Das Information Security Management System – Grundpfeiler der Informationssicherheit

Welche Werte gilt es zu schützen?

Die Quantität und Qualität von Informationen nehmen in unserer stark vernetzten Gesellschaft völlig neue Dimensionen an. Die Geschwindigkeit und die Fähigkeit, Informationen gewinnbringend zu nutzen, sind somit zum entscheidenden Wettbewerbs- und Erfolgsfaktor geworden. Informationen müssen daher als weiterer Wert – neben Werkstoffen, Betriebsmitteln und ausführender Arbeit – eingeordnet werden. Konsequenterweise rückt damit verstärkt der Bedarf an nachhaltigem Schutz von Informationen in den Vordergrund.

Es gibt vielfältige Gründe, Informationen zu schützen.

Management, eine vernachlässigte Disziplin?

Informationssicherheit unterscheidet nicht nach privaten oder öffentlichen, nach kleinen, mittelständischen oder großen Organisationen, nach Branchen oder Standorten. Informationssicherheit ist permanent präsent. Gründe dafür sind Kundenanforderungen, gesetzliche Vorgaben, spezifische Vorschriften und die damit verbundenen Compliance-Anforderungen. Sie sind für Unternehmen ein Wegweiser, wie Informationen verarbeitet, gespeichert, verteilt und geschützt werden.

Nicht zuletzt fordert dies gleichwohl der Markt mit seinem Wettbewerbsdruck: Eine positive Außendarstellung und ein seriöses Image geben Kunden und Lieferanten die Gewissheit, dass die Unternehmen verantwortungsvoll mit ihren Daten umgehen. Planloser Aktionismus wäre jetzt aber der falsche Ansatz. Ohne ein geordnetes Management kommt es rasch zu einem undurchschaubaren Dickicht, wenn nicht frühzeitig angemessene Kontroll- und Steuerungsmechanismen etabliert und betrieben werden. Eine Aufgabe, die vom Unternehmens-Management getrieben und die vom gesamten Unternehmen gelebt werden muss.

Information Security Management Systeme (ISMS) sorgen dafür, dass Informationssicherheit kontrollierbar und steuerbar, transparent, effektiv und effizient betrieben wird. Immer mehr Organisationen erkennen daher die Notwendigkeit eines systematischen Vorgehens und bauen ein ISMS auf. An der Implementierung eines ISMS führt mittel- und langfristig kein

Weg vorbei, sei es nach dem internationalen Standard ISO 27001 oder nach den vom BSI veröffentlichen Standards 100-1 bis 100-4, die auf der IT-Grundschutz-Methodik basieren. In allen diesen Standards finden sich Best Practices in Form von themenspezifischen Bausteinen, die zur Implementierung und zum Betrieb eines ISMS notwendig sind.

Der Weg ist das Ziel?

Ein ISMS hat zum Ziel, IT-Risiken für die Organisation zu identifizieren, zu analysieren und durch entsprechende Maßnahmen beherrschbar zu machen. Durch einen ganzheitlichen Ansatz erzielen die Organisationen dabei entscheidende Vorteile:

- Stärkeres Sicherheitsbewusstsein für Mitarbeiter, Führungskräfte und Leitung
- Sicherung der Ziele Vertraulichkeit, Integrität und Verfügbarkeit
- Beitrag zur Sicherung der Geschäftskontinuität und damit des Erfolges
- Rechtssicherheit durch systematische Befolgung der relevanten Gesetze zur Informationssicherheit und zum Datenschutz
- Reduzierung des Haftungsrisikos der verantwortlichen Führungskräfte
- Kosteneinsparungen durch Vermeidung von Sicherheitsvorfällen

Erst ein kontinuierlicher Verbesserungsprozess (KVP), der das Ziel hat, ein nachhaltiges, stabiles und effizientes ISMS zu betreiben, kann den Schutz des Wertes „Information“ gewährleisten. Ein KVP nach dem PDCA-Zyklus von William Edwards Deming, der sich beispielsweise auch in der ISO 27001 wiederfindet, trägt dazu bei, den Reifegrad eines zuvor definierten Sicherheitsniveaus zu festigen und bei Bedarf zu steigern. Alle Aktivitäten und Maßnahmen, die zum Aufbau und Betrieb eines ISMS erforderlich sind, lassen sich so den einzelnen Prozessphasen zuordnen:

Plan – Planen:

- Festlegung von Sicherheitspolitik und -zielen sowie der relevanten Sicherheitsprozesse und Verfahren
- Festlegung der Vorgehensweise zur Risikoeinschätzung, zur Identifikation, Einschätzung und Behandlung der Risiken sowie Genehmigung des Restrisikos

Do – Durchführen:

- Umsetzung des ISMS gemäß der beschlossenen Sicherheitspolitik, Maßnahmen, Prozesse und Verfahren
- Einbindung der Mitarbeiter durch Festlegung der Verantwortung, Rechte und Pflichten sowie Auswahl und Schulung des Personals
- Lenkung der Dokumente und des Umgangs mit Daten

Check – Prüfen:

- Durchführen interner Audits, einschätzen und ggf. messen der Sicherheitslage anhand der Vorgaben sowie Auswerten von Sicherheitsvorfällen
- Berichterstattung an das Management zwecks Bewertung

Act – Handeln:

- Ergreifen von Korrektur- und Vorbeugungsmaßnahmen basierend auf den Ergebnissen der Überprüfung von Sicherheitsvorfällen
- Ableitung von Maßnahmen zur kontinuierlichen Verbesserung des ISMS

Wie ist ein ISMS aufgebaut und wie arbeitet es?

Egal nach welcher Norm (ISO 27001) oder welchem Standard (BSI 100-1) ein ISMS aufgebaut wird – die zugrundeliegenden Prinzipien, Rollen und Prozesse sind stets die gleichen. Eine wesentliche Rolle nimmt hierbei das Top-Management ein. Diese oberste Führungsebene haftet persönlich dafür, dass die Informationssicherheit in der Organisation etabliert und gelebt wird. Sie hat hierbei sogar eine Vorbildfunktion zu erfüllen. Ohne den Rückhalt und die Unterstützung des Managements kann kein ISMS in der Organisation eingeführt werden.

Verantwortung bedeutet hierbei auch die Bereitstellung von ausreichenden finanziellen Ressourcen, die die Umsetzung von technisch-organisatorischen Maßnahmen oder die Schulung aller Mitarbeiter in Fragen der Informationssicherheit gewährleisten. Aber auch der Aufbau einer Informationssicherheits-Organisation in Form einer eigenen Abteilung oder Stabsstelle sowie das dafür notwendige Personal und seine Qualifizierung gehören dazu. Dokumentiert wird diese Management-Verantwortung in der Sicherheitsleitlinie oder Sicherheitspolitik, die vom Top-Management als Aussage und Verpflichtung zugleich abgezeichnet wird – sie gibt den Rahmen und die generelle Richtung für alle weiteren ISMS-Aktivitäten vor.

Besonders große Organisationen stellen sich oft die Frage, wo sie anfangen sollen. Sie werden sicherlich nicht zeitgleich an allen Standorten weltweit damit beginnen. Für ein ISMS muss daher zunächst ein geeigneter Geltungsbereich definiert und dokumentiert werden: Für welche Geschäftsprozesse, Unternehmens-bereiche, Standorte etc. soll das ISMS gelten.

Neben der übergeordneten Sicherheitsleitlinie gibt es noch weitere Sicherheitsrichtlinien, die für einen abgegrenzten Bereich gelten (z. B. für Passwortgebrauch, Internet-Nutzung, Zugangskontrolle) und dort verbindlich für alle Beteiligten und Mitarbeiter die Leitlinien und Regelungen vorgeben, in denen sich diese bewegen dürfen. Im Form einer solchen Richtlinie ist auch die Klassifizierung der Informationen zu regeln: Wie wichtig sind die Informationen und daraus resultierenden Daten für das Unternehmen? Jede Art von Information ist dazu mindestens hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit zu beurteilen und einer Schutzbedarfsklasse, beispielsweise normal, hoch oder sehr hoch, zuzuordnen. Wie diese Klassen im Einzelnen aussehen, ist stark vom Geschäftszweck der Organisation abhängig und muss daher individuell festgelegt werden. Diese Klassifizierung ist notwendig, da im nächsten Schritt eine Risikoanalyse durchzuführen ist, die ermittelt, welche Risiken bei der Verarbeitung und Speicherung der damit verbunden Daten auftreten können.

Die Auswahl einer geeigneten Risikoanalysemethodik ist ein obligatorischer Bestandteil bei der Einführung eines ISMS. Hierbei muss aber das Rad nicht neu erfunden werden, denn Normen wie ISO 27005 oder der BSI-Standard 100-3 können dazu genutzt und individuell an die Bedürfnisse der Organisation angepasst werden.

Es gilt nun, die organisatorischen und technisch-organisatorischen Maßnahmen auszuwählen, die einen adäquaten Schutz der Informationen sicherstellen. Die Auswahl darf nicht willkürlich erfolgen, sondern muss einem risikobasierten Ansatz folgen. Je höher das Risiko ist, desto umfangreicher und damit ggf. auch kostenintensiver kann die betreffende Maßnahme ausfallen. Die ausgewählten Maßnahmen sind dann – je nach Norm oder Standard – auf unterschiedliche Art und Weise zu dokumentieren und müssen vom Management zur Umsetzung genehmigt werden.

Wie wird ein ISMS betrieben und aufrecht erhalten?

Da es sich bei dem ISMS um einen Prozess handelt, beginnt die eigentliche Arbeit erst nach der Implementierung. Ein wichtiger Punkt dabei ist die formale Dokumentation. Ein externer Auditor wird diese Dokumente im Detail prüfen, um festzustellen, ob die beschriebenen und definierten Prozesse auch in der täglichen Praxis gelebt werden. Die Erstellung von Dokumenten wie beispielsweise Sicherheitskonzepten, Systemdokumentationen, Notfallkonzepten oder Verfahrensanweisungen dient aber nicht nur formalen Aspekten. Sie stellen auch sicher, dass bei der Planung und dem Betrieb von IT-Systemen keine wichtigen Sicherheitsmaßnahmen vergessen werden und die Informationen somit ausreichend geschützt sind.

Genauso wie IT-Systeme unterliegen auch die Dokumentationen einem Lebenszyklus und müssen regelmäßig gepflegt werden. Weil sich die Sicherheitsanforderungen oder Gefährdungen im Laufe der Zeit ändern können – sei es durch neue Geschäftsfelder oder Änderungen der globalen Bedrohungslage –, muss die Organisation in regelmäßigen Abständen interne Audits durchführen. Sie muss überprüfen, ob die definierten Prozesse, Verfahren und Maßnahmen zum einen konsequent umgesetzt wurden und anderseits noch angemessen sind oder ggf. entsprechend der geänderten Risikolage angepasst werden müssen. Die Ergebnisse dieser internen Audits müssen – ebenso wie die Ergebnisse der durchgeführten Risikoanalysen – in regelmäßigen Abständen dem Management zur Prüfung (Review) vorgelegt werden. Dieses kann dann entscheiden, ob das ISMS noch ordnungsgemäß funktioniert oder angepasst werden muss. Auch hier ist wieder das Management in der Pflicht, die Verantwortung zu übernehmen – beispielsweise bei der Akzeptanz von Risiken, die sich nicht oder nur mit einem unangemessen hohen Aufwand behandeln lassen.

Ein weiterer wichtiger Punkt sind Schulung und Sensibilisierung aller Beteiligten und Mitarbeiter zum Thema Informationssicherheit. So schaffen Organisationen das Bewusstsein, dass die betreffenden Informationen wichtig sind und mit Bedacht und verantwortungsvoll behandelt werden müssen. Es gibt keine 100-prozentige Sicherheit, schon gar nicht allein durch technische Maßnahmen.

Tritt dennoch ein Sicherheitsvorfall ein, muss eine Organisation ihre Lehren daraus ziehen. Da das Ziel eines ISMS eine Optimierung der Prozesse im Rahmen eines kontinuierlichen Verbesserungsprozesses ist, muss definiert werden, wie mit Sicherheitsvorfällen im Unternehmen umgegangen wird. Wie kann ein Unternehmen aus solchen Vorfällen lernen, durch Korrekturmaßnahmen entsprechend gegensteuern oder durch Vorbeugemaßnahmen dafür sorgen, dass solche Vorfälle nicht auftreten können?

Das wichtigste bei einem ISMS ist, dass sich eine Organisation immer bewusst ist, dass es sich beim ISMS um einen Prozess handelt und nicht um ein Projekt. Die ISMS-Einführung wird zwar in Form eines Projektes durchgeführt. Doch das eingeführte ISMS muss in der Linienorganisation in der betrieblichen Praxis gelebt werden. Nur so wird es seinem Ziel gerecht, die Informationssicherheit in der Organisation dauerhaft zu verbessern.

Ein Information Security Management System berücksichtigt alle potenziellen Risikofaktoren. Um die Sicherheit des Systems zu gewährleisten, muss es kontinuierlich überprüft und verbessert werden.

Integrationsfähigkeit eines ISMS in bereits bestehende Management-Systeme

Als ein normiertes Management-System unterliegt das ISMS den gleichen Prinzipien wie bereits etablierte Management-Systeme. Rollen, Verantwortlichkeiten, Strukturen, Organisation und Dokumentation sind die Prinzipien, die ein Management-System ausmachen. Obwohl inhaltlich differenzierter und in seiner Ausprägung und Zielsetzung verschieden, kann das ISMS in bereits etablierte Management-Systeme integriert werden. So können der Wirkungsgrad und die Qualität eines ISMS anhand etablierter Qualitäts-Management-Systeme wie ISO 9001 bewertet und innerhalb eines KVP verbessert werden. Das Regelwerk der ISO 27001 lehnt sich dabei in seinem Aufbau bewusst an die von ISO 9001 bekannte Vorgehensweise des PDCA-Regelkreises an und bietet dadurch die Möglichkeit der einfachen Integration eines ISMS in ein bestehendes Management-System.

Ziel sollte es sein, das ISMS in die verschiedenen in einer Organisation betriebenen Management-Systeme soweit wie möglich strukturell und organisatorisch zu integrieren und eine gemeinsame Management-Plattform zu schaffen. So lassen sich Redundanzen vermeiden. Hier hat beispielsweise die Automobilbranche in einer Vorreiterrolle gezeigt, dass Wirtschaftlichkeit in Verbindung mit Qualitätsbewusstsein (ISO 9001), Umweltschutz (ISO 14001) und Informationssicherheit (ISO 27001) kein unvereinbarer Gegensatz sind, sondern Bestandteile einer erfolgreichen Unternehmensstrategie.

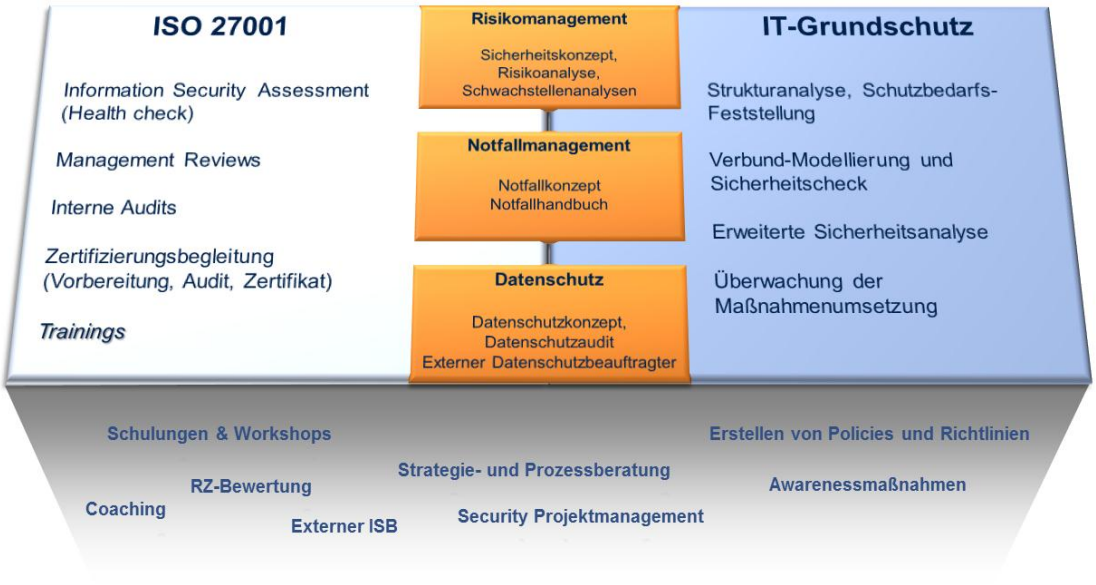
Mehr Sicherheit mit Beratung von MATERNA

Das MATERNA-Portfolio deckt sowohl Beratungsleistungen für das Verfahren zum IT-Grundschutz als auch für die Zertifizierung nach dem international gültigen Standard ISO 27001 ab. Die IT-Experten von MATERNA verfügen über langjährige Erfahrung im Umgang mit Methoden, internationalen Standards und Best Practices. MATERNA begleitet ihre Kunden von der Planung über Analyse, Konzept und Einführung bis zum Audit beziehungsweise der erfolgreichen Zertifizierung.

Unsere Leistungen

- **Beratung ISO 27001**
- **Beratung IT-Grundschutz**
- **IT-Risiko-Management (Sicherheitskonzept, Risikoanalyse, Schwachstellenanalysen)**
- **IT-Notfall-Management (Notfallkonzept und Notfallhandbuch)**
- **Datenschutz (Datenschutzkonzept, Datenschutzaudit und externer Datenschutzbeauftragter)**

Unser Portfolio in der Gesamt-Übersicht:



Kontakt

MATERNA GmbH
Information & Communications

E-Mail:
ism-consulting@materna.de
marketing@materna.de

www.materna.de