Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Certificate of Advanced Studies Information Security – Management 25

Fallstudie SANAMED ISMS

❒ Lösung zur Aufgabenstellung

Einführung eines ISMS bei SANAMED

Gruppe 5

- Aiello Flavio
- Hauswirth Daniel
- Stadelmann Adrian
- Vogt Andreas
- Zibung Marc

Version: 0.9

7. September 2018

Klassifikation: Intern

Management Summary

Das Leitbild attestiert SANAMED einen schweizweit ausgezeichneten Ruf. Als Privatspital soll oberstes Unternehmensziel die klare Ausrichtung auf die Patientenzufriedenheit sein. SANAMED will deshalb die Interessen der Patienten umfassend und nachhaltig schützen.

Mit zunehmender Digitalisierung und Vernetzung im Gesundheitswesen, drängen sich vermehrt Fragen zur Informationssicherheit auf. Zudem wurde im Rahmen eines internen Audits festgestellt, dass keine nachhaltigen Bestrebungen hinsichtlich Einführung eines Managementsystem für Informationssicherheit vorhanden sind. Deshalb wurde durch die Geschäftsleitung beschlossen, die Erarbeitung der weiteren Schritte zur Einführung eines solchen Managementsystems freizugeben.

Die Beratungsfirma CAS-IS-M Risk & Security Consulting AG hat von SANAMED den Auftrag erhalten, ein Konzept zur Ausgestaltung und Einführung eines Managementsystems für Informationssicherheit auszuarbeiten. Dabei sollen die branchenüblichen Standards berücksichtigt und geltende gesetzliche Auflagen eingehalten werden. Zudem sollen die einmaligen und über drei Jahre gerechneten wiederkehrende Kosten und einen Einführungsplan unterbreitet werden.

Das Vorgehen im Beratungsmandat startet mit der Ermittlung der Lieferobjekte und Studium der von SANAMED erhaltenen Unterlagen zur Durchführung einer Risikoanalyse. Gleichzeitig wird der auf einem Geschäftsrisikoansatz basierende Informationssicherheitsprozess gemäss ISO/IEC 27001 festgelegt und anhand zweier ausgewählten Geschäftsprozesse initialisiert und unmittelbare Erkenntnisse im festgelegten Prozess verbessert. Das im Anschluss vorliegende Risikoportfolio und die resultierende Risk-Map bilden einen wesentlichen Bestandteil des Risiko-Assessment Verfahrens.

Grundsätzlich ist die Sensibilisierung für Informationssicherheit bei der Belegschaft als unzureichend zu bewerten. Die Risikoanalyse zeigt auf, dass vorrangiger Handlungsbedarf bei den kritischen Risiken «Falsche Medikation im Hochrisikobereich», «Kontrollübernahme eines Endgerätes», «Mangelhafte Sicherheitsorganisation» sowie «Informationsabfluss an unautorisierte Dritte» besteht.

Die erforderlichen Ressourcen für die Sicherheitsorganisation stehen SANAMED durch Reorganisation zeitnah zur Verfügung. Hierzu werden ein Sicherheitsausschuss und die Neupositionierung des Informationssicherheitsbeauftragten als Direktionsstab vorgeschlagen. Kritischer Erfolgsfaktor ist die Teilnahme eines Geschäftsleitungsmitgliedes, vorzugsweise Herr Beat Abgottspon im Ausschuss.

Wir haben die Zusammenarbeit mit dem Informationssicherheitsbeauftragten von SANAMED, unserem Auftraggeber Herr Peter Sicher äusserst konstruktiv und zielführend erlebt. Die Vorgehensplanung und die groben Entwürfe der Arbeit konnten bereits frühzeitig abgestimmt und so zielgerichtet die relevanten Themen für das Projekt «Einführung eines ISMS bei SANAMED» angegangen werden.

Damit der zeitgemässe und sichere Spitalbetrieb hergestellt werden kann, ist es unabdingbar ein ISMS zeitnah einzuführen. Die Projektplanung ergibt unter Berücksichtigung der Ressourcenplanung eine rollende Durchlaufzeit von sieben Monaten, sofern die Umsetzungsfreigabe per Ende September erfolgt. Die einmaligen Investitionskosten betragen CHF 493’ und jährlich wiederkehrend CHF 42’. Unter Berücksichtigung einer Lernkurve und Subsummierung über drei Jahre, entstehen wiederkehrende Kosten von CHF 170’. Bis auf Lizenz-, Wartungs- und Betriebskosten, sind alle Kosten Indikativ nach Aufwand berechnet. Erfahrungsgemäss ist es der Projektdurchlaufzeit und Kostenkontrolle zuträglich, wenn ITIL wie bei SANAMED bereits etabliert ist.

Inhaltsverzeichnis

1 Ausgangslage

Mit zunehmender Digitalisierung und Vernetzung im Gesundheitswesen, drängen sich vermehrt Fragen zur Informationssicherheit auf. Die verarbeiteten Patientendaten durch Organisationen im Gesundheitswesen sind gemäss DSG Art. 3 besonders schützenswerte personenbezogene Daten. Die Durchgängigkeit von klinischen Prozessen mit elektronischer Verarbeitung und Analyse von Patientendaten bis hin zu Administration und Abrechnung sowie auch in Steuerungswerkzeugen für das Management, ist stark zunehmend. Die Informationssicherheit ist deshalb als grundlegender und zwingender Baustein aller Beteiligten im Gesundheitswesen avanciert.

Im Rahmen eines internen Audits im Spital SANAMED wurde festgestellt, dass keine nachhaltigen Bestrebungen hinsichtlich Einführung eines Managementsystem für Informationssicherheit vorhanden sind. Zudem wurde festgestellt, dass für die vorhandenen sicherheitsbezogenen Kontrollen keine Dokumentation vorliegt und kein übergreifendes nachvollziehbares risikobasiertes Verfahren implementiert ist.

Deshalb wurde durch die Geschäftsleitung beschlossen, die Erarbeitung der weiteren Schritte zur Einführung eines spezifischen Managementsystems für Informationssicherheit als externes Beratungsmandat freizugeben. Der Informationssicherheitsbeauftragte Hr. Peter Sicher, hat die Beratungsfirma CAS-IS-M Risk & Security Consulting AG hat beauftragt, ein Konzept zur Ausgestaltung und Einführung eines Managementsystems für Informationssicherheit, mitsamt umfangreichem Begleitmaterial auszuarbeiten.

2 Zielsetzungen und Rahmenbedingungen

Übergreifendes Ziel ist der nachhaltige Investitionsschutz der Medisan-Stiftung als alleinige Eignerin von SANAMED AG. Sie ist interessiert daran, Informationssicherheitsrelevante Verstösse proaktiv zu verhindern, welche finanzielle Folgen und einen Reputationsschaden nach sich ziehen würden.

Die SANAMED Geschäftsleitung will die Interessen der Patienten umfassend und nachhaltig schützen. Demnach muss Informationssicherheit ein integraler Bestandteil des Geschäftsbetriebs werden. Dazu müssen die Zielsetzung einer kontinuierlichen Sicherstellung der Patienten- und Mitarbeitersicherheit für die Einführung eines Managementsystems für Informationssicherheit berücksichtigt werden.

Gleichzeitig müssen Rahmenbedingungen aus dem gegenwärtigen Geschäftsbetrieb und gesetzliche Auflagen berücksichtigt werden. Allfällige Organisationsanpassungen müssen sich möglichst nahtlos in die bestehende Organisation einfügen.

Das Managementsystem für Informationssicherheit soll nach dem üblichen Standard im Gesundheitswesen ISO/IEC 27001 erfolgen. Die neue Norm ISO/IEC 27799 für Medizinische Informatik wird gegenwärtig nicht berücksichtigt.

3 Managementsystem für Informationssicherheit

Als Bestandteil des übergreifenden Spitalweiten Managementsystems, stellt ein spezifisches Managementsystem für Informationssicherheit (nachstehend ISMS genannt) nach ISO/IEC 27001 ein

Modell für den Aufbau, Implementierung, Betrieb, Überwachung und Unterhalt zur Verbesserung des Schutzes von Vermögenswerten und Informationen, um basierend auf einem Geschäftsrisikoansatz die Geschäftsziele zu erreichen[1].

Der Schutzbedarf von Vermögenswerten und Informationen und demnach auch die Definition und Implementation geeigneter Massnahmen und Kontrollen, kann im Laufe der Zeit ändern. Deshalb ist das ISMS als prozessorientierten wiederkehrenden Zyklus zu verstehen.

Die Phasen des wiederkehrenden Zyklus nach ISO/IEC 27001 für Informationssicherheit basiert auf dem generellen Prozess-Ansatz der ISO Management Systeme mit den Phasen

- Plan (Establish) → Zieldefinition, Erstellung von Plänen
- Do (Implement) → Implementierung der Pläne
- Check (Maintain) → Messen der Ergebnisse aus der Implementierung
- Act (Continual Improvement) → Korrekturen und Verbesserungen

Die erfolgreiche Einführung eines ISMS ist wichtig, damit SANAMED

- eine grössere Sicherheit erhält, dass ihre Vermögenswerte angemessen geschützt sind,
- ein strukturiertes und umfassendes Rahmenmodell unterhält, mit welchem Informationssicherheitsrisiken identifiziert und bewertet sowie Kontrollen selektiert, eingeführt und verbessert werden kann,
- ihr Kontrollumfeld kontinuierlich verbessern kann und
- die rechtlichen und regulatorischen Anforderungen erfüllen kann.

3.1 *Plan*: Aufbau und Etablieren des ISMS

Die Planungsphase befasst sich mit dem Aufbau des ISMS. Zunächst ist der Umfang des ISMS zu bestimmen, also der Gegenstand, der durch das ISMS abgedeckt wird (vgl. Kapitel XY). Im Rahmen des definierten Umfanges gelten für das ISMS von SANAMED folgende Anforderungen.

3.1.1 Anwendungsbereich

Der Anwendungsbereich des Informationssicherheitsmanagementsystems konzentriert sich auf die übergreifenden Themen der Patienten- und Mitarbeitersicherheit. Die Geschäftsprozesse, welche hinsichtlich der genannten übergreifenden Themen keine Anwendung finden, sind aus dem ISMS ausgeschlossen.

Anhand zweier ausgewählten Geschäftsprozesse a) Apotheke/Medikation und b) Patientenadministration wird das ISMS initialisiert und unmittelbare Erkenntnisse dem vorgängig festgelegten Prozess korrigierend zugeführt.

[1] CAS-IT Sec Technik 49, Unterrichsunterlagen Tom Schidt EY

3.1.2 Organisation

Das Spital SANAMED ist ein Privatspital mit 220 Betten und liegt in Risch am Zugersee. Es ist im Belegarztsystem geführt und legt Wert auf medizinische Fachkompetenz, persönliche Pflege und Ambiente. Dieses Angebot nutzen jährlich rund 10'000 stationäre und 18'000 ambulante Patienten aus der ganzen Schweiz. In der Gebärstation erblicken jährlich rund 1'200 Kinder das Licht der Welt

Das Spital wird geführt durch die Stiftung Medisan welche 100% Eigentümerin der SANAMED AG ist. Es ist auf drei Führungsbereiche aufgebaut. Die jeweiligen Bereichsleiter bilden zusammen mit dem Spitaldirektor die Geschäftsleitung. Der Ärzterat vertritt die Interessen der Belegärzte gegenüber der Geschäftsleitung und dem Stiftungsrat (siehe Bild (Quelle SANAMED-Beschreibung)). Die Belegärzte sind nicht von der SANAMED AG angestellt.

Die Stelle des Informationssicherheitsbeauftragten (ISB) ist durch Peter Sicher besetzt, jedoch ist diese noch nicht im Organigramm ersichtlich. Der Leiter Technik und Sicherheit, Hubert Portmann, ist in seiner Funktion Sicherheitsbeauftragter (SIBE) der SANAMED AG.

Das Spital SANAMED ist als klassische Aufbauorganisation auf drei Führungsbereichen aufgebaut. Die jeweiligen Bereichsleiter bilden zusammen mit dem Spitaldirektor die Geschäftsleitung.

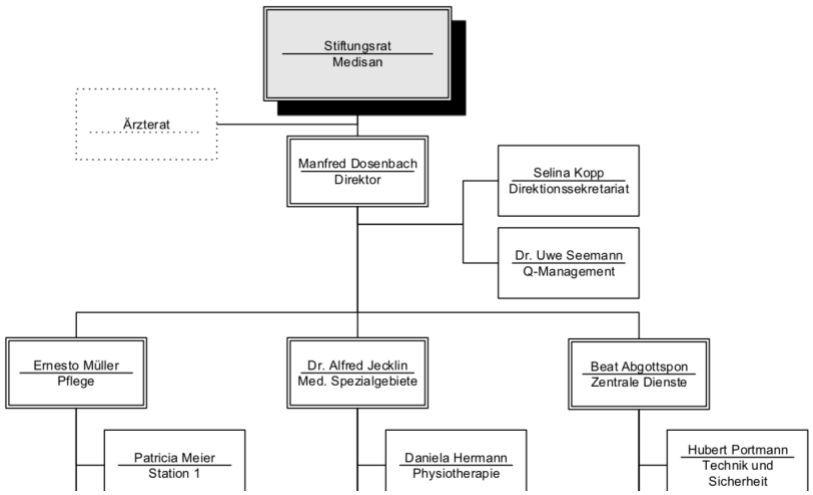


Abbildung 1 – Ausschnitt Organigramm

SANAMED will die Interessen der Patienten umfassend schützen. Zur nachhaltigen Sicherstellung der Patienten- und Mitarbeitersicherheit, soll Informationssicherheit ein integraler Bestandteil des Geschäftsbetriebs werden.

Die internen für die Informationssicherheit primär wesentlichen Organisationen sind in den zentralen Diensten zu finden.

Abteilung «Med. Spezialgebiete»

- Medizinische Informatik
- Beratungsdienste
- Radiologie

Abteilung «Zentrale Dienste»

- Technik und Sicherheit
- Informatik und Projekte
- Finanzen und Controlling
- Patientenadministration
- Hotellerie
- Einkauf Logistik

Folgende externe Organisationen sind für die Informationssicherheit relevant

- Labor Dr. Svenson AG (Labordienstleistungen)
- Ingenieurbüro Beisshart (Datenaustausch behindertengerechte Umbauarbeiten)
- Swisscom (Überwachung/Support der Telefonzentrale)
- Hubertus EDV AG (Service DB-Server E*Gate)
- McCormick (VPN-Tunnel ins LAN des Spitals)
- Microwell AG (VPN-Tunnel ins LAN des Spitals)
- Masterplan AG (VPN-Tunnel ins LAN des Spitals)

3.1.3 Stakeholder

Die Einführung eines ISMS bei SANAMED ist im Interesse folgender Stakeholder:

- Die Stiftung Medisan ist Eignerin von 100% des Aktienkapitals der SANAMED AG. Sie ist interessiert daran, dass es keine Informationssicherheitsrelevante Verstösse gibt, welche finanzielle Folgen und Reputationsschaden nach sich ziehen würden.
- Für die Patienten ist der Persönlichkeitsschutz von grossem Interesse. Alle gesundheitsbezogenen Daten sind besonders schützenswert und sollten durch in einem ISMS abgedeckt sein.
- Einige Lieferanten primär im IT-Bereich mit direktem Zugang ins Netz der
- Lieferanten von Medizinalprodukten und Pharmafirmen
- Regulatoren und Bundesamt für Gesundheit
- Interne Ärzte und Pflegepersonal
- Externe Belegärzte
- Andere Spitäler und Praxen, beispielsweise beim Übermitteln von Patientendaten.
- Besucher von Patienten können von der ISMS ebenfalls beeinflusst fühlen.

3.1.4 Dokumentenanforderungen

Die nachstehend aufgeführten Dokumente, deren Hierarchie und Verantwortlichkeiten sind wesentliche Grundlagen zur Etablierung eines ISMS bei SANAMED.

	Erstellung	Überprüfung	Genehmigung
1. Sicherheits-Politik und -Prinzipien (vgl. Anhang A) Die **Sicherheitspolitik** gibt Aufschluss über Zielsetzungen, gesetzliche Anforderungen und die generellen Rahmenbedingungen innerhalb SANAMED. **Sicherheitsprinzipien** sind allgemeingültige, einfache Regeln für Mitarbeiter, damit diese aktiv Schaden vom Unternehmen fernhalten und die Sicherheit positiv beeinflussen können.	ISB	SIBE	GL
2. Weisungen **Weisungen** definieren einheitliche unternehmensweit gültige Regeln und Massnahmen und haben für die gesamte SANAMED Gültigkeit.	ISB	SIBE	SA
3. Richtlinien **Richtlinien** werden für einzelnen Bereiche, aber auch für spezifische Themenbereiche der Sicherheit erlassen. Unter Beachtung der obigen können bei Bedarf detaillierte Normen und Anweisungen erlassen werden.	ISB	SA	BL

Tabelle 1 – Dokumentenhierarchie

3.1.5 Anforderungen an das Risikomanagement

SANAMED verfügt über einen systematischen Risikomanagementansatz in sechs Schritten. Das im Anschluss vorliegende Risikoportfolio und die resultierende Risk-Map bilden einen wesentlichen Bestandteil des Risiko-Assessment Verfahrens.

1. Risikoidentifikation

Bei der Identifizierung der Risiken wird wie folgt vorgegangen:

- Identifizieren der Schutzobjekte und der Schutzobjektverantwortlichen
- Identifizieren der Bedrohungen für diese Schutzobjekte
- Identifizieren der Schwachstellen, die durch die Bedrohungen ausgenutzt werden können
- Identifizieren der Auswirkungen auf die Schutzobjekte, die durch Verluste an Vertraulichkeit, Integrität und Verfügbarkeit entstehen können

Geschäftskritische Systeme und Applikationen werden regelmässig einer Risikoanalyse unterzogen, um die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Systemen sicherzustellen. Die Ergebnisse werden dokumentiert und dienen ihrerseits dazu, Massnahmen zu den Verbesserungen der IT-Sicherheit definieren und realisieren zu können.

2. Risikobewertung

Bei der Risikobewertung wird wie folgt vorgegangen:

- Bewerten des potentiellen geschäftlichen Schadens, unter Berücksichtigung der Konsequenzen eines Verlusts der Vertraulichkeit, Integrität oder Verfügbarkeit der Schutzobjekte
- Bewerten der realistischen Wahrscheinlichkeit, unter Berücksichtigung der vorherrschenden Bedrohungen und Schwachstellen sowie bereits implementierten Kontrollen
- Abschätzung der Risikoniveaus
- Bestimmen, ob das Risiko akzeptabel ist oder eine Risikobehandlung unter Benutzung der definierten Kriterien erfordert

3. Massnahmenidentifikation und -evaluation

Mögliche Massnahmen für die Risikobehandlung sind:

- Anwendung angemessener Kontrollen
- Wissentliche und objektive Akzeptanz der Risiken, unter der Bedingung, dass die Kriterien für die Akzeptanz der Risiken klar erfüllt sind
- Vermeidung von Risiken
- Übertragen der Geschäftsrisiken auf Dritte, beispielsweise auf Versicherer oder Lieferanten

4. Sicherheitszielen und Massnahmen

Auf der Grundlage der Risikobehandlungsplanung werden für jede Risikobewertung vorgängig die notwendigen Sicherheitsziele und Massnahmen bestimmt. Die Gründe für die Auswahl sind auf der Basis der Schlussfolgerungen des Risiko-Assessment zu belegen.

5. SoA: Erklärung zur Anwendbarkeit (vgl. Anhang C)

Die ausgewählten Sicherheitsziele und Massnahmen und die Gründe für deren Auswahl werden in einer Erklärung zur Anwendbarkeit (Statement of Applicability SoA) dokumentiert.

6. Managementfreigabe

Das Management muss der Umsetzung der Sicherheitsziele und Massnahmen zustimmen. Wir erachten die die gelebte Management-Verantwortung als kritischen Erfolgsfaktor für ein ISMS.

3.2 *Do*: Implementierung und Betrieb

SANAMED legt den Rahmen für die Implementierung und den Betrieb des ISMS fest, um auf identifizierte Risiken zu reagieren bzw. um die jeweilig definierten Massnahmen umzusetzen. Diese Phase des PDCA-Zyklus befasst sich mit der Umsetzung der Planung.

3.2.1 Umsetzung Organisation

(ISO-Kapitel 7.1, 7.2)

Gemäss Informationssicherheitshandbuch[2] werden für den Betrieb einer Sicherheitsorganisation folgende Positionen benötigt:

- Verantwortlicher Manager für Informationssicherheit in oberster Leitungsebene (Geschäftsleitung)
- Mindestens ein Sicherheitsbeauftragter, welcher unabhängig von der Geschäftsleitung berichten können. Die Position als Informationssicherheitsbeauftragter (ISB) existiert bereits in der Person von Peter Sicher bei der SANAMED
- Je nach Grösse wird ein Steering-Committee (Sicherheitsausschuss) aus Führungspersonen von verschiedenen Abteilungen empfohlen. Bei der SANAMED mit 585 Angestellten ist ein solches Komitee angebracht.

Wir schlagen eine Organisation gemäss Organigramm (siehe unten) vor. Der Sicherheitsausschuss besteht aus einem Vertreter der GL, drei Abteilungsleitern und dem Informationssicherheitsbeauftragten; die Mitglieder und Pflichten des Ausschusses werden weiter unten beschrieben.

Der Informationssicherheitsbeauftragte soll neu eine Stabsstelle werden. Als Sicherheitsverantwortlicher Manager in der GL schlagen wir den Leiter der Zentralen Dienste vor.

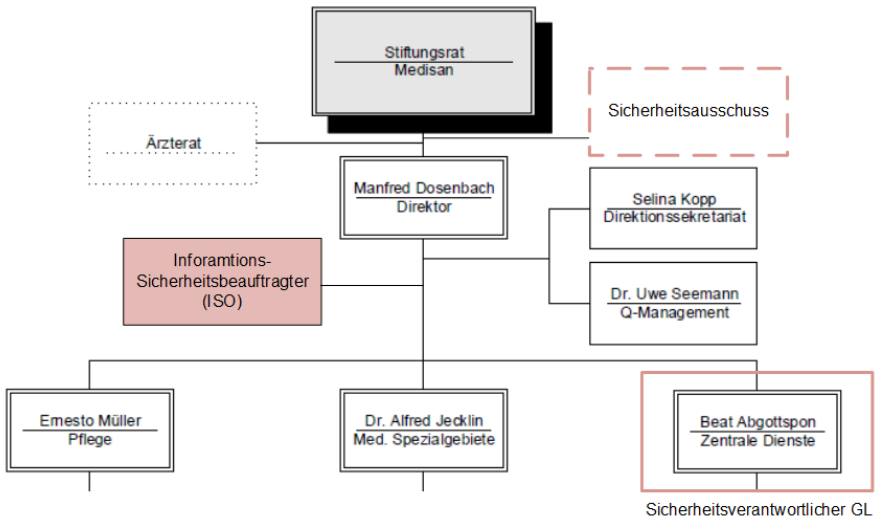


Abbildung 2 – Umsetzung Organisation

3.2.1.1 Informationssicherheitsbeauftragter ISB

Qualifikation

Die Position des Informationssicherheitsbeauftragten (ISB) existiert bereits. Jedoch wurde bisher kein Stellenprofil mit nötigen Qualifikationen und Pflichten für diese Position erstellt. Grundsätzlich sollten folgende Qualifikationen zutreffen, was vollständig auf den aktuellen ISB Peter Sicher zutrifft:

[2] Fachhochschule Luzern (2015) Informatiksicherheitshandbuch für die Praxis (Auflage 8/2015). ISBN 978-3-90613069-9

ISB Anforderungen

- Erfolgreich abgeschlossenes Studium in den Fachbereichen Informatik, Wirtschaftsinformatik oder eine vergleichbare Qualifikation
- Mehrjährige einschlägige Berufserfahrung im Bereich IT Security
- Sehr guter Wissensstand zu den aktuellen Sicherheitsstandards, Normen und Gesetzen
- Gute Fachkenntnisse in Betriebssystemen, Netzwerktechnologien, Datenbanken und (Web-) Applikationen
- Erfahrungen in der Durchführung von internen und externen Audits sowie im Risikomanagement

Pflichten

Der ISB ist verantwortlich für die firmenübergreifende Weiterentwicklung der Sicherheitsstandards und -richtlinien. Er treibt die Einführung und Pflege des Information Security Managements nach ISO 27001 voran. Er ist Ansprechpartner für Sicherheitsfragen im Unternehmen und zuständig für die Implementation, Pflege und Überwachung der Informationssicherheits-Politik, die Aufrechterhaltung des Informationssicherheitsniveaus und das Erstellen des Informationssicherheitskonzeptes. Er definiert auch Sicherheitsstandards, erlässt Weisungen und Richtlinien, berät Fachbereiche in Sicherheitsfragen, Projekten sowie zum Thema Datenschutz und organisiert entsprechende Schulungen und Sensibilisierungsmassnahmen. Der Informationssicherheitsbeauftragte rapportiert direkt der Geschäftsleitung und informiert diese auch über die durch ihn dokumentierten Sicherheitsvorfälle.

Weitere Aufgabenbereiche sind:

- Sicherstellung des aktuellen Schutzes der Unternehmen und Auswahl der notwendigen Tools und Massnahmen
- Erstellung von Risikoanalysen
- Ansprechpartner für die internen Fachabteilungen bezüglich Fragen zur IT-Sicherheit

Jährlich berichtet der ISB zuhanden der Geschäftsleitung über die Erfolgskontrolle des Sicherheitsprozesses und klärt diese über mögliche Risiken und Konsequenzen aufgrund fehlender Informationssicherheit auf. Die beinhaltet unter anderem folgende Punkte (frei nach Sicherheitshandbuch HSLU[3] und BSI[4])

- Haben die Rahmenbedingungen geändert?
- Sind die Sicherheitsziele noch angemessen?
- Ist die Aktualität der Sicherheitspolitik noch gegeben?
- Darstellung der Sicherheitsrisiken und der damit verbundenen Auswirkungen und Kosten
- Auswirkungen von Sicherheitsvorfällen auf die kritischen Geschäftsprozesse
- Gesetzliche und vertragliche Sicherheitsanforderungen
- Übersicht über Standard-Vorgehensweisen zur Informationssicherheit für die Branche

Schwerpunkt liegt dabei auf der Gesamtbetrachtung des Prozesses und nicht auf der Überprüfung einzelner Massnahmen. Auf dieser Basis soll die die Geschäftsleitung in der Lage sein, den Sicherheitsprozess zu bewerten.

[3] Fachhochschule Luzern (2015) Informatiksicherheitshandbuch für die Praxis (Auflage 8/2015). ISBN 978-3-90613069-9

[4] www.bsi.de

3.2.2 Sicherheitsausschuss

Vorsteher und Moderator des Sicherheitsausschusses ist der ISB, mit Stellvertretung durch den SIBE Herrn Hubert Portmann der bei Bedarf beigezogen wird. Sporadische Mitglieder schlagen wir je einen Abteilungsleiter aus jedem Führungsbereich vor. Erste informelle Gespräche zeigten, dass folgende Abteilungsleiter Interesse und Fähigkeit besitzen:

Führungsbereich	Name	Abteilung
Stabsstelle	Peter Sicher	Informationssicherheitsbeauftragter ISB
Sicherheitsverantwortlicher GL	Beat Abgottspon	Zentrale Dienste
Pflege	Stephanie Bachmann	Station 1
Med. Spezialgebiete	Dr. Franz X. Hirschmann	Medizinische Informatik
Zentrale Dienste	Anton Grisiger	Informatik und Projekte

Tabelle 2 – Sicherheitsausschuss

Der Sicherheitsausschuss tagt quartalsweise. Die Mitglieder des Ausschusses werden vom ISB über den aktuellen Stand der Einführung des ISMS informiert. Weiter können aktuelle Risiken und Schutzmassnahmen thematisiert werden. Die Mitglieder können Inputs aus Ihren Geschäftsbereichen zurückgeben. Mit dem Steuerungsausschuss soll sichergestellt werden, dass das ISMS und die Informationssicherheit bei den verschiedenen Führungsbereichen auf Akzeptanz und Verständnis stösst.

3.2.3 Verantwortlicher Manager GL für Informationssicherheit

Wir schlagen Beat Abgottspon als den für Informationssicherheit verantwortlichen Manager in der Geschäftsleitung vor. Er ist der direkte Ansprechpartner des ISB und fungiert als Bindeglied. Er ist verantwortlich für die Berichte des ISB zuhanden der GL. Er stellt sicher, dass informationssicherheitsrelevante Themen mit Überschreitung der Kompetenzordnung des Sicherheitsausschusses bei den Geschäftsleitungssitzungen traktandiert werden.

3.2.4 Dokumentierte Information

(ISO 7.5)

Alle für das ISMS relevanten Dokumente werden in der bestehenden Dokumentationsplattform erfasst. Dazu entsteht ein neuer Bereich für das ISMS, welcher nach der Kapitelstruktur des ISO 27001 aufgebaut ist. Die Dokumentplattform bietet indexierte Suche, Versionshistorie, kollaboratives Arbeiten und Nachvollziehbarkeit. Weiter wird mittels Berechtigungsschema sichergestellt, dass Personen ihrer Rolle im Prozess entsprechenden Zugriff erhalten.

3.2.5 Umsetzung Risikobehandlung

(ISO Kapitel 8.2)

Im Rahmen der Realisierung wird im Risikoportfolio die relevante Teilmenge zur Risikobehandlung ausgewählt. Damit lassen sich die Risiken priorisieren und den Status der Umsetzung sowie die notwendigen Massnahmen zwecks Umsetzung einheitlich verwalten. Die Massnahmen beinhalten auch Umsetzungsrelevante Informationen wie die allfällig erforderlichen finanziellen Mittel, Ressourcenzuordnung sowie Rollen und Verantwortlichkeiten.

Während des Risiko Assessments für die 2 ausgewählten Business Prozesse, wurden die 10 unten aufgeführten Risiken identifiziert

Risiko ID	Risiko Beschrieb
R1	Betrügerischer System-Administrator
R2	Informationsabfluss an unautorisierte Dritte
R3	Mangelhafte Sicherheitsorganisation
R4	Übernahme der Kontrolle eines Endgerätes
R5	Dateien mit Schadsoftware werden ins MediFile geschrieben
R6	Nachlässige Berechtigungsadministration
R7	Falsche Medikation im Hochrisikobereich
R8	Manipulation Medikamente im Hochrisikobereich
R9	Entwendung Medikamente im Hochrisikobereich
R10	Manipulation Medikationsplan

Tabelle 3 – Auszug der relevanten Risiken zur Risikobehandlung aus dem Risikoportfolio

Danach erfolgt unter Berücksichtigung der Finanzierung, Verantwortlichkeiten und Rollen die Umsetzung zur Erreichung der identifizierten Sicherheitsziele.

Der Risikomanagement-Prozess gemäss ISO 27005 hat Rückkopplungen und zyklische Wiederholungen (vgl. Bild unten). Somit wird die stetige Verbesserung dieses Prozesses sichergestellt. Die Rückkoppelungen beinhalten u.a. folgende Punkte:

- Entscheidungspunkte zum Einbezug von Führungspersonen
- Durch Iterationen werden Verbesserungen und Optimierungen der Ergebnisse erreicht.

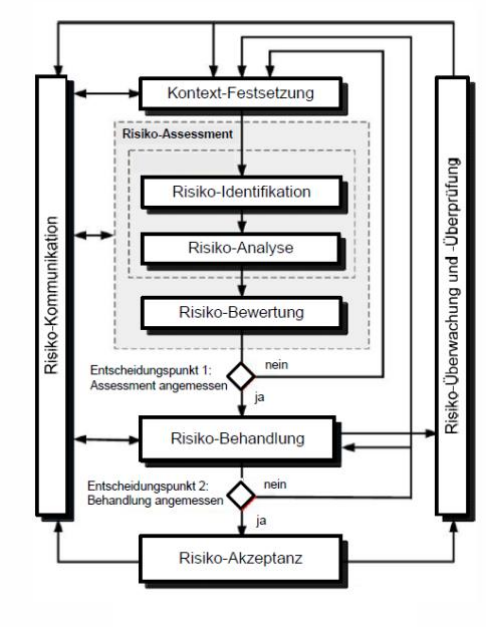


Abbildung 3 – Risikomanagement-Prozess nach ISO/IEC 27005

Die Überprüfung des Risiko-Assessment wird periodisch durch den ISO initiiert. Dazu werden nach Implementation des ISMS durch den ISB Key-Performance-Indikatoren (KPI) definiert, welche die Effektivität und Effizienz der Massnahmen messen[5]. Weiter werden Key-Risk-Indikatoren (KRI) erarbeitet, welche Alarm schlagen, wenn entsprechende Situationen eintreten. Gemäss Königs sind «solche Alarmsituationen […] denkbar bei Veränderungen des Risko-Kontexts.

Mit regelmässigen Audits durch externe und unbefangene Personen, wird das Risikomanagement jährlich überprüft. Der ISO stellt sicher, dass ein solches Audit als Teil der Jahres-Revision durchgeführt werden kann.

Mittels jährlichem Risiko-Bericht, ähnlich den Budgetberichten, wird über folgendes informiert[6].

«

- Statusmeldungen aktuelle und voraussichtliche Risikosituation
- Eingetretene oder fast eingetretene Risikoereignisse […]
- Stand, Wirksamkeit und Effizienz der Massnahmen-Umsetzungen und allfällige Verbessrungsvorschläge
- Geplante Ereignisse und Aktivitäten zur Verbesserung der Riskmanagements […]
- Voraussichtliche Veränderung und resultierende Konsequenzen für das Risikomanagement […]

»

[5] Hans Peter Königs(2013) IT-Risikomanagement mit System (4. Auflage) Kapitel 3.10 S65, ISBN 978-3-8348-1687-0

[6] Hans Peter Königs(2013) IT-Risikomanagement mit System (4. Auflage) Kapitel 3.11 S66, ISBN 978-3-8348-1687-0

3.2.5.1 Risk-Map

Die SANAMED Geschäftsleitung hat folgende Risiko Akzeptanz festgelegt. (Vgl. Kapitel 3.2.5.2) Alle Risiken, welche sich ausserhalb dieser Norm befinden müssen durch gezielte Massnahmen falls möglich vermindert werden. Für Risiken, welche nach Applizierung der Massnahmen immer noch ausserhalb der Akzeptanzbereichs sind, müssen durch den Approval-Prozess vom Management genehmigt werden und durch den stetigen Monitoring Prozess des ISMS überwacht werden.

3.2.6 Umsetzung der Massnahmen

Zur Erreichung der Sicherheitsziele müssen die in der PLAN-Phase ausgewählten Sicherheitsziele und Massnahmen umgesetzt werden.

3.2.7 Security Events und Security Incidents

(teilw. ISO Kapitel 8.1)

Um von (möglichen) Sicherheitsvorfällen zu erfahren, empfehlen wir ein Verbesserungs- und Meldewesen einzuführen, welches vom ISO unterhalten wird. Dies gibt den Mitarbeitern die Möglichkeit, dem ISO Verbesserungen und Sicherheitsvorfälle zu melden. Dies kann mit einem zentralen Ticketing-Tool oder mit einem einfachen Formular im Intranet bewerkstelligt werden. Die Meldungen fliessen in den PDCA-Zyklus ein. Der Sicherheitsbeauftragte ist verpflichtet, die Meldungen zu archivieren.

Eine Meldestelle ist insofern wichtig, da in den definierten primären Geschäftsprozessen Vorfälle passieren können, welche nicht mit IT-Mitteln erkannt werden können.

Folgende Checkliste soll bei den Verbesserungsiterationen zugezogen werden[7].

- Besteht eine zentrale und neutrale Meldestelle?
- Ist diese allen Mitarbeitenden bekannt?
- Werden Sicherheitsverstösse und Fehler gemeldet?
- Werden anonyme Meldungen eingereicht?
- Werden die Mitarbeiter über die Möglichkeiten des Verbesserungs- und Meldewesens informiert?
- Stehen die Formulare auf einem internen Server zur Verwendung bereit?
- Werden die Mitarbeiter über aktuelle Verbesserungsvorschläge und Meldungen informiert?
- Werden die eingereichten Verbesserungen auch umgesetzt?
- Werden gemeldete Fehler behoben?
- Wird gegen gemeldete Sicherheitsvorfälle etwas unternommen?
- Ziehen die gemeldeten Sicherheitsverstösse Sanktionen nach sich?

[7] Fachhochschule Luzern (2015) Informatiksicherheitshandbuch für die Praxis (Auflage 8/2015). ISBN 978-3-90613069-9

3.2.8 Verwaltung von Ressourcen

SANAMED ermittelt regelmässig die erforderlichen Mittel und stellt diese bereit. Für die Durchführung des ISMS und Realisierung aller Sicherheitsmassnahmen werden angemessene Ressourcen (Personal, Zeit und Geld) zugewiesen. Hierzu gehören die Dokumentierung aller umgesetzten Massnahmen und die aktive Pflege der ISMS Dokumentation.

3.2.9 Implementierung von Prozessen und Verantwortlichkeiten

Zur Gewährleistung des korrekten und sicheren Betriebs des ISMS sind entsprechende Prozesse und Verantwortlichkeiten definiert. Diese Prozesse und Verantwortlichkeiten sind dokumentiert, werden laufend ergänzt, verbessert und bei Bedarf angepasst.

3.2.10 Implementierung von Sicherheitskontrollen

Innerhalb der SANAMED sind Prozesse und Massnahmen implementiert, die eine sofortige Entdeckung und Reaktion auf Sicherheitsvorfälle ermöglichen.

3.2.11 Implementierung von Schulungsprogrammen

(ISO-Kapitel 7.3 7.4)

Zur Unterstützung der Mitarbeiter und zur Förderung des Sicherheitsbewusstseins werden Awareness- und Ausbildungsprogramme definiert. Diese werden regelmässig durchgeführt. Erfolgskontrollen überprüfen die Wirksamkeit der Ausbildungs- und Sensibilisierungsmassnahmen.

Für die in der ersten Iteration des ISMS angepeilten Geschäftsprozesse «Apotheke/Medikation» und «Patientenadministration» müssen die Mitarbeiter Kompetenzen erlangen. Hierzu werden die Mitarbeiter bezüglich der vorherrschenden Risken in Ihrem Bereich geschult. Zum einen beim Eintritt in SANAMED und im Weiteren jährlich bei einem der regelmässig stattfindenden Abteilungsmeetings. Verantwortlich dafür sind die Abteilungsleiter. Es wird eine für jeden Mitarbeiter über das Intranet zugängliche Dokumentation über die vorhandenen Risiken in ihrem Bereich erstellt.

Um das Bewusstsein zu schaffen, wird das Awareness Grobkonzept «Hilfsbereitschaft als Angriffsvektor»[8] weiterentwickelt und gezielt um den Punkt der Informationssicherheitspolitik erweitert. So kann bereits eine bestehende Awareness-Kampagne das Bewusstsein für das ISMS schaffen.

[8] CAS-IT Sec Management 25 Gruppe 5, Flavio Aiello

3.2.12 Kommunikation

Folgende Fragen müssen für die Kommunikation geklärt werden:[9]

- Welches Zielpublikum muss bedient werden?
- Muss Kommunikation für verschiedenen Funktionen/Rollen konkretisiert werden?
- Gibt es bereits institutionalisierte Kommunikationskanäle?
- Ist das Vorgehen der Kommunikation abgesprochen mit Beteiligten, Auftraggeber, der Geschäftsleitung und der KOM Abteilung?

In einer ersten Iteration des PDCA-Zyklus des ISMS wird die Kommunikation einfach gehalten. Die Mitarbeiter in den betreffenden Geschäftsprozessen werden mit Schulungen auf die in ihren Bereichen vorherrschenden Risiken aufmerksam gemacht. Das Bewusstsein für Informationssicherheit wird mit der Awareness-Schulung sichergestellt.

Die Mitarbeitenden sollten im Weiteren über die Änderungen in der Organisation informiert werden. Sobald die Organisationsänderung mit ISO und Sicherheitsausschuss definitiv bestimmt sind, wird in einem internen Newsletter über die Änderungen im Organisationsaufbau informiert. Ein solcher interner Newsletter wird bereits regelmässig von der Abteilung «Personal und Entwicklung» verschickt.

3.2.13 Schulungs- und Kommunikationsplan

ID	Aktion	Adressaten	Häufigkeit	Umfang
1	Einführung in Informationssicherheit	Mitarbeiter Prozesse «Apotheke/Medikation» und «Patientenadministration»	Arbeitsantritt und initial einmal	1h
2	Refresh Informationssicherheit	Mitarbeiter Prozesse «Apotheke/Medikation» und «Patientenadministration»	Jährliches Abteilungsmeeting	0.5h
3	Intranet-Informationssicherheitsdokumentation	Primär: Mitarbeiter Prozesse «Apotheke/Medikation» und «Patientenadministration» Sekundär: alle interessierte Mitarbieter	Individuell	0.5h
4	Awareness-Schulung	Alle Mitarbeiter	Jährlich	1h

[9] Gemäss Unterrichtsunterlagen CAS-IT Sec Management 25, Marcus Griesser

5	Information über neues ISMS via Newsletter	Alle Mitarbeiter	Einmalig	0.25h
6	Information über Organisationsänderung (Newsletter)	Alle Mitarbeiter	Einmalig	0.25h

Tabelle 4 – Schulungs- und Kommunikationsplan

3.3 *Check*: Überwachung, Überprüfung und Review des ISMS

In geplanten Abständen muss das ISMS (bzw. müssen das Framework, sicherheitsrelevante Prozesse, Massnahmen und Verantwortlichkeiten) überprüft werden, um deren Effizienz und Effektivität sicherzustellen. Die Ergebnisse der Überprüfung sind klar zu dokumentieren, Verbesserungen sind zu bewerten und Veränderungen sind vorzunehmen. Daneben gilt es aber auch, den Betrieb zu überwachen. Zu diesem Zweck haben die SANAMED folgende Kontroll- und Überwachungsmassnahmen implementiert:

3.3.1 Monitoring

Die Überwachung des laufenden Betriebs beinhaltet das Aufspüren von Verfahrensfehlern, die Überwachung der ISMS-Aktivitäten, Sicherheitsverletzungen und Massnahmenverfolgung bei Sicherheitsverletzungen.

Ziele des Monitorings und anderer Kontrollen auf Betriebsebene sind:

- Fehler, die im Processing auftreten, möglichst schnell zu entdecken
- Erfolglose und erfolgreiche Sicherheitsverstösse umgehend zu entdecken
- Dem Management eine Beurteilungsgrundlage zu geben, ob die an Personen delegierten Sicherheitskontrollen bzw. automatisierte Kontrollen und -mechanismen wie erwartet wirken
- Massnahmen zu ergreifen, damit entsprechend dem operativen Geschäft auf Sicherheitsverstösse reagiert werden kann

3.3.2 Überprüfung der Wirksamkeit des ISMS

Die Effizienz des ISMS wird regelmässig im Rahmen von Reviews überprüft. Gegenstand solcher Reviews sind:

- Zielerreichung hinsichtlich Sicherheitspolitik und -zielen
- Wirksamkeit von Sicherheitsmassnahmen
- Ergebnisse von Audits
- Vorkommnisse und Vorfälle
- Verbesserungsvorschläge
- Feedback und Rückmeldungen von Interessierten

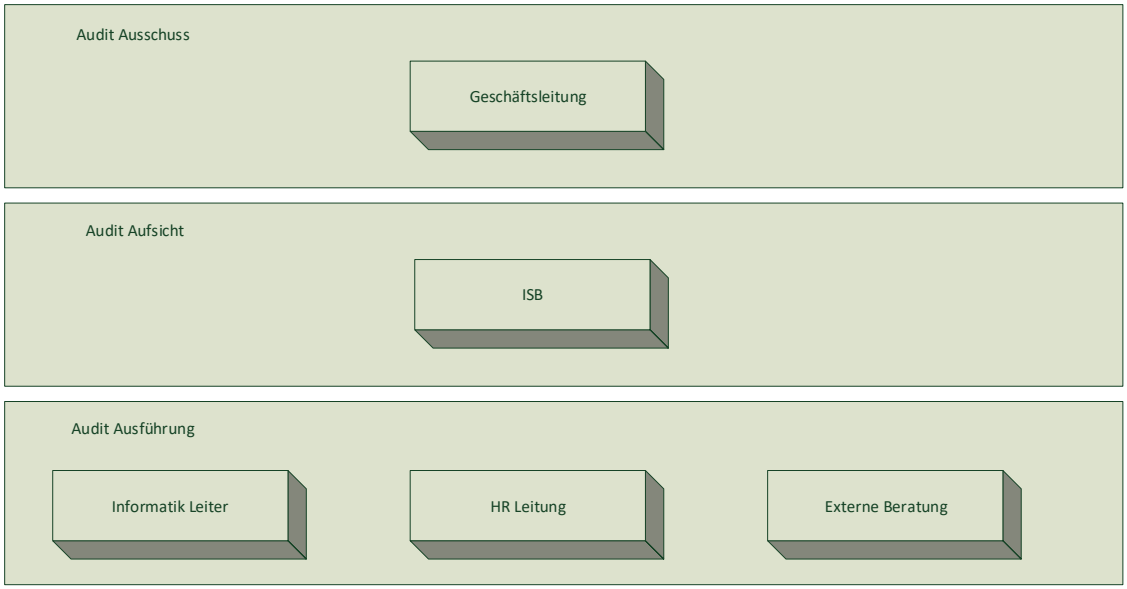
3.3.3 Interne ISMS-Audits

Interne ISMS Audits spielen eine wichtige Rolle für das Erreichen der Ziele und die Wirksamkeit der Ziele zu überprüfen, welche zur stetigen Informationssicherheit und Verbesserung dienen. Audits sind planmässige Überprüfungen welche das Ziel haben die Einhaltung sowie die effektive Umsetzung der Prozesse und Massnahmen festzuhalten. Die internen Audits sind mindestens einmal pro Jahr durchzuführen und die Ergebnisse müssen in Form eines Prüfberichts festgehalten werden.

Die Ergebnisse von Audits sind:

- aktuelle Mängel (vgl. unten: Korrekturmassnahmen)
- potentielle Mängel (vgl. unten: Vorbeugungsmassnahmen)
- Verbesserungsmöglichkeiten (vgl. unten: kontinuierliche Verbesserung)

Folgender Ablauf wurde definiert: Der ISB startet Minimum 1 jährlich den internen Audit Prozess. Das Gremium setzt sich aus Vertreter der Informatik Leitung, Personalabteilung Leitung sowie ein externer autonomer Berater zusammen. Der Audit Bericht danach der Geschäftsleitung SANMED ausgehändigt.



3.3.4 Management-Überprüfung des ISMS

Das Management führt in regelmässigen Abständen Reviews durch, um die kontinuierliche Zweckmässigkeit, Angemessenheit und Effektivität des ISMS zu bestätigen.

Zu diesem Zweck beauftragen die Geschäftsleitung und die Linienvorgesetzten, in gegenseitiger Absprache, den SIBE oder die interne Revision mit der Durchführung entsprechender Reviews.

Gegenstand des Reviews sind unter anderem Audit- und Review-Ergebnisse, Korrektur- und Vorbeugungsmassnahmen, Verbesserungsvorschläge, neue Techniken und Verfahren.

Die Ergebnisse von Management-Überprüfungen ergeben:

- Korrekturen des ISMS
- Verbesserungen des ISMS und/oder
- zusätzlich notwendige Ressourcenbereitstellungen

3.3.5 Aufzeichnungen

Aktionen und Ereignisse, die einen Einfluss auf die Effizienz des ISMS haben könnten, werden laufend dokumentiert. Zu diesem Zweck werden von den Verantwortlichen Besucherlisten, Logbücher, Protokolle, System-Logs, etc. geführt und ausgewertet.

Der ISBD führt zusätzlich ein Journal, in dem von den Mitarbeitern gemeldete Sicherheitsverstösse, Vorfälle, unzureichende Massnahmen und vorgefundene Risiken eingetragen werden.

Aufzeichnungen müssen erstellt und aufrechterhalten werden, um einen Nachweis zu liefern, dass die implementierten Prozesse und Massnahmen angemessen wirksam sind.

3.3.6 Überprüfung der Restrisiken

Die verbleibenden und akzeptierten Restrisiken werden regelmässig in Hinblick auf die Auswirkungen auf die Organisation, die Technologie, die Geschäftsziele und -prozesse, identifizierte Bedrohungen und das Unternehmensumfeld (wie beispielsweise Gesetzgebung, Überwachung oder soziales Umfeld) überprüft.

3.4 *Act*: Wartung und Verbesserung des ISMS

Die ACT-Phase ist die Phase der Verbesserung gemäss ISO/IEC 27001 - 10.1. In dieser Phase werden kontinuierlich Verbesserungen implementiert, Korrektur- und Vorbeugungsmassnahmen ergriffen, die Ergebnisse mit allen Betroffenen kommuniziert und diskutiert sowie die Umsetzung der Verbesserungsmassnahmen überwacht.

3.4.1 Korrekturmassnahmen

Korrekturen von Nichtkonformität meint das erkennen und behandeln von Abweichungen zu ISMS Vorgaben. Die besagte Behandlung (Korrektur) sollte eine Rückführung zur Konformität erfüllen.

Wir kennen zwei Stufen der Korrekturmassnahmen:

- Reaktive Korrekturmassnahmen (engl. "corrections"): Sofortmassnahmen zur schnellen (graduellen) Rückführung in die Konformität.
- Nachhaltige Korrekturmassnahmen (engl. "corrective actions"): Das systematische Aufarbeiten der Nichtkonformität und deren Ursachen und das Ableiten von Massnahmen.

Reaktive Korrekturmassnahmen

Reaktive Korrekturmassnahmen haben zum Ziel, schnell aber in angemessener Weise die Konformität zum Standard wiederherzustellen. Dabei sollte Korrekturmassnahme den Schaden nicht vergrössern und die Wirkung der Massnahmen soll überprüft werden.

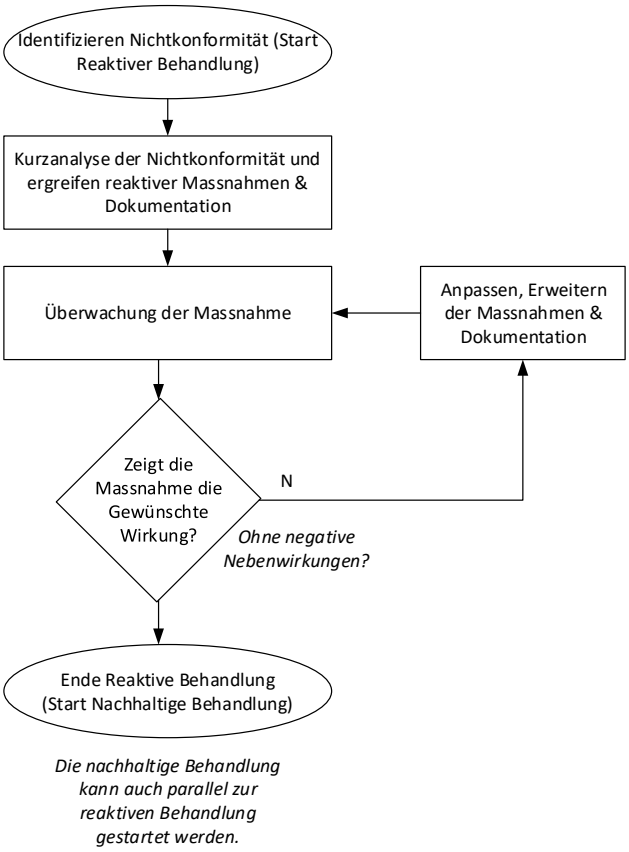


Abbildung 4 – Reaktive Korrekturmassnahmen

Nachhaltige Korrekturmassnahmen

Eine nachhaltige Korrektur der Abweichung erfordern eine Analyse der Ursache der Nichtkonformität und behebt diese so, dass die Nichtkonformität nicht mehr auftreten kann. Bei der Analyse wird geprüft, ob vergleichbare, verwandte Nichtkonformitäten bestehen oder auftreten können. Die Massnahmen sollte gegenüber der Nichtkonformität angemessen sein (vgl. Kosten und Ergebnis bzw. Wirkung der Massnahme).

Das Massnahmenpaket zur Beseitigung der Ursachen muss zeitnah umgesetzt und die Wirksamkeit überprüft werden.

Sämtliche Nichtkonformitäten, deren Ursachen, der getroffenen Massnahmen sowie deren Wirkung müssen dokumentiert werden.

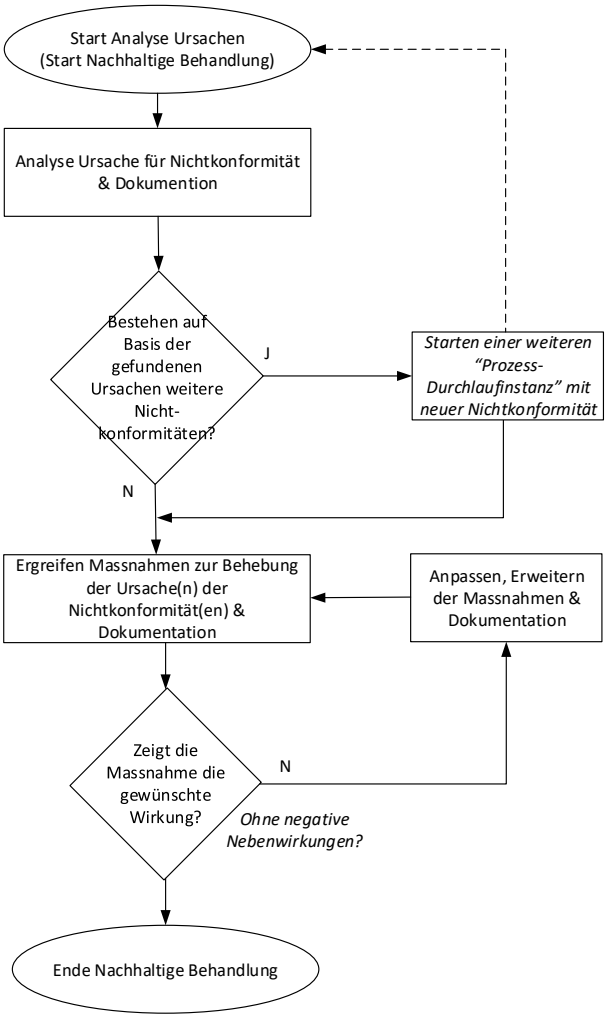


Abbildung 5 – Nachhaltige Korrekturmassnahme

3.4.2 Fortlaufende Verbesserungen

Das ISMS muss kontinuierlich den neuen bzw. geänderten Anforderungen entsprechend angepasst bzw. verbessert werden (vgl. KVP).

Dabei werden die Verantwortlichen sowie die Fachstellen (gem. ihrer Rolle im Prozess) in der Erarbeitung der Verbesserungsmassnahmen involviert. Die Ergebnisse werden den Betroffenen kommuniziert bzw. geschult und die Umsetzung der Verbesserungen wird bezüglich Wirkung im Ziel überwacht.

Der Verbesserungsprozess kann von verschiedenerer Seite angestossen werden:

- Rückmeldungen von Seite der Kunden (Patienten)
- Rückmeldungen von Seite der Belegschaft (und Partnern)
- Rückmeldungen von Seite Legal
- Ergebnisse aus internen wie externen Auditberichten
- Anforderungen durch neue bzw. geänderte Gesetze, Regularien und Normen

- Ergebnisse aus Riskmanagement
- Analyseergebnisse aus Ereignissen (Security Incidents) sowie "Nichtkonformitäten" und deren Ursachen.

Der Verbesserungsprozess kann auch ohne konkretes Ereignis im Sinne eines periodischen Reviews des ISMS, optimalerweise alle Jahre, maximal alle drei Jahre stattfinden.

Verbesserungen können Overall oder punktuell eingeführt werden, jedoch muss darauf geachtet werden, dass das ISMS konsistent bleibt und die Kosten der Massnahmen dem Nutzen angemessen ist. Auch sollten die definierten Verbesserungen zeitnahe eingeführt werden.

Sämtliche Verbesserungen bzw. Anpassungen am ISMS müssen nachvollziehbar dokumentiert werden.

Identifizierte Verbesserungen des ISMS werden schnellstmöglich implementiert. Es muss sichergestellt werden, dass die Verbesserungen auch tatsächlich die beabsichtigten Ziele erreichen. Der Wartungs- und Verbesserungsprozess findet kontinuierlich statt.

4 Projektplanung

Aus Gründen der Übersichtlichkeit wird zudem die Phase „Realisierung“ in zwei Teile gegliedert:

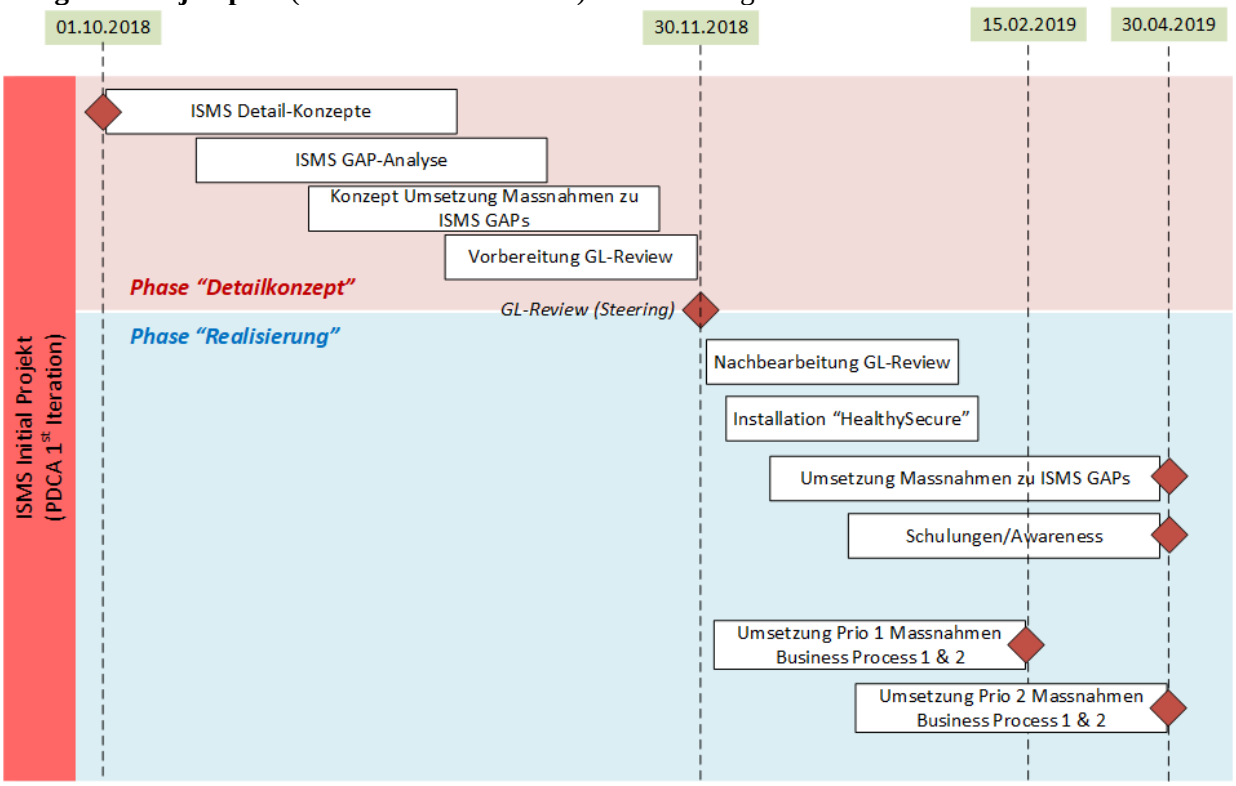
- Inbetriebnahme ISMS
- Umsetzung Massnahmen aus initialer Risiko-Analyse

Die Inbetriebnahme des ISMS erfolgt rollend, d.h. das ISMS ist nicht erst nach Ablauf aller vier Phasen betriebsbereit, sondern wird anlässlich der Durchführung des ersten Management Reviews formal produktiv. Anschliessend wird es parallel zur Betriebsführung bis zum voraussichtlichen Ende des Projekts im weitentwickelt und verfeinert.

Die Phasen «Einführung eines ISMS bei SANAMED» sind mit der Fertigstellung und Abnahme des vorliegenden Dokumentes durch den Projektauftraggeber abgeschlossen.

Die verbleibenden Phasen „Detailkonzept“ und „Realisierung“ werden in Arbeitspakete aufgeteilt und in einem Zeitraum von voraussichtlich sieben Monaten umgesetzt.

Der **grobe Projektplan** (erster PDCA Durchlauf) sieht wie folgt aus:



Eine **Detail-Planung** der Phase “Realisierung” passiert in der Vorbereitung zum Projekt-Steering Meeting “GL-Review” (Freigabe der Phase “Realisierung”), jedoch werden die angegebenen Daten (Milestones) als bindend erachtet.

Die **grobe Aufwandschätzung** ergibt:

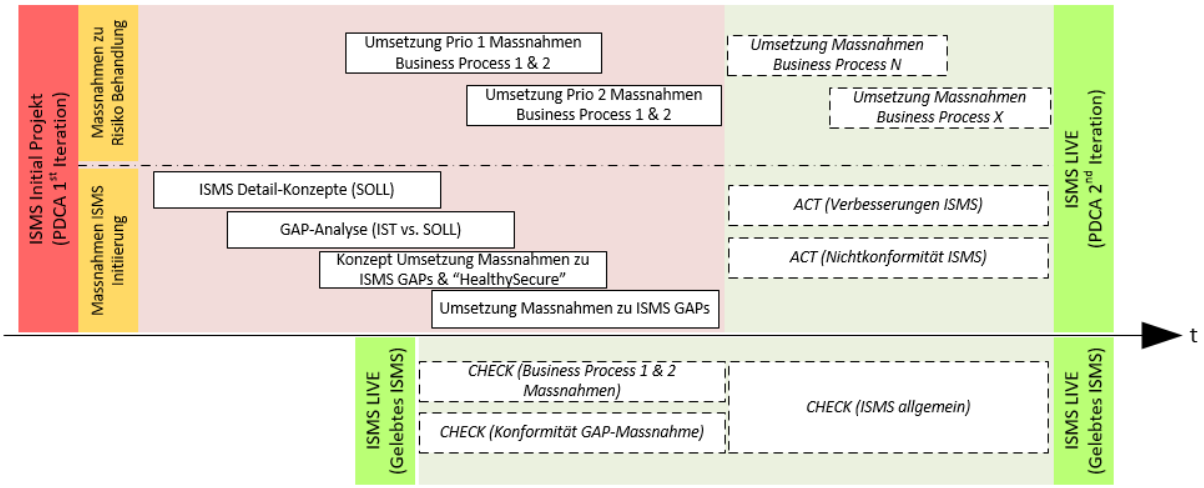
		Aufwandschätzung in PT					
Phasen	**Arbeitspakete**	**GL**	**SA**	**ISB**	**MA**	**Sanamed intern Total**	**Extern Total**
Detailkonzept	ISMS Detail-Konzept	0	10	10	10	**30**	20
	ISMS GAP-Analyse	0	10	5	5	**20**	15
	Konzept Umsetzung Massnahmen zu ISMS GAPs	0	5	5	15	**25**	5
GL Review (Steering)	Vorbereitung, Durchführung & Nachbearbeitung GL-Review (Projekt Steering)	2	5	5	0	**12**	5
Umsetzung	Installation "HealthySecure" (IS Policy Framework System)	0	0	2	10	**12**	5
	Umsetzung Massnahmen zu ISMS GAPs (inkl. Schulung/Awareness)	0	10	10	100	**120**	10
	Umsetzung Massnahmen (Prio 1) - Business Process 1 & 2	0	0	2	60	**62**	0
	Umsetzung Massnahmen (Prio 2) - Business Process 1 & 2	0	0	2	80	**82**	0
Total		**2**	**40**	**41**	**280**	**363**	**60**

Legende: GL = Geschäftsleitung, SA = Sicherheits Ausschuss, ISB = Information Security Beauftragter, MA = Fachpersonal

Zusammengefasst ergibt dies einen Aufwand von:

- Interne Aufwände Sanamed: ~370 Personentage
- Externe Coaching & Support: 60 Personentage

Die folgende Grafik ermöglicht eine Vorstellung über den **Übergang Projekt- zu Prozess-Modus**:



5 Wirtschaftlichkeit

5.1 Kostenindikation

Position			Einmalig	Wiederkehrend	
ISMS Software «HealthySecure»					
Lizenz und Wartung Variante On-Premise		CHF	28’		5’
Integrations- und Betriebskosten (auf bestehendem Server)		CHF	12’		8’
Dienst- und Arbeitsleistungen					
Coaching & Unterstützung externe Beratung	60PT	CHF	90’	6PT	9’
SANAMED Projekt- und Betriebsaufwand	363PT	CHF	363’	20PT	20’
Total		**CHF**	**493’**		**42’**

Tabelle 5 – Kostenindikation

Für die Kostenindikation wurden pro PT Aufwand extern CHF 1500 und intern CHF 1000 veranschlagt. Bis der neue Rahmenvertrag für Beratungsleistungen vorliegt, wird der gegenwärtige Tagessatz in Rechnung gestellt.

Die einmaligen Investitionskosten für das gesamte Projekt „Einführung eines ISMS bei SANAMED“ betragen CHF 493’ und jährlich wiederkehrend CHF 42’. Im ersten und zweiten Jahr nach Einführung, gehen wir von einer Lernkurve mit einem Mehraufwand für Dienst- und Arbeitsleistungen von 100% im ersten und 50% im zweiten Jahr aus. Dies ergibt ein Total an wiederkehrenden Kosten über drei Jahre gerechnet von CHF 170’.

5.2 Nutzen des Projekts

Durch Umsetzung des Projektes „Einführung eines ISMS bei SANAMED“ resultiert folgender Nutzen:

- eine grössere Sicherheit erhält, dass ihre Vermögenswerte angemessen geschützt sind,
- ein strukturiertes und umfassendes Rahmenmodell unterhält, mit welchem Informationssicherheitsrisiken identifiziert und bewertet sowie Kontrollen selektiert, eingeführt und verbessert werden,
- ihr Kontrollumfeld kontinuierlich verbessern und
- die rechtlichen und regulatorischen Anforderungen erfüllen kann.

5.3 Nichtrealisierung

Bei einer Nichtrealisierung des Projektes „Einführung eines ISMS bei SANAMED“ würde in der weiteren Bearbeitung der Sicherheitsthemen der Fokus nicht konsequent auf Informationssicherheit gerichtet. Dies kann dazu führen, dass die Wahrscheinlichkeit für Sicherheitsvorfälle bestenfalls konstant

bleibt und nicht systematisch gesenkt werden kann. Somit würden die Nachvollziehbarkeit und Strukturierung aufgrund eines international anerkannten Standards fehlen. Bei einer Nichtrealisierung kann die Informationssicherheit nicht durchgängig umgesetzt und anhand eines international anerkannten Standards geprüft realisiert werden.

Die Optimierung der Prozesse kann nicht übergreifend angegangen werden, d.h. die heutige Situation resp. die Diskrepanz zwischen dokumentierten Prozessen (bspw. ITIL) und gelebten Prozessen würde weiter bestehen und sich womöglich noch ausdehnen.

Die Nichterfüllung der Zielsetzungen der systematischen Informationssicherheit zur nachhaltigen Verbesserung der Patienten- und Mitarbeitersicherheit, kann längerfristig in Investitionsausfällen münden.

5.4 Projektrisiken

Die Risiken in Verbindung mit diesem Projekt sind:

- Fehlende oder unzureichende Managementunterstützung
- Fehlendes oder unzureichendes Verständnis der Mitarbeitenden für Sicherheitsthemen oder Unwille sich diesen Themen anzunehmen
- Fehlende Bereitschaft zur Optimierung von allfällig bestehenden Prozessen oder der Einführung von neuen Prozessen
- Fehlende Ressourcen um die notwendigen Projektarbeiten wahrzunehmen

5.5 Abhängigkeiten

Es bestehen gegenwärtig keine bekannten Abhängigkeiten zu anderen Projekten.

Abbildungsverzeichnis

Tabellenverzeichnis

Anhänge

A Sicherheits-Politik

Vgl. beiliegende Datei «Anhang A Sicherheits-Politik.pdf»

B Risikoportfolio

Vgl. beiliegende Datei «Anhang B Risikoportfolio.pdf»

C Statement of Applicability (SoA)

Vgl. beiliegende Datei «Anhang C SoA.pdf»

D RestRisk Akzeptanz

Vgl. beiliegende Datei «Anhang D RestRisk Akzeptanz.pdf»