ALLGEIER CyRis

DocSetMinder® Ready for Audit

MODUL ISMS-ISO/IEC 27001

Motivation

Mit zunehmender Komplexität und Abhängigkeit von der IT steigt auch ihre Anfälligkeit, nicht zuletzt durch gezielte Cyberkriminalität. Die Vertraulichkeit, Integrität und Verfügbarkeit der Geschäftsdaten und Informationen kann nur mit Hilfe von sorgfältig geplanten organisatorischen und technischen Maßnahmen gewährleistet werden. Die ISO/IEC 27000-Reihe liefert diverse Standards für die Planung und Umsetzung eines Informationssicherheits-Managementsystems (ISMS).

ISO/IEC 27001

Die **ISO/IEC 27001** definiert die Regeln für die Planung, Umsetzung, Aufrechterhaltung und permanente Verbesserung eines dokumentierten ISMS. Weitere Normen aus der ISO/IEC 27000-Reihe ergänzen die Implementierung, u. a.:

- ISO/IEC 27002 – Implementierungsleitfaden für den Anhang A (Maßnahmenziele und Maßnahmen) der ISO/IEC 27001.
- ISO/IEC 27005 – Leitlinie für ein prozessorientiertes Risikomanagement in der Informationssicherheit.

Die Gliederung der Norm entspricht der ISO High Level Structure und stellt eine einheitliche Verzeichnisstruktur und Terminologie für alle Managementsysteme dar. Durch einheitliche Struktur und Gemeinsamkeiten, wie z. B.: Kontext der Organisation, Führung, Politik und Verantwortlichkeiten, Risikoanalyse oder Verbesserung unterstützt die High Level Structure eine einfache und strukturierte Integration von mehreren Managementsystemen. Die Implementierung der Norm erfolgt im PDCA-Zyklus.

Die Planung und Umsetzung des ISMS gemäß der ISO/IEC 27001 kann wie folgt skizziert werden:

- Kontext der Organisation und Geltungsbereich festlegen
  - Umfeldanalyse
  - Geltungsbereich
  - Informationssicherheitsleitlinie und Ziele
- Rollen, Verantwortlichkeiten und Kompetenzen
- Unternehmenswerte identifizieren
  - Auflistung der primären und sekundären Informationen, Daten und IT-Komponenten
  - Relation zwischen den Werten dokumentieren
- Risikoanalyse
  - Methode festlegen
  - Risikoparameter definieren
  - Risikoakzeptanzparameter definieren
  - Risikobehandlung festlegen
  - Risikoanalyse durchführen
- Maßnahmenziele und Maßnahmen festlegen und durchführen
  - Wer macht was und bis wann
  - Kommunikation, Aufklärung und Schulung
  - Erklärung zur Anwendbarkeit (SoA)
- Überprüfung und Messung
  - Interne Audits
  - KPI
  - Sicherheitsvorfälle

Die Norm stellt eine sehr hohe Anforderung an die Dokumentation des ISMS, die im Audit dem Prüfer vorgelegt werden muss. Folgende dokumentierte Informationen müssen verfügbar sein:

- Geltungsbereich des ISMS
- Informationssicherheitsleitlinie und technische Richtlinien
- Risikoanalyse und -behandlung
- Anwendbarkeitserklärung (SoA)
- Informationssicherheitsziele
- Kompetenzen
- Betriebliche Planung und Steuerung
- Bewertung der Leistung
- Verbesserung (Nichtkonformitäten)
- Diverse Dokumente als Ergebnis der Umsetzung der Maßnahmen aus dem Anhang A der Norm

Unsere Lösung für Sie

Mit dem **DocSetMinder®** Modul **ISMS – ISO 27001** erhalten Unternehmen jeder Größe eine sehr effiziente und intuitiv bedienbare Softwarelösung für die Umsetzung, Aufrechterhaltung und Dokumentation des ISMS. Die Modulstruktur ist für die ISO/IEC 27001 konzipiert worden und bildet die geforderten Dokumentationsaspekte ab:

- Die Modulstruktur bildet die High Level Structure (Normkapitel 4 – 10) ab und stellt gleichzeitig einen leicht bedienbaren Umsetzungsleitfaden für das ISMS-Team dar
- Maßnahmenziele und Maßnahmen aus dem ISO 27001 Anhang A und dem BSI-Grundschutz-Kompendium sind im Lieferumfang enthalten
- ISMS-Organisation (Rollen, Verantwortlichkeiten, Kompetenzen)
- Grafische Darstellung der Organisation und Prozesse mit dem integrierten Flowchart-Editor (nach ISO und BPMN)
- Richtlinienmanagement für die erforderlichen Leit- und Richtlinien
- Erfassung der Organisationswerte (Organisation und IT-Dokumentation inkl. Verantwortlichkeiten und Schutzbedarf)
- DIN EN ISO 9001- konforme Dokumentvorlagen für die Erfassung der Verfahrensanweisungen, Prozesse und Arbeitsanweisungen
- Rechtskataster
- Risikoanalyse gemäß IT-Sicherheitskatalog ISO/IEC 27005
- Schwachstellenkatalog (Self-Assessment)
- Umsetzung der ISO 27001 auch unter Einbeziehung von BSI-Grundschutz-Methoden (Vererbung des Schutzbedarfs etc.) möglich
- Automatische Erstellung der Anwendbarkeitserklärung (SoA)
- Schulungspläne
- Die gesamte ISMS-Dokumentation kann dem Auditor in Form eines MS Office Word-Dokumentes zur Verfügung gestellt werden. Alternativ kann der Auditor die Sachverhalte im System prüfen.
- Ausführliche **DocSetMinder®** Reporting-Services liefern den aktuellen Status der Maßnahmen und erinnern an die Revision
- Sicherheitsvorfälle
- Planung und Durchführung der internen Audits inkl. KPIs
- Drei unterschiedliche Maturity-Modelle für die Bestimmung des ISMS-Reifegrades
- Integration mit weiteren Modulen, z. B. VDA-ISA

Fazit

Der Funktionsumfang der Software macht den Einsatz weiterer Tools oder Office-Anwendungen für die Dokumentation und Zertifizierung nach ISO/IEC 27001 überflüssig. Die Lösung ist einfach zu implementieren und intuitiv bedienbar. Mit **DocSetMinder®** sind Sie jederzeit **Ready for Audit**.

Wir unterstützen Sie

- bei der Einführung der Software
- bei der Ermittlung und Erfassung der Organisationswerte
- bei der Durchführung der Schwachstellen- und Bedrohungsanalyse
- bei der Durchführung der Risikoanalyse und Festlegung der notwendigen Maßnahmen
- bei der Dokumentation der ISMS-Sachverhalte
- bei der Durchführung der Schulungen
- mit begleitendem Coaching
- mit technischem Support