ISMS nach ISO 27001 für KMU. Mit den neuen Entwicklungen wie Virtualisierung oder Cloud-Computing wird die Informationssicherheit überlebenswichtig. Deshalb sind Informationen zu schützen. Dazu dient die internationale Norm ISO 27001.

VON CHRISTIAN KATZ*

Im Zentrum eines ISMS (Informationssicherheits-Managmentsystem) steht die Risikoanalyse und -bewertung. Es geht dabei um die Sicherheit der für das Unternehmen wichtigen Informationen und der dafür notwendigen Einrichtungen (IT und mehr). Dabei kommen viele Schwächen ans Licht. Oft wird das diffuse Bauchgefühl durch den systematischen Ansatz gestärkt; es werden massgebliche Risiken entdeckt, an die man bisher gar nicht gedacht hat. Die Behandlung der Risiken lässt den Unternehmer ruhiger schlafen, denn die Massnahmen wirken auf der organisatorischen, menschlichen und technischen Ebene, und deren Wirksamkeit wird überwacht. Ein ISMS nach ISO 27001 hilft auf systematische Weise, Risiken einzuschätzen und Massnahmen zur Risikobehandlung gezielt umzusetzen.

Vorurteile und Erfahrungen. Für die Informationssicherheit hat die ISO 27001 eine ähnliche Bedeutung wie die ISO 9001 für Qualität, denn die Abhängigkeit von Informationen und IT wächst über die Unternehmensgrenzen hinweg. Die negativen Erfahrungen mit der ISO 9001 in den 90er-Jahren wirken aber immer noch: Viele Unternehmer glauben, dass die ISO-Managementsystemnormen für ein KMU kaum zu erfüllen seien, zu viel Aufwand bedeuten, überflüssige Papierflut erzeugen, effizientes Arbeiten behindere und kaum Nutzen bringen. In der Zwischenzeit wurden aber die Normen weiterentwickelt. Berater und Anwender haben einen sinnvollen Umgang mit den Normen gelernt. Auch die ISO 27001 ist für Organisationen jeder Art und Grösse geeignet, denn in der Norm sind abstrakte und sinnvolle Anforderungen beschrieben. Nicht beschrieben ist die konkrete Art und Weise, wie man diese umsetzen soll.

Ein typisches KMU hat nur knappe Ressourcen, die Organisation ist einfach und das Tätigkeitsfeld überschaubar. Auch wenn vieles auf Zuruf funktioniert, weiss jeder, wer die unternehmerische Verantwortung trägt. Zudem kennen sich die Leute im Betrieb persönlich und sie wissen, was sie können. Meistens herrscht eine Vertrauenskultur. In dieser Charakteristik steckt das Potenzial, ein ISMS mit beschränktem Aufwand zu implementieren und zu betreiben, denn die Norm ist offen für einfache Lösungen. Auch für die Zertifizierung dürfen die Anforderungen auf einfache Art erfüllt sein. Meistens ist es so, dass einige Anforderungen bereits erfüllt sind, jedoch nicht systematisch und auch nicht dokumentiert. Der pragmatische Ansatz ist also, die bestehende Praxis zu beschreiben und als Vorgabe für alle zu systematisieren. Dadurch sind die Regeln und Prozesse nicht fremd. Dies führt zu einer grossen Akzeptanz.

Motivation für ein ISMS. Es gibt interne und externe Faktoren, die Unternehmer zur Einführung eines ISMS bewegen:

Intern:

> Organisationsbedarf und die Einsicht, dass viele Prozesse suboptimal laufen.
> Viele unnötige Diskussionen darüber, wer etwas auf welche Art machen muss und wie dies zu dokumentieren ist.
> Zukunftsorientierung: ISMS als strategischer Vorteil.
> Der Unternehmer kann angesichts der vermuteten Risiken nicht mehr gut schlafen.
> Der Unternehmer hat gemerkt, dass er unnötigen Haftungssrisiken ausgesetzt ist.

Extern:

> Auftrag der Aufsicht (VR)
> Forderungen oder Wünsche von Kunden
> Konkurrenzdruck

Nutzen eines ISMS. Ein ISMS, ja bereits schon das Projekt für dessen Implementierung, liefert folgende Vorteile:

Operativ:

> Die Organisation wird optimiert. Schon im Projekt kommen viele Reibungsstellen auf den Tisch.
> Kontinuierliche Verbesserung der Informationssicherheit.
> Optimaler Einsatz der Ressourcen, weil Massnahmen koordiniert werden.
> Das Managementsystem hilft, Strategien wirksam umzusetzen.
> Die Geschäftsprozesse haben auch die Informationssicherheit im Fokus.

Strategisch:

> Managementperspektive auf Risiken und Massnahmen.
> Die Unternehmenssteuerung wird präziser.
> Kontinuierliche Verbesserung als strategisches Aufgabe.
> Risiken werden bekannt, behandelt oder bewusst akzeptiert.
> Versicherungen sind günstiger, weil durch das ISMS die Risiken kleiner sind.
> Vorteile auf dem Markt.
> Die Informationssicherheit wird gestärkt (Mensch – Organisation – IT).

* **Christian Katz** ist Inhaber und Geschäftsführer von wissen.org Consulting GmbH. Er pflegt ganzheitliche Ansätze und Methoden zur Unternehmensentwicklung, Organisationsentwicklung und Implementierung von Managementsystemen. **www.wissen.org**

DIE ISO 27001:2013

Seit 2013 gibt es die ISO 27001 in einer neuen Ausgabe. Sie wurde an die High Level Structure aus Annex SL der ISO angepasst:

> Scope
> Normative references
> Terms and definitions
> Context of the organisation
> Leadership
> Planning
> Support
> Operation
> Performance evaluation
> Improvement

Die High Level Structure fordert eine intensive Auseinandersetzung mit dem Kontext des Unternehmens. Die Leitung der Organisation und das Knowhow der Mitarbeitenden erhalten ein grösseres Gewicht. Zudem verlangt sie, dass der systematische Umgang mit Risiken und Chancen in jedes zukünftige Managementsystem gehört. Die High Level Structure ist die Vorgabe u.a. auch für ISO 9001:2015, ISO 14001:2015.

> Es wird einfacher, integrierte Managementsysteme zu bauen.

> Managementsysteme, welche den Anforderungen mehrerer Normen und weiterer Compliance-Kriterien genügen, werden sich durchsetzen, denn sie unterstützen sowohl die strategische Ausrichtung des Unternehmens als auch dessen betrieblichen Alltag.

> Das Management von Risiken der Informationssicherheit lässt sich direkt ein (hoffentlich bestehendes) Risikomanagement integrieren.

> Dank der von der ISO vorgegebenen, klar definierten Begriffe wird manches Missverständnis vermieden.

> Auch ein Managementsystem nach ISO 27001:2013 dient eindeutig dem Business.

> Eine Besonderheit der ISO 27001:2013 ist der Annex A. Darin sind 114 Steuerungselemente für die Risikobehandlung sowie 35 Sicherheitsziele beschrieben, die das Unternehmen berücksichtigen muss.

Kultur:

> Personal ist sensibilisiert.
> Das Sicherheits- und Risikobewusstsein steigt.
> Das Personal tritt gegenüber dem gegenüber dem Kunden professioneller auf.
> Das Vertrauen des Kunden wächst.

Herausforderungen im ISMS-Projekt. Das Wichtigste ist wohl, die Anforderungen der ISO 27001 zu verstehen und so umzusetzen, dass es zum Unternehmen passt. Oft hilft genau hier ein Berater, der geübt ist im Interpretieren der abstrakten Aussagen in der Norm und hilft, pragmatische Lösungen zu entwickeln.

Das Projekt braucht über einen längeren Zeithorizont interne Ressourcen. Nötig sind eine langfristige Ressourcenplanung und ein klares Commitment für das Projekt. Die Risikoanalyse und -bewertung kann eine endlose Geschichte werden, wenn man keine Abbruchkriterien festlegt oder die Wahrscheinlichkeiten und Auswirkungen allzu genau berechnen will. Alle erkannten Aufgaben sollten in die Geschäftsprozesse integriert werden. Voraussetzung dafür ist eine Geschäftsprozessübersicht. Diese kann am Anfang des Projektes erarbeitet werden. Die Dokumentation ist möglichst schlank, jedoch ausreichend detailliert zu gestalten:

> Vorgaben, Regeln, Prozessbeschreibungen, Verfahrensanweisungen, Checklisten usw.
> Nachweise, die zeigen, dass die Regeln eingehalten wurden und dass das ISMS wirkungsvoll ist.

Aufwand für die Implementierung. Bei überschaubaren KMU ist die Spanne sehr weit: Der interne Aufwand kann 10 bis 80 Tage umfassen, der externe 5 bis 70 Tage (Erfahrungswerte des Autors). Folgende Faktoren beeinflussen den Aufwand:

> Reife, gut dokumentierte Organisation versus Organisation auf Zuruf
> Interne Ressourcen (Zeit, Finanzen)
> Unternehmensgrösse und Business
> Anzahl Standorte
> Vorhandensein eines Qualitätsmanagementsystem mit dokumentierten Geschäftsprozessen
> Commitment der Unternehmensleitung mit entsprechender Offenheit für Veränderungen
> Zielorientierung und Priorisierung für das Projekt.

Empfehlungen zum Vorgehen. Nehmen Sie von Anfang an einen externen Berater! Dies spart Zeit und Geld, denn es braucht einschlägige Erfahrung, die Anforderungen der Norm in die Praxis zu übersetzen. Empfehlenswert ist folgendes Vorgehen:

1. Commitment der Unternehmensleitung einholen (Sponsor, Projektsteuerung)
2. Projekt aufsetzen, Schulung der Beteiligten (Zieltermin; wer in welcher Rolle? Zeitkapazität?)
3. Auseinandersetzung mit dem Kontext, Geltungsbereich, IS-Politik festlegen
4. Gap-Analyse, Risikoeinschätzung (Dokumentenprüfung; Prüfung der bestehenden Sicherheitsmassnahmen; Risiken erkennen und einschätzen; Risikobehandlungsplan entwerfen)
5. Management Review (Aufwandschätzung, weitere Implementierung planen)
6. Umsetzung gemäss Projektplan

Als Reihenfolge für die Erarbeitung der Dokumentation empfiehlt sich:

1. Alle dokumentierten Regeln sichten.
2. Die gelebten, jedoch nicht dokumentierten Regeln dokumentieren.
3. In einem evolutionären Vorgehen die übrigen Regeln definieren: Piloten aufsetzen, ausprobieren, vom Provisorischen zum Beständigen gehen.

Fazit: Auch für ein KMU ist die ISMS-Implementierung mit beschränktem Ressourceneinsatz machbar. Ein im KMU-Feld erfahrener Berater ist eine wichtige Stütze, denn er hat die zu einem KMU passende Denkweise und liefert die passende Methodik. In verschiedenen ISMS-Projekten hat sich gezeigt, dass der grösste Nutzen dann entsteht, wenn ein Managementsystem aufgebaut wird, das nicht nur die Anforderungen der ISO 27001 erfüllt, sondern auch die Führungs- und die operativen Prozesse abdeckt.