Information Security Management System (ISMS)

Was ist ein ISMS und warum sollte man es betreiben?

Ein Information Security Management System ist eine in sich zusammenhängende Sammlung von Methoden, Vorgaben und Regeln innerhalb eines Unternehmens zur dauerhaften Steuerung und Verbesserung der Informationssicherheit.

Das primäre Ziel eines ISMS ist es, die Risiken in Bezug auf seine verarbeiteten Informationen zu kennen und zielgerichtet zu steuern.

Der Aufbau eines ISMS generiert zahlreiche Mehrwerte:

- Erfüllung regulativer und vertraglicher Anforderungen (Compliance)
- Nachweisbarkeit der Informationssicherheit gegenüber Dritten
- Identifikation, Bewertung und Behandlung der bestehenden Risiken
- Verbesserung der Wirtschaftlichkeit durch risikoorientierte Maßnahmenplanung

Im Fokus steht die Information

Im Mittelpunkt eines ISMS stehen die für das Unternehmen und dessen Zielerreichung wichtigen Informationen und alle hierfür erforderlichen Ressourcen. Hierbei handelt es sich vielfach um IT, da diese in der Regel den primären Unterstützungsprozess darstellt. Aber auch weitere Bereiche, Informationen in Form von Dokumenten, Personal und Gebäudesicherheit müssen berücksichtigt werden.

In Anlehnung an die Unternehmensziele und die Wertschöpfung werden die wesentlichen Informationen und Unternehmenswerte identifiziert und hinsichtlich ihrer Anforderungen an Vertraulichkeit, Verfügbarkeit und Integrität bewertet.

Risikoorientierter Ansatz und anerkannte Standards

In Bezug auf die ausgewählten Werte werden die bestehenden Risiken identifiziert, bewertet und behandelt. Durch das Risikomanagement wird eine valide und vor allem transparente und reproduzierbare Basis für die Planung und Implementierung angemessener Maßnahmen geschaffen. Darüber hinaus besteht die Option der gezielten Risikoakzeptanz, -vermeidung oder -übertragung.

Im Rahmen des Risikomanagements werden die zu treffenden Maßnahmen im Regelfall aus anerkannten Standards abgeleitet. Hierbei orientiert man sich insbesondere an den Standards ISO/IEC 27002:2013, dem IT-Grundschutz oder branchenüblichen Standards. Diese Standards bilden in Ergänzung zum Risikomanagement eine fundierte Basis zur Erreichung des angestrebten Informationssicherheitsniveaus.

Der Schlüssel zum Erfolg

Ein ganzheitlicher Ansatz bildet den Schlüssel zum Erfolg eines ISMS, da der Schutz von essentiell wichtigen Informationen über alle Bereiche der Wertschöpfungskette im Fokus steht. Bei der Realisierung des angestrebten Sicherheitsniveaus greift ein ISMS tief in die bestehende Organisationen und deren Prozesse ein. So werden neben der IT vor allem auch Themen, wie

- Unternehmensorganisation
- Personalsicherheit
- Physikalische Sicherheit
- Zugangskontrolle
- Störungsmanagement
- Geschäftskontinuitätsplanung

in einem ISMS berücksichtigt.

Kontinuierlicher Verbesserungsprozess

Aufbau und Betrieb eines ISMS stellen keinen einmaligen Prozess dar. Vielmehr handelt es sich um einen kontinuierlichen, iterativen Prozess. Alle Regel-Aktivitäten, wie das Risikomanagement, interne Audits und Management Reviews werden umgesetzt. Darüber hinaus werden die ISMS Prozesse, Regelungen und Ergebnisse fortlaufend kritisch hinterfragt, bei Bedarf angepasst und entsprechend eine Verbesserung herbeigeführt.

Angemessenheit und Wirtschaftlichkeit

Durch die strukturierte Koordination in einem ISMS werden vor allem komplexe und meist kostenintensive Maßnahmen nicht isoliert umgesetzt. Vielmehr geschieht dies in dem entsprechenden Kontext von bestehenden Risiken und wirtschaftlicher Realisierbarkeit. Dies schafft Synergien und hilft Kosten für die Planung, Implementierung und den fortlaufenden Betrieb nachhaltig zu senken.

Zusätzlich zeigt sich in der Praxis, dass zentrale Lösungen in der Regel ressourcenschonender, sicherer und zuverlässiger betrieben werden können als ggf. konkurrierende und sich vielfach überschneidende Individuallösungen.

Betrieb integrierter Management-Systeme

Ein ISMS muss nicht als isoliertes System entwickelt und betrieben werden. Vielmehr kann es in bestehende Management-Systeme (z.B. QMS, BCMS) integriert oder daran angelehnt werden. So werden Synergien genutzt, Redundanzen vermieden und die Akzeptanz bei den Mitarbeitern nachhaltig erhöht.

Nachweisbarkeit durch Zertifizierung

Ein ISMS, welches konform zu nationalen oder internationalen Standards (z.B. ISO/IEC 27001:2013 und IT-Grundschutz) implementiert ist, kann durch ein akkreditiertes Unternehmen zertifiziert werden.

Ein Zertifikat bietet die Möglichkeit Informationssicherheit gegenüber Dritten, wie z.B. Behörden, Wirtschaftsprüfern, Kunden und Partnern nachzuweisen.

TÜV Rheinland Services

- Gap-Analysen zur aktuellen Standortbestimmung
- Analyse bestehender ISMS
- Konzeption, Implementierung von ISMS
- Kontinuierlicher Betrieb von ISMS (externer CISO)
- Durchführung von Risk-Assessments
- Gestaltung und Durchführung von Awareness-Kampagnen
- Coaching von Informationssicherheitsverantwortlichen

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln
Tel. +49 221 806-4050
Fax +49 221 806-2293
service@i-sec.tuv.com