ALLGEIER CyRis

DocSetMinder® Ready for Audit

MODUL IT-Grundschutz

Motivation und Ziele

Informationssicherheit im Zeitalter der digitalen Transformation ist keine einmalige Investition oder Aktivität, die das Problem der Cyber-Bedrohungen regelt. Vielmehr handelt es sich um einen Sicherheitsprozess, in dem eine Reihe von sorgfältig geplanten technischen und organisatorischen Maßnahmen umgesetzt werden müssen, um ein Mindestniveau an IT-Sicherheit zu erreichen. Die BSI-Standardreihe zur Informationssicherheit definiert in drei unterschiedlichen Vorgehensweisen (Basis-, Kern- und Standardabsicherung) die Planung und Etablierung der Informationssicherheit im angestrebten Sicherheitsniveau. Damit eignet sich der IT-Grundschutz nicht nur für große Organisationen und Behörden, sondern auch für kleine und mittelständische Unternehmen. Das in zehn Schichten strukturierte BSI IT-Grundschutz-Kompendium liefert die erforderlichen Sicherheitsanforderungen und Umsetzungshinweise in Form von Bausteinen. Eine weitere Komponente des IT-Grundschutz-Kompendiums ist der G0 Katalog der 47 elementaren Gefährdungen. Sie werden u. a. bei der Identifikation und Bewertung der Risiken gemäß dem BSI-Standard 200-3 verwendet.

BSI-Standardreihe 200-1, 200-2, 200-3

Der BSI-Standard 200-1 definiert die Anforderungen an ein Managementsystem für Informationssicherheit (ISMS) und ist vollständig mit dem ISO/IEC 27001 Standard kompatibel. Die Methodik der Umsetzung eines ISMS ist im BSI-Standard 200-2 detailliert und praxisnah beschrieben. Der BSI-Standard 200-3 definiert die Risikoanalyse und beschreibt den gesamten Prozess der Identifikation, Analyse, Bewertung und Behandlung von Risiken in der Informationssicherheit. Der Sicherheitsprozess **(IT-Grundschutz-Methodik)** ist in folgenden Schritten

Schritt 1: Die Etablierung des ISMS beginnt mit der **Initiierung des Sicherheitsprozesses** indem die Leitung der Organisation die Verantwortung für das Vorhaben übernimmt und einen organisatorischen und finanziellen Rahmen schafft.

Schritt 2: In der Konzeptions- und Planungsphase werden unterschiedliche Einflussfaktoren aus der Sicht der Informationssicherheit im Kontext der Organisation ermittelt, **Informationssicherheitsziele, Geltungsbereich (IT-Verbund) und Sicherheitsniveau** festgelegt.

Schritt 3: Festlegung der **Vorgehensweise** (Basis-, Kern- und Standard-Absicherung) und des **Geltungsbereichs.**

Schritt 4: Erstellung der **Leitlinie** zur Informationssicherheit (Motivation, Ziele und Verantwortlichkeiten).

Schritt 5: Festlegung der **IS-Organisation**. Es werden Rollen, Teams, Verantwortlichkeiten, Befugnisse und Aufgaben defniert. Die Aktivitäten der IS-Organisation werden in die Prozesse der Organisation integriert.

Schritt 6: Dokumentation im Sicherheitsprozess. Festlegung der **Dokumentationsregeln** und -lenkung sowie Definition der Regeln für die **Klassifikation von Informationen**.

Schritt 7: Erstellung der **Sicherheitskonzeption** gemäß der ausgewählten Vorgehensweise (Basis-, Kern- und Standardabsicherung).

Schritt 8: Umsetzung der **Sicherheitsanforderungen** (Maßnahmen) in definierter Reihenfolge (Priorität) und nach Verantwortlichkeiten. Durchführung der Risikoanalyse für Zielobjekte mit hohem und sehr hohem Schutzbedarf.

Schritt 9: **Aufrechterhaltung** und kontinuierliche **Verbesserung** der Informationssicherheit (PDCA-Zyklus).

ALLGEIER CyRis

DocSetMinder® Ready for Audit

Unsere Lösung für Sie

Mit dem **DocSetMinder®** Modul **IT-Grundschutz** erhalten Organisationen eine sehr effiziente und intuitiv bedienbare Softwarelösung für die Planung, Umsetzung und Dokumentation des ISMS gemäß der BSI-Standardreihe 200. Die wichtigsten Eigenschaften auf einen Blick:

- Die Modulstruktur und Dokumentklassen bilden vollständig und detailliert die IT-Grundschutz-Methodik ab.
- Das Schichtenmodell (prozess- und systemorientierte Schichten) kann individuell erweitert werden. Nicht benötigte Schichten können ausgeblendet werden.
- Unterstützung mehrerer Informationsverbünde.
- Kopieren oder Verlinken von Zielobjekten, Bausteinen, Risikoanalysen.
- Automatischer Vorschlag für die Zuordnung der Bausteine zu den Zielobjekten (Modellierung).
- Konfigurierbare Sicherheitsanforderungsstufe (Basis-, Standardanforderungen und Anforderungen mit erhöhtem Schutzbedarf).
- Dokumentation der Unternehmens- und Behördenorganisation im Modul **Organisation** (Organisatorische Einheiten und Prozesse).
- Dokumentation der IT-Infrastruktur im Modul **IT-Dokumentation**: Netzpläne, Anwendungen, Daten/Informationen, Server, Arbeitsplätze, ICS, IoT, Peripheriegeräte, aktive und passive Netzwerkkomponenten, WAN-Leitungen, Gebäude, Räume, Infrastruktur und Standorte.
- IS- und IT-Prozesse können in der ITIL Struktur dokumentiert werden.
- Dokumentation des Rollenkonzeptes, der Verantwortlichkeiten, Kompetenzen und Zuständigkeiten.
- Grafische Darstellung der IS-Organisation und -Prozesse mit dem integrierten Flowchart-Editor (nach ISO und BPMN).
- Richtlinienmanagement für die erforderlichen IS-Leit- und Richtlinien.
- Anforderungen an die Kennzeichnung der Dokumente und Dokumentenlenkung sind vollständig umgesetzt.
- Drei unterschiedliche Methoden stehen für die Klassifikation von Informationen zur Auswahl.
- Import der IT-Komponenten aus Fremdsystemen.
- Integration von komplexen IT-Managementsystemen (ohne Datenimport).
- Optionaler Schwachstellenkatalog für die Risikoanalyse.
- Risikoanalyse gemäß BSI-Standard 200-3 mit automatischer Zuordnung der elementaren Gefährdungen.
- Individuell definierbare Korrekturmaßnahmen.
- Erfassung und Meldung der Sicherheitsvorfälle.
- Planung und Durchführung von Cyber-Sicherheits-Checks (nach ISACA und BSI).
- Audit- und Schulungspläne.
- Drei unterschiedliche Methoden für die Bestimmung des Reifegrades des ISMS zur Auswahl.
- KPI Erfassung und Auswertung.
- Bereitstellung der Referenzdokumente für die Zertifizierung nach ISO 27001 auf Basis vom IT-Grundschutz (A0 bis A6) in Form von MS Office Word-Dokumenten oder als Reports.

Wir unterstützen Sie

- bei der Einführung der Software
- bei der Ermittlung und Erfassung der Prozesse und IT-Komponenten
- bei der Durchführung der Schutzbedarfsanalyse und Modellierung
- bei der Durchführung der Risikoanalyse
- bei der Dokumentation der ISMS-Sachverhalte
- bei der Erstellung von individuellen Reports
- bei der Durchführung der Schulungen
- mit begleitendem Coaching
- mit technischem Support

Besuchen Sie uns online:
www.docsetminder.de

Telefonischer Kontakt:
+49 431 53 033 990

Kontakt per E-Mail:
info@docsetminder.de