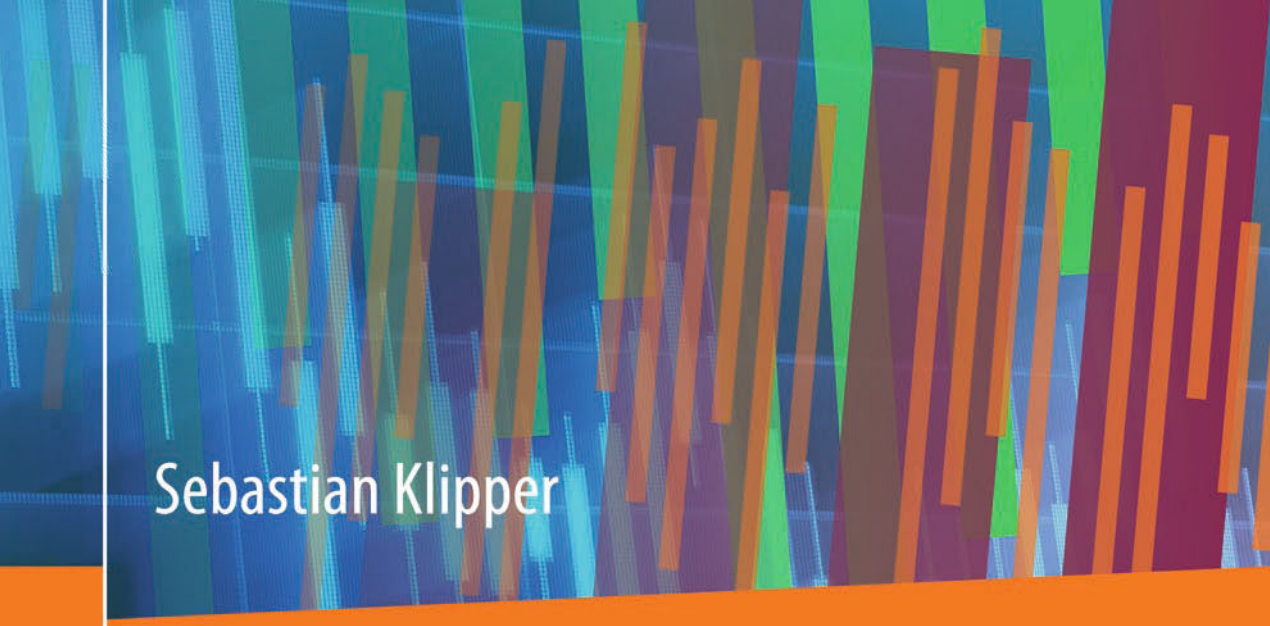

Sebastian Klipper

Information Security Risk Management

Risikomanagement mit ISO/IEC 27001, 27005 und 31010

2. Auflage

‹kes›

Springer Vieweg

Edition <kes>

Herausgegeben von
P. Hohl, Ingelheim, Deutschland

Mit der allgegenwärtigen Computertechnik ist auch die Bedeutung der Sicherheit von Informationen und IT-Systemen immens gestiegen. Angesichts der komplexen Materie und des schnellen Fortschritts der Informationstechnik benötigen IT-Profis dazu fundiertes und gut aufbereitetes Wissen.

Die Buchreihe Edition <kes> liefert das notwendige Know-how, fördert das Risikobewusstsein und hilft bei der Entwicklung und Umsetzung von Lösungen zur Sicherheit von IT-Systemen und ihrer Umgebung.

Herausgeber der Reihe ist Peter Hohl. Er ist darüber hinaus Herausgeber der <kes> – Die Zeitschrift für Informations-Sicherheit (s. a. www.kes.info), die seit 1985 im SecuMedia Verlag erscheint. Die <kes> behandelt alle sicherheitsrelevanten Themen von Audits über Sicherheits-Policies bis hin zu Verschlüsselung und Zugangskontrolle. Außerdem liefert sie Informationen über neue Sicherheits-Hard- und -Software sowie die einschlägige Gesetzgebung zu Multimedia und Datenschutz.

Sebastian Klipper

Information Security Risk Management

Risikomanagement mit ISO/IEC 27001, 27005 und 31010

2., überarbeitete Auflage

Springer Vieweg

Sebastian Klipper
Kiel, Deutschland

Edition <kes>
ISBN 978-3-658-08773-9 ISBN 978-3-658-08774-6 (eBook)
DOI 10.1007/978-3-658-08774-6

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Fachmedien Wiesbaden ist Teil der Fachverlagsgruppe Springer Science+Business Media
(www.springer.com)

Dank

„Begegnet uns jemand, der uns Dank schuldig ist, gleich fällt es uns ein. Wie oft können wir jemandem begegnen, dem wir Dank schuldig sind, ohne daran zu denken!"
-- Johann Wolfgang von Goethe

Ich möchte all meinen Mitstreitern und Auftraggebern danken, mit denen ich in den vielen Jahren als IT-Sicherheitsbeauftragter und Security Consultant intensiv an neuen Ideen und Sicherheitslösungen arbeiten konnte.

Weiterer Dank gilt den Lesern der ersten Auflage, die das Buch so erfolgreich gemacht haben, dass nun auch die zweite überarbeitete Auflage vorliegt.

Vorwort

„Nichts geschieht ohne Risiko, aber ohne Risiko geschieht auch nichts."
-- Walter Scheel

Motivation

Die Geschichte dieses Buchs begann vor etwa fünf Jahren, als ich es selbst kaufen wollte. Sie haben ganz Recht, da war es noch gar nicht geschrieben. Ich war auf der Suche nach einem Buch, das sich explizit mit dem Management von Sicherheitsrisiken auf Basis des ISO/IEC-Standards 27005 beschäftigt. Meine Vorstellung war es, ein Buch zu finden, in dem das Thema Risikomanagement als integraler Bestandteil der ISO/IEC Normenreihe 27000 verstanden und beschrieben wird. Ich musste feststellen, dass es so ein Buch noch nicht gibt und beschloss daher, es selbst zu schreiben.

Welche Norm ist die passende?

Hierzu gehörte insbesondere die Frage, welche Standards der ISO/IEC-Normenreihen für die Implementierung eines Risikomanagementsystems wichtig sind und welche nicht. Will man dieser Frage auf den Grund gehen, indem man die Standards selbst zu Rate zieht, belaufen sich die Investitionskosten schnell auf einige

tausend Euro. Das Buch will diese Standards natürlich keinesfalls ersetzen. In der Regel sollten Sie einige davon trotzdem erwerben. Besonders die Standards 27001, 27002 und 27005 dürfen in keiner Grundausstattung fehlen, wenn Sie sich ernsthaft mit ISO/IEC 27000 auseinandersetzen wollen.

Von der Theorie zur Praxis

Der reine Kauf von Standards und deren Lektüre führt jedoch auch nicht zwangsläufig zum Erfolg. Daher war eine weitere wichtige Frage, die ich mir stellte, wie sich die generischen Formeln eines Standards in die Praxis übertragen lassen und welche Möglichkeiten es gibt, auf der ISO-Klaviatur zu improvisieren. Niemandem ist geholfen, wenn man Standards vom Blatt abliest. Die eigentliche Kunst ist es, sie im eigenen Unternehmen oder dem Unternehmen des Kunden umzusetzen.

Der Mensch steht im Mittelpunkt …

Ich werde mich daher nicht nur der Frage widmen, was die Standards vorschlagen, sondern ebenso erörtern, wie sich die Anforderungen und Vorschläge eines Standards mit den anderen Zwängen, Zielen, Prioritäten und Risiken eines Unternehmens oder einer Behörde in Einklang bringen lassen. Wie schon in meinem ersten Buch *„Konfliktmanagement für Sicherheitsprofis“* [1] steht dabei der Mensch im Mittelpunkt. Spitze Zungen fügen diesem geflügelten Wort gerne folgenden Halbsatz hinzu: *„…und damit allen im Weg“*. Richtig muss es heißen:

> *Der Mensch steht im Mittelpunkt … jeder Sicherheitsbetrachtung!*
> *Oder noch besser:*
> *Menschliches Handeln und Unterlassen steht im Mittelpunkt jeder Sicherheitsbetrachtung!*

Wie schwierig es ist, die Frage nach der praktischen Umsetzung ausschließlich anhand des Standards zu beantworten, zeigt sich bei einem kleinen Test: Der gesamte Risikomanagementprozess soll laut Standard durch die Kommunikation von Informationssicherheitsrisiken überspannt werden.

> *ISO/IEC 27005*
> *11. Kommunikation von Informationssicherheitsrisiken:*
> *Tätigkeit: Informationen zu Risiken sollen zwischen den Entscheidungsträgern und anderen Prozessbeteiligten ausgetauscht und/oder geteilt werden.*

Erläutert wird diese Tätigkeit im Standard auf nur einer Seite. Das reicht in der Praxis kaum aus, um vor einer Bruchlandung bewahrt zu werden. Mit jedem Beteiligten wachsen die unterschiedlichen Interessen und damit auch die unterschiedlichen Sichtweisen auf die Risiken. Mit jeder Kommunikation leitet man eine Quasi-Evaluierung der kommunizierten Risiken ein und bringt den mühsam etablierten Risikomanagementprozess wieder ein wenig ins Wanken.

Unsicherheit

Selbst hervorragend analysierte Risiken sind nicht unerheblich von geschätzten Größen abhängig. Potentielle Schadenshöhen oder Eintrittswahrscheinlichkeiten stehen nicht in irgend einer international anerkannten Tabelle, aus der man nur abzulesen bräuchte. Es handelt sich hierbei um interne oder externe Schätzgrößen oder Erfahrungen der Vergangenheit, zu deren Festlegung man unterschiedlichster Meinung sein kann.

Eingetretene Pfade verlassen

Das Buch wird regelmäßig versuchen die durch die Standards eingetretenen Pfade zu verlassen und nach weiteren Wegen suchen, auf denen Sie Ihre Ziele erreichen können. Ein eigenes Kapitel beschäftigt sich so zum Beispiel mit der Frage, ob man ISO/IEC 27005 in einem IT-Grundschutzprojekt einsetzen kann, in dem eine erweiterte Risikoanalyse notwendig ist.

Fragen über Fragen

Im Grunde ging es bei der Arbeit an diesem Buch darum, die Fragen zu beantworten, die sich mir selbst bei meinen Projekten als Security-Consultant gestellt hatten. Ich hatte bereits erwähnt, dass ich das Buch ursprünglich kaufen und nicht selbst schreiben wollte. Ergänzt wurden meine Fragen durch weitere, die sich in zahlreichen Gesprächen ergeben haben, die ich während der Recherche zu diesem Buch mit Anwendern der ISO/IEC 27000 Familie geführt habe.

Möglichst große Schnittmenge

Meine Hoffnung ist es, dass die Schnittmenge mit Ihren Fragen dadurch besonders groß ist und Sie in dem Buch die Antworten finden, die Sie in Ihrem täglichen Schaffen weiterbringen. Sollten

trotzdem Fragen offen geblieben sein, möchte ich Sie einladen, direkt mit mir Kontakt aufzunehmen. Eventuell habe ich einen Tipp, der in diesem Buch noch nicht berücksichtigt wurde, oder ich kann Ihnen auf anderem Weg weiterhelfen. Besuchen Sie doch einfach meine Webseite:

http://psi2.de
(Webseite des Autors)[1]

2. Auflage kompakter im Inhalt

Die Neuauflage dieses Buches wurde deutlich verschlankt. Viele der bisherigen Inhalte, wie z.B. die Softwaretipps waren recht schnell veraltet und haben mit der Zeit ihren Wert verloren. Aber auch einige der prozessualen Bestandteile haben das Thema weiter ausgedehnt, als es in der Praxis erforderlich ist. Diese Abschnitte wurden meist entfernt oder entsprechend gekürzt und überarbeitet, was das Buch um einiges kompakter und damit nicht zuletzt für Sie kostengünstiger gemacht hat.

Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg bei der Anwendung in der Praxis.

Sebastian Klipper
Januar 2015

[1] Zur Bedeutung des grafischen Codes rechts neben dem Hinweis auf die Webseite zum Buch beachten Sie bitte Erklärung zu QR-Codes auf Seite 9.

Inhaltsverzeichnis

1. Kapitel

1 Einführung

"Es ist unmöglich, ein unnötiges Risiko einzugehen. Denn ob das Risiko unnötig war, findet man erst heraus, wenn man es längst eingegangen ist."
-- Giovanni Agnelli

1.1 Wie wir uns entscheiden

Sie halten das Buch *„Information Security Risk Management"* in den Händen und stehen möglicherweise vor der Frage: *„Direkt kaufen, erst mal ein wenig durchblättern oder sofort wieder weg legen?"* Für manchen Zeitgenossen ist diese Frage der einzige Grund weiterhin in Buchhandlungen zu gehen, statt in Online-Shops einzukaufen: Es geht darum, erst einmal ins Buch zu schauen, es einer ersten Vor-Ort-Prüfung zu unterziehen und erst dann zu entscheiden, ob sich der Kauf wohl lohnen könnte. Letztlich geht es darum, das Risiko zu verringern, mit dem Kauf vollständigen Schiffbruch zu erleiden.

S. Klipper, *Information Security Risk Management,* Edition <kes>,
DOI 10.1007/978-3-658-08774-6_1, © Springer Fachmedien Wiesbaden 2015

„drive-by"-Risikoanalyse

In meinem Buch „Konfliktmanagement für Sicherheitsprofis" [1] habe ich diese Art von Schnellprüfung *„drive-by"*-Risikoanalyse genannt. Die Frage, wie wir Menschen Risikoentscheidungen treffen, ist nämlich wirklich spannend. Warum gibt es Menschen, die auf der einen Seite Brücken über hunderte Meter tiefe Schluchten bauen und sich auf der anderen Seite mit einer halb in Russisch geschriebenen Phishing-Mail die Zugangsdaten zu ihrer Bank stehlen lassen? Warum sind Menschen gleichzeitig so schlau und doch so dumm? Das liegt daran, dass wir uns bei unseren Entscheidungen auf zwei Systeme des Denkens stützen: ein automatisches und ein reflektierendes [2].

Automatisches System

Das automatische System kommt z.B. zum Zuge, wenn Menschen sich jeden Tag durch einen Berg von E-Mails klicken. Hier kann es schnell passieren, dass das automatische System die Oberhand gewinnt. Das Logo der eigenen Bank und deren Corporate Design legen den Risiko-Schalter um und schon werden die Zeilen mit dem russischen Akzent vom automatischen System ins Unterbewusste verbannt. Ohne Scheu kramen jeden Tag tausende Menschen, wie schon hunderte Male zuvor, die Zettel mit den PINs und TANs heraus und geben drei davon in das Eingabefeld einer dubiosen Web-Seite ein. Auf diese Weise klickt das automatische System die Menschen Tag für Tag durch die E-Mail-Fluten.

Bauchgefühl

Würden die Opfer die Gefahr erkennen, würde das reflektierende System sie dazu veranlassen, die Phishing-Mail genau zu prüfen und ihnen würden die Rechtschreibfehler auffallen. Sie würden merken, dass in der Adresszeile des Browserfensters nicht die Adresse der Bank steht, sondern eine ganz andere und sie würden merken, dass die Seite auch kein Sicherheitszertifikat zur Verfügung stellt. Viel zu viele Menschen verlassen sich auf ihr Bauchgefühl und das automatische System übernimmt die Entscheidungen. Bei einer Umfrage, die ich 2009 in der Zeitschrift <kes> veröffentlicht habe [3], hatten immerhin 36% der befragten IT-Sicherheitsfachleute gesagt, dass sie sich bei der Planung ihrer IT-Sicherheitsprojekte auf ihr Bauchgefühl verlassen. Die *„drive-by"*-Risikoanalysen spielen also nicht nur bei der individuellen Entscheidungsfindung eine Rolle, sondern auch im Security Management.

Gerade wenn es um Sicherheit geht, sollte man sich jedoch nicht auf das Bauchgefühl verlassen. Die Komplexität heutiger Informationssysteme ist ohnehin schwer verdaulich. Das damit verbunde-

ne Bauchgefühl muss also zwangsläufig unangenehm sein und es verursacht schon seit vielen Jahren den Ruf nach Unterstützung bei der schwierigen Aufgabe des Managements von Informationssicherheit. In komplexen Informationssystemen, wie wir sie heute kennen, lässt sich die Flut an Informationen unmöglich mit dem fehlerbehafteten automatischen System abarbeiten.

Reflektierendes System

Das reflektierende System hingegen tritt in Erscheinung, wenn sich ein Mensch schwierigen Entscheidungen stellt. Diese Entscheidung trifft er bewusst und kontrolliert.

Risikomanagementsystem

Richtet man sich im Unternehmen nach ISO/IEC 27001 [4] steht man irgendwann vor der Etablierung eines Risikomanagementsystems. Zu einem solchen Risikomanagementsystem gehört es, Risiken festzustellen und dann festzulegen, wie mit ihnen umgegangen werden soll. Nicht zuletzt geht es darum, eine leistungsfähige Risikokommunikation zu etablieren. Es geht sozusagen um die Aktivierung des reflektierenden Systems des Unternehmens.

Auf welchen Industriestandard man sich dabei abstützt, und welchen Anforderungen er genügen muss, ist dabei nicht festgelegt und hängt nicht zuletzt von den Wünschen des Unternehmens oder der Behörde und der Person des Auditors ab.

Zielsetzung dieses Buchs

Während sich ISO/IEC 27001 nur am Rande mit dieser wichtigen Frage auseinandersetzt, ist ISO/IEC 27005 [5] genau dafür ausgelegt. Dieses Buch erläutert den Standard, ordnet ihn in die ISO/IEC 27000 [6] Familie ein und gibt Ihnen Tools und Frameworks an die Hand, mit denen Sie ein Risikomanagementsystem aufbauen können.

1.2 ISMS – Managementsysteme für Informationssicherheit

ISMS

Bevor man jedoch mit dem Management von Risiken für die Informationssicherheit beginnen kann, müssen gewisse Voraussetzungen geschaffen werden. Information Security Risk Management besteht also nicht losgelöst von anderen Sicherheitsbemühungen. Im Gegenteil: es ist integraler Bestandteil eines Managementsystems für Informationssicherheit (ISMS) und nicht etwa eine beliebige Erweiterung.

Auswahl von Maßnahmen

Die Auswahl von Sicherheitsmaßnahmen basiert in einem ISMS auf Entscheidungen, die auf Grundlage von Kriterien zur Risikobehandlung oder gar zur Risikoakzeptanz getroffen werden. Wie sie zustande kommen, damit befasst sich das Risikomanagement. Nicht zuletzt spielen dabei nationale und internationale Gesetze eine Rolle, was üblicherweise unter dem Begriff Compliance zusammengefasst wird.

Risikomanagementprozess

An dieser Stelle wollen wir einen ersten Blick auf eine Grafik werfen, die uns im Verlauf des Buches noch einige Male begegnen wird. Sie ist noch nicht vollständig, aber wir werden sie im Laufe des Buchs mit Inhalt füllen. Was wir bisher identifiziert haben ist also Risikobehandlung und Risikoakzeptanz als die zwei unumgänglichen Bestandteile des Risikomanagements:

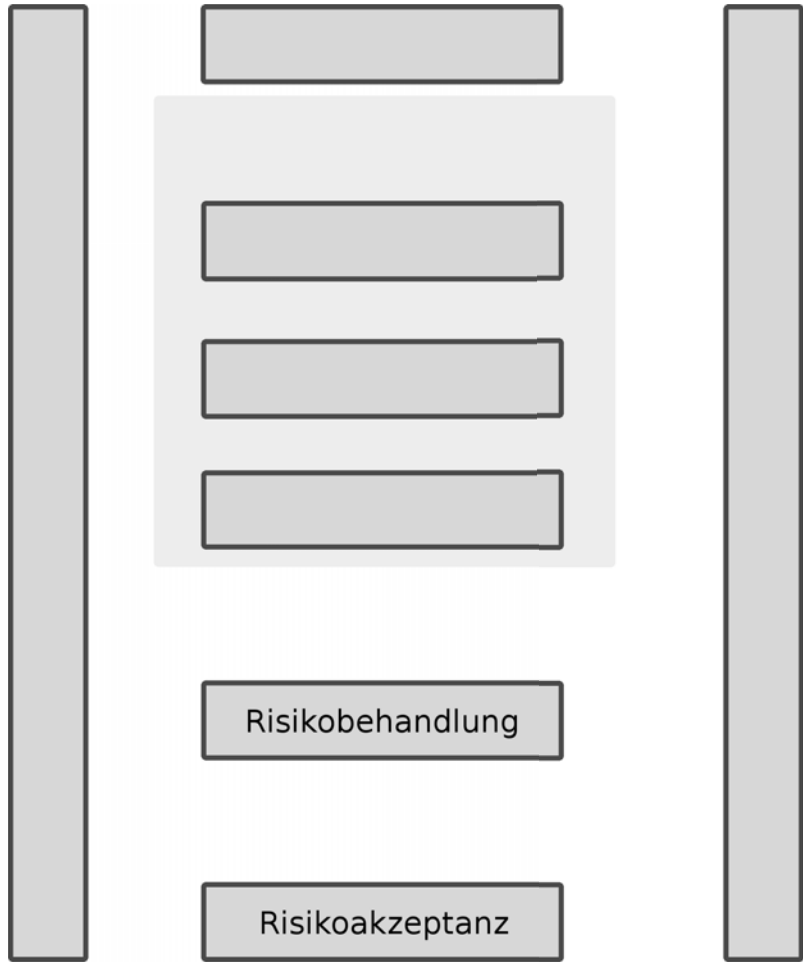

Abbildung 1: Der erste Grundriss des Risikomanagementprozesses (nach [5])

Black-Box Risikomanagement

Es ist wichtig zu erkennen, dass die zwei ersten Felder, die in der Grafik zum Risikomanagementprozess gefüllt wurden, ganz unten stehen. Die Felder Risikobehandlung und Risikoakzeptanz sind die entscheidenden Schnittstellen zum ISMS, mit dem der Risikomanagementprozess in Verbindung steht.

Die weiteren Felder bilden für das ISMS quasi eine Black-Box, denn Risiken werden immer irgendwie behandelt oder akzeptiert. Wie diese Entscheidung zustande kommt variiert unter Umständen beträchtlich. Wenn sie allerdings nicht auf soliden Füßen steht, ist die Wirksamkeit des ganzen ISMS in Frage gestellt.

Daher gehört Risikomanagement auch zu jedem ISMS. Die Standards ISO/IEC 27001 und 27002 sind jedoch recht zurückhaltend, wenn es darum geht zu klären, wie Risikomanagement aussehen soll. ISO/IEC 27005 ist daher in gewisser Weise der Inhalt für die Black-Box. Führen Sie sich jedoch vor Augen, dass Risikomanagement nicht etwa ein kleines Add-On ist, sondern eine beachtliche Aufgabe. Allein der Blick auf die Seitenzahl der Standards macht diesen Trend deutlich. Während ISO/IEC 27001 mit nur 32 Seiten zurecht kommt, benötigt ISO/IEC 27002 bereits 90 Seiten und ISO/IEC 27005 76 Seiten. Damit wird der Risikomanagement-Standard 27005 fast genau so umfangreich wie der Code of Practice der 27002. In den Vorgängerversionen aus dem Jahr 2005 bzw. 2008 war 27002 noch deutlich länger und 27005 kürzer. Aus diesem Blickwinkel „wächst“ die Bedeutung des Risikomanagements innerhalb der Normenreihe der ISO/IEC 27000.

Nun ist es natürlich nicht statthaft, die Wichtigkeit eines Standards beziehungsweise den Aufwand bei dessen Umsetzung anhand der Seitenzahl zu bestimmen. Sie sollten jedoch bedenken, dass Sie sich etwas Eigenes einfallen lassen müssen, wenn Sie sich dagegen entscheiden, die Risikomanagement-Black-Box mit ISO 27005 zu füllen.

Hand in Hand

Am Ende kann es eigentlich nur einen Schluss geben: Wer ein ISMS etabliert, kommt nicht mit ISO/IEC 27001 aus und wird daher auf den Code of Practice aus ISO/IEC 27002 zurückgreifen. Und wer den Code of Practice einsetzt muss sich etwas zum Risikomanagement einfallen lassen. Was liegt da näher, als den passenden Standard aus der ISO/IEC 27000 Familie zu verwenden. Dabei können die Standards jeweils nur schwer voneinander losgelöst betrachtet werden.

ISO/IEC 27003 und 27004

Wenn Sie jetzt nach den dazwischenliegenden Nummern 27003 und 27004 fragen, stellen Sie keine unberechtigte Frage. Die Standards befassen sich mit Implementierung und Design eines ISMS beziehungsweise mit dessen Bewertung. Das sind natürlich ebenfalls wichtige Themen, wenn es um ein ISMS geht. Sie bilden jedoch beide kein neues Stück vom Kuchen, sondern eher Zuckerguss und Sahne. Beides natürlich auch wichtig, aber nicht unverzichtbar. Sie sollten nicht vergessen, dass es für den ISO/IEC 27000 Kuchen noch jede Menge Schokoraspel, Candy und Marzipan-Figürchen gibt:

https://psi2.de/RM-Liste-des-SC27
(Liste der Security-Standards des ISO/IEC Subcommittee 27)[2]

1.3 Schritt für Schritt

Lassen Sie uns nun einen Blick darauf werfen, was Sie in diesem Buch inhaltlich erwartet. Wenn Sie bereits einige Erfahrung mit der ISO/IEC 27000 Familie haben, finden Sie hier eine Orientierung, welche Abschnitte für Sie besonders interessant sind und wo Sie welchen Stoff schneller finden können.

Kapitel 1

Das erste Kapitel (Sie vermuten richtig: das ist das Kapitel, das Sie gerade lesen) soll Ihnen helfen, sich zum Thema Risikomanagement zu orientieren und einen gedanklichen **Einstieg** zu finden. Darüber hinaus enthält es einige technische Hinweise und Tipps, wie Sie mit dem Buch am effektivsten arbeiten können, ohne viel Zeit mit Blättern zu verbringen.

Kapitel 2

Im zweiten Kapitel sollen die **Grundlagen** vermittelt werden, die benötigt werden, um mit der ISO/IEC 27000 Familie arbeiten zu können. Dafür müssen wir uns zunächst auf die verwendeten Begriffe einigen und die Standards in einen Zusammenhang setzen. Um das zu erreichen, ist es unumgänglich, sich damit auseinanderzusetzen, wie ISO-Standards entstehen, und wie sie

---

[2] Zur Bedeutung des grafischen Codes rechts neben dem Hinweis auf die Webseite zum Buch beachten Sie bitte Erklärung zu QR-Codes auf Seite 9.

aufeinander aufbauen. Am Ende dieses Grundlagenkapitels sollten Sie auf dem ISO-Terrain ein gewisses Maß an Trittsicherheit gesammelt haben. Es sollte klar sein, dass ISO/IEC 27005 nicht im luftleeren Raum schwebt, sondern großflächige Schnittstellen mit der ISO/IEC 27000 Familie und den Standards der 31000er Reihe hat. Am Ende des Kapitels stehen die ersten kleineren Fallbeispiele, die den Praxisbezug herstellen.

Kapitel 3

Bezogen auf den Titel des Buches ist Kapitel 3 das Herzkreislaufsystem des Risikomanagements. Der **Risikomanagementprozess** hält die Aktivitäten in gelenkten Bahnen und sorgt für eine gleichmäßige Verteilung von Informationen. Die Bruchstücke dieses Prozesses werden wir bereits in den ersten beiden Kapiteln zusammentragen und sie danach zu einem vollwertigen Gesamtkonzept zusammenfügen. Die nachfolgenden Kapitel bauen darauf auf und ergänzen dieses Herzkreislaufsystem um wichtige Organe und Körperteile. Denn das, was Sie in Ihrem Unternehmen oder Ihrer Behörde zu einem funktionierenden System führt, ist in ISO/IEC 27005 allein nicht enthalten.

Kapitel 4

Die Verwendung von ISO/IEC 27005 im **BSI IT-Grundschutz** ist eine Möglichkeit, die Grundschutz Vorgehensweise zu ergänzen. Hier können aber beide Welten voneinander lernen und sich gegenseitig ergänzen. Insbesondere die IT-Grundschutz-Kataloge sind ein wertvoller Ideenpool, auf den es sich lohnt, einen genaueren Blick zu werfen, was wir in diesem Kapitel auch tun werden.

Kapitel 5

Kapitel 5 befasst sich mit den Inhalten des Standards **ISO/IEC 31010**, der sich mit allgemeinen Risiko-Assessment-Methoden beschäftigt. Eine Auswahl davon eignet sich auch für Assessments der Information Security, die jeweils in einem Steckbriefvorgestellt werden. Hier gibt es übrigens kein falsch oder richtig. Eine Assessment-Methode, die in einen Unternehmen ein voller Erfolg war, kann im anderen Unternehmen in einem Fiasko enden.

Kapitel 6

Ein oft vernachlässigtes Thema ist die **Risikokommunikation**. Man kann fast den gesamten Risikomanagementprozess im stillen Kämmerlein durchziehen, ohne darüber mit jemandem zu sprechen. So kommt man schnell zu Ergebnissen, deren Wert anzuzweifeln ist und sich sicher kaum an der Realität messen lassen kann. Wäre es anders müsste man Managementsysteme für Informationssicherheit nicht vor Ort auditieren. Eine Dokumen-