Informations-sicherheit & Compliance

Unterstützung bei der Einführung eines
Informationssicherheits-Managementsystemes nach ISO/IEC 27001

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY

Das ISMS: Ein strukturierter Ansatz zur Sicherung sensibler Daten und zur Erfüllung von Compliance-Anforderungen

Während die Digitalisierung enorme Chancen und Lösungen für viele der aktuellen Herausforderungen in Wirtschaft und Gesellschaft bietet, setzt sie insbesondere Unternehmen auch enormen Cyber-Bedrohungen aus.

Wir begegnen diesen Herausforderungen bei unseren Kunden Tag für Tag. Um ein möglichst hohes Niveau in der Cyber- und Informationssicherheit zu erreichen, unterstützen wir unsere Kunden bei der Implementierung ihrer IT-Sicherheitsarchitektur und bei der Umsetzung der aktuellen, hohen regulatorischen Anforderungen der IT-Compliance.

Ein solides Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 bietet einen strukturierten Ansatz zur Sicherung sensibler Daten, zur Verringerung von Risiken und zur Erfüllung von Compliance-Anforderungen wie NIS2, DORA oder dem Cyber Resilience Act. Ein ISMS bietet aber nicht nur den Schutz von Informationen, sondern es ermöglicht auch, dass ein Unternehmen in einer digitalen Welt sicher agieren kann, weil seine Daten und Systeme sicher sind.

Diese Sicherheit unterstützt die operative Exzellenz, das Vertrauen von Kunden und den langfristigen Unternehmenserfolg.

10 Gründe, warum auch Sie ein ISMS einführen sollten:

1

Schutz von sensiblen Daten
Ein ISMS trägt dazu bei, vertrauliche Informationen, einschließlich geistigen Eigentums, Kundendaten und Finanzunterlagen, vor unbefugtem Zugriff, Diebstahl oder Verstößen zu schützen.

2

Management von Sicherheitsrisiken
Ein ISMS ermöglicht die Umsetzung von Kontrollen zur Abschwächung von Bedrohungen, zur Verringerung von Schwachstellen und zur Vermeidung von Sicherheitsvorfällen.

3

Sicherstellung der Compliance
Organisationen müssen Richtlinien wie GDPR, NIS2, DORA oder dem CRA einhalten. Ein ISMS gewährleistet die Einhaltung und verringert das Risiko rechtlicher Sanktionen.

4

Stärkung des Sicherheitsbewusstseins
Ein ISMS fördert eine Sicherheitskultur, schult Mitarbeiter in bewährten Verfahren und verringert die Wahrscheinlichkeit, dass menschliches Versagen zu Sicherheitsverletzungen führt.

5

Skalierbarkeit von Sicherheitsrisiken
Wenn Organisationen wachsen, bietet ein ISMS einen skalierbaren Rahmen für die Verwaltung von Sicherheitsrisiken bei größeren Betrieben, mehr Mitarbeitern und zunehmenden Datenmengen.

6

Minimierung finanzieller Verluste
Cyberangriffe, Datenschutzverletzungen und Geldbußen können zu erheblichen finanziellen Verlusten führen. Ein ISMS verringert diese Risiken durch die Implementierung von Präventivmaßnahmen.

7

Erhalt der Geschäftskontinuität
Ein ISMS umfasst Maßnahmen zur Vermeidung von Unterbrechungen, die durch Cyberangriffe, Systemausfälle oder Katastrophen verursacht werden.

8

Gewinnen von Kundenvertrauen
Die Umsetzung eines soliden ISMS zeigt, dass sich eine Organisation für die Sicherheit ihrer Daten einsetzt und stärkt dadurch das Vertrauen und die Loyalität von Kunden.

9

Schutz des Renommees
Eine Sicherheitsverletzung kann den Ruf einer Organisation schädigen und zu einem Verlust von Vertrauen führen. Ein ISMS schützt vor solchen Vorfällen und bewahrt das öffentliche Ansehen.

10

Sichern von Wettbewerbsvorteilen
Organisationen mit einem zertifizierten ISMS, z.B. nach ISO/IEC 27001, verschaffen sich einen Wettbewerbsvorteil, indem sie ihr Engagement für die Datensicherheit demonstrieren.

Maßgeschneidertes Sicherheitsmanagement: Die Lösung für Ihre individuellen Anforderungen

Informationssicherheit ist unverzichtbar. Als Bestandteil der Unternehmensführung muss sie darauf ausgerichtet sein, die Unternehmensziele optimal zu unterstützen.

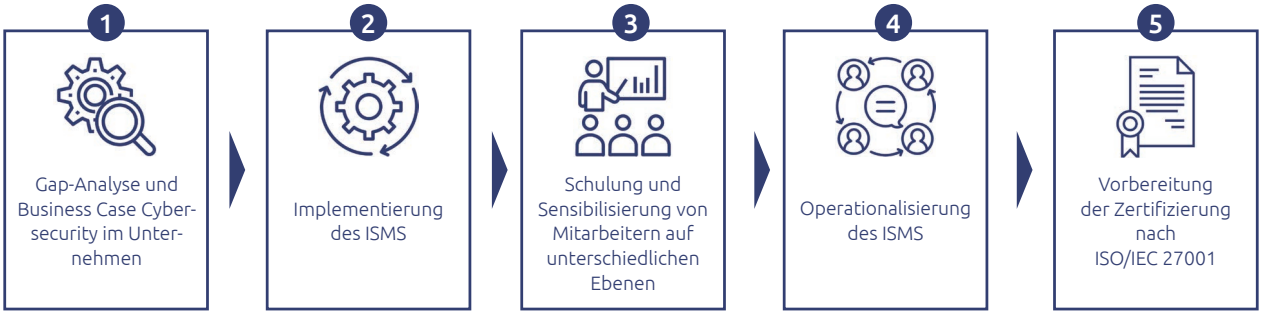
Die wachsende Komplexität von Cyberbedrohungen sowie die steigende Zahl regulatorischer und geschäftsbezogener Anforderungen machen einen strukturierten Ansatz für das Management der Sicherheitsorganisation und der Sicherheitsprozesse in einem Unternehmen unabdingbar.

Die EInführung eines Informationssicherheitsmanagementsystems nach ISO 27001 bietet die optimale Grundlage für die effiziente und effektive Umsetzung einer ganzheitlichen Sicherheitsstrategie. Ein gesundes und sich ständig verbesserndes ISMS hilft, Risiken zu mindern. Um sicherzustellen, dass Ihr ISMS auf Ihr Unternehmen zugeschnitten ist und den internationalen Standards entspricht, kann die Anleitung und Beratung durch Experten auf diesem Gebiet erforderlich sein.

Unsere Sicherheitsarchitekten und -experten arbeiten eng mit Ihnen zusammen, um ein wirklich maßgeschneidertes ISMS zu entwickeln und innovative Lösungen für Ihre speziellen Sicherheitsherausforderungen zu finden. Wir versprechen Ihnen einen soliden Aufbau Ihres ISMS, der nicht nur jedem Audit standhält, sondern auch und vor allem einen Mehrwert bietet, der es Ihnen ermöglicht, Ihre Sicherheitsprozesse zu steuern und Ihre Herausforderungen zu lösen.

5 Schritte zu einem effektiven Sicherheitsmanagement

SAMA PARTNERS verfügt über langjährige Erfahrung bei der Unterstützung von Unternehmen bei der Einführung von Informationssicherheits-Managementsystemen nach ISO/IEC 27001 sowie dem aktiven Management der Informationssicherheit und verfolgt hierbei einen klar strukturierten Ansatz in 5 Schritten:



Bei der Implementierung eines ISMS verfolgt SAMA PARTNERS sowohl die Umsetzung organisatorischer Maßnahmen – wie z.B. die Einführung von Richtlinien, Prozessen und Verfahren sowie die Ausweitung des Geltungsbereiches und den Aufbau zentraler Führungs- und Berichtsstrukturen – als auch die Umsetzung von technischen Maßnahmen, wie z.B. proaktive, korrektive und reaktive Maßnahmen. Die Etablierung eines internen Kontrollsystems inklusive eines kontinuierlichen Verbesserungsprozesses bildet den letzten Schritt bei der ISMS-Implementierung.

SAMA PARTNERS – Ihr erfahrener Partner für Cyber- und Informationssicherheit

Seit 2010 unterstützen wir Geschäftsführer und Sicherheitsmanager dabei, die Cyber-Risiken in ihrem Unternehmen zu bewerten und deren Behandlung zu einer organisatorischen Priorität zu machen. Unsere Kunden nutzen unsere branchenübergreifende Erfahrung, unser aktuelles Wissen über sicherheitsrelevante und rechtliche Compliance-Anforderungen, sowie unsere weitreichenden Einblicke in die aktuelle und sich entwickelnde Bedrohungslandschaft. Dadurch erhalten sie einen 360-Grad-Blick auf die relevanten, geschäftsbezogenen Bedürfnisse für Informations- und Cybersicherheit und damit die Möglichkeit, ihr Unternehmen sowohl resilient gegen Cyber-Angriffe zu machen, als auch regulatorische Anforderungen zu erfüllen.

Sind Sie von aktuellen Compliance-Anforderungen wie NIS2, DORA oder dem Cyber Resilience Act betroffen? Sie haben bereits ein ISMS, wissen aber nicht, ob es den aktuellen Anforderungen standhält? Nutzen Sie unsere kostenlose Erstberatung. Wir prüfen, ob Ihr Unternehmen betroffen ist und ob Ihr ISMS die aktuellen regulatorischen Anforderungen erfüllt.

Wir machen Digitalisierung sicher.

Cybersicherheit ist keine kurzfristige Modeerscheinung, sondern eine grundlegende Voraussetzung für den wirtschaftlichen Erfolg und das nachhaltige Bestehen eines Unternehmens.

Wir helfen Ihnen dabei, Cyberangriffe zu verhindern, Ihre Cyberabwehr zu stärken und einen hohen Reifegrad im Bereich der Cybersicherheit zu erreichen.

SAMA PARTNERS
Business Solutions GmbH
Hermsheimer Straße 3 (Eastsite VII)
68163 Mannheim

Tel.: +49 621 10759977
info@samapartners.com
www.samapartners.com

SAMA PARTNERS ist ein nach ISO-IEC 27001-zertifiziertes Unternehmen.

SAMA PARTNERS
THE SECURITY INTELLIGENCE COMPANY