



Die Projektron GmbH profitierte bei der **Einführung eines Informationssicherheitsmanagementsystems (ISMS)** von der vertrauensvollen Zusammenarbeit mit der *secuvera GmbH* und der *r-tec Security GmbH*. Mit der **Zertifizierung nach ISO 27001** durch die

TÜV Süd AG wurde das Projekt im Februar 2018 erfolgreich abgeschlossen.



Projektron GmbH

www.projektron.de

Branche: Softwareentwicklung
Projektdauer: Oktober 2016 - Februar 2018
Partner: *secuvera GmbH*, *r-tec Security GmbH*, TÜV SÜD AG

Gemeinsames Projekt: Einführung und Zertifizierung eines Informationssicherheitsmanagementsystems (ISMS)

von Dotchka Pentcheva

Leiterin Qualitätsmanagement und ISMS-Beauftragte | Projektron GmbH

Die Projektron GmbH entwickelt und vertreibt seit 2001 die webbasierte Projektmanagement-Software Projektron BCS. Das Kürzel BCS steht für Business Coordination Software und drückt unseren Anspruch aus, Kunden nicht nur im Projektmanagement zu unterstützen, sondern auch angrenzende Geschäftsprozesse wie das

Kundenmanagement (CRM) oder das Personalmanagement zu assistieren. Davon profitieren neben unseren mehr als 700 Kunden auch wir selbst. Denn: Alle Mitarbeiter von Projektron organisieren die eigene Arbeit mit Projektron BCS.

Ergänzend zur Software bieten wir vielfältige Serviceleistungen: Diese

reichen von der Einführungsbegleitung und Kundenbetreuung über Schulungen und Workshops bis zur Anwenderunterstützung durch unseren Support. Unsere Software entwickeln wir nach der agilen Methode Scrum. Und so erscheint quartalsweise ein neues Release von Projektron BCS.

Gründe für ein zertifiziertes ISMS

Sicherheit und Qualität genießen bei der Projektron GmbH einen hohen Stellenwert darauf basierte auch unsere Motivation, ein Informationssicherheitsmanagementsystem (ISMS) einzuführen und zertifizieren zu lassen. Das wichtigste Projektziel war: die Informationssicherheit über die gesamte Wertschöpfungskette sicherzustellen und zu erhöhen. Zudem sahen wir



einen Wettbewerbsvorteil in der Zertifizierung unserer Prozesse, Dienstleistungen und Produkte.

Der Beschluss, ein ISMS für die Bereiche Entwicklung, Support, IT-Dienstleistungen sowie der internen IT-Administration zu schaffen, wurde im Oktober 2016 gefasst.

uns von der secuvera GmbH zu den Projektzielen, der Konzeption und der Projektplanung beraten zu lassen.

In der Umsetzungsphase stand uns die r-tec Security GmbH als weiterer Beratungsdienstleister zur Seite. Das Unternehmen zählt ebenfalls

Projektbeschreibung

Das Projekt zur Einführung eines ISMS wurde im Oktober 2016 initialisiert und im Februar 2018 mit der Zertifizierung nach ISO 27001 abgeschlossen. In diesen eineinhalb Jahren wurden von den ISMS-Beauftragten, dem ISMS-Koordinator, den Fachverantwortlichen der einzelnen Prozesse sowie der Geschäftsführung ca. 150 Tage an Aufwand investiert. Die Kosten für das Projekt beliefen sich auf Basis der entstanden Aufwände und der in Anspruch genommenen Dienstleistungen auf ca. 100.000€.

Im Folgenden werden der Ablauf des Projekts und seine vier Phasen geschildert.



Unsere Partner

Im Zuge des Einführungsprojektes haben wir Dienstleistungen von zwei Beratungsunternehmen in Anspruch genommen. Diese halfen uns, ein qualitativ hochwertiges und auf unser Unternehmen angepasstes ISMS einzuführen. Für die Zertifizierung vertrauten wir auf die TÜV SÜD AG.

Die secuvera GmbH ist ein zertifizierter Sicherheitsdienstleister mit langjähriger Erfahrung in der Beratung zum Thema Informationssicherheit. Sie setzt für den effizienten Betriebsablauf die Software Projektron BCS ein und ist damit langjähriger Kunde der Projektron GmbH. Das gewonnene Vertrauensverhältnis hat uns dazu bewegt,

zu unseren Kunden, sodass auch hier bereits eine vertrauensvolle Zusammenarbeit bestand und wir auf die Projektmanagement-Kompetenz des Teams vertrauen konnten. Überzeugt haben uns die schnelle Reaktionszeit, die fachliche Expertise sowie die Erfahrung der Berater von r-tec.

Die Zertifizierung wurde durch die TÜV SÜD AG vorgenommen. Diese ist weltweit als Zertifizierungsstelle anerkannt. Aufgrund des guten Rufs und der auch hier bestehenden guten Kundenbeziehung, haben wir uns für eine Zusammenarbeit beim Thema Informationssicherheit entschieden.

Phase 1: Beratung, initiale Schulungen und Konzeption

Zum Auftakt des Projekts wurden 10 Mitarbeiter in einem dreitägigen Workshop durch secuvera im Thema ISMS und Anforderungen der ISO 27001 geschult. Dieser Workshop diente dazu, die Anforderungen an ein ISMS nach ISO 27001 kennen zu lernen, den damaligen Stand der Sicherheitsmaßnahmen zu ermitteln und eine Abweichungs- und Umsetzungsanalyse für die Entwicklung eines ISMS zu erstellen.

Anschließend erarbeitete das ISMS-Team gemeinsam mit einem Berater von secuvera das Konzept zur Anwendung der Norm auf unser Unternehmen. Insbesondere wurde eine detaillierte GAP-Analyse durchgeführt und

zur Anwendung der Norm auf unser Unternehmen. Insbesondere wurde eine detaillierte GAP-Analyse durchgeführt und die Erklärung der Anwendbarkeit erstellt.

Phase 2: Optimierung des ISMS und Integration der Prozesse und Dokumente in Projektron BCS

Mithilfe der Berater von r-tec haben wir anschließend das bestehende ISMS-Konzept ausgearbeitet und verbessert. Hierbei kam uns der Einsatz unserer eigenen Projektmanagement-Software sowie unseres internen Wiki-Systems zugute. Projektron BCS stellt Funktionen für das Prozess- und Risikomanagement bereit, wodurch wir in der Lage waren, in unserer gewohnten Umgebung schnell und einfach die ISMS-Prozesse zu dokumentieren, Schwachstellen zu ermitteln und Gegenmaßnahmen zu entwickeln.

Auf diese Art fällt es uns auch im laufenden ISMS-Betrieb leicht, den kontinuierlichen Verbesserungsprozess umzusetzen.

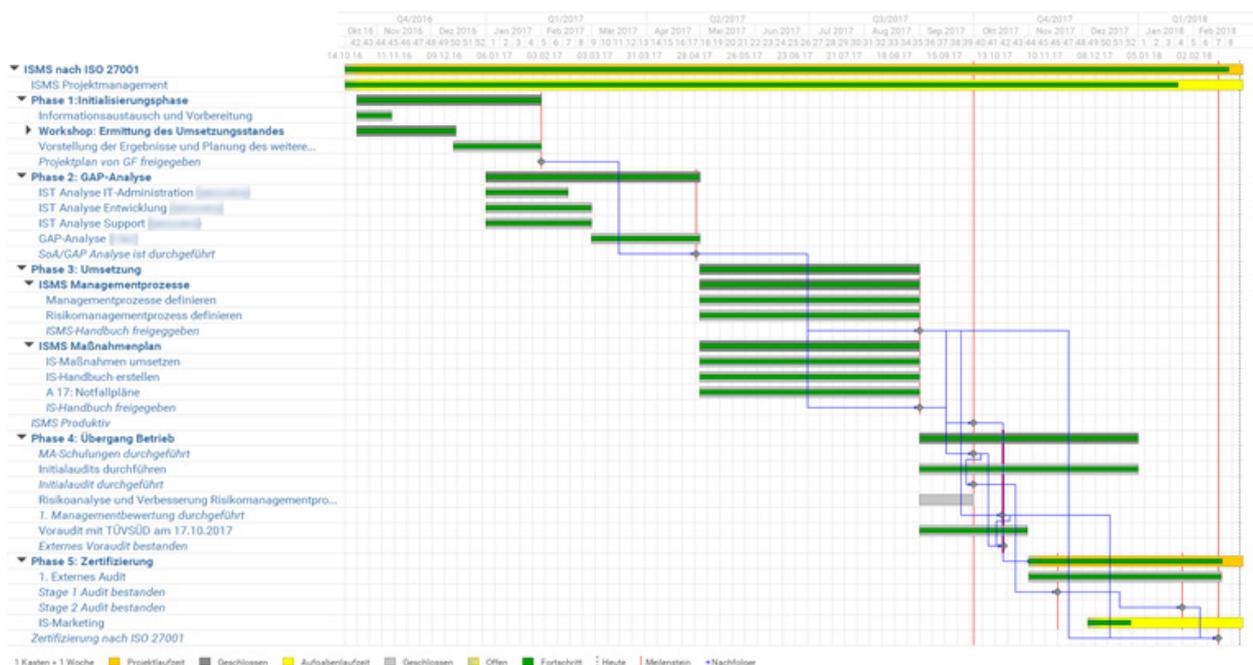
Phase 3: Interne Audits und Vorprüfung

Das etablierte ISMS wurde im Folgenden auf die Tauglichkeit und Normkonformität geprüft. Hierbei wurden insbesondere die entstandenen Managementvorgaben und deren Umsetzung betrachtet. Die Überprüfung fand in Form von drei Audit-Tagen durch einen Auditor von r-tec statt. Das Audit bestätigte uns einen in dieser Phase bereits sehr weit fortentwickelten Stand. Nichtsdestotrotz wurden auch Auffälligkeiten und Verbesserungsmöglichkeiten ermittelt, die schnellstmöglich zur Verbesserung der Informationssicherheit bei der Projektron GmbH umgesetzt

wurden.

Phase 4: Externes Audit und Zertifizierung nach ISO 27001

Die Zertifizierung des ISMS wurde durch die TÜV SÜD AG in drei Schritten vorgenommen. Durch ein eintägiges Voraudit wurde zunächst die Tauglichkeit des aktuellen Stands des ISMS für die Zertifizierung geprüft. Das externe Audit wurde anschließend an zwei Terminen durchgeführt. Am ersten Termin, dem Stage 1 Audit, wurde das Managementsystem auf Normkonformität überprüft. Da das ISMS der Projektron GmbH in diesem Termin als zertifizierungswürdig eingestuft wurde, konnte das Stage 2 Audit folgen. In diesem wurden die Regelungen für die Mitarbeiter bewertet. Die Zertifizierung konnte im Februar 2018 erfolgreich abgeschlossen werden.



Fazit

Mit der ISMS-Einführung und Zertifizierung wurde die Informationssicherheit organisatorisch in unserem Unternehmen verankert. Heute gelten über alle Unternehmensbereiche hinweg die allgemeinen Ziele der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit. Unser Informationssicherheitsmanagementsystem beinhaltet dabei alle relevanten Bestimmungen und Richtlinien. Die ISMS-Beauftragten und das Team arbeiten aktiv und kontinuierlich an der Informationssicherheit und den damit verbundenen Prozessen. Alle Mitarbeiter

erhalten bedarfsgerechte Schulungen und sind im Hinblick auf die Informationssicherheit sensibilisiert. Notfallhandbücher dokumentieren die Notfallversorgungskonzepte und ermöglichen eine zügige Reaktion und Schadensbegrenzung bei Sicherheitsvorfällen. In der Produktentwicklung und bei der Erbringung von Dienstleistungen (Hosting/SaaS, Support) berücksichtigen wir die Sicherheit von Informationen in besonderem Maße. Risiken werden laufend identifiziert und durch Gegenmaßnahmen minimiert. Wir konnten somit nicht nur unsere digitalen Geschäftsprozesse, sondern auch

die Daten unserer Kunden besser absichern.

Mit der erfolgreichen Zertifizierung nach ISO 27001 haben wir außerdem ein wichtiges Differenzierungsmerkmal gegenüber Wettbewerbern erhalten. Das ISMS wollen wir auch weiter ausbauen. Geplant sind ein Lieferantenaudit und die Einführung eines Passwortmanagements.

Weitere Kooperationsberichte und mehr Informationen zu **Projektron BCS** finden Sie unter: www.projektron.de