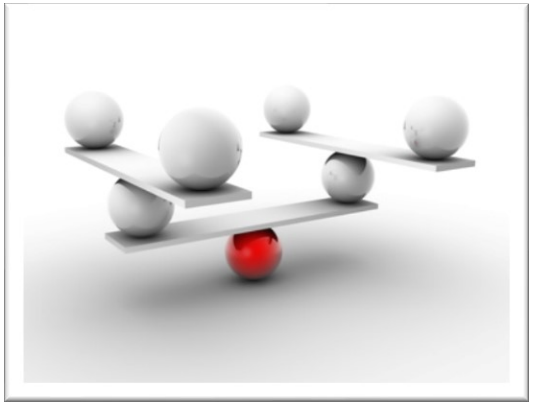
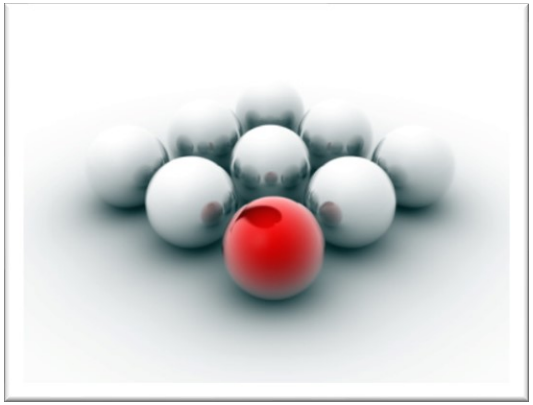
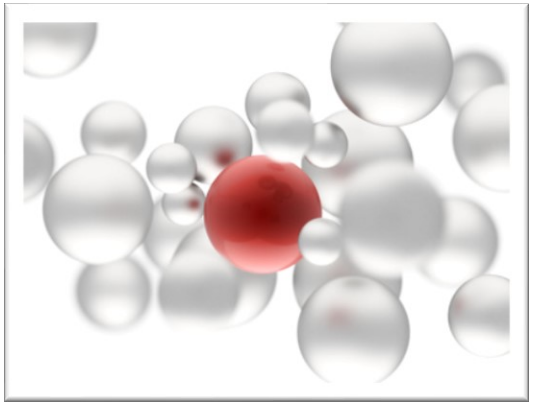
CETUS
Health · IT · Leadership







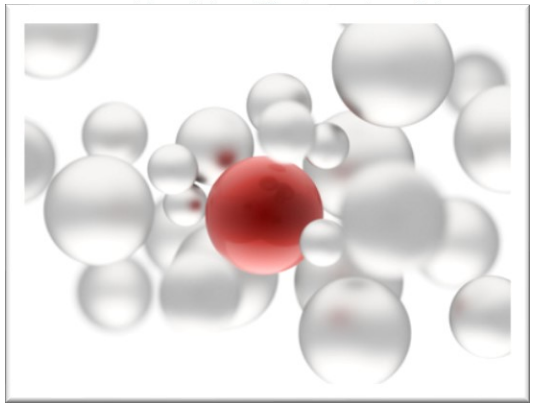
Risikomanagement im medizinischen IT-Netz im Licht der EU-DSGVO

Risiken ohne Nebenwirkungen.

Mission und Vision

Die CETUS Consulting GmbH ist ein Premium-Anbieter spezialisierter Beratungsleistungen im Umfeld der Informationssicherheit.

Wir verstehen uns als Partner der Kunden und erarbeiten gemeinschaftlich Lösungen



Unsere Qualität

- Wir erkennen Ihren Bedarf.
- Wir entwickeln gemeinsam Strategien und Lösungen.
- Wir sind Denker und Lenker.

Unsere Vision

- Wir sind Garant für Informationssicherheit im Krankenhaus
- Unser Arbeit liefert nachhaltige Erfolge

Unsere Kunden (Auszug)

CETUS

GDF SUEZ
BY PEOPLE FOR PEOPLE

universitäts klinikum bonn

ATEGRIS

St. Bonifatius Hospital

LÄPPLE
Systempartner der Automobilindustrie

valeo-KLINIKEN GmbH
Evangelische Krankenhäuser

ST. ELISABETH GRUPPE
KATHOLISCHE KLINIKEN RHEIN-RUHR

FUJITSU

Katholisches Klinikum Bochum

DIE JOHANNITER
Aus Liebe zum Leben

pius Hospital Oldenburg
Medizinischer Campus Universität Oldenburg

UK RUB UNIVERSITÄTSKLINIKUM DER RUHR-UNIVERSITÄT BOCHUM

KKeL
Katholische Kliniken Emscher-Lippe GmbH

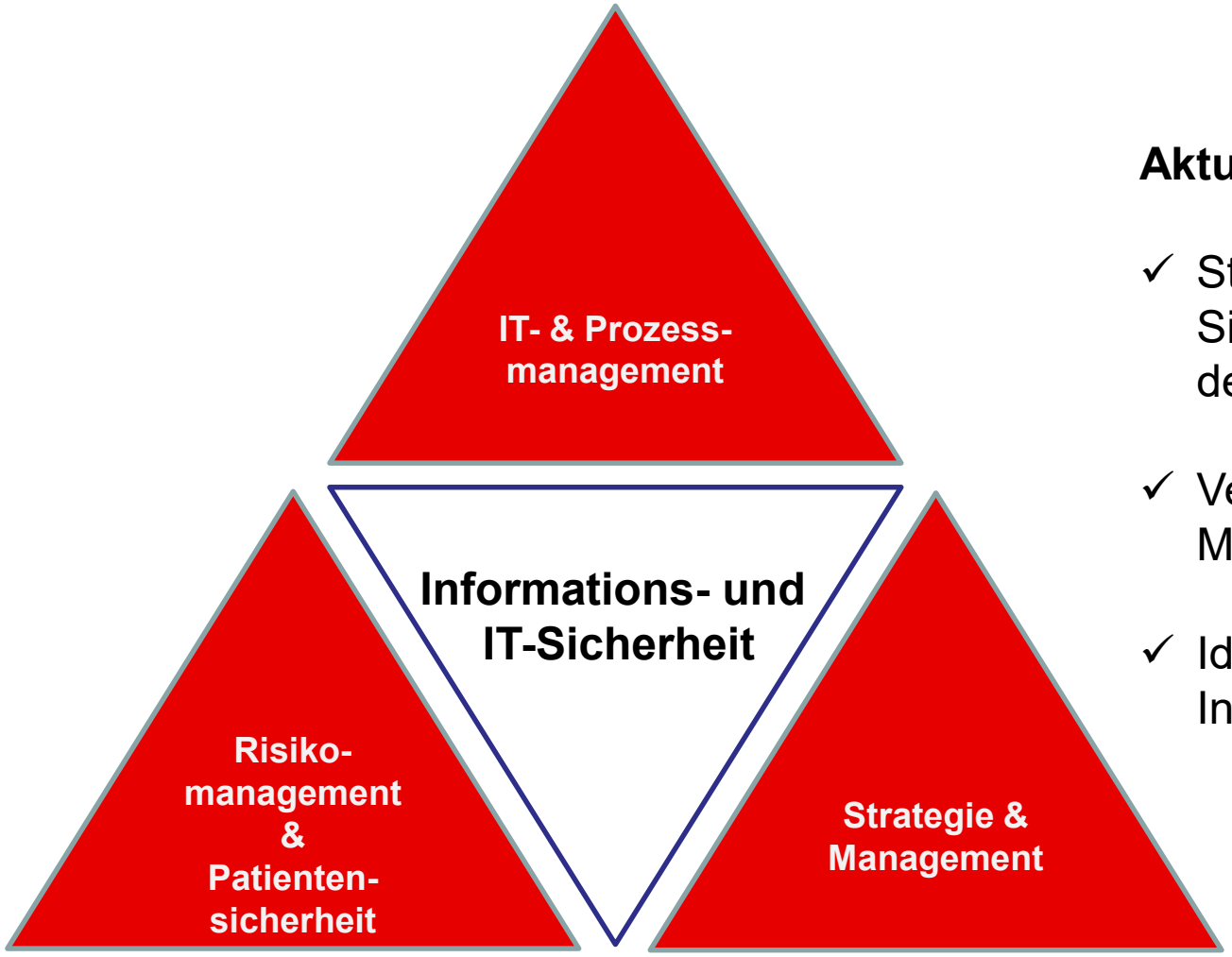
T

POLIZEI
BADEN-WÜRTTEMBERG

ST. JOSEPH-STIFT
DRESDEN

MISERICORDIA
TRÄGERGESELLSCHAFT

Was wir beraten

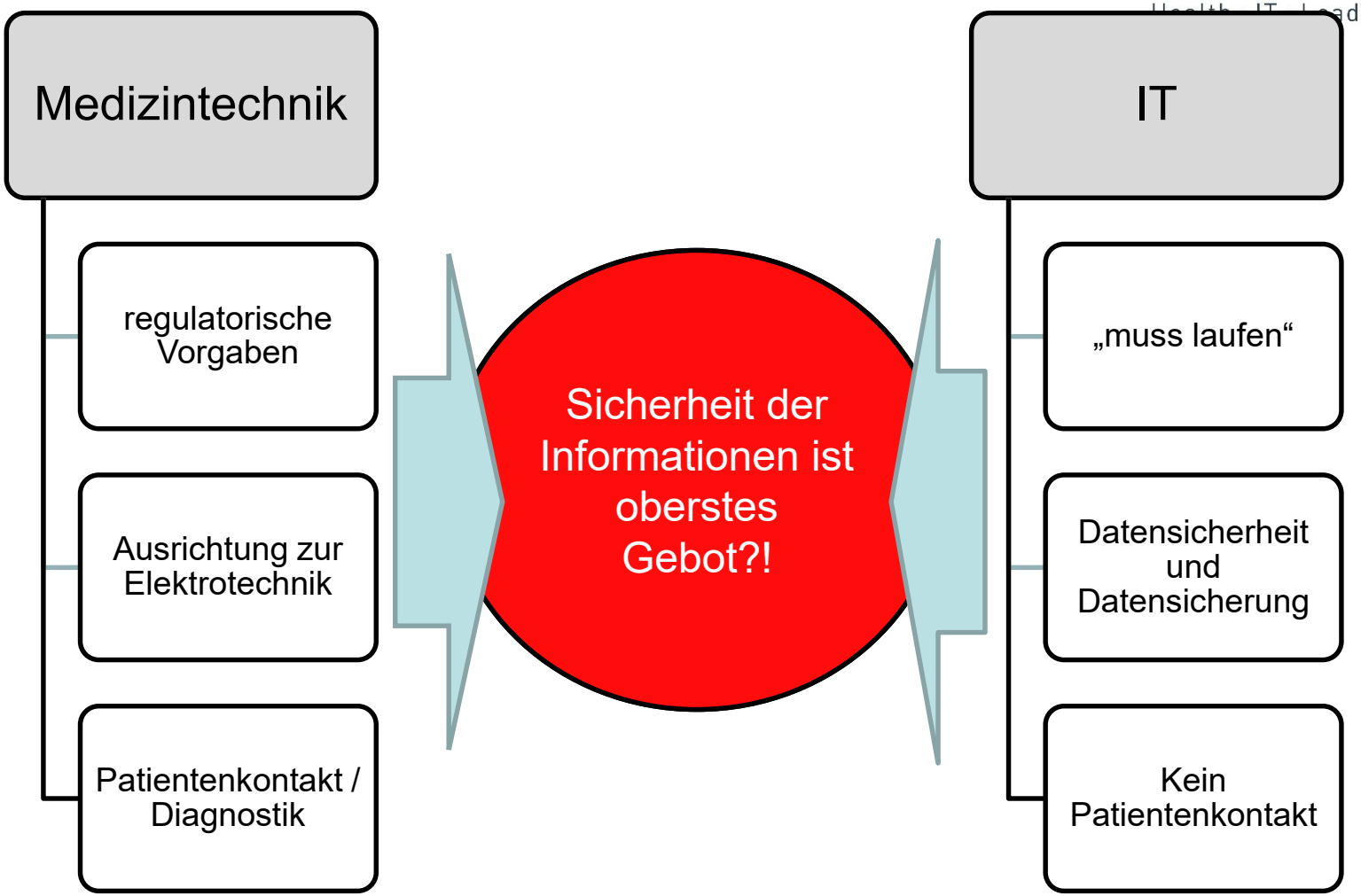


Aktuelle Initiativen

- ✓ Standardisierung von IT-Sicherheitsstandards nach dem IT-SiG
- ✓ Verbindung von Medizintechnik & IT
- ✓ Identifikation kritischer Infrastrukturen

DIE HERAUSFORDERUNG

Zwei Inseln nebeneinander



Unterschiedliche Schutzziele

CETUS
Health · IT · Leadership

Medizintechnik

- **Safety** = Patientensicherheit
- **Effectiveness** = zur rechten Zeit in rechter Qualität am rechten Ort
- **Security** = Datenschutz & Datensicherheit

Der Patient steht im Mittelpunkt!

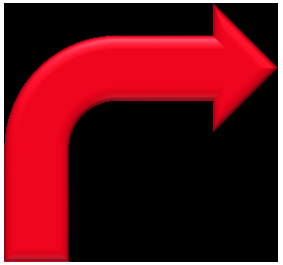
IT / Informationssicherheit

- **Integrität** = unverfälschte und korrekte Informationen
- **Verfügbarkeit** = zur Rechten Zeit am Rechten Ort
- **Vertraulich** = Zugang nur für Berechtigte

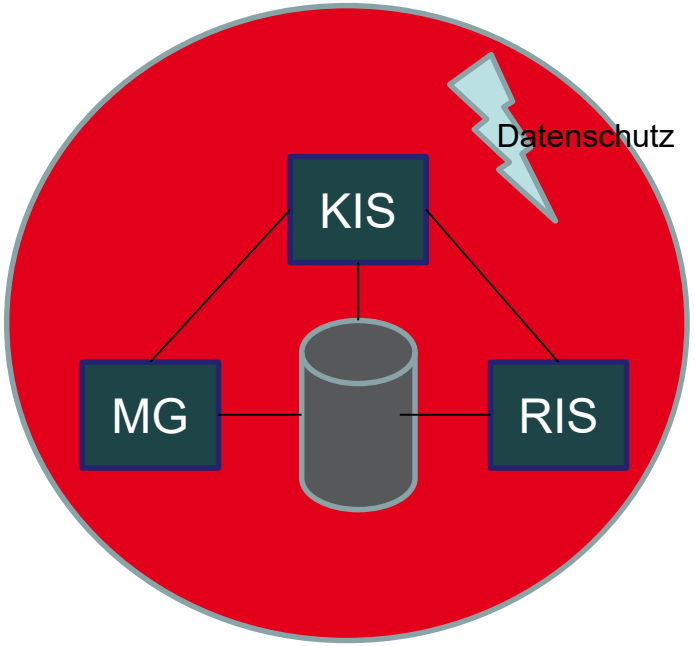
Die Information / der Prozess steht im Mlttelpunkt

Von Inseln zu Konvergenz

Von „getrennten“ Plattformen…
- Analoge Medizingeräte
- Medienbrüche
- Unterschiedliche Systeme
- Getrennte Verantwortung



… zu konvergenten Netzen
- Ein medizinisches IT-Netzwerk
- Zentrale Datenverarbeitung
- Zusammenwachsen von MT & IT
- Gemeinsame Verantwortung



Klinischer IT-Betrieb im Spannungsfeld

CETUS
Health · IT · Leadership

Drittanforderungen

- Nationales / EU-Recht (MPBEtreibV, etc.)
- Herstellervorgaben (Konfigurationen, CE-Konformität, etc.)
- KRITIS
- EU-DSGVO
- …

Normen

- ISO 9001, KTQ, EFQM
- Spezielle Zertifizierungen
- ISO 27001/2, ISO 20000, DIN EN 80001-1
- Sonstige Regelwerke

Klinischer IT-Betrieb

Dienste
KIS, RIS,
LIS, PACS,
Archiv, Datenaustausch,
Abrechnung, Klinischer
Arbeitsplatz, Medizingeräte, …

Anforderungen
Patientendatenschutz
Verfügbarkeit
24/7 Betrieb
Zugriffsschutz
Help-Desk, …

CETUS
Health · IT · Leadership

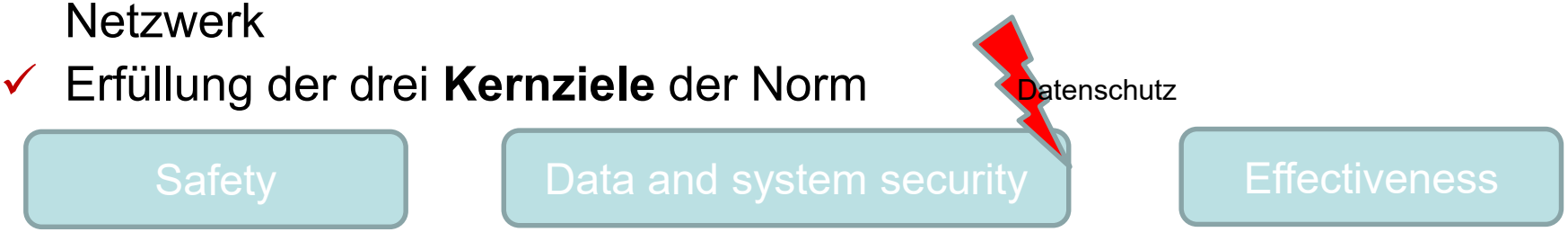
FAKTEN ZUR DIN 80001

Zielsetzung der DIN EN 80001-1:2011

- ✓ Die Norm fordert vom Betreiber systematische Prozesse bei der Netzwerk-Erstellung und – Betrieb
- ✓ Sie definiert Zuständigkeiten und Verantwortlichkeiten bei Betreibern, Modalitäten Herstellern und IT-Herstellern
- ✓ Sie beleuchtet Risiken und Management-Aktivitäten bei der IT-Vernetzung von Medizinprodukten

Warum die IEC 80001-1:2011?

- ✓ Beschreibt den Stand der Technik mit Bezug zum Risikomanagement von IT-Netzwerken
- ✓ Für Hersteller von Medizinprodukten gibt es Standards, Normen und Zulassungsbestimmung an diese gebunden sind
- ✓ Es gibt keine spezielle Zertifizierung für Klinik IT-Netzwerke und keine Normen oder Standards für das Einbinden von Medizinprodukten ins Netzwerk
- ✓ Erfüllung der drei **Kernziele** der Norm



ist bisher häufig dem Prinzip „Zufall“ überlassen

- ✓ Durchgeführte Risikomanagements erfolgen meist nicht Strukturiert

Schutzziele der DIN EN 80001-1:2011

Durch die Einführung des Risikomanagements sollen die drei Kernziele der Norm erfüllt werden

Safety

keine unvertretbaren Risiken hinsichtlich:

- physischer Verletzung oder Schädigung der Gesundheit von Menschen

- Schädigung von Eigentum oder Umwelt

Data and system security

Medizinisches IT-Netzwerk befindet sich in einem Zustand, in dem die Daten und Systeme vor Beeinträchtigung der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Datenschutz

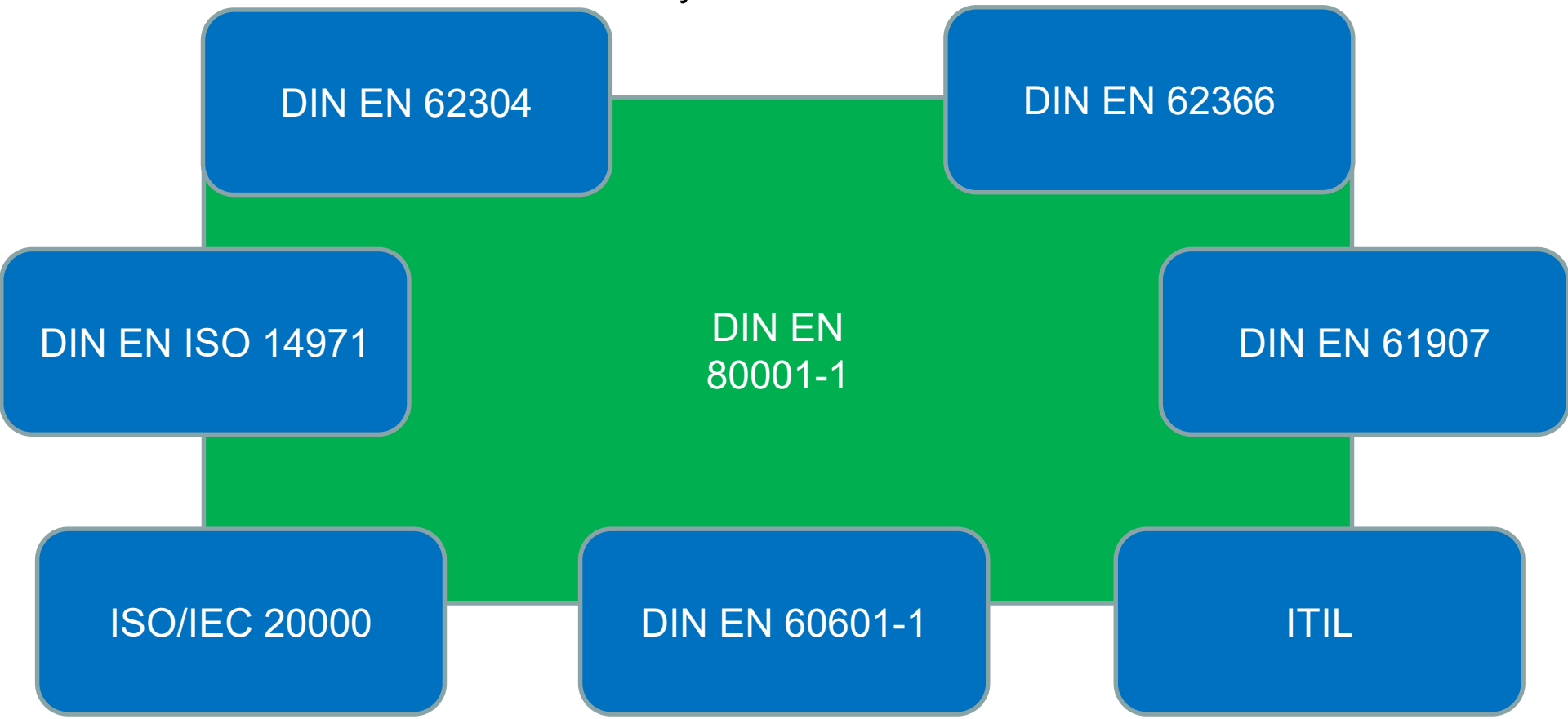
Ausreichend geschützt sind

Effectiveness

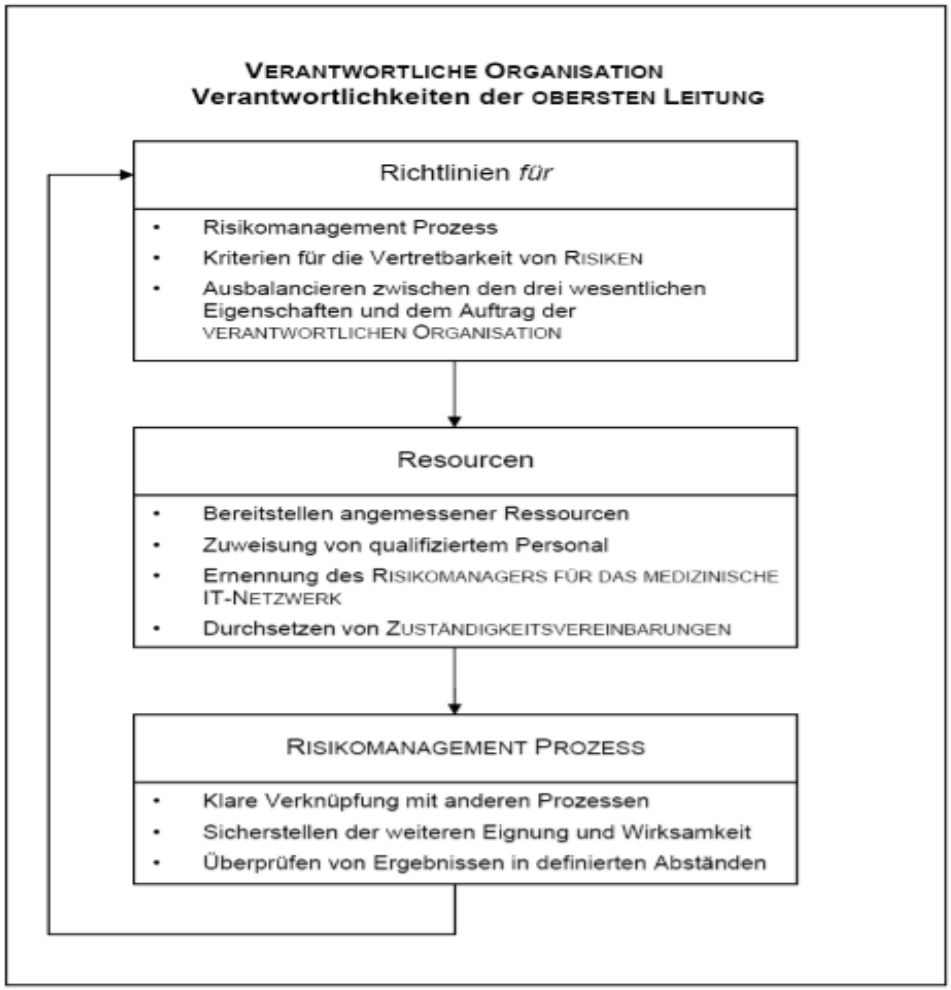
Fähigkeit, das beabsichtigte Ergebnis für den Patienten und die verantwortliche Organisation zu erzeugen

Begleitnormen zur DIN EN 80001-1:2011

Für das Inverkehrbringen von Medizinprodukten gelten Normen und Gesetze, die Hersteller während des Produktlebenszyklus beachten müssen



Verantwortung der Geschäftsleitung



Risikomanager

Der Risikomanager

- Qualifikation
- Kompetenz
- Kenntnisse

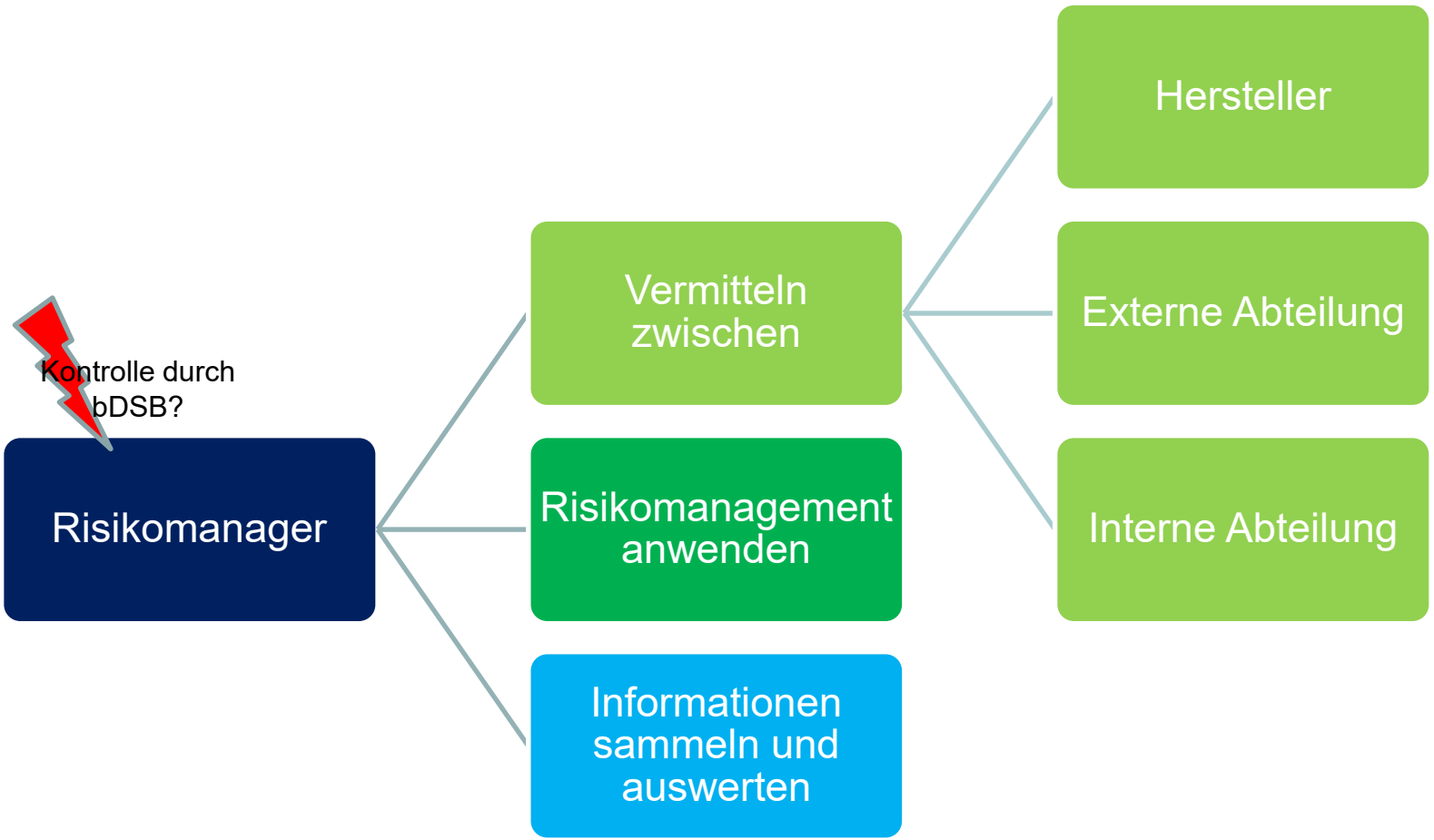
Interne Lösung

- **Zentral / dezentral**
- **Stabsstelle**
  Geschäftsführung / Bereich IT
- **Informationstechnologie (IT)**
- **Medizintechnik (MT)**
- **(MIT)**
  (gemeinsamer Bereich IT+MT)
- **Qualitätsmanagement**

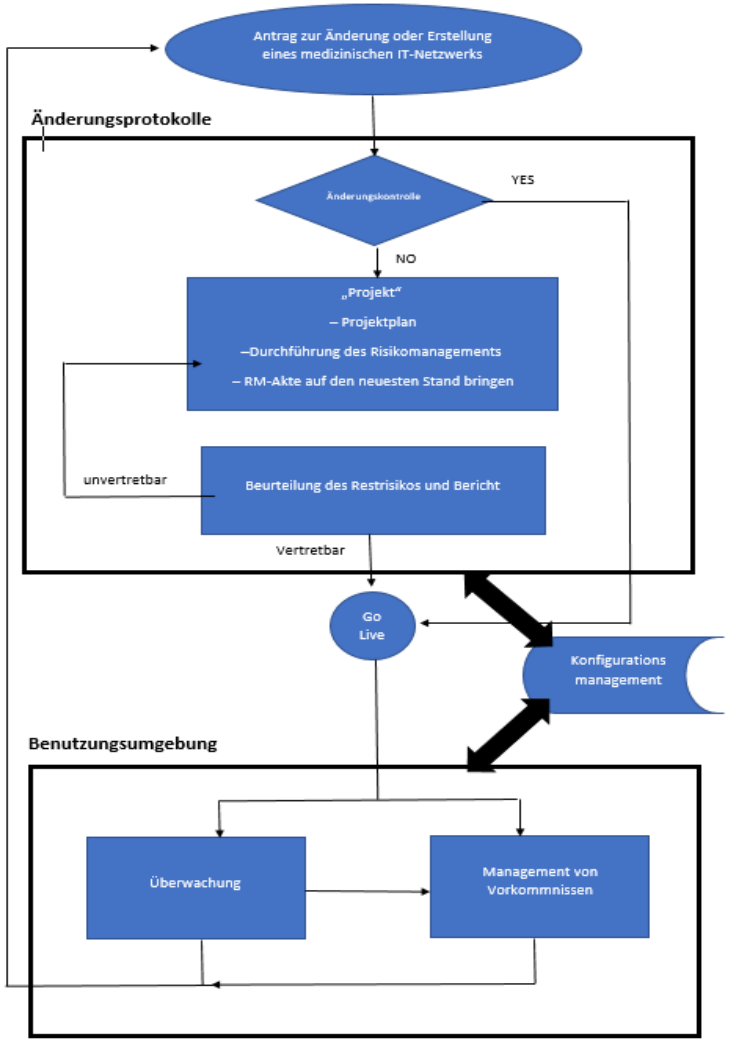
Interne Lösung

- **Externer Partner**
- **Gerätehersteller**
- **Sonstiger Dienstleister**

Risikomanager – Funktion

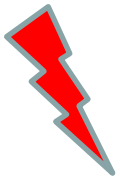


Lebenszyklus-Risikomanagement für Medizinische IT-Netzwerke



Verantwortung der Hersteller

- ✓ Begleitpapiere müssen bei jedem Medizinprodukt vorhanden sein:
  - ➢ Angaben zur Zweckbestimmung
  - ➢ Anweisung für den sicheren und effektiven Gebrauch
  - ➢ Anweisung für die Einbindung in ein IT-Netzwerk
    - Den Zweck der Einbindung
    - Geforderte Eigenschaften
    - Liste möglicher Gefährdungssituationen

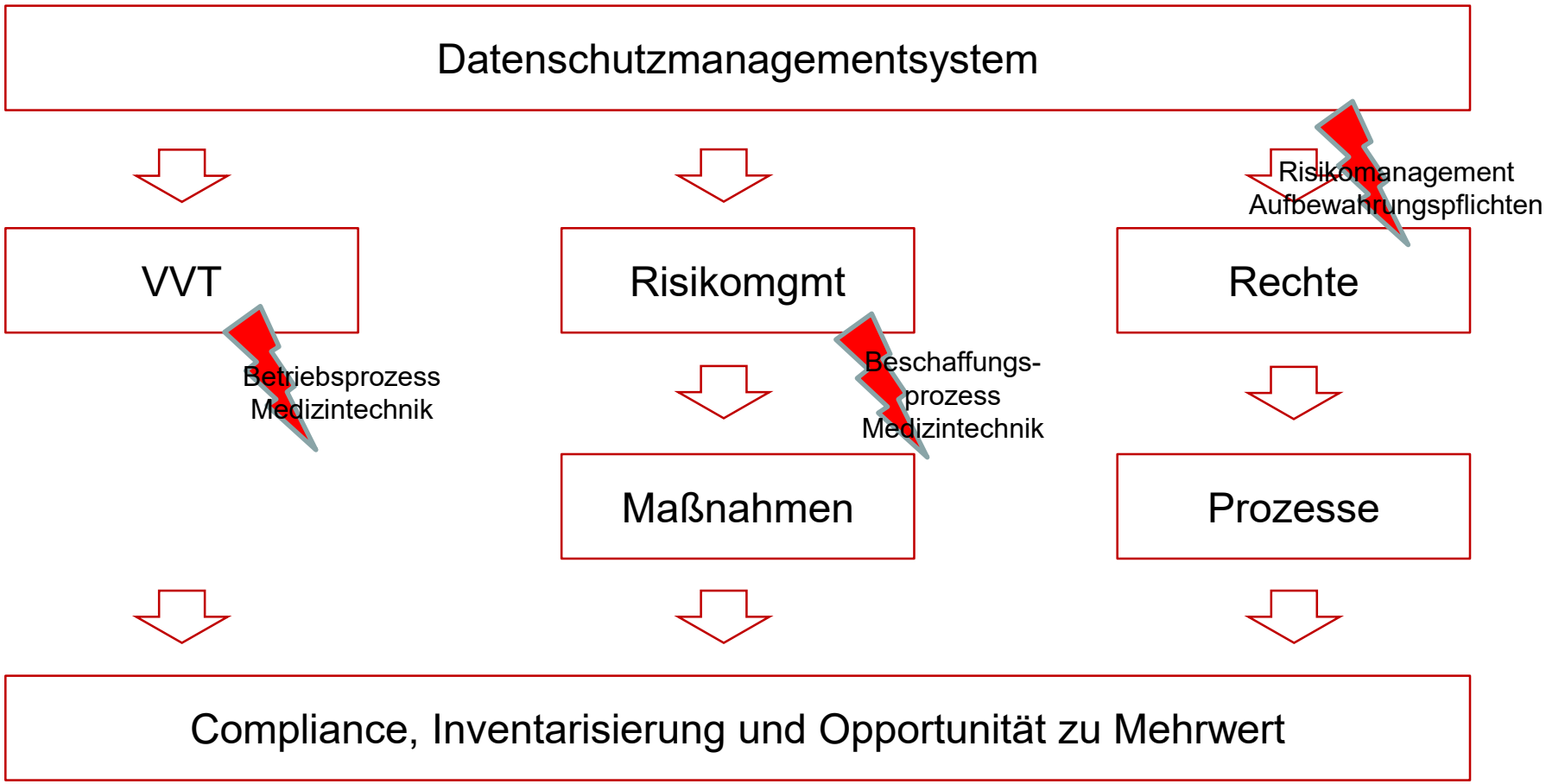


Einbeziehung des bDSB

CETUS
Health · IT · Leadership

EU-DSGVO

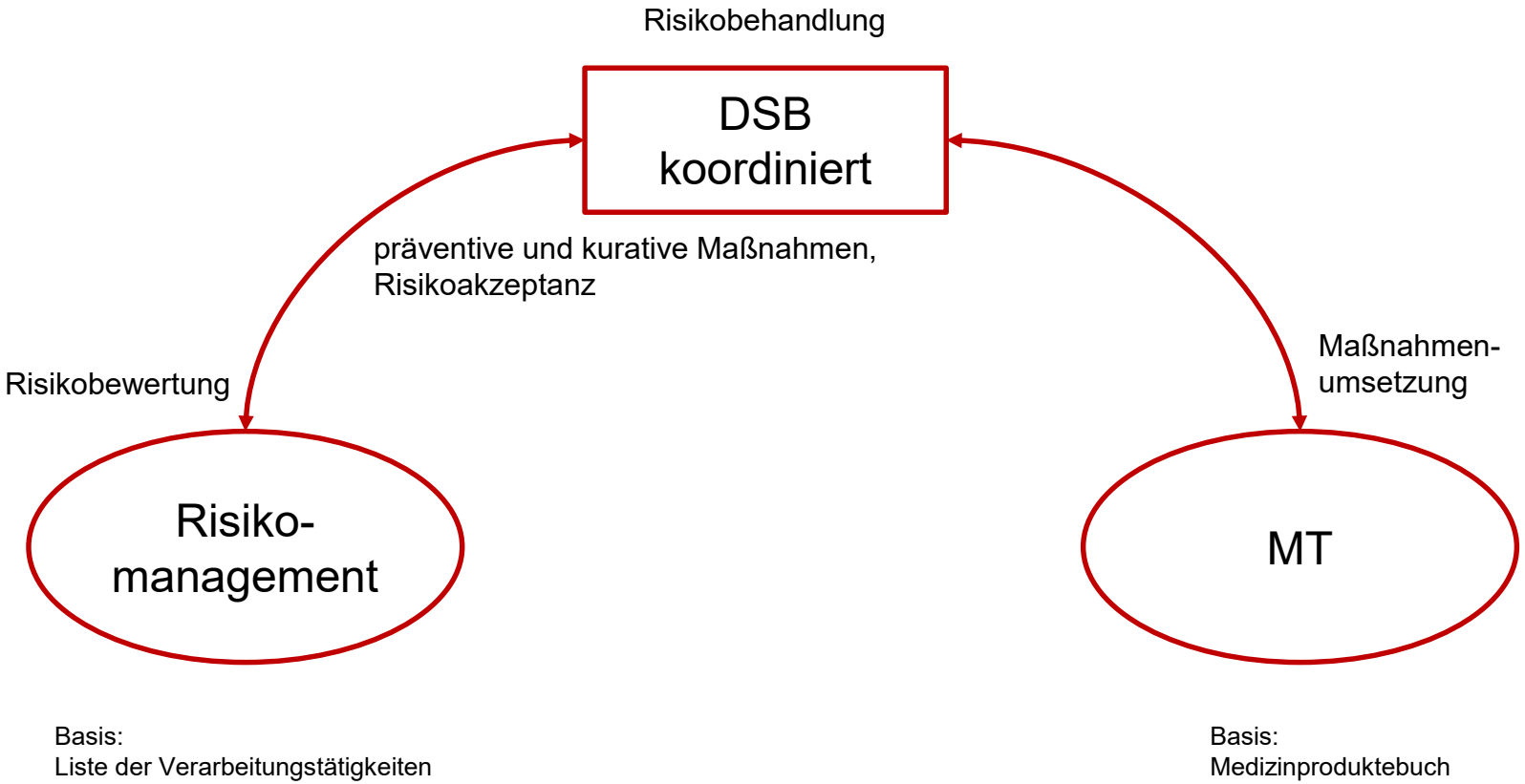
Summary


Datenschutzmanagementsystem
VVT
Risikomgmt
Rechte
Risikomanagement
Aufbewahrungspflichten
Betriebsprozess
Medizintechnik
Beschaffungs-
prozess
Medizintechnik
Maßnahmen
Prozesse
Compliance, Inventarisierung und Opportunität zu Mehrwert

6 Grundsätze der EU-DSGVO

- ✓ Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- ✓ Zweckbindung
  - ➢ Verarbeitung nur für festgelegte, eindeutige und legitime Zwecke
- ✓ Datenminimierung
  - ➢ „dem Zweck angemessen und auf das notwendige Maß beschränkt“
- ✓ Richtigkeit
  - ➢ „angemessene Maßnahmen sind zu treffen um unrichtige personenbezogene Daten unverzüglich zu löschen oder zu berichtigen“
- ✓ Speicherbegrenzung
  - ➢ Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht wie es erforderlich ist“
- ✓ Integrität und Vertraulichkeit
  - ➢ Angemessene Sicherheit und Schutz vor unbefugter Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung und unbeabsichtigter Schädigung

Datenschutzfolgenabschätzung



FAZIT

Zusammenfassung (1)

- ✓ Mit der EU-DSGVO wird die Einhaltung von Vorgaben im Risikomanagement auch für Medizintechnik verbindlich.
- ✓ Jedes Medizingerät oder der von ihm betroffene Behandlungsprozess sollte in der Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden.
- ✓ Bei der Beschaffung von vernetzten und nicht vernetzten Medizingeräten sollte eine Datenschutzfolgenabschätzung erfolgen.
- ✓ Patienten sollten auch bei der Behandlung mit diagnostischen Verfahren über den Umfang der gesammelten Daten aufgeklärt werden.

Zusammenfassung (2)

- ✓ Der Beschaffungsprozess sollte die Datenschutzfolgen und die Datenschutzcompliance bei den Geräten kontrollieren.
- ✓ Die Umsetzung der DIN 80001 hilft, angemessene technische und organisatorische Maßnahmen zu ergreifen, folglich die EU-DSGVO einzuhalten.
- ✓ Mit der Integration eines DSMS mit einem Risikomanagement für medizinische IT-Netze nimmt die Geschäftsführung ihre Verantwortung vollumfänglich wahr.
- ✓ Bei der Überwachung der Benutzerumgebung eines Medizingerätes sind die Grundsätze der Datensparsamkeit zu beachten.

Ansprechpartner

CETUS Consulting GmbH
Frederik Humpert-Vrielink
Mendelstraße 11
48149 Münster

Telefon 0251-980 1620
Telefax 0251-980 1621

E-Mail: frederik.humpert-vrielink@cetus-consulting.de