Kompaktanalyse und Workshop - Vorbereitung ISO 27001 Zertifizierung

Ziel des Workshops ist es den aktuellen Stand des Unternehmens zu bestimmen und die Aufwände abzuschätzen, die erforderlich sind um eine Zertifizierung erfolgreich zu bestehen.

Inhalt der Kompaktanalyse

Bei der Vorbereitung auf eine Zertifizierung sind mehrere Vorschriften und Normen zu beachten. Dies sind vor Allem:

- **ISO/IEC 27001** : Die internationale Zertifizierungsnorm
- **ISO/IEC 27002** : Leitfaden für die Umsetzung vom Maßnahmen
- Verschiedenen Gesetze wie **BDSG, TKG, TMG**

Die Kompaktanalyse beinhaltet

1. Vorbereitung,
2. Workshop
    a. Sichtung und Diskussion von Dokumenten und Prozessen,
    b. Interviews mit verantwortlichen Personen,
    c. Begehung des Rechenzentrums anderer Infrastruktur und
3. schriftliche Ausarbeitung der Ergebnisse.

Die Durchführung erfolgt anhand eines Leitfadens und den Checklisten der Süd IT.

Ablauf der Kompaktanalyse

Vorbereitung

Im Vorfeld des Workshops stellt Ihnen die Süd-IT eine Liste mit Dokumenten und Prozessen zur Verfügung, welche von der Norm gefordert werden. Zur Vorbereitung des Workshops ist es sinnvoll, wenn die vorhandenen Dokumente zu dem Thema der Süd IT vorab zur Verfügung gestellt werden können und bereits eine gemeinsame Vorstellung über den geplanten Geltungsbereich des Zertifikates erarbeitet werden kann.

Rechtzeitig vor dem Workshop sprechen wir mit Ihnen den zeitlichen Ablauf ab und welchen Personen für Interviews und Auskünfte zur Verfügung stehen sollten.

Workshop

Geltungsbereich

Im ersten Schritt des Workshops wird der geplante Geltungsbereich des Zertifikates besprochen, da dieser wesentlich für alle weiteren Schritte ist

ISO 27001 - der Standard für Sicherheit und Vertrauen

Dokumente
Im Folgenden werden die vorhandenen Dokumente und Aufzeichnungen zusammen mit dem Verantwortlichen für Informationssicherheitsmanagement im Unternehmen besprochen und Differenzen zu den Forderungen der relevanten Dokumente erörtert.

Prozesse
Die ISO 27001 ist, neben den formalen Anforderungen in wichtigen Bereichen, eine stark prozessorientiert Norm. Neben den Dokumenten werden daher die geforderten Prozesse analysiert und deren Umsetzungsgrad im Vergleich zu den Forderungen der Norm bestimmt.

Infrastruktur
Es werden die anwendbaren Maßnahmen bestimmt und der Grad der Abweichung gegenüber der Norm ermittelt.

Personal
Ein wichtiger Aspekt ist die Auswahl und Fortbildung des Personals sowie die Prozesse er Einstellung, Verpflichtung auf Vorschriften und der Entlassung von Mitarbeitern. Die diesbezüglichen Anforderungen der Norm werden vorzugsweise mit einem Mitarbeiter der Personalabteilung oder eines Personalverantwortlichen besprochen und der Grad der Übereinstimmung mit der Norm bestimmt.

Begehung
Den Abschluss des Workshops bildet eine Begehung der wichtigsten Infrastrukturen. Dazu zählen in der Regel das Rechenzentrum, ein allgemeiner Büroraum, Räume der Personalabteilung und weitere Räume nach Anforderung.

Ausarbeitung des Ergebnisses

Als Ergebnis der Kompaktanalyse erhalten Sie eine schriftliche Dokumentation aller im Rahmen des Workshops analysierten Elemente, zusammen mit einer Feststellung zum Grad der Normerfüllung. Zu jedem Punkt erarbeiten wir Hinweisen welche Maßnahmen für eine Normerfüllung erforderlich sind.

Bei der Umsetzung der Maßnahmen unterstützen wir Sie gerne. Basierend auf unserer Erfahrung erhalten Sie eine Aufstellung der geschätzten Aufwendungen mit einem Vorschlag zur Aufteilung der Tätigkeiten auf unsere Berater und Ihre Mitarbeiter.

Kontakt

Falls Sie noch Fragen zu dem Thema
haben freue ich mich auf Ihre
Kontaktaufnahme

Dr. Stefan Krempl
089 461 3505 12
krempl@sued-it.de
ISO 27001 Auditor, Datenschutzbeauftragter