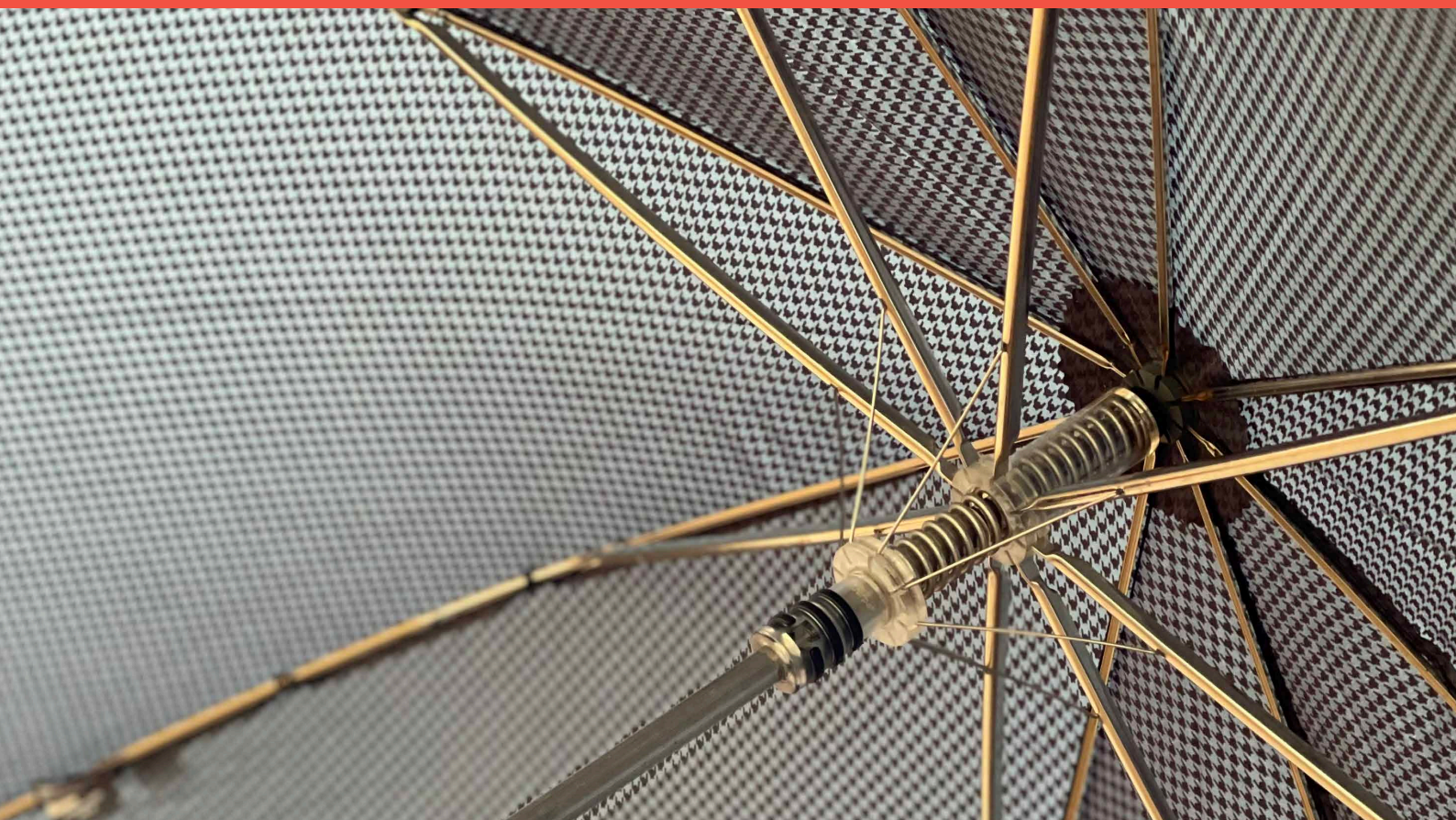
Rödl & Partner

INTEGRIERTES MANAGEMENT VON INFORMATIONS-SICHERHEIT UND DATENSCHUTZ

Rödl & Partner entwickelt ISDMS



Unsere Welt wird digitaler, komplexer und technologiegetriebener. Digitale Systeme und intelligente Services oder Apps sind fester Bestandteil einer dynamischen und agilen Gesellschaft im 21. Jahrhundert. Die Entwicklung von künstlichen Intelligenzen, Cloud- und Smart-Home-Lösungen, Videotelefonie sowie Homeoffice- und Schooling stellen nur einige Beispiele dar, deren Einsatz in einer modernen Gesellschaft nicht mehr wegzudenken ist. Vor allem in der kommunalen Datenverwaltung zeichnet sich – sicherlich spätestens geprägt durch die Corona-Pandemie – unlängst ab, dass die Verwaltungsprozesse digital und smart werden müssen. Gleichzeitig erhöhen sich die Abhängigkeit und die Anfälligkeit für zunehmende Sicherheitsbedrohungen. Manipulierte, missbräuchlich verwendete, zerstörte oder gestohlene Daten können für verantwortliche Stellen ernsthafte rechtliche und finanzielle Konsequenzen bedeuten.

Es ist höchste Zeit, dass Informationssicherheit und Datenschutz ernst genommen werden!

In diesem Artikel möchten wir Ihnen ein Konzept vorstellen, in welchem wir beide Disziplinen zu einem integralen Managementsystem verbunden haben. Im Auftrag für einen Mandanten aus der öffentlichen Verwaltung (>600.000 Einwohner) haben wir ein sogenanntes **Informationssicherheits- und Datenschutzmanagementsystem ISDMS** entwickelt.

Rödl & Partner berät und betreut viele öffentliche Verwaltungen im Zuge ihrer Digitalisierungsstrategien und bei der Einführung von Compliance-, Informationssicherheits- oder Datenschutzmanagement-Systemen. Die Organisationen sind meist dezentral in ihren Organisationseinheiten bzw. Ämtern aufgestellt. Zuständigkeiten und klare Dokumentationen können mitunter massiv von den eigentlich geforderten Standards abweichen. Dabei muss das oberste Ziel der kommunalen Datenverwaltung ein adäquates und nachhaltiges Schutzniveau sein. Vor allem gegenüber den Bürgerinnen und Bürgern, Beschäftigten und Vertragspartnern muss der Verantwortliche als professionelle und vertrauenswürdige Verwaltungsbehörde hinsichtlich der Verarbeitung von sensiblen und personenbezogenen Daten auftreten.

Die Grundlagen für ein ISDMS

Zunächst war es das Ziel, dass der Mandant versteht, nach welcher Logik wir ein zukünftiges ISDMS aufbauen wollen. Da durch das BSI, die ISO/IEC 27001 und den PH. 9.860.1 des IDW bereits Regelwerke existieren, die jeweils thematisch die Informationssicherheit bzw. den Datenschutz würdigen, war es für uns eine logische Konsequenz, dass wir in einem zukünftigen ISDMS auf die bereits vorhandenen Regelwerke zurückgreifen werden. Wo die ISO/IEC 27001 sich „exklusiv" um die Informationssicherheit kümmert und der IDW PH 9.860.1 „exklusiv" den Datenschutz thematisiert, sollte ein späteres ISDMS eben genau diese Disziplinen als anwendbares Regelwerk kombiniert integrieren. Eine wesentliche Grundlage beim Aufbau eines ISDMS ist das Verständnis der eingebundenen Normen und Standards:

– ISO/IEC 27001 für das Managementsystem
– IDW PH.9.860.1 für den Datenschutz
  sowie die gemeinsame Basis für die Sicherheitskonzeption,
– der BSI IT-Grundschutz.

Den Zusammenhang zwischen den Sicherheitsanforderungen der Norm ISO/IEC 27001 und dem IT-Grundschutz einerseits und den weiterführenden Datenschutzanforderungen andererseits stellt die nebenstehende Grafik dar.

A.5	Informationssicherheits-Richtlinien
A.6	Organisation der Informationssicherheit
A.7	Personalsicherheit
A.8	Asset Management
A.9	Zugriffskontrolle
A.10	Kryptografie
A.11	Physische & Umgebungssicherheit
A.12	Betriebssicherheit
A.13	Kommunikationssicherheit
A.14	Systemerwerb, Entwicklung & Wartung
A.15	Lieferantenbeziehungen
A.16	Informationssicherheits-störfallmanagement
A.17	Informationssicherheitsaspekte des Geschäftskontinuitätsmanagements
A.18	Compliance / Konformität

+

DATENSCHUTZ (EU-DSGVO)

- Verarbeitungsverzeichnis
- Archivierungs- & Löschkonzept
- Verpflichtung Mitarbeiter & Auftragsverarbeiter
- Datenschutzkonformität der Website und Kollaborations-services
- Prozess & Betroffenenrechte
- Prozess Datenpannen
- Enabling & Awareness

= *ISDMS*

Methodische Herangehensweise im Projekt

Um überhaupt an die konzeptionelle Arbeit gehen zu können, mussten wir das Projekt in drei Phasen unterteilen. Unsere methodische Herangehensweise begann mit einer Bestandsaufnahme, in welcher wir einen Überblick über die Bedarfe und Rahmenbedingungen bekamen. Auf Grundlage dessen konnten wir eine Bewertung des Ist-Zustandes und eine Priorisierung der Bedarfe vornehmen. Erst jetzt war es überhaupt möglich, auf die individuellen Gegebenheiten zu reagieren und ein entsprechendes ISDMS aufzubauen.

PHASE 1
ANALYSE DER BEDARFE UND RAHMENBEDINGUNGEN

Abbildung 1: Darstellung des Vorgehens zur Ermittlung des Ist-Zustandes

PHASE 2
BEWERTUNG UND PRIORISIERUNG DER BEDARFE

Beim Aufbau der Gruppierung muss zunächst grundlegend zwischen zwei Bereichen beim Aufbau eines ISDMS unterschieden werden:

- Bedarfe hinsichtlich des Managementprozesses (dem Regelkreislauf) und
- Bedarfe hinsichtlich der Umsetzung konkreter technischer oder organisatorischer Maßnahmen aus der Arbeit im Regelkreislauf (erforderliche neue Schutzmaßnahmen).

PHASE 3
AUFBAU DES INTEGRIERTEN INFORMATIONSSICHERHEITS- UND DATENSCHUTZMANAGEMENTSYSTEMS (ISDMS)

Ein integriertes Managementsystem für Informationssicherheit und Datenschutz (ISDMS) ist ein umfassendes und standardbasierendes Managementsystem mit definierten Richtlinien, Regeln und Prozessen zur Planung, Durchführung, Steuerung und fortlaufenden Optimierung der Informationssicherheit und des Datenschutzes. In unserem Projekt haben wir empfohlen, dass der Mandant ein Informationssicherheits- und Datenschutzmanagementsystem nach ISO 27001 auf Basis des BSI-IT-Grundschutzes umsetzen sollte. Zur Erreichung dessen ist zunächst ein Verständnis darüber erforderlich, dass die originäre IT-Grundschutz-Vorgehensweise (BSI-Standard 200-2) um ein Informationssicherheitsmanagementsystem ISMS (BSI-Standard 200-1) erweitert wird. Das Informationssicherheitsmanagementsystem wiederum setzt eine Methodik zur regelmäßigen Risikoprüfung (BSI-Standard 200-3) voraus.

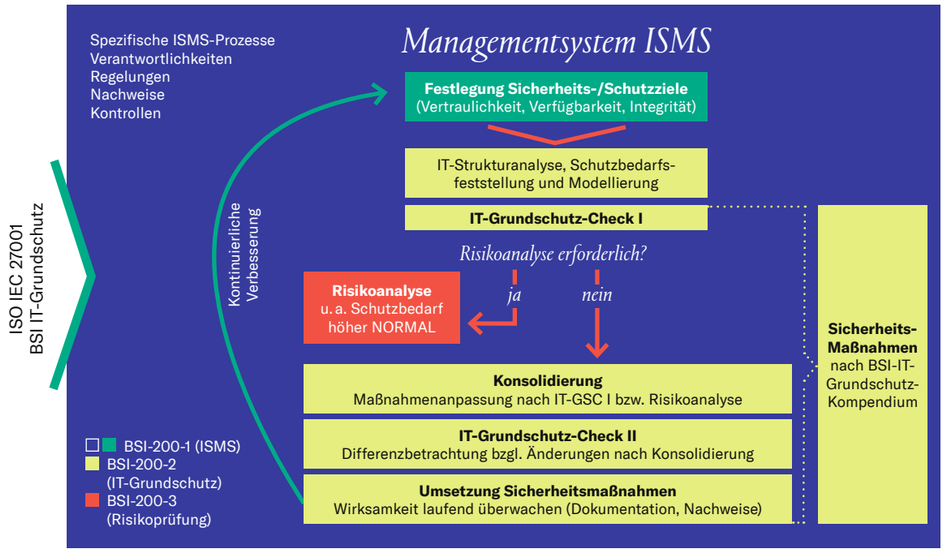


Abbildung 2: Darstellung der BSI-Standards 200-1 bis 200-3

Der IT-Grundschutz des BSI ist sehr flexibel, da er modular aufgebaut ist. Im Zusammenhang mit dem IT-Grundschutz-Kompendium, welches in der Regel einmal im Jahr vom BSI aktualisiert wird, stellt es für typische Prozesse, Anwendungen und IT-Komponenten entsprechende IT-Grundschutz-Bausteine zur Verfügung. Zu jedem Baustein werden nicht nur Sicherheitsmaßnahmen empfohlen, sondern auch die wichtigsten Gefährdungen beschrieben, vor denen sich der Mandant schützen sollte.

Aufbau des spezifischen Regelwerkes in einem ISDMS

Folgende schematische Abbildung zeigt auf, inwieweit die gesetzlichen Anforderungen der DSGVO und der Informationssicherheitsvorgaben wirken:

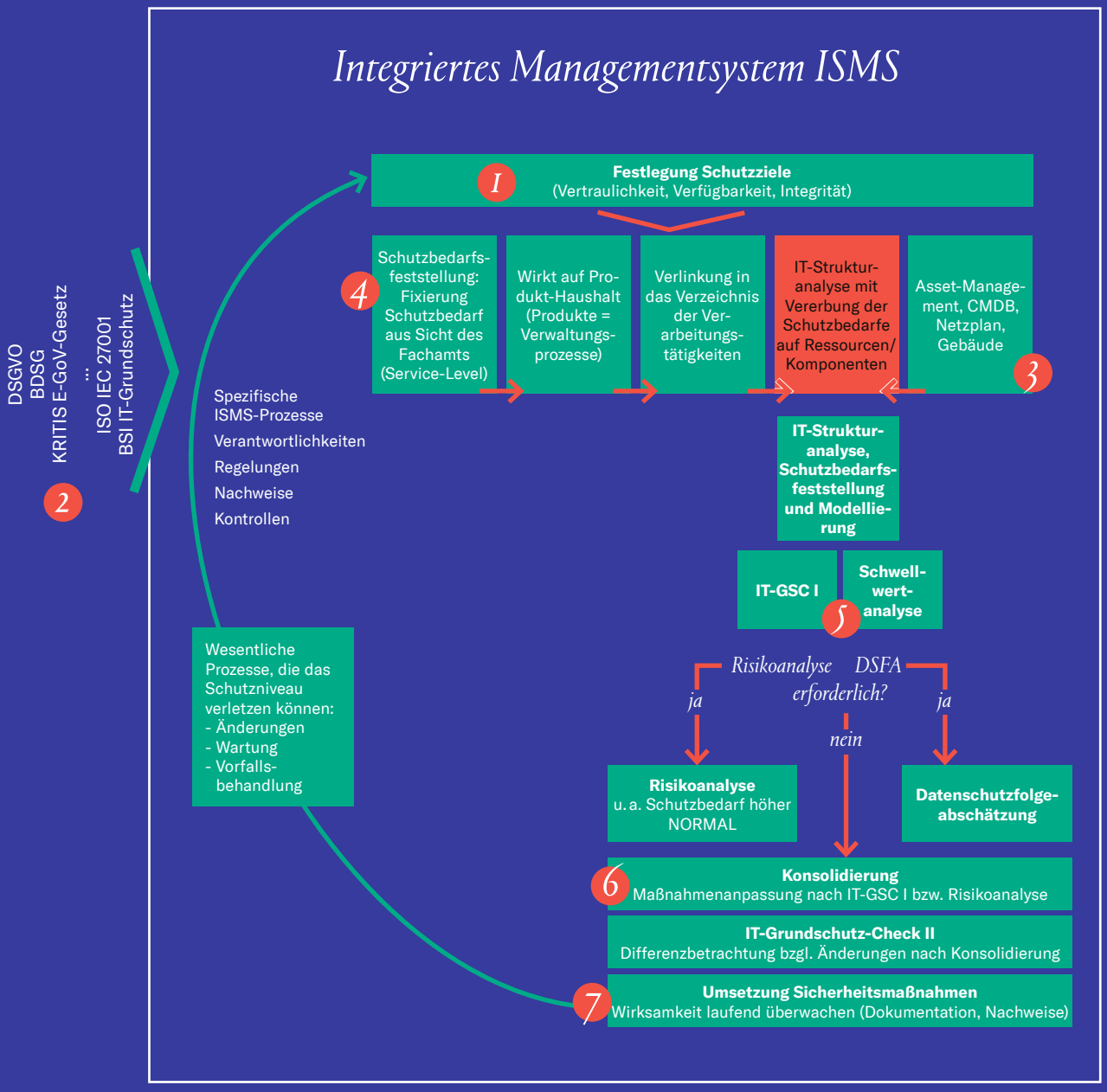


Abbildung 3: Integriertes Managementsystem ISDMS

1 Der Mandant legt, orientiert an den gesetzlichen Standards, die Datenschutz- und Informationssicherheitsstrategie fest. Im Idealfall leiten sich diese aus der Digitalisierungsstrategie ab.

2 Die Anforderungen der bekannten Frameworks (ISO/IEC 27001 Informationssicherheit & IDW PH 9.860.1 Datenschutz werden danebengelegt. An den Stellen, an denen die ISO27001 keine konkreten Anforderungen des IDW PH 9.860.1 fordert, wird entsprechend der Datenschutz-Anforderungen das Element (z. B. Datenschutzfolgeabschätzung) ergänzt.

3 Ein Sicherheitskonzept kann nur auf verlässlichen Daten und Informationen aufgebaut werden. Grundlage hierfür sind ein funktionierendes Asset-Management, also die Erfassung von entsprechenden Netzplänen, einer Configuration-Management-Database (CMDB) sowie die Kenntnis aller Gebäude (Eigentum, in Miete oder anderweitige Mitnutzung). Um erkennen zu können, welchen Schutz diese Komponenten liefern müssen, ist eine Verlinkung zu den Prozessen und Daten notwendig.

Das heißt in 3 findet eine Integration des Framework Datenschutz mit dem Framework Informationssicherheit statt. Das Asset-Management beider Frameworks kann zusammengefasst werden und muss als „Single Point of Truth“ betrachtet werden.

4 Die Datenschutzanforderungen sehen das Führen eines Verzeichnisses der Verarbeitungstätigkeiten vor. In diesem Verzeichnis werden alle Prozesse geführt, welche personenbezogene Daten verarbeiten. Die Informationssicherheit kennt keine „Prozesse von Verarbeitungen personenbezogener Daten“, sondern führt stattdessen ein Verzeichnis auf Ebene von Informationen (allen Informationen, nicht nur personenbezogenen) innerhalb von Prozessen und hat zum Ziel, herauszufinden, welche IT-Systeme dafür notwendig sind und welches infrastrukturelle Umfeld vorliegt. Dieses Verzeichnis ist unter dem Begriff „Asset-Register“ bekannt.

Das Verzeichnis kann eigenständig geführt werden. Oder aber es wird mit vorhandenen Listen / Verzeichnissen so kombiniert, dass eine Doppelarbeit vermieden wird. Beispiel für vorhandene Listen ist eine Übersicht aller Prozesse, welche für die Digitalisierung vorgesehen sind. Eine solche Liste wird seitens des CDO oder des verantwortlichen Amtes / Stabes für Digitalisierung vorbereitet. Eine weitere Quelle könnte der Produktkatalog sein.

Um Datenschutz und Informationssicherheit zu integrieren, wird zunächst eine gedankliche Verlinkung zwischen dem Verzeichnis der Verarbeitungstätigkeiten und dem schon geführten Produktkatalog (Produkthaushalt) hergestellt.

Der Gedanke speist sich aus der Tatsache, dass alle Produkte auch Verarbeitungsprozesse beinhalten und dass die „Vorarbeit“ aus dem Produktkatalog der Haushaltssystematik ideal für das Führen des Verzeichnisses verwendet werden kann. Ein Beispiel aus dem Produktbereich des Gesundheitsamtes soll diesen Zusammenhang verdeutlichen:

Abbildung 4: Beispiel Produktbeschreibung

Die Nutzung des Produktkatalogs hat viele Vorteile: Die Verantwortung, die gesetzliche Grundlage sowie eine Beschreibung sind definiert. Zudem ist der Katalog vorhanden und aufgrund der jährlichen Haushaltsplanung auch weitgehend aktuell und allen Beteiligten bekannt. Es fehlen lediglich die Verknüpfungen zu den Daten- und Betroffenenkategorien sowie die verwendeten Systeme.

Auf dieser Basis formulieren die Verantwortlichen für die Produkte den jeweiligen Schutzbedarf der Daten und Informationen und beschreiben die Verwaltungsprozesse zu den jeweiligen Produkten. Sodann kann im nächsten Schritt die Strukturanalyse mit verlässlichen Daten vorgenommen werden.

Bei der Schutzbedarfsfeststellung ist demnach zu fragen, welcher Schaden entstehen kann, wenn für einen Prozess bzw. Daten die Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit verletzt werden. Dies wäre der Fall, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der Vertraulichkeit), die Korrektheit der Informationen und der Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der Integrität), autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der Verfügbarkeit).

5 Konkret heißt das, dass in einem CHECK I zunächst hinterfragt wird, ob ein „besonderer Sachverhalt“ vorliegt. Dies regelt der Datenschutz über eine sogenannte Schwellwertanalyse, nämlich mit der Fragestellung, ob z. B. besonders schützenswerte personenbezogene Daten (Gesundheitsdaten etc.) verarbeitet werden. In unserem obigen Beispiel dürfte dies gegeben sein. Der BSI-IT-Grundschutz fragt auf dieser Ebene, ob in Bezug auf die Daten und Prozesse ein erhöhter Schutzbedarf gegeben ist und dies wird nur beantwortet werden können, wenn die aus 4 notwendigen Angaben vorliegen.

So trennt sich die Herangehensweise in Bezug auf Risikoanalyse in Richtung datenschutz-rechtlicher sogenannter Datenschutzfolgeabschätzung und in Richtung BSI-IT-Grundschutz in Analyse bei erhöhtem Schutzbedarf. Diese beiden Analysen lassen sich in einer integrierten Analyse effizient zusammenfassen.

Bei allen normalen Schutzbedarfen erfolgt keine tiefergehende Analyse.

6 Es erfolgt die Modellierung von Maßnahmen anhand des aufgedeckten Schutzbedarfes aus Schritt 5. Das BSI-Kompendium setzt Maßnahmen um, die innerhalb der Frameworks Datenschutz und Informationssicherheit gefordert sind. Es findet somit die Umsetzung des IT-Grundschutzes (200-2) statt.

Sofern aus der Schutzbedarfsfeststellung in Schritt 4 hohe Risiken im Sinne des Datenschutzes oder im Sinne der Informationssicherheit festgestellt werden können (nämlich immer dann, wenn Verarbeitungen oder Prozesse oder relevante Systeme hoch schutzwürdig sind), muss eine erweiterte Risikokontrolle durchgeführt werden. Auch an dieser Stelle verlangen die Frameworks Datenschutz und Informationssicherheit individuelles Vorgehen.

Eine Integration der DSFA und Risikoanalyse ist die logische Erweiterung des zuvor angefertigten Asset-Verzeichnisses. Als Abschluss der Risikoanalyse sind die zusätzlichen Maßnahmen in das vorhandene Sicherheitskonzept zu integrieren (= Konsolidierung des Sicherheitskonzepts) und darauf aufbauend ist der Sicherheitsprozess fortzusetzen.

7 Sowohl eine DSFA als auch eine Risikoanalyse erfordern technisch organisatorische Maßnahmen zur Absicherung bzw. Verringerung des betrachteten Risikos. Die Maßnahmen müssen wirksam sein und nachweisbar kontrolliert werden.

Fazit: Beim Mandanten sind perspektivisch alle Anforderungen erfüllt. Es wurde mit Hilfe einer integrierten Risikoanalyse festgestellt, dass auch solche Prozesse und Daten mit ihren Komponenten angemessen geschützt sind, die einen besonderen Schutzbedarf haben müssen.

Es gilt nun, das erreichte Niveau zu erhalten und zu verbessern. In der Regel führen IT-Grundschutz-Checks und zusätzliche Risikoanalysen aber zu einem anderen Ergebnis: Irgendwelche Defizite gibt es immer, seien es Lücken in den vorhandenen organisatorischen Regelungen oder mangelnde Kontrolle der geltenden Regeln. Bei der Umsetzungsplanung geht es darum, diese Lücken wirksam und effizient zu schließen.

Schließlich kann das ISDMS in seinen Wirkbetrieb genommen werden.

ISDMS Regelkreislauf im Betrieb

Nachdem Maßnahmen zur Umsetzung der Anforderungen der Informationssicherheit und des Datenschutzes durch das integrierte Managementsystem ergriffen worden sind, muss den Verantwortlichen klar sein, dass das ISDMS-Management einer kontinuierlichen Kontrolle bedarf. Der Regelkreislauf bzw. PDCA-Zyklus (Plan-Do-Check-Act) stellen sicher, dass die eingeführten ISDMS-Prozesse regelmäßig kontrolliert, bewertet und kontinuierlich verbessert werden. 8 Es gilt als angemessen, wenn ein internes Kontrollsystem (analog bzw. ein Auszug aus den Controls des Anhang A) aufgebaut und regelmäßig berichtet wird.

9 Dieses Kapitel entwickelt einen Überblick über die Nachvollziehbarkeit, dass fortlaufend Änderungen unterliegt. Und Änderungen können im schlimmsten Fall das schon erreichte Schutzniveau gefährden. Erfahrungen haben gezeigt, dass drei Prozesse wesentlich sind und hier eine Einbettung der notwendigen Anforderungen bzw. Kontrollen wichtig sind. Vor allem die folgenden Prozesse sind betroffen:

- Änderungsprozess: Dazu zählt jede Änderung in Bezug auf Organisation, Personal und Technik. Auch Neuanschaffungen sind hierunter zu verstehen.
- Wartungsprozess: Eine fehlerbehaftete Wartung von Komponenten kann immer das Sicherheitsniveau verletzen.
- Vorfallhandhabung: Wird im Support eine Notlösung installiert, kann diese Sicherheitsverletzungen nach sich ziehen. Besonders ist es dann bedeutend, wenn die Notlösung nicht mehr zurückgeführt wird. Viele gleichgeartete Vorfälle können in Summe eskalieren und einen echten Notfall auslösen.

In diesen Prozessen muss geklärt sein, ob – begonnen mit der Strukturanalyse – unterjährig eine erneute Prüfung des bestehenden Sicherheitskonzeptes erfolgen muss.

Der regelmäßige Durchlauf der Anwendung des Regelkreislaufs (dabei spielt zunächst keine Rolle, ob unterjährig aufgrund der drei relevanten Prozesse – Änderung, Wartung, Vorfall – oder im Regelturnus auf jährlicher Kontrollbasis) beginnt immer mit einer erneuten Betrachtung der Strukturanalyse.

Zur Durchführung der Strukturanalyse sind ein aktuell geführter Netzplan sowie die Asset-Liste und das Verarbeitungsverzeichnis der Verarbeitungstätigkeiten zwingend vorauszusetzen (4).

Der aktuelle Netzplan sowie die aktuelle Asset-Liste (inkl. Anwendungen, IT-Systeme, IT-Infrastruktur und Räumlichkeiten bzw. Gebäude) wird seitens der IuK laufend zur Verfügung gestellt. Das dazugehörige Verzeichnis der Verarbeitungstätigkeiten wird durch die Fachämter über den Datenschutz bereitgestellt.

Integration des Datenschutzes im Betrieb

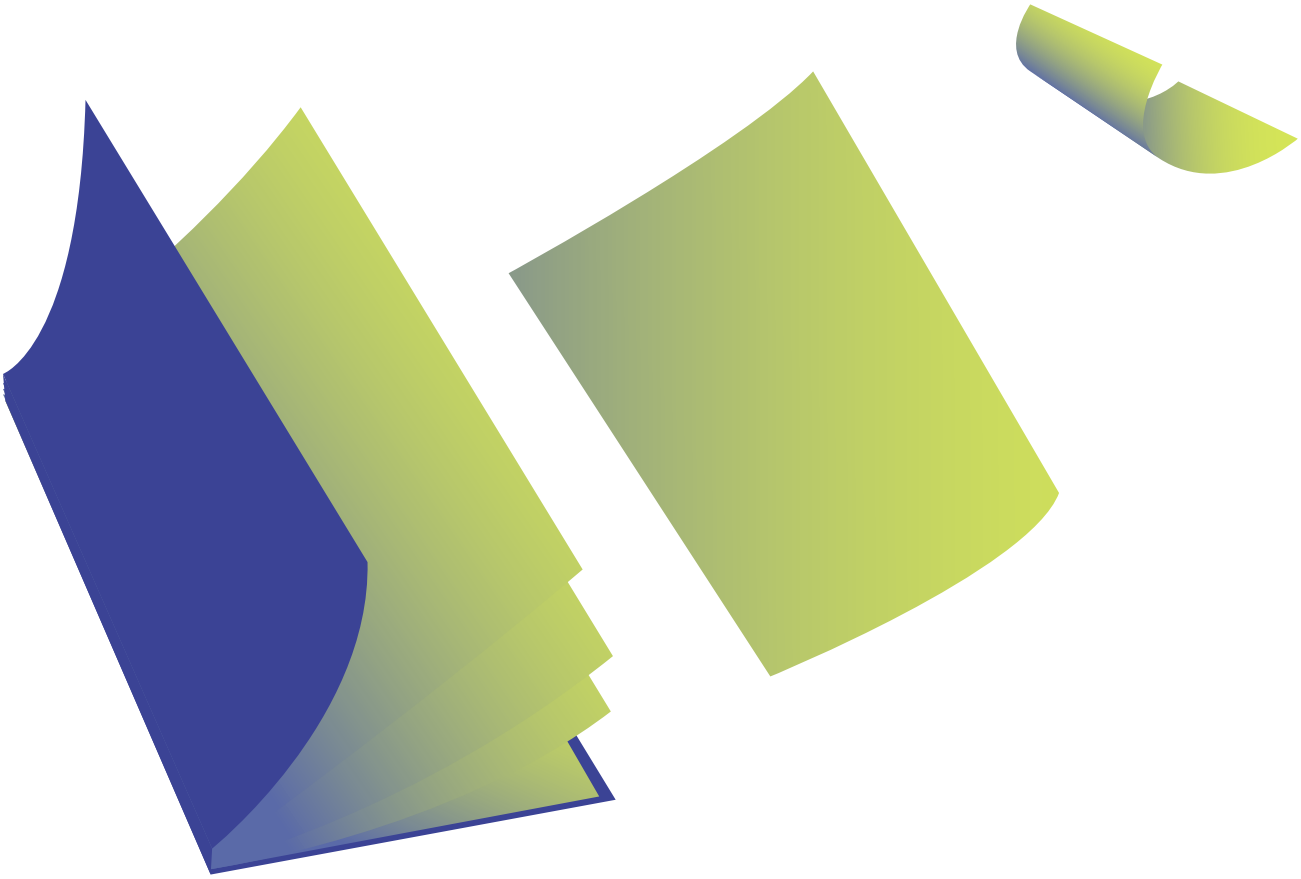
Wie bereits dargestellt, integriert das BSI-IT-Grundschutz-Vorgehen nicht automatisch alle Anforderungen des Datenschutzes. Folgend die Anforderungen der Datenschutzregularien, die in das ISDMS bzw. das BSI-IT-Grundschutz-Vorgehen integriert werden:

Dazu gehören folgende Elemente 5, 6 und 7:

- Sicherheitskonzept Artikel 32 der DSGVO
- Schwellwertanalysen
- Datenschutzfolgeabschätzung
- Grob- und Feinkonzepte personenbezogener Daten
- Technisch organisatorische Maßnahmen

Wie bekannt, enthält der Datenschutz exklusive Anforderungen, welche durch das BSI-IT-Grundschutz-Vorgehen nicht abgedeckt werden. In rot markiert wurden also jene Datenschutz-Prozesse, welche eben noch nicht in den Regelkreis aufgenommen wurden. Dazu gehören folgende Elemente 4 und 8:

- Verarbeitungsverzeichnis
- Archivierungs- und Löschkonzept
- Auftragsdatenverarbeitungsverträge
- Datenschutzerklärungen auf Website und sonstige Kollaborationsinstrumente (Teams, One-Drive etc.)
- Prozess „Sicherstellung der Betroffenenrechte“
- Prozess „Datenschutzverletzung“



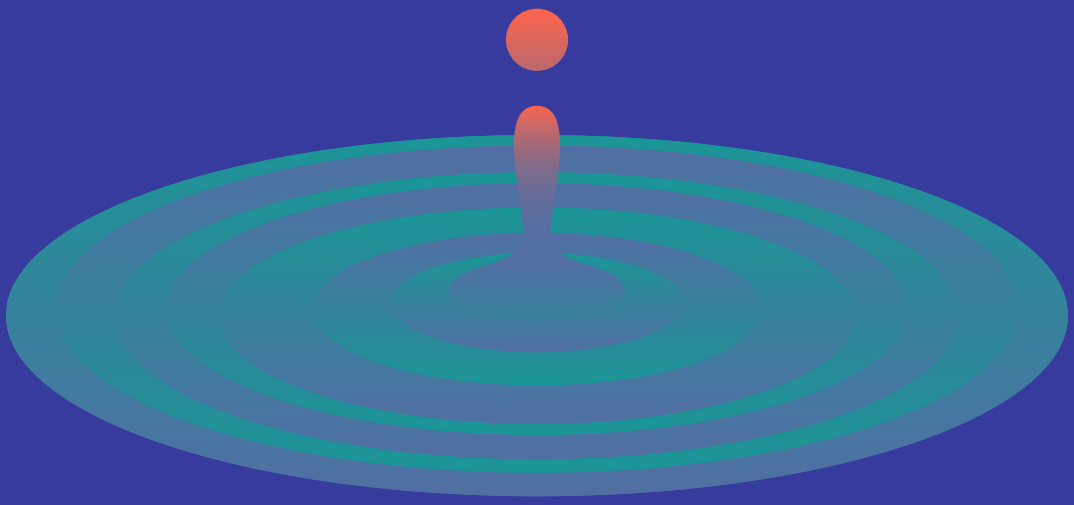
Anpassung der Dokumentation und Organisationsstruktur

Es müssen zum Aufbau und zur Aufrechterhaltung des Schutzniveau-Öko-Systems unter Anwendung des ISDMS Strukturen geschaffen werden, welche Verantwortungen und Aufgabenbereiche klar regeln und abgegrenzen. Entscheidend wird es sein, vorhandene Strukturen (Organisationseinheiten, einzelne Stellen und Verwaltungsprozesse) so aufzugreifen und anzupassen, dass eine Umsetzung des integrierten ISDMS erfolgreich ist.

Nur logisch ist, dass auch entsprechende Regelungen, Arbeitsanweisungen, Leitlinien und sonstige Dokumente angepasst werden. Gar neu erstellt wird im Rahmen einer Projektierung die Sicherheitsstrategie, welche Ziele und Erwartungen sowie konzeptionelle Leitgedanken enthält.

Das Endergebnis: Eine wasserdichte Compliance

Sicherlich stellt die Projektierung eines ISDMS – das merkt man alleine an der Länge der Projektdarstellung innerhalb dieses Artikels – eine zunächst komplex erscheinende Aufgabe dar. Da Rödl & Partner aber ein „adaptives Baukastensystem“ für die Konzipierung Ihres zukünftigen ISDMS anwendet, kann ressourcenschonend gearbeitet werden. Die Investition in kontrollierbare, dokumentierte und nachhaltige Informations- und Datensicherheit wird sich lohnen.



IHRE ANSPRECHPARTNER

Gerne stehen wir für weitergehende Fragen zur Verfügung!

Bastian Schönnenbeck LL.M.

B. Sc. Betriebswirtschaft, Master of Laws (Informationsrecht)

T +49 221 949 909 426
E bastian.schoennenbeck@roedl.com

Hannes Hahn

CISA- CSP- DSB, IT Auditor IDW

T +49 221 949 909 200
E hannes.hahn@roedl.com

Falk Hofmann

ISO/ICE27001/KRITIS -Auditor
IT-Auditor, ISO27001 Auditor, DSB

T +49 30 81 079 584
E falk.hofmann@roedl.com

Rödl & Partner
Äußere Sulzbacher Straße 100
90491 Nürnberg

www.roedl.de