



Lieber Interessent,

gerade im Umfeld der kleinen und mittleren Betriebe ist das Thema Informationssicherheit oft ein Stiefkind, weil andere Themen, die direkt mit dem Wertschöpfungsprozess zusammen hängen, nicht nur vermeintlich wichtiger, sondern in der Regel auch überlebensnotwendiger sind. So ist es nicht weiter verwunderlich, dass in unseren Zeiten, in der die Konjunktur gerade wieder anfängt, sich langsam zu erholen, das kostenträchtige Thema „Informationssicherheit“ nach wie vor im Hintergrund bleibt.

Dass es dennoch ein wichtiges Thema ist, bleibt unbestritten, hören wir doch täglich die mahnenden Worte in den Werbeanzeigen vieler Sicherheitsunternehmen, so dass es fast schon unsere Schmerzgrenze übersteigt. Wir können es bald nicht mehr hören, diese oft mit erhobenem Zeigefinger präsentierten „Horrorszenarien“ über insolvente Firmen, haftende Geschäftsführer und entlassene Mitarbeiter, verursacht durch riesige Sicherheitslücken im Unternehmen, die sich dann doch irgendwann einmal rächen.

Ich bin davon überzeugt, dass Sie als Verantwortlicher für Ihren Bereich, als Abteilungsleiter oder vielleicht als Geschäftsführer Ihres Unternehmens für dieses Thema bereits gewissermaßen „sensibilisiert“ sind, sonst hätten Sie sich wahrscheinlich nicht auf unsere Seite verirrt. Daher liegt es mir fern, Sie noch zusätzlich mit altbekannten Phrasen zu „schulmeistern“.

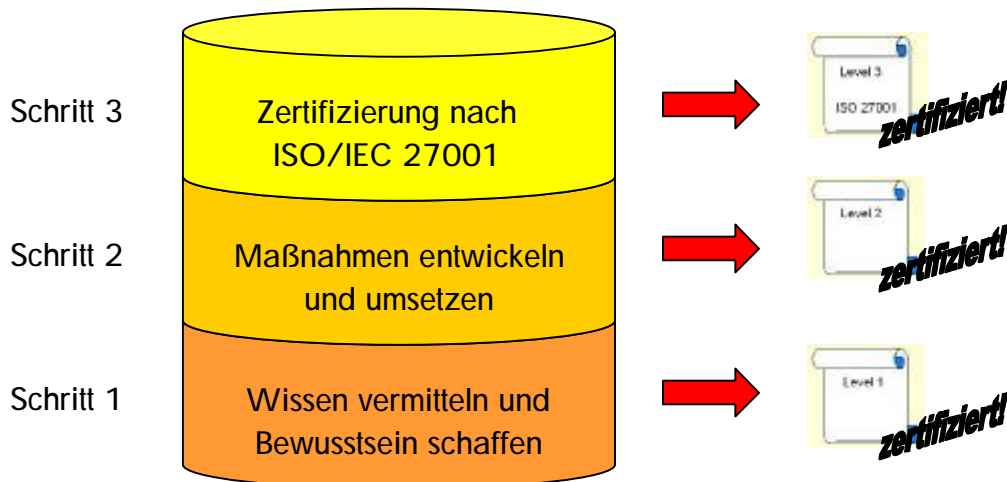
Jedoch möchte ich Ihnen als kleines Dankeschön für Ihr Interesse, einen äußerst praxisorientierten Weg vorstellen, der Ihnen zeigen soll, wie Sie mit wenig Aufwand viel erreichen und sogar in den Genuss eines anerkannten Zertifikats kommen können. Das Erfolgsrezept heißt „MODULARE ZERTIFIZIERUNG“.

Dabei wünsche ich Ihnen viel Spaß beim Lesen!

Ihr

Michael Tomas
Leiter der Zertifizierungsstelle

Kleine Schritte für Sie und Ihre Mitarbeiter – Ein Großer Schritt für Ihr Unternehmen



Schritt 1 – Wissen vermitteln und Bewusstsein schaffen:

Jedes neue Projekt braucht qualifizierte Koordinatoren und "Promoter", ohne die es nie zum erfolgreichen Abschluss gelangen würde. Daher beginnen wir ein Zertifizierungsverfahren stets mit einem Workshop, in dem den verantwortlichen Personen in Ihrem Unternehmen die Anforderungen aus der ISO 27001 sowie die Erwartungshaltung einer Zertifizierungsstelle näher gebracht werden. Das Ziel ist es, Ihr Unternehmen in die Lage zu versetzen, ein Informationssicherheits-Managementsystem nach ISO 27001 aufzubauen, zu unterhalten und weiter zu entwickeln. Sie werden sehen, dass dies gar nicht so schwer ist.

In den Tagen nach dem Workshop beginnt dann eine strukturierte Risikoanalyse, bei der es darum geht, die materiellen und ideellen Werte Ihres Unternehmens zu erfassen und auf deren Schwachstellen hin zu analysieren. Diese Risikoanalyse führen Sie entweder selbst oder mit externer Hilfe durch. Die fruchtbaren Diskussionen, die sich bei diesem Schritt entwickeln, lassen Sie meistens bereits im Vorfeld Schwerpunkte erkennen, die zukünftig angegangen werden sollen. Durch die gewonnen Erkenntnisse aus der Risikoanalyse lässt sich ein Maßnahmenplan entwickeln, der die Schwachstellen größtenteils eliminieren soll. Ein Restrisiko wird hier ganz bewusst als fester Bestandteil unternehmerischen Handelns akzeptiert.

Wir als Zertifizierungsstelle prüfen und bestätigen hierbei die Nachvollziehbarkeit und Transparenz Ihrer Risikoanalyse – also dass Sie sich quasi „Ihrer Risiken bewusst sind“ – und beurkunden dies mit einem Zertifikat (Level 1).

Sie lernen ...

- was wir als Zertifizierungsstelle von einer zu zertifizierenden Organisation erwarten
- wie wir den Standard interpretieren
- mit welchem Aufwand Sie bei einer Zertifizierung rechnen müssen (intern und extern)
- einen der gangbaren Wege Ihre Risiken zu analysieren
- die Meilensteine eines derartigen Projektes
- einen pragmatischen Ansatz, realistisch und schlank
- dass Sie nicht nur das „Stück Papier“ (Zertifikat) sondern auch einen echten Mehrwert für Ihr Unternehmen erreichen können

Sie werden ...

- sich Ihrer Risiken bewusst sein
- Ihre Risiken bewerten und entsprechende Schlussfolgerungen ziehen
- einen Teil Ihrer Risiken als Grundlage unternehmerischen Handelns akzeptieren
- einen Prozess implementieren, Ihre Risiken regelmäßig zu bewerten
- durch kompetente Spezialisten auf Ihrem Weg begleitet werden

Schritt 2 – Maßnahmen entwickeln und umsetzen:

Aus der Risikoanalyse entwickeln Sie nun Maßnahmen, die Sie in einem Informationssicherheits-Managementhandbuch (ISMS-Handbuch) dokumentieren, welches später als Arbeitsgrundlage für Ihre Sicherheitskoordinatoren dient und die Basis für eine spätere akkreditierte Zertifizierung nach ISO/IEC 27001 darstellt. Unsere Philosophie heißt hier ganz pragmatisch: "Klasse statt Masse".

Unsere Aufgabe in diesem zweiten Schritt ist es, Ihr ISMS-Handbuch im Rahmen eines sog. „Desktop Reviews“ auf Konformität mit ISO/IEC 27001 zu prüfen und zu bewerten. Eventuelle Abweichungen von der Norm werden von uns in einem Abweichungsbericht erfasst und an Sie versandt. Nach erfolgreicher Beseitigung der Abweichungen beurkunden wir Ihre Konformität mit der Norm mit einem weiteren Zertifikat (Level 2).

Sie erhalten ...

- Informationen über Ihr ISMS
- ein Feedback von einer akkreditierten Zertifizierungsstelle
- eine gute Vorbereitung für ein Zertifizierungsaudit
- ein Gefühl dafür, was Sie bereits erreicht haben und welcher Weg noch vor Ihnen liegt

Schritt 3 – Zertifizierung nach ISO/IEC 27001:

Ein Zertifizierungsaudit setzt sich zusammen aus Interviews mit kompetenten Gesprächspartnern in Ihrem Hause und persönlicher Inaugenscheinnahme Ihrer Prozesse durch unsere Auditoren. Während beim Desktop Review im Schritt 2 lediglich die Dokumentenlage – also der "Soll-Zustand" – analysiert wird, so untersuchen wir während des Audits, ob dieser letztendlich der Realität entspricht – also auch in Ihrem Hause "gelebt" wird.

Zum Abschluss der Zertifizierung erhalten Sie von uns eine akkreditierte Zertifizierungsurkunde als Nachweis für ein funktionstüchtiges ISMS nach ISO/IEC 27001 (Level 3). Natürlich wird unsere Tätigkeit auch in einem Abschlussbericht dokumentiert, in dem wir alle relevanten Punkte festhalten. Auf diese Weise können Sie unsere Bewertungen jederzeit nachvollziehen.

Sie erhalten ...

- ein Gefühl dafür, wie Ihr ISMS "gelebt" wird
- ein weiteres Feedback durch eine akkreditierte Zertifizierungsstelle
- ein akkreditiertes Zertifikat für Ihr ISO/IEC 27001-konformes ISMS und erfüllen somit bereits heute die Anforderungen der nahen Zukunft

Selbstverständlich können Sie auch alle Module in einem Zug durchlaufen und dementsprechend die ersten beiden Zertifikate überspringen. Die Schritte bleiben hierbei dieselben.

Ihre Vorteile auf einen Blick:

Nicht nur „Schwarz oder Weiß“

Jeder Schritt den Sie gehen, erhöht Ihre Sicherheit um ein Vielfaches auch ohne, dass Sie das Gesamtprojekt zu Ende führen müssen.

Anerkannte Sicherheit

Nach jedem Schritt erhalten Sie ein Zertifikat von einer akkreditierten Zertifizierungsstelle als Nachweis für die Vertrauenswürdigkeit Ihres Unternehmens. Jeder Schritt erhöht damit zusätzlich Ihre Wettbewerbsfähigkeit.

Geringes Kostenrisiko

Sie können den einmal eingeschlagenen Weg nach jedem Schritt verlassen oder sich eine ausgiebige Ruhepause gönnen und stehen dennoch nicht mit leeren Händen da. Mit dem erfolgreichen Abschluss eines Moduls können Sie jederzeit mit dem nächsten Modul beginnen.

Geringe Ressourcenbindung

Bewahren Sie sich die Flexibilität, die der Markt von Ihnen fordert. Geben Sie Ihr Tempo selbst vor und setzen Ihre Mitarbeiter entsprechend ein.