Kontext des Unternehmens

Der erste Artikel (erschienen in MB 4/18, Seite 30) dieser ISO-Reihe zeigte eine Übersicht über die ISO-Normen 27001 und 27002. Der zweite Teil geht auf das Kapitel 4 «Kontext des Unternehmens» ein. Mit diesem Punkt haben die Unternehmen erfahrungsgemäss am meisten Mühe. Da dies jedoch die Basis für alle weiteren Dokumente, Definitionen und Messpunkte darstellt, sollte genügend Zeit dafür reserviert werden.

In einem ersten Schritt gilt es die folgende Anforderung zu erfüllen: «Die Organisation muss externe und interne Themen (Bild) bestimmen, die für ihren Zweck relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse ihres ISMS zu erreichen.»

Bei den internen Themen gilt es folgende abzudecken:

Governance

Damit sind die Führung und Steuerung des Unternehmens gemeint. Wie ist das Unternehmen strukturiert? Welche Funktionen sind vorhanden? Welche Rechte und Pflichten sind mit diesen Funktionen und Aufgaben verbunden? Ein Organigramm kann hier einen ersten Hinweis auf das Unternehmen bringen. Daraus abgeleitet werden die Funktionen und Aufgaben beschrieben.

Risiko-Management

Das Risiko-Management stellt eine Schlüsselposition dar. Im vierten Teil werden wir uns intensiv mit den Anforderungen an das Risiko-Management auseinandersetzen. Dies ist nicht nur nach ISO 27001 ein Pflicht-Thema, auch gesetzliche Anforderungen existieren, wie die IKS-Pflicht nach OR728a.

Compliance

Damit ist die Einhaltung von Gesetzen, Verträgen, aber auch internen Richtlinien gemeint. Das Unternehmen muss nach ISO 27001 A.18.1.1 die anwendbaren Gesetzgebungen und die vertraglichen Anforderungen festhalten. Denn nur was bekannt ist, kann auch eingehalten werden. Wie erwähnt gehören auch die internen Richtlinien dazu. Was wurde im Bereich der Informationssicherheit bereits definiert? Diese Punkte gilt es zu überprüfen und einzuhalten.

Assurance

Unter Assurance wird die Sicherheit oder auch Zusicherung verstanden, das heisst, dass die Regeln auch eingehalten werden. Für ein Unternehmen bedeutet dies, dass regelmässig gemessen und je nach Ergebnis entsprechende Schritte eingeleitet werden müssen.

Information und Kommunikation

Rund um diese Themen gilt es sicherzustellen, dass alle die notwendigen Informationen auch erhalten. Wenn ich die (internen) Regeln nicht kenne, wie soll ich diese dann einhalten? Eine saubere Kommunikation über alle Stufen muss sichergestellt sein, damit der Informationsfluss nicht versiegt.

Das Dreieck ist aber nicht für sich alleine, aussenherum hat es verschiedene Themengebiete, die es ebenfalls abzudecken gilt:

Erwartungen des Marktes

Der Markt entwickelt sich stetig weiter. Damit verbunden auch die Erwartungen unserer Kunden, Partner und Lieferanten. Diese gilt es im Auge zu behalten, um frühzeitig darauf reagieren zu können.

Geschäftsstrategie

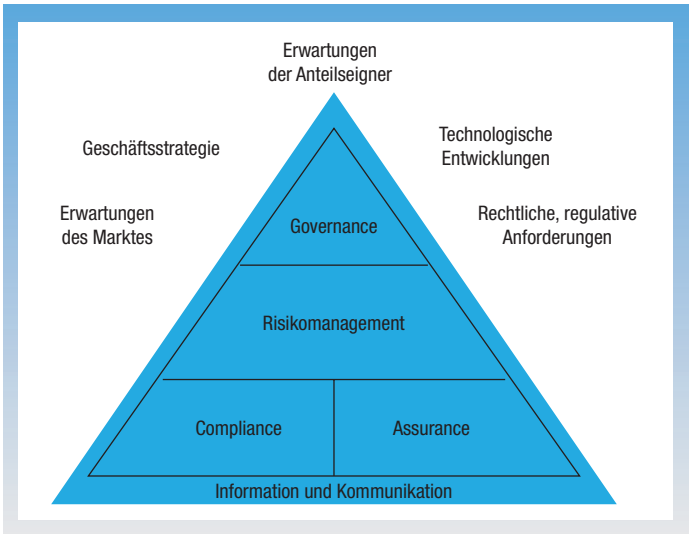
Was sieht die eigene Firmenstrategie vor? Ist ein Wachstum geplant? Werden neue Felder akquiriert? Die Strategie muss mit der Informationssicherheit in Einklang gebracht werden.

Erwartungen Anteilseigner

Was erwarten die Anteilseigner eines Unternehmens? Das kann «nur» eine Dividende sein, aber auch eine stabile Firma, genügend finanzielle Reserven, eine gesunde Wachstumsstrategie usw. können Ziele sein. Diese gilt es ebenfalls auf dem Radar zu haben.

Technologische Entwicklungen

Die vergangenen Jahre haben gezeigt, es geht immer schneller. Was heute noch neu ist, ist morgen Standard und übermorgen bereits wieder veraltet. Ein Unternehmen muss sich immer schneller mit den neuen Technologien auseinandersetzen. Welche Chancen, aber auch welche Risiken sind damit verbunden? Vernachlässigt ein Unternehmen dies, kommen die neuen Geräte fliessend dazu.



Externe und interne Themen.

Rechtliche, regulative Anforderungen

Auch auf der rechtlichen Seite ist vieles im Umbruch, immer mehr und neue Gesetze versuchen alles zu reglementieren und zu steuern. Für ein Unternehmen ist es essenziell wichtig, genügend früh zu erkennen, welche Veränderungen und damit verbunden welche neuen Anforderungen entstehen.

Wenn alle diese Punkte erarbeitet sind, gilt es im zweiten Schritt die interessierten Parteien zu bestimmen (4.2a). Idealerweise werden diese in einer Tabelle erfasst. Hier gilt es, sich in eine Unternehmung hineinzudenken und durch alle die Räumlichkeiten zu laufen. Was sehe ich? Welche Personen sind da? Welche Räume gibt es? Welche Werkzeuge und (Hilfs-)Mittel werden eingesetzt? Wie sehen Prozesse aus? Was wird selber gemacht? Wo wird auf externe Unterstützung gesetzt? Welche Dienstleistungen werden angeboten? Welche werden eingekauft? So kann eine Liste erstellt werden, wer Interesse am Unternehmen hat (oder haben könnte). Wichtig, das muss nicht zwingend einen Einfluss auf die Informationssicherheit haben. Darum wird die Tabelle mit einer Spalte «ISMS-relevant» ergänzt.

In einem weiteren Schritt wird eine Liste mit den vorhandenen Prozessen, Abläufen und mehrheitlich technischen Massnahmen erstellt. Diese Liste hilft zu erkennen, an welchen Stellen das Unternehmen Berührungspunkte mit der Informationssicherheit hat.

Die ISO-Norm verlangt nun im nächsten Schritt festzuhalten, welche Anforderungen die interessierten Parteien in Bezug auf die Informationssicherheit haben (4.2b). Die bereits erstellte Tabelle kann nun mit der Spalte «Interesse» ergänzt werden. Bei für Kunden gehosteten Systemen könnte dies beispielsweise folgende Aussage sein: «Es besteht ein grosses

Bild: Archiv

Wichtig für jedes Unternehmen: Informationssicherheit.

Interesse an der Informationssicherheit der für Kunden betriebenen Systeme (sichere Konfiguration, eingeschränkte Berechtigungen, regelmässige Wartung, Aktualisierung, vollständiges Backup). Zudem erwarten die Kunden eine fristgerechte und korrekte Lieferung beziehungsweise Auftragsausführung.»

Festlegen des Anwendungsbereichs

Im Gegensatz zu anderen Normen findet ISO 27001 nicht zwingend auf das ganze Unternehmen statt. Das Unternehmen kann den Anwendungsbereich selber festlegen. Wenn zum Beispiel ein Unternehmen über ein Rechenzentrum verfügt, kann es nur dieses als Bereich definieren. Oder eine Software-Entwicklungsfirma definiert den Bereich nur um den Entwicklungsprozess. Die Norm stellt dabei folgende Anforderung: «Die Organisation muss die Grenzen und die Anwendbarkeit des ISMS bestimmen, um dessen Anwendungsbereich festzulegen».

Wir haben ja inzwischen eine Tabelle erstellt und ergänzen diese um die entsprechende Spalte. Was von den erwähnten Punkten gehört in den Anwendungsbereich? Nun gilt es im Organigramm festzulegen, welche Organisationseinheiten in den Fokus gehören. Damit verbunden, welche Prozesse, Standorte, IT-Netzwerkbereiche, (Kunden-)Daten oder Lieferanten müssen im Rahmen des ISMS genauer betrachtet werden. Anhand dieser Informationen kann eine geeignete Ausrichtung des ISMS, inkl. der Schnittstellen und Abhängigkeiten erfolgen. Hinweis: bei kleinen Unternehmen sollte der Anwendungsbereich direkt auf das gesamte Unternehmen gesetzt werden, da eine Unterscheidung oft einen Mehraufwand mit sich bringt, zum Beispiel wenn zwei getrennte HR-Prozesse umgesetzt werden müssen.

Die Norm fordert explizit, dass dies als dokumentierte Information vorliegen muss. So steht auch ein Nachweis für die externen Auditoren zur Verfügung.

Informationssicherheits-Managementsystem

Die letzte Anforderung im Kapitel 4 ist ein Einzeiler. Darin wird gefordert, dass ein ISMS aufgebaut, verwirklicht, aufrechterhalten und fortlaufend verbessert werden muss. Der bekannte PDCA-Zyklus (Plan-Do-Check-Act) gilt es zu etablieren. Das ISMS darf keine einmalige Sache sein. Die Norm definiert zwar keinen fixen Rhythmus, aber ein jährlicher Zyklus sollte eingehalten und dokumentiert werden.

Die Norm macht übrigens keine Anforderung an die eingesetzten Werkzeuge. Es kann sowohl Word und Excel zum Einsatz kommen, wie auch ein professionelles Tool. Der Markt bietet hier eine Vielzahl von Möglichkeiten. Gerade für das Erfassen und Bewerten der Assets lohnt es sich, ein (einfaches) Tool zu evaluieren. Weiter muss die Risikoanalyse nachvollziehbar durchgeführt werden. Möglichkeiten für diese Durchführung der Risikoanalyse folgen im vierten Blog-Artikel.

Zusammenfassend kann festgehalten werden, dass dieser erste Schritt komplex, aber enorm wichtig ist. Ohne entsprechende Basis ist es schwer, ein funktionierendes und vor allem vollständiges ISMS aufzubauen. Investieren Sie genügend Zeit in die Grunderfassung des Kontextes, der interessierten Parteien und deren Anforderungen. Sie sparen sich damit später Zeit und Geld.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch