ISO-Konformität für Unternehmen und Krankenkassen

Information Security Management Systeme

Nicht nur im Rahmen der Einführung der elektronischen Gesundheitskarte (eGK) spielt das Thema Konformität mit ISO 27001 eine immer größere Rolle für Unternehmen und Krankenkassen. Die heutigen Anforderungen an die Compliance, die sich in erster Linie aus dem Bundsdatenschutzgesetz (BDSG), Basel II oder dem Sarbanes Oxley Act (SOX) ergeben, verlangen von praktisch jedem Unternehmen die Führung eines dokumentierten Informationssicherheits-Managementsystems.

Durch die Errichtung eines Information Security Management System (ISMS) macht das Thema IT-Security den Schritt von der rein technischen Ebene auf die Managementebene.

Durch verschiedene Projekte, u.a. im Rahmen der elektronischen Gesundheitskarte verfügt exceet Secure Solutions AG über ein fundiertes Fachwissen im Bereich von ISO-konformen Sicherheitskonzepten, deren Umsetzung und der Einführung eines Sicherheitsmanagements.

Unser Consulting Team bietet Ihnen praxisorientierte Beratungsunterstützung, wenn es um die Einrichtung Ihres ISO-konformen ISMS geht.

Die folgende Liste gibt einen Überblick über die Dokumente, die typischerweise für die Implementierung eines ISMS verfügbar sein sollten. Der Umfang kann je nach Implementierung jedoch schwanken. Auch sind nicht alle Dokumente für eine Zertifizierung zwingend notwendig, sondern einige können ggf. als optional betrachtet werden. Dies ist aber im Einzelfall zu bewerten.

ISMS Projektimplementierungsdokumente

- ISMS Scope Definition
- ISO 27002 Fragebogen / GAP Analysis Report
- ISM Generic Business Plan
- SMS Implementation Plan
- Risk Treatment Plan
- Statement of Applicability
- Risikomanagementstrategie
- ISMS Organisationsplan
- Glossar Information Security

ISMS Information Security Policy

- Informations-Sicherheitsleitlinie
- Access Control Policy
- Clear Desk und Clear Screen Policy
- Information Classification Policy
- Richtlinien für die Vernichtung von Informationen, Medien und Geräten
- eCommerce Security Policy
- Risikoanalyse der Informationssicherheit
- E-Mail Security Policy
- Laptop Security Policy
- Mobile Computing und Teleworking Policy
- Outsourcing Policy
- Passwort Policy
- Penetration Testing Policy
- Personenbezogene Sicherheitspolicy
- Umgebungsbezogene Sicherheitspolicy
- Datenschutzrichtlinien
- Software Copyright Richtlinien
- Spam Policy
- Datensicherungsrichtlinien
- Virus / Malware Policy
- Grundsätzliche technische Standards

Dokumentation, die die Sicherheits- und Konfigurations-parameter verschiedener technischer Plattform definiert

- Applikationsserver
- Datenbanken
- Desktops, Laptops, PDAs
- Entwicklungssysteme
- Geräte in demilitarisierten Zonen
- Firewalls
- Mainframes
- Betriebssysteme
- Router und Switche
- Textsysteme
- Systeme von Dritten, die im LAN benutzt werden
- Kabelgebundenes und kabelloses Netzwerk

ISMS Management Prozesse

- Corrective Action Plan
- Dokumentenkontrolle
- Interne ISMS Audit Prozesse
- Awareness Material
- ISMS Auditing Guideline
- Risikoanalyse-Sheet

Sicherheitsrelevante Jobbeschreibungen

Information Asset Owner
Information Security Analyst
Information Security Architect
Information Security Manager
Information Security Officer
Information SecurityTester
IT Auditor
Security Administrator

Sicherheitsrelevante Prozesse

- Backupverfahren
- Revisions- und Auditverfahren
- Incident Management Verfahren
- Patch-Management Verfahren
- Sicherheitsrelevante administrative Aufgaben (erstellen neuer Benutzer-ID's, Änderung von Benutzerrechten, usw.)
- System Hardening Verfahren
- Testverfahren
- Benutzersupport

exceet Secure Solutions GmbH
Phone +49 (0) 211 436989-0
Email info@exceet-secure-solutions.de
Web www.exceet-secure-solutions.de