**x-tention Unternehmensgruppe**

## Ihr Kontakt zu x-tention


**x-tention Informationstechnologie**
AT +43 7242 2155 office@x-tention.at
DE +49 8214 559 0320 office@x-tention.de
CH +41 43 222 60 22 info@x-tention.ch
UK +44 203 983 9860 hello@x-tention.co.uk

**soffico**
DE +49 821 455 901 00 info@soffico.de

**InterComponentWare**
DE +49 6227 385 0 info@icw.de
US +1 650 281 2872 info@icw-global.com

**FAKTOR D consulting**
DE +49 821 56 74 74 34 info@xd-consulting.de

**it for industries**
AT +43 7242 2155 0 office@itforindustries.at


x-tention.com

**Michael Punz**
Informationssicherheit & Datenschutz

**Telefon** +43 7242 2155 6325
**Mobil** +43 664 80009 6325
**E-Mail** michael.punz@x-tention.at


# ISMS-Aufbau im Krankenhaus

**Wie geht man ein ISMS-Projekt im Krankenhaus an?**

Seit der Verabschiedung der NIS-Richtlinie müssen Krankenhäuser, die als Betreiber wesentlicher Dienste (KRITIS) eingestuft werden, ein Informationssicherheits-Managementsystem (ISMS) aufbauen. x-tention unterstützt Sie bei der Projektplanung, dem ISMS-Aufbau und der Einführung mit fachlichem Know-how sowie langjähriger Erfahrung.

# Das ISMS-Projekt

## Worauf muss ich achten?

Der Aufbau eines ISMS ist kein einmaliges Projekt, das einmal umgesetzt und anschließend abgeschlossen ist. Ein ISMS muss laufend betrieben, aktualisiert und erweitert werden, denn auch die Bedrohungen und Risiken verändern sich ständig.

### Welcher Detailgrad ist beim Aufbau notwendig?

Beim initialen ISMS-Aufbauprojekt ist es wichtig, sich nicht im Detail zu verlieren. Starten Sie das ISMS in einem „Basis-Setup“ und ergänzen Sie das System im Laufe der Zeit mit weiteren Details.

**Praxistipp**
Gerade am Beginn eines ISMS gilt, dass weniger oft mehr ist. Wenn Sie Ihre Organisation von Beginn an mit einem „ausgewachsenen“ ISMS überfordern, ist die Wahrscheinlichkeit groß, dass dieses nicht gelebt wird und zu einem „Papiertiger“ in der Schublade mutiert.

### Wie sieht der Geltungsbereich/Scope aus?

Im Krankenhausbereich orientiert sich der Scope an den Kernprozessen zur medizinischen Versorgung von Patienten. Üblicherweise sind dies die fünf Kernprozesse Aufnahme, Diagnose, Therapie, Pflege und Entlassung. Sämtliche Richtlinien, Prozessbeschreibungen und Dokumentationen sind auf diesen Scope abzustimmen, wodurch auch ersichtlich wird, dass die IT alleine ein solches Thema nicht vollumfänglich bewältigen kann.



# Projekt-umsetzung

# Die Projektumsetzung

## Was sind die konkreten Schritte beim ISMS-Aufbau?

Ein ISMS-Projekt ist kein reines IT-Thema und betrifft beinahe alle Fachbereiche eines Krankenhauses. Im Kernteam sollten sich neben der IT auch Vertreter aus der Medizin- und Haustechnik sowie aus dem Datenschutz und dem Personalwesen wiederfinden. Für das Gelingen eines derartigen Projektes ist es außerdem von großer Wichtigkeit, dass dieses vom obersten Management aktiv mitgetragen und als wichtiges Thema kommuniziert wird. Zudem sollte bei der Erstellung von Mitarbeitervorgaben nicht die frühzeitige Einbindung des Betriebsrates vergessen werden.

### 1. Projekt starten

Zum Projektbeginn erfolgt ein gemeinsamer Kick-off-Termin mit Vertretern aller relevanten Fachbereiche (IT, Medizin- und Haustechnik, Datenschutz, Personalwesen usw.) und dem obersten Management. Bei diesem Termin werden der Projektauftrag, der Projektplan und die jeweiligen Arbeitspakete vorgestellt.

**Praxistipp:**

Nur mit einem klaren Bekenntnis des obersten Managements zur Wichtigkeit eines derartigen Projektes ist ein erfolgreicher ISMS-Aufbau möglich.

### 2. Prozessanalyse durchführen

Anschließend erfolgt eine Analyse der Geschäftsprozesse und der medizinischen Kernprozesse. Dazu werden sämtliche Supportprozesse im Haus, die für die Sicherstellung der Kernprozesse (Aufnahme, Diagnose, Therapie, Pflege und Entlassung) notwendig sind, identifiziert.

Darauf aufbauend werden in einem weiteren Schritt die kritischen Prozesse erhoben. Für jeden als kritisch bewerteten Prozess wird zudem ermittelt, welche IT-Unterstützung zur dauerhaften Serviceerbringung notwendig ist (zum einen IT-Anwendungen aus Anwendersicht und zum anderen IT-Komponenten aus IT-Infrastruktur-Sicht). Typische IT-Anwendungen im Krankenhaus, die hier betrachtet werden, sind zum Beispiel KIS, LIS, RIS, PACS, DMS, OP-Planungssystem, Transportlogistik usw.

**Praxistipp:**

Neben den üblichen Kernapplikationen im Krankenhaus sind auch IT-Systeme und Komponenten aus den Bereichen Medizintechnik, Versorgungstechnik (z. B. Wasser- und Energieversorgung), Kommunikationstechnik (z. B. Rufsysteme und Telefonie) und Informationstechnik (z. B. Domänen-Controller, IP-Datennetzwerke und Drucker) zu beachten.

### 3. Risikomanagement aufbauen

Auf Basis der durchgeführten Geschäftsprozessanalyse kann nun eine Risikoanalyse der kritischen Prozesse erfolgen. Es werden Risikokataloge erstellt, die sich aus den Anforderungen gängiger Normen (z. B. ISO/IEC 27001 oder 27002) sowie konkreter Serviceprozesse (z. B. Absicherung der Übertragungswege vom und zum Service) ableiten lassen.

Alle identifizierten Risiken werden in ein zentrales Informationssicherheits-Risikomanagementsystem überführt. Nach ausführlicher Analyse und Bewertung werden geeignete Maßnahmen zur Risikobehandlung entwickelt.

**Praxistipp:**

Beim initialen Aufbau eines Informationssicherheits-Risikomanagementsystems sind oftmals einfache Tabellen zur Dokumentation und Bewertung von Risiken ausreichend. Wichtig ist vielmehr, dass Sie eine nachvollziehbare Risikobewertungs-Systematik entwickeln und die jeweilige Bewertung, die Auswirkung und die Eintrittswahrscheinlichkeit in eigenen Worten begründen.

## 4. Vorgaben definieren

Ein jedes ISMS benötigt entsprechende Leit- bzw. Richtlinien, die einerseits generelle Vorgaben enthalten (z. B. Rollen, Verantwortlichkeiten, Management Commitment usw.), aber auch spezifische Regeln definieren (z. B. Entscheidungskompetenz eines Mitarbeiters).

### Praxistipp:

Derartige Leit- bzw. Richtlinien sollten nicht „das Blaue vom Himmel" enthalten, sondern der Wahrheit und Realität entsprechen. Zudem sollen Vorgaben auch für die Mitarbeiter „einhaltbar" und nicht praxisfremd sein. Bitte beachten Sie, dass Vorgaben auch regelmäßig auf Einhaltung kontrolliert werden sollten.

## 5. Abläufe dokumentieren

Parallel zur Prozessanalyse erfolgt die Dokumentation der Prozesse und Abläufe. Meistens gibt es bereits gelebte Prozesse, die jedoch großteils nicht oder unzureichend dokumentiert sind. Viele der zu dokumentierenden Prozesse betreffen primär die IT: beispielsweise das Zugriffsmanagement (z. B. Active Directory), die Security-Systeme (z. B. Firewall, Virenschutz, Verschlüsselung, Logging, Monitoring), das Anforderungs- und Beschaffungsmanagement (z. B. Inventar, IT-Systeme), Backup und Recovery, das Change Management (z. B. Prüfung und Freigabe von Änderungen), die Dokumentation der Infrastruktur (z. B. Rechenzentrum, Netzwerk und Zentralkomponenten), das Patch- und Schwachstellen-Management (z. B. Testen und Ausrollen von Security Patches), der Umgang mit Sicherheitsvorfällen sowie das Personalmanagement (z. B. Berechtigungsanpassung bei Ein- und Austritt von Mitarbeitern).

### Praxistipp:

Führen Sie mit den jeweiligen Fachabteilungen Workshops in kleinen Gruppen durch und dokumentieren Sie in einem ersten Schritt den Ist-Stand. Nehmen Sie eventuelle Abweichungen in das Informationssicherheits-Risikomanagement auf und behandeln Sie diese dort weiter.

## 6. Notfallpläne erstellen

Die Erstellung von Notfallplänen ist in einem Krankenhaus unerlässlich, denn die Patientenversorgung muss unter allen Umständen gewährleistet sein (zum Beispiel Stromausfall, Pandemie usw.). Daher ist nicht nur die Erstellung, sondern auch die Durchführung regelmäßiger Übungen Pflicht. Neben herkömmlichen Notfallszenarien wie zum Beispiel Brand sollten auch IT-bezogene Notfallszenarien betrachtet werden (z. B. Ausfall aller Rechenzentren).

### Praxistipp:

Vergessen Sie nicht, Ihre Notfallpläne an mehreren Stellen im Haus auch in ausgedruckter Form griffbereit zu halten. Denn bei einem Komplettausfall der IT stehen Dokumente in digitaler Form nicht zur Verfügung.



## 7. Mitarbeiter schulen

Die wichtigsten Vorgaben müssen in der Organisation bekannt sein. Jedem Mitarbeiter muss klar sein, was er darf und was verboten ist bzw. muss er verstehen, warum etwas verboten ist. Ohne ein praxistaugliches Schulungskonzept kann kein durchgängiges Sicherheitsniveau in Ihrem Haus erreicht bzw. dauerhaft sichergestellt werden!

### Praxistipp:

Aufgrund der großen Mitarbeiteranzahl im Gesundheitswesen hat sich eLearning für die breite Masse als praxistaugliches Mittel der Wahl etabliert. Mitarbeiter können dadurch selbst entscheiden, wann und wo sie eine Schulung absolvieren und werden nicht aus der Arbeit „herausgerissen", wenn sie eigentlich keine Zeit für eine Schulung haben. Zudem liefern eLearning-Systeme einen einfachen Nachweis über die Teilnahme (anstelle einer Unterschriftenliste). Führungskräfte können zusätzlich in Form von Workshops geschult werden, damit sie das Know-how in die jeweiligen Fachbereiche weitertragen können.

## 8. ISMS kontinuierlich verbessern

Nach erfolgter Einführung eines ISMS muss dieses gelebt und kontinuierlich verbessert bzw. erweitert werden. Dabei sind mehrere Vorkehrungen zu treffen, wie zum Beispiel die Definition von messbaren Kennzahlen (z. B. Wie viele Mitarbeiter nehmen an den Schulungen teil?) oder die Festlegung von Audits (z. B. Überprüfung von Berechtigungen im KIS). Durch die Auswertung von Kennzahlen und Audits lässt sich ein ISMS messbar machen, steuern und kontinuierlich verbessern. Zudem sollte auch das oberste Management aktiv in die Verbesserung des ISMS eingebunden werden. Dazu eignet sich am besten ein jährlicher Management Review, also ein jährlicher Ist-Status des ISMS mit den Ergebnissen aller Audits und den Kennzahlen sowie Verbesserungsvorschlägen.

### Praxistipp:

Versuchen Sie, Kennzahlen messbar zu machen und grafisch darzustellen. Aussagekräftige Visualisierungen stellen optimale Entscheidungsgrundlagen für das Management dar.

# Erfahrungen & Referenzen

# Tipps und Erfahrungen

## Aus der Praxis

- Eine sehr nützliche Grundlage für den ISMS-Aufbau in einem Krankenhaus ist der „Branchenspezifische Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus“ (B3S) von der Deutschen Krankenhausgesellschaft.
- Der Aufbau des Informationssicherheits-Risikomanagements und die Erstellung der Notfallpläne stellen in der Praxis meist die größten Hürden dar. Ein Informationssicherheits-Risikomanagement ist in vielen Fällen nicht vorhanden und muss von der grünen Wiese weg aufgebaut werden, ist also auch für das Management meist ein neues Thema. Notfallpläne sind zwar in vielen Fällen vorhanden, aber oft nicht vollständig bzw. veraltet oder werden nicht gelebt.
- Aufgrund der großen Mitarbeiteranzahl in Krankenhäusern werden Mitarbeiterschulungen zu den Themen Informationssicherheit und Datenschutz gerne vernachlässigt. Mit Ende der Übergangsfrist zur DSGVO ist die Wichtigkeit und Bedeutung von Schulungen ins Bewusstsein gerückt und hat zu einem Umdenken geführt. eLearning-Plattformen haben sich als ideale und praxistaugliche Lösung herauskristallisiert.
- Die Überführung der definierten Vorgaben, Abläufe und Prozesse in den alltäglichen Krankenhausbetrieb stellt eine größere Herausforderung dar und erfordert viel Fingerspitzengefühl.
- Der ISMS-Aufbau ist kein reines IT-Thema, dennoch betreffen viele Arbeitspakete eines ISMS-Aufbaus die IT direkt und müssen von IT-Mitarbeitern umgesetzt werden. Oftmals sind die personellen Ressourcen auf den technischen IT-Betrieb ausgerichtet, das Thema ISMS betrifft jedoch zum Großteil organisatorische Aspekte. Zudem stehen in vielen Fällen kaum mehr personelle Ressourcen für den dauerhaften und nachhaltigen Betrieb eines ISMS in der IT zur Verfügung. Daher empfiehlt es sich, hierfür einen internen oder externen Informationssicherheitsbeauftragten (CISO) einzusetzen und als eigene Stabsstelle direkt der Geschäftsführung zuzuordnen.

# Auswahl an Kundenreferenzen

## Leopoldina Krankenhaus der Stadt Schweinfurt GmbH

„In Zusammenarbeit mit x-tention wurde in organisierter und nachhaltiger Weise ein ISMS in unsere kritischen Prozesse integriert. Von Anfang an war das Projekt durch eine knappe Zeitvorgabe geprägt. Die rasche und unkomplizierte Zusammenarbeit mit x-tention war deshalb eine wertvolle Unterstützung für uns. Durch die von x-tention bereitgestellten ISMS-Vorlagen konnten wir den Aufwand zum Aufbau eines ISMS deutlich reduzieren, da die Anpassungen der Dokumente direkt von den Fachbereichen durchgeführt und anschließend zum Leben erweckt wurden. Die breite Erfahrung aus der Praxis und das flexible Eingehen von x-tention auf die Begebenheiten in unserem Krankenhaus haben dazu geführt, dass in kurzer Zeit ein ISMS aufgebaut wurde, das optimal zu uns passt. Das Engagement von allen Beteiligten wurde am Ende durch ein ausgezeichnetes Resultat beim Nachweis-Audit durch die Prüfstelle belohnt."

Thomas Balling MSc | Geschäftsbereichsleitung IT

## SRH IT Solutions GmbH

„Die Vorlagen von x-tention waren uns eine große Hilfe, in unserem KRITIS-Haus in Gera ein nachhaltiges ISMS aufzubauen. Wir konnten viel Zeit und Aufwand durch die hervorragend aufgebauten Vorlagen sparen, die inhaltlich umfassend und branchenspezifisch aufgebaut waren. Damit konnten wir die gemäß § 8a BSIG geforderten Nachweise bis 30.06.2019 erfolgreich und zeitgerecht erbringen."

Dr. Stefan Müller | CISO

## Marienhospital Stuttgart

„Mit dem Vorlagenpaket und dem Know-how von x-tention ist es gelungen, zügig und ressourcenschonend entsprechende Vorgaben und Prozesse im Unternehmen zu definieren und ein praxistaugliches ISMS aufzubauen."

Stephan Rühle | Geschäftsbereichsleitung IT/MTECH

## Klinikum Hanau

„Im Zuge der NIS-Richtlinie wurde im Klinikum Hanau ein ISMS aufgebaut, um die neuen gesetzlichen Anforderungen zu erfüllen. Dabei wurde auf x-tention als kompetenter Berater zum Thema ISMS zurückgegriffen. Durch die von der Firma x-tention bereitgestellten Vorlagen konnte der Aufwand zur Einführung eines ISMS deutlich minimiert werden. Das positive Resultat bei der Nachweisprüfung bestätigte die gute Zusammenarbeit und den Erfolg des Projektes."

Hüseyin Gökceoglu | IT-Leiter

# Das Vorlagen-Komplettpaket

## Das Ergebnis jahrelanger Erfahrung — für Ihren Erfolg

x-tention stellt seinen Kunden Vorlagen für Richtlinien, Prozessbeschreibungen und andere notwendige Dokumente bereit und passt diese individuell an die Bedürfnisse und Gegebenheiten der jeweiligen Organisation an.

### Sicherheitsrichtlinien

Erstellung zentraler ISMS-Dokumente (z. B. Informationssicherheitspolitik, Nutzungsrichtlinien usw.)

### Prozessbeschreibungen

Definition der geforderten Informationssicherheitsprozesse (z. B. Backup-Konzept, Patch Management, Security Incident Management usw.)

### Rollen und Verantwortliche

Erstellung von Rollendefinitionen, Rollenzuordnungen, Stellvertreter-Regelungen usw.

### Informationssicherheits-Risikomanagement

Methodik zur Risikoidentifikation, -bewertung und -behandlung, Dokumentation von Risiken und Maßnahmen

### Awareness-Programm

Erstellung eines Awareness-Konzepts, Schulung von Mitarbeitern zu Themen der Informationssicherheit

### Auditplanung

Erstellung eines Auditprogramms sowie einer Vorlage für Auditberichte, Definition von internen und externen Audits

### Kennzahlen

Definition und regelmäßige Erhebung von Kennzahlen, Einleiten von Verbesserungsmaßnahmen

### Management Review

Regelmäßige Berichterstattung an das Management, Einleiten von Verbesserungsmaßnahmen