CHARITÉ
UNIVERSITÄTSMEDIZIN BERLIN

Riechen Consulting GmbH

Modernisierter BSI-Grundschutz für kritische Infrastrukturen

verinice bei der Charité Universitätsmedizin Berlin

Vorstellung

Michael Römling
CISO / Informationssicherheitsbeauftragter
Leiter der Stabsstelle Informationssicherheit
Charité – Universitätsmedizin Berlin

Ulf Riechen
Riechen Consulting GmbH
verinice.PARTNER

IT-Sicherheit im KRITIS-Sektor Gesundheit

Stationäre medizinische Versorgung

- Budget vorgegeben durch Fallpauschalen
- Qualitätsmanagement vorhanden und zertifiziert
- Kaufmännisches und Medizinisches Risikomanagement vorhanden
- Datenschutz oft ohne Verbindung zu IT-Sicherheit
- Sicherheit wird durch IT-Abteilungen „gelebt“, Orientierung an Best Practices der Hersteller
- Oft flache Netze mit einer Mischung aus Medizintechnik, Versorgungstechnik, kaufmännischer IT sowie Forschung und Lehre

IT-Sicherheit in der Charité

Ausgangslage (2015)

- Hohe technische Sicherheitsstandards
- Datenschutz dokumentiert über Word- und Excel-Dateien
- Verinice.PRO vorhanden, ca. 50 Objekte eingepflegt
- Risikomanagement global, Bezug zu Systemen fehlt

„In Bezug auf die Sicherheit der Daten musste die Charité bekennen, dass sie für keines der betriebenen Verfahren über ein dem Stand der Technik entsprechendes Sicherheitskonzept verfügt. Mehrere Anläufe zu einer Erarbeitung auch mit externer Unterstützung waren in den vergangenen Jahren im Sande verlaufen.“

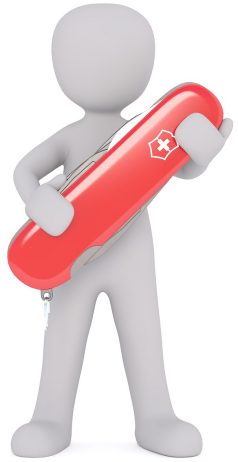
Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 2016

1. Schritt: Gruppierung

- Zentrale Infrastruktur:
  - Vertraulichkeit: hoch
  - Integrität: hoch
  - Verfügbarkeit: hoch
- Modellierung mit Grundschutz-Bausteinen (alt)
- Soll-Ist-Vergleich
  => insbesondere Dokumentationen fehlen!
- Umsetzung

2. Schritt: Dokumentations-Standard entwickeln

- Sicherheitsrichtlinie
  - Beschreibung der Sicherheitsstruktur
  - Vorgaben für sichere Installation, Konfiguration, Protokollierung, Backup, Überwachung
  - Sicherheitsregeln für Administratoren, Benutzer
- Betriebshandbuch
  - Beschreibt regelmäßige und anlassbezogene Tätigkeiten
- Wiederanlaufplan
  - Teil des übergreifenden Notfallhandbuchs
- Systemlog
  - Dokumentation durchgeführter Tätigkeiten
  - Möglichst automatisieren, bestehende Arbeitsweisen weiter nutzen



Dokumentations-Standard

- Sicherer IT-Betrieb
  - Alle Vorgaben sind in Sicherheitsrichtlinien beschrieben
  - Alle Tätigkeiten/Prozeduren sind in Betriebshandbüchern beschrieben
  - Alle durchgeführten Tätigkeiten werden im Systemlog dokumentiert
  - Notfallprozeduren werden anhand der Wiederanlaufpläne bei Übungen getestet und optimiert

- Ablage in Microsoft SharePoint:
  - Versionskontrolle
  - Zugriffsrechte
  - Workflows
  - Volltextsuche

Reifegradmodell

- Reifegrad 1
  - Hersteller/Lieferanten-Dokumentation
  - Tätigkeiten benannt
- Reifegrad 2
  - Sicherheitsrichtlinie erstellt
  - Tätigkeiten grob beschrieben
  - Wichtige Änderungen im Systemlog dokumentiert
- Reifegrad 3
  - Sicherheitsrichtlinie vollständig
  - Tätigkeiten so beschrieben, dass sie ein sachkundiger Dritter übernehmen kann
  - Systemlog und Änderungsmanagement vollständig
  - Wiederanlaufplan vollständig und getestet

Aktuelle Herausforderungen

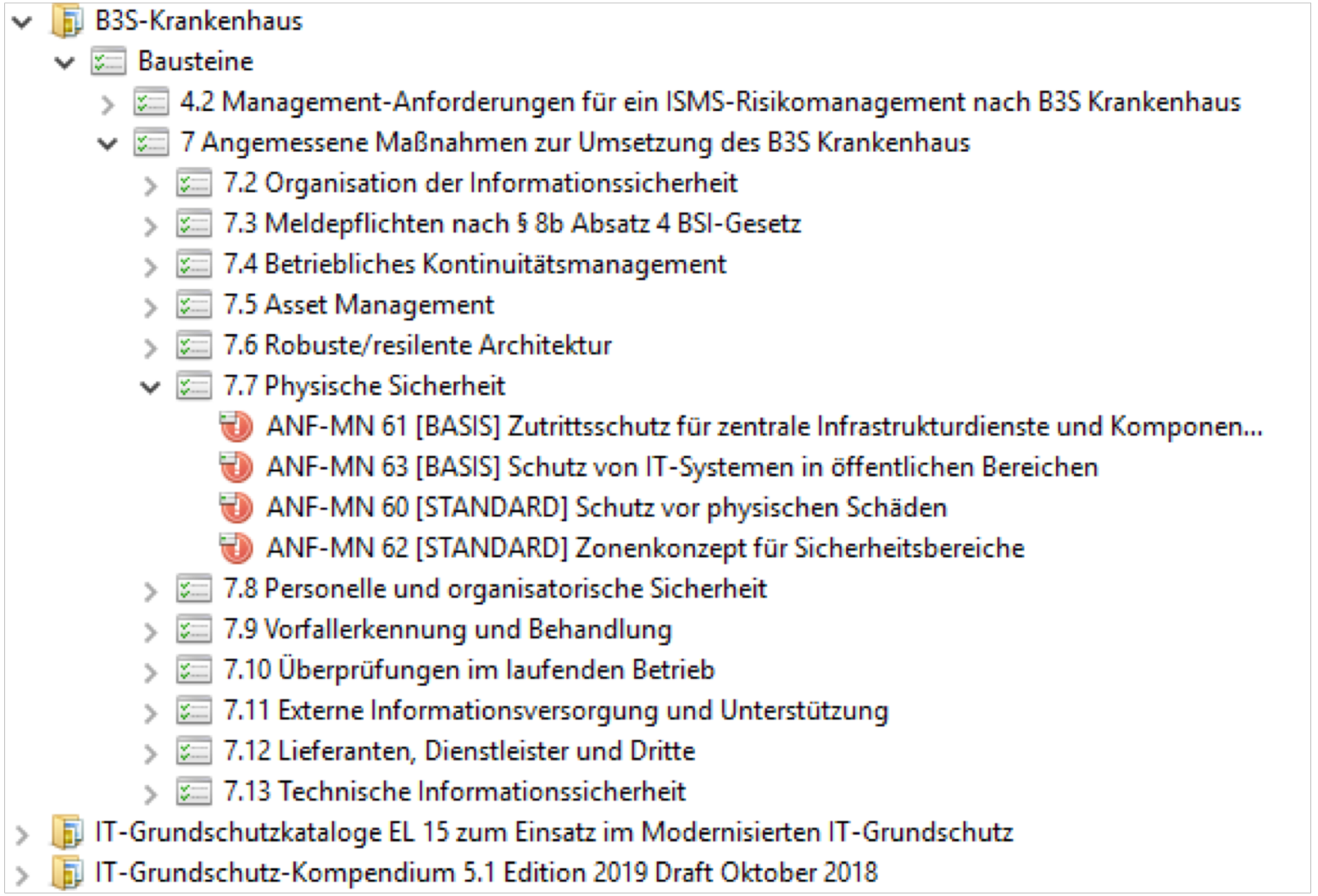
- Grundschutz-Modernisierung (ab 2017)
- DSGVO: Angemessene Sicherheitsmaßnahmen nach „Stand der Technik“, Risikomanagement (ab 2018)
- KRITIS: Prüfnachweis bis Juni 2019 für Krankenhäuser ab 30.000 vollstationäre Fälle / Jahr
- Branchenspezifischer Sicherheitsstandard B3S (Dezember 2018)

B3S in Verinice

B3S-Maßnahmen

=> Benutzerdefinierter Baustein

- MUSS => BASIS
- SOLL => STANDARD



Mapping Grundschutz-Gefährdungen

- Bedrohung aus B3S => Elementare Gefährdung Grundschutz
- Grundschutz-Baustein deckt Bedrohungen ab

Beispiel:

BED 1	Höhere Gewalt und Elementarschadensereignisse	G 0.1 Feuer G 0.3 Wasser G 0.5 Naturkatastrophen G 0.6 Katastrophen im Umfeld

3. Schritt: Dokumentation in Verinice

- Parallele Struktur im modernisierten Grundschutz
- Änderungen nur in der modernisierten Perspektive
- Manuelle Migration mit erneuter Grundschutz-Erhebung

4. Schritt: Charité-Strukturen abbilden

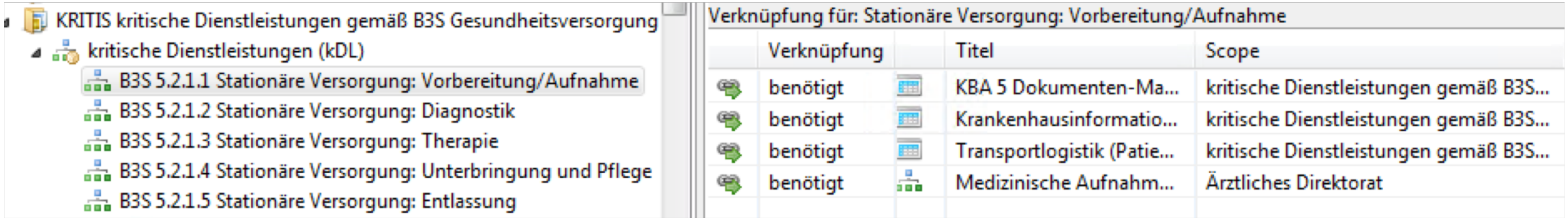
- Informationsverbünde anhand der Betriebsverantwortung
- Delegation der Pflege der Daten in verinice.PRO
- Verknüpfungen zwischen Objekten verschiedener Verbünde

Modernisierter IT-Grundschutz

- Ärztliches Direktorat
- Auftragsverarbeitung nach Extern
- Charité-Centren
- Fakultätsleitung (Dekanat)
- Fundraising und Alumni
- GB Corporate Governance
- GB Einkauf
- GB Finanzen
- GB Forschung
- GB IT: Administrative Verfahren (AV)
- GB IT: Forschung & Lehre (F&L)
- GB IT: Klinische Verfahren (KV)
- GB IT: Netzwerk (Netz)
- GB IT: Service & Support (SuS)
- GB IT: System (SYS)
- GB IT: übergreifend
- GB Klinisches Prozess- und Ressourcenmanagement
- GB Personal
- GB Recht
- GB Strategische Unternehmensentwicklung
- GB Studium und Lehre
- GB Technik und Betriebe: Bau-, Anlagen- und Flächenmanagement
- GB Technik und Betriebe: CFM IT
- GB Technik und Betriebe: CFM Medizintechnik
- GB Technik und Betriebe: Infrastrukturelles Facility-Management
- GB Unternehmenscontrolling

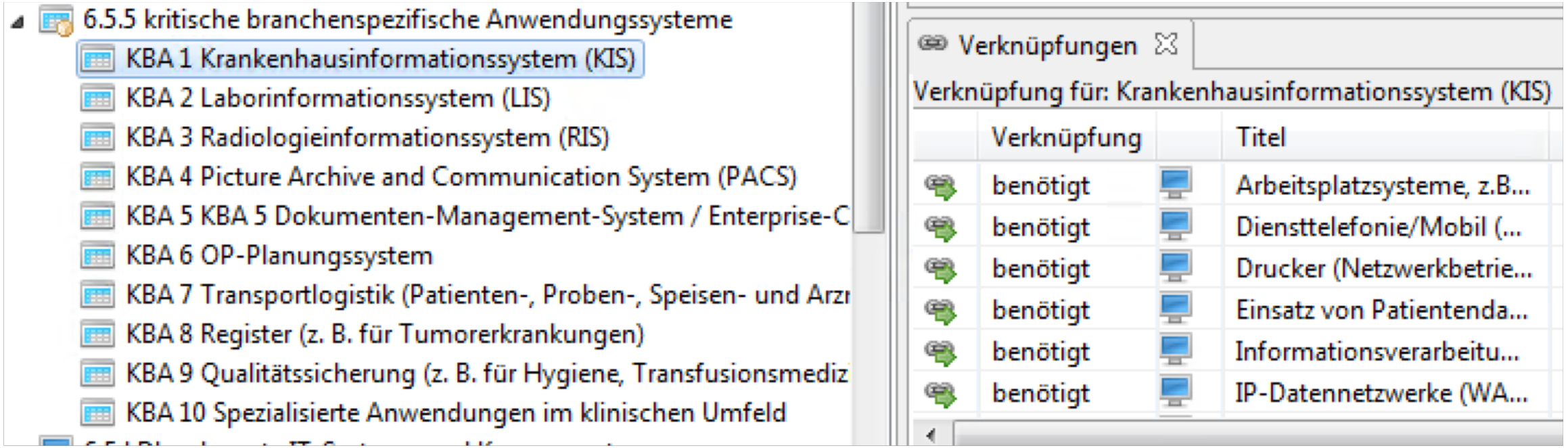
B3S in Verinice - Geschäftsprozesse

- Kritische Dienstleistung => Grundschutz-Geschäftsprozess
- Verknüpfung mit Anwendungen oder anderen Geschäftsprozessen



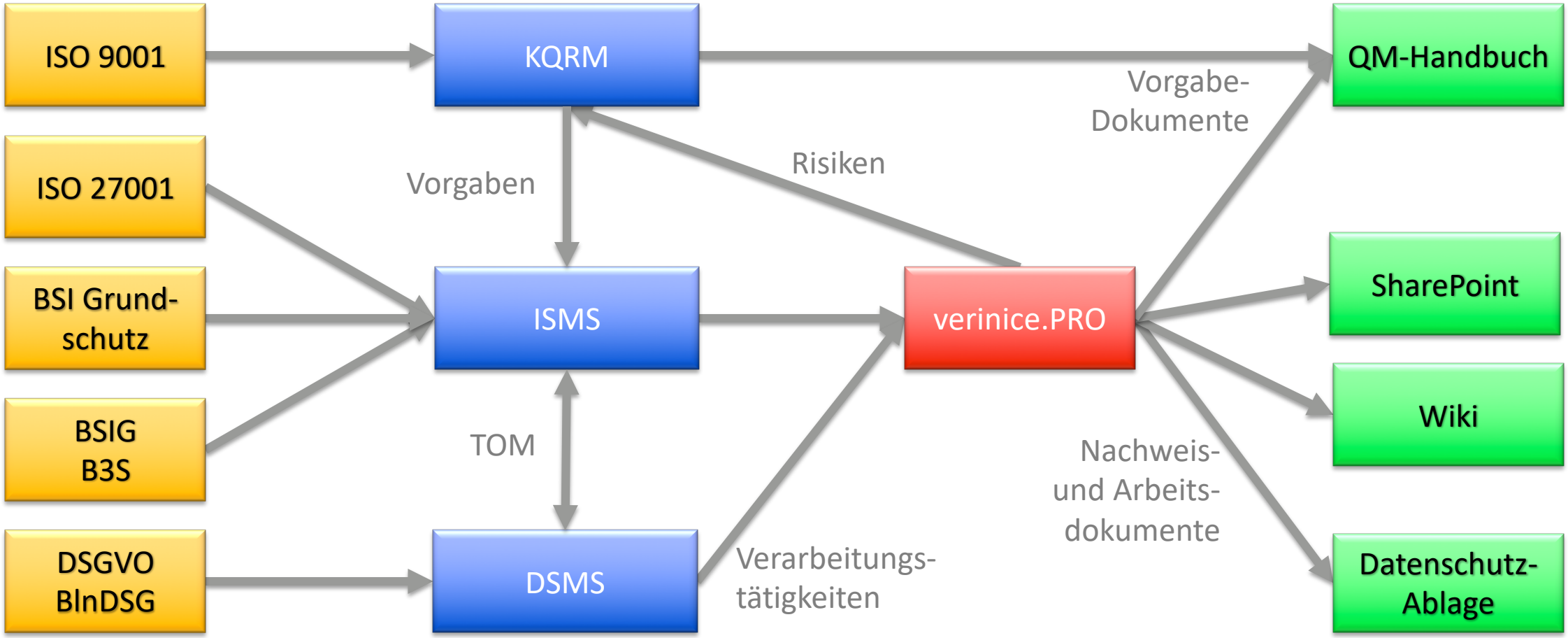
B3S in Verinice - Anwendungen

- Anwendungen werden mit Ressourcen verknüpft



5. Schritt: Integration der Managementsysteme

- Qualitätsmanagement nach ISO9001 als übergeordnetes Managementsystem
- Vorgaben für Dokumentenstruktur aus QM
- Gemeinsame Dokumentation für Datenschutz und ISMS
- Datenschutz nutzt für technisch-organisatorische Maßnahmen das ISMS und Verinice
- Umsetzung der Anforderungen von ISO 9001, ISO 27001, BSI Grundschutz, DSGVO und B3S


ISO 9001
ISO 27001
BSI Grund-schutz
BSIG B3S
DSGVO BlnDSG
KQRM
ISMS
DSMS
Vorgaben
Risiken
TOM
Verarbeitungs-tätigkeiten
verinice.PRO
Vorgabe-Dokumente
Nachweis- und Arbeits-dokumente
QM-Handbuch
SharePoint
Wiki
Datenschutz-Ablage

Fragen?

Michael Römling

www.charite.de
michael.roemling@charite.de

Ulf Riechen

www.riechen.consulting
ulf@riechen.consulting