



White Paper

Compliance verbessern durch ISO 27001 & ISMS

Information-Security-Management-Systeme
Basis für die erfolgreiche ISO 27001 Zertifizierung

Reduzierung von Haftungsrisiken
speziell für Führungskräfte im eHealth

AuthentiDate International AG
Rethelstraße 47
40237 Düsseldorf / Germany
Fon +49 (0)211 – 43 69 89 0

info@authentidate.de
www.authentidate.de



© 2009-2011 AuthentiDate International AG (alle Rechte vorbehalten)

Vervielfältigung nur mit ausdrücklicher Genehmigung der AuthentiDate International AG. Alle genannten Marken sind Marken ihrer jeweiligen Eigentümer. Irrtümer, Änderungen und Verfügbarkeit bzgl. genannter Produkte, Leistungen, Eigenschaften und Nutzungsmöglichkeiten vorbehalten. Produkte und Services werden durch die AuthentiDate Deutschland GmbH bereitgestellt. AuthentiDate übernimmt keine Gewähr für die Richtigkeit von Angaben Dritter über Eigenschaften, Leistungen und Verfügbarkeit. Im Zuge der Produktentwicklung behält sich AuthentiDate das Recht vor Änderungen an Produkten und Leistungen auch ohne vorherige Benachrichtigung vorzunehmen. Keine der Ausführungen und Darstellungen stellen eine Rechtsberatung dar oder dürfen in solcher Weise interpretiert werden. Im Fall von Abweichungen zu, in diesem Dokument in Zusammenhang stehenden Vertragsdokumenten und allgemeinen Geschäftsbedingungen der AuthentiDate, gehen die Vertragsdokumente bzw. allgemeinen Geschäftsbedingungen diesem Dokument stets vor.

Stand der Dokumentation: Jan. 2011, Version 1.5

Fragen und Anregungen senden Sie bitte an obige Kontaktangaben.

Inhalt

1.	Executive Summary	4
2.	Grundlagen ISO 27001.....	7
2.1.	Was verbirgt sich hinter ISO 27001	7
2.2.	Warum bei ISO 27001 Zertifizierungen branchenspezifisches Fachwissen unentbehrlich ist.....	7
2.3.	Kosten-Nutzen Betrachtung - Warum sich Investitionen in ISO 27001 Zertifizierungen lohnen	9
2.4.	ISO 2700x Standards und deren Zusammenhang	10
3.	Informations-Sicherheits-Management-Systeme (ISMS)	11
3.1.	Schritte zur Umsetzung einer ISO 27001 Zertifizierung	12
3.1.1.	Benötigte Ressourcen zur Umsetzung eines ISMS.....	13
3.1.2.	Vorarbeiten zur Einrichtung eines ISMS	13
3.2.	Einrichtung eines ISMS.....	14
3.3.	Die ISO 27001 Zertifizierung – Das Audit	15
4.	Über AuthentiDate	16
5.	Legal Disclaimer	17

1. Executive Summary

Durch die zunehmende Digitalisierung der geschäftlichen Abläufe nimmt die Komplexität von Prozessen täglich zu. Insbesondere das Gesundheitswesen nimmt hier mit der Einführung der elektronischen Gesundheitskarte eine Vorreiterrolle ein. Viele der Prozesse sind dabei höchst unternehmenskritisch. D.h. wenn diese unplanmäßig verlaufen oder ausfallen entsteht unverzüglich ein nur schwer oder gar nicht regulierbarer Schaden für das Unternehmen bzw. die Organisation.

Gleichzeitig steigt, nicht nur im Gesundheitswesen, die Menge der sensiblen personenbezogenen Daten, die verarbeitet, weitergeleitet und langfristig vorgehalten werden müssen.

Für Führungskräfte in Krankenhäusern, Rehabilitationszentren, bei Krankenkassen, Krankenversicherungen und auch Einkaufsgemeinschaften und auch der Zulieferindustrie wird daher sowohl die Prozess-, als auch Datensicherheit immer schwerer kontrollierbar.

Die Verantwortlichen müssen sicherstellen, dass die Informationssicherheit zu jedem Zeitpunkt gewährleistet ist, um eigene Haftungsrisiken zu minimieren.

Hierbei gilt es für die Verantwortlichen nicht nur unbeabsichtigte Fehler zu vermeiden, sondern auch absichtlichen Manipulationen von Prozessen und Daten vorzubeugen.

Schäden durch nicht verfügbare Prozesse, wie z.B. nicht funktionierende IT gehören hierzu genauso, wie die Veröffentlichung von sensiblen Patientendaten. In beiden Fällen entsteht der Organisation ein Schaden. In einem Fall dadurch, dass eine Leistung nicht erbracht werden kann und somit Umsatzausfälle zu verzeichnen sind, im anderen Fall durch Schadensersatzklagen oder Imageschaden.

Um ein höchstmögliches Maß an Informationssicherheit in allen Facetten sicherzustellen hat sich in der Praxis der Einsatz von Informations-Sicherheits-Management-Systemen (ISMS) bewährt. Die Vorgehensweise für die Einrichtung eines ISMS ist mittlerweile in internationalen Standards festgeschrieben. Die Konformität mit diesen Standards ist sogar zertifizierbar, so dass hierüber ein Nachweis gegenüber Dritten erbracht werden kann. Der meist verbreitete Standard dieser Form ist der ISO/IEC 27001:2005; kurz ISO 27001

Die Einrichtung eines ISMS bietet Verantwortlichen in Unternehmen und Organisationen gleich mehrere Vorteile:

1. Erkennen von bislang verborgenen Sicherheitslücken im Prozess

Bereits während der Einrichtung des ISMS werden Unternehmensprozesse umfänglich erfasst und dokumentiert. Somit werden Fehler im Prozess direkt erkannt und können behoben werden. (z.B. fehlendes 4-Augen-Prinzip bei einer kritischen Applikationen)

2. Dauerhafte Transparenz für Prozesse

Durch die Prozessdokumentation sind alle Prozesse transparent. Notwendige Prozessänderungen können schnell umgesetzt werden.

3. Kennzahlen zur schnellen Kontrolle

Bei Einrichtung eines ISMS werden Kennzahlen zur Prozesskontrolle eingeführt. Die Verantwortlichen müssen nur ein Minimum an Arbeit aufwenden, um die Ordnungsmäßigkeit der Prozesse zu überwachen. Die Kontrolle der Kennzahlen ermöglicht bereits eine gute Prozessüberwachung ohne ins Detail zu gehen.

4. Substanzielle Schadensbegrenzung und -reduzierung durch Früherkennungssystem

Durch die Verwendung von Kennzahlen können Risiken, Prozessfehler, Datenverluste und –manipulationen schneller erkannt und Gegenmaßnahmen ergriffen werden. Zusätzlich werden durch regelmäßige Reviews und Kennzahlenabgleiche über einen längeren Zeitraum unternehmensspezifische Vergleichswerte ermittelt. Das ISMS verbessert somit quasi selbst die Aussagekraft der Kennzahlen, da auch kleinste Abweichungen von den Standards sofort erkannt werden.

5. Kostenreduktion durch nachweisbare Reduktion von Schadensfällen und Unternehmensrisiken

Da die Einrichtung eines ISMS im Allgemeinen immer mit einer ISO 27001 Zertifizierung durch unabhängige Dritte abgeschlossen wird, erhält die Organisation einen anerkannten Nachweis zur Sicherstellung der Informationssicherheit. Dieser kann z.B. gegenüber den Haftpflichtversicherern zur Reduktion von Versicherungspolicen verwendet werden.

6. Positive Außenwirkung

Die ISO 27001 Zertifizierung stellt ein allgemein anerkanntes Gütesiegel dar und kann daher gegenüber Geschäftspartnern und Kunden als „Verkaufsargument“ verwendet werden.

Bei Ausschreibungen im eHealth Markt wird die Einführung eines ISMS (oder darauf aufsetzend eine ISO 27001 Zertifizierung) häufig als Selektionskriterium verwendet.

7. Reduzierung des Haftungsrisikos für Führungskräfte

Schnelleres Erkennen von Fehlern und Eingreifen mindert die Haftungsrisiken für Prozessverantwortliche und Führungskräfte. Zusätzlich stellt die Einrichtung eines ISMS und ISO 27001 Zertifizierung einen Nachweis darüber dar, dass die Führungskraft ihrer Pflicht zur Sicherung der Informationssicherheit bestmöglich nachgekommen ist. Falls dennoch Schadensfälle eintreten sollten, können die Verantwortlichen nachweisen, dass sie ihrer Sorgfaltspflicht nachgekommen sind und bestmöglich Maßnahmen ergriffen haben, um diesen Schadensfall zu verhindern.

2. Grundlagen ISO 27001

2.1. Was verbirgt sich hinter ISO 27001

Durch eine ISO 27001 Zertifizierung kann der Nachweis erbracht werden, dass unabhängige Dritte die Erfüllung von Compliance Anforderungen nach festgelegten Kriterien geprüft und bestätigt haben. Daher stellt eine ISO 27001 Zertifizierung ein bedeutendes und allgemein anerkanntes Hilfsmittel zur Reduzierung von Haftungsrisiken für alle Verantwortlichen in eHealth Geschäftsprozessen dar.

Der Focus von ISO 27001 liegt darauf, die Rahmenbedingungen zu definieren, nach welchen ein ISMS (Informations-Sicherheits-Management-System) aufgesetzt und betrieben werden muss, um darauf basierend die ISO 27001 Zertifizierung erfolgreich zu durchlaufen. Der ISO 27001 Standard liefert damit quasi einen Kriterienkatalog für die „Zertifizierung“ eines ISMS.

Spricht man davon, dass sich ein Unternehmen nach ISO 27001 zertifizieren lassen will, so verbirgt sich dahinter nichts anderes als der Aufbau eines ISMS, welches später von unabhängigen Dritten nach festgelegten Kriterien geprüft und bestätigt wird. Bei erfolgreicher Prüfung und Bestätigung ist die ISO 27001 Zertifizierung anschließend das Resultat.

Der Aufbau eines ISMS bildet das Herzstück einer ISO 27001 Zertifizierung.

In Zusammenhang mit Informationssicherheit spricht man in der Regel vom ISO 27001 Standard. Dies gibt jedoch genau betrachtet nur einen Teilaspekt wieder. Der Standard ISO 27001 wird durch eine ganze Reihe weiterer Standards ergänzt. ISO 27001 alleine ist im Grunde überhaupt nicht anwendbar. Daher spricht man häufig auch von der ISO 27000 Familie oder von ISO 2700x.

2.2. Warum bei ISO 27001 Zertifizierungen branchenspezifisches Fachwissen unentbehrlich ist

ISO Richtlinien sind grundsätzlich branchenneutral gefasst. Die ISO Richtlinien definieren daher aus einer Art Vogelperspektive welche Prozesse, Kennzahlen, Kontrollzahlen, etc. herangezogen werden sollen, um die Informationssicherheit in einem Unternehmen bzw. in einer Organisation langfristig zu gewährleisten.

Wie man sich leicht vorstellen kann, sind die Prozesse und Kennzahlen meist branchenspezifisch geprägt. Daraus ergibt sich, dass jede Branche selbstverständlich auch ihre „eigenen“ kritischen Prozesse und Kennzahlen hat. Ein Prozess, der nicht ordnungsgemäß (also wie geplant) abläuft kann in einer Branche das gesamte Unternehmen lahm legen und Ausfälle in Millionenhöhe mit sich ziehen und in einer anderen Branche so gut wie gar keine Auswirkungen auf die Geschäftstätigkeit haben.

Somit sollte derjenige, der eine ISO 27001 Zertifizierung leitet und für das Unternehmen den Aufbau eines ISMS realisiert zwingend über umfangreiche ISO-bezogene Branchenkenntnisse verfügen. Dabei ist es wichtig, dass die Personen Kenntnisse und Erfahrungen aus der praktischen Umsetzung einer ISO 27001 Zertifizierung in den jeweiligen Branchen gesammelt haben. Nur so können auch wirklich die kritischen Prozesse identifiziert und durch das ISMS abgedeckt werden.

Eine ISO 27001 Zertifizierung ohne branchenspezifisches ISO-KnowHow führt leicht dazu, dass die wirklich kritischen Prozesse gar nicht identifiziert werden, falsche Kennzahlen herangezogen werden und somit keine Erhöhung der Unternehmenssicherheit und keine Minimierung von Risiken für das Unternehmen erzielt wird. Somit würden auch die Haftungsrisiken für die Verantwortlichen im Unternehmen nicht reduziert werden, was auch wesentlicher Aspekt und Zielsetzung einer ISO 27001 Zertifizierung ist.

Personen, die ISO 27001 Zertifizierungen durchführen und dazu ein ISMS aufbauen, sollten zwingend über umfangreiche praktische und branchenspezifische Kenntnisse der Compliance-Anforderungen verfügen.

Am Beispiel des Asset Managements (= Management schützenswerter Objekte) kann einfach und plakativ verdeutlicht werden, warum branchenspezifische ISO-Kenntnisse unabdingbare Voraussetzung für die schnelle und erfolgreiche Umsetzung einer ISO 27001 sind. Eine ISO Richtlinie gibt lediglich an, dass ein Asset Management erfolgen muss. D.h. sie legt fest, dass Objekte in Bezug auf Vertraulichkeit, Verfügbarkeit und Integrität geschützt werden müssen. Welche Objekte geschützt werden müssen und welchen Schutzbedarf sie haben variiert jedoch je nach Branche. Schützenswerte Objekte können in einem eHealth Prozess weit anders definiert sein, als in einem Prozess eines Energieversorgers. Die Identifizierung und Klassifizierung der schützenswerten Objekte ist daher stets branchenspezifisch vorzunehmen. Sie erfordert eine hohe branchenspezifische Expertise derjenigen, die das Unternehmen auf die ISO 27001 Zertifizierung und den zugehörigen Aufbau eines ISMS vorbereiten.

Speziell im Bereich eHealth hat die gematik eine Vielzahl von allgemeingültigen ISO Anforderungen konkretisiert und auf die branchenspezifischen Anforderungen im eHealth ausgerichtet.

Auch dies lässt sich am eben dargestellten Beispiel Asset Management gut verdeutlichen. Im eHealth kommt beispielsweise den Versichertendaten sehr hohe Bedeutung zu. Sie sind äußerst sensibel und daher besonders schützenswert. In anderen Branchen wird es hingegen andere Daten geben, die einen derart hohen Schutzbedarf aufweisen. So z.B. in der Automobilindustrie die Einkaufspreise der Zulieferindustrie. An diesem einfachen Beispiel wird deutlich, wie individuell bzw. branchenspezifisch eine ISO 27001 Zertifizierung ausgerichtet ist. Grundsätzlich beginnt jedoch bereits bei Konzeption und Umsetzung des ISMS die branchenspezifische Ausrichtung, da das ISMS die Basis für jede ISO 27001 Zertifizierung bildet.

2.3. Kosten-Nutzen Betrachtung - Warum sich Investitionen in ISO 27001 Zertifizierungen lohnen

Vielfach stellt sich die Geschäftsführung die Frage, ob sich die Investitionen in eine ISO 27001 Zertifizierung und den Aufbau eines ISMS lohnen. Diese Frage lässt sich fast immer mit einem klaren „JA“ beantworten. Und diese Antwort lässt sich bereits vor Beginn einer ISO 27001 Zertifizierung mit relativ wenig Aufwand belegen. Sowohl qualitativ als auch quantitativ kann vor Beginn einer ISO 27001 Zertifizierung ermittelt werden, welchen Nutzen ein Unternehmen bzw. eine Organisation von einer ISO 27001 Zertifizierung hat.

Hierzu können beispielsweise einige kritische Prozesse innerhalb der Organisation bzw. des Unternehmens ausgewählt werden. Innerhalb des Prozesses wird ein möglicher Schadensfall ausgewählt und näher betrachtet. Im eHealth könnte dies z.B. der Verlust von Patientendaten sein. Mit dem Verlust der Patientendaten treten bestimmte Folgeschäden und Haftungsrisiken für z.B. das Krankenhaus ein, welches die Daten „verloren“ hat, z.B. Schadensersatzforderungen des Patienten, Imageverlust des Krankenhauses etc.. In einer Vorstudie können diese Schadensfälle bewertet und somit monetär auch messbar gemacht werden. Anschließend wird bewertet inwieweit der Einsatz eines ISMS das Auftreten des Schadens vermeidet oder abmildert. Auf diese Weise kann ebenfalls monetär bewertet werden, wie hoch das Einsparpotential durch die ISO 27001 Zertifizierung und ISMS Einführung ist.

Eine ISO 27001 Zertifizierung auf Basis eines ISMS kann nachweisbar Kosten senken, da die Wahrscheinlichkeit von Schadensfällen sinkt.

Sehr gut deutlich wird dies auch am Beispiel von Versicherungspolicen, die Unternehmen für bestimmte Schadensfälle, darunter auch für Datenverluste, abschließen. Die Versicherungen richten ihre Versicherungsprämien in der Regel danach aus, wie hoch die

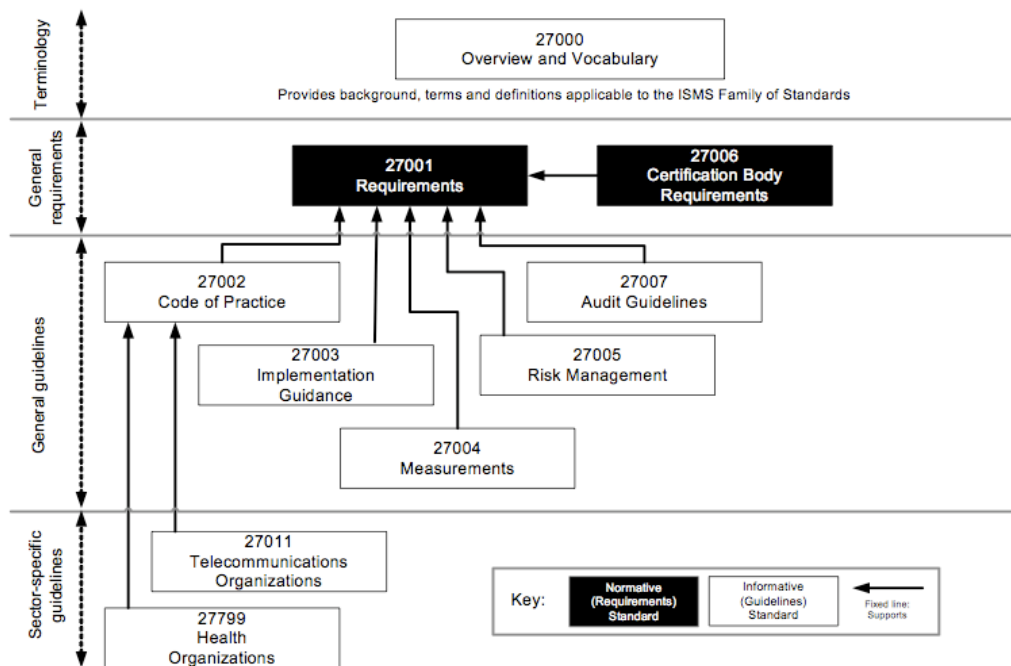
Wahrscheinlichkeit ist, dass der jeweils versicherte Schaden eintritt und sie somit in die Pflicht genommen würden den Schaden zu regulieren. Sobald das Unternehmen nachweisen kann, dass die Wahrscheinlichkeit, dass der Schaden eintritt reduziert wurde, z.B. durch organisatorische Maßnahmen, so wird auch der Beitrag für die Versicherungspolice sinken.

2.4. ISO 2700x Standards und deren Zusammenhang

ISO 27001 definiert die Grundanforderungen an ein ISMS. Bei Konzeption und Umsetzung des ISMS fällt jedoch schnell auf, dass einige Anforderungen in weiteren ISO Standards näher spezifiziert sind. D.h. es gibt zusätzliche Standards, die Teilaspekte definieren. So z.B. der ISO 27002; ein Leitfadern zur Implementierung von ISMS. Er definiert verschiedene Zielsetzungen und Kontrollziele, welche durch das ISMS erreicht werden müssen.

Aktuell sind sieben Standards für den Aufbau eines ISMS von Bedeutung. Dies sind die nachfolgend aufgelisteten:

- ISO 27000
 - Definitionen und Begriffe der Normenreihe
- ISO 27001
 - Definiert die Zertifizierungsanforderungen an ein ISMS (Informations-Sicherheits-Management-System) und hat den BS7799 abgelöst. Die ISO 27001 enthält Querverweise auf die ISO 27002 und die ISO 13335.
- ISO 27002
 - Ist ein Leitfadern zur Implementierung. Enthält Zielsetzungen sowie Kontrollziele und löst die ISO 17799 ab.
- ISO 27003
 - Befasst sich tiefergehend mit der Einführung eines ISMS. Die ISO 27003 befindet sich derzeit in der Entwicklung.
- ISO 27004
 - Definiert Kennzahlen für das ISMS. Die ISO 27004 befindet sich derzeit in der Entwicklung.
- ISO 27005
 - Unter dem Titel „Information-Security-Risk-Management“ werden Details zum IT-Risikomanagement beschrieben. Wurde im Juli 2008 veröffentlicht.
- ISO 27006
 - Beschäftigt sich speziell mit dem Thema Disaster Recovery. Ist noch nicht erschienen.
- ISO 2700x
 - Ist reserviert für weitere Veröffentlichungen.



Grafik1: Beziehung der ISO 2700x Standards untereinander

3. Informations-Sicherheits-Management-Systeme (ISMS)

Ein Informations-Sicherheits-Management-System, kurz ISMS, ist ein ganzheitlicher Ansatz, um sensible, unternehmenskritische Informationen langfristig und zu jedem Zeitpunkt mit der notwendigen Sorgfalt zu verwalten, um möglichst jeden Schaden vom Unternehmen bzw. der Organisation abzuhalten. Hierbei sollen Schäden aller Art vermieden werden. Das bedeutet: es sollen sowohl Schäden vermieden werden, die durch den Verlust oder Manipulation von Daten entstehen, also qualitativ und quantitativ relativ gut messbar sind, als auch immaterielle Schäden, wie z.B. ein Imageverlust des Unternehmens aufgrund einer Datenpanne. Hier gibt es gerade in jüngerer Zeit eine Reihe von Beispielen aus der Praxis, bei denen Datenpannen zu hohen Kosten geführt haben, da Kunden das Vertrauen in ein Unternehmen verloren und ihre persönlichen Daten anderen Anbietern anvertrauten.

Ein ISMS ist somit darauf ausgerichtet, sämtliche Prozesse eines Unternehmens, bei denen mit sensiblen Daten umgegangen wird kritisch zu untersuchen und derart zu dokumentieren und mit Qualitätskriterien zu versehen, dass eine kontinuierliche Kontrolle

erfolgen kann. Diese kontinuierliche Kontrolle soll ermöglichen, dass sofort bemerkt wird, wenn ein unternehmenskritischer Prozess außerhalb der definierten Kontrollziele abläuft und entsprechend unmittelbar eingegriffen und korrigiert werden kann. Auf diese Weise sollen Schäden im Idealfall vermieden oder zumindest auf ein Minimum reduziert werden.

Da kein Prozess ohne die Interaktion von Mitarbeitern ablaufen kann, müssen bei einem ISMS immer die Arbeitsabläufe der beteiligten Mitarbeiter mit einbezogen werden. Das heißt neben IT-Systemen, spielen Menschen und ihre kontrollierbaren und unkontrollierbaren Handlungen bei der Umsetzung eines ISMS eine wichtige Rolle.

3.1. Schritte zur Umsetzung einer ISO 27001 Zertifizierung

Wie beschrieben bildet das ISMS (Informations-Sicherheits-Management-System) das Herzstück einer ISO 27001 Zertifizierung. Vor Einrichtung des ISMS (und auch danach) sind eine Reihe von Aktivitäten erforderlich, um eine erfolgreiche ISO 27001 Zertifizierung zu erreichen. Das ISMS soll z.B. gewährleisten, dass hoch sensible Informationen, wie z.B. Patientendaten, langfristig sicher elektronisch verwaltet werden. Dies gilt sowohl für den Fall, dass die Daten intern weiterbearbeitet, weitergeleitet oder archiviert werden, als auch den Fall, dass die Daten an Externe distribuiert werden.

Häufig wird im Zusammenhang mit der Distribution an Externe auch die „Verkehrsfähigkeit“ der Daten betrachtet. Diese stellt sicher, dass Daten auch langfristig unverändert von Dritten als Information genutzt werden können und die Nutzung unabhängig von einem System, z.B. dem System in welchem die Daten erzeugt wurden, möglich ist. In diesem Bereich spielt der Einsatz elektronischer Signaturen und qualifizierter Zeitstempel gemäß Signaturgesetz eine große Rolle. Durch den Einsatz qualifizierter Zeitstempel kann z.B. unabhängig vom System auch nach Jahren (30 Jahre und länger) nachgewiesen werden, dass die Daten seit der Erstellung unverändert vorliegen.

Nicht zu verwechseln mit der Verkehrsfähigkeit ist die sichere Übertragung und Speicherung der elektronischen Daten. Hier sind die elektronischen Daten, z.B. durch Verschlüsselung, vor Zugriffen und/oder Manipulationen zu schützen.

Je nach Branche und Zielsetzung kann ein „fertiges ISMS“ aus unterschiedlichen Teilbereichen bestehen. Diese sind z.B. Policies, wie bestimmte Prozesse abzuwickeln sind, Dokumente, welche Sicherungsmechanismen beschreiben oder eine Dokumentation zu Kennzahlen, die die Qualität von Prozessen messbar machen. Hervorzuheben ist, dass für jedes Unternehmen bzw. Organisation individuell festgelegt werden muss, welche Dokumente, Kennzahlen,

Prozessanweisungen, etc. individuell erstellt werden und zum tragen kommen. Innerhalb der einzelnen Branchen ergeben sich zumeist eine Vielzahl von ähnlichen Qualitätsmaßstäben und Faktoren zur Bewertung der Sicherheit, weshalb eine Branchenexpertise wie schon skizziert unabdingbar ist. Der letzte Feinschliff der Beurteilungsfaktoren ist jedoch immer individuell für das jeweilige Unternehmen vorzunehmen und anzupassen.

3.1.1. Benötigte Ressourcen zur Umsetzung eines ISMS

Ein ISMS kann in Unternehmen und Organisationen nicht einfach durch ein zusätzliches Stück Software umgesetzt werden. Mit einem ISMS wird ein ganzheitlicher Ansatz verfolgt, welcher Hardware, Software, Prozesse und das Verhalten der Menschen, die in sämtliche Prozesse eingebunden sind, berücksichtigt.

Grundvoraussetzung für die erfolgreiche Umsetzung eines ISMS ist daher immer die Unterstützung des Managements. Dieses muss den Mitarbeitern klar signalisieren, dass das Aufsetzen eines ISMS und vor allem ein kontinuierlicher Review einen spürbaren Mehrwert für das Unternehmen bzw. die Organisation mit sich bringt. Das Management muss vermitteln, dass dieser Mehrwert sich substantziell für das Unternehmen auswirkt. Hierzu ist es häufig hilfreich sowohl dem Management als auch den Mitarbeitern einige ausgewählte Prozesse darzustellen, die im Rahmen der Risikoanalyse eines ISMS betrachtet werden. Wie auch im Bereich der Kosten-Nutzenbetrachtung erläutert, kann es zur Erhöhung der Akzeptanz sinnvoll sein, gemeinsam mit den Mitarbeitern Kosten-Nutzenbetrachtungen durchzuführen.

3.1.2. Vorarbeiten zur Einrichtung eines ISMS

Soweit die Unterstützung des Managements für die ISO 27001 Zertifizierung sichergestellt ist, kann mit den eigentlichen Vorarbeiten zur Einrichtung des ISMS begonnen werden.

Hierbei wird im Allgemeinen in vier Schritten gearbeitet:

1. Definition des Geltungsbereichs
Zunächst muss definiert werden für welchen Bereich des Unternehmens bzw. der Organisation das ISMS eingerichtet werden soll. Diese Abgrenzung ist wichtig, da sonst nicht lückenlos erfasst werden kann, welche Prozesse, Daten und Menschen an dem Projekt beteiligt sind.

Ein ISMS innerhalb eines Krankenhauses kann sich z.B. mit der Sicherheit von Patientendaten beschäftigen.

2. Bestandsaufnahme der Vermögenswerte
Um mögliche Schäden auch quantitativ bewerten zu können, ist es erforderlich alle Vermögenswerte zunächst exakt zu erfassen. Hierzu zählen selbstverständlich sowohl materielle als auch immaterielle Vermögenswerte, wie z.B. Patente und Intellectual Property eines Unternehmens. Im Bereich des eHealth stellen z.B. Patientendaten einen hohen, besonders schützenswerten Vermögenswert dar.
3. Durchführung einer Risikoanalyse
Zur Durchführung der Risikoanalyse stehen dem Team, welches das ISMS einführt, eine Reihe von standardisierten Verfahren zur Verfügung. So kann z.B. eine quantitative und/oder qualitative Risikoanalyse durchgeführt werden. Wendet man dies auf unser Beispiel der Patientenakten an, so kann ein Teilbereich der Risikoanalyse darin bestehen, die Wahrscheinlichkeit dafür zu ermitteln, dass Patientendaten absichtlich manipuliert werden.
4. Statement of Applicability und Umgang mit Risiken
In diesem letzten Schritt vor der eigentlichen Einrichtung des ISMS wird exakt untersucht, welche ISO Standards für den Geltungsbereich anwendbar sind. In diesem Schritt werden somit wichtige Grundlagen für eine erfolgreiche ISO Zertifizierung gelegt. Die Einhaltung der hier definierten Standards wird bei der ISO Zertifizierung im Detail geprüft.

3.2. Einrichtung eines ISMS

Die Einrichtung eines ISMS erfolgt durch eine Vielzahl an Teilprojekten. Hierzu gehören z.B. die Erstellung von Prozessdokumentationen und deren praktische Umsetzung. Mit den Prozessdokumentationen wird lückenlos die Erfassung, Verarbeitung und Speicherung aller Daten dokumentiert und geregelt, die in den Geltungsbereich des ISMS fallen.

Die Prozessdokumentation nimmt insofern einen wichtigen Stellenwert ein, als dass die Verantwortlichen stets wissen bzw. nachvollziehen können, wo sich Daten befinden und wie diese verarbeitet und gespeichert wurden. Hierauf aufsetzend können z.B. Kontrollkennzahlen ermittelt und festgelegt werden. Über diese Kontrollkennzahlen können die Verantwortlichen später schnell, automatisch und selbstständig jederzeit prüfen, ob Fehler im Prozess

vorliegen. Falls ja können unverzüglich Gegenmaßnahmen ergriffen werden und Schäden vom Unternehmen abgewendet werden.

Im Fall von Patientendaten können z.B. Kontrollzahlen definiert werden, mit deren Hilfe die Vollständigkeit im Archivsystem ermittelt und überprüft werden kann. Dies ist nur eine sehr einfache Maßnahme von vielen, um zu verdeutlichen, wie die Verantwortlichen in Unternehmen und Organisationen einfacher ihre Aufsichts- und Kontrollpflichten wahrnehmen können.

Die Einrichtung eines ISMS hilft Verantwortlichen dabei Ihre Kontroll- und Aufsichtspflicht einfacher auszuüben und bei Schadensfällen schneller zu reagieren.

Durch die Einrichtung eines ISMS können Verantwortliche nachweisen, dass sie ihrer Kontroll- und Aufsichtspflicht jederzeit nachgekommen sind.

Ziel bei der Einrichtung eines ISMS ist es, den Verantwortlichen in einer Organisation ein Instrument zur dauerhaften und lückenlosen Kontrolle von Prozessen an die Hand zu geben. Da die dauerhafte Kontrolle ein wesentliches Merkmal eines ISMS darstellt, ergibt sich automatisch, dass eine kontinuierliche Anpassung eines ISMS an geänderte Anforderungen und Strukturen unerlässlich ist.

Um neue Anforderungen berücksichtigen zu können, finden nach Einrichtung des ISMS regelmäßige Reviews statt. In bestimmten Intervallen werden die Maßnahmen kontrolliert und ggf. korrigiert. Zur einfacheren Kontrolle der Maßnahmen können ebenfalls Kennzahlen verwendet werden.

3.3. Die ISO 27001 Zertifizierung – Das Audit

Mit der Einrichtung eines ISMS hat das Unternehmen bzw. die Organisation bereits einen hohen Beitrag dazu geleistet, die Risiken und möglichen Schadensfälle zu reduzieren und die Transparenz in Bezug auf die Informationssicherheit zu erhöhen. An dieser Stelle könnte man den Prozess als abgeschlossen betrachten. Im Allgemeinen schließt sich jedoch hier die formale ISO Zertifizierung an. Diese wird in Form eines Audits durch speziell akkreditierte Gutachter durchgeführt.

Vor dem Audit sollte dieses mit Hilfe externer Berater noch einmal exakt durchgespielt werden und das ISMS auf Herz und Nieren geprüft werden. So vermeidet man unnötige und kostenintensive doppelte Audits.

Das Audit erfüllt zwei wichtige Funktionen. Zum einen wird durch einen formalen externen Prozess noch einmal die Sicherheit und

Vollständigkeit aller Maßnahmen überprüft. Eventuelle Lücken und Fehler können somit entdeckt werden. Das Unternehmen bzw. die Organisation gewinnt somit noch ein zusätzliches Maß an Sicherheit.

Zum anderen bietet eine ISO Zertifizierung einen hohen Marketing-Wert und unabhängigen Nachweis darüber, dass das Unternehmen sehr hohe Sicherheitsauflagen erfüllt.

Wie in der Kosten-Nutzenbetrachtung skizziert kann die ISO Zertifizierung z.B. gegenüber Versicherungsgesellschaften als Nachweis verwendet werden, um günstigere Policen abzuschließen.

Darüber hinaus wird das Unternehmen die ISO Zertifizierung zur Werbung nutzen. Gegenüber Kunden und Geschäftspartnern kann das Unternehmen bzw. die Organisation nachweisen, dass es vertrauenswürdig mit sensiblen Kunden- und Geschäftsdaten umgeht. So kann ein Krankenhaus nachweisen, dass die ihm anvertrauten Patientendaten sicher und vertraulich behandelt werden. Gerade in der heutigen Zeit stellt dies ein nicht unerhebliches Argument in der Abgrenzung zum Wettbewerb dar.

Die erfolgreiche ISO Zertifizierung stellt ein wichtiges Marketinginstrument dar. Sie bietet die Möglichkeit sich gegenüber Wettbewerbern abzugrenzen und Neukunden durch ein hohes Vertrauen in die Qualität des Unternehmens und der angebotenen Leistungen zu gewinnen.

4. Über AuthentiDate

AuthentiDate verfügt über langjährige Erfahrung in der Einführung von Informations-Sicherheits-Management-Systemen. Eine besonders ausgeprägte Branchenkompetenz besteht aufgrund zahlreicher Praxisprojekte im Gesundheitswesen. Hier ist AuthentiDate nicht nur mit den seit langen geltenden Vorschriften der Sozialgesetzgebung, sondern insbesondere auch mit den neuen Anforderungen, die sich aus der Einführung der elektronischen Gesundheitskarte ergeben, bestens vertraut.

AuthentiDate International AG (mit Sitz in Deutschland, Düsseldorf) wurde am 9. Nov. 2001 als erstes Unternehmen mit Schwerpunkt qualifizierte Zeitstempel von der Bundesnetzagentur (früher Regulierungsbehörde für Telekommunikation und Post) als akkreditierter Zertifizierungsanbieter nach neuem deutschem Signaturgesetz und europäischen Richtlinien akkreditiert. Damit bieten die von AuthentiDate International AG gelieferten Zeitstempel für alle elektronischen Daten den gesetzlich anerkannten höchsten Schutz in



High Security
Signaturgesetz

regtp Z 0 0 1 5

Form von qualifizierten elektronischen Signaturen mit Anbieterakkreditierung.

Qualifizierte Zeitstempel der AuthentiDate International AG entsprechen auch den Anforderungen der EU-Signaturrechtlinie. Sie können somit auch international für rechtssichere elektronische Prozesse verwendet werden.

Die AuthentiDate Deutschland GmbH, eine 100%ige Tochter der AuthentiDate International AG, liefert und entwickelt eigenständig herstellerunabhängige Softwarelösungen zur Integration von Zeitstempeln und personenbezogenen Signaturen in Geschäftsprozesse aller Art. Hierbei können sowohl qualifizierte als auch fortgeschrittene Signaturen und Zeitstempel genutzt werden.

5. Legal Disclaimer

Das vorliegende White Paper enthält ausschließlich unverbindliche technische und rechtliche Informationen. Irrtümer bleiben vorbehalten. Verbindliche technische Aussagen zu den einzelnen Produkten, die in diesem Dokument genannt werden, sind ausschließlich den jeweiligen Produktspezifikationen zu entnehmen.

AuthentiDate haftet nicht für die Aktualität, Korrektheit, Vollständigkeit oder Qualität, der in diesem Dokument enthaltenen Informationen. Haftungsansprüche, welche sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der hier dargebotenen Informationen bzw. durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht werden, sind grundsätzlich ausgeschlossen.

Rechtliche Aussagen sind in keinem Fall verbindlich. Im Fall von Abweichungen zu, mit diesem Dokument in Zusammenhang stehenden Vertragsdokumenten oder allgemeinen Geschäftsbedingungen der AuthentiDate, gehen die Vertragsdokumente bzw. allgemeinen Geschäftsbedingungen der AuthentiDate diesem Dokument stets vor.