



Integration der Anforderungen eines Informationssicherheitsmanagementsystems nach ISO/IEC 27001 in das bestehendes Qualitäts- und Umweltmanagementsystem

Branche/Kunde: Hardware- und Softwarehersteller

Zeitraum: 12 Monate

Rolle: Projektleiter, Auditoren und Managementbeauftragte

Zielsetzung:

Erhöhung des Sicherheitsniveaus im Umgang mit sensiblen Daten durch Einführung eines Informationssicherheitsmanagements nach ISO/IEC 27001.

Ausgangslage:

Bereits seit 10 Jahre bestand ein Managementsystem nach ISO 9001 und ISO 14001.

Vorgehen und Lösungsweg:

- > Projektplanung in Anpassung auf das bestehende Managementsystem.
- > Analyse der Anforderungen aus den verschiedenen Normen, Identifizieren der Redundanzen und Konsolidierung aller Anforderungen zu einem unternehmenseigenen Gesamtkonzept.
- > Erfassung aller Anforderungen aus den 3 Regelwerken in einer Bestands-Datenbank unter Nutzung bestehender Prozesse
- > Herunterbrechen der neuen Normanforderungen auf die Prozesslandschaft und Abteilungsprozesse des Unternehmens
- > Durchführung interner Audits zur Verifizierung der Normkonformität im Arbeitsalltag, insbesondere von Kombi-Audits zur Konsistenzprüfung des Gesamtkatalogs der Anforderungen
- > Schulung und Weiterqualifizierung der internen Auditoren
- > Vorbereitung und Begleitung des Zertifizierungsaudits durch akkreditierte Zertifizierungsgesellschaft

Ergebnis und Nutzen:

- > Verbesserung des Sicherheitsniveaus im Unternehmen
- > Kosteneinsparung durch Senkung der Gesamtaudits im Unternehmen (Kombi-Audits)
- > Identifizierung zusätzlicher Verbesserungspotentiale
- > Verbesserung der Qualifikation der Mitarbeiter im Umgang mit sensiblen Daten und Informationen
- > Weiterqualifizierung der internen Auditoren um bei gestiegenen Anforderungen die Autarkie des Unternehmens zu erhalten.

