Case Study:
dhpg begleitet GOPA Group Service GmbH bei ISO/IEC 27001-Zertifizierung

„Durch die Projektbegleitung der dhpg-Sicherheitsexperten konnten wir unser Informationssicherheitsmanagement, wie geplant, Ende 2020 durch den TÜV Rheinland zertifizieren lassen und die Informationssicherheit in unserem Unternehmen weiter maßgeblich verbessern.“

Stefan Doerr, IT-Solution Architect der GOPA Group Service GmbH

1. Die Herausforderung: Informationssicherheit anhand hoher Standards sicherstellen

Die GOPA Group, Bad Homburg ist das führende deutsche Unternehmen in der Beratung von Entwicklungs- und Schwellenländern. Als international tätige Consulting-Gesellschaft gilt es, den Kunden und Geschäftspartnern ein hohes Maß an Sicherheit zu bieten und die Verfügbarkeit der an den Unternehmensprozessen beteiligten IT-Systeme zu gewährleisten. Das Unternehmen setzt auf die dhpg als erfahrenen Partner in der Umsetzung des weltweiten Standards ISO/IEC 27001 für die Bewertung der Sicherheit von Informationen und IT-Umgebungen.

In diesem Zusammenhang war es Aufgabe der dhpg, die Sicherheit der Informationen und IT-Systeme strukturiert zu prüfen, Unternehmensprozesse zur Verfügbarkeit der IT-Systeme sowie Gewährleistung der IT-Sicherheit weiterzuentwickeln und die erfolgreiche Zertifizierung durch den TÜV Rheinland vorzubereiten sowie zu begleiten.

2. Die ISO/IEC 27001-Zertifizierung: Internationale Norm für die IT-Sicherheit

Die ISO/IEC 27001-Zertifizierung ist der weltweit führende Standard für die Informationssicherheit. Sie beschreibt die Anforderungen an die Umsetzung sowie die Dokumentation eines Informationssicherheits-Managementsystems (ISMS). Die Zertifizierung ist für Unternehmen jeder Größe geeignet und bestimmt Anforderungen an die Einführung, Umsetzung, Überwachung, Dokumentation und Verbesserung eines Informationssicherheits-Managementsystems. Die ISO/IEC 27001-Norm bietet dadurch einen strukturierten, systematischen Ansatz für einen besseren Schutz vertraulicher Daten und eine höhere Verfügbarkeit von IT-Systemen. So können Risiken minimiert und Sicherheitsstandards im Unternehmen etabliert werden, die zur nachhaltigen Optimierung der Qualität der Systeme und Prozesse beitragen.

Die Zertifizierung verankert das Thema Informationssicherheit fest im Unternehmensalltag über alle Hierarchieebenen hinweg, optimiert systematisch die Informationssicherheit und passt diese an individuelle Anforderungen an. Ein robustes ISMS schützt darüber hinaus auch vor Unterbrechungen im Betriebsablauf und steigert die Wettbewerbsfähigkeit. Mit der Zertifizierung der ISMS wird die Informationssicherheit bewusst in den Fokus gerückt und dies auch nach außen präsentiert. Ein Zertifikat nach dem ISO/IEC 27001-Prüfzeichen zeigt Kunden und Geschäftspartnern, dass Informationssicherheit eine Unternehmenspriorität ist und schafft Vertrauen.

3. Der dhpg-Ansatz: Gemeinsame Weiterentwicklung des Sicherheitskonzepts

Ziel der dhpg war die Begleitung und Vorbereitung der Zertifizierung des Informationssicherheits-Managementsystems der GOPA Group Service GmbH nach dem weltweiten Standard ISO/IEC 27001 durch den TÜV Rheinland.

3. Der dhpg-Ansatz: Gemeinsame Weiterentwicklung des Sicherheitskonzepts - Vorgehensweise

- Analyse und Bestandsaufnahme der aktuellen individuellen Situation der Informationssicherheitspolitik, u.a. in den Bereichen der Kernziele Vertraulichkeit, Integrität und Verfügbarkeit.
- Durchführung einer GAP-Analyse anhand eines Katalogs von Fragen im Interviewverfahren. Das Ergebnis stellt eine detaillierte Auswertung anhand von Kennzahlen zum Reifegrad der aktuellen Informationssicherheit dar.
- Identifikation der wichtigsten Assets und Unterstützung bei der Erstellung eines Assets-Verzeichnisses.
- Identifikation von Schwachstellen und Bedrohungen in Hinsicht auf die erfassten Assets – Bewertung der identifizierten Risiken, Erstellung einer Risikolandkarte und Erarbeitung eines Risikobehandlungsplans.
- Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems und Einweisung in das Thema ISO/ICE 27001.
- Begleitung bei der Konzeptionierung und Definition eines passgenauen Sicherheitskonzepts zur Risikominimierung und Erfüllung spezifischer Anforderungen.
- Erstellung eines Maßnahmenplans zur Vorbereitung und Durchführung der TÜV-Zertifizierung basierend auf der GAP-Analyse.
- Festlegung einer Zeitplanung zur Umsetzung der identifizierten Maßnahmen.

3. Der dhpg-Ansatz: Gemeinsame Weiterentwicklung des Sicherheitskonzepts - Vorgehensweise

- Bestimmung von Verantwortlichkeiten, Sicherheitsrollen und Überwachungsmaßnahmen. Dazu gehört z.B. die Unterstützung bei der Bestellung des Information Security Officer sowie die Festlegung seiner Befugnisse und Verantwortlichkeiten.
- Erstellung eines Schulungskonzeptes.
- Schulung und interne Auditierung der Mitarbeiter der für das ISMS notwendigen Prozesse sowie zur Risikobewertung und -management in Bezug auf grundlegende Kenntnisse zur ISO/IEC 27001.
- Coaching der verantwortlichen Bereichsleiter für Auditgespräche.
- Erstellung geforderter Dokumente – z.B. Richtlinien, Anwendbarkeitserklärung und Risikobewertungen.
- Zertifizierungsvorbereitung anhand von Dokumentprüfungen und Durchführungen von Test-Audits.
- Entwicklung von Strategien zur weiteren Verbesserung des Sicherheitskonzepts und zur Weiterentwicklung der Kernziele der Informationssicherheit.

4. Das Ergebnis: Zertifizierung schafft Vertrauen in die Qualität IT-Systeme

- Erfolgreiche Vorbereitung und Durchführung der TÜV-Zertifizierung – Ausstellung des Zertifikats und Siegels.
- Weiterentwicklung der Kernziele der Informationssicherheit: Vertraulichkeit, Integrität und Verfügbarkeit.
- Nachweis der Informationssicherheit schafft Vertrauen im Unternehmen und auf Seiten von Kunden sowie Partnern.
- Optimierung der Informationssicherheit und Anpassung an spezifische Anforderungen.