

Informationssicherheits- management nach ISO 27001 und BSI Grundsatz



**Karner & Schröppel Partnerschaft
Sachverständige für Informationssicherheit und
Datenschutz**

Unser Konzept



Informationssicherheit und Datenschutz als Managementaufgabe

Die ganzheitliche Betrachtung der Informationssicherheit fängt bei der „Organisatorischen Sicherheit“ an, beleuchtet die Umsetzung der technischen (IT-)Sicherheit, und geht bis hin zum Themengebiet der Notfallvorsorge oder -planung (BCM, Business Continuity Management).

Aus der Erkenntnis heraus, dass Informationssicherheit mehr ist wie die Summe der einzelnen Teile, entwickelte sich das Konzept für SECIANUS, Informationssicherheit ganzheitlich zu betrachten und, abgestimmt auf die jeweiligen Bedürfnisse des Kunden, anzubieten.

Informationssicherheit ist ein Management-Prozess, der gelebt und einer laufenden Bewertung und Kontrolle unterworfen sein sollte.

Nur wenn sich Informationssicherheit als Prozess etabliert und vom Management eines Unternehmens aktiv unterstützt und gelebt wird, können Daten und Informationen sicher und jederzeit verfügbar gespeichert und verarbeitet werden.

In der letzten Zeit hat sich außerdem der Bereich Datenschutz als immer wichtiger werdendes Thema herausgestellt. Auf Grund der vielen Synergie-Effekte sollten daher Informationssicherheit und Datenschutz einheitlich bewertet, betrachtet und umgesetzt werden.



Informationssicherheitsmanagement- Eine Managementaufgabe

Daten und Informationen, egal ob über Kunden, eigene Produkte, Preise, etc. sind echte und bedeutende Werte eines Unternehmens.

Gehen diese Daten verloren, werden entwendet, egal ob fahrlässig oder vorsätzlich, bedeutet dies einen Verlust. Je nach Informationsgehalt der Daten kann ein solcher Verlust „nur“ den Verlust des Wettbewerbsvorteils bedeuten. Im schlimmsten Fall kann dies aber auch bis zum völligen Ruin des Unternehmens gehen.

Informationen sind mehr als nur elektronische Daten. Informationen finden sich auch auf Papier wieder oder können als Wissen in den Köpfen der Mitarbeiter stecken.

Aus diesem Grund darf Informationssicherheit sich nicht nur mit der technischen Sicherheit befassen, sondern sollte umfassend und bereichsübergreifend betrachtet werden.

Nur wenn Informationssicherheit fester Bestandteil der Unternehmenspolitik wird, kann diese wirkungsvoll und nachhaltig umgesetzt werden.

Damit dies erfolgreich geschehen kann, benötigt die Realisierung die vollste Unterstützung durch das Management. Aber auch dann verbleibt die Verantwortung beim Management. Um sicher zu gehen, sollten vom Management die notwendigen Maßnahmen initiiert, sowie deren Umsetzung kontrolliert werden.



Informationssicherheit ist mehr wie IT-Sicherheit

Informationssicherheit ist mehr wie nur IT-Sicherheit. IT-Sicherheit ist zwar unabdingbar notwendig, aber nur ein Bestandteil eines umfassenden Informationssicherheitsmanagement.

Informationssicherheit beginnt bereits bei einer angemessenen Absicherung der baulichen Infrastruktur mit allen Aspekten, wie Einbruchsschutz, Brandschutz, Notstromversorgung, etc., befasst sich natürlich auch mit der technischen Sicherheit, inklusive Firewalls, Virenschutz, geht über die Betrachtung der Einhaltung gesetzlicher und vertraglicher Regelungen, bis hin zu organisatorischen Maßnahmen, wie Richtlinien, Notfallmanagement und Sensibilisierungsprogrammen.

Welche Methode dabei zum Einsatz kommt, die ISO 27001, der BSI

Grundschutz oder eine Kombination aus beiden Welten, hängt alleine von den Anforderungen Ihres Unternehmens ab.

Beide Verfahren haben Vor- und Nachteile, so dass keine generelle Empfehlung gegeben werden kann.

Unsere Empfehlung:

- Meist lassen sich Synergie-Effekte schaffen, wenn man Datenschutz und Informationssicherheit gemeinsam betrachtet
- Überlegen Sie, ob Sie das Thema Informationssicherheit außerhalb der IT-Abteilung ansiedeln können. Die IT-Abteilung „denkt“ meist in technischen Lösungen und weniger in Geschäftsprozessen



Informationssicherheit mit ISO 27001

Bei der ISO 27001 handelt es sich um einen zertifizierbaren, internationalen Standard, der den Aufbau eines ISMS (Information Security Management System) beschreibt.

Ergänzend zur ISO 27001 gibt es eine Reihe weiterer Dokumentationen, Empfehlungen oder Leitfäden, die die Anwendung der ISO 27001 konkretisieren oder Anhaltspunkte zur Umsetzung geben.

Der ISO 27001 Standard ist stark prozessorientiert und geht von den Geschäftsprozessen in einem Unternehmen aus. Das Ziel ist es, Risiken für das Unternehmen zu identifizieren, zu analysieren und durch entsprechende Maßnahmen möglichst beherrschbar zu machen.

Unsere Leistungen:

- Erstellung von Sicherheitskonzepten und Dokumenten nach ISO 27001
- Zertifizierungsvorbereitung nach ISO 27001
- Aufbau und Einführung eines ISMS nach ISO 27001
- ISO 27001 Prüfungsvorbereitung und Voraudit
- Management-Sensibilisierungen
- Schulungen zum Thema ISO 27001
- Mitarbeitersensibilisierungen

Ein Tipp in eigener Sache:

Sollten Sie über keine personellen Ressourcen für einen Informationssicherheitsbeauftragten (CISO) verfügen, so können wir Ihnen diese Aufgabe in Form eines externen (IT-)Sicherheitsbeauftragten abnehmen.



Informationssicherheit mit den BSI Grundschutzkatalogen

Auch die Umsetzung eines ISMS (Information Security Management System) nach den BSI Grundschutzkatalogen ist zertifizierbar. Dabei handelt es sich allerdings um einen nationalen Standard, im Gegensatz zur ISO 27001.

Im Gegensatz zur ISO 2700x-Reihe bieten die BSI-Grundschutzkataloge gezielt Hilfestellung bei der Umsetzung an. So gibt es sog. Bausteine, die sich sowohl mit der organisatorischen Sicherheit wie auch mit der technischen, baulichen und personellen Sicherheit befassen.

Unsere Leistungen:

- Erstellung von Sicherheitskonzepten und Dokumenten nach den Anforderungen der BSI Grundschutzkataloge
- Zertifizierungsvorbereitung auf eine BSI Grundschutz Zertifizierung
- Aufbau und Einführung eines ISMS nach BSI Grundschutz
- Prüfungsvorbereitung und Voraudit
- Quick-Check auf Basis des Prüfungsschemas des BSI
- Management- und Mitarbeiter-Sensibilisierungen
- Schulungen zum Thema BSI Grundschutz

Ein Tipp in eigener Sache:

Um das Thema Informationssicherheit umsetzen zu können, empfiehlt sich die Einführung der Rolle eines Informationssicherheitsbeauftragten. Sollten Sie über keine personellen Ressourcen verfügen, übernehmen wir gerne diese Aufgabe.



Unsere weiteren Leistungen

Datenschutz

- wir beraten Sie in allen gängigen Fragen rund um den Datenschutz
- wir übernehmen für Sie die Aufgabe des Datenschutzbeauftragten – als externer Datenschutzbeauftragter
- wir erstellen für Sie alle notwendigen Datenschutzdokumente
- wir führen alle notwendigen und gesetzlich vorgeschriebenen Schulungen für Sie und Ihre Mitarbeiter durch
- u.v.m.

Notfallmanagement/BCM

- wir beraten Sie beim Aufbau eines effektiven Notfallmanagements nach BS 25999 oder BSI Standard 100-4
- Unterstützung bei der Erstellung eines Notfallhandbuchs
- Planung und Durchführung von Notfall-Test und Rahmenübungen
- u.v.m.

Kontakt:

SECIANUS – Karner & Schröppel Partnerschaft
Sachverständige für Informationssicherheit und Datenschutz

Postanschrift:

Hanserauweg 3
92342 Freystadt

Büro:

Marktplatz 30
92342 Freystadt

Web: www.secianus.de

E-Mail: info@secianus.de

Telefon:

Herr Karner: +49 (0) 175 22 39 010

Herr Schröppel: +49 (0) 174 93 44 228

IMPRESSUM:

SECIANUS – Karner & Schröppel Partnerschaft
Hanserauweg 3
92342 Freystadt

Vertreten durch:

Herrn Jörg Karner

Herrn Reiner Schröppel

Registereintrag:

Eintragung im Partnerschaftsregister

Registergericht: Amtsgericht Nürnberg

Registernummer: PR 169

USt-IdNr. DE271954132