Welchen Nutzen hat ein ISMS?

Neben der Einhaltung der gesetzlichen Vorgabe zum Betrieb eines ISMS für bestimmte Organisationen werden folgende Mehrwerte generiert:

- Zertifizierbare Prozesse als Nachweis eines adäquaten Sicherheitsniveaus gegenüber Dritten
- Identifizierung der möglichen Risiken für eine Organisation und der damit verbundenen:
  - Reduktion der finanziellen Schadensauswirkungen bei Beeinträchtigungen der Unternehmensprozesse
  - Reduktion der Eintrittswahrscheinlichkeit einer Beeinträchtigung
  - Aufrechterhaltung der Kernprozesse im Falle eines Notfalls oder einer Krise, damit verbunden eine
  - Steigerung der Überlebensfähigkeit des Unternehmens

Zusätzlich weisen alle ISMS Parallelen zu IT-Service-Management-Systemen sowie den Anforderungen im Bereich Datenschutz auf. Dadurch arbeiten diese Bereiche „Hand in Hand“ und können sich gegenseitig unterstützen und ergänzen.

Partner der Bundesrepublik Deutschland
Mitglied der Allianz für Cyber-Sicherheit
Bundesverband IT-Sachverständige & Gutachter
Auditoren für ISO 27001, ISO 20000, FitSM
Traininginstitut ITIL®, FitSM, ISO 27000, IT-Sec, ISIS12

Weitere Informationen zum Thema finden Sie auf unserer Webseite unter:

www.consectra.de

Sie haben Fragen zum Thema oder wollen sich diesbezüglich beraten lassen? Kontaktieren Sie uns telefonisch unter:

+49.781.203588-00

oder per E-Mail an:

info@consectra.de

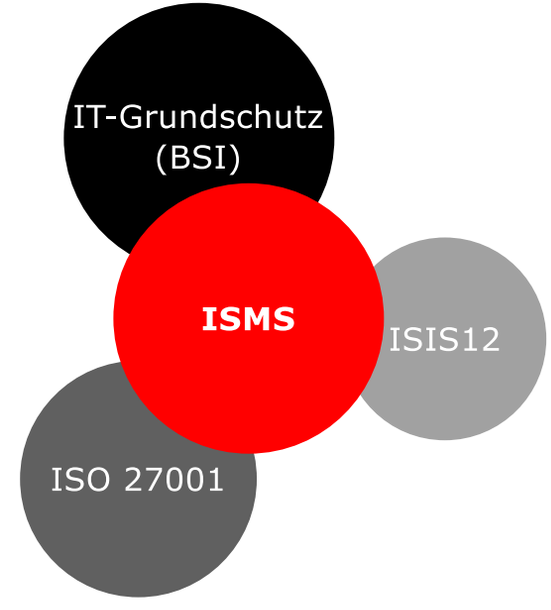
Unsere Firmenadresse:

consectra GmbH
Im Unteren Angel 13
77652 Offenburg

consectra
mIT-Sicherheit ein guter Partner

Information Security Management System

Zertifizierbare Sicherheit



Verwaltung von Risiken und Gefahren zur Steigerung der Informationssicherheit

consectra
mIT-Sicherheit ein guter Partner

Was ist ein ISMS?

Als Informationssicherheits-Managementsysteme (kurz: ISMS) werden Systeme bezeichnet, die folgende Ziele verfolgen:

- Identifikation des aktuellen und benötigten Sicherheitsniveaus
- Identifikation von Bedrohungen und Risiken
- Einführung und Umsetzung von Schutzmaßnahmen

Wie funktioniert ein ISMS?

Ein ISMS besteht aus einer Reihe von Verfahren und Regeln, die den Schutz der IT-Infrastruktur sowie der Informationen und Daten eines Unternehmens verbessern. Dabei werden alle betroffenen Prozesse des Unternehmens kontinuierlich auf Effektivität geprüft, weshalb ein ISMS auch stets als Kreislauf und nicht als einmalige Maßnahme zu betrachten ist. Inhaltlich besteht ein ISMS aus technischen, organisatorischen sowie Sensibilisierungsmaßnahmen.

Ein ISMS setzt dabei bei der Unternehmensführung an und arbeitet sich von dort abwärts durch alle spezifizierten Bereiche der Organisation.

Wer braucht ein ISMS?

Organisationen, die:

- gesetzlich dazu verpflichtet sind, z.B. gemäß Europäischer Datenschutzgrundverordnung oder KRITIS.
- aufgrund von Kooperationen dazu verpflichtet sind.
- ihre IT-Sicherheit auf ein mess- und nachweisbares Niveau anheben wollen.

Welche ISMS gibt es?

Die drei bekanntesten ISMS derzeit sind:

IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Bundesamt für Sicherheit in der Informationstechnik

Der nationale Ansatz für Behörden und Unternehmen:

Ein maßnahmenbezogener Ansatz mit hohem Detaillierungsgrad.

Der internationale Standard ISO/IEC 27001

ISO/IEC 27001

Der internationale Standard für mittlere und große Organisationen:

Ein generischer Ansatz für größeren Handlungsspielraum.

ISIS12 des IT-Sicherheitsclusters

ISIS 12

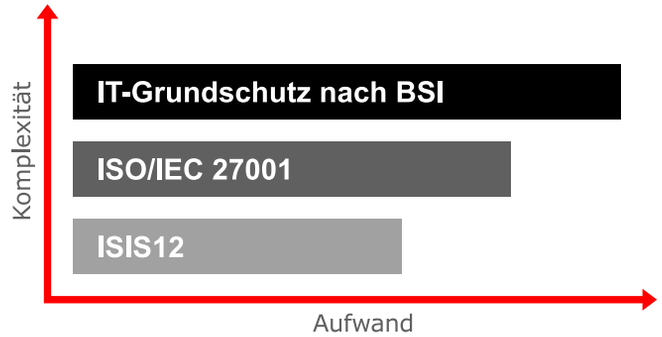
Informationssicherheit für den Mittelstand

Das ISMS für den Mittelstand.

Reduzierter Umfang auf die wesentlichen Kernpunkte und doch jederzeit erweiterbar auf ein größeres Rahmenwerk.

Was sind die Unterschiede?

Der wesentliche Unterschied der drei Systeme ist die Komplexität und der damit verbundene zeitliche, finanzielle und personelle Aufwand.



IT-Grundschutz und ISO/IEC 27001 sind grundlegend dafür geeignet, in jeder Organisation Anwendung zu finden, allerdings ist der Umfang an umzusetzenden Maßnahmen und der damit verbundene organisatorische und finanzielle Aufwand gerade für kleinere Unternehmen als eher schwierig zu bewerten.

Die Lösung bietet der IT-Sicherheitscluster durch ISIS12, welches auch als zertifizierbarer Zwischenschritt für eine Zertifizierung nach ISO/IEC 27001 und IT-Grundschutz genutzt werden kann.

Was bedeutet das für eine Organisation?

Der unterschiedliche Ansatz der Systeme ermöglicht einer Organisation das jeweils am besten passende Verfahren auszuwählen. Dabei kann im Laufe des Wachstums einer Organisation oder einem veränderten Bedarf der Zertifizierung jederzeit von einem kleineren auf ein größeres Rahmenwerk erweitert werden.