Sicherheit und Risiken managen mit ISO 27001

Informationen und Daten bilden die Existenzgrundlage von Unternehmen. Durch die rasante Entwicklung der Informations- und Kommunikationstechnologie ändern sich die zugehörigen Risiken in hohem Tempo: Eine Herausforderung für jedes Unternehmen. Der Management Standard ISO 27001 liefert eine praxisorientierte Basis, um Informationen systematisch zu schützen und um die Risiken aktiv zu managen.

ISO 27001: Weltweiter Standard für das Management der Informatioinssicherheit

Die strategische Bedeutung von Information im Wertschöpfungsprozess, die globale Vernetzung von Unternehmen aber auch schnell wachsende Bedrohungen verlangen nach wirkungsvollen Managementsystemen, die einen lebbaren und bezahlbaren Informationsschutz ermöglichen.

2005 wurde der Standard ISO 27001 für Informationssicherheits-Managementsysteme verabschiedet. ISO 27001 ist die Fortsetzung des erfolgreichen British Standard BS 7799. Dank ISO wird das Informationssicherheits-Management ähnliche Bedeutung erlangen wie Qualitäts-Management.

Marktkenner erwarten ein rasantes Wachstum der Zertifizierungen. Das ISO 27001-Zertifikat wird als Qualitätslabel für risikobewusste Unternehmensführung anerkannt.

Die elementaren Vorteile von ISO 27001

- Der Standard beschränkt sich nicht auf technologische Massnahmen, sondern legt den Schwerpunkt auf eine Informationssicherheit mit einer Rundumsicht fürs ganze Unternehmen.
- ISO 27001 erachtet Informationssicherheit als umfassenden Prozess. Dies ist eine wirkungsvolle Unterstützung des Managements, da Prozesse gezielt geplant, betrieben, überwacht, gemessen und optimiert werden können.
- ISO 27001 verlangt periodisch durchzuführende Analysen und Bewertungen der Informationsrisiken. Zusammen mit den in ISO 27002 beschriebenen Best Practices werden die Sicherheitskosten optimiert.
- Der Standard ist mit anderen wichtigen internationalen Standards (ISO 9001 / ISO 14001) harmonisiert. Benutzerfreundliche, integrierte Managementsysteme lassen sich ohne Überschneidungen realisieren.

Was ist Informationssicherheits-Management?

Im allgemeinen Sprachgebrauch wird IT-Sicherheit oft mit Informationssicherheit gleichgesetzt. Dies ist nicht zutreffend, denn IT-Sicherheit beschränkt sich lediglich auf die IT-Infrastruktur und elektronische Daten.

«50 Prozent aller Firmen, die wichtige Daten bei einer Katastrophe verloren haben, konnten sich nie davon erholen. 90 Prozent jener Firmen mussten in der Folge innerhalb von zwei Jahren ihre Geschäftstätigkeit aufgeben.»

Quelle: Center for Research on Information Systems, University of Texas

Die bestimmenden Erfolgsfaktoren

- Commitment der Unternehmensführung. Informationssicherheit ist Chefsache!
- Aktives Mitwirken von Management und Mitarbeitern
- Sicherheitspolitik, Ziele und Massnahmen sind auf die Kernziele des Unternehmens ausgerichtet
- praxisbezogene, systematische Risikoanalyse, die sich am Geschäft orientiert, nicht an komplizierten mathematischen Modellen,
- pragmatische Vorgehensweise bei der Realisierung des ISMS: Vorhandenes integrieren, optimieren und bei Bedarf ergänzen. Weniger ist mehr!
- Ein bewährtes Grundgerüst für das zu dokumentierende System, das alle von der Norm ISO 27001 geforderten Elemente enthält.

Informationssicherheit ist umfassend und meint den Schutz aller relevanter Informationen, Informationsquellen, Informationsträger und zugehöriger Infrastruktur. Das Ziel ist die Gewährleistung von

- Vertraulichkeit: Beschränkung des Informationszugangs auf berechtigte Nutzer,
- Integrität: Sicherung der Richtigkeit und Vollständigkeit der Information,
- Verfügbarkeit: Sicherung des bedarfsorientierten Zugangs zu Informationen.

Dabei geht es um alle Arten von Informationen und alle dazu verwendeten Medien und Hilfsmittel: Hardware, Software, elektronische Daten, Papierdokumente und mündlich kommunizierte Informationen. Mensch, Technik und Organisation sind gleichermassen im Fokus.

Das Informationssicherheits-Managementsystem (ISMS) basiert auf der Analyse der Geschäftsrisiken und umfasst alle Massnahmen, die zur Gewährleistung der Informationssicherheit notwendig sind.

Damit ist klar, dass Informationssicherheit kein IT-Thema, sondern Aufgabe und Verantwortlichkeit der Unternehmensleitung ist. Informationssicherheit gehört zur professionellen Corporate Governance.

ISO 27001 in der Praxis

Zentrales Merkmal von ISO 27001 ist, dass Informationssicherheit als geplanter, gelebter, überwachter und sich kontinuierlich verbessernder Prozess verstanden wird. Unternehmensziele, externe Einflüsse (Gesetze, Bedrohungen) und interne Rahmenbedingungen (Risikofähigkeit, Geschäftsprozesse etc.) werden berücksichtigt. Die regelmässige Überprüfung der Wirksamkeit und deren Verbesserung ist wichtiger Bestandteil des Systems. Dadurch wird es «lernfähig» und passt sich wechselnden Bedingungen an.

Der Standard lässt bei der Implementierung grosse Flexibilität zu. Es ist nur

festgelegt, was, jedoch nicht wie etwas getan werden muss. Dies hat den Vorteil, dass schlanke, pragmatische Managementsysteme aufgebaut und zertifiziert werden können. Die Wirksamkeit der Massnahmen steht im Vordergrund, ein «Wasserkopf» wird vermieden.

Zentrales Element des ISMS ist die Risikoanalyse. Systematisch werden die wichtigen Informationswerte des Unternehmens und die damit verbundenen Risiken identifiziert und der notwendige Schutz festgelegt. Die Risikoanalyse ist die Basis für angemessene Massnahmen.
Die Erfahrung zeigt, dass qualitativ-heuristische Methoden der Risikoanalyse ohne mathematischen Ballast sehr schnell zu guten, nachvollziehbaren Ergebnissen führen. Reale «Katastrophenszenarien» werden mit dem Management und verantwortlichen Mitarbeitern systematisch hinterfragt und analysiert. Anstelle von abstrakten Begriffen und Gewichtungsmethoden wird die betriebstypischeTerminologie angewandt. Der Bezug zum vertrauten Tagesgeschäft ist sehr hoch.

Die Vorteile sind:

- Der Gestaltungsprozess wird transparent und verständlich.
- Das Risikobewusstsein wird an den eigenen Geschäftsrisiken geschärft.
- Management und verantwortliche Mitarbeiter können sich wirkungsvoll einbringen und Verantwortung für getroffene Entscheidungen übernehmen.
- Eine hohe Identifikation des Managements mit dem ISMS.

Nutzen der Investition für ein ISMS

Der interne und externe Aufwand für den Aufbau und den Betrieb eines ISMS sind stark abhängig von den unternehmensspezifischen Gegebenheiten und dem gewählten Vorgehen. Die Durchlaufzeit bis zur Zertifizierung beträgt sechs bis zwölf Monate.

Ein ISMS bringt dem Unternehmen folgenden Nutzen:

^ Hohe Risikotransparenz
- bewusster Umgang mit Risiken, Reduktion des Risikopotentials
- gesteigertes Risikobewusstsein von Management und Mitarbeitern (Sicherheitskultur)
- koordinierte Sicherheitsmassnahmen: weniger Überschneidungen, weniger Lücken
- finanzielle Vorteile, kleinere Fehlerkosten, weniger Ertragsausfälle
- Sicherstellung der Leistungserbringung dank Business Continuity Management
- Erhöhung des Vertrauens von Kunden, Geschäftspartnern und Lieferanten dank gelebter Sicherheit
- Zertifizierung: kommunizierbare und belegbare Informationssicherheit mit internationaler Anerkennung

Fazit

Aktives Management der Informationssicherheit ist ein Muss für alle Unternehmen, die Informationen besitzen oder verarbeiten und eine risikobewusste Unternehmensführung anstreben. Wirkungsvoll implementiert und professionell betrieben ist ein ISMS ein wichtiger Pfeiler des Unternehmenserfolges.

Mit ISO 27001 steht erstmals ein bewährter, global anerkannter und zertifizierbarer Standard für Informationssicherheit zur Verfügung. Bereits bestehende Managementsysteme - z.B. ISO 9001 Qualitätsmanagement - werden sinnvoll ergänzt und können integriert werden. Dank der Skalierbarkeit des Standards lässt sich ISO 27001 sowohl in KMU's als auch in Konzernen effizient umsetzen.

Dieser Standard verbreitet sich schnell. Die Zertifizierung nach ISO 27001 wird zu einem Qualitätslabel für eine risikobewusste Unternehmensführung.

Kontakt

Christian Katz
wissen.org
Katz & Partner
Rudwies 17
CH-9322 Egnach
T. +41 78 603 03 40
M. katz@wissen.org