

DIN EN 80001-1
(VDE 0756-1)
DIN

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.

VDE

ICS 11.040.01; 35.110; 35.240.80

Einsprüche bis 2018-10-03
 Vorgesehen als Ersatz für
DIN EN 80001-1
(VDE 0756-1):2011-11

Entwurf

**Sicherheit, Effektivität und Daten- und Systemsicherheit bei
 Implementierung und Gebrauch von eingebundenen Medizinprodukten
 oder eingebundener Gesundheitssoftware –
 Teil 1: Anwendung von Risikomanagement
 (IEC 62A/1244/CD:2018); Text Deutsch und Englisch**

Safety, effectiveness and security in the implementation and use of connected medical devices
 or connected health software –

Part 1: Application of risk management

(IEC 62A/1244/CD:2018); Text in German and English

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-08-03 wird der Öffentlichkeit zur Prüfung und
 Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses
 Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-
 Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de,
 sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser
 Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für
 Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in
 DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten
 Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 72 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE
 DIN-Normenausschuss Medizin (NAMed)

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Inhalt	Seite
Nationales Vorwort.....	4
Einleitung	5
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Grundsätze	13
5 Struktur	13
5.1 Allgemeines	13
5.2 Führung und Verpflichtung	13
5.2.1 Allgemeines	13
5.2.2 Integration von Risikomanagement.....	15
5.3 Gestaltung/Planung	15
5.3.1 Verstehen der Organisation und ihres Kontexts	15
5.3.2 Artikulieren der Risikomanagementverpflichtung.....	15
5.3.3 Zuweisung von organisatorischen Rollen, Rechenschaftspflichten, Verantwortlichkeiten und Befugnissen.....	17
5.3.4 Zuordnung von Ressourcen	19
5.3.5 Einrichten der Kommunikation und Konsultation	19
5.4 Implementierung	19
5.4.1 Richtlinie für das RISIKOMANAGEMENT.....	19
5.4.2 RISIKOMANAGEMENT-PROZESS	19
5.4.3 Risikomanagement-Planung	20
5.4.4 Beschreibung der risikorelevanten Elemente.....	20
5.5 Risikobewertung	21
5.6 Verbesserung	21
6 Prozess.....	21
6.1 Allgemeines	21
6.2 Kommunikation und Konsultation.....	21
6.3 Einrichten des Kontextes.....	21
6.3.1 Allgemeines	21
6.3.2 Festlegung von Zweck und Anwendungsbereich des Prozesses.....	22
6.3.3 Interner und externer Kontext.....	22
6.3.4 Festlegung von Risikokriterien	22
6.4 RISIKOBEURTEILUNG	22
6.4.1 Allgemeines	22
6.4.2 Risikoidentifikation.....	22

6.4.3	RISIKOANALYSE.....	22
6.4.4	RISIKOBEWERTUNG	22
6.5	Risikobehandlung.....	23
6.5.1	Analyse der Wahlmöglichkeiten der Risikobeherrschung.....	23
6.5.2	Maßnahmen der Risikobeherrschung.....	23
6.5.3	Umsetzung von Maßnahmen zur Risikobeherrschung.....	24
6.5.4	VERIFIZIERUNG von Maßnahmen der RISIKOBEHERRSCHUNG	24
6.5.5	Neue RISIKEN, die von Maßnahmen der RISIKOBEHERRSCHUNG herrühren.....	24
6.5.6	Bewertung des RESTRIKOS und Berichterstattung.....	24
6.5.7	PROZESS DES ÄNDERUNGS- UND AUSLIEFERUNGSMANAGEMENTS.....	25
6.5.8	Entscheidung, wie das Risikomanagement angewandt wird.....	25
6.6	Start des Echtbetriebs.....	27
6.7	Risikomanagement im Echtbetrieb	28
6.7.1	Überwachung	28
6.7.2	EREIGNISMANAGEMENT	28
6.8	Überwachen und Überprüfen	28
6.9	Aufzeichnen und Berichten	28
6.9.1	Allgemeines.....	29
6.9.2	Hersteller von MEDIZINPRODUKTEN	29
6.9.3	Anbieter sonstiger IT-Technologie	30
6.9.4	Dokumentation des MEDIZINISCHEN IT-Netzwerks	30
6.9.5	Verantwortlichkeitsvereinbarungen.....	31
6.9.6	Risikomanagement-Plan für das medizinische IT-Netzwerk	32
6.9.7	Dokumentenprüfung.....	33
Anhänge und Literaturhinweise.....		34
Vorläufiger Anhang – Zuordnung von Text aus IEC 80001-1 zum umstrukturierten Dokument (Abschnitt für Abschnitt).....		35

Nationales Vorwort

Das internationale Dokument IEC 62A/1244/CD:2018 „Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 1: Application of risk management“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine noch nicht autorisierte deutsche Übersetzung.

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung des CD entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom SC 62A „Common aspects of electrical equipment used in medical practice“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und den nationalen Komitees zur Stellungnahme vorgelegt.

Die IEC und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Da der Abstimmungszeitraum für einen FDIS bzw. Schluss-Entwurf FprEN nur 6 Wochen beträgt, und dann keine sachlichen Stellungnahmen mehr abgegeben werden können, sondern nur noch eine „JA/NEIN“-Entscheidung möglich ist, wobei eine „NEIN“-Entscheidung fundiert begründet werden muss, wird bereits der CD als DIN-Norm-Entwurf veröffentlicht, um die Stellungnahmen aus der Öffentlichkeit frühzeitig berücksichtigen zu können.

Für dieses Dokument ist das nationale Arbeitsgremium UK 811.3 „Sicherheit von medizinisch genutzten Geräten/Systemen/Einrichtungen in der vernetzten Anwendung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Änderungen

Gegenüber **DIN EN 80001-1 (VDE 0756-1):2011-11** wurden folgende Änderungen vorgenommen:

- a) Umstellung auf die Struktur einer Qualitätsmanagementnorm ähnlich DIN EN ISO 14385;
- b) Verbesserungen im Prozessablauf;
- c) Die deutsche Fassung wurde in **Abschnitt 3** an die aktuellen Standardtexte angepasst.

Sicherheit, Effektivität und Daten- und Systemsicherheit bei Implementierung und Gebrauch von eingebundenen Medizinprodukten oder eingebundener Gesundheitssoftware – Teil 1: Anwendung von Risikomanagement

Einleitung

Der folgende Text leitet sich aus der durch IEC/SC 62A und ISO/TC 215 genehmigten Absicht und Begründung ab, die zu Beginn der Überarbeitung von IEC 80001-1 bestätigt wurden.

Aus berichteten Vorfällen, aus der Forschung und aus Veröffentlichungen (z. B. der Bericht „Health IT and Patient Safety“ des U.S. Institute of Medicine (IOM) vom November 2012) geht hervor, dass Sicherheitsrisiken überall in den Phasen des Lebenszyklus eingebracht werden können.

Im November 2014 hat IEC/SC 62A, unterstützt von ISO/TC 215 die Überarbeitung von IEC 80001-1 grundsätzlich genehmigt. Unter Berücksichtigung der laufenden Arbeiten der Ad-Hoc-Gruppe ISO/TC 215 „Health Software“ (Gesundheitssoftware), zu der auch Fachleute von SC 62A gehörten, stimmten die Verantwortlichen von 62A zu, den formellen Beginn der Überarbeitung von IEC 80001-1 zu verschieben, bis die Ad-hoc-Gruppe ihren Bericht abgeschlossen hat.

Die Ad-Hoc-Gruppe ISO/TC 215 „Health Software“ benötigte zwei Jahre für die Arbeiten, die zu ISO/TS 17791 führten und sich mit der erweiterten Fragestellung befassten, wie das Risikomanagement im Kontext der Informationslenkung und dem Gesamt-Sicherheitsmanagement innerhalb einer Organisation im Gesundheitswesen zu behandeln ist. Die Ad-Hoc-Gruppe veröffentlichte im Jahr 2015 einen Bericht, „Health Software & Health IT Safety Standards, Future State Architecture/Framework and Roadmap“, der spezifische Empfehlungen für zukünftige Arbeiten sowohl im Kontext mit der Überarbeitung der Dokumente IEC 80001 als auch an neuen „grundlegenden“ Dokumenten, die den gesamten Lebenszyklus von HIT (IT im Gesundheitswesen) abdecken, enthielt.

Gleichzeitig liefen mehrere Projekte zur Implementierung der Normenreihe IEC 80001 in verschiedenen Ländern, in welchen Anbieter und klinische Fachleute daran arbeiteten, Risikomanagement auf vernetzte Medizintechnologie anzuwenden. Diese Projekte waren unterschiedlich erfolgreich, einige mehr als erwartet, aber viel andere verliefen enttäuschend und führten teilweise zur Frage, ob die Normenreihe IEC 80001 brauchbar sei und ihr Ziel der erheblichen Verbesserung der Sicherheit und Effektivität von Medizintechnologien erreichen könne.

- Zusätzlich zur schwierigen „behördlichen“ Sprache, die in Teilen der Normenreihe 80001 verwendet wurde, ermittelten die Implementierungsprojekte die folgenden Hindernisse für eine Übernahme dieser Normen.
- unzureichende Berücksichtigung der Patientensicherheit an potentiellen Problemstellen;
- unzureichende Unterstützung durch die Geschäftsleitung innerhalb der HDO (Gesundheitsorganisation; en: health delivery organization);
- Bedeutung der Norm in der modernen Welt von „Plattform/Software/usw. als eine Dienstleistung“ und komplexer Softwaresysteme;
- Unstimmigkeiten im Zusammenhang mit Sicherheit zwischen Organisationen und ihren Prozessen;
- Herausforderungen mit der Skalierbarkeit der Norm und kein klares Verständnis davon, „wo man anfangen soll“;
- Mangel an Bewusstsein und Verständnis hinsichtlich der Verknüpfungen zwischen Sicherheitsfragen in Bezug auf Medizinprodukte und vernetzte Umgebungen;

Der Zweck dieser Überarbeitung ist die Behandlung dieser Fragen innerhalb von IEC 80001-1 und die Erweiterung des Anwendungsbereichs (wie in ISO/TC 215 Resolution 2015-41 gefordert) auf:

- a) Erweiterung des Anwendungsbereichs von Netzwerken mit eingebundenen Medizinprodukten auf IT-Infrastruktur mit eingebundenen Medizinprodukten oder eingebundener Gesundheitssoftware;
- b) Erweiterung des Anwendungsbereichs, um Risikomanagement innerhalb des weiteren Kontexts von IT-Service-Management zu behandeln;

- c) Behandlung des internen und externen Kontexts, einschließlich Personen, Technologie, Organisation, Prozess, Umgebung, und
- d) Erforschung des Bedarfs zur Anwendung von Konzepten der Systemplanung auf Prozesse des IT-Lebenszyklus im Gesundheitswesen.

Die Elemente des Risikomanagements, die in dieser Überarbeitung von **IEC 80001-1** zu behandeln sind, beruhen auf bestehenden Normen, wobei Konzepte für einen Gebrauch durch eine Gesundheitsorganisation (HDO) und an der Unterstützung der Implementierung und des klinischen Gebrauchs vernetzter Medizinprodukte oder vernetzter Gesundheitssoftware von Beteiligten nach Bedarf übernommen und erweitert wurden. Die unternommenen Arbeiten sind mit bestehenden Normen, einschließlich Richtlinie 73, ISO 31000 und ISO 14971, abgestimmt und nutzen diese.

1 Anwendungsbereich

Der nachgenannte Anwendungsbereich wurde als Teil des Vorschlags zur Überarbeitung von IEC 80001-1:2010 genehmigt. Im Gegensatz zu diesem Anwendungsbereich wurde der restliche Text aus IEC 80001-1 übernommen, wurde jedoch umstrukturiert, um der Struktur der neuen Ausgabe von ISO 31000 zu folgen, wie in der Einleitung erläutert.

Die Implementierung und der Gebrauch von vernetzten Medizinprodukten oder vernetzter Gesundheitssoftware zur Unterstützung von IT-Systemen im Gesundheitswesen und Dienstleistungen bringt Risiken mit sich. Diese Internationale Norm enthält allgemeine Anforderungen für die Anwendung von Risikomanagement auf Systeme der Informationstechnologie in der Medizin (HIT), indem die Schutzziele von Sicherheit, Effektivität und sowohl Daten- als auch Systemsicherheit (einschließlich Vertraulichkeit) behandelt werden, und dabei zweckmäßige Interessengruppen einbezogen wurden. In diesem Kontext bezieht sich „Implementierung“ auf die Phasen und Tätigkeiten eines Technologie-Lebenszyklus, die gefordert sind, nachdem Gesundheitssoftware und Medizinprodukte herausgegeben und auf dem Markt eingeführt wurden, und für die Vernetzung und den Gebrauch vorbereitet werden.

Vernetzte Geräte, Software und HIT-Systeme beruhen im Allgemeinen auf gemeinsam benutzter IT-Infrastruktur, die aus drahtgebundenen und drahtlosen Netzwerken, direkten Verbindungen (z. B. RS232, USB) oder internetbasierten Diensten (z. B. Cloud-Dienste) aufgebaut sein darf. Diese IT-Infrastrukturen werden häufig sowohl für klinische als auch für nicht-klinische Organisationsfunktionen (z. B. Abrechnung, Zeitplanung, soziale Vernetzung, Multimedia, gemeinsame Datennutzung) verwendet – woraus sich Auswirkungen auf den Anwendungsbereich von Risikomanagement ergeben. Diese Norm wird auf bestehende oder neue HIT-Systeme anwendbar sein und wird von der Einbindung eines einzelnen Produkts oder einer einzelnen Software-Instanz bis hin zu großen eingebundenen HIT-Systemen gelten.

Diese Norm stellt Anforderungen und einen Leitfaden für die vielen Interessengruppen bereit, die potentiell an der Anwendung von Risikomanagement auf HIT-System beteiligt sind. Beispiele sind unter anderem Gesundheitsorganisationen, Hersteller von Medizinprodukten, IT-Service-Anbieter in der Gesundheitsversorgung. Sie gilt auch für Gesundheitsorganisationen die ihre eigene Gesundheitssoftware oder -hardware geschaffen haben.

Diese Norm behandelt kein Risikomanagement, das durch einen Hersteller von Medizinprodukten oder einen Entwickler von Gesundheitssoftware während jenen Phasen des Lebenszyklus von der Konzipierung bis zur Freigabe angewendet wird.

Diese Norm behandelt keine regulatorischen oder gesetzlichen Anforderungen.

ANMERKUNG In dieser Norm wird die Konjunktion „oder“ als ein „einschließendes oder“ verwendet, wodurch eine Erklärung wahr ist, wenn eine beliebige Kombination der Bedingungen wahr ist.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: unter <http://www.iso.org/obp>

3.1

BEGLEITPAPIER

Dokument, das einem MEDIZINPRODUKT oder einem Zubehör beigelegt ist und das Informationen für die VERANTWORTLICHE ORGANISATION oder den BEDIENER enthält, insbesondere bezüglich der SICHERHEIT

Anmerkung 1 zum Begriff: Angepasst aus IEC 60601-1:2005, Definition 3.4.

3.2

ÄNDERUNGS- UND AUSLIEFERUNGSMANAGEMENT

PROZESS mit entsprechenden Eingaben und Ergebnissen, der sicherstellt, dass alle Änderungen am IT-NETZWERK in einer kontrollierten Weise beurteilt, genehmigt, implementiert und überprüft wurden und dass Änderungen in einer kontrollierten Weise mittels eines KONFIGURATIONSMANAGEMENTS bis zur Auslieferung der Änderung übergeben, verteilt und verfolgt werden

Anmerkung 1 zum Begriff: Angepasst aus ISO/IEC 20000-1:2005, 9.2 (Änderungsmanagement) und 10.1 (Auslieferungsmanagement).

3.3

ÄNDERUNGSERLAUBNIS

Ergebnisdokument des RISIKOMANAGEMENT-PROZESSES, das eine spezifizierte Änderung oder einen Änderungstyp ohne weitere Risikomanagement-Tätigkeiten innerhalb spezifizierter Randbedingungen erlaubt

3.4

KONFIGURATIONSMANAGEMENT

PROZESS, der sicherstellt, dass Konfigurationsinformationen von Komponenten und vom IT-NETZWERK in präziser und kontrollierter Weise definiert und gepflegt werden, und der einen Mechanismus für die Identifizierung, Kontrolle und Verfolgung von Versionen des IT-NETZWERKS LIEFERT

Anmerkung 1 zum Begriff: Angepasst aus ISO/IEC 20000-1:2005, 9.1.

3.5

DATEN- UND SYSTEMSICHERHEIT

(EN: DATA AND SYSTEM SECURITY)

Betriebszustand eines medizinischen IT-Netzwerks, in dem wichtige Informationen (Daten und Systeme) vor Beeinträchtigung der Vertraulichkeit, vor Beeinträchtigung der Integrität und vor Beeinträchtigung der Verfügbarkeit ausreichend geschützt sind

Anmerkung 1 zum Begriff: Wenn „Security“ (Sicherheit) in dieser Norm erwähnt wird, sollte sie immer so betrachtet werden, dass DATEN- UND SYSTEMSICHERHEIT eingeschlossen sind.

Anmerkung 2 zum Begriff: Die Daten- und Systemsicherheit ist durch Richtlinien, Anleitungen, Infrastruktur und Dienste gewährleistet, die zum Schutz wichtiger Informationen und Systeme entwickelt wurden, mit denen Informationen erfasst, übertragen, gespeichert und angewendet werden, um die Ziele der Organisation anzustreben.

3.6

EFFEKTIVITÄT

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

3.7

EREIGNISMANAGEMENT

PROZESS, der sicherstellt, dass alle Ereignisse, die den Betrieb des IT-NETZWERKS negativ beeinflussen können oder könnten, in einer kontrollierten Weise erfasst, bewertet und bearbeitet werden

Anmerkung 1 zum Begriff: Angepasst aus ISO/IEC 20000-1:2005, 8.2 (Management von Ereignissen) und 8.3 (Management von Problemen).

3.8

SCHADEN

physische Verletzung oder Schädigung der menschlichen Gesundheit oder Schädigung von Gütern oder der Umwelt oder Verringerung der EFFEKTIVITÄT oder Verletzung der DATEN- UND SYSTEMSICHERHEIT

Anmerkung 1 zum Begriff: Angepasst aus ISO 14971:2007, 2.2.

3.9

GEFÄHRDUNG

potentielle SCHADENS-Quelle

[QUELLE: ISO 14971:2007, 2.3]

3.10

ZWECKBESTIMMUNG

(EN: INTENDED USE/INTENDED PURPOSE)

Verwendung, für die ein Produkt, ein PROZESS oder eine Leistung gemäß der durch den Hersteller gelieferten Spezifikationen, Anweisungen und Angaben bestimmt ist

[QUELLE: ISO 14971: 2007, Definition 2.5]

3.11

INTEROPERABILITÄT

Eigenschaft, die es ermöglicht, dass unterschiedliche Systeme oder Komponenten für einen festgelegten Zweck zusammenarbeiten

3.12

IT-NETZWERK

(INFORMATIONSTECHNOLOGIE-NETZWERK)

System oder Systeme, die aus Kommunikationsknoten und Übertragungsstrecken bestehen, um eine physikalisch verbundene oder drahtlose Übertragung zwischen zwei oder mehr Kommunikationsknoten zu ermöglichen

Anmerkung 1 zum Begriff: Angepasst aus IEC 61907:2009 Begriff 3.1.1.

Anmerkung 2 zum Begriff: Der Anwendungsbereich des medizinischen IT-Netzwerks wird in dieser Norm durch die verantwortliche Organisation definiert, basierend auf der Frage, wo sich die Medizinprodukte im medizinischen IT-Netzwerk befinden und basierend auf der definierten Anwendung des Netzwerks. Es kann eine IT-Infrastruktur enthalten sowie Elemente der häuslichen Pflege und nicht-klinische Elemente. Siehe auch [6.9.4](#).

3.13

SCHUTZZIELE

(EN: KEY PROPERTIES)

drei Merkmale von IT-NETZWERKEN (SICHERHEIT, EFFEKTIVITÄT und DATEN- UND SYSTEMSICHERHEIT), auf die sich das Risikomanagement bezieht

3.14

MEDIZINPRODUKT

alle Instrumente, Apparate, Geräte, Maschinen, Vorrichtungen, Implantate, In-vitro-Reagenzien, Kalibriermittel, Software, Stoffe oder andere ähnliche oder zugehörige Gegenstände:

- a) die vom Hersteller zur Anwendung für Menschen einzeln oder in Kombination für einen oder mehrere der folgenden spezifischen Zwecke bestimmt sind:
- Diagnose, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten;
 - Diagnose, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen;
 - Untersuchung, Ersatz, Veränderung oder Unterstützung des anatomischen Aufbaus oder eines physiologischen Prozesses;
 - Unterstützung oder Erhaltung des Lebens;
 - Empfängnisregelung;
 - Desinfektion von Medizinprodukten;
 - Lieferung von Informationen für medizinische oder diagnostische Zwecke durch In-vitro-Untersuchung von Proben, die aus dem menschlichen Körper gewonnen werden;

- b) deren Hauptwirkung im oder am menschlichen Körper nicht durch pharmakologische, immunologische oder metabolische Mittel erreicht wird, deren Wirkungsweise aber durch solche Mittel unterstützt werden kann.

Anmerkung 1 zum Begriff: Die Definition eines Gerätes für die *In-vitro*-Untersuchung schließt unter anderem Reagenzien, Kalibratoren, Vorrichtungen zur Gewinnung und Speicherung von Proben, Kontrollmaterialien und zugehörige Instrumente und Apparate ein. Die Information eines solchen *In-vitro*-Diagnosegerätes kann für Zwecke der Diagnose, Überwachung oder Kompatibilität bestimmt sein. In manchen Rechtsräumen können einige *In-vitro*-Diagnosegeräte einschließlich der Reagenzien und Ähnlichem durch eigene Vorschriften geregelt sein.

Anmerkung 2 zum Begriff: Produkte, die in einigen Rechtsräumen als Medizinprodukt angesehen werden dürfen, für die jedoch noch keine harmonisierte Herangehensweise vorliegt, sind unter anderem:

- Hilfen für Behinderte;
- Produkte für die Behandlung bzw. Diagnostik von Krankheiten und Verletzungen bei Tieren;
- Zubehör für Medizinprodukte (siehe Anmerkung 3);
- Desinfektionsmittel;
- tierisches und menschliches Gewebe enthaltende Produkte, die möglicherweise den Anforderungen der obigen Definition entsprechen, jedoch unterschiedlichen Kontrollmaßnahmen unterliegen.

Anmerkung 3 zum Begriff: Zubehör, das von Herstellern spezifisch zur Verwendung zusammen mit einem „Haupt“-Medizinprodukt vorgesehen ist, damit dieses Medizinprodukt seine Zweckbestimmung erfüllen kann, sollte den gleichen GHTF-Verfahren unterliegen, die für das Medizinprodukt selbst gelten. Zum Beispiel wird ein Zubehör so klassifiziert, als ob es ein eigenständiges Medizingerät wäre. Das kann dazu führen, dass das Zubehör eine andere Klassifizierung hat als das Hauptgerät.

Anmerkung 4 zum Begriff: Komponenten für Medizingeräte werden im Allgemeinen durch das Qualitätssystem des Herstellers und die Verfahren der Konformitätsbewertung kontrolliert. In manchen Rechtsräumen sind Komponenten in der Definition des „Medizingerätes“ enthalten.

[QUELLE: GHTF SG1/N29R16:2005]

3.15

MEDIZINPRODUKTE-SOFTWARE

Softwaresystem, das entwickelt wurde, um in das MEDIZINPRODUKT integriert zu werden, oder das für die Benutzung als selbstständiges MEDIZINPRODUKT vorgesehen ist

[QUELLE: IEC 62304:2006, 3.12, modifiziert]

3.16

MEDIZINISCHES IT-NETZWERK

IT-Netzwerk, das mindestens ein MEDIZINPRODUKT enthält

3.17

MED-IT-RISIKOMANAGER

RISIKOMANAGER FÜR EIN MEDIZINISCHES IT-NETZWERK

Person, die für das Risikomanagement eines medizinischen IT-Netzwerks verantwortlich ist

3.18

BEDIENER

Person, die Geräte handhabt

[QUELLE: IEC 60601-1:2005, Definition 3.73]

3.19

PROZESS

Satz von in Wechselbeziehung oder Wechselwirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt

[QUELLE: ISO 14971:2007, 2.13]

Anmerkung 1 zum Begriff: Der Begriff „Tätigkeiten“ umfasst die Anwendung von Ressourcen.

3.20

RESTRISIKO

Risiko, das nach der Durchführung von Maßnahmen zur Risikobeherrschung verbleibt

[QUELLE: ISO 14971:2007, Definition 2.15]

3.21

VERANTWORTLICHKEITSVEREINBARUNG

ein oder mehrere Dokumente, die zusammen die Verantwortlichkeiten aller Beteiligten vollständig definieren

Anmerkung 1 zum Begriff: Diese Vereinbarung kann ein rechtskräftiges Dokument sein, z. B. ein Vertrag.

3.22

VERANTWORTLICHE ORGANISATION

Betreiber, der die Sachherrschaft über den Gebrauch und die Instandhaltung eines medizinischen IT-Netzwerks besitzt

Anmerkung 1 zum Begriff: Der verantwortliche Betreiber kann z. B. ein Krankenhaus, ein praktizierender Arzt oder eine Telemedizin-Organisation sein.

Anmerkung 2 zum Begriff: Angepasst aus IEC 60601-1:2005, Definition 3.101.

3.23

RISIKO

Kombination der Wahrscheinlichkeit des Auftretens eines SCHADENS und des Schweregrades dieses SCHADENS

[QUELLE: ISO 14971:2007, Definition 2.16]

3.24

RISIKOANALYSE

systematische Verwendung von verfügbaren Informationen zur Identifizierung von GEFÄHRDUNGEN und zur Einschätzung von RISIKEN

[QUELLE: ISO 14971:2007, 2.17]

3.25

RISIKOBEURTEILUNG

Rahmen-Prozess, der eine Risikoanalyse und eine Risikobewertung enthält

[QUELLE: ISO/IEC Guide 51:1999, Definition 3.12]

3.26

RISIKOBEHERRSCHUNG

PROZESS, in dem Entscheidungen getroffen und Maßnahmen implementiert werden, durch die RISIKEN auf festgelegte Bereiche verringert oder auf diesen gehalten werden

[QUELLE: ISO 14971:2007, 2.19]

3.27

RISIKOBEWERTUNG

PROZESS des Vergleichs des eingeschätzten RISIKOS mit gegebenen RISIKO-Kriterien, um die Akzeptanz des RISIKOS zu bestimmen

[QUELLE: ISO 14971:2007, 2.21]

3.28

RISIKOMANAGEMENT

systematische Anwendung von Managementstrategien, Verfahren und Praktiken auf die Aufgaben der Analyse, Bewertung, Beherrschung und Überwachung von RISIKEN

[QUELLE: ISO 14971:2007, 2.22]

3.29

RISIKOMANAGEMENT-AKTE

Satz von Aufzeichnungen und sonstigen Dokumenten, die beim RISIKOMANAGEMENT entstehen

[QUELLE: ISO 14971:2007, 2.23]

3.30

SICHERHEIT

Freiheit von unvertretbaren RISIKEN der physischen Verletzung oder der Schädigung der Gesundheit von Menschen oder der Schädigung von Eigentum oder der Umwelt

Anmerkung 1 zum Begriff: Angepasst aus ISO 14971:2007, 2.24.

3.31

OBERSTE LEITUNG

Person oder Personengruppe, welche die VERANTWORTLICHE ORGANISATION leitet und überwacht und die für das MEDIZINISCHE IT-NETZWERK auf oberster Ebene verantwortlich ist

Anmerkung 1 zum Begriff: Angepasst aus ISO 9000:2005, 3.2.7.

3.32

VERIFIZIERUNG

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Der Begriff „verifiziert“ wird benutzt, um den entsprechenden Zustand zu kennzeichnen.

Anmerkung 2 zum Begriff: Bestätigungen können aus Tätigkeiten bestehen, wie:

- Durchführen alternativer Berechnungen;
- Vergleichen einer neuen Entwicklungsspezifikation mit einer bereits bewährten Entwicklungsspezifikation;
- Durchführung von Prüfungen und Erbringen von Nachweisen;
- Bewertung von Dokumenten bevor sie herausgegeben werden.

Anmerkung 1 zum Begriff: Während der Entwicklung beschreibt die VERIFIZIERUNG den PROZESS der Ergebnisprüfung einer gegebenen Tätigkeit, um die Übereinstimmung mit den festgelegten Anforderungen dieser Tätigkeit zu bestätigen.

[QUELLE: ISO 14971:2007, 2.28, modifiziert – Ergänzung von Anmerkung 3 zum Begriff.]

4 Grundsätze

Es ist die Absicht die Struktur von 31000 widerzuspiegeln und dieser Abschnitt ist Teil jener Struktur. Das grundlegende Prinzip wird zu einem gewissen Maß in ISO 81001-1 enthalten sein, die NACH dieser Überarbeitung veröffentlicht wird. JWG7 wird berücksichtigen müssen, in welcher Form dies hier zu behandeln ist. Wird Text zur Verweisung auf die zukünftige ISO 81001-1 hinzugefügt? Wird der Abschnitt gelöscht? Wird grundlegender Text aus IEC 81001-1 hier hinzugefügt?

5 Struktur

5.1 Allgemeines

Aus IEC 80001-1:2010, Abschnitt 3.2.

Die Gesamtverantwortung für das RISIKOMANAGEMENT für ein MEDIZINISCHES IT-NETZWERK muss bei der VERANTWORTLICHEN ORGANISATION liegen.

Die VERANTWORTLICHE ORGANISATION muss der Eigentümer des PROZESSES für das RISIKOMANAGEMENT des MEDIZINISCHEN IT-NETZWERKS sein. Dieser Prozess erstreckt sich über die Planung, Entwicklung, Installation, Geräteverbindung, Konfiguration, Anwendung, Wartung und das Außerbetriebnehmen von Geräten.

Die Einhaltung wird durch Beurteilung der VERANTWORTLICHEN ORGANISATION geprüft.

5.2 Führung und Verpflichtung

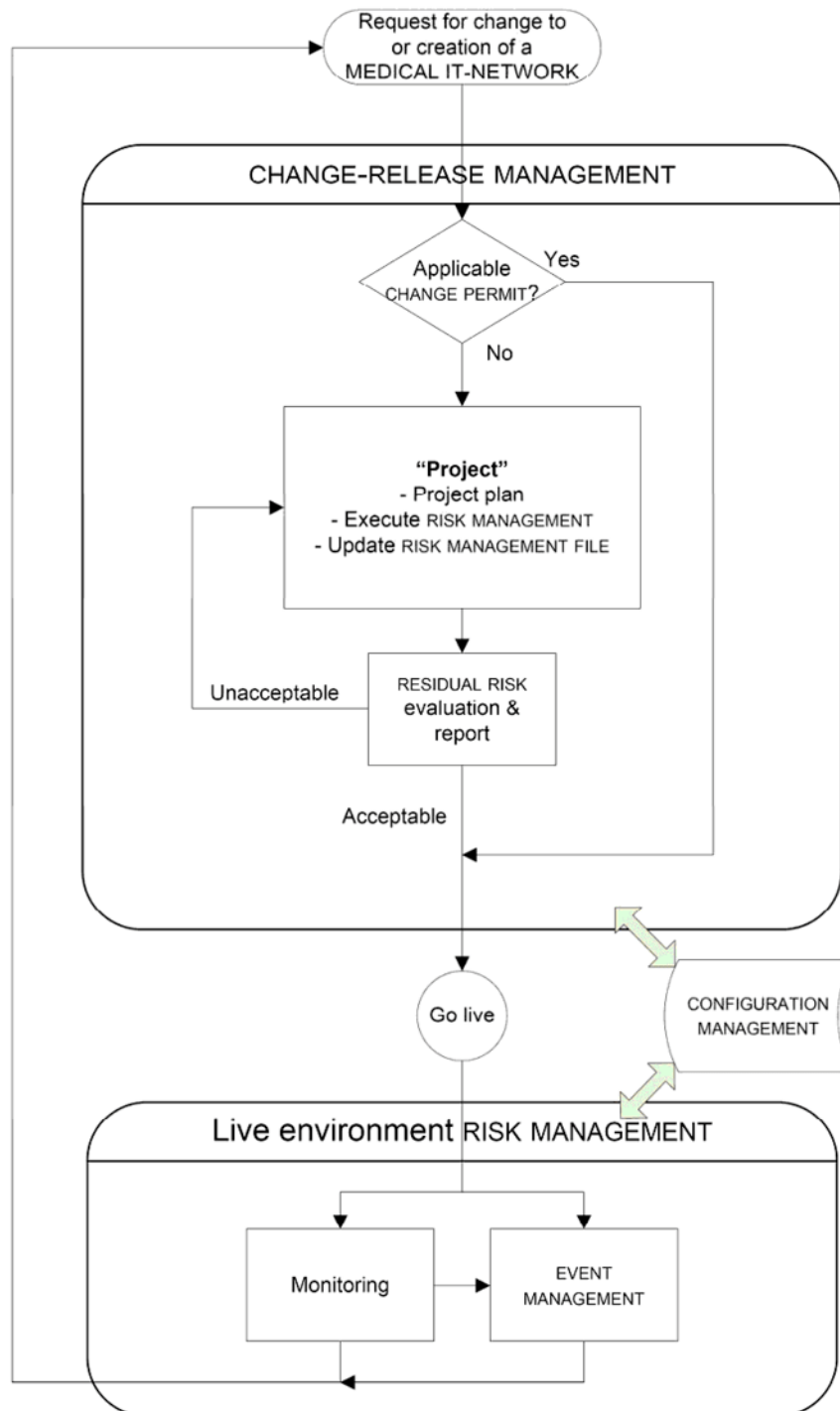
5.2.1 Allgemeines

Aus IEC 80001-1:2010, Abschnitt 4.1.

Die VERANTWORTLICHE ORGANISATION muss die SCHUTZZIELE während des gesamten Lebenszyklus des MEDIZINISCHEN IT-Netzwerks aufrechterhalten.

ANMERKUNG Der Lebenszyklus für MEDIZINISCHE IT-NETZWERKE einschließlich Risikomanagement ist in [Bild 1](#) dargestellt.

Die Einhaltung wird durch Einsichtnahme in die RISIKOMANAGEMENT-AKTE des MEDIZINISCHEN IT-NETZWERKS geprüft.



Englisch	Deutsch
Request for change to or creation of a MEDICAL IT-NETWORK	Antrag zur Änderung oder zur Errichtung eines MEDIZINISCHEN IT-NETZWERKS
CHANGE-RELEASE MANAGEMENT	ÄNDERUNGS- UND AUSLIEFERUNGSMANAGEMENT
Applicable CHANGE PERMIT	ÄNDERUNGSERLAUBNIS anwendbar?
Yes	Ja
No	Nein
Project	Projekt
Project plan	Projektplan
Execute RISK MANAGEMENT	Durchführung des RISIKOMANAGEMENTS
Update RISK MANAGEMENT FILE	RISIKOMANAGEMENT-AKTE auf den neuesten Stand bringen
Unacceptable	Unvertretbar

Englisch	Deutsch
Acceptable	Vertretbar
RESIDUAL RISK	RESTRISIKO
evaluation & report	Bewertung & Berichterstattung
Go live	Start des Echtbetriebs
CONFIGURATION MANAGEMENT	KONFIGURATIONS-MANAGEMENT
Live environment RISK MANAGEMENT	RISIKOMANAGEMENT im Echtbetrieb
Monitoring	Überwachung
EVENT MANAGEMENT	EREIGNIS-MANAGEMENT
NOTE A request for change can be a request to decommission a MEDICAL DEVICE or the MEDICAL IT-NETWORK. This decommissioning requires planning and RISK MANAGEMENT similar to other changes.	ANMERKUNG Eine Änderungsanforderung kann eine Anforderung sein, ein MEDIZINPRODUKT oder das MEDIZINISCHE IT-NETZWERK außer Betrieb zu nehmen. Diese Außerbetriebnahme erfordert, wie bei anderen Änderungen, eine Planung und ein RISIKOMANAGEMENT.

ANMERKUNG Eine Änderungsanforderung kann eine Anforderung sein, ein MEDIZINPRODUKT oder das MEDIZINISCHE IT-Netzwerk außer Betrieb zu nehmen. Diese Außerbetriebnahme erfordert, wie bei anderen Änderungen, eine Planung und ein RISIKOMANAGEMENT.

Bild 1 – Übersicht über den Lebenszyklus eines medizinischen IT-Netzwerks einschließlich RISIKOMANAGEMENT

5.2.2 Integration von Risikomanagement

Dies wird in IEC 80001-1:2010 nicht behandelt. JWG7 sollte prüfen, was hier (gegebenenfalls) aufgenommen werden sollte. Es ist eine Überarbeitung von ISO 31000 vorzuschlagen, um zu prüfen, ob Text oder Inhalt zweckmäßig ist und hier wirksam eingesetzt werden kann.

5.3 Gestaltung/Planung

Wird bezeichnet als „Gestaltung“ in ISO 31000 und als „Planung“ in Anhang SL.

5.3.1 Verstehen der Organisation und ihres Kontexts

Hier könnte Text hinzugefügt werden, der in IEC 80001-2-7 vorhanden ist, oder Text aus einem der anderen vier Technischen Berichte. Sofern dies zweckmäßig ist, könnte auch neuer Text verfasst werden.

5.3.2 Artikulieren der Risikomanagementverpflichtung

5.3.2.1 Verantwortung der OBERSTEN LEITUNG

Überschrift von IEC 80001-1:2010, Abschnitt 3.3.

Für das RISIKOMANAGEMENT eines MEDIZINISCHEN IT-Netzwerks muss die oberste Leitung:

- eine Richtlinie für das RISIKOMANAGEMENT bezüglich der Einbindung von MEDIZINPRODUKTEN erstellen;
- eine Richtlinie definieren, wie vertretbare RISIKEN bestimmt werden, wobei entsprechende internationale Normen und nationale oder regionale Vorschriften berücksichtigt werden müssen;
- die notwendigen Ressourcen bereitstellen;
- sicherstellen, dass qualifizierte Personen für das Management, für die Durchführung der Arbeit sowie für Tätigkeiten der Bewertung bestimmt werden;
- die Ergebnisse der RISIKOMANAGEMENT-Tätigkeiten einschließlich des EREIGNISMANAGEMENTS (siehe 6.7.2) in regelmäßigen Abständen überprüfen, um die weitere Eignung und Wirksamkeit des Risikomanagement-Prozesses sicherzustellen.

Die vorgenannten Punkte müssen in der RISIKOMANAGEMENT-AKTE für das MEDIZINISCHE IT-Netzwerk dokumentiert werden.

5.3.2.2 Med-IT-Risikomanager

Überschrift von IEC 80001-1:2010, Abschnitt 3.4.

Der MED-IT-RISIKOMANAGER muss für die Organisation des RISIKOMANAGEMENT-PROZESSES verantwortlich sein.

Der MED-IT-RISIKOMANAGER muss die Durchführung des RISIKOMANAGEMENT-PROZESSES überwachen, um die SCHUTZZIELE des MEDIZINISCHEN IT-NETZWERKS aufrechtzuerhalten.

Der MED-IT-RISIKOMANAGER muss für die folgenden Aspekte des RISIKOMANAGEMENTS von IT-NETZWERKEN, in die Medizinprodukte eingebunden sind, verantwortlich sein:

- a) Gesamtleitung des RISIKOMANAGEMENT-PROZESSES;
- b) Berichten über den RISIKOMANAGEMENT-PROZESS an die oberste Leitung;
- c) Aufbau und Aufrechterhaltung der erforderlichen Kommunikation zwischen den internen und externen Teilnehmern am RISIKOMANAGEMENT. Sofern zweckmäßig, dürfen solche Teilnehmer sein:
 - 1) Hersteller von MEDIZINPRODUKTEN;
 - 2) andere Lieferanten von IT-Geräten, Software und Dienstleistungen;
 - 3) interne IT-Abteilung und andere Abteilungen des Gebäudemanagements;
 - 4) klinische Anwender, und
 - 5) technischer Service für MEDIZINPRODUKTE (z. B. Biomedizintechnik).

Der MED-IT-RISIKOMANAGER muss verantwortlich für die Durchführung des RISIKOMANAGEMENT-PROZESSES SEIN. Dies umfasst unter anderem die Verantwortlichkeit für:

- d) Zusammenstellung aller RISIKORELEVANTEN Informationen zu den MEDIZINPRODUKTEN;
- e) Planung der Einbindung dieser MEDIZINPRODUKTE gemäß den jeweiligen Herstellerangaben und in Übereinstimmung mit den Richtlinien der VERANTWORTLICHEN ORGANISATION;
- f) Durchführung des RISIKOMANAGEMENT-PROZESSES, wenn ein MEDIZINPRODUKT in einem IT-NETZWERK hinzugefügt wird;
- g) Durchführung des RISIKOMANAGEMENT-PROZESSES, wenn ein eingebundenes MEDIZINPRODUKT oder das MEDIZINISCHE IT-NETZWERK verändert wird;
- h) Autorisierung für die Fortsetzung des Echtbetriebs nach einer Änderung am MEDIZINISCHEN IT-NETZWERK;
- i) Informieren der VERANTWORTLICHEN ORGANISATION über unvertretbare RISIKEN bezüglich des MEDIZINISCHEN IT-NETZWERKS und den damit verbundenen GEFÄHRDUNGEN, DIE SICH AUS JEGLICHEN Konfigurationsänderungen ergeben, und
- j) Überwachung aller Projekte oder Veränderungen in Bezug auf ein MEDIZINISCHES IT-NETZWERK, für das der MED-IT-RISIKOMANAGER verantwortlich ist.

Diese Aufgaben dürfen delegiert werden, aber der MED-IT-RISIKOMANAGER bleibt für die Sicherstellung einer ordnungsgemäßen Durchführung verantwortlich.

Die Einhaltung wird durch Beurteilung der VERANTWORTLICHEN ORGANISATION geprüft.

5.3.2.3 Medizinprodukte-Hersteller

Überschrift und Inhalt von IEC 80001-1:2010, Abschnitt 3.5. Der Rest dieses Abschnitts (der die Dokumentation behandelt) wurde im vorliegenden Dokument nach 6.7.2 verschoben.

In Übereinstimmung mit gültigen Vorschriften und den entsprechenden Normen muss jeder MEDIZINPRODUKTE-Hersteller in den BEGLEITPAPIEREN für die VERANTWORTLICHE ORGANISATION Angaben zur ZWECKBESTIMMUNG sowie Anweisungen für den sicheren und effektiven Gebrauch des MEDIZINPRODUKTES machen.

5.3.2.4 Anbieter sonstiger IT-Technologie

Überschrift und Inhalt von IEC 80001-1:2010, Abschnitt 3.6. Der Rest dieses Abschnitts (der die Dokumentation behandelt) wurde im vorliegenden Dokument nach 6.7.3 verschoben.

Anbieter sonstiger IT-Technologie (keine MEDIZINPRODUKTE) dürfen das Folgende bereitstellen:

- a) Infrastrukturkomponenten;
- b) Infrastrukturdienste;
- c) Clients, die keine MEDIZINPRODUKTE sind;
- d) Server;
- e) Anwendungssoftware, oder
- f) Middleware.

5.3.3 Zuweisung von organisatorischen Rollen, Rechenschaftspflichten, Verantwortlichkeiten und Befugnissen

Überschrift und Inhalt von IEC 80001-1:2010, Abschnitt 3.3.

Die OBERSTE LEITUNG muss einen MED-IT-RISIKOMANAGER zuweisen, der die erforderlichen Qualifikationen, Fachkenntnisse und Kompetenzen für die Anwendung eines Risikomanagements auf MEDIZINISCHE IT-NETZWERKE aufweist (siehe 5.3.2.2).

Die OBERSTE LEITUNG muss die Zusammenarbeit mit dem MED-IT-RISIKOMANAGER der benannten Personen sicherstellen, die für die nachfolgenden Aufgaben verantwortlich sind:

- a) das Sammeln, Analysieren, Bewerten und Speichern von Informationen, die für das RISIKOMANAGEMENT erforderlich sind;
- b) das Management von in IT-NETZWERKEN EINGEBUNDENEN MEDIZINPRODUKTEN während des Lebenszyklus;
- c) Überprüfen und Akzeptieren von RESTRIKTIKEN im Auftrag der OBERSTEN LEITUNG;
- d) Instandhaltung der MEDIZINISCHEN IT-Netzwerke;
- e) Auswahl und Beschaffung von MEDIZINPRODUKTEN.

Die OBERSTE LEITUNG muss sicherstellen, dass der RISIKOMANAGEMENTPROZESS für MEDIZINISCHE IT-NETZWERKE auch das für das Folgende zuständige Management umfasst:

- f) MEDIZINISCHE IT-Netzwerke;
 - g) allgemeine IT-Aktivitäten;
 - h) das Management von in IT-NETZWERKEN EINGEBUNDENEN MEDIZINPRODUKTEN während des Lebenszyklus;
- BEISPIEL 1 Biomedizinische Technik, radiologische Technik.

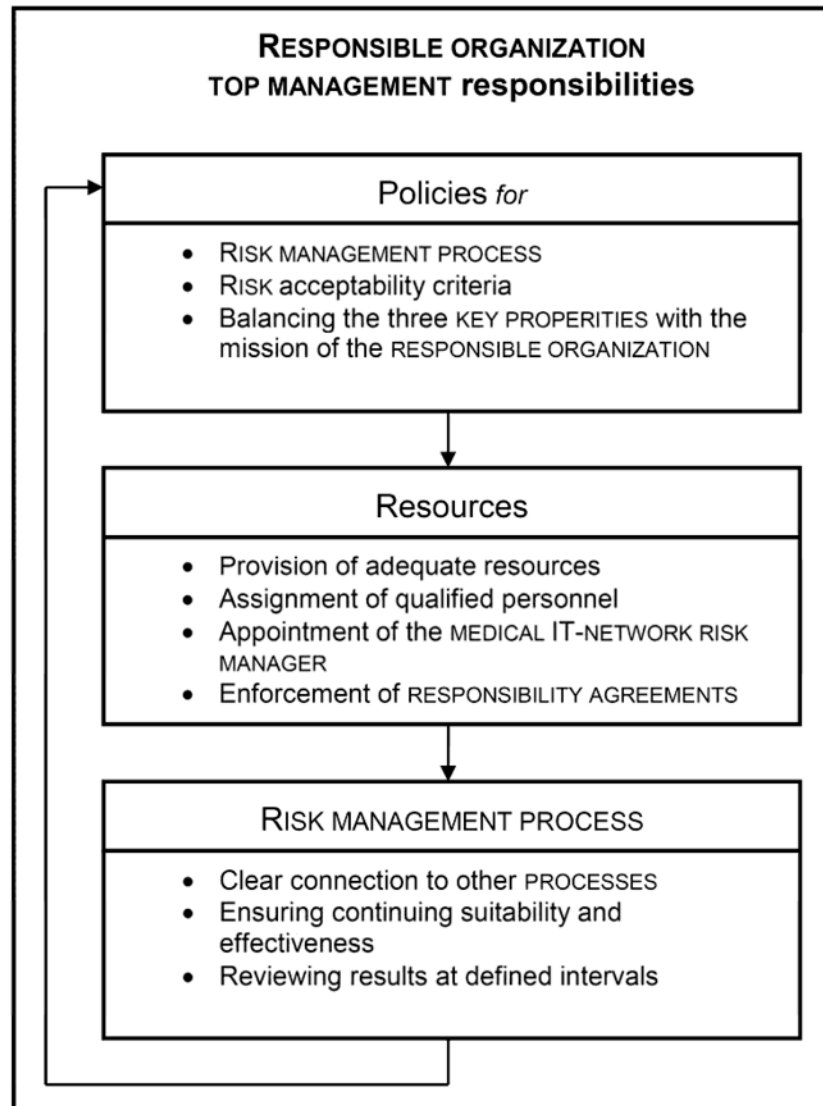
- i) die Benutzung von MEDIZINPRODUKTEN, und
- BEISPIEL 2 Erfahrene Benutzer aus klinischen Abteilungen.

- j) Instandhaltung und technische Unterstützung für MEDIZINPRODUKTE,
- BEISPIEL 3 Abteilung für Biomedizintechnik.

Die OBERSTE LEITUNG muss sicherstellen, dass:

- k) die gesamte Überwachung, der Betrieb, die Installation und Instandhaltung von MEDIZINISCHEN IT-NETZWERKEN während des gesamten Lebenszyklus gemäß dem Risikomanagement-Plan durchgeführt werden und dass sie den Ergebnissen des Risikomanagement-Prozesses für IT-Netzwerke folgen, unabhängig davon, wer diese Aufgaben durchführt;
- l) alle Parteien, die Aufgaben der Überwachung, des Betriebs, der Installation, des Service, der Fehlerdiagnose und Fehlerbehebung und der Instandhaltung von MEDIZINISCHEN IT-NETZWERKEN durchführen, in angemessener Weise über ihre Verantwortung entsprechend der vorliegenden Norm informiert werden. Dies schließt ihre Verantwortung für die Wirksamkeit von Maßnahmen der Risikobeherrschung ein.

ANMERKUNG Die Verantwortlichkeiten der OBERSTEN LEITUNG sind in Bild 2 dargestellt.



Englisch	Deutsch
RESPONSIBLE ORGANIZATION	VERANTWORTLICHE ORGANISATION
TOP MANAGEMENT responsibilities	Verantwortlichkeiten der OBERSTEN LEITUNG
Policies for	Richtlinien für
RISK MANAGEMENT PROCESS	RISIKOMANAGEMENTPROZESS
RISK acceptability criteria	Kriterien für die Vertretbarkeit von Risiken
Balancing the three KEY PROPERTIES with the mission of the RESPONSIBLE ORGANIZATION	Abwägung der drei SCHUTZZIELE hinsichtlich der Zielsetzung der VERANTWORTLICHEN ORGANISATION
Resources	Ressourcen
Provision of adequate resources	Bereitstellen angemessener Ressourcen
Assignment of qualified personnel	Zuweisung von qualifiziertem Personal
Appointment of the MEDICAL IT-NETWORK RISK MANAGER	Ernennung des RISIKOMANAGERS FÜR EIN MEDIZINISCHES IT-NETZWERK
Enforcement of RESPONSIBILITY AGREEMENTS	Abschluss von VERANTWORTLICHKEITSVEREINBARUNGEN
Clear connection to other PROCESSES	Eindeutige Verknüpfung mit anderen Prozessen
Ensuring continuing suitability and effectiveness	Sicherstellung der andauernden Wirksamkeit und Nachhaltigkeit
Reviewing results at defined intervals	Überprüfen von Ergebnissen in festgelegten Zeitintervallen

Bild 2 – Darstellung der Verantwortlichkeiten der OBERSTEN LEITUNG

Die Einhaltung wird durch Einsichtnahme in die RISIKOMANAGEMENT-AKTE des MEDIZINISCHEN IT-NETZWERKS geprüft.

5.3.4 Zuordnung von Ressourcen

Für diesen Abschnitt muss ein neuer Text verfasst werden.

5.3.5 Einrichten der Kommunikation und Konsultation

Für diesen Abschnitt muss ein neuer Text verfasst werden.

5.4 Implementierung

5.4.1 Richtlinie für das RISIKOMANAGEMENT

Überschrift gemäß 80001-1, Abschnitt 4.2.1.

Um das MEDIZINISCHEN IT-NETZWERK während seines Lebenszyklus zu unterstützen, muss die OBERSTE LEITUNG eine RISIKOMANAGEMENT-Richtlinie erstellen und dokumentieren, welche die Einbindung von MEDIZINPRODUKTEN in ein IT-Netzwerk regelt. Die RISIKOMANAGEMENT-Richtlinie muss das Folgende enthalten:

- a) Abwägung zwischen den drei Schutzziele und der Zielsetzung der verantwortlichen Organisation;
- b) ein Mittel zur Festlegung von Kriterien für die Risiko-Akzeptanz für jedes der Schutzziele; unter Berücksichtigung relevanter Internationaler Normen sowie nationaler oder regionaler Vorschriften;
- c) eine Beschreibung für oder Verweisung auf Prozesse, die für medizinische IT-Netzwerke gelten und mindestens das Folgende enthalten:
 - 1) EREIGNISMANAGEMENT;
 - 2) ÄNDERUNGS- UND AUSLIEFERUNGSMANAGEMENT;
 - 3) KONFIGURATIONSMANAGEMENT, UND
 - 4) Überwachung.

ANMERKUNG Tätigkeiten für den Lebenszyklus des medizinischen IT-Netzwerks können in einer IT-Service-Management-Richtlinie zusammengefasst werden (z. B. gemäß ISO 20000), vorausgesetzt, dass es einen klaren Bezug zur Risikomanagement-Richtlinie gibt.

Die Richtlinie muss so geschrieben sein, dass sie für alle Tätigkeiten des RISIKOMANAGEMENTS angewendet werden kann.

Die Einhaltung wird durch Einsichtnahme in die RISIKOMANAGEMENT-AKTE des MEDIZINISCHEN IT-NETZWERKS geprüft.

5.4.2 RISIKOMANAGEMENT-PROZESS

Überschrift und Inhalt von IEC 80001-1:2010, Abschnitt 4.2.

Der MED-IT-RISIKOMANAGER muss einen PROZESS festlegen und aufrechterhalten, um GEFÄHRDUNGEN zu identifizieren, die damit verbundenen RISIKEN einzuschätzen und zu bewerten, diese RISIKEN zu beherrschen und die Wirksamkeit der Maßnahmen zur RISIKOBEHERRSCHUNG zu überwachen, und dabei die vorgesehene Verwendung des MEDIZINISCHEN IT-NETZWERKS berücksichtigen.

ANMERKUNG Nachträgliche Änderungen am MEDIZINISCHEN IT-NETZWERK können neue RISIKEN verursachen und ergänzende Untersuchungen erforderlich machen.

Die Einhaltung wird durch Einsichtnahme in die Risikomanagement-Akte des medizinischen IT-Netzwerks geprüft.

5.4.3 Risikomanagement-Planung

Die Überschrift von **IEC 80001-1:2010, Abschnitt 4.3**, die in jenem Dokument „Planung und Dokumentation des Risikomanagements“ lautet, wurde angepasst – In der vorliegenden Überarbeitung enthält Abschnitt 5.4.3 Text aus Abschnitt 4.3.1 und 4.3.21 des alten Dokuments.

Die VERANTWORTLICHE ORGANISATION muss das RISIKOMANAGEMENT für das MEDIZINISCHE IT-NETZWERK durch Bereitstellung folgender Unterlagen planen:

- a) Beschreibung der risikorelevanten Elemente;

ANMERKUNG 1 Siehe 5.4.4 für eine Beschreibung und Beispiele von risikorelevanten Elementen.

- b) Dokumentation des IT-Netzwerks, und
- c) einen Risikomanagement-Plan für das medizinische IT-Netzwerk.

ANMERKUNG 2 Die Überprüfung und Dokumentation der Struktur des Netzwerks ist von grundlegender Bedeutung, um die erforderliche Information für die RISIKOANALYSE und RISIKOBEWERTUNG zu liefern.

Wegen der Eigenschaften von IT-NETZWERKEN sollten sowohl der Istzustand des IT-NETZWERKS als auch geplante Änderungen betrachtet werden.

Die Errichtung von neuen MEDIZINISCHEN IT-NETZWERKEN und Änderungen an bestehenden MEDIZINISCHEN IT-NETZWERKEN, die nicht durch dokumentierte ÄNDERUNGSERLAUBNISSE abgedeckt sind, müssen in Form von Projekten umgesetzt werden.

ANMERKUNG 3 Ein MEDIZINISCHES IT-NETZWERK kann mehrere gleichzeitige oder sequenzielle Projekte haben.

ANMERKUNG 4 Siehe auch 5.4.4 für Projekte von MEDIZINISCHEN IT-NETZWERKEN und 6.5.8.2 für die Änderungserlaubnis.

Die Einhaltung wird durch Einsichtnahme in die Risikomanagement-Akte des medizinischen IT-Netzwerks geprüft.

5.4.4 Beschreibung der risikorelevanten Elemente

Die VERANTWORTLICHE ORGANISATION muss eine Liste derjenigen Elemente von IT-NETZWERKEN erstellen, die mit MEDIZINPRODUKTEN verbunden sind. Typische Elemente sind unter anderem Hardware, Software und Daten, die für die ZWECKBESTIMMUNG des MEDIZINPRODUKTES und die vorgesehene Verwendung des MEDIZINISCHEN IT-NETZWERKS wichtig sind. Die Liste der Elemente darf z. B. das Folgende enthalten:

- a) bestimmte Komponenten des MEDIZINISCHEN IT-NETZWERKS und alle eingebundenen MEDIZINPRODUKTE und andere Geräte (z. B. Modalitäten der Bildgebung, Netzwerkkomponenten) der IT-Infrastruktur;
- b) Betriebsmerkmale der IT-Infrastruktur des MEDIZINISCHEN IT-Netzwerks (z. B. Leistungsmerkmale wie die Bandbreite);
- c) Informationen zum KONFIGURATIONSMANAGEMENT;
- d) medizinische Anwendungssoftware;
- e) Daten über die Konfiguration von Hardware und Software;
- f) Charakterisierung von identifizierbaren Patientendaten, die sich im MEDIZINISCHEN IT-NETZWERK befinden oder die vom eingebundenen Medizinprodukt benutzt werden, einschließlich Art, Umfang und Sensibilität;
- g) Informationen zu medizinischen Behandlungsverfahren, einschließlich der Vorgeschichte der Anwendung und Einzelheiten zu BEDIENERN/Anwendern.
- h) eine Sicherheitsbeschreibung und andere Unterlagen, die für die Betrachtung der gesamten SICHERHEITSRISIKEN des Systems relevant sind (für den Fall, dass die „Security“ ein Aspekt der SICHERHEIT ist).

Die Einhaltung wird durch Einsichtnahme in die Risikomanagement-Akte des medizinischen IT-Netzwerks geprüft.

5.5 Risikobewertung

Für diesen Abschnitt muss ein neuer Text verfasst werden.

5.6 Verbesserung

Für diesen Abschnitt muss ein neuer Text verfasst werden.

6 Prozess

6.1 Allgemeines

Von IEC 80001-1:2010, Abschnitt 4.4.

Dieser Abschnitt beschreibt RISIKOMANAGEMENT-PROZESSE, die sowohl die Durchführung eines Projektes innerhalb eines MEDIZINISCHEN IT-NETZWERKS als auch die Entscheidung zur Aufnahme des Echtbetriebs einer jeden einzelnen Änderung unterstützen.

Die RISIKOMANAGEMENT-Tätigkeiten der RISIKOANALYSE, der RISIKOBEWERTUNG, der RISIKOBEHERRSCHUNG, der Bewertung und der Berichterstattung des RESTRISIKOS und der Genehmigung müssen dokumentiert sein. Diese Dokumentationen dürfen sowohl Bestandteil des RISIKOMANAGEMENT-Plans als auch ein getrenntes Dokument in der RISIKOMANAGEMENT-AKTE des MEDIZINISCHEN IT-NETZWERKS sein. Aktionspläne, die als Folge der RISIKOBEURTEILUNG aufgestellt werden, müssen den PROZESS des ÄNDERUNGS- UND AUSLIEFERUNGSMANAGEMENTS einhalten.

ANMERKUNG Um zu verhindern, dass Maßnahmen der RISIKOBEHERRSCHUNG für ein bestimmtes Projekt oder eine bestimmte Änderung mit bestehenden Maßnahmen der RISIKOBEHERRSCHUNG für das MEDIZINISCHE IT-Netzwerk oder mit Maßnahmen der RISIKOBEHERRSCHUNG, die von einem gleichzeitig laufenden Projekt vorgeschlagen wurden, in Konflikt stehen, darf es nur einen gültigen Dokumentensatz zum RISIKOMANAGEMENT je MEDIZINISCHEM IT-NETZWERK geben.

Die Einhaltung wird durch Einsichtnahme in die Risikomanagement-Akte des medizinischen IT-Netzwerks geprüft.

6.2 Kommunikation und Konsultation

Abschnitt 6.2 wurde aus der Struktur von ISO/DIS 31001 übernommen. Sofern maßgeblich, werden Inhalte für diesen Abschnitt entwickelt. Anderenfalls darf der Abschnitt gelöscht werden.

6.3 Einrichten des Kontextes

Abschnitt 6.3 (6.3.1 bis 6.3.4) wurde aus der Struktur von ISO/DIS 31001 übernommen. Sofern maßgeblich, werden Inhalte für diesen Abschnitt entwickelt. Anderenfalls darf der Abschnitt gelöscht werden.

6.3.1 Allgemeines

6.3.2 Festlegung von Zweck und Anwendungsbereich des Prozesses

6.3.3 Interner und externer Kontext

6.3.4 Festlegung von Risikokriterien

6.4 RISIKOBEURTEILUNG

Abschnitt 6.4.1 bis 6.4.3 wurden aus der Struktur von ISO/DIS 31001 übernommen. Sofern maßgeblich, werden Inhalte für diese Abschnitte entwickelt. Anderenfalls darf der Abschnitt gelöscht werden.

6.4.1 Allgemeines

6.4.2 Risikoidentifikation

6.4.3 RISIKOANALYSE

Von IEC 80001-1:2010, Abschnitt 4.2.

Die VERANTWORTLICHE ORGANISATION muss GEFÄHRDUNGEN identifizieren, die mit einer gewissen Wahrscheinlichkeit vom MEDIZINISCHEN IT-NETZWERK ausgehen können.

Die VERANTWORTLICHE ORGANISATION muss unter Berücksichtigung verfügbarer Informationen oder Daten für jede identifizierte GEFÄHRDUNG die entsprechenden RISIKEN abschätzen.

ANMERKUNG Die zu analysierenden Risiken erstrecken sich über die gesamte Nutzungsdauer des MEDIZINISCHEN IT-Netzwerks, insbesondere auf die Implementierung von Änderungen sowie den Routinebetrieb.

Wenn die Wahrscheinlichkeit des Auftretens eines SCHADENS nicht abgeschätzt werden kann, müssen die möglichen Folgen zur Benutzung bei der RISIKOBEWERTUNG und bei der RISIKOBEHERRSCHUNG aufgelistet werden.

Die Ergebnisse dieser Tätigkeiten müssen in der RISIKOMANAGEMENT-AKTE des MEDIZINISCHEN IT-NETZWERKS dokumentiert werden.

Die Einhaltung wird durch Einsichtnahme in die Risikomanagement-Akte des medizinischen IT-Netzwerks geprüft.

6.4.4 RISIKOBEWERTUNG

Von IEC 80001-1:2010, Abschnitt 4.4.3.

Für jede identifizierte GEFÄHRDUNG muss die VERANTWORTLICHE ORGANISATION unter Benutzung der im RISIKOMANAGEMENT-Plan festgelegten Kriterien entscheiden, ob:

- das (die) abgeschätzte(n) Risiko (Risiken) so gering ist (sind), dass eine Reduzierung des Risikos nicht weiterverfolgt werden muss. In diesem Fall muss die Begründung für diese Entscheidung in der Risikomanagement-Akte des medizinischen IT-Netzwerks dokumentiert werden.
- das (die) abgeschätzte(n) Risiko (Risiken) unvertretbar ist (sind). In diesem Fall müssen Maßnahmen der Risikobeherrschung gemäß 6.5 umgesetzt werden.

Die Einhaltung wird durch Einsichtnahme in die Risikomanagement-Akte des medizinischen IT-Netzwerks geprüft.