

## Case Study: Überprüfung und Restrukturierung des Informationssicherheitshandbuches nach ISO 27002

### Branche

Versicherungen

### Projekthalt

Ziel des Projektes war der Überprüfung des Sicherheitshandbuches des Unternehmens einschließlich eines Abgleichs (Gap Analysis) gegen den ISO-Standard 27002. Auf Grundlage der Ergebnisse der Überprüfung sollte eine Überarbeitung und Restrukturierung des Sicherheitshandbuches mit dem Ziel einer weitgehenden ISO 27002-Konformität durchgeführt werden. Während der detaillierten Überprüfung der Richtlinien wurde auf drei Kriterien hin überprüft:

- Inhalt und Aufbau: Kern dieses Teils der Analyse war die Bewertung von Inhalt, Struktur und Einheitlichkeit des Abstraktionsgrades der Richtlinien.
- Auditierbarkeit: Hierbei wurde überprüft, ob alle Maßnahmen so formuliert sind, dass ihre Umsetzung durch einen Auditor überprüfbar ist.
- ISO Konformität: Hier wurde festgestellt, welche Maßnahmenempfehlungen der ISO-Norm nicht Teil des Sicherheitshandbuches sind. Das Ergebnis wurde sowohl in Form detaillierter Empfehlungen als auch in Form von Prozentzahlen für die einzelnen Maßnahmenbereiche ausgedrückt. Im zweiten Schritt wurde empfohlen, welche Sicherheitsmaßnahmen vordringlich in das Sicherheitshandbuch aufgenommen werden sollten.

Für alle drei Kriterien wurden umfangreiche Verbesserungsvorschläge unterbreitet und mit dem Auftraggeber abgestimmt. Nach Ausschluss von ISO Bereichen welche nicht berücksichtigt werden sollten, folgte im zweiten Schritt die Restrukturierung der Richtlinie nach ISO 27002, unter Einbezug der Ergebnisse der Gap Analysis. Während der Restrukturierung wird besonders auf eine vollständige Verknüpfung der Richtlinien mit bereits bestehenden Prozessen geachtet, um letztlich ein gut integriertes und lebbares Regelwerk zu erhalten. Prozesse, welche nicht oder nur im geringem Maße vorhanden waren, werden durch entsprechende Verfahrensanweisungen ergänzt.

### Fazit

Das Projekt wurde erfolgreich im festgelegten Zeit- und Budgetrahmen abgeschlossen. Entscheidend für den Erfolg sind eine enge Abstimmung aller Prozesse mit dem Auftraggeber, die Formulierung überprüfbarer Maßnahmen und die Wahl eines angemessenen Abstraktionsgrades für die verschiedenen Richtlinienebenen.