Security Management auf Basis von ISO 27001

Informationssicherheit hat allgemein den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein.

Vordringliches Ziel der Informationssicherheit ist der Schutz elektronisch gespeicherter Informationen und deren Verarbeitung, wobei stets die Vertraulichkeit, Integrität und Verfügbarkeit der unternehmenskritischen Daten zu gewährleisten ist. Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach einer Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur IT-Sicherheit entstanden. Die internationale Norm ISO/IEC 27001:2005, «Information technology – Security techniques – Information security management systems – Requirements» ist der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht. Diese spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen berücksichtigt.

ZUM AUTOR

Dipl.-Ing, FH, CISSP, Andreas Wisler
IT-Redaktor Maschinenbau
Geschäftsführer GO OUT
Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 320 91 20
www.goout.ch
info@goout.ch

Risikobeurteilung

Nachfolgend wollen wir uns mit dem ISO-Standard 27001 etwas genauer beschäftigen. Bevor Massnahmen umgesetzt werden können, muss zuerst das Risiko bekannt sein. Als Risiko wird nach ISO 73 eine Kombination aus der Wahrscheinlichkeit eines (unerwünschten, unerwarteten, schädlichen) Ereignisses und dessen Konsequenzen definiert. Es stellen sich damit zwei Fragen: Welche Ereignisse gilt es zu untersuchen? Welche Konsequenzen können daraus entstehen?

Nach ISO 27001 soll ein Informationssicherheits-Managementsystem (ISMS) aufgebaut werden, welches die Grundlage zur Identifikation und Beherrschung der Informationssicherheitsrisiken sowie zur Sicherstellung der Zuverlässigkeit von Systemen bietet.

Mögliche Ereignisse, die auf eine Organisation einwirken können sind zum Beispiel gezielte Angriffe von Personen auf technische oder organisatorische Schwachstellen; Elementarereignisse wie Erdbeben, Feuer, Wassereinbruch, Blitzschlag; Fahrlässige Handlungen oder Fehlbedienung von Systemen; Verstösse gegen Gesetze oder Verträge; sowie potentielle Schädigung von Personen (Ansehen, Gesundheit, Leben).

Die Konsequenzen können je nach Ereignis unmittelbaren monetären Schaden verursachen, aber auch Imageverlust, Verlust der Kreditwürdigkeit oder Entzug von Genehmigungen mit sich bringen.

Der ISO-Standard verlangt für jeden erkannten Informationswert die Risiken bezüglich der Verfügbarkeit, Vertraulichkeit und Integrität und gegebenenfalls weiterer Ziele zu identifizieren und abzuschätzen. Dabei gehen die Bedrohungen, Schwachstellen sowie die Einschätzung von Ausmass und Häufigkeit der Schäden ein.

Vorgehen

Wie bereits aus anderen Bereichen bekannt, verwendet auch ISO 27001 das PDCA-Modell von William Edwards Deming («Plan-Do-Check-Act» – «Planen, Durchführen, Prüfen, Handeln»):

Planen (Festlegen des ISMS)
Festlegen der ISMS-Leitlinie, -Ziele, -Prozesse und -Verfahren, die für das Risikomanagement und die Verbesserung der Informationssicherheit notwendig sind, um Ergebnisse im Rahmen aller Grundsätze und Ziele einer Organisation zu erreichen.

Durchführen (Umsetzen und Durchführen des ISMS)
Umsetzen und Durchführen der ISMS-Leitlinie, Massnahmen, Prozesse und Verfahren.

Prüfen (Überwachen und Überprüfen des ISMS)
Einschätzen und gegebenenfalls Messen der Prozessleistung an der ISMS-Leitlinie, den ISMS-Zielen und praktischen Erfahrungen, und Berichten der Ergebnisse an das Management zwecks Überprüfung.

Handeln (Instandhalten und Verbessern des ISMS)
Ergreifen von Korrekturmassnahmen und Vorbeugungsmassnahmen, basierend auf den Ergebnissen von internen ISMS-Audits und Überprüfungen des Managements und anderen wesentlichen Informationen, zur ständigen Verbesserung des ISMS.

Die ISO-Norm 27001 beschreibt das Informationssicherheits-Managementsystem im folgenden Satz: «Die Organisation muss ein dokumentiertes ISMS im Kontext ihrer allgemeinen Geschäftsaktivitäten und der Risiken, der sie sich gegenübersieht, festlegen, umsetzen, durchführen, überwachen, überprüfen, instandhalten und verbessern.»

Die gesamte ISO-2700x-Reihe besteht aus verschiedenen Standards, die sich ergänzen:

Standard	Veröffentlichung	Inhalt
ISO 27000	10.2005	Begriffsdefinitionen zum ISMS
ISO 27001	10.2005	Definition der Zertifizierungsanforderungen an ein ISMS; Löst BS 7799-2 ab
ISO 27002	2007	Leitfaden zur Implementierung, Kontrollfragen Löst ISO 17799 beziehungsweise BS 7799-1 ab
ISO 27003	in Arbeit	Einführungshilfe für ein ISMS
ISO 27004	2006	Definition von Kennzahlensystemen für ein ISMS
ISO 27005	6.2008	Risikomanagement zum ISMS Löst BS 7799-3 ab
ISO 27006	3.2007	Kriterien für Institutionen die das Audit und die Zertifizierung durchführen
ISO 27007	in Arbeit	Richtlinien für das Audit

Aufbau von ISO 27001

Die ISO-Norm 27001 ist in verschiedene Kapitel unterteilt:

Einleitung
Beschreibt den prozessorientierten Ansatz sowie die Verträglichkeit mit anderen Managementsystemen

Anwendungsbereich
Zeigt, wie die Norm angewendet werden soll.

Begriffe
Alle in der Norm verwendeten Begriffe werden in kurzen Sätzen beschrieben

Informationssicherheits-Managementsystem
Der erste Teil der Norm beschreibt die allgemeinen Anforderungen an ein ISMS. Ein wichtiger Aspekt gilt dem Festlegen (Definition des Anwendungsbereichs und der Grenzen; Identifizierung der Risiken inkl. Analyse und Bewertung; Optionen für die Risikobehandlung mit anschliessender Auswahl der Massnahmen zur Risikobehandlung) und dem anschliessenden Umsetzen und Durchführen. Die Norm verlangt hier unter anderem klar, dass ein Programm zur Schulung und Bewusstseinsbildung umgesetzt wird. Weiter gehören auch das Überwachen und Überprüfen in regelmässigen Abständen dazu. Die Norm verlangt, dass in regelmässigen Abständen, jedoch mindestens einmal pro Jahr, interne beziehungsweise eigene Audits erfolgen müssen. Diese «internen» Audits dürfen an externe, spezialisierten Firmen in Auftrag gegeben werden. Dies kann sich sicherlich lohnen, kommt doch eine unabhängige Drittmeinung dazu. Alle drei Jahre ist die Zertifizierung zu wiederholen. Sollten in den internen und externen Audits Mängel festgestellt werden, sind diese Instand zu stellen und zu verbessern.

Ein weiteres Kapitel im ersten Teil beschreibt die Dokumentationsanforderungen. Die Dokumentationen müssen Aufzeichnungen von Managemententscheidungen enthalten, sicherstellen, dass sich Aktivitäten auf Managemententscheidungen und Grundsätze zurückverfolgen lassen, und sicherstellen, dass die aufgezeichneten Ergebnisse reproduzierbar sind. Es ist wichtig, dass es möglich ist, die Beziehung von den ausgewählten Massnahmen zurück zu den Resultaten des Risikoeinschätzungs- und Risikobehandlungsprozesses nachzuweisen, und weiterhin zurück zu der ISMS-Leitlinie und den -Zielen.

Verantwortung des Managements
Der zweite Teil nimmt das Management in die Pflicht. Es muss in acht Punkten nachweisen, dass es seine Verpflichtungen wahr nimmt. Dazu gehört auch das Ermitteln und Bereitstellen der erforderlichen Ressourcen. Weiter muss die Organisation sicherstellen, dass die Schulungen, das Bewusstsein und die Kompetenzen vorhanden sind.

Managementbewertung des ISMS
Wie bereits erwähnt gilt es das ISMS mindestens einmal pro Jahr zu überprüfen. Dieses Kapitel der Norm zeigt, was die Manage-

Bild: Archiv

mentbewertung im Minimum enthalten muss. Die Ergebnisse der Managementbewertung müssen Entscheidungen und Aktivitäten zur Verbesserung und Wirksamkeit sowie die Aktualisierung des Risikoeinschätzungsplans enthalten.

Verbesserung des ISMS
Ein eigenes Kapitel erhält auch die Pflege und Verbesserung des ISMS. Wie der PDCA-Zirkel zeigt, bewegt sich das ISMS immer weiter. Ein Stillstand ist nicht möglich. Die Organisation muss Massnahmen zur Beseitigung der Ursachen von Nichtkonformitäten mit den ISMS-Anforderungen ergreifen, um deren erneutes Auftreten zu verhindern. Weiter gehören Vorbeugungsmassnahmen dazu, damit potenzielle Probleme erst gar nicht auftreten können.

Anhang A: Massnahmenziele und Massnahmen
Der Anhang umfasst die Kontrollfragen von ISO 27002 in einer kurzen Übersicht (siehe folgendes Kapitel).

Der Anhang B
Enthält die OECD-Grundsätze und das PDCA-Modell. Zum Schluss zeigt der Anhang C die Übereinstimmungen zwischen ISO 9001:2000, ISO 14001:2004 und ISO 27001.

ISO 27002/ISO 27005

Obwohl die ISO-Norm 27001 klare Anweisungen und Aufgaben enthält, ist es nicht immer einfach entsprechende Massnahmen abzuleiten. Hier helfen der neue Standard «Information Security Risk Management», kurz: ISO/IEC 27005:2008, welcher den Prozess des Security-Risk-Managements beschreibt und entsprechende Handlungsempfehlungen für Unternehmen liefert. Das Ziel von ISO 27002 «Information technology – Code of practice for information security management» definiert ein Rahmenwerk für das IT-Sicherheitsmanagement. Es befasst sich mit den erforderlichen Schritten, um ein funktionierendes IT-Sicherheitsmanagement aufzubauen und gliedert sich in elf Managementgebiete mit 39 Massnahmenzielen. Die Massnahmenziele enthalten insgesamt 133 Massnahmen (baseline controls), die zur Zielerreichung umgesetzt werden können. Die elf Managementgebiete umfassen dabei folgende Punkte: Sicherheitsleitlinie, Organisation der Informationssicherheit, Management von organisationseigenen Werten, Personalsicherheit, Physische und umgebungsbezogene Sicherheit, Betriebs- und Kommunikationsmanagement, Zugangskontrolle, Beschaffung, Entwicklung und Wartung von Informationssystemen, Umgang mit Informationssicherheitsvorfällen, Sicherstellung des Geschäftsbetriebs und Einhaltung von Vorgaben.

Dokumentation

Eine grosse Herausforderung stellt die Dokumentation dar. Ständig kommen neue Informationen dazu, die Prozesse ändern und Risiken verlagern sich. Es ist wichtig, dass das Management ständig einen Überblick über den Stand der Arbeiten hat und entsprechende (Korrektur-)Massnahmen einleiten kann. Auf dem Markt gibt es einige Programme, die hier Unterstützung bieten. Oft sind diese aber auf ein Teilgebiet beschränkt (zum Beispiel Risikoerkennung und -steuerung). Grösste Firmen haben in der Regel mit grossem Aufwand eine eigene Lösung geschaffen. Die Pflege bedarf aber eines grossen Aufwands.

Abhilfe schafft die |Q| SEC Suite der Firma WMC. Es umfasst alle Teilbereiche des Sicherheitsmanagements, von der konsequenten Weiterentwicklung des betrieblichen Informationssicherheitskonzeptes bis hin zum aktiven Management der gesamten Sicherheitsarchitektur. Auf einfachste Weise können die Geschäftsprozesse und Untersuchungsbereiche erfasst werden. Anschliessend können die Kritikalitäten dieser Prozesse bewertet werden. Ein umfassender Fragenkatalog hilft bei der korrekten Erfassung und Bewertung. Kontrollpunkte werden anschliessend sauber ausgegeben. Somit verfügt die Geschäftsleitung über ein umfassendes und einfach zu steuerndes Reporting-System.

Zertifizierung

Bei der Zertifizierung nach ISO 27001 versuchen sich die Auditoren in die Lage des Unternehmens zu versetzen und selber die Risikostellen zu identifizieren. Anschliessend werden diese mit denjenigen des Unternehmens verglichen. Sind alle vorhanden? Sind weitere erkannt worden? Werden entsprechende Massnahmen abgeleitet?

Erst danach werden die entsprechenden Massnahmen genauer angeschaut. Dabei geht es weniger um die technischen Details, sondern um die korrekte Erkennung und das Einleiten von Massnahmen. Diese Schritte müssen zwingend dokumentiert werden. Protokolle der Managementsitzungen und internen Audits bilden einen weiteren Kontrollpunkt der Auditoren. Sind auch hier Risiken und passende Massnahmen enthalten sowie Umsetzungen durchgeführt? Falls dies regelmässig und vollständig stattfindet, steht einer erfolgreichen Zertifizierung nach ISO 27001 nichts mehr im Wege.