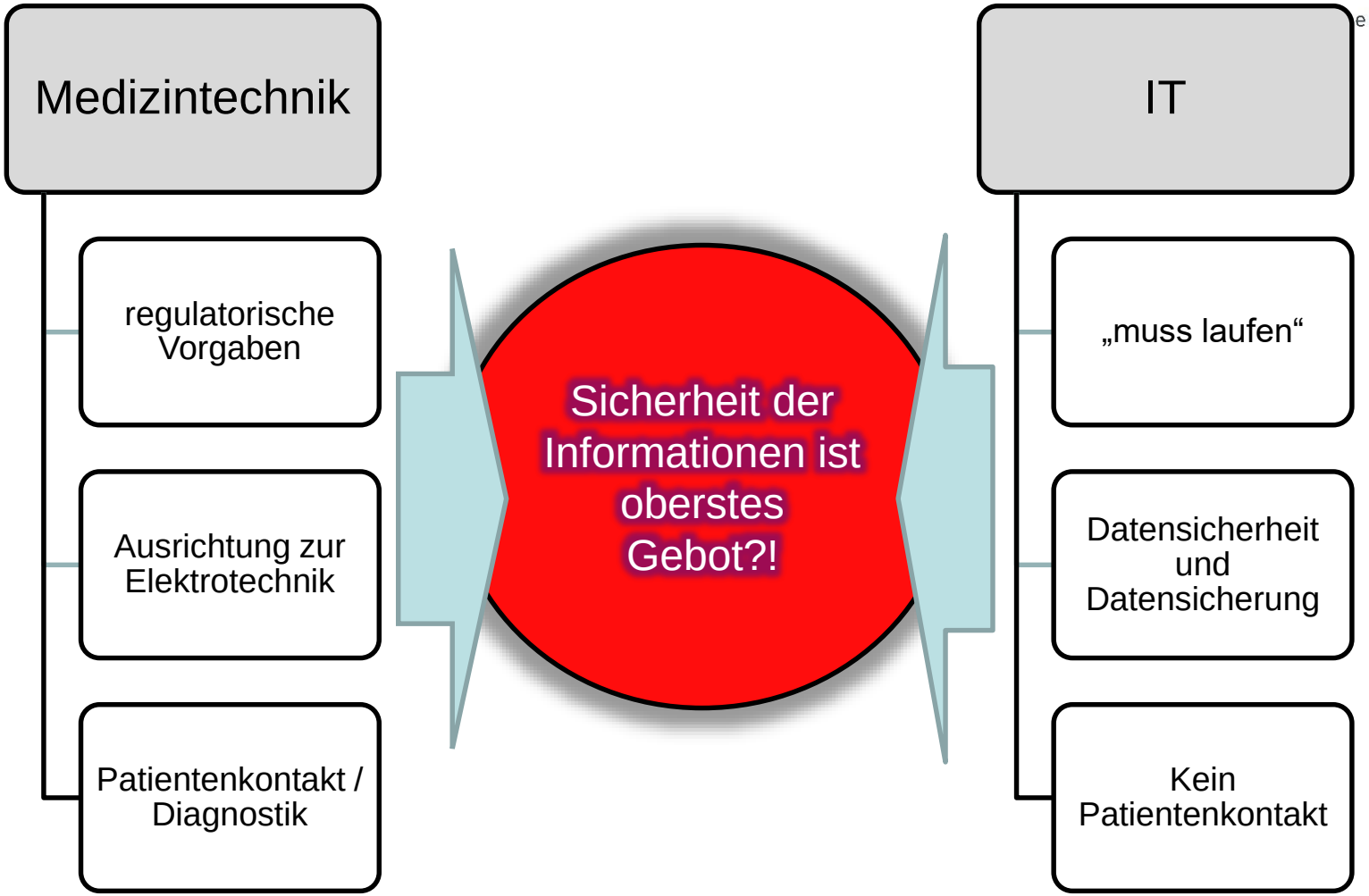
- Eine Auswirkung ist primär, wenn sich eine Bedrohung **unmittelbar** auf das betrachtete Objekt auswirken kann
- Eine sekundäre Auswirkung besteht, wenn eine Bedrohung sich **indirekt** auf das betrachtete Zielobjekt auswirken kann.

Wahrscheinlichkeiten abschätzen

- ✓ Mit welcher Wahrscheinlichkeit treten die identifizierten Risikoszenarien ein und verletzten tatsächlich die betrachteten IT-Komponenten?
- ✓ Je nach Bedrohungskategorie gibt es unterschiedliche Faktoren für die Eintrittswahrscheinlichkeit:
  - Vorsätzliche Angriffe
  - Menschliche Fehlhandlungen
  - Technisches Versagen
  - Natürliche Ereignisse
  - Organisatorische Mängel
- ✓ Hilfreiche Hinweise dazu finden sich in den einschlägigen Normen, wie zum Beispiel ISO 14971 oder ISO 27005

UMGANG MIT MEDIZINGERÄTEN

Zwei Inseln nebeneinander

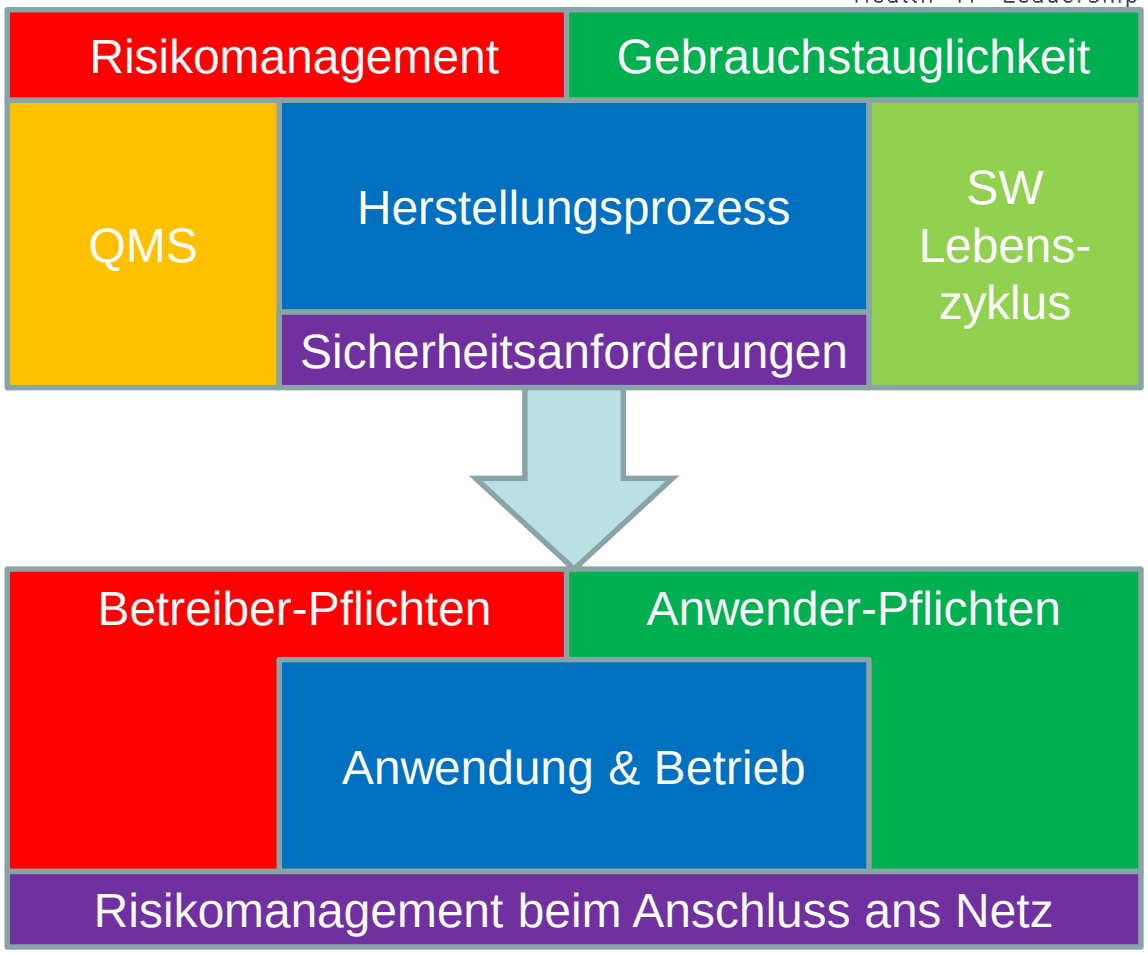


Schutzziele der IEC 80001-1

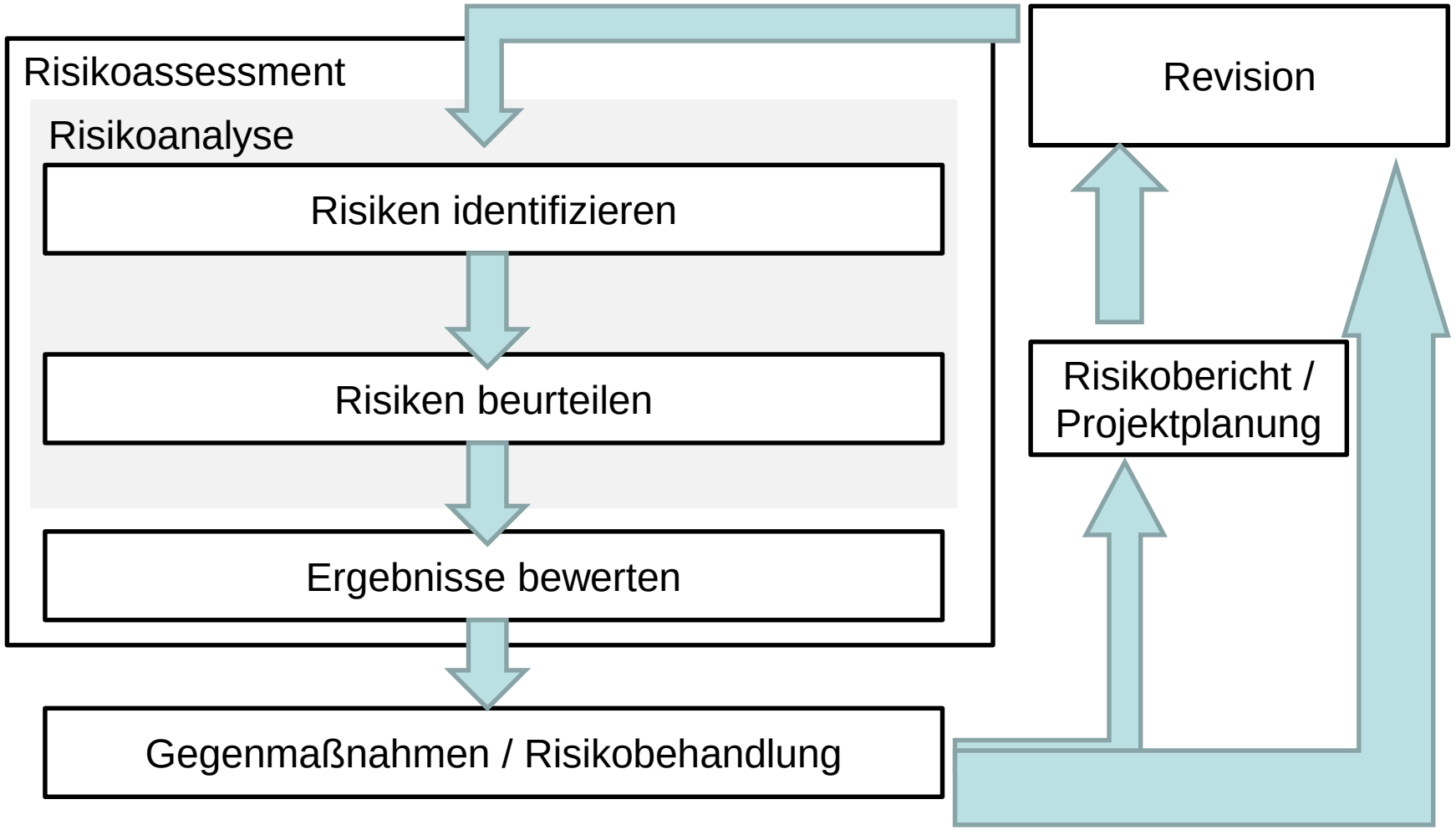
Effectiveness Wirksamkeit	• Informationen zu richtigen Zeit am richtigen Ort unter Laborbedingungen.
Safety Patientenschutz	• Schutz vor Gefahren für Leib und Leben.
Security Sicherheit	• Summe von Verfügbarkeit, Vertraulichkeit und Integrität

Hersteller vs. Anwender

- ✓ Herstellerrisiken sind andere, als Betreiberrisiken
- ✓ Betreiber-Pflichten sind andere, als Herstellerpflichten
- ✓ Hersteller definiert anhand seines „Bauplans“
- ✓ Betreiber muss Produkt unverändert betreiben

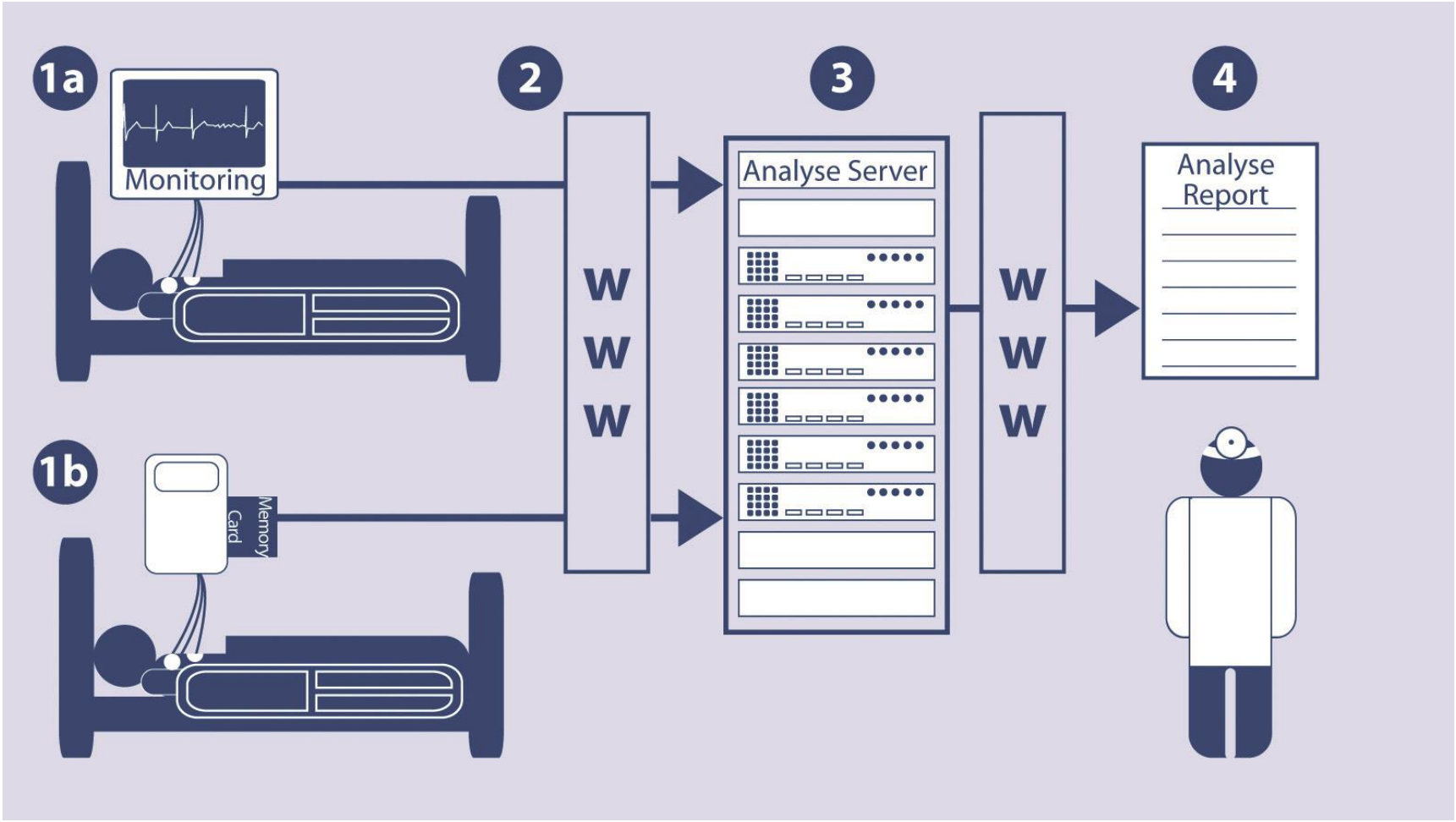


Prozess des Risikomanagements



RIKRIT AM BEISPIEL EINER NOTAUFNAHME

Schematische Darstellung



Potenzielle Schwachstellen

- ✓ Netzwerkverbindung zum Schwesterplatz
- ✓ Ggf. mobile Alarmierung via App / Hausruf
- ✓ http-Anbindung zur Administration via Browser
- ✓ Fehlende Regelungen welcher Alarm führt
- ✓ Offenes Netzwerk, Zeitverzögerungen

Methoden zur Risikoermittlung

Szenariotechnik

Beantwortung von „Was-wäre-wenn-Fragen“ und Abbildung verschiedener Wege und Ergebnisse mit Abschätzung der Auswirkungen

Workshops / Anwenderinterviews

Abfrage der bereits eingetretenen Risiken bei Anwendern in Workshops, Frage nach möglichen Konsequenzen und bekannten Fehlern

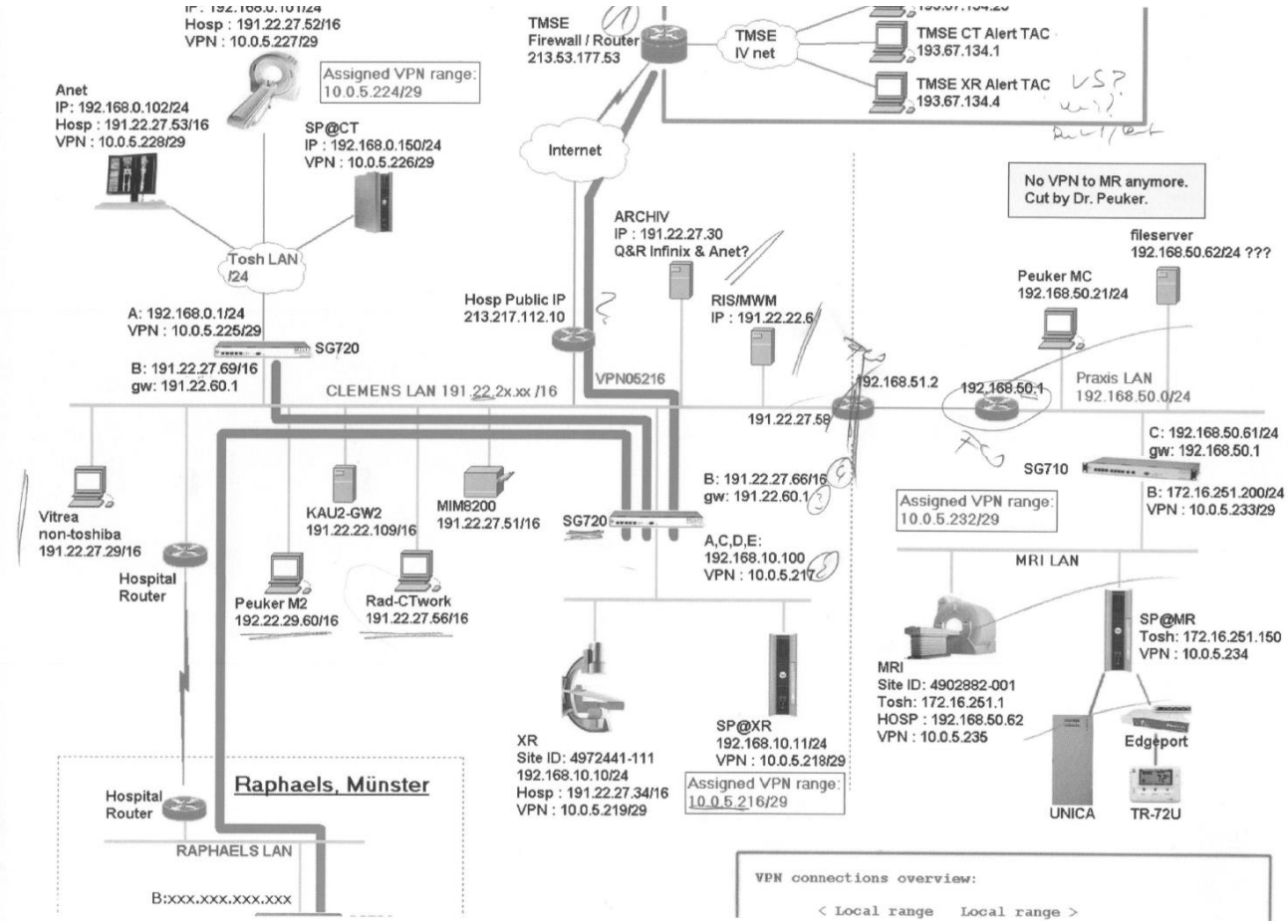
FMEA

Fehlermöglichkeiten und Einflussanalyse (Qualitätsmanager könnten das kennen)

technische Schwachstellenanalyse

IT-technische Analyse auf verschiedene mögliche Schwachstellen anhand der technischen Implementierung

Arbeitsbeispiel



Ersteller / Ansprechpartner

CETUS Health IT Leadership
Frederik Humpert-Vrielink

Weidkamp 180
45356 Essen

Mobil 0176-826 280 16

frederik.humpert-vrielink@cetus-consulting.de

Danke für Ihre Aufmerksamkeit.