

Case Study: Informationssicherheits-Management-System (ISMS) nach ISO 27001

Branche

Versicherungen

Projekthalt

Ziel des Projektes war die Entwicklung der wesentlichen Prozesse und Dokumente zum Aufbau eines Informationssicherheits-Management Systems, das

- eng mit den bestehenden Prozessen zum konzernweiten Risikomanagement integriert ist und
- den Anforderungen des ISO-Standards 27001 genügt.

Das Projekt umfasste dabei folgende Teilabschnitte:

- **Projekt Charta:** Die Projekt Charta sorgt für Transparenz für alle Stakeholder, auch solche die nicht Teil des Projektteams sind (z.B. das Konzernmanagement). Die Charta definiert die wesentlichen Vorgehensweisen und Verantwortlichkeiten.
- **Leitlinie zur Informationssicherheit:** Die Leitlinie zur Informationssicherheit belegt die Bedeutung der Informationssicherheit für das Unternehmen sowie die nachhaltige Unterstützung der damit verbundenen Aktivitäten durch das Konzernmanagement. Die schließt u.a. die Lenkung der Informationssicherheit, die Zuordnung der wesentlichen Verantwortlichkeiten sowie die Bereitstellung der erforderlichen Ressourcen ein.
- **Sicherheitsorganisation:** Die Sicherheitsorganisation definiert die für ein funktionierendes ISMS benötigten Rollen sowie deren Verantwortlichkeiten für die Schaffung und Aufrechterhaltung der Informationssicherheit.
- **Verwaltung der Informationswerte:** Als Grundlage für den Schutz der Informationswerte des Unternehmens wird hier festgelegt, wie Informationswerte inventarisiert, hinsichtlich ihres Schutzbedarfs klassifiziert und einem verantwortlichen "Eigentümer" zugeordnet werden.
- **Risikomanagement:** Das Risikomanagement beschreibt den Prozess der Risikoidentifizierung, -bewertung, -meldung und -behandlung.
- **Dokumentenlenkung:** Die Dokumentenlenkung legt die Richtlinienhierarchie fest und gibt den Rahmen vor, in dem alle Dokumente des ISMS zu erstellen, zu strukturieren, freizugeben und zu lenken sind.

Die Entwicklung des ISMS fand in enger Abstimmung mit dem Kunden statt, so dass nicht nur ein standardkonformes ISMS entstand, sondern auch eines, dass an die Gegebenheiten des Kunden angepasst und damit lebbar ist. Bei der Integration mit den konzernweiten Risikomanagement -prozessen wurde sichergestellt, dass die Ergebnisse das ISMS direkt im Risikomanagement verwendet werden können und etablierte Skalen und Semantiken bestehen bleiben.

Fazit

Das Projekt wurde innerhalb der festgelegten Zeit- und Budgetrahmens erfolgreich abgeschlossen. Wesentlich für den Erfolg des Projektes waren die strenge Ausrichtung nach ISO 27001 und die enge Anpassung an die Randbedingungen des Kunden.