Systemgestütztes ISMS nach ISO 27001

Ein Leitfaden zur Abbildung des Informations-Sicherheits-Management-Systems (ISMS) nach ISO 27001 mit ibi systems iris

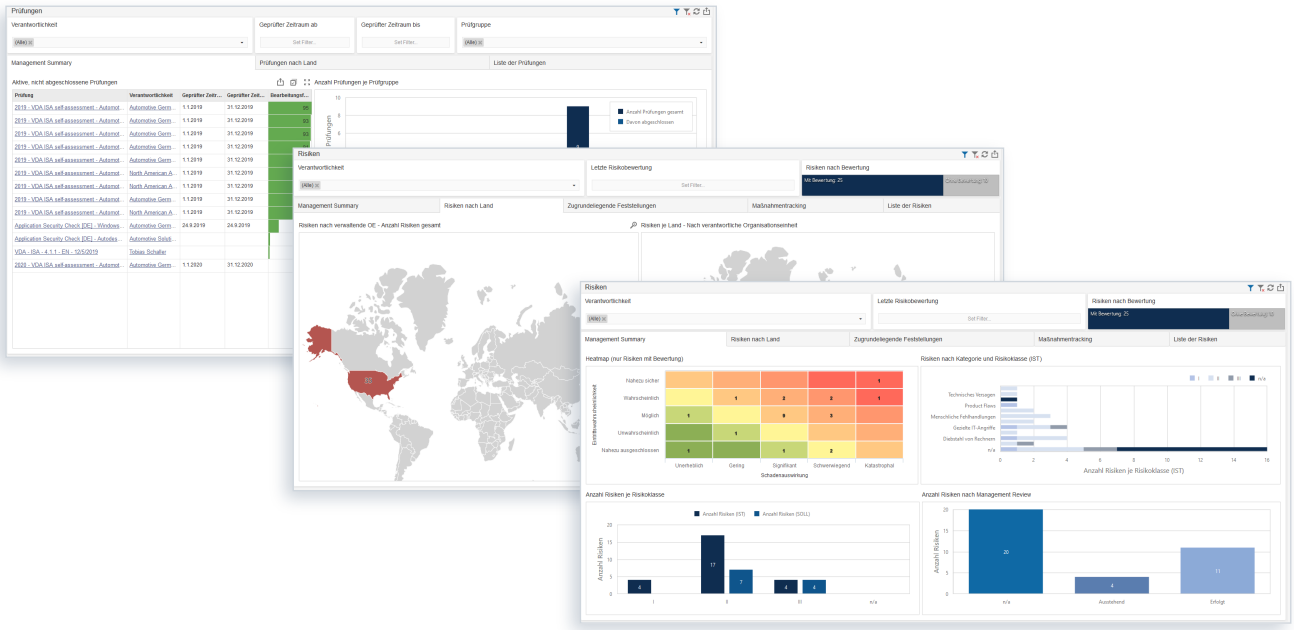
Jede Organisation, unabhängig der Branche, Rechtsform oder Größe, ist heute und in Zukunft auf eine angemessene Informationssicherheit angewiesen. Dies liegt daran, dass nahezu kein Geschäftsprozess ohne IT-Unterstützung effektiv und effizient ausgeführt werden kann und Daten und Informationen von immenser Wichtigkeit für die einzelnen Organisationen sind. Angriffe auf die Informationssicherheit stellen daher eine nicht zu verachtende Bedrohungslage dar, die von existentiellen wirtschaftlichen Verlusten bis hin zu personenbezogenen Schäden führen kann. Daher ist ein angemessener Schutz der Informationen bzw. ein angemessenes Niveau der Informationssicherheit inhärentes Interesse jeder Organisation und zudem Inhalt diverser rechtlicher und regulatorischer Anforderungen.

Stellt sich die Frage, wie setzt man Informationssicherheit angemessen um? Die international anerkannte Norm für Informations-Sicherheits-Management-Systeme (ISMS) ***ISO/IEC 27001*** *bietet Organisationen einen Rahmen, die Informationssicherheit zu planen, umzusetzen, zu überwachen und kontinuierlich zu verbessern. Durch die optionale Zertifizierung kann die Einhaltung des Standards bestätigt und damit die Wettbewerbsfähigkeit gesteigert sowie das Unternehmensimage in der Öffentlichkeit und bei Geschäftspartnern gestärkt werden.*

- Ganzheitlicher Ansatz nach ISO 27001
- Steigerung der Reputation
- Effektivitäts- und Effizienzgewinn

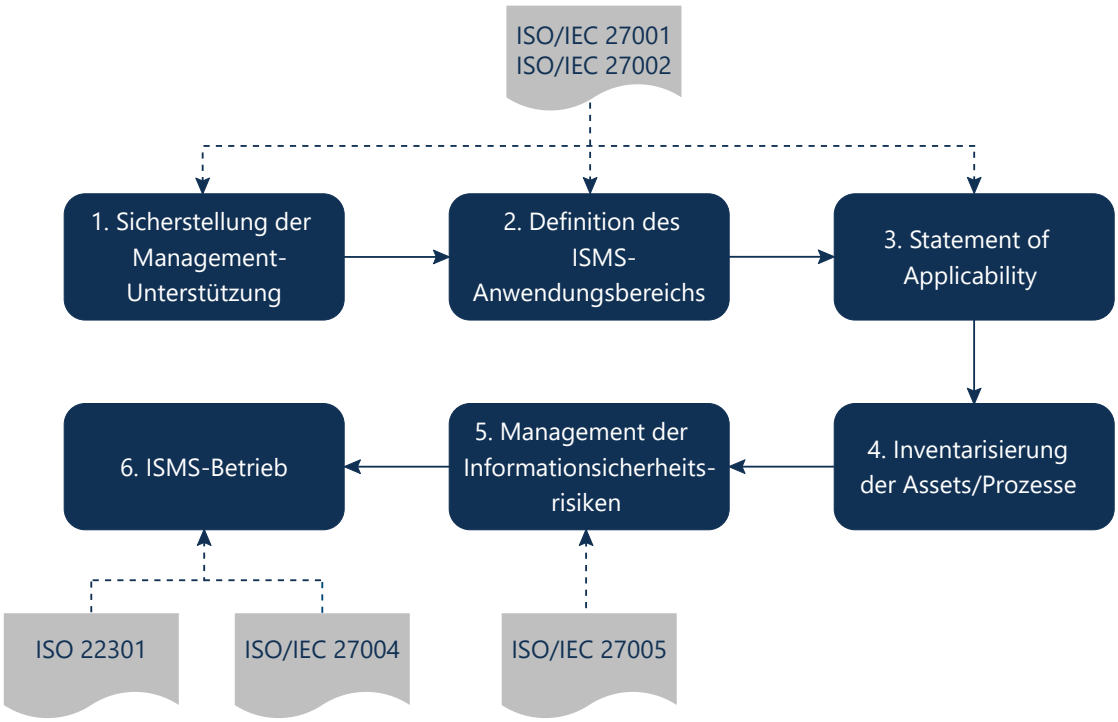
Doch wie lässt sich eine ganzheitliche und umfassende Informationssicherheit im Unternehmen garantieren bzw. wie lässt sich der Zertifizierungsprozess unterstützen und somit leichter bewältigen? Die Antwort ist ein systemgestütztes ISMS. Hierdurch wird ein nachhaltiger Mehrwert bei gleichzeitiger Kostenreduktion generiert. Die Software „ibi systems iris" bietet dies und garantiert einen erheblichen Effektivitäts- und Effizienzgewinn.

Wie ein mögliches Vorgehen zur Umsetzung der ***ISO 27001*** *mit ibi systems iris aussehen kann, wird in diesem Leitfaden beschrieben.*



Systemgestütztes ISMS in sechs Schritten

Im Folgenden wird zuerst ein Überblick über den Prozess des systemgestützten Informationssicherheitsmanagementsystems in ibi systems iris gegeben. Danach wird genauer auf die einzelnen Schritte zur Umsetzung eingegangen.



Überblick zum Prozess

Zu Beginn ist es entscheidend, die Unterstützung des Managements sicherzustellen und im Anschluss den Anwendungsbereich des ISMS genau zu definieren. Anschließend gilt es zu überprüfen, welche Controls aus dem Anhang A der ISO 27001 umgesetzt werden müssen bzw. welche Controls ausgeschlossen werden können. Das Ergebnis ist das Statement of Applicability. Aufbauend darauf gilt es, alle Assets und Prozesse zu inventarisieren. Nach diesen in gewisser Weise noch vorbereitenden Tätigkeiten gilt es, den ISMS-Betrieb zu etablieren. Dies umfasst Prüfungen, Kennzahlen und Sicherheitsvorfälle.

1. Sicherstellung der Management-Unterstützung

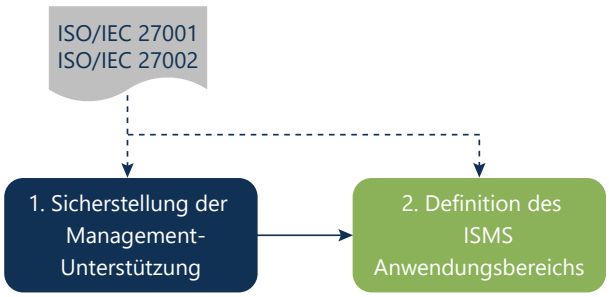
Die ersten Schritte zum Aufbau eines ISMS sind nur bedingt mit Softwareunterstützung umzusetzen. Denn zu Beginn gilt es, durch Initiative der Geschäftsführung den Stein ins Rollen zu bringen. Hierbei ist es nicht von Bedeutung, ob die Einführung eines ISMS durch Gesetze oder Kunden vorgeschrieben wird oder auf internen Vorschlägen beruht – der Sicherheitsprozess muss von der Geschäftsleitung angestoßen, genehmigt und auch (kontinuierlich) vorgelebt werden.

Nur wenn das Management seiner Vorbildfunktion gerecht wird (**Kapitel 5 Führung aus der ISO 27001**) und sich um Informationssicherheit bemüht, wird die Aufgabe „Informationssicherheit" auch wahrgenommen.

Das geht von organisatorischen, dokumentierten Leit- und Richtlinien zur Informationssicherheit bis hin zum täglichen Handeln (z. B. Umgang mit vertraulichen Dokumenten). Das bedeutet aber auch, dass die Leitung – nach innen wie auch nach außen – verantwortlich für den adäquaten Umgang mit Risiken und die Zurverfügungstellung von finanziellen und personellen Ressourcen zur Umsetzung des Prozesses ist.

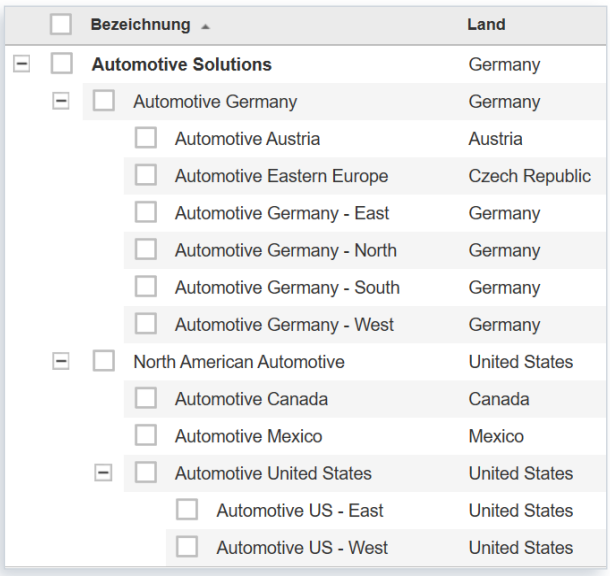
2. Definition des ISMS-Anwendungsbereichs

Von besonderer Bedeutung ist die angemessene Definition des Geltungsbereichs des ISMS (**Kapitel 4 Kontext der Organisation aus der ISO 27001**). Gerade bei größeren Organisationen ist dies nicht immer einfach und ein Ausrollen auf die Gesamtorganisation oder mehrere Abteilungen parallel will gut bedacht sein. Eine Software erleichtert es enorm, auch später weitere Geschäftsbereiche in den Geltungsbereich mit aufzunehmen.



Durch die Informationssicherheitsleitlinie legt das Management fest, mit welcher Strategie das angestrebte Sicherheitsniveau im Geltungsbereich erreicht werden soll und definiert die Organisation des Sicherheitsprozesses. Neben der Leitungsebene, die letztlich die Verantwortung für die Informationssicherheit trägt, muss auch eine Organisation für das operative Geschäft aufgebaut werden. Hierzu sollte ein Informationssicherheitsbeauftragter (ISB) eingesetzt werden. Dieser übernimmt die verantwortliche Führung des Informations-Sicherheits-Management-Systems im Sinne der Planung, Implementierung, Weiterentwicklung und Prüfung des ISMS und kümmert sich unter anderem um die Feststellung von Schwachstellen sowie deren Beseitigung.

Um die Leitung, den Informationssicherheitsbeauftragten (ISB) und andere Verantwortliche wie auch diejenigen, die bestimmte Maßnahmen zur Risikoreduzierung schlussendlich umsetzen müssen, adäquat zu unterstützen, eignet sich eine softwaregestützte Umsetzung eines ISMS. Dadurch können Ziele besser überprüft und schneller gesteuert werden. Ein Software-Tool kann zugleich Management-Cockpit für die Leitung, operatives Unterstützungswerkzeug für den ISB als auch Hilfe zur Umsetzung bestimmter Maßnahmen für die jeweiligen Ansprechpartner sein. Des Weiteren können Ziele, die unter anderem in der Leitlinie festgelegt wurden, durch verschiedenste Prüfungen oder durch ein Kennzahlensystem überprüft werden.

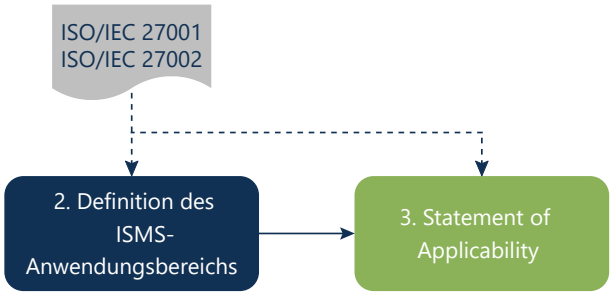


Bezeichnung	Land
Automotive Solutions	Germany
Automotive Germany	Germany
Automotive Austria	Austria
Automotive Eastern Europe	Czech Republic
Automotive Germany - East	Germany
Automotive Germany - North	Germany
Automotive Germany - South	Germany
Automotive Germany - West	Germany
North American Automotive	United States
Automotive Canada	Canada
Automotive Mexico	Mexico
Automotive United States	United States
Automotive US - East	United States
Automotive US - West	United States

Wie beschrieben, haben vor allem die Leitungsebene als verantwortliche Stelle sowie der bestellte ISB eine Sonderstellung in der Aufbauorganisation. Gerade der ISB muss die nötigen Mittel besitzen, um seine Aufgaben durchführen zu können und Ergebnisse direkt an die Leitung zu berichten. Der ISB ist die zentrale Instanz, bei der alles zusammenlaufen muss. Außerdem sollte jeder Mitarbeiter im Anwendungsbereich aktiv am ISMS mitgestalten, sei es durch die Umsetzung einzelner Maßnahmen oder die Meldung von Sicherheitsereignissen, die dann vom ISB überprüft und bewertet werden. Diese Meldung kann beispielsweise direkt in ibi systems iris erfolgen. All die Verantwortlichen sollten in ibi systems iris angelegt werden, um ihre Aufgaben systemunterstützt effizient erfüllen zu können.

In ibi systems iris können u. a. interne und externe Regelwerke, Standards und Gesetze angelegt und verwaltet werden. Die Kompendien können manuell in ibi systems iris angelegt oder automatisiert importiert werden und werden anschließend in einer Baumstruktur angezeigt. Die verschiedenen Kompendien und deren Kapitel können in der Software verknüpft und genutzt werden.

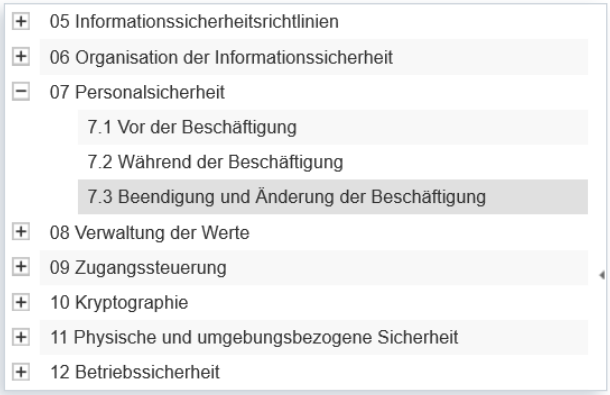
3. Statement of Applicability



Um die Erklärung zur Anwendbarkeit (=Statement of Applicability, SoA) nach ISO 27001 auszufüllen, bietet sich eine Prüfung in ibi systems iris an. Hier ist die Prüfvorlage schon vorhanden und muss nur entsprechend befüllt werden. Somit ist es ein Leichtes, Controls der ISO 27002 (bzw. Anhang A der ISO 27001) auszuschließen und den Ausschlussgrund zu dokumentieren oder auch anwendbare Controls näher zu beschreiben.

In der Prüfungsansicht hat der Auditor die Möglichkeit, sich mithilfe der Navigation durch eine Prüfung zu navigieren.

Dies kann auch durch weitere Dokumente (z. B. Verknüpfungen zu Richtlinien) passieren. Somit kann bei einem gelebten ISMS auch immer die SoA als Ausgangspunkt für Audits genutzt werden, da hier die notwendigen Richtlinien oder auch Prozessbeschreibungen leicht auffindbar sind.

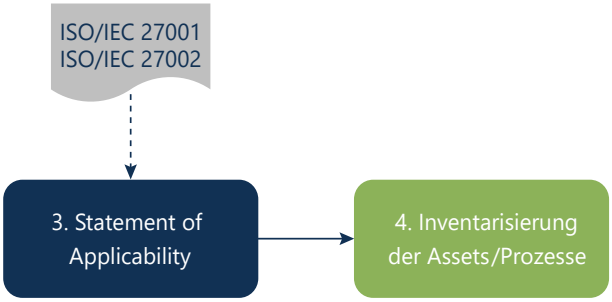


Parallel zum Ausfüllen der SoA können auch erste Feststellungen und Maßnahmen angelegt werden. Abschließend kann über die SoA-Prüfung ein Bericht erzeugt werden, der für die Zertifizierung verwendet werden kann.

Ergebnisse:

- Direkte Hinterlegung von Dokumenten und Erstellung von Feststellungen bzw. Schwachstellen
- Ständig aktueller und verfügbarer Nachweis im ISMS-Betrieb und bei der Zertifizierung

Geschäftsprozesse und Assets



Sind der Scope und die anwendbaren Controls definiert, können die Geschäftsprozesse der Organisation inklusive Verantwortlichkeiten sowie die verarbeiteten Informationen ermittelt werden – sei es innerhalb oder außerhalb von IT-Systemen. In einem ersten Schritt ist es auch sinnvoll, sich schon über den Schutzbedarf dieser Informationen Gedanken zu machen: Gibt es also Informationen, die bezüglich der Vertraulichkeit, Integrität oder Verfügbarkeit von besonderer Wichtigkeit sind?

Dieses Vorgehen impliziert eine Ersterfassung aller Prozesse und Werte der Organisation. Dass dies nicht alleine von einem ISB bewerkstelligt werden kann, scheint klar. Deswegen müssen zu einer detaillierten und umfänglichen Erfassung auch weitere Ansprechpartner in den Prozess einbezogen werden. Nur so kann schlussendlich der gesamte Anwendungsbereich betrachtet und gesichert werden.

Sinnvoll ist es, die relevanten Werte und Prozesse nach Kategorien zu erfassen. Dazu liefert ibi systems iris von Haus aus die entsprechenden Kategorien zum Beispiel nach IT-Grundschutz, die von Gebäuden und Räumen über IT-Systeme, Anwendungen, Netzen bis hin zu Daten und Personal reichen. Es muss entschieden werden, ob man alle Objekte mit den jeweiligen Verantwortlichkeiten detailliert erfassen möchte, oder dies nur auf Basis von vereinfachten, übergeordneten Kategorien tun möchte, in denen man ähnliche Objekte zusammenfasst.

Durch die Möglichkeit der Abbildung der Architektur können Sie die Anforderungen **A.8.1.1 Inventarisierung der Werte** und **A.8.1.2 Zuständigkeit für Werte aus dem Anhang A der ISO 27001** darstellen. Zu jedem Wert bzw. Datensatz kann in ibi systems iris eine Verantwortlichkeit eingetragen werden.

Ausgehend von der Erfassung der Objekte können diese miteinander in Zusammenhang gebracht werden und die Abhängigkeit modelliert

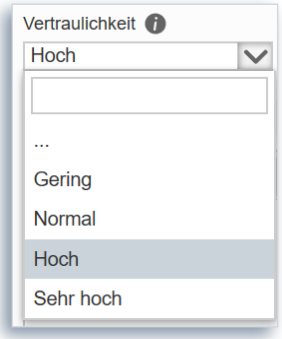
werden. Dadurch entsteht in ibi systems iris ein vereinfachter Netzplan.

Auf Basis dieser Inventarisierung kann auch der Schutzbedarf festgelegt werden. Außerdem können interne oder gesetzliche Bestimmungen bzw. branchenspezifische Sicherheitsstandards, die als Kompendien in ibi systems iris hinterlegt sind, den einzelnen Objekten zugeordnet werden, um diese näher zu beschreiben oder spezielle Sicherheitsanforderungen zu definieren.

Sollte vorher schon eine Erfassung der einzelnen Assets stattgefunden haben, sei es in Form einer Excel-Tabelle oder auch in einer Configuration Management Database (CMDB), kann man über einen Import oder eine Anbindung der Daten an ibi systems iris nachdenken.

Wichtig für das gesamte Vorgehen ist, dass man die einzelnen Schritte dokumentiert und wichtige Dokumente direkt an den jeweiligen Stellen verknüpft. So können Assets und Prozesse durch Verweise detaillierter beschrieben werden und die entsprechende Dokumentation ist direkt ohne Medienbruch über ibi systems iris aufrufbar.

Schutzbedarf bestimmen



Als nächster Schritt können die Schutzbedarfe nach Verfügbarkeit, Vertraulichkeit, Integrität und – falls gewünscht – Authentizität zugeordnet und vererbt werden. Der eigene Schutzbedarf des Prozesses/Assets kann eingetragen werden und zusätzlich wird der tatsächliche Schutzbedarf unter Berücksichtigung aller vererbenden/erbenden Verknüpfungen zum ausgewählten Prozess/Asset berechnet. Das bedeutet, wenn ein nachgelagertes Asset einen höheren Schutzbedarf als das bearbeitete Asset hat, wird dieser direkt vererbt. Befindet sich beispielsweise ein kritischer Server in einem eigentlich als unkritisch eingestuften Serverraum, wird der Schutzbedarf des Serverraums automatisch ebenfalls höhergestuft und der Schutzbedarf angepasst.

Verantwortlichkeiten

Sowohl bei Assets als auch bei Prozessen werden Verantwortlichkeiten zugewiesen. In ibi systems iris kann eine Person oder eine Organisationseinheit als Verantwortlichkeit eines Assets/Prozess hinterlegt werden.

Zusätzlich kann ein Datensatz durch eine Organisationseinheit verwaltet werden, dies ermöglicht die Weitergabe eines Datensatzes (z. B. eines Prozesses) an eine andere Organisationseinheit bzw. Teilbereich des Unternehmens.

Berechtigungen

Berechtigung für	Berechtigungsumfang
Verantwortlichkeit	
Automotive Solutions	Benutzer/Organisationseinheit
Verwaltet durch Organisationseinheit	
Automotive Solutions	Benutzer/Organisationseinheit

Business Impact Analysen

Für jeden Prozess kann in ibi systems iris der Business Impact angegeben werden. Zusätzlich wird der Business Impact unter Berücksichtigung von nachgelagerten, wesentlichen Prozessen systemseitig automatisch berechnet. Des Weiteren können die Wiederherstellungszeitpunkte (RPO) und die maximal tolerierbare Ausfallzeit (MTD) für einen Prozess angegeben werden. Diese Angaben werden im Funktionsbereich Notfall genutzt.

Business Continuity Management

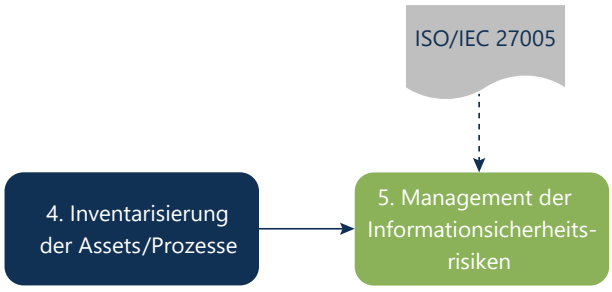
Weiteren Input für das Notfallmanagement liefern die Angaben aus dem Bereich Business Continuity Management eines Prozesses oder Assets. In ibi systems iris ist es möglich, die Aktivitäten inklusive Wiederanlaufzeit (RTO) und Wiederherstellungszeit (WRT) für einen Prozess/Asset anzugeben.

Durch die Business Impact Analyse und das Business Continuity Management in ibi systems iris können Sie die Anforderung **A.17.1 Aufrechterhalten der Informationssicherheit** aus dem **Anhang A der ISO 27001** erfüllen und dokumentieren.

Ergebnisse:

- Zuständigkeiten für Assets und Prozesse klar definiert
- Automatisierte Handlungsempfehlungen je Kategorie (Gefährdungen und Maßnahmen)
- Modellierung inkl. (vererbten) Schutzbedarf

5. Management der Informationssicherheitsrisiken



Die **ISO 27001** fordert in **Kapitel 6 (Planung)** und **8 (Betrieb)** u. a., Maßnahmen zum Umgang mit Risiken und deren regelmäßige Beurteilung und Behandlung festzulegen. Die geforderten Punkte aus der ISO 27001 können mithilfe der Software ibi systems iris umgesetzt werden.

In allen Funktionsbereichen werden die Datensätze in einer übersichtlichen Listenansicht angezeigt. Beispielsweise können Sie sich alle Risiken aufgelistet anzeigen lassen. Die Spalten der Listenansicht können per Drag & Drop geändert werden. Zusätzlich können Spalten per Klick ein- und ausgeblendet werden. Somit ist es benutzer-

spezifisch möglich, sich seine eigene Listenansicht zu generieren. Die Datensätze sind zusätzlich filterbar. Alle Datenfelder können als Filtermöglichkeit genutzt werden. Die definierten Filter können abgespeichert werden und zukünftig per Mausklick ausgewählt werden. Risiken können manuell erstellt, aus vordefinierten Gefährdungen abgeleitet oder importiert werden.

Bezeichnung	Risikokategorien
Theft of Laptop (CAD workstation)	Diebstahl von Rechnern
Unauthorized access of confidential data on Android mobile devices	Gezielte IT-Angriffe
Unauthorized access of CAD database	Gezielte IT-Angriffe

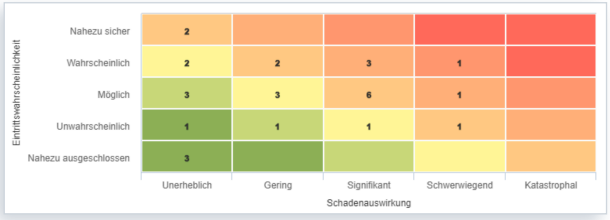
Risikoidentifizierung und -erfassung

Für ein Risiko können allgemeine Daten wie eine Bezeichnung und Schlüsselwörter für eine bessere Filterung und Kategorisierung angegeben werden. Zusätzlich können Eigenschaften wie eine Risikokategorie, ein Management Review und eine Verantwortlichkeit eingetragen werden. Auf der Übersichtsseite eines Datensatzes haben Sie die Möglichkeit, sich die wichtigsten Stammdaten im Steckbrief anzeigen zu lassen, um somit die wichtigsten Daten des Datensatzes betrachten zu können.

Steckbrief	
iris-ID	RSK_000007
Verknüpfte Risiken	Terroristische Akte
Erstellt am	07.02.2020
Management Review	Ausstehend
Verantwortlichkeit	Matthias Pröpster
Risikokategorien	Branchenspezifischer Sicherheitsstandard (B3S)
Themengebiet	ISMS
Letzte Bewertung am	07.02.2020 (Details) durch Matthias Pröpster
Risikoklasse (IST)	II
Schadenauswirkung (IST)	Signifikant
Eintrittswahrscheinlichkeit (IST)	Möglich

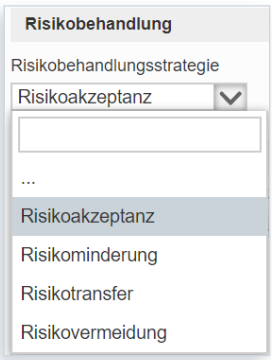
Risikobewertung und Risikobehandlung

Nach der Risikoerfassung in ibi systems iris kann eine erste IST-Bewertung des Risikos erfolgen.



Das Risiko wird in den Dimensionen Schadenauswirkung und Eintrittswahrscheinlichkeit bewertet und in einer konfigurierbaren Risikomatrix anschließend grafisch dargestellt. Die Dimensionen können in einer einfachen oder kategoriebasierten Bewertungsmethode bewertet werden. Durch die Möglichkeit, Risiken kategoriebasiert zu bewerten, kann beispielsweise die Anforderung des IT-Sicherheitskatalogs für die Energiewirtschaft umgesetzt werden. Der IT-Sicherheitskatalog fordert die Risikoeinschätzung bzw. Risikobewertung in mehreren Kategorien (z. B. Betroffener Bevölkerungsanteil oder Finanzielle Auswirkungen). Zusätzlich unterscheidet die Software zwischen dem qualitativen und quantitativen Ansatz. Neben der Bewertung kann der Benutzer eine Beschreibung eintragen, um die Bewertung zu dokumentieren

und zu erklären. Durch dieses Vorgehen unterstützt ibi systems iris, die Anforderungen aus der **ISO 27001 6.1.2 Informationssicherheitsrisikobeurteilung** und **8.2 Informationssicherheitsrisikobeurteilung** zu erfüllen und umzusetzen.



Im nächsten Schritt des Risikoprozesses wird eine Risikobehandlungsstrategie gewählt und eine oder mehrere risikominimierende Maßnahmen ausgewählt. Die Risikobehandlungsstrategien können Sie sich selbst in der Software konfigurieren. In den meisten Anwendungsfällen werden die bekannten Behandlungsstrategien Risikoreduktion, Risikotransfer, Risikoübernahme und Risikovermeidung genutzt. Bei den Risikobehandlungsstrategien können Sie wählen, ob eine SOLL-Bewertung des Risikos bei Auswahl der Behandlungsstrategie erforderlich ist oder nicht.

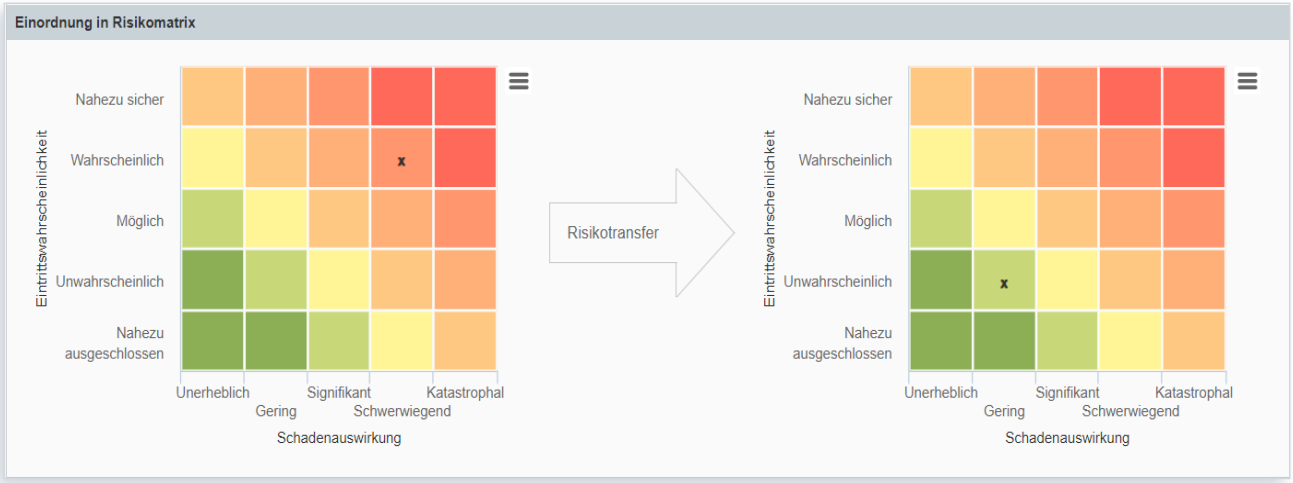
Die Maßnahme kann in ibi systems iris manuell hinzugefügt, aus einem Regelwerk (z. B. einem internen Maßnahmenkatalog) hergeleitet oder importiert werden. Zusätzlich können bereits in der Software bestehende Maßnahmen ausgewählt werden. Somit können die Anforderungen aus der **ISO 27001 6.1.3 Informationssicherheitsrisikobehandlung** und **8.3 Informationssicherheitsrisikobehandlung** innerhalb des Risikomanagementprozesses in ibi systems iris erfüllt werden.

Für eine Maßnahme können ein oder mehrere Empfänger eingetragen werden. Die Empfänger sind verantwortlich für die Umsetzung der Maßnahme. In der Listenansicht werden die Maßnahmen mit einem Fortschrittsbalken und u. a. dem Umsetzungsdatum angezeigt. Weitere Spalten können Sie sich jederzeit in der Listenansicht anzeigen lassen.

Anschließend kann in der Software ibi systems iris eine SOLL-Bewertung im Rahmen des Risiko-Prozesses vorgenommen werden. Identisch wie bei der IST-Bewertung werden bei der SOLL-Bewertung die Dimensionen Schadenauswirkung und Eintrittswahrscheinlichkeit bewertet. Im Anschluss kann das Vorgehen innerhalb des Risiko-Prozesses übersichtlich betrachtet werden. Es ist auf einen Blick ersichtlich, welche IST-Bewertung, Risikobehandlungsstrategie, Maßnahmen und SOLL-Bewertung für das Risiko definiert wurden.

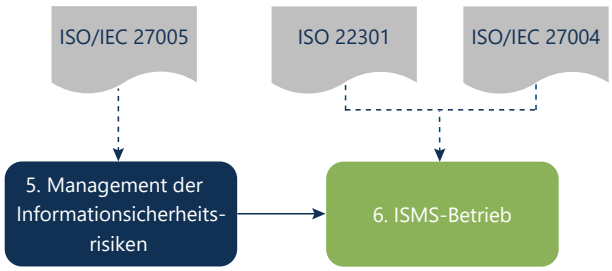
Ergebnisse:

- Erfassung, Bewertung und Behandlung der Risiken nach definiertem Risikoprozess
- Regelmäßige oder Ad-hoc-Reports über aktuelle Risikolage abrufbar



6. ISMS-Betrieb

Audit/Prüfungen



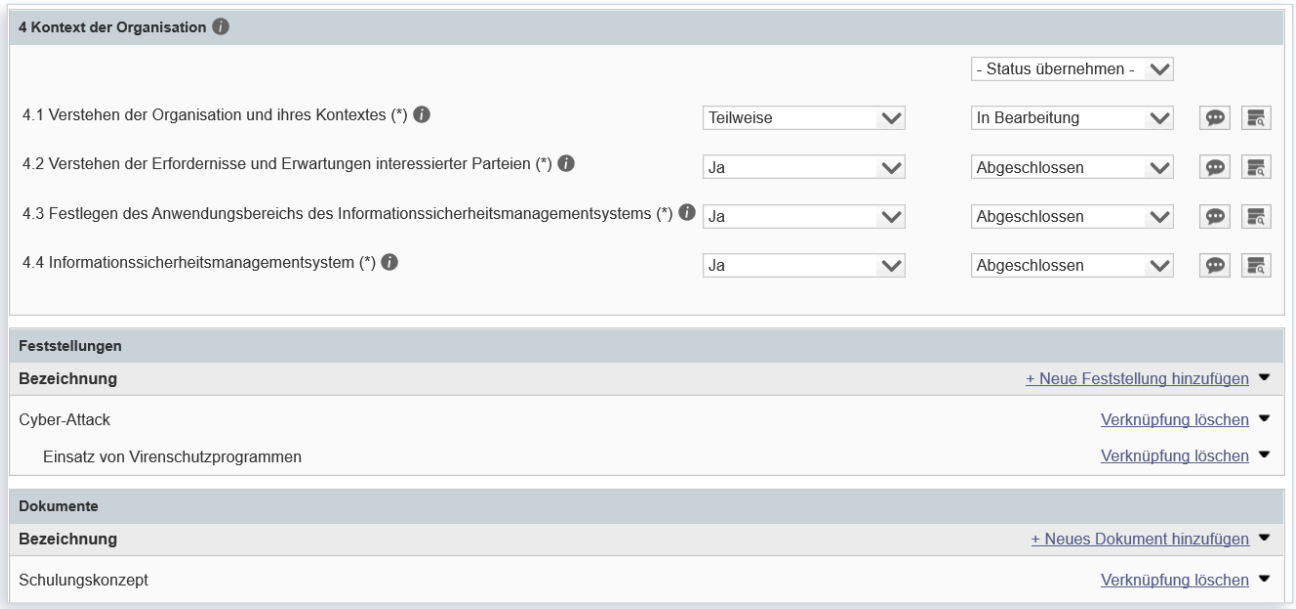
Eine detaillierte Prüfungsplanung und -durchführung sowie Reviews ermöglichen es, Feststellungen, wie Schwachstellen oder Verbesserungspotenziale zu erkennen. Die Feststellungen können wiederum Risiken hervorrufen, die im Sinne der Informationssicherheit berücksichtigt werden müssen.

Die Software ibi systems iris ist vielfältig nutzbar. Beispielsweise können interne/externe Audits, Checklisten oder Fragebögen als Prüfung abgebildet werden. Die **ISO 27001** fordert in **Kapitel 9 (9.2 Internes Audit)**, interne Audits in geplanten Abständen durchzuführen. Durch Prüfungen und in deren Rahmen identifizierte Feststellungen sowie definierte Maßnahmen kann die Anforderung der **ISO 27001** im **Kapitel 10 (10.1. Nichtkonformität und Korrekturmaßnahmen** und **10.2 Fortlaufende Verbesserung)** softwaregestützt durchgeführt werden.

Mithilfe der Prüfvorlagen erstellen Sie Templates für Audits und Prüfungen, welche anschließend benutzerfreundlich und schnell durch einen Klick zu einer durchführbaren Prüfung erstellt werden und in der Zukunft wiederverwendet werden können. So ist es ein Leichtes, beispielsweise die **Controls** des **Anhang A** der ISO 27001 (regelmäßig) abzufragen oder zu auditieren. Die Anforderung **A.18.1. Bestimmung der anwendbaren Gesetzgebung und der vertraglichen Anforderungen** aus dem **Anhang A der ISO 27001** können Sie beispielsweise durch die Funktionsbereiche Regelwerke und Prüfungen abbilden. Einerseits können Sie die benötigten Gesetze und Richtlinien als Kompendium in der Software darstellen und andererseits über den Funktionsbereich Prüfungen die jeweiligen Anforderungen aus den Gesetzen prüfen.

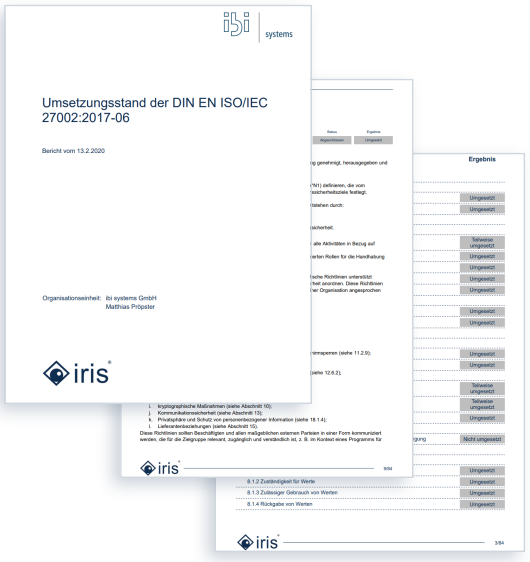
Prüfungsplanung: Mit der umfassenden Prüfungsplanung ist es möglich, für eine Prüfung oder für jeden einzelnen Prüfblock einen oder mehrere Prüfer und Reviewer für die ausgewählte Prüfung zu definieren. Zusätzlich können optional ein Prüfungszeitraum und Angaben zum Prüfungsabschluss festgelegt werden.

Prüfungsdurchführung: Der Prüfungswizard unterstützt den Prüfer bei der Durchführung der Prüfung durch eine kompakte Ansicht der zugewiesenen Prüfblöcke. Für jede Kontrollfrage kann das Kontrollergebnis, der Status und ggf. ein Kommentar gesetzt werden. Zusätzlich ist es möglich, Dokumente anzuhängen und direkt aus einer Prüfung Feststellungen – und daraus entstehende Maßnahmen – zu identifizieren und zu erfassen.



Nach Durchführung der Prüfung kann das System einen Report generieren, welcher die Prüfungsergebnisse, Kommentare und Feststellungen ausgibt.

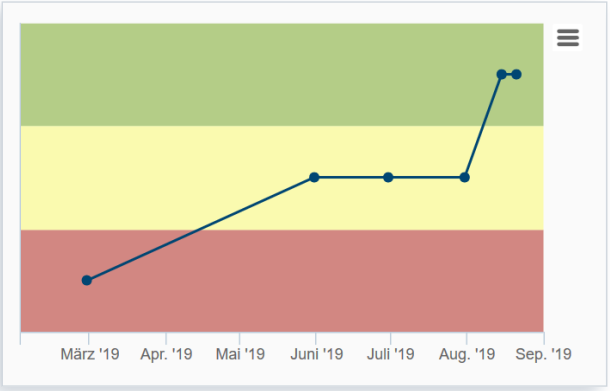
Durch unsere Reporting-Engine können individuelle Berichte erstellt, bearbeitet und erzeugt werden. Für die Berichte stehen Ihnen alle verfügbaren Datenfelder aus ibi systems iris zur Verfügung, welche per Baukastenprinzip in die Berichte eingefügt werden können. Um eine Managementbewertung nach **ISO 27001 Kapitel 9 (9.3 Managementbewertung)** durchführen zu können, können Sie in ibi systems iris eigene Managementberichte erstellen, um dem Management die gewünschten bzw. geforderten Informationen zur Verfügung zu stellen.



Indikatoren/Kennzahlen

Als Indikatoren können beispielsweise Key Performance Indicators (KPIs) angelegt und verwaltet werden. Die erfassten Messwerte des Indikators können in der Listenansicht eingesehen werden. Je nach konfigurierten Schwellwerten wird der aktuelle Messwert als grün, gelb oder rot angezeigt. Indikatoren können für sämtliche messbare Bereiche verwendet werden: So lassen sich beispielsweise globale ISMS-Ziele verfolgen, Maßnahmen detailliert tracken oder Risiken permanent überwachen. Somit kann der Funktionsbereich Indikatoren für das **Kapitel 9 (9.1 Überwachung, Messung, Analyse und Bewertung**) aus der **ISO 27001** genutzt werden.

In ibi systems iris ist es ebenfalls möglich, ein Risiko mit einem Indikator zu verknüpfen, um somit das Risiko stets überwachen zu können und infolge dessen Aktionen durchzuführen. Des Weiteren besteht die Möglichkeit, den zeitlichen Verlauf des Indikators zu verfolgen.



Die **ISO 27001** fordert in **Kapitel 7 (7.2 Kompetenz und 7.3 Bewusstsein)** u. a., dass Mitarbeiter die Kompetenz und das Bewusstsein für die Informationssicherheitspolitik im Unternehmen besitzen. Dies kann in ibi systems iris über einen Indikator (z. B. Schulungsquote der Mitarbeiter) getrackt werden und anschließend kann bei Notwendigkeit durch Maßnahmen gegengesteuert werden.

Sicherheitsvorfälle

ibi systems iris unterstützt Sie bei der Erfassung und Dokumentation von Sicherheitsvorfällen bzw. Incidents, um somit die **Anforderung A. 16 Handhabung von Informationssicherheitsvorfällen aus dem Anhang A der ISO 27001** softwaregestützt umzusetzen.

Bei der Erfassung eines Sicherheitsvorfalls haben Sie u. a. die Möglichkeit, eine Bezeichnung, das Vorfalldatum oder eine Verantwortlichkeit zu definieren. Des Weiteren ist es möglich, weitere Datensätze (z. B. Anfragen, Feststellungen oder verwandte Vorfälle) zu verknüpfen. Abschließend können Sie die Schadenshöhe, einen Status und einen Kommentar zum Vorfall dokumentieren.

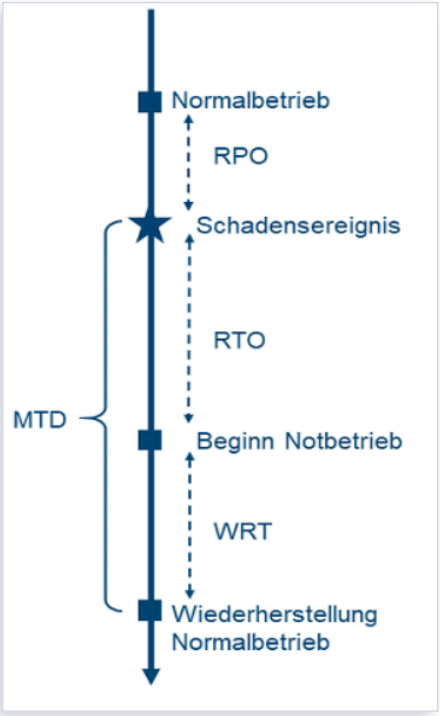
Zusätzlich kann in der Software ein Sicherheitsvorfall mit einem Risiko verknüpft werden. Dies hat zum Vorteil, dass eingetretene Sicherheitsvorfälle bei der Risikobewertung mitberücksichtigt werden können.

Nach erfolgter Verknüpfung von einem oder mehrerer Sicherheitsvorfälle zu einem Risiko be-

steht die Option, diese historischen, eingetretenen Vorfälle für die Risikobewertung zu übernehmen. Dabei wird die durchschnittliche Eintrittswahrscheinlichkeit des Risikos anhand der Anzahl an Vorfällen in einem bestimmten Zeitfenster (z. B. die letzten drei Jahre) berechnet. Ebenso wird die Schadenauswirkung anhand des betrachteten Zeitrahmens und unter Berücksichtigung der summierten Bruttoschadenshöhe für das ausgewählte Risiko berechnet.

Business Continuity Management/Business Continuity Impact Analyse

Wie im Kapitel 1.4.4 und 1.4.5 beschrieben, können Sie für Ihre Prozesse und Assets eine Business Impact Analyse und Business Continuity Management definieren. Durch die Funktionalität einer Notfallsimulation haben Sie in ibi systems iris die Möglichkeit, eine Simulation inklusive Auswählbarkeit verschiedener Assets/Prozesse durchzuführen. Hierbei wird die maximal tolerierbare Ausfallzeit (MTD) aus der Business Impact Analyse der Wiederanlaufzeit (RTO) aus dem Business Continuity Management gegenübergestellt. Dadurch erhalten Sie einen schnellen Überblick über kritische Prozesse und Auswirkungen in Notfallsituationen. Die Notfallsimulation können Sie anschließend als Notfallszenario oder Notfallereignis abspeichern.



Ergebnisse:

- Aktuelle Prüfergebnisse, Kennzahlen und Informationen zu Vorfällen etc.
- Reportfunktion für Prüfungen bzw. Audits

Fazit

Mit ibi systems iris betreiben Sie Ihr Informationssicherheitsmanagementsystem über die ganze Organisation hinweg und bilden sowohl die Organisationsstruktur, Assets, Prozesse als auch interne und externe Regelwerke ab. So können etablierte Standards wie die ISO/IEC 27001 genutzt und interne Dokumente referenziert werden. Der von Ihnen im Unternehmen betriebene Risikoprozess ist ebenso in ibi systems iris abbildbar.

Durch die vielfältigen Import- und Exportmöglichkeiten in bzw. aus ibi systems iris heraus können Sie problemlos mit vorhandenen Daten (beispielsweise Assets, Risiken etc.) in der Software weiterarbeiten und können diese, falls gewünscht, im Nachgang ohne viel Aufwand exportieren.

Mit ibi systems iris finden Sie alle Daten mit Bezug zur Informationssicherheit an einer zentralen Stelle.

Abgerundet wird das Angebot der Software ibi systems iris mit der Option, für Anwender der Software eine Zertifikatsschulung zu absolvieren.

„Durch unser interdisziplinäres Know-how unterstützen wir unsere Kunden in allen Projektphasen – beginnend bei fachlichen Fragestellungen im ISMS- und GRC-Umfeld über die Auswahl und Konzeption einer auf die individuellen Bedürfnisse zugeschnittenen Systemumgebung bis hin zur erfolgreichen Pilotierung und Einführung der Software ibi systems iris. Die persönliche Betreuung unserer Kunden durch unsere erfahrenen Fachexperten stellt für uns auch nach der Pilotierung und Einführung eine Selbstverständlichkeit dar. Die daraus entstehende enge Partnerschaft ermöglicht es uns, gezielt auf Kundenwünsche einzugehen und die Weiterentwicklung unserer Software am Bedarf unserer Partner auszurichten.“, ergänzt Dr. Christian Ritter, Senior Product Manager der ibi systems GmbH.