Andreas Wisler, Dipl. Ing. FH, Inhaber

ISMS: MEHRWERT ODER GELDVERSCHWENDUNG?

Die Anforderungen an die Informationssicherheit steigen stetig. Täglich ist von neuen Schwachstellen zu lesen, Angriffe auf Firmen und Privatpersonen nehmen zu und die gesetzlichen und regulativen Anforderungen sind immer aufwändiger zu erfüllen. ISO 27001 stellt die Anforderungen an ein Informationssicherheitsframework, welches den Umgang mit diesen Themen für das eigene Unternehmen vereinfacht.

Informationssicherheit wird zu einem immer wichtigeren Thema für jedes Unternehmen. Jede Firma möchte die eigenen und von Dritten übergebenen Daten sicher aufbewahren und schützen. Um für Kundinnen und Kunden, Lieferanten und Partner auch einen Nachweis zu haben, sollte ein ISMS (InformationsSicherheitsManagementSystem) aufgebaut werden. ISO 27001 bildet ein Framework, mit welchem das ISMS aufgebaut, unterhalten und stetig weiterentwickelt werden kann. Hat das System einen guten Stand erreicht, kann es durch eine akkreditierte Stelle zertifiziert und ein Nachweis ausgestellt werden.

Die ISO 27000-Reihe besteht aus verschiedenen (Sub-) Standards. Laufend kommen weitere dazu, vor allem im Bereich der sektionsspezifischen Standards in bestimmten Bereichen wie Telekommunikation, Finanzen, Gesundheitswesen und Energieversorgung. Die Basis bilden aber immer die beiden Normen ISO 27001 und ISO 27002.

Inhalt
ISO 27001 beschreibt den Aufbau des Frameworks. Die Kapitel umfassen den Kontext der Organisation (Aufbau, Prozesse, involvierte Stellen, Geltungsbereich und das Managementsystem), Anforderungen an die Führung (Verantwortung und Zuständigkeiten, Leitlinie), der Planung (Risiko-Analyse, Umsetzungspläne), die Unterstützung (Ressourcen, Kompetenzen, Schulungen, Kommunikation), den Einsatz (Planung, Durchführung und Behandlung von Risiken), die Auswertung (Überwachung, Messung, Analyse und Auswertung) sowie die stetigen Verbesserungen.

Im Anhang werden konkrete Massnahmen gefordert. Total handelt es sich um 114 so genannte Controls, aufgeteilt in 14 Kapitel. Dabei werden Themen wie die Organisation, Sicherheit des Personals, Management von Werten, Zugriffskontrolle, physische Sicherheit, Betriebssicherheit, Unterhalt und Wartung, Beziehungen mit Lieferanten, Management von Sicherheitsvorfällen sowie Business Continuity Management behandelt. Da aus der 27001 nur ersichtlich ist, wie die Massnahme lautet, hilft die 27002 weiter. Hier werden detaillierte Erklärungen an diese Controls beschrieben (Anleitung zur Umsetzung genannt).

Management-Anforderungen
Nur mit dem Auftrag ein ISMS aufzubauen, ist es aber nicht getan. Mit der letzten Überarbeitung im Jahr 2013 kamen klare Anforderungen dazu, die die Leitung des Unternehmens in die Pflicht nimmt. Die Norm definiert die folgenden Anforderungen, die es zu erfüllen gibt:

- Übernahme der Gesamtverantwortung für die Informationssicherheit
- Informationssicherheit in alle Prozesse und Projekte integrieren
- Informationssicherheit steuern und aufrechterhalten
- Erreichbare Ziele setzen
- Sicherheitskosten gegen Nutzen abwägen
- Vorbildfunktion

Oft stehen Management-Systeme in der Kritik, dass viel Papier erstellt werden muss, dies aber für das Unternehmen nur wenig bringt. Dies ist sicherlich teilweise richtig. Auch für ISO 27001 müssen einige (Pflicht-) Dokumente erstellt werden. Aus meiner Erfahrung bei verschiedenen Projekten, sind dies aber Dokumente, die ein Unternehmen auch ohne Zertifizierung erstellen sollte. Gerade die Leitlinie zum Umgang mit der Informationssicherheit ist essentiell. Aber auch die Risikoanalyse ist wichtig und wird ebenfalls für das Interne Kontrollsystem IKS nach OR 728a gefordert.

Erfolgreicher Abschluss
Wann kann der Projektstatus abgeschlossen werden? Nach der Norm gilt ein Informationssicherheitssystem dann als erfolgreich, wenn folgende Punkte erfüllt sind:

1. es gibt eine definierte Leitlinie, welche sich an den Zielen und Massnahmen der Geschäftsziele orientiert undan das Vorgehen zum Management der Informationssicherheit der Unternehmenskultur angepasst ist,
2. ein Budget für Informationssicherheitsmanagement zugeteilt wurde und die Aktivitäten zur Informationssicherheit von der Geschäftsführung unterstützt werden,
3. in der Organisation das Verständnis für die Anforderungen an Informationssicherheit verbreitet ist, Risikoanalysen durchgeführt und Notfallvorsorge betrieben wird,
4. die Benutzer hinreichend für Informationssicherheit sensibilisiert und geschult sind und die geltenden Sicherheitsvorgaben und Regelungen bekannt sind sowie
5. ein Sicherheitsprozess mit einer regelmässig wiederholten Beurteilung und Verbesserung des ISMS existiert.

Ablauf zur Zertifizierung
Wie kann ein Unternehmen nun den Weg in Richtung ISO 27001 einschlagen? Welche Dinge gilt es in welcher Reihenfolge umzusetzen? Nachfolgende Schritte zeigen einen pragmatischen Weg zu einer erfolgreichen Zertifizierung auf:

1. Unterstützung der Geschäftsleitung einholen
2. Projekt-Plan erstellen
3. Anforderungen und Rahmenbedingungen ermitteln (Interessierte Parteien, vertragliche und rechtliche Anforderungen). Dazu sollten unter anderem die folgenden Fragen beantwortet werden:

a. Welche Geschäftsprozesse gibt es und wie hängen diese mit den Geschäftszielen zusammen?
b. Welche Geschäftsprozesse hängen von einer funktionierenden, also einer ordnungsgemäss und anforderungsgerecht arbeitenden IT ab?
c. Welche Informationen werden für diese Geschäftsprozesse verarbeitet?
d. Welche Informationen sind besonders wichtig und damit in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit schützenswert und warum (z. B. personenbezogene Daten, Kundendaten, strategische Informationen, Geheimnisse wie Entwicklungsdaten, Patente, Verfahrensbeschreibungen)?
e. Gibt es Partner, Kunden oder weitere Stellen, die Zugriff auf Firmenwerte benötigen?
f. Welche vertraglichen Anforderungen müssen erfüllt werden?

4. Anwendungsbereich definieren (welcher Bereich soll zertifiziert werden?)
5. Informationssicherheitsrichtlinie erstellen
6. Prozess zur Risikoeinschätzung etablieren (Prozesse und Assets erfassen), Kritikalität definieren
7. Risikoeinschätzung durchführen
8. Umsetzung der daraus entstehenden Massnahmen
9. Durchführung von Trainings und Awareness-Schulungen
10. Internes Audit durchführen (Überprüfung des ISMS und der 114 Controls aus ISO 27002)
11. Management-Bewertung durchführen
12. Anmeldung zur Zertifizierung
13. Durchführen des ISO 27001-Audits durch eine akkreditierte Stelle

Es lohnt sich dabei, als Unterstützung oder Begleitung auf einen erfahrenen Spezialisten zu setzen. Dieser kennt die notwendigen Schritte, kann an den richtigen Stellen nachfragen und setzt auch etwas Druck auf, damit das Projekt in der Hektik des Tagesgeschäftes nicht untergeht. Doch nicht alle Schritte können durch eine externe Stelle schnell umgesetzt werden. Gerade die Beschreibung von Prozessen, das Erfassen von Assets (Firmenwerten) und der damit verbundenen Risikoanalyse kann das Unternehmen oft besser und schneller durchführen, sind diese doch schon bekannt. Die erforderlichen Dokumente, der Aufbau des ISMS, eine allenfalls notwendige Anpassung von Prozessen, die Schulung von Mitarbeitern (Stichwort Sensibilisierung) und die Begleitung durch die notwendigen Kontrollen (Internal Audit, Management-Bewertung) können abgegeben werden.

Nutzen
Durch den Aufbau eines effektiven ISMS können verschiedene Nutzen erreicht werden:

- Klare Verbindlichkeit des Managements inkl. Vorbildfunktion
- Klare Vorgaben an alle involvierten Stellen
- Regelmässige Awareness
- Nachvollziehbare Prozesse
- Risiken werden systematisch erkannt, bewertet und behandelt
- (noch) ein Wettbewerbsvorteil
- Reduktion von Audits durch Dritte
- Klare Verbindlichkeiten gegenüber Partnern, Lieferanten und Kunden.

Mit einem ISMS können klare Vorgaben definiert, umgesetzt und geprüft werden. Trotz hohen initialen Aufwands kann durch gemanagte Prozesse in der Folge Geld gespart werden. Zudem existiert ein anerkannter Nachweis, dass in diesem Unternehmen die Informationssicherheit nachhaltig behandelt und verbessert wird.

Der Ruf nach einer Cyber-Polizei ist verständlich. Aus schon erwähnten Gründen sind wir bezüglich effektiver Wirkung auf internationaler Ebene skeptisch. Mit unseren demokratisch austarierten