INSTITUT
PROF
DR
BECKER

Das IT-Sicherheitsgesetz: Risikoaudits

KGNW-Fachtagung
Praxisdialog Krankenhaus-IT und Medizintechnik 2015

Dortmund, 13.01.2015

INSTITUT
PROF
DR
BECKER

Grundlagen

Entwurf IT-SG: Ziele

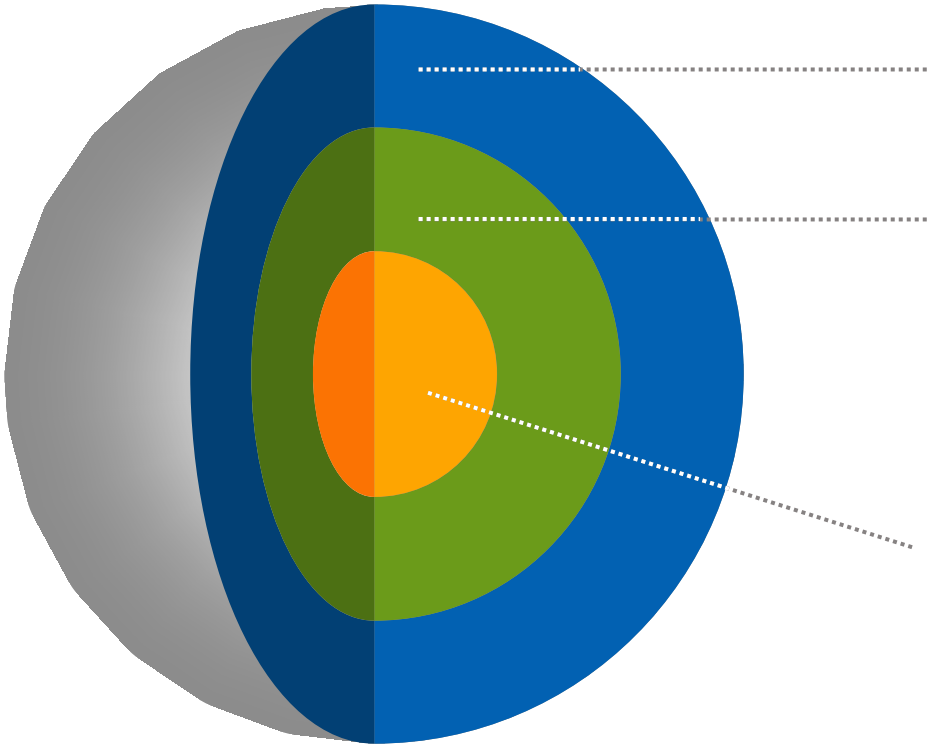
- Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden.
- … den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern …
- Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).

Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Stand 08.12.2014

Risiko

- Risiken sind untrennbar mit jeder unternehmerischen Tätigkeit verbunden.
- Risiken müssen eingegangen werden, ohne Risiken kein Fortschritt.
- Sie können den Prozess der Zielerreichung negativ beeinflussen.
- Sie resultieren ursachenbezogen aus der Unsicherheit zukünftiger Ereignisse, wobei dies mit einem unvollständigen Informationsstand einhergeht.
- Werden Risiken nicht rechtzeitig erkannt und bewältigt, können sie die erfolgreiche Weiterentwicklung der Unternehmung gefährden, sogar in Krisen im Sinn von überlebenskritischen Prozessen einmünden.

Risikoarten



Das **allgemeine** Risiko, das mit allem Handeln verbunden ist

Das **darüber hinausgehende** Risiko

a) das man sich leisten kann, wenn es eintritt – und das man daher auch eingehen kann

b) welches nicht einzugehen man sich nicht leisten kann, weil man keine Wahl mehr hat – man muss dieses Risiko also eingehen

Das Risiko, das man sich **nicht leisten** kann, weil es zur Katastrophe führt – und das man daher nicht eingehen darf

Beliebte Angriffsziele

- Patientendaten.
- Mess- und Laborsysteme.
- Unterstützungs- und Erhaltungssysteme .

- Privatsphäre.
- Vertrauen.
- **Gesundheit und Leben.**

Risikowandel

Ein Patient tauscht das Risiko der unbehandelten Erkrankung ein gegen das Risiko der Erkrankung unter Behandlung.

INSTITUT
PROF
DR
BECKER

Verantwortung für Träger und Leitung

Integration auf Unternehmensebene

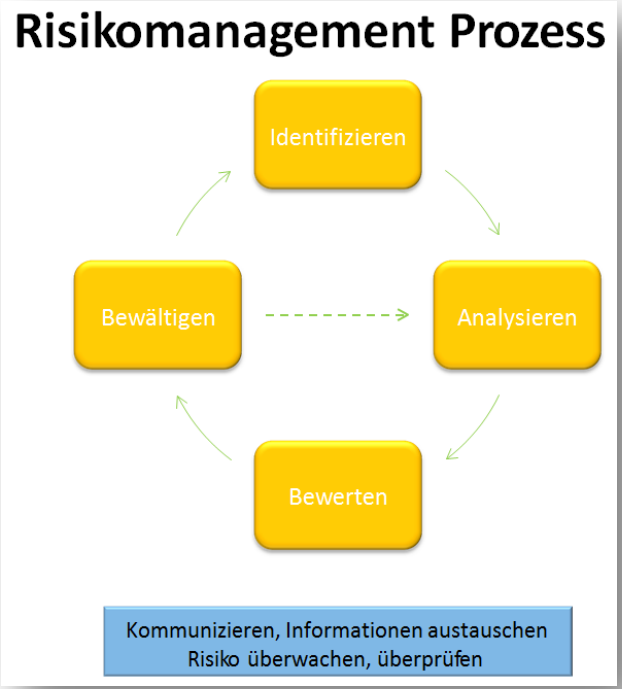
Erhöhung Patientensicherheit, Abwenden bestandsgefährdender Risiken, Förderung Sicherheitskultur, Erfüllung gesetzlicher Aufgaben

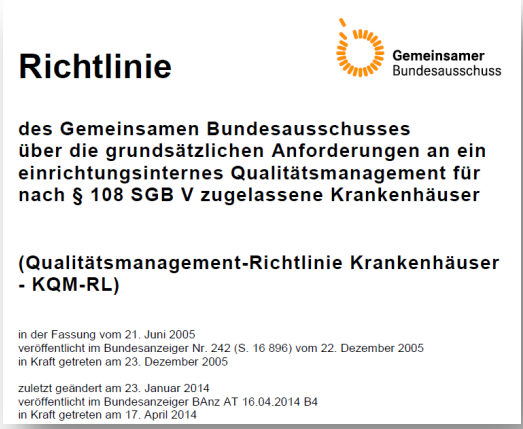
Qualitäts- und Risikomanagement in nicht klinischen Bereichen

- IT
- Versicherung
- Verträge
- Personal
- Erlösmanagement
- Arbeitssicherheit
- Umwelt
- …

Qualitäts- und Risikomanagement in Kliniken & Instituten

- Versicherung
- Verträge
- Personal
- Erlösmanagement
- IT
- Arbeitssicherheit
- Umwelt
- …





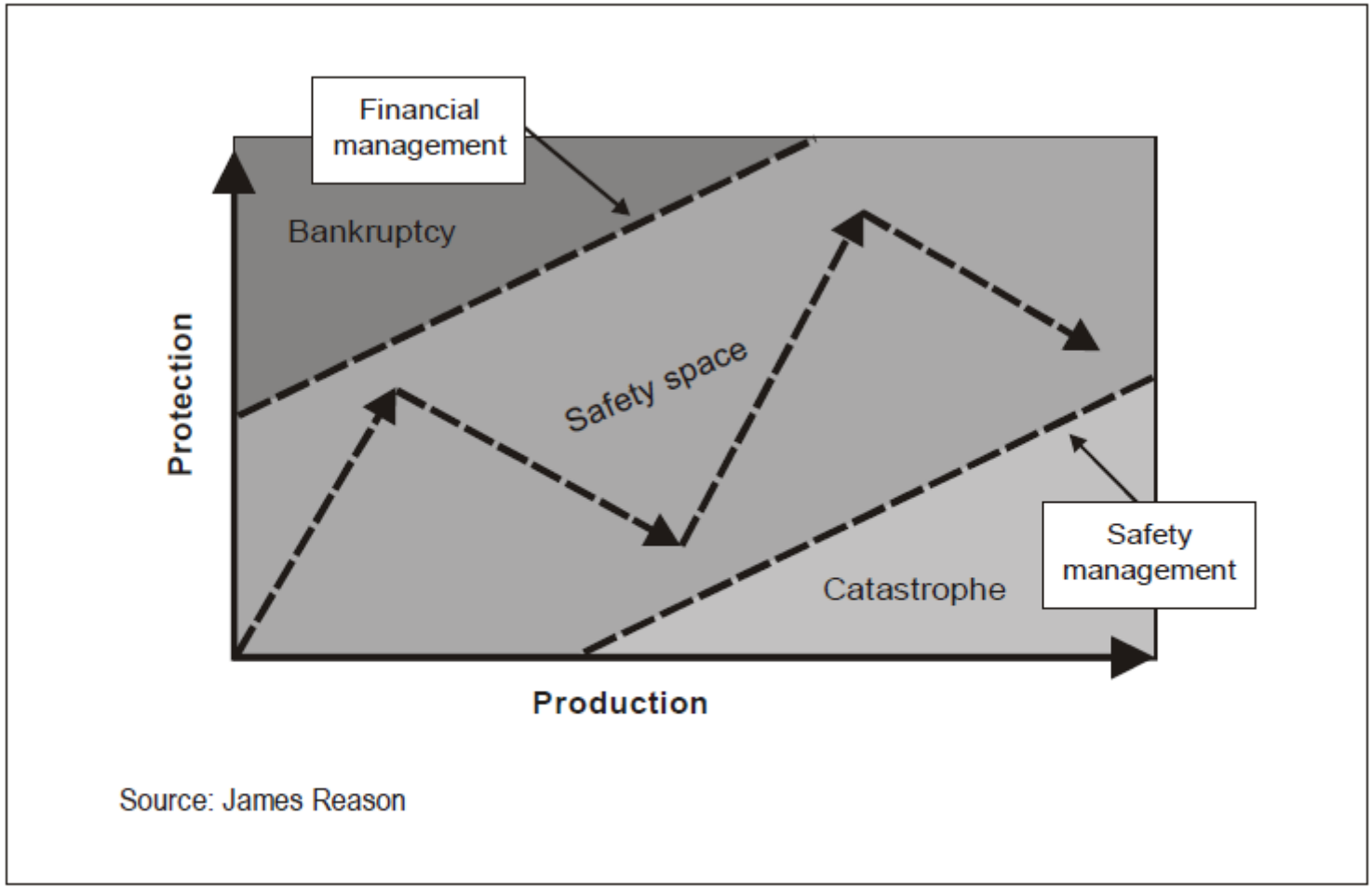


Figure 3-3. The safety space

In: Safety Management Manual (SMM) International Civil Aviation Organization (ICAO) Second Edition - 2009

Verantwortung Leitung

- Sicherstellen, dass die für das Informationssicherheitsmanagementsystem erforderlichen Ressourcen bereitstehen.
- Führen und Unterstützen von Personen, damit diese einen Beitrag zur Wirksamkeit des Informationssicherheitsmanagementsystems leisten.
- Fördern der laufenden Verbesserung.

- Einen Kreislauf von Informationen sicherstellen.
- Sich regelmäßig mit diesen Informationen beschäftigen (Stichwort »Managementbewertung« aus QM- und RM-Normen).

INSTITUT
PROF
DR
BECKER

Audit

Audit

Systematischer, **unabhängiger** und **dokumentierter** Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind.

ÖNORM EN ISO 19011, Ausgabe 2013-10-01, Abschnitt 3.1

Audit

Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die **Auditkriterien** erfüllt sind.

Auditkriterien

Verfahren, Vorgehensweisen oder Anforderungen, die als Bezugsgrundlage (Referenz) verwendet werden, anhand derer ein Vergleich mit dem Auditnachweis erfolgt.

ÖNORM EN ISO 19011, Ausgabe 2013-10-01, Abschnitt 3.1 | 3.3 | 3.2

Auditkriterien: Auch Patientensicherheit!

- Neben anderen Auditkriterien – die ja noch definiert werden – würde mich interessieren, welche Risiken IHRE Organisation mit direktem Patientenbezug identifiziert hat.
- So lerne ich schon eine Menge über ihr Krankenhaus und sein Sicherheitsverständnis.

- Automatisierte patientenindividuelle Abpackung von Arzneimitteln (»Unit-Dose«).
- Steuerung von Beatmungsgeräten.
- Steuerung von Infusionspumpen.
- Berechnung und Applikation von Strahlung.
- Verfügbarkeit von (dringlichen) Befunden.
- Verwechslung von Laborergebnissen.
- ….

Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1

Ahlbrandt J, Röhrig R, Dehm J, Wrede C., Imhoff M, Sektion IT & Medizintechnik der Deutschen Interdisziplinären Vereinigung für Intensiv- und Notfallmedizin e.V., Deutsche Gesellschaft für Biomedizinische Technik (DGBMT) im VDE e.V., Fachausschuss Methodik der Patientenüberwachung. Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1. GMS Med Inform Biom Epidemiol. 2013;9(3):Doc09.

Artikel online frei zugänglich unter
http://www.egms.de/en/journals/mibe/2013-9/mibe000137.shtml

Audit

Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von **Auditnachweisen** und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind.

Auditkriterien

Verfahren, Vorgehensweisen oder Anforderungen, die als Bezugsgrundlage (Referenz) verwendet werden, anhand derer ein Vergleich mit dem Auditnachweis erfolgt.

Auditnachweis

Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen, die für die Auditkriterien zutreffen und verifizierbar sind.

ÖNORM EN ISO 19011, Ausgabe 2013-10-01, Abschnitt 3.1 | 3.3

Audit

Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind.

Auditfeststellungen

Ergebnisse aus der Bewertung der gesammelten Auditnachweise im Hinblick auf Auditkriterien.

Auditschlussfolgerungen

Ergebnis eines Audits nach Berücksichtigung der Auditziele und aller Auditfeststellungen.

ÖNORM EN ISO 19011, Ausgabe 2013-10-01, Abschnitt 3.1 | 3.4. | 3.5

Audittypen

- Internes Audit (»first party audit«)

- Externes Audit
  - Lieferantenaudit (»second party audit«)
  - Auditierung durch unabhängige Dritte (»third party audit«)
    Rechtliche, gesetzliche und ähnliche Zwecke, Zertifizierungszwecke.

ÖNORM EN ISO 19011, Ausgabe 2013-10-01, Seite 5

Entwurf IT-SG: § 8a Abs. 3

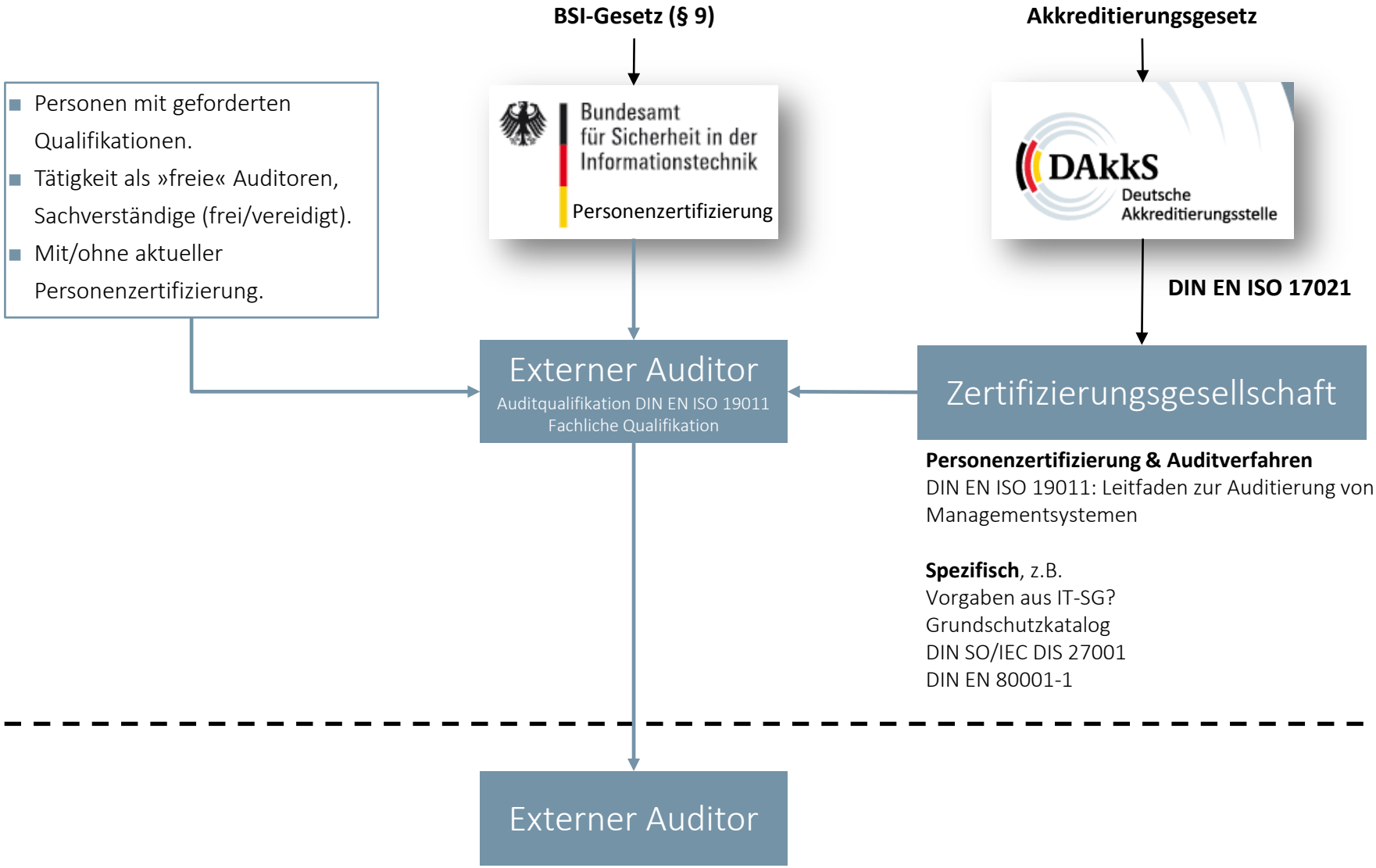
- Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen.
- Der Nachweis kann durch Sicherheits**audits**, Prüfungen oder Zertifizierungen erfolgen.
- Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.
- Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Stand 08.12.2014

Entwurf IT-SG: Begründung zu § 8a

- Die Sicherheitsaudits, Prüfungen oder Zertifizierungen sollen von dazu **nachweislich qualifizierten** Prüfern bzw. Zertifizierern durchgeführt werden.
- Ein Auditor gilt als qualifiziert, wenn er seine **Qualifikation zur Überprüfung der Einhaltung der Sicherheitsstandards** gegenüber dem BSI auf Verlangen formal glaubhaft machen kann.
- Bei Zertifizierungen nach internationalen, europäischen oder nationalen Standards kann auf die bestehenden Zertifizierungsstrukturen zurückgegriffen werden.
- Denkbar ist in diesem Zusammenhang etwa die Anknüpfung an Zertifizierungen, die für die fachlich-technische Prüfung im jeweiligen Sektor angeboten werden (zum Beispiel zertifizierte Prüfer für bestimmte ISO-Normen oder Ähnliches).

Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Stand 08.12.2014


BSI-Gesetz (§ 9)
Akkreditierungsgesetz
Personen mit geforderten Qualifikationen.
Tätigkeit als »freie« Auditoren, Sachverständige (frei/vereidigt).
Mit/ohne aktueller Personenzertifizierung.
Bundesamt für Sicherheit in der Informationstechnik
Personenzertifizierung
DAkkS
Deutsche Akkreditierungsstelle
DIN EN ISO 17021
Externer Auditor
Auditqualifikation DIN EN ISO 19011
Fachliche Qualifikation
Zertifizierungsgesellschaft
Personenzertifizierung & Auditverfahren
DIN EN ISO 19011: Leitfaden zur Auditierung von Managementsystemen
Spezifisch, z.B.
Vorgaben aus IT-SG?
Grundschutzkatalog
DIN SO/IEC DIS 27001
DIN EN 80001-1
Umwelt (außen)
Krankenhaus (innen)
Externer Auditor

Interne Audits (DIN EN 15224; 8.2.2)

Die Organisation muss in geplanten Abständen interne Audits durchführen.

… Prozesse und Bereiche sowie die Ergebnisse früherer Audits berücksichtigt werden müssen.

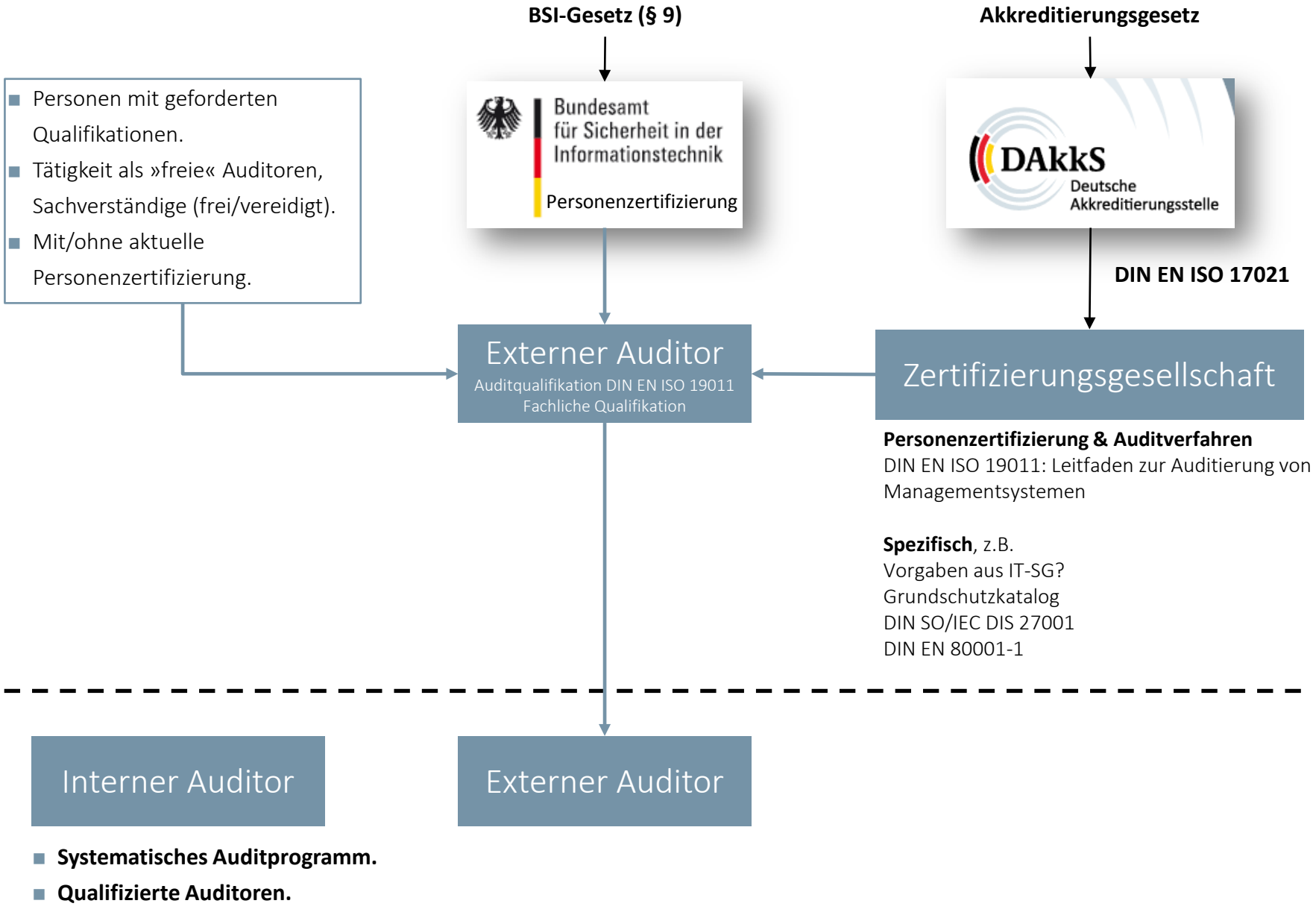
Die Auditkriterien, der Auditumfang, die Audithäufigkeit und die Auditmethoden müssen festgelegt werden.

Ein dokumentiertes Verfahren zur Festlegung der Verantwortungen für und der Anforderungen an die Planung und Durchführung von Audits, an die Erstellung von Aufzeichnungen und an das Berichten von Ergebnissen muss eingerichtet werden.

Aufzeichnungen über die Audits und deren Ergebnisse müssen geführt werden.

Folgemaßnahmen müssen die Verifizierung der ergriffenen Maßnahmen und die Berichterstattung über die Verifizierungsergebnisse enthalten.

Analoge Ausführungen sind in weiteren Normen/Regeln zu finden, so zum Beispiel
DIN ISO/IEC DIS 27001; ONR 49001


BSI-Gesetz (§ 9)
Akkreditierungsgesetz
Personen mit geforderten Qualifikationen.
Tätigkeit als »freie« Auditoren, Sachverständige (frei/vereidigt).
Mit/ohne aktuelle Personenzertifizierung.
Bundesamt für Sicherheit in der Informationstechnik
Personenzertifizierung
DAkkS
Deutsche Akkreditierungsstelle
DIN EN ISO 17021
Externer Auditor
Auditqualifikation DIN EN ISO 19011
Fachliche Qualifikation
Zertifizierungsgesellschaft
Personenzertifizierung & Auditverfahren
DIN EN ISO 19011: Leitfaden zur Auditierung von Managementsystemen
Spezifisch, z.B.
Vorgaben aus IT-SG?
Grundschutzkatalog
DIN SO/IEC DIS 27001
DIN EN 80001-1
Umwelt (außen)
Krankenhaus (innen)
Interner Auditor
Externer Auditor
Systematisches Auditprogramm.
Qualifizierte Auditoren.

Synergien der internen Auditverfahren

- Wenn es ihren Krankenhäusern geplante Auditverfahren gibt, dann sollte die Frage nach Synergien gestellt werden.
- Auch in klinischen Auditverfahren können bestimmte Inhalte aus Sicht der IT thematisiert werden.
- Falls angemessen vorhanden, können evt. auch Personalressourcen aus dem »klinischen QM« genutzt werden.
- Soviel inhaltliche Trennung wie erforderlich, aber soviel Integration, wie sinnvoll!

INSTITUT
PROF
DR
BECKER

Modernes Auditverständnis

Das Audit als PDCA-Zyklus

P Planen: Thema? Ziele? Kriterien? Wo? Wann? Wer? Wie?

D Durchführen

C Auditfeststellungen? Was haben wir gelernt? Welche Erkenntnisse gewonnen?

A Empfehlungen?

Das Audit als PDCA-Zyklus

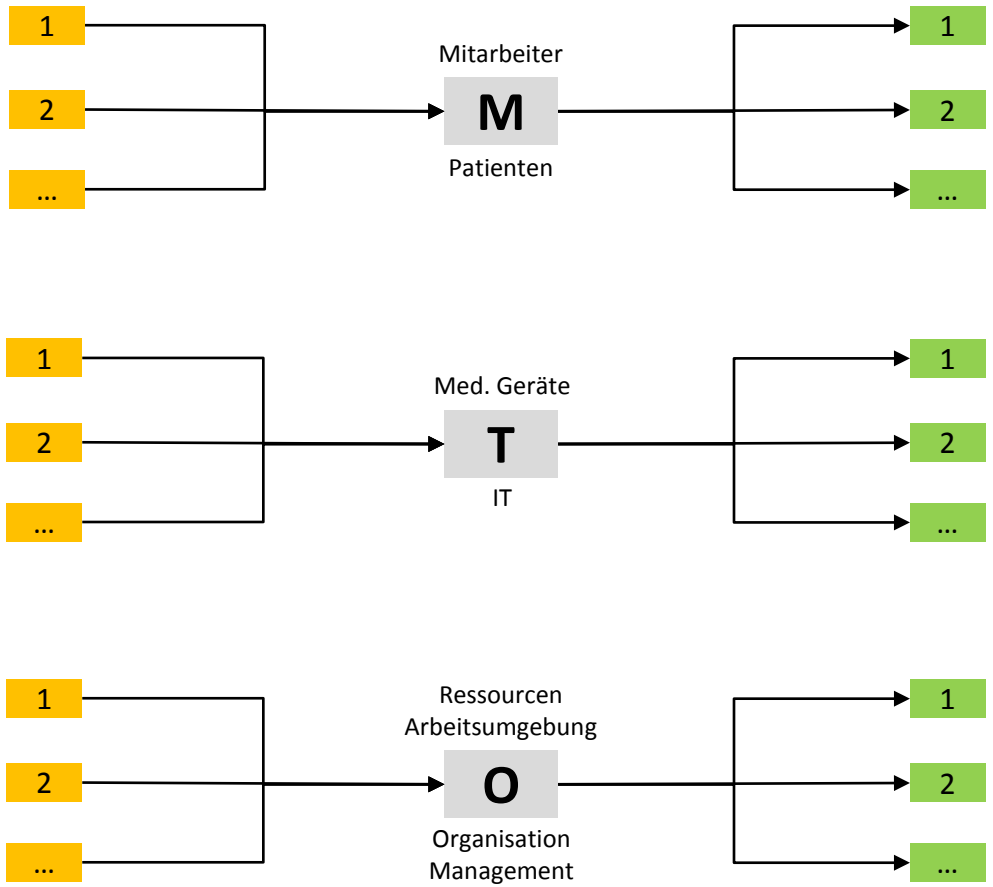
- Unter diesem modernen Verständnis ist Auditieren mehr als nur »Anforderungen abhaken«!
- Identifizierung neuer Risiken.
- Risikoüberwachung.
- Prävention!
- Mitarbeiter in Szenarien denken lassen (Systemische Fragen).
- Mitarbeitermotivation.
- …

Problemseite (Ursachen/Quellen)

Das wären dann auch die Punkte zum Auditieren im Rahmen der Risikoüberwachung!

Lösungsseite

Hier lege ich dann auch fest, an wen ich die Lösung adressieren muss.
»Wen brauche ich, wen kann ich ungestraft weglassen?«



Veränderungsprozesse

- Es soll ein neuer, systematischer Prozess eingeführt werden, aber ist der Veränderungsprozess selber systematisch?

- Der Übergang von dem alten zu einem neuen Muster birgt Gefahren!

Daumenregel

Sie können maximal 20% der Prozesse durch direkte Führung begleiten bzw. beeinflussen, die restlichen 80% nur durch Ausbildung und intelligente Qualitätssicherung (Führungsprozesse!)

Patient safety – two approaches

- Descriptive approach: Written standards, Accreditation …

- Performance approach: Transfer in daily processes

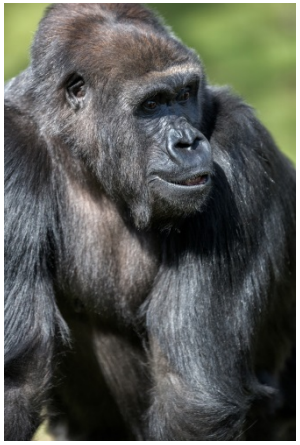
Moving beyond traditional accreditation: applying lessons from safety-critical industries
Karen Timmons; US

The International Society for Quality in Health Care. 29th International Conference, Geneva, 21.-24.10.2012

Entwicklungsstadien der Sicherheitskultur

Sicherheit wird als **kontinuierlicher Verbesserungsprozess** angesehen, zu dem **jeder Einzelne** beitragen kann.

Sicherheit wird **Unternehmensziel** und wird vor allem mit **Sicherheitszielen operationalisiert**.



Sicherheit basiert hauptsächlich auf **Regeln** und **Vorschriften** und deren Einhaltung (technische Aspekte).

Restrisiko

- Risiko, welches nach der Umsetzung aller angemessenen Maßnahmen der Risikobewältigung verbleibt.
- Enthält auch alle noch unbekannten Risiken!

- Ich versichere Ihnen, die Interpretation des »Restrisikolevels« ist recht variabel …

INSTITUT
PROF
DR
BECKER

Vielen Dank!

T +49 2205 920 460
F +49 2205 920 462
M +49 172 29 88 040
E becker@i-pdb.de
W www.i-pdb.de

Institut Prof. Dr. Becker
Nonnenweg 120a
51503 Rösrath