KOCHBUCH ISMS

Informationssicherheits-Management nach ISO 27001

INHALTSVERZEICHNIS

1. EINLEITUNG

1.1 Definitionen

1.2 Kurzbeschreibung Informationssicherheits-Managementsystem (*ISMS*)

1.3 Kurzbeschreibung ISO 27001

1.4 Auditprozess

1.5 Machbarkeitsanalyse ISMS

Einleitend möchte ich erwähnen, dass ich versucht habe eine möglichst deutsche Sprachführung zu verwenden. Manch englische Begriffe haben sich jedoch derart eingedeutscht, dass es schwerfällt, diese durchgängig in Deutsch zu verwenden.

Die Informationssicherheit wird immer bedeutender. Das ist im Zeitalter der Informationen sicher nicht verwunderlich.

Das Zeitalter der Informationen wurde nicht eingeleitet, weil wir plötzlich alle angefangen haben zu lesen. Vielmehr liegt es an der Verarbeitung der Informationen. Wenn ich ein Buch verschicken möchte, muss das nicht erst zum Buchdrucker geliefert, gesetzt, gedruckt und anschließend verschickt werden, sondern es kann einfach elektronisch per eMail verschickt werden. In weniger als einer Minute ist dieses Buch beim Empfänger.

Wenn ich früher einen Vertrag vereinbaren musste, musste ich diesen per Hand schreiben und verschicken. Nur selten bin ich mit dem ersten Versuch fertig geworden und musste mehrere Exemplare erstellen.

Die Verarbeitung der Informationen findet in schwindelerregender Geschwindigkeit statt. Das führt nicht nur zum schnellen Austausch, sondern auch zum besonderen Nutzen. Maschinen werden nicht mehr handgesteuert und Rezeptbestandteile nicht mehr handgewogen und handgemischt.

Diese Verarbeitungsgeschwindigkeit führt auch zu mehr Vielfalt. Wenn ein Schneider früher froh war, sobald er den Schnitt für eine Jacke fertiggestellt hatte, kann eine Maschine mit einem Knopfdruck einfach ein neues Schnittmuster umsetzen.

Diese Beispiele zeigen, dass die Informationsverarbeitung nicht nur für mehr Geschwindigkeiten sorgt, sondern auch der Umfang der Verarbeitung steigt. Die Informationen nehmen eine immer bedeutendere Rolle ein.

Mit der größeren Bedeutung erhöht sich auch der Schutzbedarf dieser Informationen. Die Sicherheit der Informationen muss gewährleistet werden, da sonst die Maschinen still stehen oder die Konkurrenz schneller ist.

Früher hatte ich das Rezept im Kopf und zur Sicherung im Tresor. Heute liegt es auf dem Computer, in der SPS-Anlage und zur Sicherheit im Backup. Und alle Systeme sind mit dem Internet verbunden.

Mit der Bedeutung der Informationen wächst auch der Neid darauf und das Bedürfnis anderer, sich diese Informationen anzueignen. Die Zahl der Angreifer ist größer geworden, die Möglichkeiten durch die Vergrößerung der Schnittstellen vervielfacht.

Es wird deutlich, dass die Informationen geschützt werden müssen. Die zugehörige Disziplin ist die Informationssicherheit.

Die Informationssicherheit betrachtet die Risiken, die auf die Informationen wirken und schafft Maßnahmen, die diese

Risiken verringern oder gar vermeiden sollen. Sie betrachtet dabei alle Organisationsbereiche und Abteilungen.

Wenn sich eine Organisation das erste Mal mit der Informationssicherheit beschäftigt, entsteht meist die Erwartungshaltung, dass es bereits ein Standardrezept für alles gibt. „Alles eine Soße“ scheinen die Verantwortlichen zu denken. Doch dem ist nicht so!

Das sollte schon beim Lesen dieser voranliegenden Zeilen klar sein. Doch es gibt noch weitere Aspekte, die zu berücksichtigen sind. Ein Zwei-Personen Unternehmen muss sicher andere Maßnahmen ergreifen, als ein zwanzigtausend mitarbeiterstarkes Unternehmen.

Und selbst im Vergleich zweier gleichgroßen Unternehmen gibt es Unterschiede.

Sicherlich geht man in einem Maschinenbauunternehmen anders mit der Sicherheit von Informationen um, als in einem Software Entwicklungsunternehmen.

Selbst der Vergleich zwischen gleichgroßen Unternehmen in derselben Branche hinkt. Die Kultur in den zwei Unternehmen kann komplett unterschiedlich sein. Ein Unternehmen ist vielleicht eher prozessorientiert, während das andere Unternehmen nach „best practice“ arbeitet. Jeder Mitarbeiter ist dann vielleicht mit maximalen Freiheiten ausgestattet und selbstverantwortlich, die best practices umzusetzen.

Wie sagte mir doch einmal ein „Vice President“ eines Software Entwicklungsunternehmens: „Wir sind alles Künstler, Regeln schränken uns ein.“

So kleinkariert das auch klingen mag, dann ist dieses Unternehmen nicht für gängige Standardprozesse geeignet und nach meiner Einschätzung von Professionalität weit entfernt.

Ein Unternehmen oder eine Organisation, wie ich die allgemeine Bezeichnung in dem Buch synonym verwende,

arbeitet nach Möglichkeit nach Zertifizierungsstandard. Das hat zum einen den Vorteil, dass diese Standards bereits nach „Best Practice“ entstanden sind und zum anderen macht man sich damit vergleichbar.

Die Best Practices dieser Standards beruhen allerdings nicht auf die Erfahrungen der begrenzten Zahl an Mitarbeitern, sondern auf die Best Practices der ganzen Industrie. Eine Organisation kann sich zudem mit einem zertifizierten Standard seinen Kunden gegenüber rühmen und damit werben. Der Kunde weiß, dass diese Organisation gute Qualität abliefert, die Umwelt schützt oder die Informationen sichert. Je nachdem, welchen Mehrwert die Organisation für ihre Kunde liefert.

Dennoch: Informationssicherheit als Einheitsbrei, ist wie das Essen einer schlechten Großküche. Jedes Gericht ist verkocht und schmeckt irgendwie immer gleich.

Die Informationssicherheit erfordert für jede Organisation ihre eigene Menükarte und individuell abgeschmeckte Menüs.

In der Informationssicherheit wird die Menükarte in einem Managementsystem abgebildet.

Wie in jeder guten Menükarte werden zunächst einmal die Inhaltsstoffe vorgestellt. So beginnt dieses Buch nach der Einleitung auch mit der Definition vielleicht unbekannter oder widersprüchlicher Begrifflichkeiten. Damit die Inhalte dieses Buches auch für jeden interessierten Leser verständlich sind, möchte ich also die missverständlichen Begriffe kurz erläutern, sofern sie nicht ohnehin an geeigneter Stelle im Buch erklärt werden. Bitte stellen Sie sicher, dass Sie die hier genannten Definitionen kennen. Sie stellen das Verständnis im Buch sicher.

1.1 Definitionen

Audit & Auditor, Review & Revisor

Möchte eine Organisation die Einhaltung ihres ISMS auf einen Standard nachweisen, lässt sie sich auditieren. Ein Auditor überprüft auf Standard-Kompatibilität und kann dabei auf Reviews zurückgreifen.

Ein Review ist auf Arbeitsergebnisse begrenzt. Wie beim Audit können dazu Dokumente eingesehen, Mitarbeiter befragt oder Stichproben genommen werden.

Die Revision „reviewed“ einzelne Arbeitsergebnisse, um die Wirtschaftlichkeit, die Zweck- und Ordnungsmäßigkeit sowie die Sicherheit einzelner Geschäftsprozesse und des internen Kontrollsystems zu überprüfen. Die interne Revision ist aus dem englischen Begriff „Internal Auditing“ entstanden, weshalb die Abgrenzung zum standardprüfenden Auditor nicht konsequent stattfindet.

Best Practices

Sie beruhen auf Erfahrungen und stellen die vermeintlich besten Lösungen der Personen dar, die diese best practices auswählen. Standards beruhen auf best practices einer ganzen Industrie, sind jedoch nicht auf eine individuelle Organisation zugeschnitten.

BSI

Das Bundesamt für Sicherheit in der Informationstechnik (*BSI*) untersteht dem Bundesministerium des Inneren und ist für den Schutz der Informationen in der Verwaltung, Wirtschaft und Gesellschaft sowie für die IT-Systeme des Bundes zuständig.

Verwechslungsgefahr besteht zum *britisch standard institute*, das maßgeblich an der Entwicklung vieler Standards des Schweizer Normungsgremiums ISO beteiligt ist und dieselbe Abkürzung verwendet.

Clauses, Controls und Kapitel

Das interne Kontrollsystem enthält Controls. Warum unterschiedliche Sprachquellen verwendet werden, ist in der „Kurzbeschreibung Informationssicherheits-Managementsystem“ beschrieben.

Die Controls sind jedenfalls in Clauses zusammengefasst. Diese Clauses sind unter Umständen noch einmal in Sub-Clauses unterteilt.

Das Ergebnis eines zentralen Risiko Management sind die Controls, um die Risiken zu verringern oder ganz auszuschalten. Das Rahmenwerk der ISO 27001 ist selbst nicht auf Controls aufgebaut. Seine Anforderungen sind in den Kapiteln der ISO 27001 formuliert. Die Mindestanforderung an Controls findet sich im Anhang A der ISO 27001.

Client / Server

Ein Server liefert den Service – den Dienst, den ein Client (*Deutsch: Kunde*) anfragt und anschließend erhält.

Wenn in der IT ein Dienst von einem anderen IT-System angenommen wird, handelt sich immer um eine Client-/Server-Beziehung. Das Dienst-anfragende IT-System ist der Client, das Dienst-liefernde IT-System ist der Server. Das gilt zum Beispiel auch in Peerto-Peer Netzwerken, die eben gerade nicht eine Client-/Server-Beziehung darstellen. Das liegt daran, dass beide Partner abwechselnd als Client oder Server fungieren. Eine eindeutige Client-/Server-Beziehung lässt sich daraus nicht ableiten.

Hacker

Grundsätzlich bezeichnet ein Hacker jemanden, der sich systemnahe Kenntnisse der IT angeeignet hat. Der Begriff „Hacker“ entstand in den Achtzigern für die Leute, die den ganzen Tag in die Tastaturen der damaligen Home-Computer „gehackt“ haben. Sie sind die Nerds der Achtziger.

Als aus dieser Szene heraus die böswilligen Aktivitäten erfolgten, entwickelte sich die negative Assoziation für den

Blackhat Hacker. Der ethisch gute Hacker ist der mit dem Whitehat. Der Greyhat Hacker hat zwar auch gute Absichten, nimmt es mit der Ethik jedoch nicht so genau.

IaaS / PaaS / SaaS

Die Angebotspalette eines Cloud-Anbieters kann die Infrastructure-as-a-Service (*IaaS*), die Platform-as-a-Service (*PaaS*) oder die Software-as-a-Service (*SaaS*) umfassen. Das Angebot geht dabei von einer reinen virtuellen Hardware-Infrastruktur aus, in der ein Kunde seine eigenen Systeme installiert (*IaaS*), eine vorinstallierte BetriebssystemPlattform (*PaaS*) erhält oder eine vollwertige Anwendungsumgebung (*SaaS*) nutzen kann. Der Kunde benötigt nur noch einen Teil an technischer Expertise, bis zu dem Punkt, an dem in der SaaS-Umgebung keine technische Kompetenz mehr erforderlich ist. Da diese „as-a-Service“ Angebote aus Marketinggründen verschiedene Auswüchse genommen haben, wurde der Begriff „XaaS“ geschaffen, um eine gemeinsame Bezeichnung aller Services zu schaffen.

IT-Sicherheit & Informationssicherheit in einem ISMS

Beiden Sparten der IT-Sicherheit und Informationssicherheit geht es um die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen. Während die IT-Sicherheit dabei den Schutz der Informationen in der technischen Verarbeitung sicherstellen möchte, nimmt sich die Informationssicherheit der kompletten Verarbeitung innerhalb einer Organisation an. Eben auch dem Umgang mit Papierware oder dem persönlichen Zutritt sowie der Einhaltung juristischer Anforderungen und der technischen Informationssicherheit. Die IT-Sicherheit ist somit ein Teilbereich der Informationssicherheit.

Idealerweise setzt man dafür ein Informationssicherheits-Managementsystem (*ISMS*) ein. Ich stelle weitere

Alternativen vor, jedoch ist das ISMS der ISO 27001 das Hauptthema dieses Buches.

Information Asset (*IT-Asset*)

Zusammengefasst aus der ISO 27005: „Ein IT-Asset ist alles, was für das Unternehmen von Wert ist und daher geschützt werden muss. Für jedes IT-Asset sollte ein Owner identifiziert werden, um die Verantwortung und Rechenschaftspflicht dafür zu übernehmen."

Die ISO 27005 betrachtet „primäre Assets" als sensible Kernprozesse und sensible Informationen sowie „unterstützende Assets", die bedroht werden können, um die primären Assets zu beeinträchtigen.

IT-Asset Owner & IT-Risk Owner

Beide Owner haben in der Regel keine Eigentumsrechte. Die „Ownerschaft" bezieht sich auf die Zuständigkeit und fachliche Verantwortung für das IT-Asset oder das ITRisiko.

Neben der fachlichen Verantwortung gibt es immer auch reine rechtliche und damit wirtschaftliche Verantwortung, die bei der Geschäftsführung liegt. Insbesondere im Zusammenhang mit der „IT-Risk Ownerschaft" kann es dabei zu Verwechslungen kommen. In der Regel ist jedoch der fachliche Owner gemeint.

Key IT-Risk Indicator (*KIRI*)

Sie messen und zeigen die Wirksamkeit der Sicherheitsmaßnahmen auf. Generell sind sie vor allem für die Messung von Controls geeignet, können jedoch auch für die Messung von Maßnahmen aus dem Rahmenwerk verwendet werden.

Organisationen & Unternehmen

In dem Buch wird möglichst der weitläufigere Begriff Organisation statt Unternehmen verwendet, um non-Profit

oder andere Organisationen in der Beschreibung nicht auszuschließen.

Wenn explizit gewinnorientierte Unternehmen gemeint sind, wird jedoch der Begriff „Unternehmen“ synonym verwendet.

Risiko Management

Das Management ist die Verwaltung des Risikos. Dazu gehört die Risikoermittlung und das Risiko Assessment sowie die Risikoverfolgung und die Aktualisierung der Risikoeinschätzungen.

Die Risikoermittlung erfolgt über die Erhebung der IT-Assets sowie die Priorisierung über die Schutzbedarfsfeststellung und dann der Risikoanalyse. Da die Risikoanalyse bereits Teil des Risiko Assessment ist, lässt sich die Risikoermittlung nicht konsequent abgrenzen.

Ein Risiko Assessment ergänzt die Risikoanalyse durch die anschließende Bewertung des Risikos.

Für das Risiko Management ergibt sich daher folgendes Bild.

Abbildung 1: Risiko Management

Die Risikoanalyse hängt vom ausgewählten Risiko Management ab.

Sie enthält immer eine Bedrohungsanalyse aus der Kombination Bedrohung x Schwachstelle x Schutzbedarf. Sie kann jedoch noch eine Konsequenzanalyse beinhalten. Mehr dazu im Kapitel „Risiko Management“.

Management Informationssicherheitsereignis & Informationssicherheitsvorfall

Alles, was die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen beeinträchtigen kann, ist erst einmal ein Informationssicherheitsereignis. Sobald eines der Sicherheitskriterien (*Vertraulichkeit, Verfügbarkeit, Integrität*) verletzt wird, wird aus einem Ereignis ein Informationssicherheitsvorfall – im Englischen ein „information security incident“.

Um diesen Vorfall zu beherrschen, muss er „gemanaged“ werden.

Stakeholder & Shareholder

Ein Stakeholder ist jeder Interessent der Organisation oder dessen Informationen. Es sind sowohl die Mitarbeiter als auch die Kunden, Lieferanten, Behörden oder sonstige Einheiten, die ein Interesse haben könnten.

Auch Shareholder gehören dazu. Sie sind die Anteilseigner und haben ein besonderes Interesse, das sich zumeist an einem ordentlichen Gewinn orientiert.

Zero-Day Attacke (*0-Day Attacke*)

Eine Schwachstelle, die noch niemand kennt, ist keine Bedrohung. Sie kann von niemanden ausgenutzt werden und stellt kein Risiko dar.

Kennt ein Angreifer jedoch eine Schwachstelle, die beim Betreiber noch unbekannt ist, ist der Angreifer im Vorteil. Für das Opfer beginnt der „Tag 0“ für diese Schwachstelle. Dieser „Zero-Day“ läuft erst ab, wenn es eine Maßnahme (*in der Regel ein Patch*) gegen diese Schwachstelle gibt.

Dieses Patch muss das Opfer nun noch installieren, um sich gegen diese Attacke zu schützen.

1.2 Kurzbeschreibung Informationssicherheits - Managementsystem

Wenn die Menükarte das Informationssicherheits-Managementsystem ist, ist das Risiko Management eine Beschreibung der Inhaltsstoffe. Die Controls wären dann die Preise für die jeweiligen Gerichte. Doch dazu nun mehr.

Wenn man nach Amerika guckt und die Unternehmen sieht, die sich auch in unseren Gefilden breitmachen, bekommen die Meisten Bauchschmerzen, beim Gedanken, wie diese mit unseren Informationen und personenbezogenen Daten umgehen. Oft haben die Amerikaner einen eher ökonomischen Blick auf die Dinge.

Irgendein Professor hatte mir mal eine passende Anekdote dazu geliefert.

„*Zwei Flugzeuge fliegen unverhinderbar aufeinander zu. Die einzige Möglichkeit, die Besatzung zu retten, wäre der Absturz eines der Flugzeuge. Der Amerikaner würde fragen, in welchem Flugzeug weniger Menschen sitzen und würde dieses Flugzeug abschießen, um das Andere zu retten.*

Ein Europäer würde es als ethisch verwerflich halten, überhaupt ein Flugzeug abzuschießen und würde beide verlieren.“

Ehrlich gesagt, fühle ich mich der europäischen Version näher. Und vielleicht würde ein Amerikaner sogar nur fragen, welches Flugzeug weniger Wert hat?!

Was ich mit dieser kleinen Anekdote deutlich machen wollte, dass die Amerikaner einen anderen Blick auf die Sicherheit und auch auf die Informationssicherheit haben. Man kann sich ihre guten Absichten nicht immer gleich erschließen, dennoch sind die Amerikaner auch in der Informationssicherheit oftmals der Vorreiter.

So hat der amerikanische Verband der Buch- und Wirtschaftsprüfer, AICPA (*American Institute of Certified Public Accountants*), bereits 1949 ein internal control system (*ics*) als notwendig erachtet.

Das ics (*Deutsch: Internes Kontrollsystem*) sollte die Zuverlässigkeit der Buchhaltung und Effizienz der prozessualen Abläufe sicherstellen. Maßnahmen, um die Finanzbuchführung zu optimieren. 1985 wurde dazu das COSO[1] Modell für den Aufbau eines angemessenen internal control system entwickelt.

Dieses COSO Modell und weitere Bestrebungen von internal controls hatten auch Einfluss auf die deutsche Wirtschaftsprüfung. Obwohl sich das Prinzip eines internal control systems in verschiedenen Gesetzgebungen wiederfand, beschrieb das Institut der Wirtschaftsprüfer (*IDW e.V.*) erst im Jahre 2001 ein internes Kontrollsystem mit seinem Prüfungsstand IDW PS 260.

In Deutschland herrschte bis dahin und weitgehend heute noch die Auffassung, dass ein internes Kontrollsystem eher Prüf- und Überwachungsaufgaben hat. Darin unterscheidet sich die Betrachtung eines internen Kontrollsystems von einem internal control system, das auf risikobasierte Sicherheitsmaßnahmen setzt.

Und das hat seine nachvollziehbaren Gründe.

Wenn ich etwas kontrolliere, kontrolliere ich zum Beispiel, ob die Hausaufgaben gemacht wurden, die Tür abgeschlossen ist oder ich kontrolliere den Verlauf der Sonne. Wenn man in Deutschland etwas kontrolliert, ist es somit meist die Prüfung oder Überwachung von technischen oder persönlichen Leistungsergebnissen.

Wir können jedoch auch ein Modellauto über eine Fernbedienung oder einen Roboter kontrollieren. In dem Fall würden wir allerdings eher sagen, dass wir das Modellauto oder den Roboter steuern.

Und genau so wird das Wort „control“ in der englischsprachigen Welt verendet. Wenn ein Engländer oder Amerikaner etwas „controls“, dann steuert er etwas. „I control you“ heißt nicht, dass ich Deine Arbeitsleistung überprüfe, sondern, dass ich Dich steuere.

Bei allem Verständnis für die auftretenden Missverständnisse, geht es in einem internen Kontrollsystem eines ISMS um Sicherheitsmaßnahmen. Es geht um Maßnahmen zur Steuerung der Informationssicherheit. Der Begriff „Kontrolle“ ist für die Sicherheitsmaßnahmen irreführend. Daher sollte in der Informationssicherheit immer der Begriff „Control“ für Sicherheitsmaßnahmen gewählt werden!

So halten wir es auch in diesem Buch. Wir verwenden das Wort „Control“ für die Sicherheitsmaßnahmen, für das interne Kontrollsystem verwenden wir jedoch die deutsche Übersetzung.

Ein internes Kontrollsystem ist zumindest in der Informationssicherheit risikobasiert angelegt. Das heißt, ich habe Risiken erkannt und möchte diese mit Sicherheitsmaßnahmen verringern. Diese Maßnahmen sind dann die „controls“ in einem internen Kontrollsystem.

In der Informationssicherheit entstehen diese Risiken auf die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** der Informationen innerhalb eines verwalteten Bereichs – innerhalb des Geltungsbereichs eines Managementsystems.

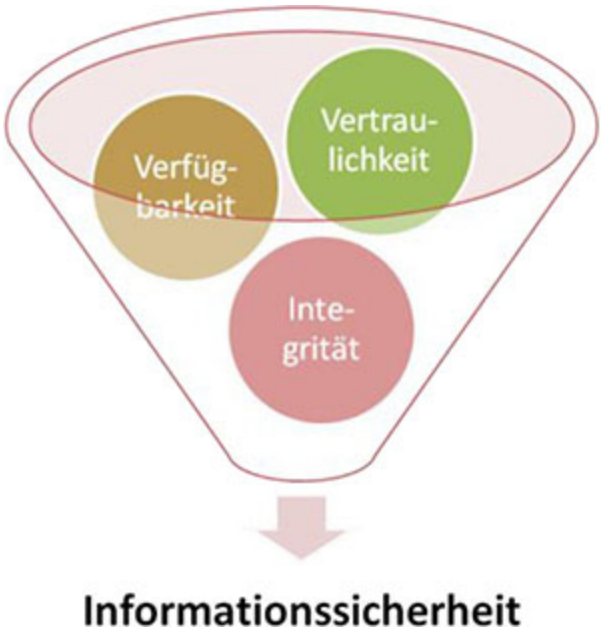

Abbildung 2: Vertraulichkeit, Verfügbarkeit, Integrität

Das heißt, ich muss meinen verwalteten Bereich bestimmen, in dem ich meine Controls zur Verringerung der Risiken einsetzen möchte. Das ist der Geltungsbereich meines Informationssicherheits-Managementsystems.

Es gibt jedoch auch eine Prüf- und Überwachungsfunktionen innerhalb eines Informationssicherheits-Managementsystems. Das sind unter anderem die **Key IT-Risk Indicator** (*KIRI*). Sie werden erstellt, um die Wirksamkeit des internen Kontrollsystems messen. In anderen Rahmenwerken heißen sie Key Performance Indicator (*KPI*) und in der alten ISO 27001 waren es die Measurements of Effectiveness (*MoE*).

Bei den Key IT-Risk Indicators handelt es sich um ausgewählte Indikatoren. Wenn es sich nicht um die Schlüssel-Indikatoren handelt, kann auch eine Bezeichnung „IT-Risk Indicator“ ausreichen.

Nun geht man hin, benennt den Geltungsbereich seines InformationssicherheitsManagementsystems, führt das Risiko Management aus und misst die Wirksamkeit.

In der Entwicklung der Informationssicherheit hat sich jedoch gezeigt, dass das nicht ausreicht.

Man hat um dieses Risiko Management und das dazugehörige interne Kontrollsystem herum, ein anerkanntes Managementsystem geschnallt: den Management Kreislauf „**Deming Wheel**“.

Die Entstehungsgeschichte ist nicht ganz klar. Er ist in Anlehnung an den Shewhart Cycle entstanden und abschließend in einem japanischen Prozess-Workshop, den W. Edwards Deming leitete, entwickelt worden.

Dieses Managementsystem sichert den kontinuierlichen Verbesserungsprozess über die Phasen „Plan“, „Do“, „Check“ und „Act“ vor.

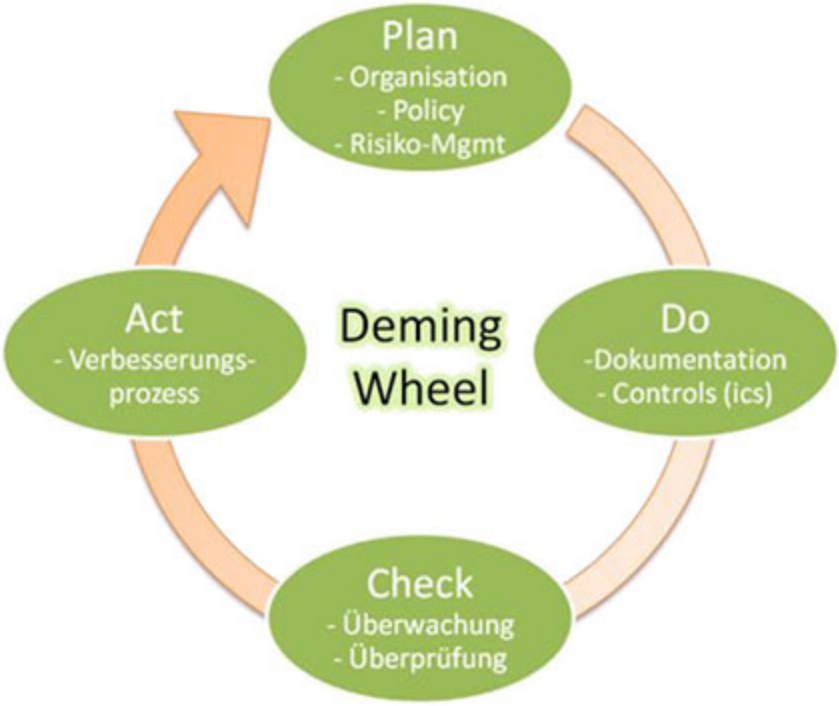

Abbildung 3: Deming Wheel

Dieser Plan-Do-Check-Act Kreislauf stellt nun den Rahmen um das Risiko Management und das sich daraus ergebene interne Kontrollsystem.

Mit diesem Managementkreislauf ist auch die Entstehungsgeschichte der ISO 27001 verbunden.

1.3 Kurzbeschreibung ISO 27001

Die ISO 27001 ist die Beschreibung eines Informationssicherheits-Managementsystems.

Sie hatte ihre Anfänge mit einem Vorschlag aus „Best Practices“.

Best Practices waren und sind Praktiken, die sich im Laufe der Zeit bewährt haben. Sie stellen Maßnahmen dar, die Informationssicherheit in den Organisationen gewährleisten sollen.

Der Ursprung dieser Best Practices der Informationssicherheit war ein Zusammenschluss niederländischer Berater, die sich mit britischen Unternehmensberatern zusammengetan haben, um diese zu einem Standard zu etablieren. Die Ergebnisse sind zunächst an das british standard institute gelangt und wurden 1995 zum BS 7799 erhoben. Dieser Standard wurde 1998 in BS 7799-1 umbenannt, da im selben Jahr das Rahmenwerk für diese Best Practices, die BS 7799-2 veröffentlicht wurde.

Im Jahre 2000 wurde die BS 7799-1 schließlich von der International Standard Organisation zur ISO 17799 erhoben. Die BS 7799-2 folgte dann 2005 als ISO 27001, worauf die ISO 17799 im Jahre 2007 zur ISO 27002 umbenannt wurde.

Beide Standards werden immer wieder einmal angepasst. Die bedeutendste Anpassung gab es zuletzt im Jahre 2013, als die ISO 27001 in der sogenannten **High Level Structure** angelegt wurde. Diese High Level Structure bildet den Plan-Do-Check-Act Kreislauf in ihrer Verzeichnisstruktur sichtbar ab und findet mehr und mehr auch in anderen Management Rahmenwerken Einzug.

Dadurch lassen sich unterschiedliche Managementsysteme viel besser einander integrieren. Als Beispiel sei die ISO 9001 des Qualitäts-Managements genannt, die oftmals auch ohne die High Level Structure gemeinsam mit der ISO 27001 implementiert wurde. Beide Standards haben nun eine einheitliche Struktur, mit ähnlichen Inhalten. Die Aktivitäten lassen sich dadurch unkompliziert parallel nutzen oder zumindest parallel abarbeiten.

Die ISO 27001 stellt einige Forderungen, auf welchen Füßen der Schutz der Vertraulichkeit, Verfügbarkeit und Integrität die Informationssicherheit zu stehen hat.

Anhand der verschiedenen Interessengruppen und des Kontextes, in dem die Organisation steht, wird eine übergreifende Informationssicherheitsrichtlinie erstellt, die dem Mitarbeiter aufzeigen soll, wo die Organisation ihre Schmerzen der Informationssicherheit sieht.

Auf Basis dessen ist dann ein Risiko Assessment erst einmal zu planen und später durchzuführen.

Das Risiko Assessment unterscheidet sich von der Risikoanalyse, da es den ganzen Bewertungsprozess betrachtet.

Das Risiko Management beinhaltet dann wieder die Plan-Do-Check-Act Phasen, um sich als ganzheitliches Managementsystem zu präsentieren.

Die ISO 27001 fordert zudem einige Zugeständnisse von der Geschäftsführung, um das Funktionieren eines Informationssicherheits-Managementsystems sicherzustellen. Da sind selbstverständlich die Ressourcen, Kompetenz der Informationssicherheit sowie Maßnahmen zur Sensibilisierung der Mitarbeiter zu nennen. Darüber hinaus fordert der Standard einen geordneten

Kommunikationsprozess und eine einheitliche Dokumentation.

Das Beste bietet der Standard mit dem kontinuierlichen Verbesserungsprozess zum Schluss. Die ISO 27001 fordert hier einige Prüf-, Überwachungs- und Berichtsmaßnahmen, um entscheidende Maßnahmen zur Verbesserung in der Act-Phase auf den Weg zu bringen.

Der Anhang A wartet dann mit einer Liste an Controls auf, die im Laufe des Erstellungsprozesses des internen Kontrollsystems zumindest berücksichtigt werden sollten. Diese Controls sind in sogenannten Clauses unterteilt, in denen einige Control Objectives (*Deutsch: Kontrollziele*) vermerkt sind. Um diese Kontrollziele zu erreichen, sind einige Controls definiert, die zur Erreichung dieser Kontrollziele beitragen.

Und da kommen wir dann endlich auch zur ISO 27002.

Sie gibt Umsetzungshinweise, wie die Controls aus dem Anhang A umgesetzt werden können. Die Auditoren bedienen sich in ihrer Argumentation oft der ISO 27002. Diese ist jedoch nicht zertifizierungsrelevant. Das heißt, die Organisation kann sich danach richten, muss sie jedoch nicht.

Sollte ein Auditor Vorhaltungen über die Umsetzung eines Controls machen und dann auf die ISO 27002 verweisen, kann man ihm gern antworten, dass „die ISO 27002 nicht zertifizierungsrelevant ist“. Dann bekommt er große Augen und wird in aller Regel still. Zertifizierungsrelevant ist die ISO 27001. Dazu gehört auch der Anhang A. Der ist allerdings so abstrakt geschrieben, dass er erhebliche Freiheiten in der Umsetzung bietet.

Um es noch einmal zu verdeutlichen:

Das saftige Filet-Steak liegt in der Mitte des Tellers. Es ist das Risiko Management, inklusive der Controls, die fein

säuberlich mit den Vorgaben aus dem Anhang A abgeschmeckt werden.

Drum herum liegt das liebevoll angerichtete Gemüse und die Kohlenhydrate, sei es Reis, Nudeln oder Kartoffeln. So angerichtet, wird jeder Auditor genussvoll schmatzen und ein positives Zeugnis ausstellen. Sollte der Auditor ein Vegetarier oder Veganer sein, kann es natürlich gern auch ein Tofu Steak sein.

1.4 Auditprozess

Wie in jeder Menükarte die Getränke ganz hinten stehen, sollten auch die Audit- und Zertifizierungsfragen in den Managementsystemen der Informationssicherheit ganz hinten stehen. Schließlich folgt das Audit und das Zertifikat dem ganzen Prozess zum Schluss.

Jedoch sind die Getränke die leichte Kost. Wer hat sich nicht schon einmal selbst dabei entdeckt, die Menükarte von hinten zu lesen, um zuerst die Getränke zu bestellen. In der Hoffnung, die Getränke kommen damit umso schneller.

Ähnlich ist es mit dem Auditprozess. Viele Fragen ergeben sich, wenn man weiß, wie der Auditprozess verläuft. Danach folgt dann noch der Zertifizierungsprozess, der uns allerdings an dieser Stelle noch nicht helfen kann. Daher bleibt er an letzter Stelle – ebenso wie die harten Getränke, die immer auch erst nach dem Essen kommen.

An dieser Stelle beschreibe ich den Auditprozess, weniger aus der Sicht des Standards heraus, sondern viel mehr aus der Praxis. Wie ein Auditor das Audit erlebt und wie die auditierte Organisation das nutzen kann.

Man sollte sich dabei vor Augen führen, dass hinter dem Auditprozess immer auch eine Dienstleistung steckt. Auf der einen Seite zahlen die Kunden und auf der anderen Seite verdienen die Dienstleister daran. Machen die Auditoren ihre

Sache nicht im Sinne des zahlenden Kunden, werden sie zum nächsten Audit nicht mehr eingeladen und müssen sich einen neuen Kunden suchen.

Der zahlende Kunde will letztendlich das Zertifikat.

Ein „guter“ Auditor findet daher am Ende immer einen Weg, das Zertifikat auszustellen.

Viele Auditoren treiben es dabei allerdings auf die Spitze.

Ich musste beispielsweise zu einem Überwachungsaudit, bei dem der Kunde keine Key IT-Risk Indicators erstellt hat. Die Key IT-Risk Indicator sind Teil des Rahmenwerkes der ISO 27001 und müssen für ein Zertifikat immer eingerichtet werden!

In dem Fall war es wohl so, dass der Auditor des vorjährigen Zertifikataudits sich mit dem Kunden gestritten hatte. Die Welt ist klein, ich kenne den Auditor persönlich und habe immer gern mit ihm zusammengearbeitet. Er war eigentlich sehr formell, ließ es allerdings manchmal an Empathie vermissen.

Jedenfalls stehe ich vor dem Kunden und frage nach den Key IT-Risk Indicators. „Hamwanich“ war die lapidare Antwort.

„Wieso haben Sie dann ein Zertifikat?“ fragte ich. Das konnten sie mir nicht beantworten.

Dieses Unternehmen hätte das Zertifikat niemals erhalten dürfen!

Die Key IT-Risk Indicators (*KIRIs*) sind oft ein Problem.

In den Fällen, in denen ich der Lead Auditor war, hatten die Kunden jedoch auch ein Qualitäts-Managementsystem implementiert und konnten mir Key Performance Indicator vorlegen, die sich auch mit der Informationssicherheit befassen. So auch in diesem Fall.

Ich gab ihnen einen Tag Zeit, um die Indikatoren der Informationssicherheit zusammenzustellen. Für das kommende Audit gab ich ihnen dann mit, die KIRIs auf die

größten Risiken der Informationssicherheit auszurichten und bot ihnen somit die Möglichkeit, sich zu verbessern.

In einem anderen Audit war ich als Dienstleister für das auditierte Unternehmen, dem **Auditee** tätig.

Es handelte sich dabei um ein Tochterunternehmen eines weltweiten Software-Herstellers. Von Anbeginn unserer Zusammenarbeit erklärte ich seinen Mitarbeitern, dass deren Risiko Assessment nicht angemessen sei. Sie ließen sogar extra einen Mitarbeiter aus Amerika einfliegen, der mir versicherte: „Das machen wir immer so und ist ausreichend.“

Richtiger Weise nahm der Auditor das Risiko Management im anschließenden Zertifizierungsaudit auseinander. Das zentrale Instrument eines InformationssicherheitsManagementsystems hatte nichts mit dem zu tun, was wir da gerade betreuten!

Das hätte nach meinem Empfinden zum Abbruch des Audits führen müssen.

Doch es ging weiter.

Dann verbissen sich die Auditoren in die Gesellschafter dieses Tochterunternehmens.

Der Mutterkonzern hätte zu viel Einfluss und könnte das Unternehmen steuern. Vollkommener Quatsch, da jedes Unternehmen seinen Eigentümer hat, der die Geschicke letztlich lenkt. Aber der Auditor hielt daran fest und hätte das Zertifikat mit dieser Auffassung abermals nicht erteilen dürfen!

Tat er aber, da er nicht der Auditor sein wollte, der eines der weltweit größten Unternehmen das Zertifikat versagte. Man schmückt sich eben gern mit diesen Federn. Außerdem wären Folgeaufträge so nicht denkbar gewesen.

Man sieht an diesen Beispielen, dass die Auditoren zum einen auch nur Menschen und nicht immer in Höchstform sind und zum anderen, dass Geld und Namen eine

wesentliche Rolle spielen. Derlei Beispiele gibt es noch viele andere.

Man kann sich jedoch vorstellen, dass die meisten Auditoren auch bereit sind, ein Zertifikat notfalls zu entsagen, wenn der Kunde sich gar nicht bewegt. Es ist immer ein Geben und Nehmen. Jeder Auditor hat da seine eigene Schmerzgrenze und kein Auditor will sich offensichtlich auf der Nase herumtanzen lassen.

Der Auditor bekommt von dem Auditee zunächst einen Satz an Dokumenten des Informationssicherheits-Managementsystems. Dazu gehört der Auditbericht und die Beanstandungen des letzten Jahres. Hinzu kommen das Statement of Applicability, der Risk Treatment Plan, das Scope Dokument, ein Organigramm und weitere Dokumente, die die Organisation und das Informationssicherheits-Managementsystem beschreiben. Das sind dann meist die Richtlinien und Prozessbeschreibungen der Organisation. Vertrauliche Dokumente werden dabei nur selten herausgegeben. Sie werden vor Ort besichtigt und besprochen.

Dennoch ist es ein umfangreicher Satz an Dokumenten, mit denen sich der Auditor vorbereiten soll.

Es gibt vom Standard festgelegte Zeiten zur Vorbereitung. Die Einhaltung dieser Zeiten prüft die jeweilige Akkreditierungsgesellschaft. Jedoch gibt es erhebliche Variationsmöglichkeiten, mit denen die Auditzeiten heruntergerechnet werden können.

Ich hatte in keinem meiner Audits mehr als zwei Tage für die Vor- und Nachbereitung, inklusive der Erstellung des Auditreports. Zu einem speziellen Auditauftrag wollte man mir einen halben Tag für die Vor- und Nachbereitung zugestehen. Ich habe dankend abgelehnt.

Letztlich bleibt den Auditoren nicht genügend Zeit, sich in das ISMS der Organisation einzuarbeiten. Das kann den auditierten Organisationen zum Vorteil gereichen.

Die Zusammenhänge sind in einigen komplexen Organisationen kaum zu verstehen. Schon gar nicht in der zur Verfügung gestellten Zeit.

Hinterfragt der Auditor einen Prozess, verweist man als Auditee einfach auf einen alternativen Prozess und verwirrt den Auditor am Ende komplett. Sollte der Auditor unerwartet darauf herumreiten, bis er die Zusammenhänge versteht, mag es vielleicht eine Abweichung geben. Die Abweichung wird abgestellt, der Auditor hat jedoch weniger Zeit zur Prüfung anderer Dinge.

Für den Auditee ist es somit ein willkommenes Szenario, wenn sich der Auditor an einem Thema verbeißt.

Wenn die Mitarbeiter die Interviews in den Audits zudem in die Länge ziehen, kommt der Auditor vollends aus dem Zeitplan.

Bei Zertifizierungsaudits gibt es zunächst ein Dokumentenaudit.

Dort bespricht der Auditor die ISMS-Dokumente mit dem Kunden. In diesen Sitzungen bekommt er dann auch die vertraulichen Dokumente zu sehen. Auch das kostet wieder Zeit. Schließlich sieht der Auditor die Dokumente das erste Mal.

Mehrfach konnte ich beobachten, dass an dieser Stelle das erste Mal über den Geltungsbereich gesprochen wird. Die Auditoren, teilweise auch die Zertifizierungsgesellschaften, wussten an dieser Stelle nicht, welche Informationen das Informationssicherheits-Managementsystem eigentlich schützen soll.

Damit sind dann eigentlich auch die Dokumente, die der Auditor zur Vorbereitung erhalten hat, für die Katz. Schließlich ist nicht klar, ob diese Dokumente zum Geltungsbereich gehören.

Natürlich steht man als auditierte Organisation während des Audits am Pranger und muss liefern.

Auch wenn die Auditoren am Ende eindreiviertel Augen zudrücken, werden sie jetzt die Inhalte der Dokumente hinterfragen. Und nicht nur das. Es geht bereits um Metadaten der Dokumente, Versionskontrolle und die Einhaltung regelmäßiger Dokumentenprüfungen – den Reviews.

Doch das ist nur die Pflicht. Die Kür folgt dann mit dem Vor-Ort Audit.

Jetzt fragt man sich vielleicht, warum es ein Vor-Ort Audit gibt, wenn das vorgelagerte Dokumentenaudit bereits vor Ort stattfindet. Das habe ich mich zunächst auch gefragt. Es ist aber so vorgesehen und macht auch Sinn.

Die Dokumente erfordern oftmals Erklärungen und der Auditor soll sich einen ersten Eindruck verschaffen, ob die Organisation ein funktionierendes Informationssicherheits-Managementsystems betreibt. Er guckt, ob die Zutrittskontrollen greifen, die Mitarbeiter eine etwaige Clean Desk Policy einhalten und sich generell angemessen zur Informationssicherheit verhalten.

Die Zertifizierungsgesellschaften handhaben es unterschiedlich, wieviel Zeit zwischen Dokumentenaudit, auch **Stufe 1 Audit**, und dem Vor-Ort Audit, dem **Stufe 2 Audit** liegen muss.

Mit dem Stufe 1 Audit hat der Auditor sich jedenfalls schon einmal einen ersten Eindruck verschafft.

Im Vor-Ort Audit (*Stufe 2*) geht es ans Eingemachte. Nun prüft der Auditor die Prozesse, die Richtlinien und gegebenenfalls die Einhaltung der Sicherheitsmaßnahmen.

Anders als in einem Zertifizierungsaudit und Rezertifizierungsaudit, wird ein Überwachungsaudit nicht in zwei Stufen aufgeteilt. Dort werden alle Aspekte in einem Vor-Ort Audit geprüft.

Technisch prüft der Auditor nichts. Jedenfalls legt er selbst keine Hand an. Audits der Informationssicherheit sind keine technischen Audits!

Durchaus kann er mal verlangen, dass man das zuletzt installierte Update zeigt oder er lässt sich die Einstellungen in den System zeigen. Hand sollte er selbst jedoch nicht anlegen. Auch sollte er wissen, was er tut, wenn er dem Mitarbeiter die Eingabe von Befehlen vorgibt. Das wird daher nur selten vorkommen.

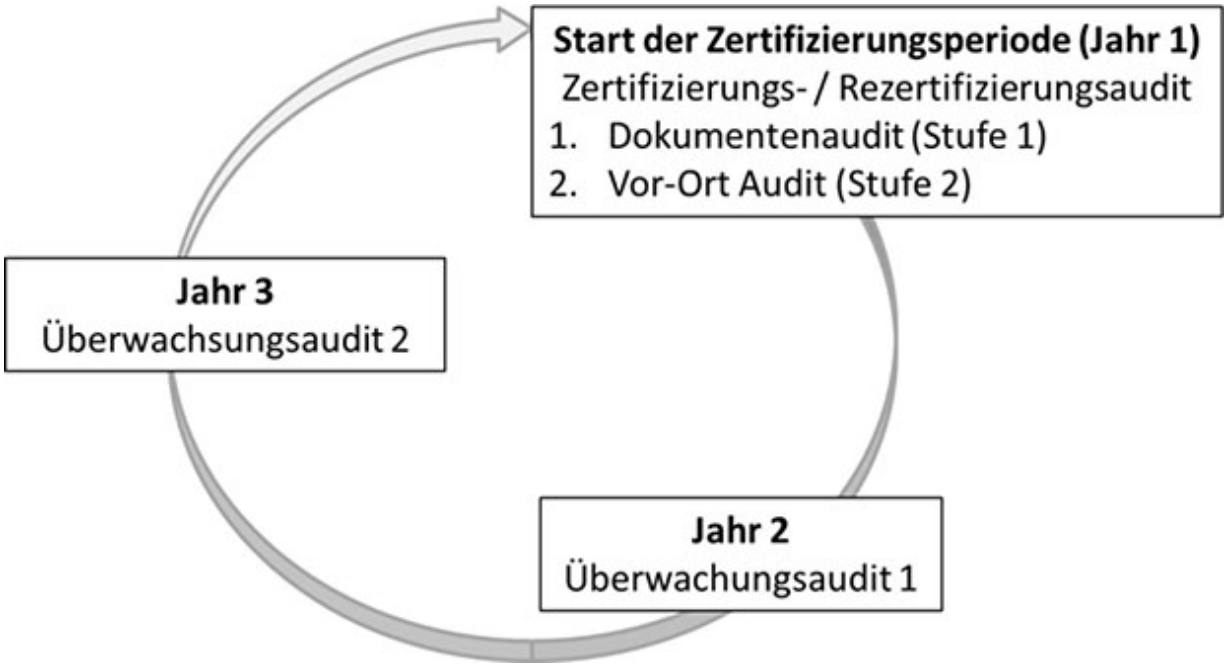

Abbildung 4: Zertifizierungszyklus

1.5 Machbarkeitsanalyse ISMS

Ein Koch mit asiatischem Erscheinungsbild sollte sich gut überlegen, ob er ein Restaurant mit deutscher Küche eröffnet. Umgekehrt mag das gerade noch gehen. Ein deutscher Koch der zum Beispiel ein italienisches Restaurant eröffnet, ist in Deutschland aufgrund der geografischen Nähe vielleicht noch angemessen.

Vertrauen auf eine gute Küche schafft jedoch auch das nicht.