
IT-Sicherheit im Krankenhaus

# Umsetzung von B3S für Krankenhäuser mit DocSetMinder

Krankenhäuser in Deutschland werden immer mehr in die Pflicht genommen, sich mit dem Schutz der verarbeiteten Daten und Informationen auseinanderzusetzen. Der Fokus liegt auf der Aufrechterhaltung der stationären Versorgung. Den Nachweis für die Umsetzung der notwendigen Maßnahmen können Verantwortliche über die Anwendung des Branchenstandards erbringen.

**Autor: Piotr W. Nürnberg,**
Allgeier GRC GmbH

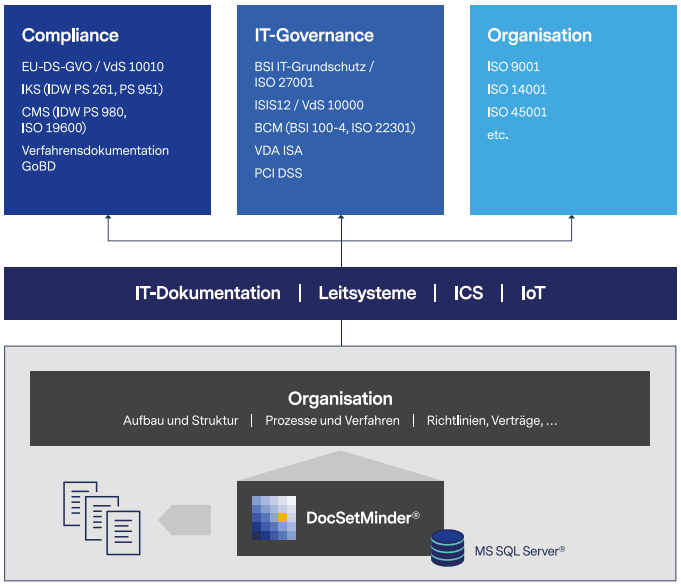
Die Etablierung eines Managementsystems für Informationssicherheit setzt eine entsprechende Priorisierung durch die Leitungsebene voraus. Diese muss für ein kompetentes Projektteam und Projektmanagement sorgen und die notwendigen Ressourcen bereitstellen. Durch die hohen normativen Anforderungen an das Dokumentenmanagement kommt der Auswahl einer ISMS-Software für die Dokumentation der Planung und Umsetzung des Informationssicherheitsprozesses eine wichtige Rolle zu.

## Strukturanalyse

Das Ziel der Informationssicherheit liegt im Schutz der Daten und Informationen selbst sowie der an ihrer Verarbeitung beteiligten Prozesse, Anwendungen, Dienste, Systeme, Kommunikation und Einrichtungen. Für die fortlaufende Inventarisierung dieser Assets bietet das ISMS-Tool DocSetMinder vorgefertigte, anpassbare Verzeichnisstrukturen und Dokumentvorlagen. Zum Aufzeigen der logischen Zusammenhänge zwischen der Aufbauorganisation (Organisationseinheiten, Verantwortlichkeiten), Ablauforganisation (Prozesse und Verfahren) und IT (passive und aktive Netzwerkkomponenten, Serversysteme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen, Gebäude, Gebäudesicherheit und Räume) werden Verknüpfungen genutzt.

## Risikomanagement

Das Modul „ISMS" in DocSetMinder orientiert sich unmittelbar an der High Level Structure der ISO 27001 und bietet neben vorgefertigten Dokumentvorlagen und Integration der branchenspezifischen Sicherheitsanforderungen ein effektives und effizientes Management der für die kritischen Dienstleistungen relevanten Risiken. Den Verantwortlichen steht eine aus der ISO 27005 abgeleitete Risikoanalyse zur Verfügung. Für die Risikoidentifikation können die mitgelieferten, erweiterbaren Kataloge (Gefährdungen und Schwachstellen) herangezogen werden. Die qualitative Bewertung des Risikos nach Schadenshöhe und Eintrittswahrscheinlichkeit erfolgt in einer 4x4-Matrix. Die Dimensionierung der Matrix sowie die zugrunde liegenden Parameter lassen sich organisationsspezifisch definieren. Im Rahmen der Risikobehandlung festgelegte technisch-organisatorische Maßnahmen können per Aufgaben- und Workflow-Funktion an einzelne Mitarbeiter oder Gruppen delegiert und der Arbeitsfortschritt getrackt werden.




## Reporting

Für die Überwachung des Informationssicherheitszustands im definierten Geltungsbereich des ISMS bietet DocSetMinder eine performante Reporting-Funktion mit fertigen Berichten für ein Audit nach B3S. Die Berichte können nach spezifischen Parametern (zum Beispiel Maßnahmenstatus) gefiltert und in gängige Formate, wie PDF, MS Word und Excel, HTML etc., exportiert werden.

## Fazit

Die Lösung DocSetMinder bildet den Informationssicherheitsprozess über alle Phasen (Plan, Do, Check, Act – PDCA) hinweg ab. Die im Modul „ISMS" enthaltenen Strukturen und Dokumentvorlagen orientieren sich an der für die Umsetzung der Anforderungen aus B3S vorgeschlagenen Schrittfolge und stellen ein für jede Organisation passendes Dokumentationsrahmenwerk dar. DocSetMinder ist Best Practice – und Sie sind jederzeit „Ready for Audit". ■

Mehr dazu hier

ALLGEIER GRC