CASE STUDY

Aufbau eines ISO-27001 Informationssicherheitsmanagementsystems

Cybersecurity & Governance Transformation

Executive Summary

Ein europäisches Technologieunternehmen mit internationaler Kundenbasis sah sich steigenden Anforderungen an Informationssicherheit gegenüber. Enterprise-Kunden verlangten strukturierte Sicherheitsnachweise, auditfähige Prozesse und eine klare Security Governance.

Im Rahmen eines strukturierten Transformationsprojekts wurde ein vollständiges Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 implementiert.

Projektbestandteile:

- Security Governance
- Risikomanagement
- Sicherheitsrichtlinien
- Audit-Vorbereitung
- Organisatorische Sicherheitsprozesse

Key Performance Indicators (Projektresultate)

KPI	Ergebnis	Impact
ISMS Implementierung	100 % ISO-27001 Struktur aufgebaut	Audit Readiness erreicht
Security Policies	20+ Policies & Standards	klare Governance & Prozesse
Risikomanagement	Vollständiges Risikoregister	strukturierte Risikosteuerung
Audit Readiness	Stage-1 & Stage-2 vorbereitet	erhöhte Zertifizierungschancen
Security Governance	C-Level Reporting etabliert	strategische Steuerung

Unternehmenskontext

Branche	Technologie / SaaS
Region	Europa
Projektumfang	ISO 27001 Implementierung Risikomanagement Governance Aufbau Audit Vorbereitung
Projektziel	Aufbau eines auditfähigen Informationssicherheitsmanagementsystems

Ausgangssituation

Das Unternehmen befand sich in einer Phase starken Wachstums und arbeitete zunehmend mit internationalen Unternehmenskunden zusammen. Dadurch stiegen die Anforderungen an Informationssicherheit deutlich.

Zentrale Herausforderungen:

- fehlende Security Governance
- keine strukturierte Risikoanalyse
- fragmentierte Sicherheitsrichtlinien
- zunehmende Security-Audits durch Kunden
- steigende regulatorische Anforderungen

Obwohl technische Sicherheitsmaßnahmen vorhanden waren, fehlte ein übergeordnetes Managementsystem zur strukturierten Steuerung der Informationssicherheit.

Projektziele

- Aufbau eines ISO-27001-konformen ISMS
- Einführung eines strukturierten Risikomanagements
- Implementierung zentraler Sicherheitsrichtlinien
- Verbesserung der organisatorischen Security Governance
- Vorbereitung auf externe Zertifizierungsaudits

Projektvorgehen

1. Sicherheitsanalyse

- Gap-Analyse gegenüber ISO/IEC 27001
- Analyse bestehender Sicherheitsprozesse
- Identifikation kritischer Informationswerte
- Definition des ISMS-Scopes

2. Governance Aufbau

- Definition von Rollen und Verantwortlichkeiten
- Integration von Security in Managementprozesse
- Aufbau eines Security Reporting Frameworks

3. Policy Framework

- Information Security Policy
- Access Control Policy

- Incident Response Policy
- Supplier Security Policy

4. Risikomanagement

- Risikobewertungsmethodik
- Risikoregister
- Statement of Applicability (SoA)

5. Audit Vorbereitung

- interne Audits
- Management Reviews
- Audit-Simulationen

Projektergebnisse

- vollständiges ISO-27001-konformes ISMS
- strukturierte Security Governance
- unternehmensweites Risikomanagement
- auditfähige Sicherheitsdokumentation
- verbesserte Sicherheitsnachweise für Kunden

Strategischer Mehrwert

- höheres Vertrauen bei Kunden und Partnern
- bessere Steuerung von Sicherheitsrisiken
- verbesserte Compliance mit regulatorischen Anforderungen
- professionalisierte Sicherheitsprozesse

Informationssicherheit wurde damit zu einem integralen Bestandteil der Unternehmensführung.

Über den Autor

Lucas Dinhof, B.Sc. M.Sc.

Cybersecurity & AI Governance Consultant