IT-Sicherheit, Notfallmanagement und Datenschutz effizient umsetzen

# DocSetMinder: Ready for Audit

**IT-Sicherheit ist eine aufwändige und nicht zu unterschätzende Aufgabe. Eine Fülle von technischen und organisatorischen Maßnahmen müssen sorgfältig geplant, umgesetzt und zyklisch auf ihre Wirksamkeit überprüft werden. Die Lösung DocSetMinder der GRC Partner GmbH unterstützt bei der Etablierung der anerkannten Sicherheitsstandards in ihrem gesamten Lebenszyklus (PDCA).**

*Von Krzysztof Paschke, GRC Partner GmbH*

Bei der Vielzahl der gesetzlichen Auflagen und Normanforderungen ist es empfehlenswert, einen organisationsweiten, ganzheitlichen Planungs- und Dokumentationsansatz in Form eines „Integrierten Managementsystems“ (IMS) für die Umsetzung der IT-Sicherheits- und Datenschutzaspekte sowie einer Zertifizierung zu etablieren. Anstatt Normen, Standards oder gesetzliche Anforderungen einzeln zu planen und womöglich mit unterschiedlichen Tools zu realisieren, ist eine globale Betrachtung von enormem Vorteil.

## DocSetMinder

Die Compliance-Management-Software DocSetMinder der GRC Partner GmbH ist bereits im Jahr 2004 für die Etablierung von unterschiedlichen Normen und Standards im Unternehmen und der Behörde entwickelt worden. Der Funktionsumfang deckt alle Anforderungen der Normen an die Lenkung der geforderten Informationen ab. Dazu gehören zum Beispiel: Revisionssicherheit und Versionskontrolle, Protokollierung der Änderungen, Dokumentenkategorien (frei definierbar), Workflowmanagement, Aufgaben- und Maßnahmenplanung, Flussdiagrammdesigner (BPMN, ISO), Texteditor, Import-/Export-Schnittstelle und Reporting, Ausgabe der Dokumentation (Word, HTML), Jahresabschluss/Periodenabgrenzung, Volltextsuche sowie Mandantenfähigkeit.

Um die Mindestanforderungen der Sicherheitsstandards und Datenschutzgesetze (EU, Bund und Länder) effizient und vollständig umzusetzen und aktuell zu halten, stehen den Anwendern der Software diverse DocSetMinder-Module zur Verfügung. In Verbindung mit dem Microsoft SQL-Server als zentralem Repository ist DocSetMinder beliebig skalierbar und eignet sich für Unternehmen und Behörden jeder Größe. Durch den modularen Aufbau kann ein bereits umgesetzter Standard um zusätzliche Normen jederzeit zu einem „Integrierten Managementsystem“ erweitert werden.

### Modul „Unternehmens- und Behördenorganisation“

Die genaue Kenntnis der Unternehmens- und Behördenorganisation ist eine elementare Voraussetzung für die Durchführung der Strukturanalyse. Das Modul stellt die notwendigen Strukturen und Vorlagen für die Dokumentation der Aufbau- und Ablauforganisation eines Unternehmens oder einer Behörde in gewünschter Tiefe zur Verfügung. Erfasst werden sämtliche Organisationseinheiten, wie zum Beispiel Bereiche, Abteilungen, Gruppen sowie Geschäftsprozesse mit den Verantwortlichkeiten (Rollen). Darüber hinaus werden in diesem Modul auch unternehmensrelevante Dokumente, wie Verträge, Leitlinien, Richtlinien, Berichte, Eintragungen und Urkunden, aufbewahrt oder erstellt.

### Modul „IT-Dokumentation“

Ein weiterer Baustein der Strukturanalyse ist die Dokumentation des IT-Verbundes. Das Modul „IT-Dokumentation“ ist vom ISO-OSI Referenzmodell abgeleitet und erlaubt eine systematische Dokumentation der IT-Infrastruktur wie passive und aktive Netzwerkkomponenten, Server-Systeme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen, Gebäude, Gebäudesicherheit und Räume. Durch den Einsatz von DocSetMinder-Schnittstellen können wesentliche Informationen aus Active Directory, LDAP oder Inventory-Systemen regelmäßig importiert werden. Für die einzelnen IT-Komponenten können der Schutzbedarf festgestellt und Wiederanlaufparameter (MTA, WAZ) definiert werden. Die Dokumentation stellt die logischen Zusammenhänge zwischen Geschäftsprozessen, dafür verantwortlicher Software und Serversysteme sowie Speicherorte für die entstehenden Daten dar. Jede IT-Komponente kann dem fachlich und technisch zuständigen Mitarbeiter zugeordnet werden.

### Modul „IT-Grundschutz“

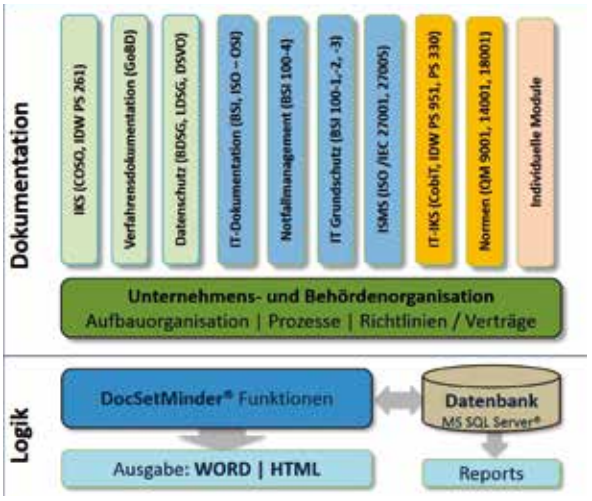
Das Modul bildet den BSI-Standard 100-2 vollständig ab. Die BSI-Methodik der Sicherheitskonzeption ist in die Modulstruktur detailliert integriert und erlaubt eine einfache Bedienung, Umsetzung und Dokumentation des IT-Grundschutzes im Unternehmen und in der Behörde. Das Modul nutzt die bereits im Grundmodul „Unternehmens- und Behördenorganisation“ und „IT-Dokumentation“ erfassten Informationen für die im Sicherheitsprozess vorgeschriebene Strukturanalyse der Organisation. Die Schutzbedarfsdefinition, Schutzbedarfsfeststellung und ihre Vererbung durch das Maximumprinzip sowie die Modellierung des IT-Verbundes sind durch die Softwareunterstützung einfach und schnell umsetzbar. Für die Durchführung der Risikoanalyse stehen zwei Methoden zur Verfügung: Risikoanalyse gemäß ISO 27005 und BSI-Standard 100-3. Sie können wahlweise, in Abstimmung mit anderen bereits umgesetzten Normen, eingesetzt werden. Zur Überwachung der Umsetzung der festgelegten Maßnahmen lassen sich der Aufgaben- und Maßnahmenplaner sowie die Reporting-Services verwenden. Das Modul „IT-Grundschutz“ wird für die unmittelbaren Bundes-, Landes- und Kommunalverwaltungen Deutschlands kostenlos angeboten.

### Modul „ISMS ISO/IEC 27001“

Die Norm ISO/IEC 27001 ist für die Planung, Umsetzung, Überwachung und stetige Verbesserung des Informationssicherheits-Managementsystems (ISMS) konzipiert. Das Modul bildet die Anforderungen der Norm ISO/IEC 27001 vollständig und detailliert ab. Die Modulstruktur erlaubt die Definition und Dokumentation des Anwendungsbereichs, der Anwendbarkeitserklärung, der Verantwortlichkeiten, der ISMS-Leitlinie, die Analyse und Bewertung der Risiken sowie die Definition von Maßnahmenzielen und Maßnahmen zur Behebung der festgestellten Risiken. Auch dieses Modul nutzt die bereits im Grundmodul „Unternehmens- und Behördenorganisation“ und „IT-Dokumentation“ erfassten Informationen für die Strukturanalyse der Organisation. Die Referenzmaßnahmenziele und Referenzmaßnahmen (Anhang A) der DIN ISO/IEC 27001 sind im Modul integriert.

### Modul „(IT-)Notfallmanagement“

Das Modul basiert auf dem BSI-Standard 100-4, ISO 22301 und BCI-GPG 2013 und bildet die Methodik zur Etablierung eines adäquaten Notfallmanagementsystems im Unternehmen oder einer Behörde ab. Es erlaubt eine vollständige Erstellung und Pflege von Dokumentationen des Anwendungsbereichs, der Notfallorganisation, der Business-Impact-Analyse, der Risikoanalyse sowie der Alarmierung und Eskalation bis hin zu Geschäftsfortführungs- und Wiederanlaufplänen (Notfallhandbücher). Die Planung und Durchführung von Notfallübungen und der Verbesserungsprozess der Notfallorganisation (PDCA) werden ebenfalls strukturiert unterstützt.




*Die Abbildung zeigt den modularen Aufbau der Compliance-Management-Software DocSetMinder.*

### Modul „Datenschutz“

Das Modul unterstützt den betrieblichen Datenschutzbeauftragten bei der Umsetzung, Kontrolle und Dokumentation der Datenschutzbestimmungen des Bundes und der Länder (BDSG und LDSG). Die Modulstruktur grenzt das öffentliche Verfahrensverzeichnis von der Verfahrensakte ab, in welcher die einzelnen internen Verfahrensübersichten dokumentiert sind. Die strengen Anforderungen an die Dokumentation der Verfahren, ihre Zweckbestimmung, betroffenen Personengruppen, Datenkategorien und Fristen können revisionssicher erfasst werden. Das Modul nutzt die bereits im Grundmodul „Unternehmens- und Behördenorganisation“ und „IT-Dokumentation“ erfassten Informationen zur Erstellung der Verfahrensübersichten. Für die Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen steht eine detaillierte Vorlage zur Verfügung. Die unterschiedlichen Datenschutzbestimmungen der Länder können sehr einfach im Modul angepasst werden.

## Fazit

DocSetMinder 3.0 bildet vollständig die anerkannten Standards für IT-Sicherheit, Notfallmanagement und Datenschutz ab. Der Funktionsumfang der Software macht den Einsatz von weiteren Tools oder Officeanwendungen für die Planung, Umsetzung und Dokumentation der umgesetzten Standards überflüssig. DocSetMinder 3.0 ist einfach zu implementieren und leicht bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet allen Verantwortlichen einen enormen Mehrwert durch die Aktualität und Zeitersparnis bei der Vorbereitung von internen und externen Prüfungen.

**GRC Partner GmbH auf der it-sa: Halle 12, Stand 121**