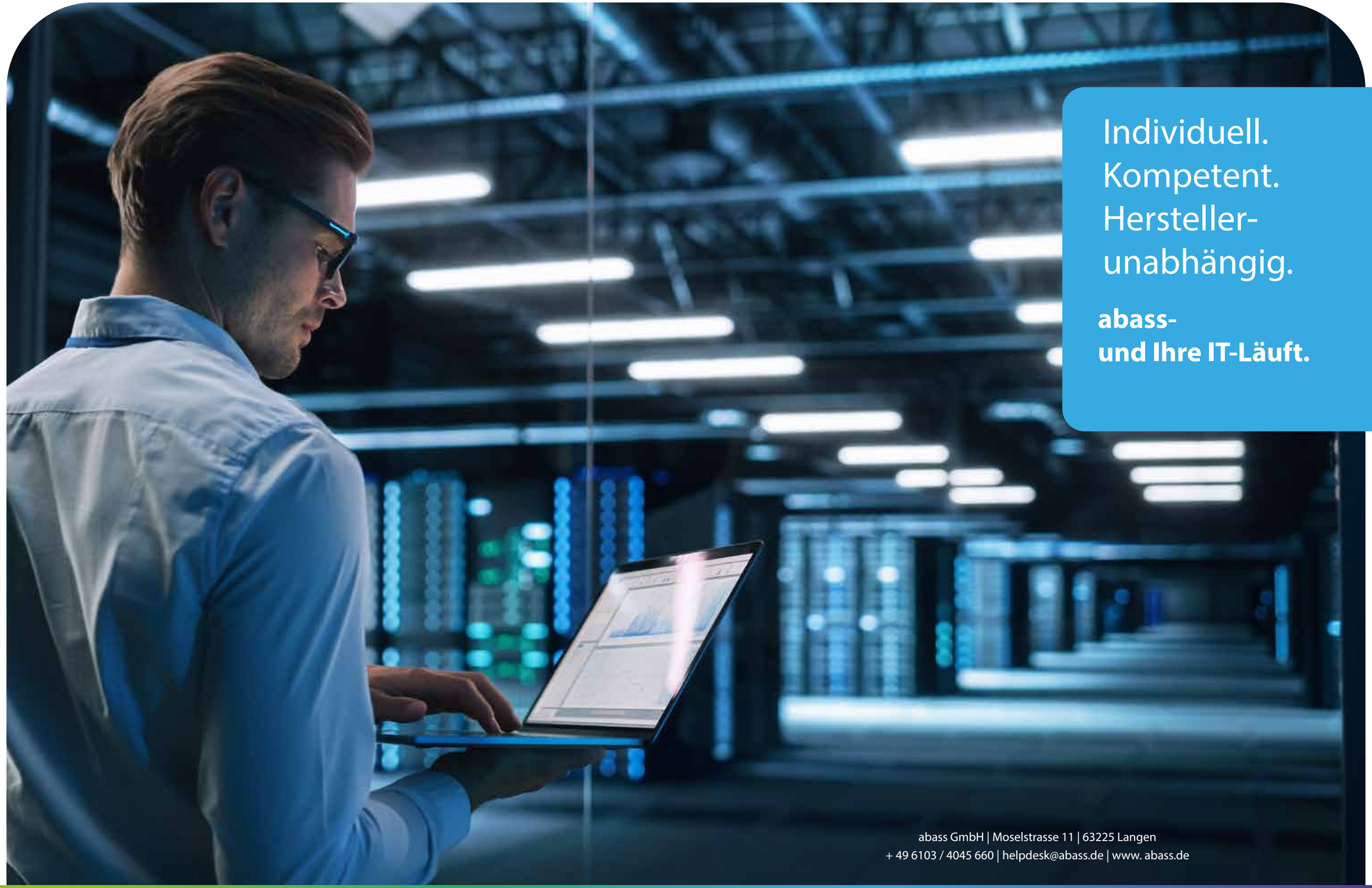
Einführung eines **ISMS gemäß ISO 27001**
in kleinen und mittelständischen Unternehmen



Individuell.
Kompetent.
Hersteller-
unabhängig.

abass-
und Ihre IT-Läuft.

abass GmbH | Moselstrasse 11 | 63225 Langen
+ 49 6103 / 4045 660 | helpdesk@abass.de | www. abass.de

Inhalt

Präambel

01

Dieses White Paper liefert ein **„Erfolgsrezept”** zur Einführung eines ISMS in mittelständischen Unternehmen (KMU) nach der **abass- Methode**.

Beschrieben werden die Kernprozesse eines ISMS mit **wertvollen Tipps aus der Praxis** für die Einführung.

WARUM EIN ISMS?

02

Warum brauche ich ein ISMS dann?

- Ein ISMS steuert die Informationssicherheit, reagiert auf Ereignisse und optimiert den Status permanent.
- Ein ISMS dokumentiert eine Risikoabschätzung und schützt die wichtigsten Werte des Unternehmens.
- Mit einem zertifizierten ISMS kann man unter Wettbewerbern herausstechen und erfüllt auch verschiedene Compliance-Anforderungen.

Klären wir doch erst einmal die Begriffe Informationssicherheit und ISMS – ein Managementsystem für Informations-sicherheit.

Informations-sicherheit:

Die Informationssicherheit bezieht sich auf den Schutz der Verfügbarkeit, Vertraulichkeit und Integrität aller Assets (=Werte) eines Unternehmens.

ISMS:

Dokumentation aller Prozesse im Unternehmen, die die Verfügbar-keit, Vertraulichkeit und Integrität der Unternehmenswerte sicherstellen. Im Rahmen der kontinuierlichen Verbesserung wird regelmäßig der aktuelle Status der Unternehmens-werte, ihrer Risiken und zugeordneten Maßnahmen erfasst und optimiert.

Die Definitionen klingen ähnlich.

Also, was ist der Unterschied?

Die Informationssicherheit bildet einen Status ab, das ISMS den Weg dorthin.

WAS MACHT EIN GUTES ISMS AUS?

03

Es ist wirksam und wird gelebt!

Die Etablierung eines zertifizierungs-fähigen ISMS fordert neben die Erstellung vieler neuer Dokumente das Schaffen von Sicherheitsbewusstsein und die Etablierung neuer Prozesse im Unter-nehmen. Dies ist eine Heraus-forderung im Alltag eines jeden Unter-nehmens. Insbesondere die Ressourcen in KMUs sind oft dafür nicht vorhanden.

Unser Whitepaper soll einen **ressourcen-schonenden** Weg aufzeigen ein ange-messenes ISMS zu etablieren.

Ein angemessenes ISMS zu etablieren, heißt, es passgenau auf Ihr Unternehmen zu bauen. Also soviel wie nötig erarbeiten aber es so einfach wie möglich halten.

Das bedeutet nicht, auf angemessene Sicherheit zu verzichten. Aber wir wollen nicht, dass ein ISMS Ihrem Kerngeschäft im Wege steht. **Es soll unterstützen, Ihre Prozesse und Ihr Kerngeschäft zu schützen.**

Grundsätzlich setzen wir beim Aufbau und Betrieb eines ISMS auf **eine kollaborative und agile Arbeitsweise.** Das heißt, wir entwickeln **mit Ihnen zusammen ein Konzept, dass in Ihr Unternehmen passt.** Dabei verwenden wir einfache Dokumente (also ein papierbasierendes Informations-system) oder, falls gewünscht und notwendig, ein softwarebasiertes ISMS. Die grundlegende Vorgehensweise bleibt gleich. Wichtig ist anzufangen, auch wenn sich die Installation eines ISMS – Systems erst einmal aufwendig anhört.

Neben einer **Zertifizierung nach ISO 27001**, die oft der Grund für die Einführung eines ISMS ist, sind die stetig steigenden **Bedrohungsszenarien** ein gutes Argument, mehr Zeit und Gedanken in die Sicherheitsstruktur des nternehmens zu stecken. Wenn es gelingt, durch die Implementierung angemessener technischer sowie organisatorischer Sicherheitsmaßnahmen Unter-nehmensschäden wie **Imageverlust, Datenverlust sowie Ausfälle im Geschäftsbetrieb zu verringern**, rechnet sich ein ISMS für alle.

Ein gutes ISMS ist in erster Linie also wirksam, und erst dann geht es darum, alle Normanforderungen zu erfüllen.

Es gibt natürlich ein paar Rahmenbedin-gungen, die zum Aufbau eines ISMS gehören.

INHALT UND AUFBAU DER **ISO 27001**

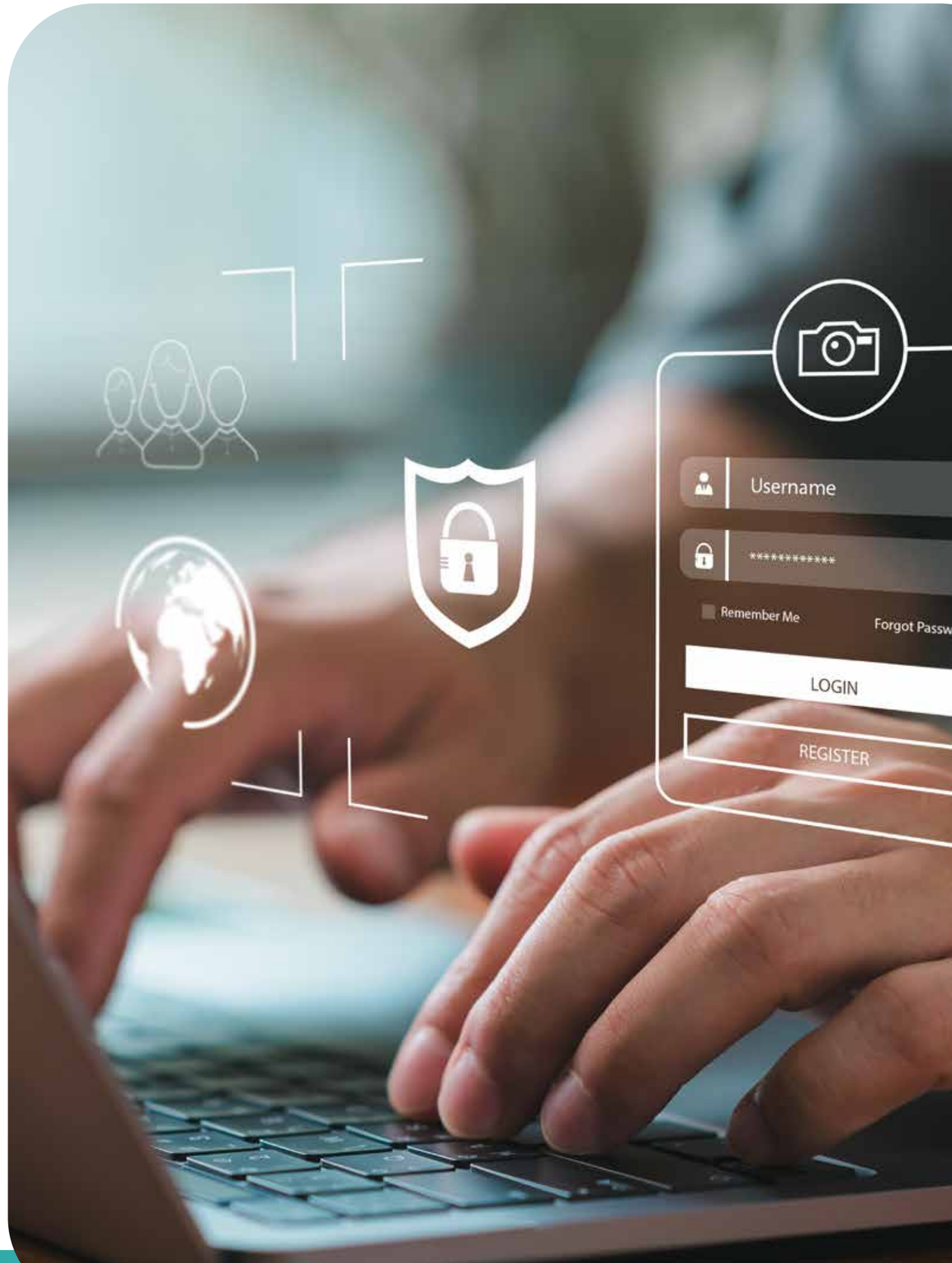
04

04.01 Allgemeines

Zentraler Standard dieser Normenfamilie ist der ISO/IEC 27001 Standard.

Der Standard definiert Anforderungen an ein Informationssicherheits-managementsystem und stellt einen prozessorientierten Ansatz vor.
Dabei ist das Dokument sehr generisch gehalten und kann in allen Organisationen unabhängig von Größe oder Typ der Organisation angewendet werden.
Während der Inhalt auf der technischen Ebene nicht detailliert wird, sind die Anforderungen an die Prozesse ausführlich definiert. Damit bildet ISO/IEC 27001 die Basis der Normenfamilie und definiert Rahmenbedingungen für ein funktionierendes ISMS.

Die Kapitel 1–3 der Norm befassen sich mit grundlegenden Dingen, zu denen keine Notwendigkeit einer Umsetzung besteht. Die Abschnitte 4–10 müssen obligatorisch (verpflichtend) umgesetzt werden.



INHALT UND AUFBAU DER **ISO 27001**

04

04.02 KAPITEL 4–10

Die ISO 27001:2013 ist eine internationale Norm, die die Anforderungen an die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines ISMS beschreibt.

Die Norm ist in zwei Bereiche aufgeteilt: den obligatorischen Managementrahmen und den Anhang A. Im Gegensatz zu den Controls (Maßnahmen) des Norm-Anhangs A, die im Rahmen der Anwendbarkeitserklärung (siehe unten) begründet abgewählt werden können, ist die Umsetzung der Vorgaben aus den Kapiteln 4–10 verpflichtend.

Anhand der folgenden Punkte können Sie zu einer ersten Selbsteinschätzung des Erfüllungsgrads in Ihrer Organisation gelangen.

HINWEIS:
Lassen Sie sich durch die Jahreszahlen in den Versionsnummern der Norm nicht irritieren. Hierbei sind lediglich die deutschen Übersetzungen gemeint. Grundlage der Zertifizierung ist aber nach wie vor die englische Version aus dem Jahr 2013.

04.02.01 KAPITEL 04–06

04 Kontext der Organisation

- Wurden interessierte Parteien festgelegt und deren (potenzielle) Auswirkung auf das ISMS dokumentiert?
- Wurde der Geltungsbereich des ISMS definiert?
- Wurden die gesetzlichen Anforderungen im Kontext des ISMS identifiziert?

05 Führung

- Wird die Geschäftsführung ihrer Verpflichtung gerecht, u. a. durch:

  Die **Festlegung einer Strategie** zur Informationssicherheit, die I**ntegration des ISMS in Geschäftsprozesse**, die **Zurverfügungstellung der erforderlichen Ressourcen**, die **Messung der Wirksamkeit** und **kontinuierlichen Verbesserung** des ISMS und die **Sensibilisierung der Mitarbeiter** auf allen Ebenen?
- Hat die Geschäftsführung eine Leitlinie zur Informationssicherheit verabschiedet und bekannt gemacht?
- Hat die Geschäftsführung Rollen, Verantwortlichkeiten und Befugnisse im Rahmen des ISMS benannt und erhält Berichte von diesen?

06 Planung

- Wurden Maßnahmen im Umgang mit den identifizierten Risiken und Chancen festgelegt?
- Wurde ein Prozess zur Identifikation, Bewertung und zur Behandlung von Informationssicherheitsrisiken festgelegt?
- Ist eine Anwendbarkeitserklärung zum Anhang A dokumentiert?
- Wurden Ziele des ISMS bestimmt und ein Plan zu deren Erreichung festgelegt?

INHALT UND AUFBAU DER **ISO 27001**

04

04.02.01 KAPITEL 07–08

07 Unterstützung

- Wurden die notwendigen Ressourcen für das ISMS bereitgestellt?
- Haben die relevanten Personen die erforderlichen Kompetenzen, um ihren Rollen im Rahmen des ISMS gerecht zu werden?
- Sind alle Mitarbeiter sensibilisiert in Bezug auf

  die ISMS-Leitlinie, ihre Mitwirkungspflicht im Rahmen des ISMS und die Konsequenzen der Nichterfüllung von ISMS-Vorgaben?
- Wurde im Rahmen des ISMS die interne und externe Kommunikation bestimmt?
- Werden die von der Norm geforderten Informationen und Nachweise zur Messung der Wirksamkeit des ISMS dokumentiert und gelenkt?

08 Betrieb

- Die Organisation muss zur Planung und Steuerung eine Reihe von Prozessen festlegen und diese dokumentieren. Dazu zählt jeweils ein Prozess:

  Zur Erfüllung der Anforderungen der Informationssicherheit, zur Steuerung von Maßnahmen, zur Steuerung von Aufgaben, die an Dienstleister ausgelagert wurden und zur Berücksichtigung der Informationssicherheit innerhalb geplanter Änderungen.
- Wird in regelmäßigen Abständen und bei signifikanten Anpassungen eine Risikobeurteilung durchgeführt?
- Wird eine Risikobehandlung durchgeführt?

INHALT UND AUFBAU DER **ISO 27001**

04

04.02.01 KAPITEL 09–10

09 Bewertung der Leistung

- Gibt es einen Prozess zur Überwachung der Wirksamkeit des ISMS?
- Werden regelmäßig interne Audits durchgeführt?
- Ist ein Auditprogramm aufgestellt?
- Wird regelmäßig eine Managementbewertung durch- geführt, die mindestens die in Kapitel 9.3 der Norm enthaltenen Punkte berücksichtigt?

10 Verbesserung

- Wird adäquat mit Maßnahmen auf eine Nichtkonformität mit den Anforder- ungen des ISMS reagiert?
- Werden die festgestellten Maßnahmen im Hinblick auf deren Notwendigkeit bewertet, ggf. eingeleitet und entsprechend ihrer Wirksamkeit überprüft?
- Wird im Rahmen des ISMS eine kontinuierliche Verbesserung sichergestellt?

INHALT UND AUFBAU DER **ISO 27001**

04

04.03 ANHANG A

Neben diesen zehn Kapiteln hat die ISO/IEC 27001:2013 auch einen Anhang A, der 114 spezifische Maßnahmen (Controls) enthält. Diese sind in die folgenden 14 Kategorien eingeteilt:

Kapitel		Anzahl der Maßnahmen
A.5	Informationssicherheitsrichtlinien	2
A.6	Organisation der Informationssicherheit	7
A.7	Personalsicherheit	6
A.8	Verwaltung der Werte	10
A.9	Zugangssteuerung	14
A.10	Kryptographie	2
A.11	Physische und umgebungsbezogene Sicherheit	15
A.12	Betriebssicherheit	14
A.13	Kommunikationssicherheit	7
A.14	Anschaffung, Entwicklung und Instandhalten von Systemen	13
A.15	Lieferantenbeziehungen	5
A.16	Handhabung von Informationssicherheitsvorfällen	7
A.17	Informationssicherheitsaspekte beim Business Continuity Management	4
A.18	Compliance	8

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.01 Allgemeine Vorgehensweise nach der PDCA-Methode

Die Plan-Do-Check-Act-Methode (PDCA-Methode), auch Deming-Kreis genannt, ist ein Prinzip, das die Basis für jedes ISMS bildet.

Die vier Phasen des Deming-Kreislaufs veranschaulichen die Kontinuität, die notwendig ist, ein ISMS sinnvoll und nachhaltig zu „betreiben".
Im Planungsschritt „Plan" wird eine Risikoanalyse durchgeführt, um den Ist-Zustand festzustellen. Anschließend werden die Maßnahmen zum Umgang mit Risken und Chancen bestimmt und die Informationssicherheitsziele und Planung zu deren Erreichung festgelegt. Mit dem Umsetzungsschritt „Do" werden die im Vorfeld bestimmten Maßnahmen geplant, durchgeführt und gesteuert. Mit dem Kontrollschritt „Check" werden die Sicherheitsmaßnahmen überwacht, gemessen und überprüft. In der letzten Phase „Act" werden Informationen zu den Sicherheitsmaßnahmen geliefert, die verbessert werden müssen, und es wird bestimmt, welche Neuerungen notwendig sind, um die Konformität, die Effizienz und die Effektivität eines ISMS fortlaufend zu gewährleisten.

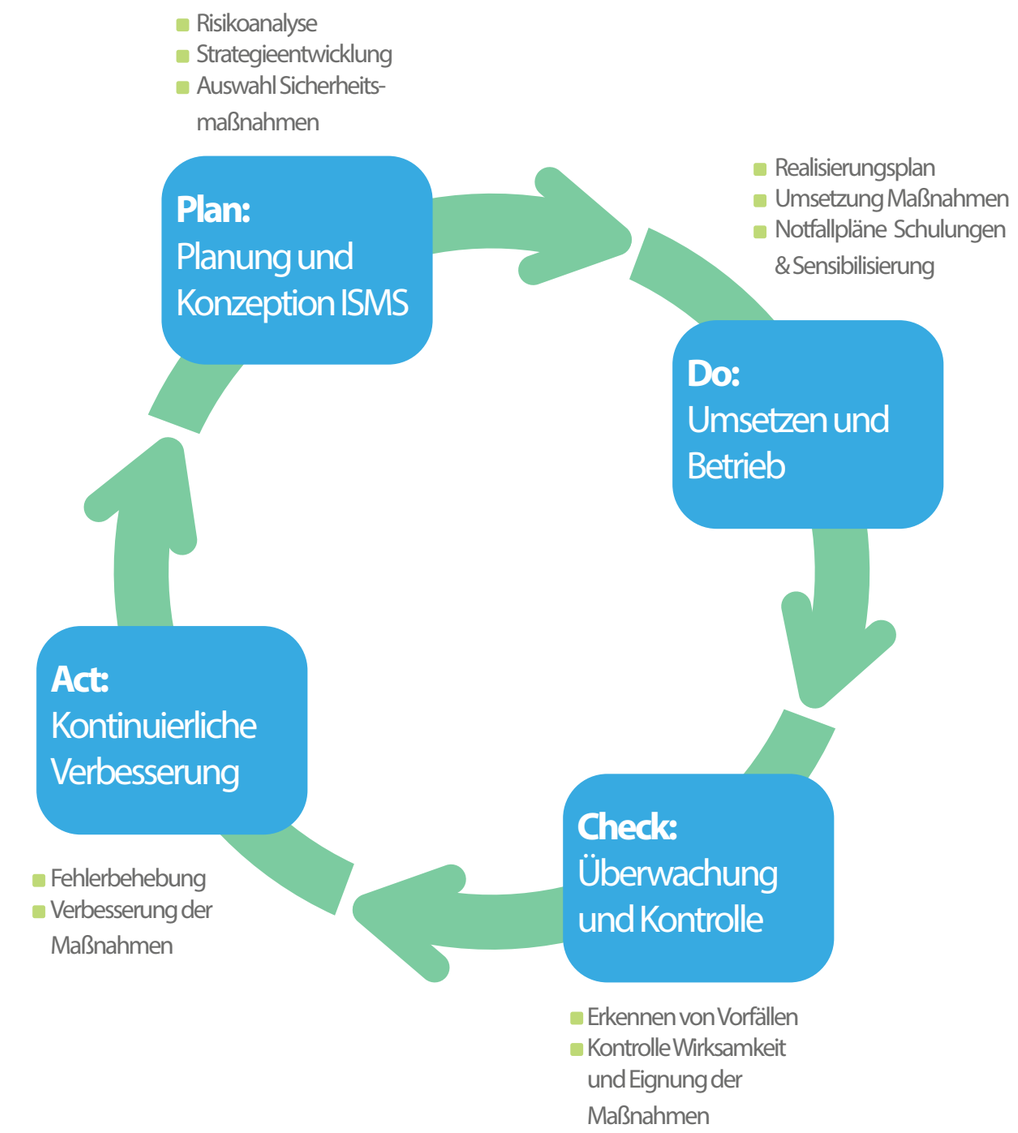


Abbildung nach Sowa, 2017, S. 19

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.02
Plan - Planung
Risikoanalyse
Strategieentwicklung
Sicherheitsmaßnahmen

Die ISO 27001 lässt Unternehmen bei der Auswahl einer Methodik für das Risikomanagement freie Hand. Allerdings muss die Methodik nachvollziehbar und dokumentiert sein. Entsprechend dem Ziel und Zweck können dabei unterschiedliche Risikoanalysen oder Standards mehr oder weniger sinnvoll sein. Mögliche Methoden zur Risikoanalyse finden sich im Standard 100-3 des Bundesamtes für Sicherheit und Informationstechnik (BSI).

Bei der Durchführung einer Risikoanalyse muss die Gefahrenquellen bzw. Bedrohungen ermittelt werden. Eine Gefahrenquelle stellt dabei jeder Umstand oder Ereignis dar, das potenziellen Schaden an einem Informationswert verursachen kann. Bedrohungen können dabei einen natürliche, menschliche oder durch Umgebungsbedingungen herbeigeführte Ursache haben. Daraus entsteht eine Liste mit möglichen Gefahrenquellen. Wichtig ist, sich vorab Gedanken über ein Bewertungsschema der Risiken zu machen.

Nur so kann man zu vergleichbaren Ergebnissen kommen und eine Priorisierung der identifizierten Risiken für die Risikobehandlung erreichen. Zur Bewertung gibt es in der ISO-27001-Norm tatsächlich auch grobe Vorgaben. Und zwar geht es darum, die Folgen bei Eintritt (Schadenshöhe) sowie die Eintrittswahrscheinlichkeit der identifizierten Risiken abzuschätzen.

Ermitteln Sie für Ihre ISMS Risikoanalyse anschließend die aktuellen Schwachstellen der Informationswerte. Schwachstellen können dabei absichtlich oder unabsichtlich ausgenutzt werden. Sie werden im Allgemeinen durch Befragen der verantwortlichen Personen sowie der Administratoren oder anhand offizieller Quellen ermittelt. Weitere Möglichkeiten, um (insbes. technische) Schwachstellen festzustellen, sind automatisierte Scanning-Tools oder Penetrationstests. Letztere werden oftmals durch externe Experten durchgeführt, die damit Informationssysteme und Netzwerkkomponenten auf Schwachstellen untersuchen.

Aufgrund der ermittelten Bedrohung und zugehöriger Schwachstellen werden die Auswirkungen auf Basis der in der Schutzbedarfsfeststellung ermittelten Anforderungen bestimmt. Das Ergebnis bildet dann die Grundlage für die Risikobewertung.

Prüfen Sie anschließend bereits vorhandene Schutzmaßnahmen und definieren Sie neue Sicherheitsmaßnahmen.

Risiken identifizieren

Überlegen Sie zuerst, welche Informationen. Geschäftsprozesse oder IT-Systeme für Ihren Geschäftsbetrieb besonders kritisch sind. Fragen Sie dann Ihren internen Experten und nutzen Sie zusätzlich Gefährdungskataloge, wie den BSI, um relevante Risiken zu identifizieren.

Risiken bewerten

Im zweiten Schritt geht es darum, die identifizierten Risiken zu bewerten. Schätzen Sie dafür die Schadenshöhe und die Eintrittswahrscheinlich für jedes Risiko ab.

Der Risikowert ergibt sich aus der Eintrittswahrscheinlichkeit und der Schadenshöhe und kann in einer so genannten Risikomatrix ermittelt werden.

Risiken behandeln

Für die Risiken mit dem höchsten Wert sollte eine Behandlungsstrategie festgelegt und dokumentiert werden.

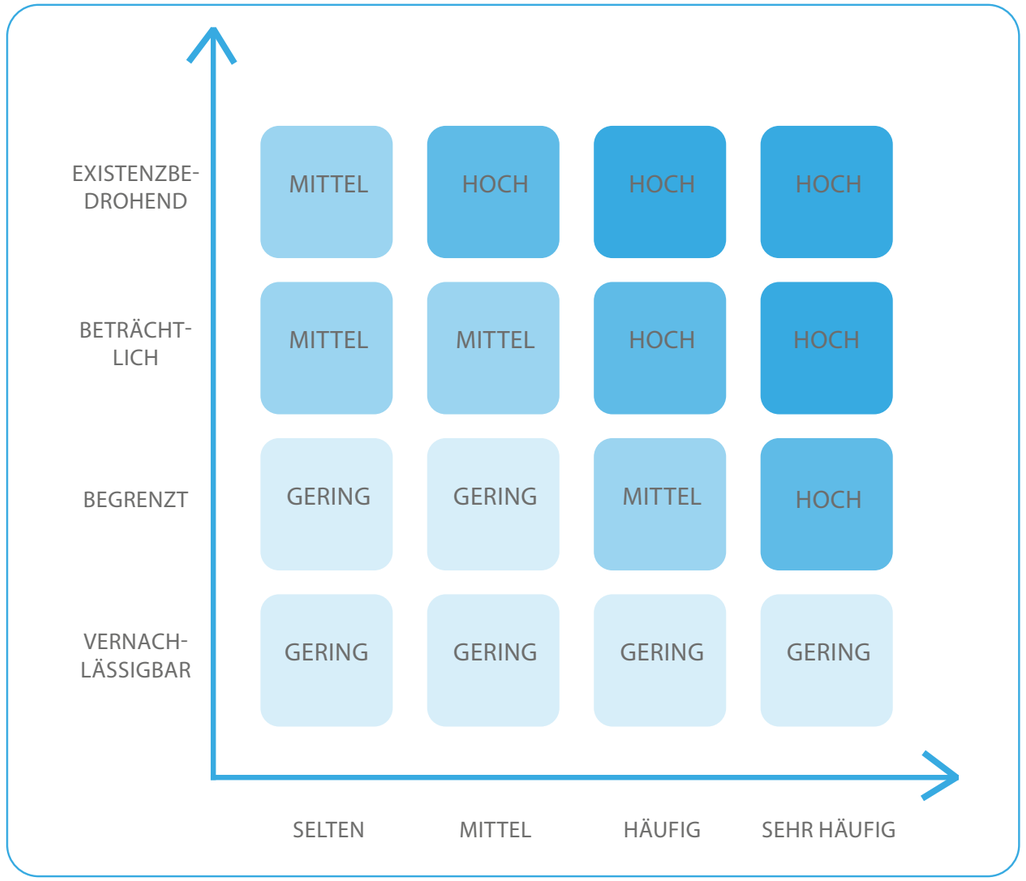
VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

Dabei kann eine Matrix helfen. Anbei ein Beispiel des BSI:

Ein risikobasiertes Vorgehen zur Behandlung bedeutet, sich zuerst den größten Risiken zu widmen. Eine sinnvolle Herangehensweise wäre, sich auf die „hohen" und „sehr hohen" Risiken zu konzentrieren und die übrigen Risiken als akzeptiert zu betrachten.
Für jedes hohe und sehr hohe Risiko sollte eine der genannten Behandlungsoptionen in einem Risikobehandlungsplan festgelegt werden.
Die Ergebnisse des Risikomanagements sowie der Behandlungsplan sollten Bestandteil der jährlichen ISMS-Berichterstattung an die Geschäftsführung sein.

RISIKOMATRIX



Quelle: BSI Standard 200-3 http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.html (Zuletzt aufgerufen am 04.05.2020)

Eintrifttshäufigkeit / Beschreibung:

Selten:
Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.

Mittel:
Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.

Häufig:
Ereignis tritt einmal im Jahr bis einmal pro Monat ein.

Sehr häufig:
Ereignis tritt mehrmals im Monat ein.

Schadenshöhe/ Schadensauswirkungen :

Vernachlässigbar:
Die Schadenauswirkungen sind gering und können vernachlässigt werden.

Begrenzt:
Die Schadensauswirkungen sind begrenzt und überschaubar.

Beträchtlich:
Die Schadensauswirkungen können beträchtlich sein.

Existenzbedrohend:
Die Schadensauswirkung können ein existenzbedrohliches, katastrophales Ausmaß erreichen.

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.03 Do-Check-Act

Auf der Basis der Risikoanalyse erfolgt die Auswahl und Umsetzung geeigneter Maßnahmen zur Risikovermeidung. Die beschlossenen und umgesetzten Maßnahmen sind in einem kontinuierlichen Prozess zu prüfen und fortlaufend zu optimieren. Werden Mängel oder neue Risiken erkannt, ist der komplette ISMS-Prozess von Beginn an neu zu durchlaufen.

05.03.01 Do - Dokumentation und Organisation

„Dokumentation" bedeutet für ein ISMS nach ISO 27001 insbesondere das Erstellen von Richtlinien zur Informationssicherheit. Es gibt einige obligatorische Richtlinien, die in einem Audit vorgelegt werden müssen.
Über den Umfang dieser Richtlinien sagt die Norm selbst jedoch nichts aus. Ganz im Gegenteil: In der Norm wird explizit erwähnt, dass sich der Umfang dokumentierter Informationen von Organisation zu Organisation unterscheiden kann. Hier kommt es insbesondere auf die Unternehmensgröße und die Art der Produkte und Dienstleistungen an. Das sollte der Verantwortliche für die Informationssicherheit bei einem KMU immer im Hinterkopf haben, wenn es an das Schreiben von Richtlinien geht.

Wichtiger als umfangreiche Dokumente ist, dass die Anforderungen, die in den Richtlinien festgehalten werden, auch wirklich im Unternehmen umgesetzt und gelebt werden.
Es ist wichtig, eine Balance zu finden und solche Dokumente regelmäßig einem Review zu unterziehen und möglicherweise zu verbessern.
Die hier beigefügten obligatorischen Richtlinien sind ein Muss bei einem Audit.

OBLIGATORISCHE RICHTLINIEN

- Leitlinie zur Informationssicherheit
- Richtlinie zum Risikomanagement
- Richtlinie zum Umgang mit Sicherheitsvorfällen
- Richtlinie Lieferanten, Dienstleister und Fremdfirmen
- Richtlinie zur Klassifizierung und Umgang mit Informationen
- Richtlinie zum sicheren IT-Betrieb
- Richtlinie für Personal- und Berechtigungsmanagement
- Allgemeine Regeln zur Informationssicherheit für alle Beschäftigten

Neben Richtlinien gibt es noch weitere normspezifische Dokumente, die in einem Audit vorliegen müssen. Hierzu zählen als Erstes der Anwendungsbereich und die sogenannte Anwendbarkeitserklärung (englisch: SoA – Statement of Applicability).

Zusammen sind sie der erste Anhaltspunkt für den Auditor, um sich ein Bild über den Umfang und die Gegebenheiten des ISMS und des Unternehmens zu machen.

Die Anwendbarkeitserklärung ist ein Dokument, das alle 114 spezifische Maßnahmen (Controls) aus dem Anhang A der ISO 27001 abbildet.

Im Rahmen der Anwendbarkeitserklärung ist zu prüfen und zu dokumentieren, welche Controls angewendet werden und deren Auswahl zu begründen. Alternativ können Controls auch begründet abgewählt werden, wenn die Vorgaben auf den Anwendungsbereich des ISMS nicht anwendbar sind.

Der Anwendungsbereich, oft auch Geltungsbereich oder Scope genannt, beschreibt in Textform, wo die Grenzen und die Anwendbarkeit des ISMS liegen.

So ist es in größeren Organisationen üblich, lediglich einzelne Geschäftsbereiche zu zertifizieren, anstatt der kompletten Organisation. Aber auch in kleineren Firmen ist es möglich, einzelne Bereiche zu zertifizieren und andere auszuschließen.

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

Die Beschreibung des Geltungsbereichs ist für die eigenen Kunden, die Eigentümer, Geschäftsführung, die Mitarbeiter*innen, Gesetzgeber, Dienstleister und andere Interessierten interessant, da hier nachvollzogen werden kann, welche Bereiche und Themen durch das ISMS abgedeckt sind und welche nicht. Auch diese Gruppen müssen dokumentiert werden. Hier bitte sich eine einfache Tabelle an. Ein weiterer Aspekt, in den es sich lohnt Gedanken zu investieren, sind Ziele der Informationssicherheit.

Die von der Unternehmensleitung festgelegte Unternehmensstrategie dient als Grundlage für die Ausgestaltung bzw. Festlegung der Ziele für die Informationssicherheit.

Vor allem zu Beginn einer ISMS-Implementierung empfiehlt es sich, zunächst wenige aber für die jeweilige Organisation sinnvolle Informationssicherheitsziele zu definieren. Diese sollten im Verhältnis von Umsetzungsaufwand und Nutzen ausgewogen sein. Die festgelegten Informationssicherheitsziele sollten darüber hinaus möglichst messbar sein.

Wie schon beschrieben ist das Wichtigste bei der Einführung und dem Betrieb eines ISMS die Dokumentation. Ob etwas aufgenommen oder eben nicht aufgenommen wird in den Kanon der Dokumente, muss beschrieben werden. Dabei ist die Form der Dokumentation zweitrangig. Es muss nur sichergestellt sein, dass die Dokumente und Informationen, die Entscheidungsgrundlagen wieder aufgefunden werden.

Anbei eine Übersicht über alle notwendigen Dokumente für ein anstehendes Audit im Rahmen einer Zertifizierung:

OBLIGATORISCHE ISMS-DOKUMENTE:

- Anwendungsbereich (auch Geltungsbereich oder Scope genannt)
- Anwendbarkeitserklärung (engl.: SoA - Statement of Applicability)
- Interessierte Parteien und deren Anforderungen
- Ziele der Informationssicherheit
- Planung der ISMS-Ressourcen
- ISMS-Rollen und -Verantwortlichkeiten
- Gesetzliche und regulatorische Anforderungen
- Interne und externe Kommunikation im ISMS
- Auditprogramm
- Managementbericht
- Risikobehandlungsplan

05.03.02 Do – Check –Interne Auditierung

Warum interne Audits?

Ein internes ISO 27001 Audit ist als Selbstprüfung Ihres Managementsystems für Informationssicherheit zu verstehen. Dabei verfolgt das ISMS Audit das Ziel, Nichtkonformitäten/ Ungereimtheiten mit den Anforderungen der Norm ISO IEC 27001 aufzudecken.

Jedoch soll das Audit nicht nur Schwächen, sondern auch Stärken aufdecken. Der Auditor sucht dabei auch nach musterhaften Lösungen, um diese betriebsintern weiter zu verbreiten. So können auch andere Bereiche von diesen profitieren.

Auch die Norm für das Informationssicherheitsmanagement fordert die regelmäßige Umsetzung interner Audits. Dabei überprüfen Betriebe, ob das Managementsystem wirksam ist und mit den Anforderungen der Norm sowie den firmeninternen Forderungen übereinstimmt. Auf dieser Basis können Abweichungen abgestellt und Verbesserungspotenziale aufgedeckt werden.

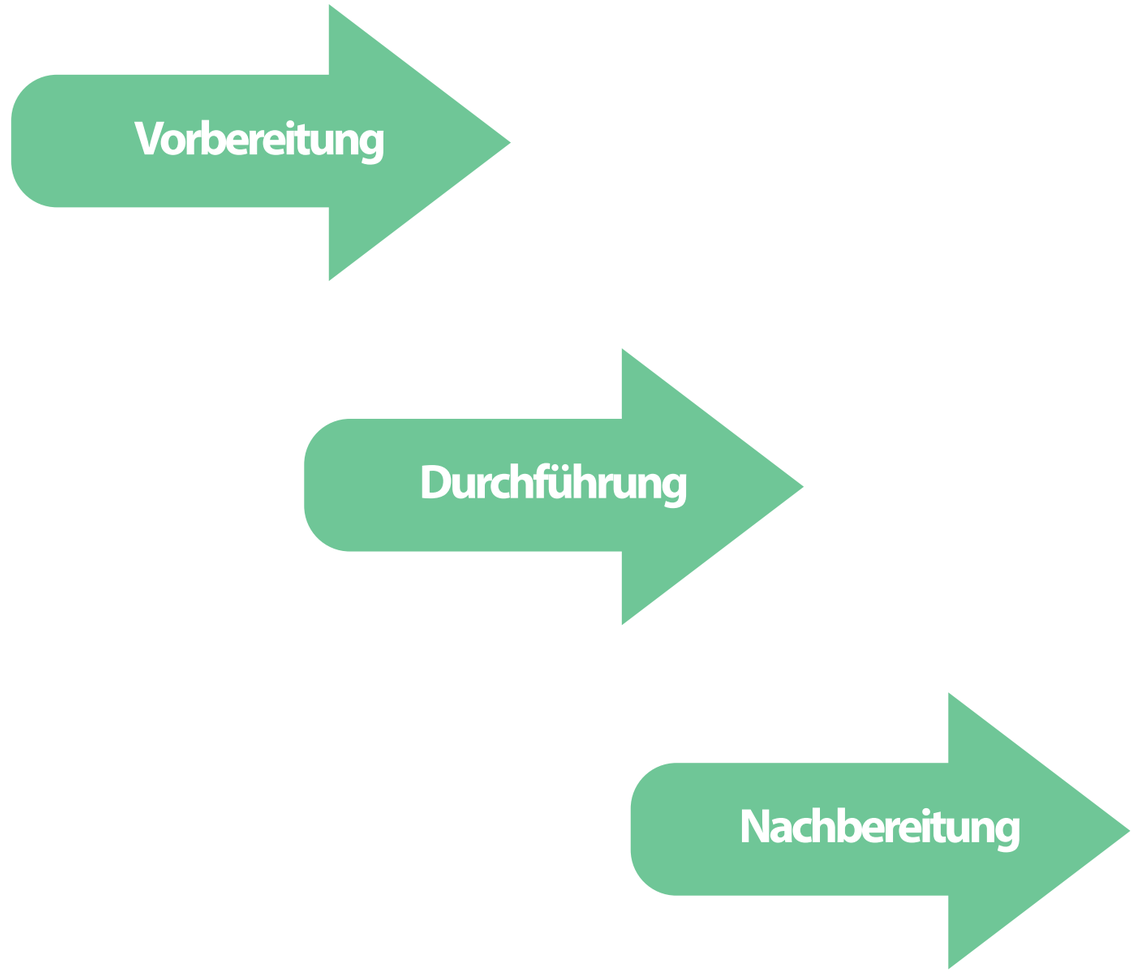
Neben internen Audits können aber auch externe Audits im Informationssicherheitsmanagement durchgeführt werden. Diese externen Audits erfolgen im Rahmen einer ISO 27001 Zertifizierung und werden daher auch Zertifizierungsaudits genannt.

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

Sehen Sie interne Audits als Möglichkeit, um für eine Verbesserung der Informationssicherheit im Unternehmen zu sorgen. Nutzen Sie Auditberichte, um auf Verbesserungsmöglichkeiten hinzuweisen! Bleiben Sie dran, denn mit jedem internen Audit erarbeiten Sie /das Unternehmen sich mehr Routine.

Ein ISM-Audit erfolgt in drei Phasen:



VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.03.02.01 Vorbereitung

Die Vorbereitung eines Audits beginnt mit der Erstellung des Auditprogramms. Dieses wird von einem benannten Auditprogrammleiter erstellt. Inhalte des Programms sind vor allem die Festlegung des genauen Ablaufs und der zu prüfenden Dokumente. Die Vorbereitung des Auditors auf das bevorstehende Audit beginnt meistens ca. 4 Wochen vor dem Audittermin. Der Auditor macht sich hierbei zunächst mit dem auditierten Bereich vertraut. Er sichtet zudem die Dokumente. Bei der Dokumentenprüfung erkennt der Auditor bereits, ob die Dokumentation nachvollziehbar und vollständig ist. Somit ist die Dokumentenprüfung auch bereits ein Teil des ISO 27001 Audits.

Auch die Erstellung einer Auditcheckliste mit allen für das Audit relevanten Punkte gehört zur Auditvorbereitung. Diese Checkliste bildet später die Grundlage für die Erstellung des Auditplans. Im Auditplan legt der Auditor den Tagesablauf zum Audit fest. Anschließend stimmt der Auditprogrammleiter den Auditplan mit dem zu auditierenden Bereich ab.

05.03.02.02 Durchführung

Die eigentliche Auditdurchführung beginnt mit einer Eröffnungsbesprechung. Bei dieser stellt der Auditor den Auditplan vor. Zudem können auch kurzfristig noch notwendige Änderungen diskutiert werden. Beim Audit an sich erfolgt dann die Sammlung von Informationen. Der Auditor benutzt dazu verschiedene Methoden

- Prüfung von Dokumenten
- Beobachtung bzw. Begehung vor Ort
- Gespräche mit Mitarbeitern

Der Auditor spricht normalerweise mit verantwortlichen Mitarbeitern über deren Tätigkeiten und Vorgehensweise. Anschließend vergleicht er diese gängige Praxis mit den Vorgaben aus dem ISMS. Stellt der Auditor dabei Abweichungen fest, muss er anschließend herausfinden, ob Änderungen an der Vorgabe oder dem Vorgehen der Mitarbeiter notwendig sind. Auf Basis der gesammelten Informationen bewertet der Auditor im ISO 27001 Audit dann, ob die Vorgaben der Norm und des Unternehmens eingehalten werden. Ist dies nicht der Fall, liegt eine Nichtkonformität vor. Liegt eine Abweichung vor, erteilt der interne Auditor Vorschläge für mögliche Korrekturmaßnahmen.

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.03.02.03 Nachbereitung

Am Ende und als Ergebnis eines Audits erfolgt die Erstellung eine Auditberichts. Auf Grund des Berichts muss der auditierte Bereich Korrekturmaßnahmen festlegen. Diese Maßnahmen verfolgen das Ziel, festgestellte Abweichungen zu beheben und ein erneutes Auftreten zu verhindern. Es gilt aber auch, Verbesserungspotenziale zu nutzen und passende Verbesserungsmaßnahmen abzuleiten. Normalerweise wird auch in diesem Rahmen eine Frist zur Behebung der Abweichungen fest. Verantwortlich für die Umsetzung der Maßnahmen ist dann der auditierte Bereich.

05.03.03 Check-Act – Am Beispiel Informations-sicherheitsvorfälle

Sicherheit ist trügerisch und eine 100% Sicherheit gibt es nicht. Aber unter Zuhilfenahme eines ISMS können eine systematische Abarbeitung der Vorfälle für alle transparent dargelegt werden.

Nehmen wir mal an, in Ihrem Unternehmen wird eine E-Mail mit wichtigen, datenschutzrelevanten und unternehmenskritischen Unterlagen an die falsche E-Mailadresse versendet.
Für solche Informationssicherheitsvorfälle gibt die Norm klare Regeln vor, allen voran eine systematische Herangehensweise bei deren Meldung und Erfassung.
Das Unternehmen ist hier in der Pflicht einen Prozess zu verankern, der die Meldung, Erfassung und Behebung definiert. Alle Mitarbeiter*innen müssen diesen Prozess und ihre Rolle/ihre Verantwortung in dem Prozess unbedingt kennen und üben. Eine regelmäßige Schulung ist deshalb unbedingt nötig.
Wenn es bereits bestehende Meldeprozesse im Unternehmen gibt, sollten diese Prozesse und Stellen bei der Etablierung des Prozesses berücksichtigt und genutzt werden.

Wenn es keine Sicherheitsvorfälle gibt, freuen Sie sich! Aber bevor Sie sich freuen, schauen Sie mal, ob nicht der Pizzalieferant an Ihrer Tür vorbeiläuft, um den Kolleg*innen das Mittagessen zu bringen. Wird er begleitet? Wer hat ihn ohne Begleitung hineingelassen. Manchmal sind es nicht die großen Dinge, die hier berücksichtigt werden müssen, manchmal sind es ganz „kleine“ Vorfälle, die zu großen Sicherheitskrisen führen.

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.03.04. Check-Act – Bewußtsein schaffen für Sicherheitsvorfälle

Und manchmal ist es nur eine E-Mail der Bank….

die ein Mitarbeiter*in öffnet und damit ein ganzes Unternehmen für Tage und Wochen lahmlegt.
Entsprechend fordert die Norm ISO 27001, dass Mitarbeiter*innen sensibilisiert werden, sich mit dem Thema Informationssicherheit auseinander zu setzen und das regelmäßig. Hier lässt die Norm viel Freiheit zur Ausgestaltung. Allerdings ist es sinnvoll, mindestens bei Eintritt in das Unternehmen und in der Folge einmal im Jahr ein Training zur Informationssicherheit anzubieten.
Dabei können dann auch die Prozesse wiederholt und weitere relevanten Sicherheitsinformationen geschult werden.
Bitte dokumentiere Sie die Schulungen, damit Sie dem Auditor auch nachweisen können, dass Schulungen stattgefunden haben.

05.03.05. Check-Act- ISMS Selbsteinschätzung

Als Teil des internen Audits hat es sich bewährt ein sogenanntes Selfassessment (eine Selbsteinschätzung) in den ISMS-Prozess zu integrieren.

Sie müssen die insgesamt 114 Maßnahmen, die im der Anhang A der ISO 27001 ausgeführt sind, grundsätzlich erfüllen, es sei denn Sie können im Rahmen der Anwendbarkeitserklärung argumentieren, warum einzelne Anforderungen auf Ihr Unternehmen nicht zutreffen.

Die Norm schreibt hier nicht vor, wie Sie sicherstellen können, dass Sie auch alle 114 Maßnahmen bewertet haben. Deshalb ist es sinnvoll im Rahmen einer Selbsteinschätzung den aktuellen Stand der Maßnahmen kontinuierlich aber immer auch im Rahmen des internen Audits zu bewerten.

Im Rahmen eines Selfassessments bewerten Sie Ihren aktuellen Stand der einzelnen Maßnahmen. Methoden der Bewertung gibt es viele. Die einfachste ist das Ampelsystem. Analog zu einem Ampelsystem können Sie definieren, welche Messwerte noch akzeptiert werden und diese mit den Farben grün/gelb/rot versehen.

Als grafische Aufbereitung einer Exceltabelle können sie in einer Auswertung den Erfüllungs- und Reifegrad Ihres Unternehmens sehr gut auch an die Geschäftsführung berichtet werden.

Nachfolgend sind einige, sogenannten KPIs (Key Performance Indicator) aufgelistet. Jedes Unternehmen muss aber für sich entscheiden, ob diese passend sind:

- Anzahl Verstösse gegen die Benutzer-Richtlinien
- Nicht eingehaltene Recovery-Zeiten gemäss BCM
- Anzahl falsch erfasster Tickets
- Anzahl Lieferanten / Partner ohne entsprechenden Vertrag
- Anzahl Sicherheitsverletzungen Intern
- Anzahl Sicherheitsverletzungen durch Externe
- Anzahl Abweichungen zur ISO-Norm
- Anzahl Personen ohne interne Awareness-Schulung
- Anzahl nicht rechtzeitig überprüfte Dokumente
- Anzahl falsch entsorgter Geräte / Festplatten / Mobile Geräte
- Anzahl falsch vergebener Berichtigungen (Systeme, File-Struktur, etc.)
- Anzahl nicht begleiteter externen Personen

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.04. Berichtswesen/ Reporting

In Unternehmen trägt die Geschäftsführung die Verantwortung. Natürlich ist sie damit auch für das ISMS und die daraus resultierenden Abweichungen, Aufgaben und Verbesserungen zuständig. Damit sie auf dem Laufenden bleibt und mögliche Missstände schon früh erfährt, muss sie einen regelmäßigen Managementbericht über den Status des ISMS erhalten – eine sogenannte „Managementbewertung".

Der Turnus dieser Berichterstattung ist nicht geregelt, es sollte aber mindestens einmal im Jahr einen Bericht geben. Je nach Reifegrad des Unternehmens kann es sinnvoll sein, auch halb- oder vierteljährliche Berichte zu erstellen.
Die Inhalte der Managementbewertung sind in der Norm wieder geregelt.

Das umfasst z. B. den Status von Maßnahmen, Ergebnisse aus internen Audits sowie dem Risikomanagement und einiges mehr (siehe ISO 27001, Kapitel 9.3.)

Da viele Dokumente schon in dem Unternehmen – allerdings oft an verteilen Stellen aufbereitet bereit liegen, macht es Sinn, Dokumente, die für die Managementbewertung wichtig sein können, zentral abzulegen bzw. zusammenzufassen.

Das einfache Zusammentragen der Informationen ergibt sich, wenn Sie bereits bei folgenden Bereichen an das ISMS und ein Audit denken:

- Beim Messen von Kennzahlen und Zielen der Informationssicherheit
- Bei der Steuerung von Maßnahmen
- Bei der Dokumentation von Sicherheitsvorfällen
- Im Risikomanagement, zu den jeweiligen Risiken sowie deren Behandlung
- Bei der Dokumentation der Ergebnisse von internen Audits
- Bei der Auswertung des Selfassessments

Es gibt darüber hinaus zwei Dinge, die unbedingt in die Managementbewertung gehören, jedoch nicht in bereits bestehenden Prozessen generiert werden:

01 Die Rückmeldung von interessierten Parteien, beispielsweise wenn sich ein Kunde, eine Behörde oder ähnlichem in Bezug auf Themen der Informationssicherheit bei Ihnen meldet.

02 Die Themen, die einen signifikanten Einfluss auf das ISMS haben. Das können beispielsweise Neuprodukte oder wesentliche Änderungen an Produkten, neue Kerngeschäftsprozesse oder neue Standorte sein.

Wenn bereits während des Berichtszeitraums hier Informationen vorliegen, können diese schnell und unkompliziert in die Managementbewertung einfließen.

Die Managementbewertung besprechen Sie gemeinsam mit der Geschäftsführung, die ihrerseits nun Rückmeldungen, neue oder angepasste Zielen, neuen Maßnahmen und mehr als Feedback einfließen lässt. Dieses Feedback gehört mit in die Managementbewertung. Ergänzen Sie diese im Nachgang und lassen Sie die Managementbewertung von der Geschäftsführung gegenzeichnen.

VORGEHENSWEISEN & ERFOLGSFAKTOREN

05

05.05. Plan-Do-Check-Act – der kontinuierliche Verbesserungsprozess (KVP)

Der Aufbau eines Managementsystems für Informationssicherheit ist eine einmalige Aufgabe. Aber das Betreiben ist ein ständiger Prozess, der kontinuierlich auf Eignung, Angemessenheit und Wirksamkeit geprüft werden muss.

Wichtig bei der kontinuierlichen Verbesserung ist, dass sämtliche Prozesse und Tätigkeiten immer wieder auf den Prüfstand kommen. Und genau das will ein Auditor sehen. Mit den obengenannten Praxisbeispielen wie Risikoanalyse, Selbsteinschätzungen oder Schulungen können diese Verbesserungen kontinuierlich erreicht werden.

Um eine kontinuierliche Verbesserung nicht aus dem Auge zu verlieren, können Sie eine interne Aufgabe definieren, die Sie in Outlook, einem Tool oder über einen Kalender regelmäßig überwachen. Sinnvoll ist es, gleich hier wieder an das Reporting zu denken und die Maßnahmen entsprechend zu klassifizieren.

Entscheidend ist, dass diese Verbesserungspotenziale in Maßnahmen überführt und nachgehalten werden. Ein konkreter Vorschlag zur Umsetzung eines KVPs wird nicht vorgeschrieben. Deshalb müssen Sie entweder auf ein Tool ausweichen oder sich einen eigenen Prozess definieren.
Die ISO 27001 fordert zwar kein konkretes Mindestlevel in Bezug auf Informationssicherheit, dafür aber ganz deutlich, dass das Managementsystem und damit die Sicherheit im Unternehmen einem kontinuierlichen Verbesserungsprozess unterliegen muss.

FAZIT

06

06.01 Sicherheit als Wettbewerbsvorteil

Ein zertifiziertes ISMS nach ISO 27001 wird zunehmend zum Wettbewerbsvorteil. Sie setzen damit ein starkes Zeichen für die Sicherheit von Informationen, Daten und Systemen. Als zukunftsfähiges Unternehmen müssen Sie sich schließlich auf eine belastbare IT verlassen können. Und nicht nur Sie, sondern auch Ihre Kunden, Ihre Stakeholder und Ihre Geschäftsführung.

Nutzen Sie das ISMS als Chance, um durch die geschaffenen Prozesse auf Bedrohungen und technische Entwicklungen schnell und angemessen reagieren zu können. Damit minimieren Sie Ihr Risiko beträchtlich und empfehlen sich als stabiler Partner.

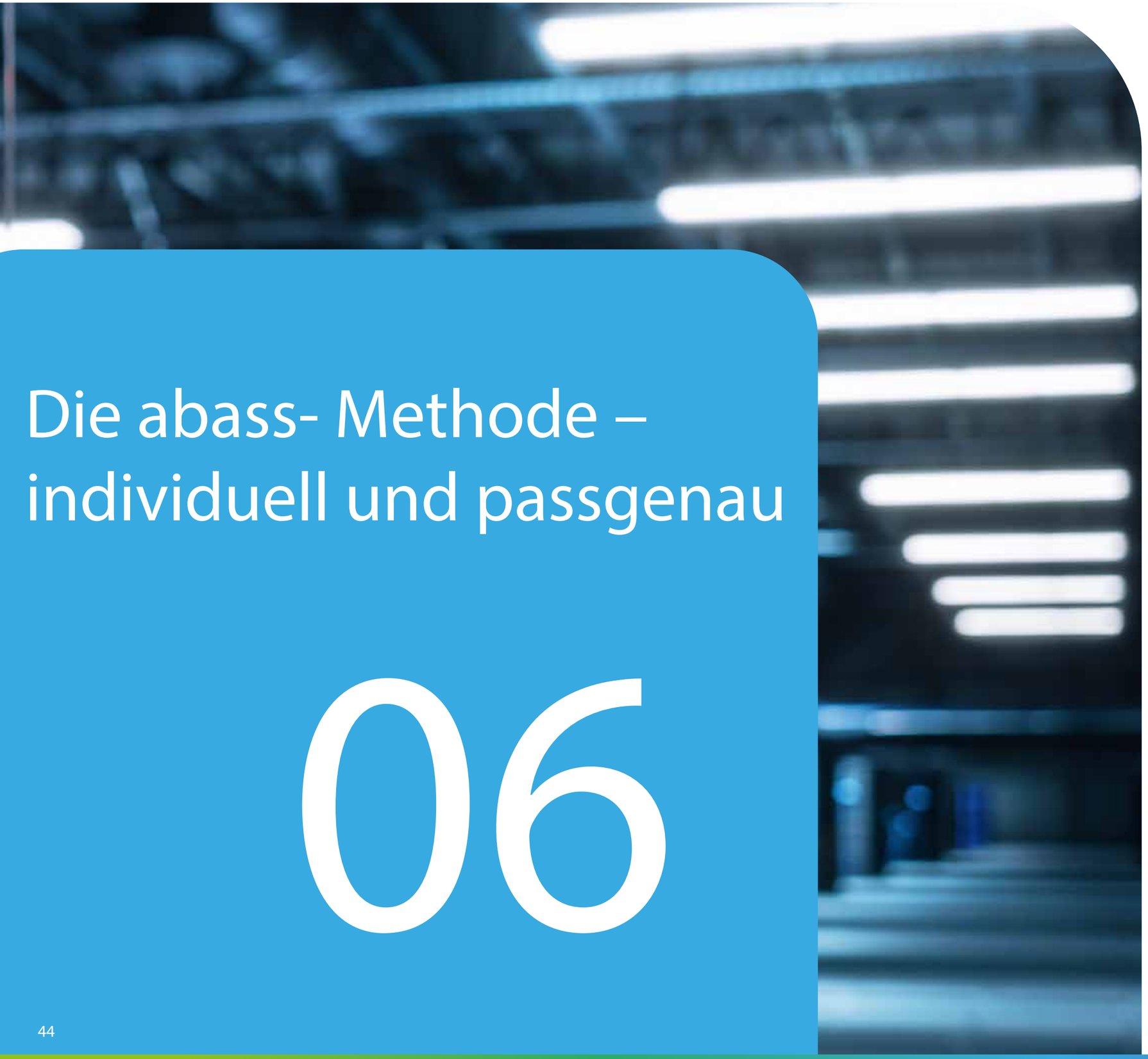
Lassen Sie sich nicht vor den zahlreichen Anforderungen der Norm abschrecken. Oft existieren im Unternehmen bereits viele dokumentierte Sicherheitsmaßnahmen oder Maßnahmen, die für ein Audit lediglich noch beschrieben werden müssen.

Nutzen Sie auch bereits existierende Prozesse, um z. B. Maßnahmen zu steuern und Vorfälle zu melden.

Insbesondere bei der Erstzertifizierung geht es darum, die notwendige Dokumentation sowie die Prozesse nachzuweisen. Die Sicherheitsmaßnahmen aus dem Anhang A der Norm müssen nicht lückenlos umgesetzt sein. Jedoch müssen notwendige Maßnahmen identifiziert und ein Weg aufgezeigt werden, wie und wann diese umgesetzt werden.

Bei der Einführung eines ISMS kann ein entsprechendes ISMS-Tool helfen. Achten Sie darauf, dass das ausgesuchte Tool zu Ihrem Unternehmen und Ihren Ressourcen passen.

Um die Akzeptanz im Unternehmen zu schaffen oder zu erhöhen, ist eine frühzeitige Einbindung in den ISMS-Einführungsprozess sinnvoll und nötig! Hier haben sich Feedbackprozesse zu Dokumenten bewährt.



Die abass- Methode – individuell und passgenau

06

Die Anforderungen an die IT – Sicherheit bei unseren Kunden wird tagtäglich größer. Wir stellen dafür seit langen Jahren unsere Expertise bereit.
Wir zeigen unseren Kunden, wie ihre Systeme sicherer werden können und unterstützen sie dabei, die Systeme – in allen Bereichen – sicher und stabil zu betreiben.

Informations-sicherheits-management – ISO/IEC 27001

Wir begleiten unseren Kunden beim Thema Sicherheit auch im Rahmen
gesetzlicher und regulatorischer Auflagen, so z.B. zur Erlangung von ISO/IEC 27001 Zertifikaten zum Betrieb sicherer IT-Infrastrukturen.

Herr Dipl. Math. Konrad Delp ist als zertifizierter Auditor für ISO/IEC 27001+27002 Ihr Ansprechpartner für alle Fragen zum Thema Informationssicherheitsmanagement

Dipl.-Math. Konrad Delp
Gesellschafter/Geschäftsführer

ISO / IEC 27001 ISMS-Officer
(Planung, Implementierung und Verbesserung
eines ISMS nach ISO/IEC 27001)
ISO / IEC 27001 ISMS-Auditor –
TÜV SÜD zertifiziert
(Planung, Durchführung und Nachbereitung eines ISMS nach ISO/IEC 27001)

IT-Sachverständiger und Gutachter
Bundesverband der IT-Sachverständigen und -Gutachter e.V.
BVMW-geprüfter Berater für mittelständische Unternehmen
Bundesverband mittelständische Wirtschaft
Unternehmerverband Deutschland e.V.
ISA/ IEC 62443 Cybersecurity Berater für mittelständige Unternehmen
VDMA e.V. geprüft (IT-Sicherheit für vernetzte Maschinen und Anlagen)

Individuell.
Kompetent.
Hersteller-
unabhängig.

abass-
und Ihre IT-Läuft.