AKRA
BUSINESS SOLUTIONS

Managementsysteme EINFACH MACHEN

ISO 27001 - auf der sicheren Seite

Informationssicherheit - strategisch managen

ISO/IEC 27001 - international anerkannt

www.akrabs.de

AKRA Business Solutions GmbH
Domstr. 17
20095 Hamburg

EINFACH MACHEN - Unternehmenswerte schützen

In Unternehmen mit Hochzuverlässigkeitscharakter bedeutet IT-Sicherheit oft mehr als den Geschäftserfolg. Bedingt durch die zunehmende Abhängigkeit der Geschäftsprozesse von der Informationstechnologie nimmt die Bedeutung der Informationssicherheit im Unternehmen stetig zu. Auch die Sicherheit des Unternehmens ist abhängig von der IT. Immer mehr Stakeholder verlangen deshalb den Nachweis über die Etablierung eines effektiven Informationssicherheits-Management-Systems (ISMS). Die internationale Norm ISO/IEC 27001 spezifiziert hierfür die Anforderungen.

Informationssicherheit - Herausforderung für Geschäftsführer und Vorstand

Informationen sind ein wesentlicher Wert des Unternehmens und müssen angemessen geschützt werden. Die **Geschäftsprozesse basieren immer mehr auf IT-Lösungen.** Die **Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik** wird, wie auch der vertrauensvolle Umgang mit Informationen, immer wichtiger. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der existenzbedrohend sein kann. Auch die geänderte Gesetzeslage trägt dazu bei, die **Sensibilität für Informationssicherheit** zu erhöhen: Vorstände und Geschäftsführer sind **persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich**. Der nachlässige Umgang mit Risiken, unter anderem im Bereich Informationssicherheit, heißt Unternehmenswerte aufs Spiel zu setzen.

WARUM ISO 27001

- **Schutz der Unternehmenswerte**
- **Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sicherstellen**
- **Vertrauen** bei Stakeholdern **festigen**
- **Geschäftsrisiken und Schutzbedarf sind identifiziert**
- **Verfügbarkeit** und **Stabilität** von IT-Systemen **signifikant erhöhen**
- **Dokumentierter Nachweis** der Informationssicherheit
- **Reduzierung des Haftungsrisikos** für Geschäftsführung und Verwaltungsrat

50% aller Unternehmen, die wichtige Daten verloren haben, konnten sich nie davon erholen. 90% dieser Unternehmen mussten in der Folge innerhalb von 2 Jahren ihre Geschäftstätigkeit aufgeben (Quelle: Center for Research in Information Systems, University Texas).

Das bedeutet: Die Verfügbarkeit und Stabilität der IT-Systeme muss jederzeit gewährleistet sein.

ISMS und Risikoanalyse

Chancen zu entdecken ist die natürliche Aufgabe des Managements eines Unternehmens.

Ein Managementsystem schützt Unternehmenswerte

Ein verlässliches und dauerhaft funktionsfähiges Informationssicherheitsmanagement wird zu einem immer wichtigeren Erfolgsfaktor für Unternehmen. Kunden, Partner und Lieferanten sowie staatliche Organe erwarten, dass die Daten – und somit die Unternehmenswerte – optimal durch ein Sicherheitskonzept geschützt und Risiken frühzeitig erkannt werden.

EINFACH MACHEN -
Transparenz schafft Sicherheit

Die Analyse der Risiken gehört ebenfalls dazu - wird aber zu oft unterschätzt. Die ISO 27001 ist der Zertifizierungsstandard für ein Informationssicherheitsmanagementsystem (ISMS). Ein ISMS ist gekennzeichnet durch ein Risikomanagement, welches darauf abzielt angemessene technische und organisatorische Maßnahmen gegen identifizierte Risiken zu ergreifen. Ausgangspunkt sind hierbei die Unternehmenswerte (engl. Assets), die einer Analyse nach dem Verlust von Verfügbarkeit, Integrität und Vertraulichkeit (Schutzziele des ISMS) unterzogen werden.

Die Einführung des ISMS und die konsequente Umsetzung stellen sicher, dass normierte Abläufe dauerhaft eingehalten werden. Was schwarz auf weiß geschrieben steht und kontrolliert, aktiv umgesetzt und ständig verbessert wird, führt zu verlässlichen Prozessen.

Es geht nicht vorrangig um den Schutz gegen Viren und Trojaner, sondern um die dauerhafte Absicherung organisatorischer Abläufe. Wichtig ist es, die **IT als Serviceerbringer für die Geschäftsprozesse** zu betrachten.

Durch das Risikomanagement werden **Risiken klar abschätzbar** und der **Aufwand** für eine optimierte Informationssicherheit **wird auf ein gewolltes Maß reduziert. Kosten und Nutzen werden transparenter.** Damit wird deutlich, dass die Maßnahmen notwendig für die Geschäftsprozesse sind. Es wird nicht mit sporadischen Maßnahmen agiert, sondern das Notwendige im System verankert.

Daneben nehmen die Anforderungen an die Informationssicherheit durch Kunden, Gesetzgeber, Banken und Versicherungen kontinuierlich zu. Immer mehr Kunden verlangen von ihren Zulieferern den konkreten Nachweis für die Etablierung eines effektiven ISMS.

Einführung ISO 27001 - Ihr Nutzen

- **Schutz der Unternehmenswerte**
- **Stärkung des Vertrauens** bei Kunden, Geschäftspartnern und Behörden durch belegbare Informationssicherheit
- **Finanzielle Vorteile** durch Senkung von Versicherungsprämien, Kreditwürdigkeit, kleinere Fehlerkosten und weniger Ertragsausfälle
- **Reduzieren von Risiken** im Unternehmen durch den bewussten Umgang und das frühzeitige Erkennen potenzieller Risiken
- **Transparenz der zu schützenden Grundwerte** für Geschäftsführung, Verwaltungs- und Aufsichtsrat
- **Erhöhen der Verfügbarkeit und Sicherstellung der Leistungserbringung** der IT-Systeme durch IT-Business Continuity Management
- **IT-Sicherheit als integraler Bestandteil der Geschäftsprozesse**

Kontinuierliche Verbesserung

Ein wichtiges Element des ISMS ist eine Maßnahmenverfolgung, mit der die Umsetzung von Maßnahmen zur Verminderung identifizierter Risiken verfolgt wird. Zugleich dient dieses Instrument auch als Anlaufpunkt für erkannte Informationssicherheitsvorfälle. Auch geforderte Korrektur- und Vorsorgemaßnahmen werden innerhalb der Maßnahmenverfolgung bearbeitet, damit eine kontinuierliche Verbesserung des ISMS gewährleistet ist.

EINFACH MACHEN -
ISO 27001 Zertifizierung

ISO 27001 und Grundschutz

Im Gegensatz zum eher technischen Ansatz des IT-Grundschutzkataloges des Bundesamtes für Sicherheit (BSI) betrachtet diese Norm das Thema Informationssicherheit aus Sicht des Managements.

Unter anderem verlangt die Norm die Implementierung eines ISMS, einer Informationssicherheitsrichtlinie und die regelmäßige Überprüfung durch Audits. Damit erzeugt man Transparenz und Vertrauen gegenüber Kunden und Partnern.

Praxisbericht

Ein deutsches Chemieunternehmen mit erheblichen Sicherheitsanforderungen beschloss 2011 die Zertifizierung nach ISO 27001 vorzunehmen. Das Unternehmen ist in internationale Konzernstrukturen eingebunden. Die IT des Unternehmens ist komplett an externe Dienstleister vergeben.

AKRA BS wurde mit der Projektleitung und Unterstützung der Projektdurchführung beauftragt. Hierzu wurde ein gemischtes Team vom Kunden und AKRA BS gebildet. Das Managementsystem wurde in einem Zeitraum von sechs Monaten erfolgreich umgesetzt. Insbesondere die Projektdurchführung nach dem Vorgehensmodell der AKRA BS und die prozessorientierte, integrierte Herangehensweise im Projekt wurde durch den Auditor TüV Rheinland besonders lobend hervorgehoben. Die mitarbeiterorientierte Arbeitsweise der AKRA BS fand bei den Mitarbeitern des Unternehmens und der Unternehmensleitung hohe Anerkennung. Die Zertifizierung wurde erfolgreich in Quality, Time und Budget abgeschlossen.

Durch Mitarbeiter der AKRA BS wurden bereits mehrfach Projekte zur ISO 27001, mit und ohne Grundschutz, erfolgreich bis zur Zertifizierung begleitet. Gleichzeitig bietet Ihnen die AKRA BS praktisch erprobte Verfahren und Werkzeuge zur Umsetzung des Projektes.

AKRA Business Solutions GmbH ist ein Hamburger Beratungsunternehmen für Geschäftsprozessorganisation, Integrierte Managementsysteme und SAP®-Beratung. Wir haben unsere Schwerpunkte in den Branchen Energie, Chemie und Logistik und sind spezialisiert auf die Belange von Hochzuverlässigkeitsunternehmen.

Unser Unternehmen bietet Beratung, Projektunterstützung und IT-Lösungen bei Aufbau und Einführung von wirksamen und effizienten Managementsystemen und Prozesscontrolling verbunden mit betriebswirtschaftlichen und SAP®-Beratungsleistungen.

Kontakt

Dipl.-Ing. Hans Schmitz
Prokurist/Bereichsleiter Managementsysteme

mailto:hans.schmitz@akra.de

AKRA Business Solutions GmbH
Domstr. 17
20095 Hamburg