



Zertifizierung nach ISO Norm 27001

Viele Unternehmen schenken dem Thema Informationssicherheits-Management noch zu wenig Aufmerksamkeit. Die Absicherung kritischer Geschäftsdaten, von Geschäftsprozessen oder der gesamten IT-Infrastruktur stehen in den wenigsten Fällen im Fokus unternehmerischen Handelns. Und dennoch sind bekannt gewordene Sicherheitsvorfälle eher selten. Nicht zuletzt aus Imagegründen werden durch Sicherheitslücken entstandene Schäden eines Unternehmens kaum öffentlich diskutiert.

Doch sind Defizite in der Informationssicherheit nicht nur ein Image-Problem. Es gibt auch eine gesetzliche Verpflichtung zur angemessenen Absicherung sensibler Daten, Prozesse oder IT-Infrastrukturen.

Gesetzesauszug: "Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden (§91 Abs.2 AktG)".

Unternehmerisches Handeln ohne Risiken ist nicht möglich. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hat durch die Änderung des §91 AktG (das übrigens auch auf GmbHs angewandt wird) die Verpflichtung des Vorstands, für ein angemessenes Risikomanagement und für angemessene interne Revision zu sorgen, explizit formuliert und damit auch zwei wichtige Attribute eines Information Security-Management-Systems beschrieben. In der Regel wird das Thema Informationssicherheit an qualifizierte Mitarbeiter delegiert. Die Verantwortung bleibt jedoch allein bei der Geschäftsleitung.

Warum eigentlich die ISO Norm 27001-Zertifizierung

Es gibt viele Standards, die sich mit dem Thema "Sicherheit" auseinandersetzen. Einer dieser Standards ist die ISO Norm 27001 – Management von Informationssicherheit.

Durch eine Zertifizierung erlangen Unternehmen die schriftliche Bestätigung, dass Ihre Geschäftsdaten und -prozesse in einen ganzheitlichen Sicherheitsprozess eingebunden wurden. Zunehmend gilt die Zertifizierung eines Informationssicherheits-Managementsystems auch als Qualitäts-Zeichen und bietet somit dem zertifizierte Unternehmen einen nicht unerheblichen Wettbewerbsvorteil. Vor allem in der Automobil- und Pharma-Industrie, die in Deutschland eine große Vorreiterrolle haben, geht der Trend verstärkt in Richtung Zertifizierung nach ISO Norm 27001. Nicht zuletzt können zertifizierte Unternehmen auf Dauer Kosten einsparen, da durch die Zentralisierung von Absicherungsmaßnahmen bereits bestehende teure Insellösungen oft abgelöst werden können.

Auf einen Blick

- Schaffung von Wettbewerbs-Vorteilen
- Erhöhung der Unternehmenssicherheit: Logisch, physikalisch, organisatorisch
- Sensibilisierung für das Thema Informationssicherheit
- Erfüllung gesetzlicher Bestimmungen
- Nutzung von Optimierungspotenzialen

Der Weg zur Zertifizierung

Schritt 1: Workshop

- 1 Jedes neue Projekt braucht qualifizierte Koordinatoren und "Promoter". Daher beginnen wir ein Zertifizierungsverfahren stets mit einem Workshop, in dem den verantwortlichen Personen in Ihrem Unternehmen die Anforderungen aus der ISO Norm 27001 sowie die Erwartungshaltung einer Zertifizierungsstelle näher gebracht werden.

Schritt 2: Risikoanalyse

- 2 Bei der strukturierten Risikoanalyse geht es darum, die materiellen und ideellen Werte Ihres Unternehmens zu erfassen und auf deren Schwachstellen hin zu analysieren. Die fruchtbaren Diskussionen, die sich bei diesem Schritt entwickeln, lassen meistens bereits im Vorfeld Schwerpunkte erkennen, die zukünftig angegangen werden sollen.

Schritt 3: Erkenntnisse umsetzen

- 3 Durch die gewonnenen Erkenntnisse aus der Risikoanalyse lässt sich ein Maßnahmenplan entwickeln, der die Schwachstellen größtenteils beseitigen soll. Ein Restrisiko wird hier bewusst als fester Bestandteil unternehmerischen Handelns akzeptiert.

Schritt 4: Maßnahmen dokumentieren

- 4 Die Maßnahmen werden in einem Informationssicherheits-Management-Handbuch (ISMS-Handbuch) dokumentiert. Dieses Informationssicherheits-Management-Handbuch dient später als Arbeitsgrundlage für Ihre Sicherheitskoordinatoren und ist die Basis für die Zertifizierung. Unsere Philosophie heißt hier: "Klasse statt Masse".

Schritt 5: Desktop Review

- 5 Beim Desktop Review wird das ISMS-Handbuch durch uns auf Konformität mit der ISO Norm 27001 geprüft und bewertet. Die Abweichungen werden von uns in einem Abweichungsbericht erfasst und an Sie versandt.

Schritt 6: Abweichungen beseitigen

- 6 Die beim Desktop Review festgestellten Abweichungen können Sie nun beseitigen. Sobald dies geschehen ist, steht einem Zertifizierungs-Audit nichts mehr im Wege.

Schritt 7: Audit

- 7 Ein Audit erfolgt in einer Mischung aus Interviews mit kompetenten Gesprächspartnern und persönlicher Betrachtung Ihrer Prozesse durch unsere Auditoren. Während beim Desktop Review 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.

Schritt 8: Abschluss Zertifizierung

- 8 Zum Abschluss der Zertifizierung erhalten Sie von uns eine akkreditierte Zertifizierungsurkunde als Nachweis für Ihr funktionstüchtiges ISMS. Selbstverständlich wird unsere Tätigkeit auch in einem Abschlussbericht dokumentiert, in dem wir alle relevanten Punkte festhalten. Auf diese Weise können Sie unsere Bewertungen jederzeit nachvollziehen.



Kontakt

Comgroup GmbH
Industriepark Würth
Drillberg 6
D-97980 Bad Mergentheim

Phone: +49 (0)7931 916 400
Fax: +49 (0)7931 916 401

E-Mail: info_d@comgroup.de
www.ccsec.com