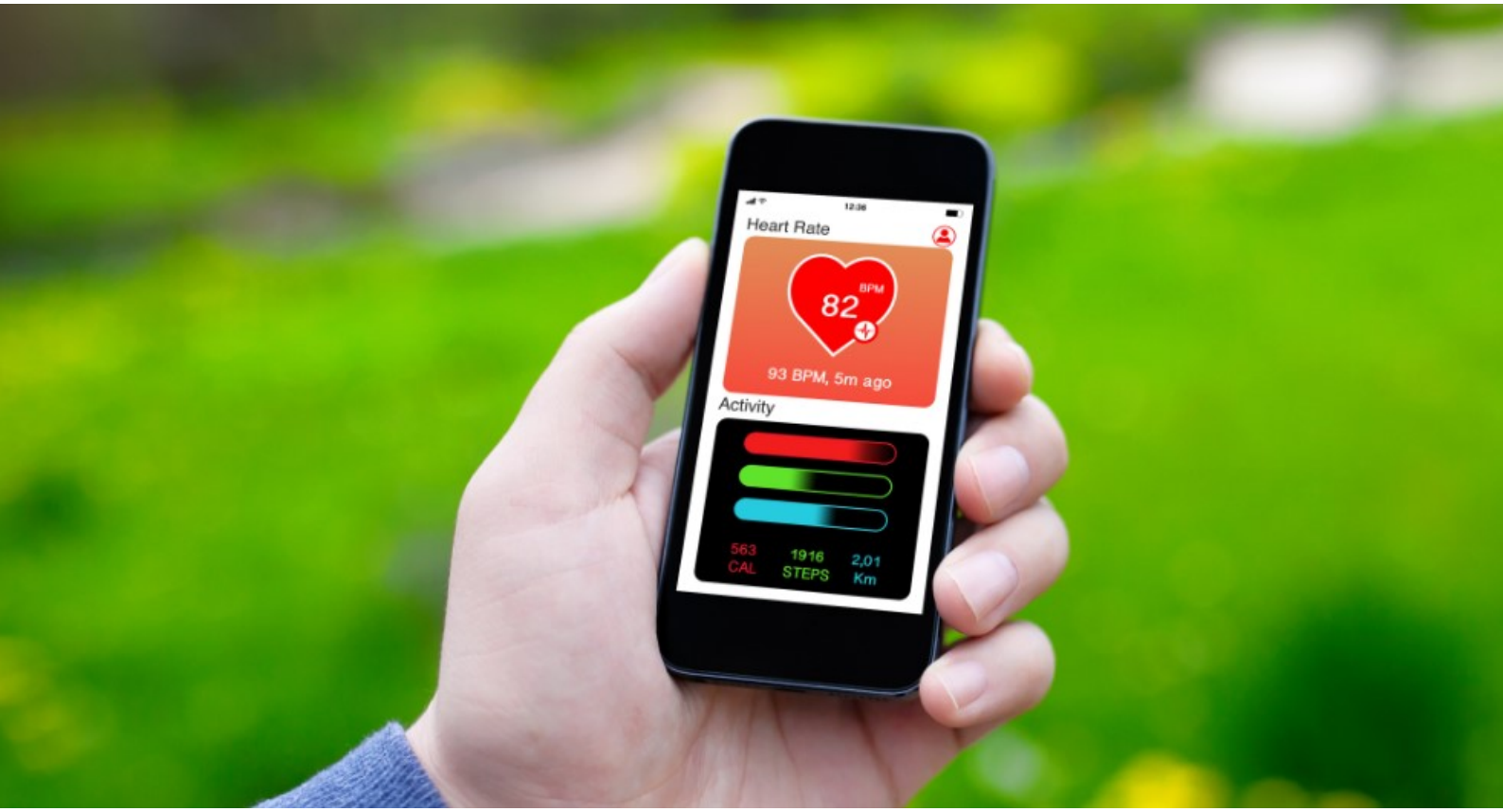
Integrierte Managementsysteme

Integration der Informationssicherheit in ein Qualitätsmanagementsystem für Medizinprodukte

mit besonderer Berücksichtigung der Anforderungen nach DiGAV



Leitfaden

Version 1.0

Stand Januar 2022

Dieser Leitfaden bezieht sich auf die:

DIN EN ISO 13485:2021-12

Medizinprodukte – Qualitätsmanagementsysteme - Anforderungen für regulatorische Zwecke

DIN EN ISO/IEC 27001:2017-06

Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen

DIN EN ISO 27799:2016-12

Medizinische Informatik - Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002

Er ist nicht dafür bestimmt, diese zu ersetzen und erhebt keinen Anspruch auf Vollständigkeit. Er ist im Internet abrufbar unter:

https://www.gut-cert.de/service/leitfaden_ISMSmed

Text GUTcert, Design in Anlehnung an AFNOR groupe.
Anregungen zu Verbesserungen oder Hinweise auf Fehler sind ausdrücklich erwünscht!
Bitten senden Sie diese an info@gut-cert.de.

Andreas Lemke und das ISMS-Team der GUTcert:

GUT Certifizierungsgesellschaft für
Managementsysteme mbH
Umweltgutachter

Eichenstr. 3b
12435 Berlin
Telefon: +49 30 2332021-0
Email: info@gut-cert.de
Die GUTcert ist Mitglied der

11, rue Francis de Pressensé
F - 93571 La Plaine Saint-Denis Cedex
Frankreich
www.afnor.org

Vorwort

Sehr geehrte Leserin, sehr geehrter Leser,

mit dem Digitale-Versorgung-Gesetz (DVG) wurde das Sozialgesetzbuch V so geändert, dass eine neue Gruppe von Medizinprodukten, die „digitalen Gesundheitsanwendungen" (DiGA), erstattungsfähig wurden. Mit der Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (DiGAV) wurden die Vorgaben für die DiGA konkretisiert.

Zuletzt wurde diese Verordnung mit der ersten Verordnung zur Änderung der Digitale Gesundheitsanwendungen-Verordnung vom 22. September 2021 geändert.

Für das ISMS sind folgende Änderungen relevant:

„Das Bundesinstitut für Arzneimittel und Medizinprodukte kann zum Nachweis der Erfüllung der Anforderungen an die Informationssicherheit spätestens ab dem 1. April 2022 zudem die Vorlage eines geeigneten Zertifikats oder Nachweises über ein Informationssicherheitsmanagement verlangen.

Ab dem 1. Januar 2023 ist die Erfüllung der Anforderungen an die Datensicherheit durch ein Zertifikat des Bundesamts für Sicherheit in der Informationstechnik nach § 139e […] nachzuweisen." Dies gilt auch für bereits gelistete Hersteller.

Mit dem hier vorgestellten Leitfaden möchten wir allen Anbietern von DiGA ein Werkzeug an die Hand geben, mit dem diese ihr Managementsystem nach EN ISO 13485 um die Komponenten des Informationssicherheitsmanagements schrittweise erweitern können. Da ein ISMS nach ISO/IEC 27001 sehr flexibel ist, lassen sich damit auch die Themenbereiche des Datenschutzes abbilden – deren Nachweis dann durch ein Zertifikat nach § 139e zum 1. April 2023 zu erbringen ist.

So erreichen Sie in drei Phasen ein vollständiges integriertes Managementsystem aus EN ISO 13485 QMS und ISO/IEC 27001 ISMS – in Phase IV geht es um die Zertifizierung.

Mein Tipp: Lesen Sie diesen Leitfaden einmal quer, um den Inhalt als Ganzes zu erfassen und gehen Sie dann in Ruhe Schritt für Schritt Ihren eigenen Weg zur Einführung. Je nach Organisationszweck, -größe, -betroffenheit oder -ziel können Sie in jeder einzelnen Phase Halt machen und verweilen oder die dazugehörigen Schritte zügig hintereinander und teilweise parallel nehmen.

Wenn Sie bei der vierten Phase angekommen sind, haben Sie „ganz nebenbei" und sicher die Anforderungen der EN ISO/IEC 27001 umgesetzt und können sich jederzeit zertifizieren lassen. Das wäre dann der letzte Schritt, um die Informationssicherheit kontinuierlich zu verbessern und den Datenschutz erfolgreich zu managen.

Der sprachlichen Gleichstellung tragen wir um der besseren Lesbarkeit Willen Rechnung, indem wir männliche und weibliche Wortfassungen willkürlich mischen. Es sind jedoch ausdrücklich alle Geschlechter angesprochen.

Andreas Lemke

Leiter der Zertifizierungsstelle

Inhalt

Einleitung

Dieser Leitfaden entstand im Rahmen des vom BMWi geförderten Forschungsprojektes AIQNET[1], bei dem die Berlin Cert als Partner beteiligt war. Teilprojektziel war zunächst eine Checkliste und dann ein Leitfaden, der die Kombination von QM-Managementsystemen zu Integrierten Managementsystemen beschreibt.

Adressaten des Leitfadens sind insbesondere solche Hersteller von Medizinprodukten, die digitale Gesundheitsanwendungen anbieten oder anbieten wollen. Speziell diese Zielgruppe ist gesetzlich gehalten, bis zum 01.04.2022 ein zertifiziertes ISMS gegenüber dem Bundesinstitut für Arzneimittel und Medizinprodukte vorweisen zu können. Der Leitfaden wendet sich an Hersteller von Software, die als Medizinprodukt zugelassen ist oder zugelassen werden soll.

Die Anwenderin des Leitfadens ist mit der EN ISO 13485 vertraut und hat ein QMS nach EN ISO 13485 etabliert, das bereits zertifiziert sein kann, aber nicht muss. Ebenso hat der Hersteller die Anforderungen nach MDR, ggf. MDD umgesetzt. Als Hersteller von Software ist der Anwender des Leitfadens mit der Begrifflichkeit der Informationstechnik vertraut. Er möchte aber den Aufbau getrennter Managementsysteme vermeiden und strebt im Idealfall eine kombinierte Zertifizierung nach EN ISO 13485 und ISO/IEC 27001 an.

Die Einführung des ISMS haben wir in drei Phasen unterteilt.

In der ersten Phase muss zunächst – basierend auf den externen Anforderungen – der Anwendungsbereich für das ISMS festgelegt werden. Auch die Aufbauorganisation für das ISMS entsteht in Phase I.

In der zweiten Phase werden dann alle Anforderungen der ISO/IEC 27001 in das Managementsystem integriert. Die erste Risikobewertung wird durchgeführt und die daraus abgeleiteten Maßnahmen werden umgesetzt.

In der dritten Phase startet dann der Verbesserungszyklus des ISMS, im Regelbetrieb muss sich die Wirksamkeit der festgelegten Prozesse erweisen.

Als vierte Phase haben wir dann die Vorgehensweise zur Zertifizierung des ISMS beschrieben.

Wenn die Implementationsschritte durchlaufen werden, entsteht neben dem QMS für die EN ISO 13485 das ISMS für die ISO/IEC 27001. Idealerweise werden beide im gleichen System (Handbuch) geführt. Die Synergieeffekte werden sich nach kurzer Zeit einstellen: Spätestens mit dem Managementbericht entsteht ein gemeinsames Dokument, das z. B. den Erreichungsgrad der Ziele des QMS und ISMS aufzeigt. Vertraulichkeit, Integrität und Verfügbarkeit der Werte (die ISO/IEC 27001 spricht hier von Assets), deren Qualität das QMS überwacht, werden durch das ISMS geschützt.

Zu den Assets gehören dabei die zu schützenden Informationen selber sowie alle anderen Einrichtungen und Hilfsmittel, die mit diesen Informationen im Zusammenhang stehen – bezogen auf IT also sowohl Hardware als auch Software und Daten.

Begleitend haben wir eine Checkliste erstellt. Sie ist als Hilfsmittel konzipiert, um die Komponenten der Informationssicherheit eines integrierten Managementsystems aus EN ISO 13485 und ISO/IEC 27001 auf Vollständigkeit zu prüfen. Die Fragen beinhalten neben den allgemeinen Anforderungen an das ISMS auch alle Maßnahmen, die nach dem verbindlichen Anhang der ISO/IEC 27001 implementiert werden müssen. Außerdem sind dort weitere Anforderungen durch die ISO 27799 sowie andere Normen und gesetzliche Regelungen berücksichtigt.

---

1 AIQNET ist das Medical Data Ecosystem eines Konsortiums, das unter dem Projekt-Akronym „KIKS“ zu den Gewinnern des KI-Innovationswettwettbewerb der Bundesregierung im Jahre 2019 gehört. Der Verbund besteht aus 16 international etablierten Unternehmen der Medizintechnik und der Gesundheitsversorgung.

Phase I

In der ersten Phase werden Ausmaß und Grenzen des ISMS definiert und die zu erfüllenden Anforderungen an das ISMS ermittelt. Außerdem wird die Aufbauorganisation für das ISMS bestimmt und es werden bestehende Prozesse identifiziert, die für ein ISMS relevant sind. Nach Abschluss der Phase ist den Nutzerinnen bekannt, an welchen Stellen unterstützende Strukturen für das ISMS implementiert werden müssen.

Anwendungsbereich des ISMS festlegen (Abschnitt 4.3 nach HLS)

Wie bei der EN ISO 13485 (und auch allen anderen Managementsystemen) muss die Organisation den Geltungsbereich des Informationssicherheitsmanagementsystems bestimmen.

Allerdings sind in diesem Fall einige Besonderheiten zu beachten, die diese Festlegung etwas komplexer werden lassen. Während man z. B. bei der EN ISO 13485 den Geltungsbereich des QMS auf bestimmte Produkte oder Produktgruppen und die für deren Herstellung erforderlichen Prozesse beschränken kann, müssen für das ISMS die zu schützenden Informationen und die für deren Verarbeitung erforderlichen Assets betrachtet werden.

In das ISMS und dessen Risikobewertung müssen dann auch alle Schnittstellen einbezogen werden, die einen Austausch von Informationen von Assets innerhalb des Geltungsbereichs des ISMS mit externen Einrichtungen ermöglichen.

Veranschaulicht wird dies am Beispiel eines Produktionsplanungs- und steuerungssystems (PPS): In ein QMS können hierbei neben der Gesamtfunktion des PPS nur die für die einbezogenen Produkte relevanten Materialströme betrachtet werden. Im Fall eines ISMS wäre es aber praktisch nicht möglich, eine Schnittstelle zwischen den produktbezogenen Daten für Erzeugnisse innerhalb und außerhalb des gewählten Geltungsbereichs zu definieren und zu überwachen. Das PPS müsste demzufolge immer vollständig mit allen Daten in das ISMS eingeschlossen werden. Dasselbe gilt auch für die gesamte IT-Infrastruktur und viele andere IT-Systeme, z. B. Backupsysteme, das active directory oder VM-Hosts.

Suchen Sie dann Assets, die den Informationsfluss von und zu diesen Systemen steuern und überwachen (üblicherweise Firewalls, Webserver oder ähnliche Assets). Das sind dann mögliche Schnittstellen der IT im Geltungsbereich Ihres ISMS nach außen.

Besonders zu beachten sind dabei auch externe (oder ggf. sogar interne) Dienstleister, auch dort müssen Schnittstellen für den Fluss von Assets betrachtet werden. Das ist z. B. für Cloudbetreiber noch relativ einfach, dort gibt es i.d.R. einen klar definierten Vertrag mit gegenseitigen Rechten und Pflichten.

Tipp:

Stellen Sie zuerst in einem Netzstrukturplan alle wesentlichen IT-Assets und deren Verbindungen (auch nach außen) dar.

Überlegen Sie sich dann, mit welchen dieser Systeme schützenswerte Informationen mit Bezug zu DiGA verarbeitet werden. Denken Sie dabei aber auch an Daten zu Mitarbeitern und Kundinnen (und natürlich an die Daten zum ISMS selbst).

Wenn aber z. B. auch Softwareentwicklung extern vergeben wird, ist die Überprüfung der Einhaltung der ISO/IEC 27001 schon deutlich komplexer. Dazu gehört dann nicht nur die Validierung der erstellten Software selbst. Auch weitere Vorgaben für die Informationssicherheit in der Entwicklung müssen mit dem Lieferanten vereinbart und deren Einhaltung auch beim Lieferanten überprüft werden. Da das in der Praxis nur mit großem Aufwand durchführbar ist, wird üblicherweise dann auch vom Lieferanten eine Zertifizierung nach ISO/IEC 27001 verlangt. Nur wenn deren Geltungsbereich auch die beauftragte Leistung umfasst, kann die Organisation selbst von Lieferantenaudits absehen.

Der Anwendungsbereich muss als dokumentierte Information verfügbar sein. Bei einem integrierten Managementsystem ist es nicht vorteilhaft, wenn die Anwendungsbereiche der die Integration betreffenden Normen unterschiedlich sind. Mithin: der Anwendungsbereich kann gemeinsam festgelegt werden.

An geeigneter Stelle im QMS (Verantwortung der Leitung) sind folgende Ergänzungen vorzunehmen:

Kontext der Organisation

Wie die ISO 9001:2015, so fordert auch die ISO/IEC 27001 von der Organisation, dass der interne und externe Kontext bestimmt wird und Themen benannt werden, die einen Einfluss auf die Fähigkeit der Organisation haben, die beabsichtigten Ergebnisse zu erreichen. Ferner müssen interessierte Parteien ermittelt werden, die für das ISMS relevant sind, auch müssen deren Anforderungen an das ISMS bestimmt werden.

Tipp:

Zu den interessierten Parteien gehören nicht nur die, die man **gerne** beteiligt. Entscheidend für die Auswahl ist, ob diese Parteien ein Interesse an den Ergebnissen des ISMS haben können. Diese Auswahl sollte also möglichst vollständig sein.

Es wird dann zu vielen Konflikten zwischen den Erwartungen der vielen verschiedenen Parteien kommen: Diese Erwartungen müssen bezüglich ihrer Relevanz bewertet werden – und nur die relevanten Anforderungen werden dann in der Weiterentwicklung des ISMS berücksichtigt.

Politik und Ziele

Die Qualitätspolitik der Organisation muss um die Informationssicherheitspolitik ergänzt werden. In diesem Zusammenhang werden auch die Informationssicherheitsziele genannt, welche für die relevanten Funktionen und Ebenen festgelegt werden. Diese müssen anwendbare Informationssicherheitsanforderungen sowie die Ergebnisse der Risikobeurteilung und Risikobehandlung berücksichtigen. Dieser Aspekt geht über die Anforderungen an die Ziele des QMS hinaus.

Die Politik muss Verpflichtungen enthalten, nach denen als zutreffend bewertete Anforderungen auch erfüllt werden und das ISMS fortlaufend verbessert wird (KVP). Wenn die Q-Politik und die ISMS-Politik gemeinsam verwaltet werden, so ist auch sichergestellt, dass diese dokumentiert sind und innerhalb der Organisation bekannt gemacht werden. Die ISMS-Politik muss für interessierte Parteien (soweit angemessen) verfügbar sein.

Rollen, Verantwortlichkeiten und Befugnisse

Für das ISMS muss in diesem Abschnitt des QMS ergänzt werden, dass eine Verantwortlichkeit und Befugnisse zugewiesen werden, die sicherstellen, dass:

- das ISMS die Anforderungen der Norm ISO/IEC 27001 erfüllt und
- an die oberste Leitung über die Leistung des ISMS berichtet wird

Wie auch in anderen Managementsystemen muss auch für das ISMS eine Vertreterin der obersten Leitung benannt werden, die die Gesamtverantwortung für das ISMS übernimmt. Üblicherweise wird dann die operative Arbeit im ISMS an einen ISMS-Beauftragten delegiert, der z. B. dann auch die von der Norm geforderte Berichtspflicht an das Top-Management übernimmt.

Andererseits haben sich bis heute für die IT-Organisation von Organisationen einige weitere Begriffe für bestimmte Funktionen eingebürgert:

- **Chief Information Officer (CIO):** die Gesamtverantwortliche für den Betrieb der IT-Infrastruktur, alternativ werden für diese Stelle auch die Begriffe „IT-Leitung“ oder „IT-Vorstand“ benutzt
- **Chief Information Security Officer (CISO):** der Gesamtverantwortliche für das Risikomanagement aller Informationswerte (Assets) einer Organisation; diese Funktion entspricht am ehesten dem ISMS-Beauftragten, hat aber eine größere inhaltliche Verantwortung. Für Verantwortliche in einzelnen Bereichen findet man auch die Bezeichnung „Information Security Officer“ (ISO)
- **Datenschutzbeauftragte (DSB):** das sind gemäß DS-GVO bzw. B-DSG geforderte Beauftragte, die intern v.a. eine beratende Aufgabe zur Umsetzung der Anforderungen der DS-GVO haben; viele Organisationen benennen eine DSB aber auch auf freiwilliger Basis

Wichtig für die Zuweisung der jeweiligen Verantwortungen ist dabei das Prinzip der Aufgabentrennung. Danach müssen in Konflikt stehende Aufgaben und Verantwortungen getrennt werden, um Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.

Das bedeutet, dass z. B. die Rollen einer Administratorin und eines (C)ISO zu trennen sind, da eine Aufgabe des CISO darin besteht, die Umsetzung der Sicherheitsanforderungen an IT-Systeme durch deren Administratorinnen zu überprüfen. Ähnliches gilt auch für DSB.

Phase II

Die unterstützenden Strukturen für das ISMS werden im QMS implementiert, die Risiken für die Assets werden identifiziert und Behandlungsmaßnahmen festgelegt (sog. controls). Es erfolgt eine erste Bewertung der vorhandenen Risiken für die Informationssicherheit. Mit Abschluss der Phase II ist die Integration des ISMS in das QMS abgeschlossen.

Dokumentierte Information

Grundsätzlich sind die Forderungen der Normelemente der EN ISO 13485 und der ISO/IEC 27001 zu diesem Abschnitt sehr ähnlich. Zur Prüfung, ob die bisherigen Regelungen im QMS ausreichen, wird auf den Abschnitt 7.5 der ISO/IEC 27001 verwiesen.

Tipp:

Gerade im Bereich der medizinischen IT ändern sich nicht nur die technischen Aspekte in einem teilweise atemberaubenden Tempo. Auch der Gesetzgeber passt seine Anforderungen in ähnlichen Abständen an. Etablieren Sie deshalb ein Monitoring, welches für Sie Änderungen von relevanten Gesetzen und Verordnungen mindestens quartalsweise ausgibt.

Führung und Verpflichtung

Wie auch bei dem vorangegangenen Punkt sind die Forderungen der Normelemente des QMS und des ISMS inhaltsähnlich. Es ist nun der Bezug zum ISMS dem QMS hinzuzufügen. Zur Prüfung, ob weitere Ergänzungen erforderlich sind wird auf den Abschnitt 5.1 der ISO/IEC 27001 verwiesen.

Ressourcen und Kompetenzen

Im Abschnitt Ressourcen des QMS muss aufgenommen werden, dass die Organisation auch die erforderlichen Ressourcen für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die kontinuierliche Verbesserung des ISMS bestimmt und bereitstellt.

Im Abschnitt Schulung und Kompetenz muss ergänzt werden, dass die Organisation:

- die erforderlichen Kompetenzen von Personen bestimmt, die Tätigkeiten im Bereich der Informationssicherheitsleistung verrichten
- sicherstellt, dass die Personen auf Grund von angemessener Ausbildung, Schulung oder Erfahrung kompetent sind
- erforderlichenfalls Maßnahmen einleitet, damit die benötigte Kompetenz erworben wird und im Nachgang die Wirksamkeit der eingeleiteten Maßnahmen bewertet
- angemessene dokumentierte Information als Nachweise der Kompetenz vorhält

Die Anforderungen sind grundsätzlich inhaltsgleich mit denen der EN ISO 13485.

Tipp:

Die häufigste Gefahr für Informationswerte einer Organisation geht von den eigenen Mitarbeitern aus. Dabei sind absichtliche Gefährdungen eher selten. Meist mangelt es am notwendigen Bewusstsein der Mitarbeiter, die festgelegten Sicherheitsmaßnahmen auch konsequent anzuwenden. Deshalb ist das Schaffen eines ausreichenden Sicherheitsbewusstseins eine der wichtigsten Aufgaben für jedes ISMS.

Bewusstsein und Kommunikation

Die Normelemente „Bewusstsein" und „Kommunikation" des QMS werden für das ISMS inhaltsgleich ergänzt. So müssen die Personen sich auch folgender Aspekte bewusst sein:

- der Informationssicherheitspolitik
- ihres Beitrags zur Wirksamkeit des ISMS, einschließlich der Vorteile einer verbesserten IS-Sicherheitsleistung
- der Folgen bei Nichterfüllung der Anforderungen an das ISMS (dieser Aspekt ist für das QMS neu)

Die Organisation muss die interne und externe Kommunikation auch in Bezug auf das ISMS bestimmen: Worüber, wann, wer, mit wem und mit welchem Prozess kommuniziert. Besondere Bedeutung hat das im Krisenfall – wenn z.B. die Organisation von einem IT-Sicherheitsvorfall betroffen ist.

Integration des ISMS in das QMS

Mit Hilfe der ISMS-Checkliste werden alle QMS-Prozesse betrachtet und die Stellen ermittelt, an denen ergänzende Maßnahmen zur Erreichung der Maßnahmenziele eingeführt werden müssen.

Dabei gibt es prinzipiell zwei Möglichkeiten zur Integration:

Definition von IS-Unterstützungsprozessen (Richtlinien)

Es bietet sich an, übergeordnete Maßnahmenziele als ISMS-Teilprozesse im QMS zu verankern. In der ISO/IEC 27001 wird dafür häufig der Begriff „Richtlinie" gebraucht. In Richtlinien werden Festlegungen getroffen, die nicht einzelnen Hauptprozessen zugeordnet werden können. Typische Beispiele für solche Richtlinien sind Regelungen zur Passwortvergabe, zum Umgang mit Mobilgeräten oder zu kryptografischen Methoden.

Integration von IS-Aufgaben in Haupt- oder Unterstützungsprozesse des QMS

An vielen Stellen bietet es sich an, die ISMS-Aufgaben in vorhandene Prozesse des QMS zu integrieren. Beispielsweise lässt sich die Schulung zum ISMS und IS-Elementen einfach in den Schulungsplan integrieren. Auch können Sicherheitschecks für zugelieferte Geräte in die übliche Wareneingangsprüfung eingegliedert werden.

Risikoanalyse und Bewertung (ISMS)

Wie allgemein üblich in Managementsystemen ist auch hier in der Norm nicht festgelegt, wie die Risikoanalyse genau durchgeführt wird, sie muss aber definiert sein und konsistent über alle Bereiche durchgeführt werden. Es ist am praktikabelsten einen ISMS-Unterstützungsprozess zu definieren, der die Risikoanalyse in Bezug auf das QMS und das ISMS übergreifend abbildet.

Der Risikomanagementprozess läuft bei Medizinprodukten immer konform EN ISO 14971 ab. Es bietet sich an, auch die Risikobeurteilung des ISMS so durchzuführen. Dabei sollte das IT-Sicherheits- und Risikomanagement des Technical Information Report 57 der Association for the Advancement of Medical Instrumentation (AAMI TIR 57) berücksichtigt werden. Es ergänzt auch die EN ISO 14971 um Fragestellungen der IT-Sicherheit (Sicherheit hier im Sinne von safety und security). An dieser Stelle der Hinweis, dass die aktuelle ISO 14971 nicht unter der MDD bzw. noch nicht unter der MDR harmonisiert ist. Der Hersteller sollte also benennen können, warum er sich für welche Version entschieden hat.

Prozessschritte im Risikomanagement:

Das Risikomanagement soll an dieser Stelle im Leitfaden nicht weiter betrachtet werden, der Prozess sollte bekannt und vertraut (aber hoffentlich nicht verhasst) sein. An dieser Stelle aber noch der Hinweis, dass die Auftretenswahrscheinlichkeiten prozessgetriggert nach einem gewissen Zeitraum mit der Anzahl der tatsächlich eingetretenen Ereignisse abgeglichen werden sollten.

Ermitteln der IS-Risiken

Ausgangspunkt für das Ermitteln der IS-Risiken sind zunächst alle Informations-Assets der Organisation. Der oben bereits erwähnte Netzstrukturplan ist dabei eine große Hilfe.

Der sicherste Weg folgt stur dem Prozessfluss und erfasst alle aufgefundenen Systeme. Da entsprechend der bereits vorhandenen (oder mindestens geplanten) QMS-Zertifizierung eine bewertete Liste der verwendeten und kritischen Software vorliegen muss, kann alternativ aber auch mit dieser Dokumentation der Software und der dabei verwendeten Hardware begonnen werden.

Danach werden Unterstützungsprozesse und ausgelagerte Prozesse (kritische Lieferanten) untersucht.

Eine Hilfestellung für das Ermitteln der Bedrohungen bietet die Tabelle im Anhang, in der häufig vorhandene ISMS-Risiken aufgeführt sind. Darüber hinaus bietet auch die Liste der elementaren Gefährdungen des BSI einen guten Einstieg.

Risikobeurteilung

Entsprechend der ISO/IEC 27001 beginnt die Risikobeurteilung mit den Schritten

- Festlegen der Risikoakzeptanzkriterien
- Festlegen der Kriterien für die Durchführung der Risikobeurteilung

Die weiteren Schritte werden an dieser Stelle als bekannt vorausgesetzt, sie entsprechen der Vorgehensweise für die EN ISO 13485.

Risikobehandlung

Für alle ermittelten Risiken muss dann bewertet werden, wie weiter mit ihnen umgegangen wird. Folgende Möglichkeiten bestehen:

- Akzeptanz des Risikos
- Abwälzen des Risikos auf Dritte
- Vermindern des Risikos durch weitere Maßnahmen

Dabei sind natürlich die Maßnahmen aus dem Anhang A der ISO/IEC 27001 einzubeziehen, damit keine erforderlichen Maßnahmen übersehen werden.

Erklärung zur Anwendbarkeit (SoA – Statement of Applicability)

Wozu brauche ich eine SoA, wenn ich doch eine komplette Managementsystemdokumentation habe, in der auch Aussagen zum Geltungsbereich meines Systems aufgeschrieben sind?

Der Grund dafür liegt in der besonderen Struktur der ISO/IEC 27001 – im Vergleich zu den anderen Managementsystemnormen.

Die ISO/IEC 27001 enthält zunächst alle Elemente, die auch andere Systeme (z. B. nach EN ISO 13485) enthalten. Diese basieren auf der sogenannten High Level Structure, die die ISO als Grundlage für alle Managementsystemnormen definiert hat.

Der nächste Schritt für alle Anwender einer derartigen Norm ist es nun, Maßnahmen zu definieren, mit denen die Ziele der Norm erreicht werden können und dafür interne Prozesse und Regelungen aufzustellen. Für die ISO/IEC 27001 übernimmt der Normengeber selbst den ersten Schritt, indem im Anhang A insgesamt 114 Maßnahmen festgelegt sind, die in jedem zertifizierten ISMS berücksichtigt werden müssen. Natürlich kann es dabei vorkommen, dass einzelne dieser Maßnahmen keine Anwendung finden – sei es, weil entsprechende Geräte nicht verwendet (z. B. A.6.2.1 Nutzung von Mobilgeräten) oder bestimmte Aktivitäten nicht durchgeführt werden (z. B. A.14.1.2 Anwendungsdienste in öffentlichen Netzwerken).

Basis für das Festlegen der Maßnahmen ist die in den vorangegangenen Abschnitten beschriebene Ermittlung und Analyse der Risiken. Dabei ist die SoA keineswegs nur auf die Maßnahmen aus der ISO/IEC 27001 beschränkt. Jeder Anwender ist aufgefordert zu prüfen, ob für die Sicherstellung eines angemessenen Risikos weitere Maßnahmen erforderlich sind. Für bestimmte Branchen gibt es dafür auch Normen, die Vorschläge für weitere Maßnahmen enthalten. Bei einer Organisation, die IT im Bereich Gesundheitswesen betreibt, ist das die DIN EN ISO 27799. Aber auch aus gesetzlichen oder vertraglichen Anforderungen können weitere Maßnahmen folgen.

Nun muss genau dokumentiert werden, welche Maßnahmen angewendet werden und welche nicht. Und es müssen die Gründe für die (Nicht-)Anwendung festgehalten werden. Das ist der Inhalt der Anwendbarkeitserklärung – also eine Erklärung über die Anwendbarkeit der vorgeschriebenen Maßnahmen aus dem Anhang der ISO/IEC 27001.

Weiterhin sollte aus der Erklärung zur Anwendbarkeit hervorgehen, wie weit Maßnahmen bereits umgesetzt wurden oder bis wann diese wie umgesetzt werden. Hier kann gut auf die laufenden oder geplanten Korrektur- und Vorbeugemaßnahmen verwiesen werden. Das heißt konkret: Bei einem integrierten Managementsystem wird die Anwendbarkeitserklärung auf die Prozesse, Richtlinien und Verfahren verweisen, die im Managementhandbuch festgelegt sind. Wenn man den Dokumentationsaufwand minimieren möchte, kann die Organisation versuchen, die Umsetzung direkt in der Anwendbarkeitserklärung zu formulieren.

Eine Erklärung zur Anwendbarkeit / SoA enthält also folgende Informationen:

- Maßnahmen
- Gründe für die Einbeziehung der Maßnahmen (unabhängig von der Umsetzung)
- Gründe für die Nichteinbeziehung
- Art und Weise, wie die Maßnahmen umgesetzt werden
- Stand der Umsetzung

Die SoA ist Teil der Zertifizierungsdokumente und wird daher auch auf dem Zertifikat genannt. Relevante Änderungen erfordern deshalb die Ausstellung eines neuen Zertifikats. Eine laufende Aktualisierung der SoA ist folglich nicht zu empfehlen. In diesem Fall ist es besser, ein Arbeitsdokument und eine offiziell vorlegbare Version vorzuhalten. Dieses Verfahren sollte der Organisation

aus dem Umgang mit dem Handbuch für die EN ISO 13485 oder der Akte des Medizinprodukts bekannt sein.

Die Anwendbarkeitserklärung ist das Dokument, mit dem die Sicherheitspolitik der Organisation gelebt wird. Gestalten Sie die Erklärung danach und leben Sie diese.

ISMS und MDR

Bisher wurde immer nur auf die EN ISO 13485 Bezug genommen. Natürlich muss bei einem Medizinprodukt auch die Verordnung (EU) 2017/745 über Medizinprodukte (Medical Device Regulation (MDR)) berücksichtigt werden, damit die Konformität erklärt werden kann. Die MDR selbst fordert kein ISMS, es wird allgemein IT-Sicherheit gefordert. Die MDCG 2019-16 gibt hier weitere Hinweise zur Cybersecurity und verdeutlicht den Einfluss von DS-GVO und NIS. Auch werden künftig weitere Normen, wie z. B. die ISO/IEC 82304-1/2; IEC 8001-5-1 unter der MDR harmonisiert. Siehe hierzu auch den folgenden Abschnitt.

Achten Sie also darauf, dass das ISMS auch die Bereiche umfasst, die nicht von der EN ISO 13485 adressiert werden, sondern durch die MDR spezifiziert sind. dazu gehören u.a. klinische Bewertung/PMCF; die Kommunikation mit den zuständigen Behörden, Benannten Stellen, weiteren Wirtschaftsakteuren, Kunden und/oder anderen interessierten Kreisen; Überwachen der Produkte nach dem Inverkehrbringen usw.

ISMS und IT-Sicherheit des Produkts

Als Hersteller müssen Sie nachweisen, dass die grundlegenden Sicherheits- und Leistungsanforderungen (GA) vom Medizinprodukt erfüllt werden. Dies ist Teil der Technischen Dokumentation (TD). Ein ISMS greift nach Definition nur auf der Managementebene. Für Software als Medizinprodukt und insbesondere DiGA gilt aber die Besonderheit, dass sich das Management nach EN ISO 13485 eben auch in der TD niederschlägt. Die TD muss also in allen relevanten Bereichen – diese sind in Phase I identifiziert – um Elemente der Risikobetrachtung des ISMS erweitert werden. Beachten Sie also, dass die durch das ISMS adressierten GA auch enthalten sind und erfüllt werden.

Um die einzelnen Punkte der IT-Sicherheit zu überprüfen, die in für Medizinprodukte relevanten Normen und Richtlinien festgelegt sind, empfiehlt sich ein Blick in die Checkliste CyberSecurity der IG-NB. Die IT-Sicherheitsanforderungen sind Bestandteil der grundlegenden Sicherheits- und Leistungsanforderungen und damit auch im integrierten Managementsystem zu dokumentieren.

Die einzelnen Elemente dieser Checkliste betreffen anerkannte Regeln der Technik, die sich mit der Zeit ändern. Die in der Checkliste genannten Quellen sind daher regelmäßig auf Aktualität zu prüfen. Anfallende Aktualisierungen werden bewertet und dann in das Integrierte Managementsystem eingepflegt.

Phase III

In der dritten Phase geht das ISMS in den Regelbetrieb, die eingeführten Prozesse werden umgesetzt und der Verbesserungszyklus des ISMS beginnt mit der ersten Bewertung durch die oberste Leitung.

Betrieb des ISMS

Die in der Phase II festgelegten Regelungen müssen nun in die Praxis überführt werden und ihre Tauglichkeit in der täglichen Arbeit beweisen.

Das beginnt in der Regel mit einer intensiven Einweisung der jeweils betroffenen Mitarbeiterinnen. Durch die Verantwortlichen wird dann laufend überwacht, ob die neuen Regelungen wirksam sind und die vorgesehenen Ziele damit erreicht werden können. Gegebenenfalls erfolgen auch bereits

erste Korrekturen für Prozesse und Richtlinien. Dafür wird gleich der festgelegte Änderungsprozess für das ISMS verwendet.

Tipp:

Scheuen Sie sich nicht, Regelungen, die sich als unpraktisch erweisen, zu ändern und an Ihre Verhältnisse anzupassen. Es gibt immer viele Möglichkeiten, die Anforderungen der Norm zu erfüllen. Wählen Sie immer einen Weg, der für Ihr Unternehmen passt und von Ihren Mitarbeitern akzeptiert wird. Das ISMS soll Ihnen helfen, Ihre Ziele bezüglich Informationssicherheit zu erreichen. Dabei ist fehlende Akzeptanz von Sicherheitsmaßnahmen ein großes Hindernis!

Auditorinnen des ISMS werden erwarten, dass in diesem Bereich auch die konkrete Durchführung und regelmäßige Wiederholung von Risikobeurteilung und Risikobehandlung beschrieben und dokumentiert wird. Wenn dies nicht – wie vom Leitfaden vorgesehen – im Bereich der Prozesse der Risikoanalyse (EN ISO 14971) geschehen ist, so sind an dieser Stelle die Prozesse zu etablieren. Zumindest die Dokumentation der Durchführung und der Ergebnisse ist hier zu erwarten.

Überwachung, Messung, Analyse und Bewertung des ISMS

Die Normelemente aus dem Abschnitt 8 der EN ISO 13485 sind ähnlich denen der ISO/IEC 27001 im Abschnitt 9. Die Prozesse des QMS sind entsprechend der Formulierung so anzupassen, dass sie auch für das ISMS mitgelten.

Im Unterschied zum QMS bereitet es Organisationen immer wieder Schwierigkeiten, geeignete Kennzahlen für die Informationssicherheit zu finden und in die Prozessüberwachung zu integrieren. Eine große Hilfe bietet dabei die ISO/IEC 27004, dort finden Sie nicht nur Vorschläge für den Prozess der Messung selbst, sondern auch viele Beispiel für mögliche Messgrößen.

Die folgende Abbildung beschreibt den Prozessfluss:

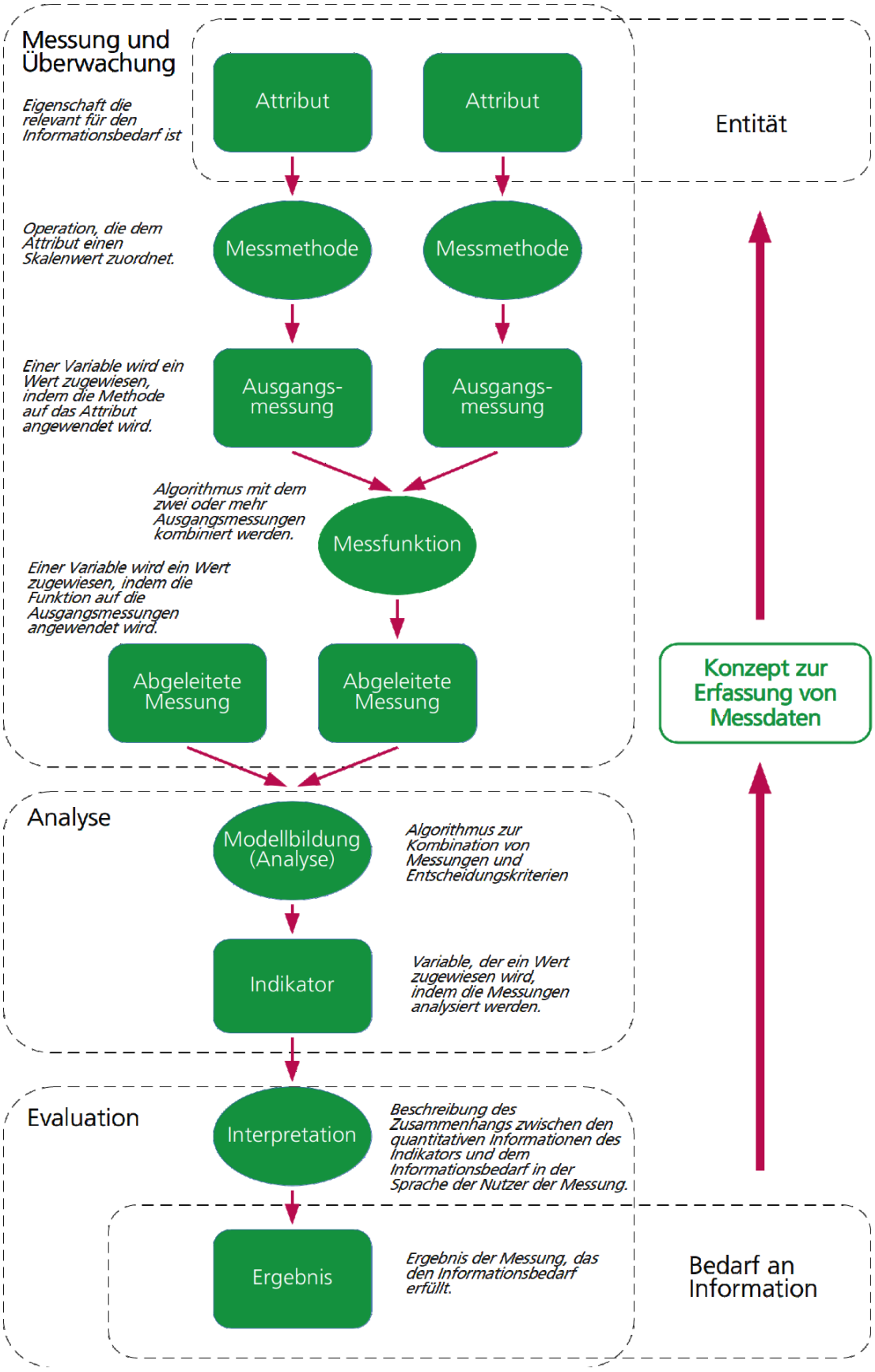


Abbildung 1: Modell zur Ermittlung von Messwerten für KPIs im Bereich des ISMS Quelle: ISO/IEC 27004:2016

Fortschreibung der Risikobewertung

Die erste Risikobeurteilung ist bereits in Phase II erfolgt. Dabei wurden i.d.R. auch Risiken ermittelt, die als nicht akzeptabel eingestuft wurden. Für diese wurden Maßnahmen zur Risikobehandlung festgelegt und in Phase III umgesetzt.

Zum Abschluss der Einführungsphase müssen die Risiken nun erneut bewertet werden – das Verfahren dafür wurde ja bereits eingeführt und erprobt. Durch die jetzt umgesetzten Maßnahmen sollten nun alle noch vorhandenen Risiken auf ein akzeptables Niveau reduziert worden sein. Es können aber durchaus noch Maßnahmen offen sein, deren Umsetzung erst zu einem späteren Zeitpunkt erfolgen soll. Die Akzeptanz bezieht sich dann auch auf den Zeitraum bis zur voraussichtlichen Wirksamkeit der Behandlungsmaßnahme.

Anpassen des internen Auditprogramms

Das Auditprogramm des integrierten Systems entsteht aus dem Auditprogramm des Qualitätsmanagementsystems. Wie im bereits vorhandenen Programm müssen alle Normelemente in sinnvollen Zeitabständen ggf. mehrfach durchlaufen werden. Sie können die Normelemente des ISMS im Auditprogramm an den passenden Stellen ergänzen. So können etwa im Bereich der Schulung für Mitarbeiterinnen neben den QMS-Schulungen auch die ISMS-Anteile auditiert werden. Für bestimmte Bereiche werden jedoch eigene Teile des Auditprogramms benötigt werden. Auch kann es sein, dass im Bereich der Infrastruktur der Fokus verschoben wird: Wenn etwa die frist- und formgerechte Installation von Updates auf Firewall-Systemen auditiert wird, dann ist dieser Punkt im Bereich Infrastruktur/ IT-Sicherheit des QMS auch berücksichtigt.

Tipp:

Bitte beachten Sie, dass bis zu einer geplanten Zertifizierung ein vollständiges internes Audit abgeschlossen sein muss. Die Vollständigkeit bezieht sich dabei auf die Prüfung aller Normanforderungen, insbesondere auch aller Maßnahmen aus dem Anhang der ISO/IEC 27001. Bei Organisationen mit mehreren Standorten müssen dabei auch alle Standorte auditiert worden sein.

Natürlich ist und bleibt ein internes Audit eine Stichprobenprüfung – für den Nachweis der Erfüllung einer Normforderung reicht deshalb die Auditierung einzelner Beispiele.

Um die Vollständigkeit des internen Audits zu gewährleisten, können Sie gerne die Checkliste der GUTcert verwenden.

Managementbewertung

Die Managementbewertung ist bereits in der EN ISO 13485 als Normelement 5.6 enthalten. Diese muss um den Aspekt des ISMS inhaltlich erweitert werden. Es wird dann gemeinsam das QMS und das ISMS bewertet. Neben den Punkten der fortdauernden Eignung, Angemessenheit und Wirksamkeit wird auch der Kontext der Organisation betrachtet. Es ist sehr sinnvoll, hier auch über den Tellerrand hinauszuschauen und das QMS miteinzubeziehen. Die Fragen sollte also lauten: Welche Veränderungen gab es bei externen und internen Themen, die das integrierte Managementsystem betreffen? Welche Rückmeldungen gab es von interessierten Parteien? In Bezug auf das ISMS neu aufgenommen werden muss ferner der Punkt „Ergebnisse der Risikobeurteilung und Status des Plans für die Risikobehandlung“. Dabei ist durch die oberste Leitung auch die Akzeptanz von Risiken zu bewerten.

Phase IV

In der vierten Phase wird beschrieben, wie die Zertifizierung des ISMS abläuft.

Vorbereitung auf die Zertifizierung

Die inhaltlichen Vorbereitungen auf die Zertifizierung sind nach Abschluss der Phase III abgeschlossen.

Allerdings sollten Sie mit der Schaffung der formalen Voraussetzungen zur Zertifizierung schon deutlich früher beginnen. Bereits nach Abschluss der Phase I haben Sie alle notwendigen Daten, um ein Angebot zur Zertifizierung anzufordern.

Dabei sollten Sie den Vorteil einer kombinierten Zertifizierung nach EN ISO 13485 und ISO/IEC 27001 nutzen. Sie haben dabei nur eine Ansprechperson, die sich um Ihr komplettes Zertifizierungsprogramm kümmert. In den Audits werden Synergieeffekte ausgenutzt und der Auditaufwand wird soweit möglich reduziert.

Tipp:

Im Rahmen des Zertifizierungsverfahrens ist auch die Durchführung eines Voraudits möglich. Ziel eines Voraudits ist das Prüfen ausgewählter Managementsystemelemente vor Ort und das gegenseitige Kennenlernen vor dem Zertifizierungsaudit.

Zeitlich sollte ein Voraudit in die Phase II eingeordnet werden. Vorher sollten zumindest die grundlegenden Regelungen für das ISMS im Entwurf vorliegen. Auch das Verfahren zur Risikobewertung sollte definiert und anhand eines ersten Beispiels bereits getestet sein.

Das Ergebnis des Voraudits ermöglicht es Ihnen, frühzeitig Korrekturbedarf für bestimmte Prozesse und Richtlinien zu erkennen und somit späteren Änderungsaufwand zu reduzieren.

Das Voraudit ist aber nicht verpflichtend – falls Sie eine erfahrene Beraterin einbezogen haben, können Sie direkt mit dem Zertifizierungsaudit starten.

Zertifizierungsverfahren

Das Zertifizierungsverfahren nach ISO/IEC 27001 läuft für alle akkreditierten Stellen entsprechend den Regeln der ISO/IEC 27006 ab, eine detaillierte Beschreibung des Verfahrens der GUTcert finden Sie hier.

Nach der formalen und inhaltlichen Auditvorbereitung findet zunächst das Stufe-1-Audit vor Ort statt. Es dient der Prüfung der Zertifizierungsreife Ihres ISMS und der intensiven Vorbereitung des nachfolgenden Audits der Stufe 2.

Zum Ende des Stufe-2-Audits präsentiert das Auditteam die Ergebnisse des Audits. Falls es an dieser Stelle noch Nichtkonformitäten gibt, wird vereinbart, wie und bis wann diese korrigiert werden. Nach erfolgreichem Abschluss erstellt das Auditteam den Auditbericht und spricht die Empfehlung zur Zertifizierung aus.

Tipp:

Mit dem Zertifizierungsaudit beginnt der jährliche Zyklus der laufenden Begutachtung und Überprüfung Ihres ISMS. Die Audittermine in den folgenden Jahren orientieren sich dann immer an diesem ersten Audittermin. Bitte beachten Sie, dass dieser Termin in Ihren Jahresterminplan passt. Später ist nur noch eine Verkürzung des Turnus möglich, eine dauerhafte Verschiebung zu einem späteren Termin ist ausgeschlossen.

Die Zertifizierung selbst erfolgt dann nach einer unabhängigen Überprüfung des gesamten Verfahrens durch die Zertifizierungsstelle.

Zeitliche Planung

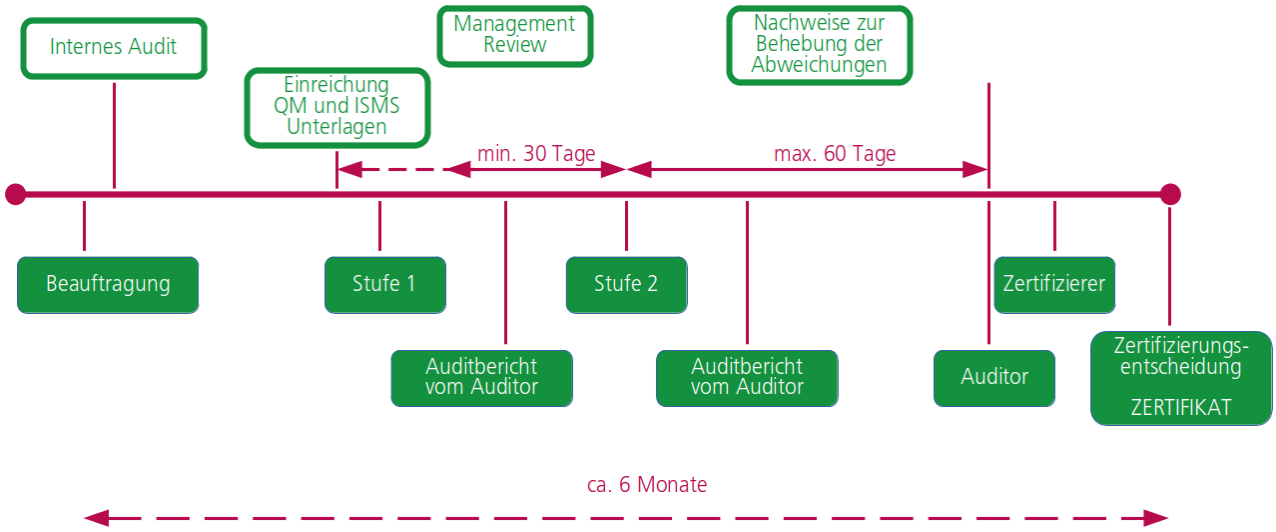


Abbildung 2: Zeitstrahl der Zertifizierung (ohne MDR), Quelle: eigene Darstellung

Anhand des Zeitstrahls können Sie sehen, dass für eine vollständige Zertifizierung eines integrierten Managementsystems aus QMS nach EN ISO 13485:2021 und ISMS nach DIN EN ISO/IEC 27001:2017 ein Zeitraum von ca. sechs Monaten einzuplanen ist. Falls ein Zertifikat nach EN ISO 13485 schon vorliegt und nur die Erweiterung um die ISO/IEC 27001 erforderlich ist, kann der Zeitraum von der vollständigen Einführung des ISMS am Ende der Phase II bis zur Zertifizierung auch auf bis zu drei Monate verkürzt werden.

Anhang | weitere Dokumente

Checkliste

Die Checkliste ist als Hilfsmittel konzipiert, um die Komponenten der Informationssicherheit eines integrierten Managementsystems aus EN ISO 13485 und ISO/IEC 27001 für die Anwendung im Bereich medizinischer Software auf Vollständigkeit zu prüfen. Basis für eine entsprechende Zertifizierung ist dabei die ISO/IEC 27001, zu berücksichtigen sind aber auch weitere Anforderungen durch die ISO 27799 sowie andere Normen und gesetzliche Regelungen.

Die Gliederung orientiert sich an den verbindlichen Maßnahmen, die nach ISO/IEC 27001 implementiert werden müssen. Für die Umsetzung der einzelnen Maßnahmen empfehlen wir, die ausführlichen Erläuterungen in der ISO/IEC 27002 mit heranzuziehen. Für viele Maßnahmen gibt es weiterhin Ergänzungen in der ISO 27799, die speziell auf die Umsetzung im Gesundheitswesen abzielen.

Crossreferenz

Wir haben Ihnen in unserem Leitfaden empfohlen, die im Anhang der ISO/IEC geforderten Maßnahmen in Ihre vorhandenen QM-Prozesse einzugliedern. Um Ihnen diese Zuordnung zu erleichtern, haben wir für Sie eine Crossreferenzliste erstellt, in der wir den verschiedenen Abschnitten der EN ISO 13485 die dazu passenden Maßnahmen zugeordnet haben. Sie finden diese Liste ebenfalls im Downloadbereich der GUTcert-Webseite.

Normen

DIN EN ISO/IEC 27001:2017

DIN ISO/IEC 27002:2016

ISO/IEC 27004:2016

DIN EN ISO/IEC 27006:2021

DIN EN ISO 27799:2016

DIN EN ISO 13485:2021

ISO/TS 14441:2013

ISO 15489-1:2016

ISO/TS 21547:2010

ISO 22857:2013

ISO 27789:2013

Die genannten Normen sind beim Beuth-Verlag erhältlich.

Gesetze zu DiGA

- Mit dem Digitale-Versorgung-Gesetz (DVG) wurde das Sozialgesetzbuch V so geändert, dass eine neue Gruppe von Medizinprodukten die „digitalen Gesundheitsanwendungen" entstand. Mit der Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (DiGAV) wurden die Vorgaben für die DiGA konkretisiert. Zuletzt wurde diese Verordnung mit der ersten Verordnung zur Änderung der Digitale Gesundheitsanwendungen-Verordnung vom 22. September 2021 geändert.
- Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesund-

heitsanwendungen-Verordnung – DiGAV) vom 8. April 2020; Bundesgesetzblatt Jahrgang 2020 Teil I Nr. 18, ausgegeben zu Bonn am 20. April 2020;

- Gesetz zur Neuregelung des Schutzes von Geheimnissen bei der Mitwirkung Dritter an der Berufsausübung schweigepflichtiger Personen (30.10.2017); Bundesgesetzblatt Jahrgang 2017 Teil I Nr. 71, ausgegeben zu Bonn am 8. November 2017
- (Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte – MBO-Ä 1997; in der Fassung der Beschlüsse des 121. Deutschen Ärztetages 2018 in Erfurt, geändert durch Beschluss des Vorstandes der Bundesärztekammer am 14.12.2018

Checkliste CyberSecurity der IG-NB

Fragenkatalog „IT-Sicherheit bei Medizinprodukten“ (Version 4, Stand: 03.12.2021)

Weitere Bemerkungen zur EN ISO 27799:2016

Die Norm wurde erstmals im Jahr 2008 veröffentlicht. Die zweite Ausgabe, die aktualisiert wurde, um die 2013 veröffentlichten Versionen von ISO/IEC 27001 und 27002 zu berücksichtigen, wurde 2016 publiziert.

Die ISO 27799:2016 wurde vom technischen ISO-Komitee TC215 entwickelt und veröffentlicht, das für die Gesundheitsinformatik zuständig ist, und nicht von JTC1/SC 27, dem gemeinsamen ISO- und IEC-Komitee, das für ISO 27000 verantwortlich ist. Ob die ISO 27799 also streng genommen Teil der ISO/IEC 27000-Normenreihe ist, ist umstritten – für die Nutzer macht es jedoch so oder so kaum einen Unterschied.

Nutzerinnen erscheint es oft merkwürdig, dass hier keine enge Abstimmung zwischen den beiden Teams stattgefunden hat. In der Folge ist die ISO 27799:2016 also keine sektorspezifische Norm nach ISO/IEC 27009 (die ebenfalls 2016 veröffentlicht wurde) und folgt dieser auch nicht. Das erklärt, wieso Teile der 27002 in der 27799 inhaltsgleich mit eigenen Worten wiedergegeben werden. Hingegen liest sie sich wie ein Implementierungsleitfaden oder Buch, etwas, das ein erfahrener Berater verfassen könnte. Sie bietet pragmatische Ratschläge – Körner der Weisheit wie z. B. den Abschnitt 6.4.1.1. und Hinweise auf das rechtliche Umfeld einiger Länder. Der Anhang B bietet eine komplette Anleitung für die Implementation im Gesundheitsumfeld, Anhang C eine eigene Checkliste. Die ISO 27799:2016 ist damit neben einer sektorspezifischen 27002 auch eine sektorspezifische 27005.

Eine Besonderheit bildet auch die Wortwahl bzgl. verbindlicher und optionaler Anforderungen. In der englischen Normsprache sind mit „shall“ immer Forderungen formuliert, die verbindlich umzusetzen sind, während „should“ für optionale Anforderungen steht. Das macht z. B. auch den wesentlichen Unterschied zwischen dem Anhang der 27001 und der 27002 aus. In beiden sind die gleichen Maßnahmen aufgeführt, in der 27001 allerdings als verbindlich formuliert und in der 27002 als Option. Begründet ist dies darin, dass die 27001 die Zertifizierungsgrundlage ist, während die 27002 Vorschläge für die Umsetzung eines ISMS macht. Die 27799 sieht sich zwar als Leitfaden zur Anwendung der 27002 in der medizinischen Informatik und sollte deshalb eigentlich auch konsequent deren Formulierungen übernehmen, allerdings werden dort die spezifischen Anforderungen teilweise als verbindlich („shall“) und teilweise als optional („should“) formuliert. Anwendern kann hier nur empfohlen werden, alle in der 27799 beschrieben Anforderungen zu bewerten und – wenn anwendbar – umzusetzen.

Übersicht zu Bedrohungen für ISMS im Gesundheitssektor

- Täuschung durch Insider
- Täuschung durch Dienstanbieter
- Täuschung durch Außenstehende
- Unbefugte Nutzung einer Anwendung für Gesundheitsinformationen
- Einschleusen von schädlicher oder störender Software
- Missbräuchliche Nutzung von Systemressourcen
- Infiltration der Kommunikation
- Abfangen von Kommunikation
- Abstreitbarkeit
- Ausfall der Verbindung
- Einbettung von bösartigem Code
- Unbeabsichtigte Fehlleitung
- Technisches Versagen des Hosts, der Speichereinrichtung oder der Netzinfrastruktur
- Ausfall der unterstützenden Umgebung
- Ausfall der System- oder Netzwerksoftware
- Ausfall der Anwendungssoftware
- Fehler des Bedieners
- Wartungsfehler
- Benutzerfehler
- Personalmangel
- Diebstahl durch Insider
- Diebstahl durch Außenstehende
- Mutwillige Beschädigung durch Insider
- Mutwillige Beschädigung durch Außenstehende
- Terrorismus

Quelle: EN ISO 27799 Anhang A