CS_PORTFOLIO

Informationssicherheits-Managementsystem [ISMS]

ConSecur

[security and consulting]

Standards für ein ISMS

Die Entscheidung für ein ISMS ist eine langfristige. Deshalb statten wir Informationssicherheits-Managementsysteme mit einer Agilität aus, die den Schutz des Unternehmenswerts „Information“ auch in einem permanenten Wandel gewährleisten kann.

Wir sehen heute dabei zu, wie sich unter dem Stichwort „digitale Transformation“ ganze Geschäftsmodelle verändern. Wir erleben den Wandel in der Kundenansprache, die zunehmend über digitale Kanäle mit individualisierten Angeboten erfolgt; wir erfahren, dass Produkte vermehrt digitalisiert werden (z. B. Schließsysteme im Automobil-Bereich) und wir verfolgen den Wandel in der Fertigungsindustrie von Wertschöpfungsketten zu Wertschöpfungsnetzen („Industrie 4.0“). Das ConSecur ISMS besitzt die Agilität für die digitale Transformation. Dabei stehen uns verschiedene Standards zur Auswahl, Informationssicherheit zu managen: z.B. der IT-Grundschutz des BSI, die ISO 27001, der Standard VdS 3473 sowie diverse Branchenstandards. Die Entscheidung für einen Standard treffen wir gemeinsam mit Ihnen.

Der Standard VdS 3473 ist vor allem für kleinere und mittlere Unternehmen ausgelegt; für Betreiber Kritischer Infrastrukturen nach dem IT-Sicherheitsgesetz bieten sich IT-Grundschutz oder die ISO 27001 an. Unsere Erfahrung zeigt, dass vor allem der ISO27001 Standard auch international sehr akzeptiert ist, viele Freiheitsgrade bei der Gestaltung bietet und somit ein guter Ausgangspunkt ist, um die unternehmensspezifisch beste Methode zu bestimmen.

Wie gehen wir vor?

Das Ziel der Informationssicherheit ist, den Unternehmenserfolg abzusichern. Damit ist es eine Management-Aufgabe. Häufig wird das Thema von der IT initiiert, da dort am ehesten die (technischen) Schwachstellen und die Bedrohungen sichtbar werden. Um Informationssicherheit wirksam und effizient managen zu können, ist es nach unserer Erfahrung enorm wichtig, die Unterstützung der Unternehmensleitung zu gewinnen. Mit diesem Management Commitment bestimmt die Unternehmensleitung einen Verantwortlichen für die Informationssicherheit. Der Informationssicherheitsbeauftragte oder CISO (Chief Information Security Officer) wird geschäftsprozessübergreifend arbeiten und die weiteren Schritte gehen. Dafür ist er mit angemessenen Kompetenzen ausgestattet und prominent in der Organisation verankert.

Unternehmenswert Information

Jedes Unternehmen hat Werte, die es am Markt erfolgreich machen. Hierzu zählen physische Werte wie Gebäude oder Maschinen; zu ihnen gehört ebenso das Know-how, das eine Organisation stark und wettbewerbsfähig macht. Dieses Wissen um Märkte, Marktteilnehmer, Produktionstechniken und Produkte ist ein ganz wesentlicher Wert für den Erfolg eines Unternehmens. Wir sprechen deshalb vom Unternehmenswert „Information".

Zum Schutz dieses Kapitals haben wir das ConSecur Informationssicherheits-Managementsystem (ISMS) entwickelt, das auf anerkannten Standards wie z.B. ISO 27001 und dem IT-Grundschutz basiert.

Kommen Sie mit uns!

Informationen als Unternehmenswerte identifizieren

Wo in Ihrem Unternehmen gibt es Informationen, die einen hohen Unternehmenswert besitzen und gleichzeitig in ihrer Vertraulichkeit, Verfügbarkeit oder Integrität gefährdet sind? Wo in Ihrem Unternehmen gibt es Informationssicherheitsrisiken?
Bei der Analyse von Informationen erkennen wir, dass nicht alle Informationen gleich „wertvoll" sind und nicht an allen Orten und in allen Systemen gleich gefährdet.
Deshalb werden wir zunächst die wertvollsten Informationen im Unternehmen identifizieren und ihr Gefährdungspotential analysieren. Überschreitet die Kombination aus Unternehmenswert „Information" und „Gefährdung" ein nicht tolerierbares Maß, liegt ein Informationssicherheitsrisiko vor, das wir durch geeignete Maßnahmen reduzieren werden.
Mit diesem risikobasierten Ansatz erkennen wir, in welchem Bereich Informationssicherheit wichtig ist und welcher Handlungsbedarf besteht.

Aufwand und Ertrag

Das ConSecur ISMS ist ein Managementsystem, das auf dem Geschäftsrisikoansatz basierend den Unternehmenswert „Information" sichert. Dabei ist das ISMS einem ausgewogenen Verhältnis von Aufwand und Ertrag verpflichtet. Das gilt auch für den laufenden Betrieb, in dem wir eingeführte Prozesse kontinuierlich verbessern.

Ein ISMS beinhaltet Prozesse zur Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit. Nach seiner Einführung werden wir ein sehr klares Bild davon haben, in welchen Bereichen Informationssicherheitsrisiken bestehen und wie sie behandelt werden.

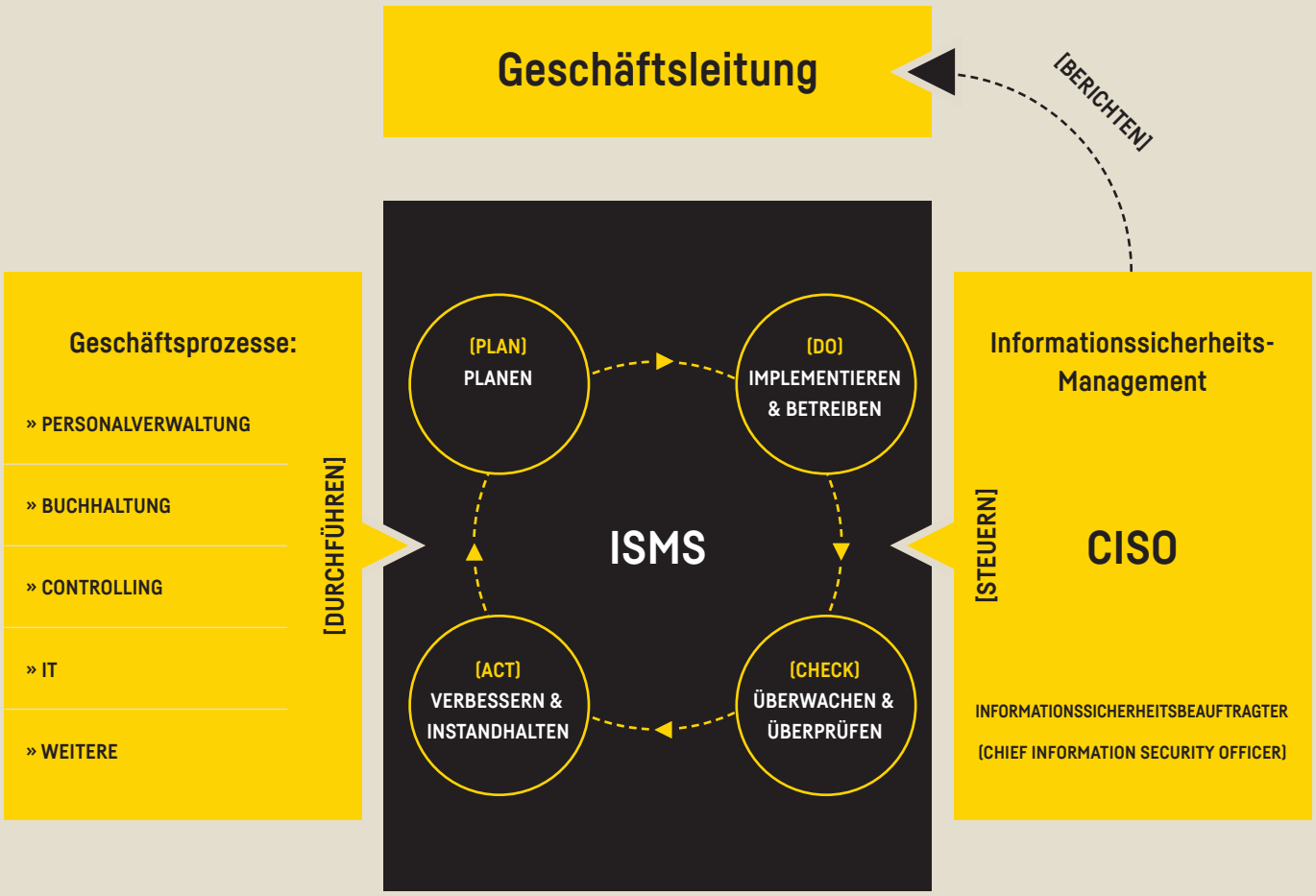
ConSecur ISMS - Informationssicherheit nachhaltig umsetzen

Das ConSecur ISMS verbindet Informationssicherheit mit der Umsetzungskompetenz der Sicherheits-Spezialisten, die auf Nachhaltigkeit und Akzeptanz basiert.

Wir möchten, dass Informationssicherheit in Unternehmen gelebt wird. Deshalb legen wir bei der Implementierung großen Wert darauf, Richtlinien, Prozesse und Maßnahmen zu gestalten, die zur Unternehmenskultur passen und von allen Beteiligten angenommen werden.

Das ConSecur ISMS ist unser Verständnis von einem kontinuierlichen, erfolgreichen ISMS.

Auf diesem Weg begleiten wir Sie.



Das ISMS im Kontext Cloud

Das ConSecur ISMS gibt Ihnen die Agilität, Geschäftsprozesse und IT-Dienste in die Cloud auszulagern. Das können Sie machen, solange Sie die Kontrolle und Aufsicht über die ausgelagerten Dienstleistungen behalten und wahrnehmen. Das gilt im Besonderen auch für den Aspekt „Informationssicherheit".
Sollten Sie einzelne Aufgaben, IT-Systeme oder komplette Prozesse an einen Dienstleister vergeben, obliegt diesem die Verantwortung für ihren Betrieb. Deshalb ist es wichtig, mit Unterstützung des CISO den richtigen Partner zu finden sowie geeignete Vertragsvereinbarungen zu schließen, die bedarfsgerechte Governance des Outsourcing Vorhabens sicherstellt.

JÖRG ECKARDT –
SENIOR BERATER

Zertifizierung - ja oder nein?

Betreiber kritischer Infrastrukturen wissen, dass sie vom Gesetzgeber angehalten sind, einen angemessenen Schutz gegen Bedrohungen ihrer IT zu gewährleisten. Verpflichtend ist eine Zertifizierung jedoch nicht für alle.

VERPFLICHTENDE ZERTIFIZIERUNG
Betreiber von Energieversorgungsnetzen gehören beispielsweise zu denjenigen, für die an einer Zertifizierung kein Weg vorbei führt. Sie sind auf der Basis eines von der Bundesnetzagentur herausgegebenen IT-Sicherheitskatalogs dazu verpflichtet, ein ISMS nach ISO 27001 zu etablieren und dieses bis zum 31.01.2018 zertifizieren zu lassen.

EMPFEHLENSWERTE ZERTIFIZIERUNG
Unternehmen, die nach der Verordnung zum IT-Sicherheitsgesetz Kritische Infrastrukturen betreiben, sollten im eigenen Interesse über eine Zertifizierung nachdenken.
Denn sie sind gesetzlich verpflichtet, einen angemessenen Schutz gegen Bedrohungen ihrer IT zu gewährleisten. Damit wird implizit ein ISMS gefordert, dessen Wirksamkeit dem BSI alle 2 Jahre darzulegen ist. Eine Zertifizierung ist empfehlenswert, da sie den regelmäßigen Wirksamkeitsnachweis stark erleichtert; explizit gefordert und damit verpflichtend ist eine Zertifizierung nicht.

ZERTIFIZIERUNG FÜR DEN GESCHÄFTSERFOLG
In allen anderen Fällen kann eine Zertifizierung sinnvoll sein, weil sie zum Beispiel einen positiven Beitrag für den Geschäftserfolg leistet. Bei Dienstleistern, die Rechenzentrums-, Cloud- oder andere Telekommunikations- und IT-Dienste anbieten, ist das sehr gut vorstellbar. Im Einzelfall sind die Vor- und Nachteile mit allen firmeninternen Interessengruppen, aber unter Umständen auch mit externen Großkunden oder Partnern abzuwägen.

ConSecur

[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de