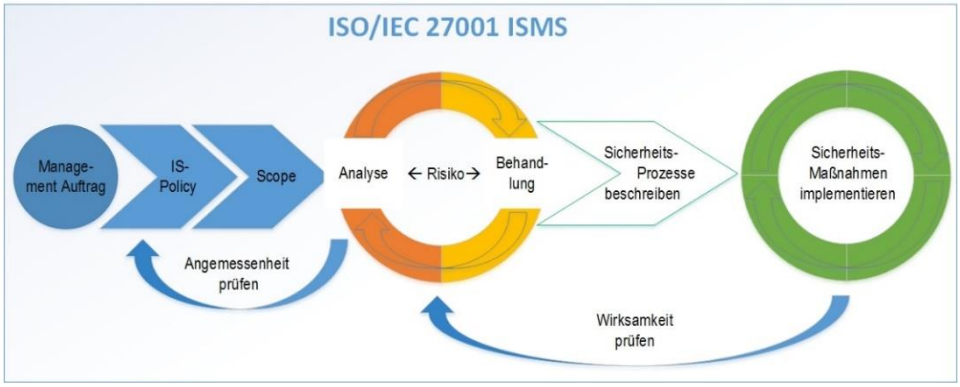
Informationssicherheit

Einführung & Betrieb eines ISMS nach ISO/IEC 27001

Nutzen eines ISMS nach ISO/IEC 27001

Aufbau und Betrieb eines Informationssicherheits-managementsystems (ISMS nach ISO/IEC 27001) bringen einem Unternehmen wichtige Vorteile bei der Aufrechterhaltung seiner Informations- und Datensicherheit. Ein ISMS bringt Transparenz hinsichtlich der Sicherheitsprozesse und zeigt mögliche Optimierungspotentiale auf. Es ermöglicht, die durch Sicherheitsvorfälle möglicherweise entstehenden Kosten zu senken und insbesondere auch die Reputation des Unternehmens zu bewahren. Ein effektiv betriebenes ISMS hilft einem Unternehmen dabei, sich rechtlich abzusichern, indem es gesetzliche und regulatorische Anforderungen auch im Sinne von „technischen und organisatorischen Sicherheitsmaßnahmen nach Stand der Technik" erfüllt.

Das Unternehmen wird in die Lage versetzt, die Sicherheit seiner Informationen und Daten dauerhaft und nicht nur ereignisorientiert zu erbringen. Die Erfüllung kann zudem durch ein weithin anerkanntes Zertifikat nachgewiesen werden. Dies schafft bei Kunden und Partnern Vertrauen und dient deshalb auch oft als Marketingargument.



ISO/IEC 27001 = IT-Sicherheit?

IT-Sicherheit trägt einen wesentlichen, oft in der ersten Wahrnehmung sogar ganz überwiegenden Beitrag zum Schutz von Informationen und Daten bei. Somit wird eine Forderung, wie z.B. die Erfüllung von „technischen und organisatorischen Maßnahmen nach Stand der Technik" oder die komplette Umsetzung der Norm ISO/IEC 27001 schnell zu einer aufwendigen Projektaufgabe für die interne IT.

In der Praxis stellt sich aber bei näherer Betrachtung der ISO/IEC 27001 heraus, dass es zunächst weniger um eine konkrete Umsetzung von einzelnen IT-technischen Sicherheitsmaßnahmen geht. Im Fokus steht vielmehr die Etablierung von Lenkungs- und Sicherheitsprozessen in den verschiedensten Themenfeldern und über viele Bereiche des Unternehmens hinweg, oft auch „weit weg" vom direkten Einfluss der IT. Immerhin sind aber noch mindestens ein Drittel der Anforderungen der ISO/IEC 27001 direkt durch die IT umzusetzen bzw. wesentlich durch diese zu unterstützen. Die verbleibenden Anforderungen sind anderweitig im Unternehmen zu erbringen.

Typischer Ablauf eines ISMS-Projektes

Ein „ISMS-Einführungsprojekt" beginnt in aller Regel mit der Analyse, welche Lenkungs- und Sicherheitsaktivitäten noch wenig oder gar nicht ausgeprägt sind (GAP-Analyse). Gleichzeitig wird aber auch beleuchtet, welche bereits vorhandenen internen Aktivitäten verwertbar bzw. ausbaubar sind (Potentialanalyse). Typische Erkenntnis hier: Es ist zumeist schon viel mehr eines „ISMS" vorhanden, als zunächst gedacht.

Entscheidend für die nächste Phase ist nun, für die konkret bestehende Unternehmensorganisation die geeigneten Rollen zum Aufbau und späteren Betrieb des ISMS zu identifizieren und das dafür vorgesehene Personal zu schulen. Dann folgen die Identifikation von bestehenden Risiken, die Bestimmung angemessener Sicherheitsmaßnahmen sowie deren Etablierung. Parallel dazu werden die lenkenden und überwachenden Prozesse des ISMS mit oben genannten Rollen beschrieben und aktiviert.

Erfolgsparameter in einem ISMS-Projekt

Die realen Herausforderungen in einem ISMS-Aufbauprojekt sind zumeist die Folgenden:

- Aufbau von umfangreichem Knowhow bei den Rollen im unternehmensinternen ISMS, die die Sicherheitsaktivitäten in Zukunft steuern sollen
- Projektmarketing soll eine hohe Akzeptanz für Veränderungen im Unternehmen schaffen
- Professionelle Projektlenkung für die gleichzeitige Bearbeitung einer Vielzahl unterschiedlicher sicherheitsrelevanter Themen
- Die möglichst frühzeitige und intensive Einbindung von Führungspersonen, Stabsstellen sowie Datenschutzbeauftragtem und u.U. Betriebsrat

GAI NetConsult GmbH, Am Borsigturm 58, D-13507 Berlin, Telefon: 030-417 898-0, Fax: 030-417 898-300
E-Mail: vertrieb@gai-netconsult.de Internet: http://www.gai-netconsult.de

Informationssicherheit

Einführung & Betrieb eines ISMS nach ISO/IEC 27001

Ziele in einem ISMS-Projekt

Um die tatsächliche Einführung und formale Wirksamkeit eines ISMS nach ISO/IEC 27001 nachzuweisen, bietet sich eine international anerkannte Zertifizierung an. Sie wird von akkreditierten Auditoren durchgeführt und ist im Abstand von drei Jahren zu wiederholen. Voraussetzung hierfür ist allerdings, die ISO/IEC 27001 vollständig umzusetzen.

Wenn die Zertifizierung nicht oder erst später angestrebt wird, sollten zumindest die für die individuelle Organisation wichtigsten Themenfelder eines ISMS etabliert werden, um die Sicherheit Schritt für Schritt zu verbessern. Aus solch modularer Sicht sind der Aufbau einer Sicherheitsorganisation und einer Schutzbedarfsmethodik oder die Etablierung eines Managements von Sicherheitsvorfällen als wichtigste Beispiele hervorzuheben.

Reichen ISMS-Dokumentensets & -Tools?

Zu Beginn eines ISMS-Projektes wird oft mit dem (kostensparenden) Gedanken gespielt, allein einen Satz von Dokumententemplates und ein ISMS-Tool als ausreichende Unterstützung einzusetzen. Dies scheint verlockend, schließlich geben sie eine erste Orientierung und lassen hoffen, schon durch kleinere Anpassungen normative Anforderungen zu erfüllen.

Hiervor sei jedoch gewarnt: Während der Projektdurchführung entstehen häufig neue Erkenntnisse. Vorgefertigte Dokumentensets müssten deshalb weitgehend generisch sein, um einen großen Adressatenkreis abdecken zu können. Die Tauglichkeit für das eigene Unternehmen wird deshalb immer nur bedingt gegeben sein, da solch generische Dokumentensets weder die konkrete Risikolage noch die vorhandenen Sicherheitsaktivitäten oder die konkrete Aufbau- und Ablauforganisation des Unternehmens berücksichtigen können. Deshalb ist in jedem Falle die enge Zusammenarbeit von eigenen Mitarbeitern und externen Beratern mit langjähriger Erfahrung im ISMS-Aufbau zu empfehlen.

Ähnlich verhält es sich mit der Unterstützung durch ISMS-Tools. Grundsätzlich ist das natürlich der Verwendung von Word und Excel vorzuziehen, aber meist stellt sich erst im Laufe eines Implementierungsprojektes heraus, welche Anforderungen ein ISMS-Tool konkret erfüllen muss, um im späteren Betrieb tatsächlich hilfreich und unterstützend zu sein. Eher selten „überleben" deshalb Tools, die schon zu Beginn eines ISMS-Betriebs ausgewählt wurden, die folgenden Jahre.

Unterstützung durch die GAI NetConsult

Durch unsere langjährige Projekterfahrung sind wir in der Lage, speziell auf ein Unternehmen abgestimmte ISMS-Projekte zu planen und zusammen mit den Verantwortlichen zu etablieren. Wir legen dabei besonderen Wert auf eine Orientierung an den vorgefundenen Geschäftsprozessen und der bestehenden Sicherheitsarchitektur sowie auf eine unkomplizierte Adoption regionaler Anforderungen in möglichen Zweigniederlassungen.

Ein ISMS lebt von kontinuierlicher Verbesserung. Unser Beratungsziel ist erreicht, wenn die Mitarbeiter im Unternehmen alle Lenkungs- und Sicherheitsprozesse eigenständig und routiniert bearbeiten können. Dafür planen wir realistische Teilprojekte und Meilensteine für eine schrittweise Migration des ISMS in die bestehende Sicherheitsarchitektur.

Die GAI NetConsult verfügt über ein großes Erfahrungspotential für die Konzeptions- und Umsetzungsphase eines Informationssicherheitsmanagementsystems. Gerade bei der Einführung eines ISMS ist der Erfolg von einer detaillierten und weitblickenden Planung abhängig. Wir bieten daher die Konzeption und die Umsetzung als getrennte, aber aufeinander aufbauende Pakete an:

☛ **Konzeption**

- ☑ Zielsetzung und Scoping
- ☑ Entwicklung der ISMS Policy
- ☑ Erfassung der aktuellen Sicherheitsarchitektur
- ☑ Durchführung der Risikoanalyse
- ☑ Erstellung eines Maßnahmenkataloges
- ☑ Entwurf der neuen Sicherheitsarchitektur
- ☑ Beschreibung der Schnittstellen zu QM, RM, …

☛ **Umsetzung**

- ☑ Erstellung der geforderten Dokumentation
- ☑ Aufbau der Sicherheitsorganisation
- ☑ Implementierung der Managementprozesse
- ☑ Formulierung der Sicherheitsarchitektur
- ☑ Sensibilisierungs- und Schulungsmaßnahmen
- ☑ Implementierung von Sicherheitsmaßnahmen
- ☑ Vorbereitung auf das Zertifizierungsaudit

GAI NetConsult GmbH, Am Borsigturm 58, D-13507 Berlin, Telefon: 030-417 898-0, Fax: 030-417 898-300
E-Mail: vertrieb@gai-netconsult.de Internet: http://www.gai-netconsult.de