ISMS für KRITIS

Best Practice: Informationssicherheit mit DocSetMinder

Die Komplexität der ISO/IEC 27001, fehlende Ressourcen und die Fristen für die Umsetzung sind nur drei Argumente für eine durchdachte und gut geplante Einführung eines Informationssicherheits-Managementsystems (ISMS). Die Compliance-Management-Software DocSetMinder unterstützt das ISMS-Projektteam in allen Phasen des Projektes (PDCA) und optimiert den Aufwand zur Erstellung der erforderlichen Audit-Dokumentation.

Von Krzysztof Paschke, GRC Partner GmbH

Zu den entscheidenden Erfolgsfaktoren bei der Etablierung eines ISMS gehört neben einem kompetenten Projektteam und -management auch das eingesetzte ISMS-Tool. Die hohen Anforderungen der Norm an das Dokumentenmanagement und fachlich inhaltliche Unterstützung im Verlauf des ISMS-Projektes können nur bedingt mit Office-Anwendungen realisiert werden. Die Compliance-Management-Software DocSetMinder stellt eine Alternative für eine effiziente Umsetzung der Informationssicherheit dar.

Die Projektpraxis zeigt, dass bei der Umsetzung des ISMS auch weitere Normen, gesetzliche Anforderungen und organisatorische Aspekte berücksichtigt werden müssen. Als Beispiele können hier das Notfallmanagement, die sehr aktuelle EU-Datenschutz-Grundverordnung (EU-DS-GVO) und der Incident- und Change-Management-Prozess genannt werden. Anstatt jede Norm oder gesetzliche Anforderung einzeln zu planen und mit unterschiedlichen Tools zu realisieren, ist eine globale Betrachtung von enormem Vorteil. Die modulare Softwarearchitektur, Modulstrukturen und individuell anpassbare Dokumentklassen unterstützen die Integration und Dokumentation der genannten Aspekte und verhindern redundante Datenhaltung. Die aufeinander aufbauenden Compliance- und Standard-Module stellen gleichzeitig einen leicht verständlichen Umsetzungsleitfaden des ISMS dar.

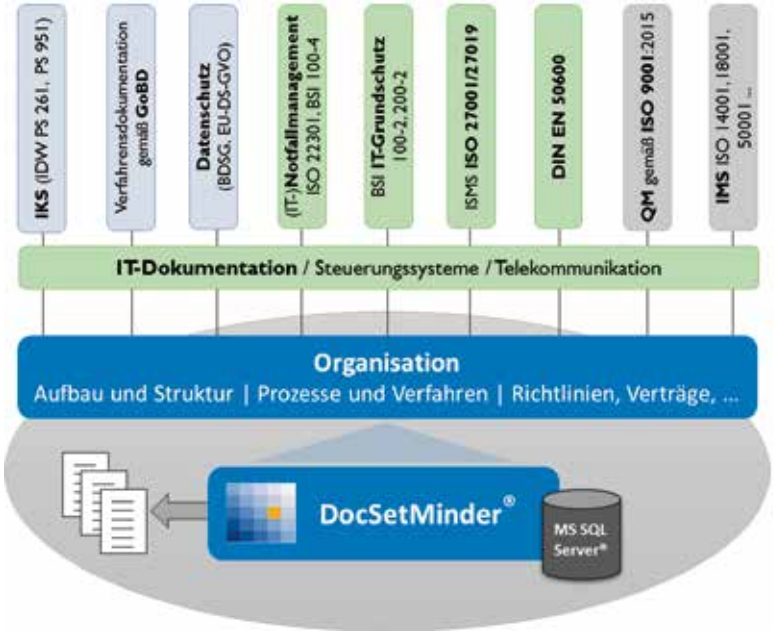
Prozessorientierter Ansatz und Methodik

Das Modul „ISO/IEC 27001" bildet die High-Level-Structure der ISO-Welt ab und fordert somit den prozessorientierten Ansatz im PDCA-Zyklus. Ergänzend stehen in den Stammdaten von DocSetMinder diverse Maßnahmenkataloge zur Verfügung. Dazu gehören vor allem die Maßnahmen aus dem Annex A der ISO/IEC 27001, optional die Maßnahmen der ISO 27019 und der BSI-Grundschutz-Kataloge. Eine individuelle Erweiterung der Gefährdungs- und Maßnahmenkataloge ist jederzeit möglich. Die Maßnahmen aus dem Annex A und der ISO 27019 werden unter anderem bei der automatischen Erstellung der Anwendbarkeitserklärung (SoA), der Projektplanung (Umsetzungsstatus der Maßnahmen und Verantwortlichkeiten) und Planung der internen Audits verwendet. Das ISMS-Projektteam kann zwischen zwei Umsetzungsmethoden wählen: ISO/IEC 27001 „nativ" oder unter Einbeziehung einiger Aspekte des BSI-IT-Grundschutzes, wie zum Beispiel Schutzbedarfsfeststellung und -vererbung.

Management der organisationseigenen Werte

Für das detaillierte Asset-Management stehen die Module „Organisation", „IT-Dokumentation" und „Steuerungs- und Leitsysteme" zur Verfügung. Die genaue Kenntnis der Unternehmensorganisation ist eine elementare Voraussetzung für die Durchführung der Strukturanalyse, der Business-Impact-Analyse und für die Planung der technischen und organisatorischen Sicherheitsmaßnahmen. Das Modul stellt die notwendigen Strukturen und Vorlagen für die Dokumentation der Aufbau- und Ablauforganisation im erforderlichen Detaillierungsgrad zur Verfügung. Erfasst werden sämtliche Organisationseinheiten (z. B. Bereiche und Abteilungen) sowie Geschäftsprozesse und Verfahren mit den Verantwortlichkeiten (Rollen) in der Organisation. Für die Dokumentation der IT-Prozesse steht die ITIL-V.3-Struktur zur Verfügung. Verträge und Richtlinien werden erstellt, aktualisiert und den Mitarbeitern kommuniziert. Der integrierte grafische Flussdiagramm-Editor unterstützt die

grafische Darstellung (unter anderem nach BPMN) der Sachverhalte. Das Modul „IT-Dokumentation“ erlaubt eine systematische Dokumentation der IT-Infrastruktur: passive und aktive Netzwerkkomponenten, Server-Systeme, Arbeitsplätze, Peripheriegeräte, Dienste und Anwendungen sowie Gebäude, Gebäudesicherheit und Räume. Die Dokumentation stellt die logischen Zusammenhänge zwischen Geschäftsprozessen, Software und Serversystemen sowie den Speicherorten für die entstehenden Daten dar. Das Modul „Steuerungs- und Leitsysteme“ ist nach den Vorgaben des IT-Sicherheitskataloges der Bundesnetzagentur in Anlehnung an den BDEW in drei Technologiekategorien strukturiert („Leitsysteme und Systembetrieb“, „Übertragungstechnik und Kommunikation“, „Sekundär-, Automatisierungs- und Fernwirktechnik“). Der erforderliche Netzstrukturplan kann mit dem DocSetMinder Flussdiagramm-Designer erstellt werden.



Aufbau der Compliance-Management-Software DocSetMinder.

Risikoanalyse und Behandlung

Die KRITIS-Organisationen sind verpflichtet, einen Prozess zur Risikoeinschätzung der Informationssicherheit zu etablieren. Dafür stehen in DocSetMinder unterschiedliche Methoden zur Verfügung: BSI-Standard 100-3, BSI-Standard 200-3, ISO 31001 und ISO 27005. Die Risikoanalyse unterstützt die Bewertung der Risiken unter Berücksichtigung von Eintrittswahrscheinlichkeit und Auswirkung in Form einer 4x4-Matrix. Die Auswirkung wird aus den durch den IT-Sicherheitskatalog vorgegebenen Schadenskategorien (Business Impact) errechnet. Optional können weitere Faktoren und Dimensionen, wie Häufigkeit (Exposition) oder MxN-Matrix, berücksichtigt werden.

Notfallmanagement

Für die Umsetzung des betrieblichen Kontinuitätsmanagements (BCM) steht das Modul „Notfallmanagement“ zur Verfügung. Mithilfe dieses Moduls kann das Notfallmanagement wahlweise gemäß BSI-Standard 100-4 oder nach ISO 22301 geplant und realisiert werden. Das Modul zeichnet sich durch eine klare Struktur mit funktionalen Vorlagen (Dokumentklassen) für die Dokumentation unter anderm des Anwendungsbereichs, der Notfallorganisation, der Business-Impact-Analyse (inklusive Berechnungsformeln) und der Risikoanalyse aus. Alarmierungen, Sofortmaßnahmen, Geschäftsfortführungs- und Wiederanlaufpläne können durch autorisierte Personen jederzeit extrahiert und als Notfallhandbücher für mobile Geräte offline zur Verfügung gestellt werden.

Datenschutz nach EU-DS-GVO

Das Modul „EU-DS-GVO“ unterstützt den betrieblichen Datenschutzbeauftragten bei der Umsetzung, Kontrolle und Dokumentation der Datenschutzbestimmungen der EU und des Bundes. Die übersichtliche Modulstruktur spiegelt detailliert Angaben zur Datenschutzorganisation, Risikobeurteilung, Dokumentation der Verarbeitungstätigkeiten und Verbesserungsprozesse wider. Für die Dokumentation der technischen und organisatorischen Sicherheitsmaßnahmen steht eine detaillierte Dokumentklasse zur Verfügung. Die strengen Anforderungen an die Dokumentation können revisionssicher erfasst und jederzeit dem Prüfer oder den Mitarbeitern verfügbar gemacht werden. Das Modul nutzt die bereits im Modul „Organisation“ und „IT-Dokumentation“ erforderlichen und zuvor für das ISMS erfassten Sachverhalte, zum Beispiel Verfahren, IT-Komponenten und Berechtigungen.

Fazit

DocSetMinder bildet die anerkannten Standards der Informationssicherheit wie auch den Datenschutz vollständig ab. Der Funktionsumfang der Software macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung der umgesetzten Standards überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Die gemeinsame Nutzung der erfassten Informationen bietet für jeden Verantwortlichen einen enormen Mehrwert durch die Aktualität und eine signifikante Zeitersparnis bei der Vorbereitung von internen und externen Audits. DocSetMinder ist Best Practice – und Ihr Unternehmen ist jederzeit „Ready for Audit“. ■