Managementsysteme sind Balance-Systeme – Diskussion relevanter Kennzahlen eines ISMS gemäß ISO/IEC 27001:2005

Wolfgang Böhmer

Fachbereich Informatik, Kryptographie und Computeralgebra,
TU-Darmstadt,
Morneweg Str. 30, 64293 Darmstadt

1 Einleitung

Die ISO27001:2005 als Informationssicherheitsmanagementsystem (ISMS) etabliert sich zunehmend als der Sicherheitsstandard in Unternehmen. Die Grundidee des ISMS basiert auf einem Management der Informationssicherheit welches ausgerichtet ist auf dem Management der Unternehmensrisiken und einen direkten Bezug zum Firmenumsatz herstellt. Bis September 2009 wurden weltweit mehr als 5822[1] zertifizierte Unternehmen registriert. Zu berücksichtigen bleibt aber, dass diese Zertifizierung nichts über Güte und Performance eines ISMS[2] aussagt. Zur kontinuierlichen Verbesserung des ISMS kann der Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) und für vorbeugenden und korrigierenden Maßnahmen die Norm selbst herangezogen werden; es sind aber keine Messmethoden[3] vorhanden, mit denen Aussagen über die Abschätzung der Güte eines ISMS getroffen werden können.

In diesem Artikel wird eine Methode zur Messung der Qualität (Performance) eines ISMS vorgeschlagen und der Zielkonflikt zwischen Effektivität und Effizienz diskutiert.

In den folgenden Abschnitten dieses Beitrages wird behandelt: die relevante Literatur, die zu beantwortende Forschungsfrage, die Systemgrenzen, die Effektivität und Effizienz als Regelgrößen, die Balance-Matrix sowie der Zielkonflikt zwischen Effektivität und Effizienz. Der Beitrag endet sodann mit

[1] Quellenangabe http://www.iso27001certificates.com/ (abgerufen Sept. 2009).

[2] Die Norm beschreibt *was zu tun* ist, jedoch nicht *wie etwas zu tun* ist.

[3] Die SC27 entwickelt derzeit die ISO 27004. Diese Norm wird ein Messverfahren beinhalten. Eine Publizierung ist jedoch erst in den nächsten Jahren zu erwarten.

einer Zusammenfassung und einem Ausblick auf erste empirische Untersuchungen zur Verifizierung eines ISMS.

2 Relevante Literatur

Prozessorientierte Managementsysteme gewinnen zunehmend an Bedeutung. Zu nennen sind z. B. die ISO/IEC 9001:2008, die eine reine Prozessbetrachtung vornimmt und ein Qualitätsmanagementsystem postuliert. Ähnlich verhält sich die ISO/IEC 14001, die die Umweltrisiken im Fokus des Managementsystems hat. Auch die ISO/IEC 20000, die eine Automatisierung bzw. Standardisierung der IT-Produktion verfolgt, ist nach gleichem Muster aufgebaut. Die ISO/IEC 27001 spezifiziert ein Managementsystem, das die Risiken der Geschäftsprozesse. Die ISO/IEC 27001:2005 ist in enger Verzahnung mit der ISO 9001:2008 und dem dort definierten Qualitätsmanagementsystem (QM) entstanden (SC27, Beuth-Verlag, 2005). Nach der EN/ISO 9001:2008 werden allgemein die Geschäftsprozesse eines Unternehmens beschrieben, jedoch nicht nach Bedeutung oder Kritikalität bewertet oder gewichtet. Alle Prozesse sind nach der EN/ISO 9001:2008 gleich wichtig. Genau hier setzt ISO 27001:2005 an. Es werden in einem ISMS nach ISO 27001:2005 diejenigen Prozesse besonders behandelt, die maßgeblich (kritisch) zum Geschäftserfolg beitragen. Diese können z. B. unter dem Begriff Wertschöpfungskette subsumiert werden. Einen ähnlichen Ansatz verfolgt (Blakley et. al., S. 97-104). Ebenso definieren B. v. Solms und R. v. Solms (2005) einen direkten Zusammenhang zwischen Informationssicherheit und der Geschäftssicherheit (Business Security). Nach Schlüter und Dunkhorst (2001) kann ein Prozess ganz allgemein als eine logisch zusammenhängende Reihe von Aktivitäten zur Erreichung eines vorab definierten Zieles aufgefasst werden. Die Prozessziele, die Prozessdurchlaufzeiten als auch die Prozessverarbeitung können mittels der o. g. Beurteilungsgrößen gemessen werden. Ein Prozess muss also grundsätzlich zum Erreichen eines Zieles geeignet sein, d. h. er muss im Idealfall einen hohen Grad an Wirksamkeit aufweisen.

Zur Bewertung von Managementsystemen bzw. Prozessen stehen in der Literatur unterschiedliche Methoden zur Messung der Performance zur Verfügung.

1. Nach einer Methode, entwickelt von der Carnegie Mellon University, kann die Performance über den Reifegrad der Prozesse, z. B. Spice (ISO/IEC 15504) oder mittels CMMI gemessen werden. Dieser Ansatz findet einen weiten Zuspruch in technischen Umgebungen z. B. Produktionsumgebungen als auch bei Managementsystemen z. B. bei ITIL (ISO/IEC 20000) und ISO/IEC 27001.
2. Eine etwas neuere Methode besteht darin den Zustandsraum der Prozesse mittels Prozess Algebra zu beschreiben. Erste Überlegungen wurden von Brandt et. al. (2008) publiziert; die Tauglichkeit dieser Methode in der Anwendung eines Beispiels für den Business Continuity Prozess (BCP) wurde von Böhmer et al.

(2009b) publiziert. Eine umfangreiche Erläuterung ist in dem Technischen Report der Universität Eindhoven (Böhmer et al. 2009a) zu finden.

3. Eine weitere Methode besteht in der Abschätzung der Performance anhand von geeigneten Kennzahlen (KPI). Die Herausforderung besteht darin, geeignete Kennzahlen zu definieren, die eine entsprechende Aussagekraft haben. Vorschläge zur Handhabung von Kennzahlen sind z. B. bei Alemanni et al. (2008) oder auch bei Rodriguez et al. (2008) zu finden. Ein Kennzahlensystem für ein ISMS ist z. B. von Tsimas et al. (2009) entwickelt worden. Es fußt auf der BORIS-Methodologie, die einen Satz von verschiedenen Werkzeugen enthält. Ein ähnlicher Weg zu einem Kennzahlensystem wurde von Böhmer (2009b) für ein Business Continuity Managementsystem (BCMS) beschritten; ein Vorläufer dieses vorliegenden Ansatzes wurde in (Böhmer, 2008a) publiziert.

Der hier vorliegende Ansatz lehnt sich an (Böhmer, 2008a) an. Jedoch wird in diesem Artikel eine Weiterentwicklung des Kennzahlensystems unter der Fragestellung des Zielkonfliktes diskutiert. Der Zielkonflikt entsteht zwischen den konträren Zielen der Effektivität und der Effizienz. Ebenso wird hinterfragt ob die Interpretation eines Managementsystem (ISMS) als ein Art Balance-System.

3 Lösungsansatz: Kennzahlenbasiertes Balance-System

In diesem Abschnitt werden das Balance-System, die Systemgrenzen und die Schlüsselkennzahlen zur Performancemessung diskutiert. Abschließend wird die Zusammenführung der Schlüsselkennzahlen in der Balance-Matrix erläutert.

3.1 Ereignisdiskrete Systeme und Managementsysteme und der Balance-Zustand

Die Wertschöpfungskette kann als ereignisdiskreter Prozess bzw. Prozesskette aufgefasst werden. Diese wird mit einem ISMS durch den PDCA-Zyklus mit seinen Vier-Phasen (Plan-Do-Check-Act) betrachtet. Es wird ein Gleichgewichtszustand durch die kontinuierliche Verbesserung angestrebt (vgl. Abb.1). Die Messung der Zustände in dem PDCA-Zyklus wird durch die beiden Schlüsselkennzahlen $Ef\!k$ und $Ef\!z$ vorgenommen. Dabei gilt es zwischen Indikator und Schlüsselindikator zu unterscheiden.

Def. 1:	Ein Indikator (I) ist eine Variable, die einer Metrik unterliegt (vgl. z. B. Gl. 6 oder Gl.13).
Def. 2:	Ein Key Performance Indikator (KPI) ist eine Schlüsselgröße, die aus mehreren Indikatoren besteht und eine signifikante Aussage über einen bestimmten abgegrenzten Sachverhalt (Zustand) liefert (vgl. z. B. Gl. 12, oder Gl. 18).

Die beiden Schlüsselkennzahlen setzten sich wiederum aus jeweils drei Indikatoren zusammen. Für die Effektivität gilt beispielsweise, dass die Indikatoren

- der Existenz (I_{ex}),
- der Umsetzung (I_{op}) und

- der Vollständigkeit (I_{co})

die Menge bilden, aus der die Effektivität (*Efk*) abzuleiten ist:

$$Efk = \{I_{ex}, I_{op}, I_{co}\} \quad (1)$$

Die Indikatoren lehnen sich an die Level Dokumente (vgl. Abb. 3) an.
Die Norm fordert den Aufbau des Managementsystems nach dem PDCA-Zyklus (Plan-Do-Check-Act), wie dieser bereits ebenso in den Normen ISO 27001 und ISO/IEC 20000 und weiteren Normen gefordert wird. Dabei geht der PDCA-Zyklus von der Idee der Imperfektion aus und verfolgt einen kontinuierlichen Verbesserungsprozess. In der Check-Phase wird z. B. geprüft ob die Planung mit der gesetzten Zielsetzung noch im Einklang steht. Falls nein, werden Korrekturen in der Act-Phase vorgenommen.

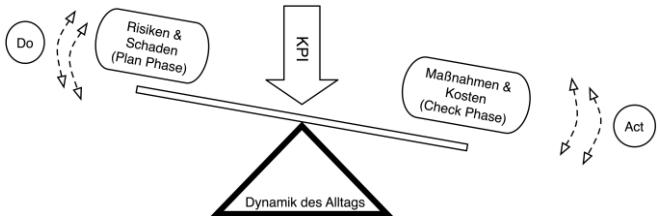

Abbildung 1: Balance System eines ISMS gemäß PDCA-Zyklus

Mittels des PDCA-Zyklus und dem geforderten kontinuierlichen Verbesserungsprozess lässt sich mit den definierten KPI der Zustand eines ISMS bestimmen. Hat der kontinuierliche Verbesserungsprozess einen Zustand erreicht, in dem keine Verbesserungen zu einem Zeitpunkt *k* mehr möglich sind, entsteht ein Gleichgewicht (vgl. Abb. 2).

Managementsysteme stellen nach der Auffassung des Autors den nächsten Entwicklungsschritt einer starren Richtlinien Orientierung (Policy) dar. Während sich reine Richtlinien[4] statisch verhalten, können Managementsysteme dynamisch auf Anforderungen bzw. Ereignisse mit einer Rückkopplung reagieren.

3.2 Indikatoren und Level-Dokumente als Grundlage eines Beurteilungssystems

In Abb. 3 wird gezeigt, wie die Level Dokumente von oben (Spitze) bis nach unten zunehmen. Diese Struktur zeigt den natürlichen Verlauf, ausgehend von einer Richtlinie (Policy) hin zu deren technischen oder organisatorischen Umsetzung (Prozeduren, Checklisten) und deren Nachweise der objektiven Umsetzung (*objective Evidence*). Diese pyramidenartige Struktur hat Alan Calder (2007) empirisch

[4] Dynamische Policies können zwar etwas flexibler reagieren, besitzen jedoch keine Rückkopplung wie ein Managementsystem.

abgleitet. Es werden vier verschiedene hierarchische Ebenen ($\lambda_1,\ldots, \lambda_4$) unterschieden, wie Abb. 3 illustriert.

Dabei wirkt die oberste Ebene λ_1 auf die nächst untere, bis schließlich die letzte Ebene λ_4 erreicht ist. Somit gilt z. B. für die definierten Policies (λ_1), dass diese Standards und Guidelines erfordern; diese sind auf der nächst unteren Ebene angeordnet. Standards und Guidelines erfordern Prozeduren zur Durchsetzung. Prozeduren ziehen wiederum Checklisten und Arbeitsanweisungen nach sich. Als Nachweis der Umsetzungen sind dann Aufzeichnungen auf der letzten Ebene (λ_4) in Form von Protokollen, Logaufzeichnungen und Daten vorhanden.

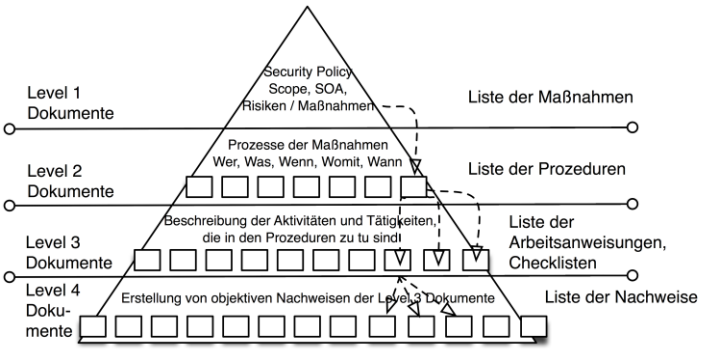

Abbildung 2: Struktur der Level Dokumente eines ISMS nach A. Calder

Diese vorliegende, durch die Dokumentation erzwungene, Struktur, dient als Grundlage, um die Wirksamkeit des ISMS zu prüfen. Weiterhin ziehen die Risikoentscheidungen (*avoid, mitigate, transfer, accept*) Kostenentscheidungen nach sich, die ggf. nach einem Fiskaljahr bei erneuter Betrachtung zu revidieren sind. Diese Struktur ist geeignet, um zu prüfen, wie wirksam und wirtschaftlich das ISMS tatsächlich ist.

3.3 Statusorientierte untere Messschranke der Effektivität

Ausgehend von den beiden o. g. Beurteilungsgrößen (Efk, Efz) können bezogen auf die Struktur der ISMS-Dokumentation für jeden Level (λ) Leistungsindikatoren (I_λ) definiert werden. Die Abb. 3 deutet durch die Dreiecksform an, dass von der Spitze (λ_1) bis zur Grundlinie (λ_4), die Anzahl (i) der Leistungsindikatoren pro Level zunimmt. Damit wird, der Forderung entsprechend, der Dreiecksform durch die Gl. (2) Ausdruck verliehen.

$$I_{\lambda_1}(i\ldots n) \leq I_{\lambda_2}(i\ldots m) \leq I_{\lambda_3}(i\ldots k) \leq I_{\lambda_4}(i\ldots l) \qquad (2)$$

Dies bedeutet, dass z. B. die Anzahl der Security Manuals (λ_1) und damit die Anzahl der quantitativen Leistungsindikatoren auf der Ebene I_{λ_1} in einem Unternehmen geringer sein müssen, als z. B. die Anzahl der quantitativen Leistungsindikatoren der Prozeduren auf der Ebene λ_2. Weiterhin wird postuliert, dass n, m, k, l mindestens dem folgenden Bildungsgesetz gehorchen muss und somit die Funktion einer unteren Schranke erfüllt.

$$m=(2n+1)-n;\ k=(2m+1)-n;\ l=(2k+1)-n \tag{3}$$

Damit sind die Zahlenfolgen (m_n, k_n, l_n) den monoton steigenden Zahlenfolgen zuzuordnen. Die Gl. (3) zeigt für verschiedene n wie sich nach dem Bildungsgesetz die untere Schranke für die vier Leitungsindikatoren verhalten. Um dies Bildungsgesetz für die quantitativen Leistungsindikatoren zu illustrieren, bedeutet z. B. für n=4, dass es mindestens fünf Leistungsindikatoren aus $I_{\lambda 1}$, sieben Leistungsindikatoren aus $I_{\lambda 2}$ und bereits elf Leistungsindikatoren aus $I_{\lambda 4}$ gebildet werden müssen.

Diese theoretische untere Schranke besagt, dass ein ISMS, das diese untere Schranke unterschreitet, hinsichtlich seiner Wirksamkeit nicht gemessen werden kann und außerhalb des Beurteilungssystems liegt. Allerdings beziehen sich die Parameter auf eine erste Abschätzung, die sich an die aufgezeigte hierarchische Struktur der Dokumentation der ISO 27001:2005 orientiert. Eine Überprüfung der unteren Schranke gegenüber der Realität muss noch durch empirische Untersuchungen verifiziert werden.

3.4 Statusorientierte obere Messschranke der Effizienz

Eine sinnvolle obere Schranke der Effizienz ergibt sich aus einer Kosten/Nutzen Relation bezogen auf den Risikoentscheidungen (*avoid*, *mitigate*, *transfer*, *accept*) für die kritischen Geschäftsprozesse und den daraus abzuleitenden Maßnahmen. Dabei beinhaltet R_G die Menge aller Risiken (Gesamtrisiko). Ausgehend von diesem Gesamtrisiko können eine Reihe von Risiken vermieden (R_{av}) werden, weitere werden verringert (R_{mi}) oder z. B. einem Versicherer übertragen, bzw. durch eine Fremddienstleistung (Outsourcing) erbracht (R_{tr}). Getragen bzw. akzeptiert werden die Restrisiken (R_{ac}). Die Gl. (4) listet die Komponenten des Gesamtrisikos auf.

$$R_G=R_{av}+R_{mi}+R_{tr}+R_{ac} \tag{4}$$

R_G hat eine monetäre Einheit. Als ein anzustrebendes Ziel für ein Unternehmen ist es, dass die Kosten für alle Maßnahmen (Prozesse, Tools, infrastruktelle Maßnahmen), die in dem SoA adressiert werden, geringer sind als die Kosten (z. B.

in Euro), die durch den möglichen Schadenseintritt von R_{av} und R_{mi} und R_{tr} und R_{ac} entstehen können. Die Gl. (5) zeigt diese Relation

$$SoA(€) \leq R_G\ (€) \tag{5}$$

Diese obere monetäre Schranke Gl. (5) kann dahingehend interpretiert werden, dass nicht mehr Kosten für die Absicherung der Risiken anfallen sollten, als die Werte der Assets bzw. der kritischen Prozesse der Wertschöpfungskette ausmachen. Eine ganz ähnliche Ansicht wird bei Sonnenreich et al. (2005) vertreten.

3.5 Bestimmung der Effektivität eines ISMS

Bei der Effektivität bzw. Wirksamkeit bezogen auf ein ISMS stehen eine Reihe von Fragen im Vordergrund. Die Fragen zielen auf die Absicherung der erkannten Risiken und damit auf die entsprechenden Maßnahmen ab.

Basierend auf den folgenden Fragen können Analysen der Wirksamkeit der Polcicies in einem Unternehmen vorgenommen werden:

- Existieren geeignete und ausreichende Policies sowie Prozeduren, die sich auf Standards oder Guidelines beziehen und werden diese angewendet (Umsetzungsgrad)? Ein Nachweis kann z. B. durch interne oder externe Audits erfolgen.
- Sind entsprechend den vorhandenen Policies geeignete und ausreichende Überprüfungspunkte (internal controls) eingerichtet worden (Operationalisierungsgrad/Durchsetzungsgrad)?
- Existieren zu allen kritischen Assets der Wertschöpfungskette entsprechende Policies zur Absicherung (Vollständigkeit)?

Die erste Kennzahl betrifft die Effektivität (vgl. Gl. 1), die durch drei Indikatoren bestimmt werden kann. Zum einen wird die Existenz der Policies pro Maßnahmen im SOA mittels Indikator (I_{ex}) bewertet, zum anderen wird der Durchsetzungsgrad der Policies mittels Indikator (I_{op}) bezogen auf die Maßnahmen betrachtet. Als dritter Indikator (I_{co}) wird die Vollständigkeit (Abdeckungsgrad) herangezogen. Dabei zeigt der Indikator bezogen auf den Scope des ISMS den Abdeckungsgrad der Risikoanalyse gegenüber den kritischen Geschäftsprozessen (cBP) an.

Der Indikator (I_{co}) bewertet die Existenz von Kontrollpunkten (Checkpoints, CP) bzw. nicht vorhandenen Kontrollpunkten (NoCP) bezogen auf ein ISMS. So sind die Clauses der ISO/IEC 27001, die in dem ISMS zur Anwendung kommen, mit Kontrollpunkten zu belegen, andernfalls kann keine Aussage über die Umsetzung des Standards getroffen werden. Dieser Sachverhalt der vorhandenen bzw. nicht vorhandenen Kontrollpunkte, pro Level, wird in der Gl. (6) dargestellt:

$$I_{ex} = \frac{\sum_{i=1}^{n} CP_{\lambda i} - \sum_{j=1}^{m} NOCP_{j(ISMS)}}{\sum_{i=1}^{n} CP_{\lambda i}} \tag{6}$$

Damit bewegt sich der Indikator des Kontrollpunktes zwischen den Eckwerten 0 und 1:

$$I_{ex} = \begin{cases} 1, falls NOCP = 0 \\ 0, falls \forall CP_{\lambda i} = 0 \\ sonst, \end{cases} \tag{7}$$

Für die ideale Existenz der Norm in einem Unternehmen ist nach Gl. (7) ein Indikator mit dem Wert $I_{ex} \approx 1$ anzustreben. Dies würde bedeuten, dass es keine Abweichungen ($NoCP \approx 0$) zwischen den Kontrollpunkten (Clauses) des Standards mit dem tatsächlichen Kontrollpunkten existieren. Im Fall von $I_{ex} \leq 1$ bedeutet dies, dass weniger Clauses des Standards zur Anwendung gekommen sind und ein Optimierungsbedarf besteht.

Die Existenz von Policies sagt jedoch wenig darüber aus, ob diese auch gelebt werden oder ob diese nur auf dem Papier existieren. Insofern stellt die Gl. 6 eine notwendige jedoch keine hinreichende Bedingung dar. Genau hier setzt der Indikator des Durchsetzungsgrades (I_{op}) an.

Der Indikator des Durchsetzungsgrads (I_{op}) prüft in der Gl. (8) inwieweit mittels Assessments Abweichungen zwischen den Maßnahmen, Prozeduren und Checklisten ($C_{\lambda i}$) und den nicht vorhandenen Umsetzungen (NoC) auf den Leveln existieren.

$$I_{op} = \frac{\sum_{i=1}^{n} C_{\lambda i} - \sum_{j=1}^{m} NOC_j}{\sum_{i=1}^{n} C_{\lambda i}} \tag{8}$$

Der Indikator bewegt sich zwischen 0 und 1 und ist analog zur Gl. (7) aufzufassen.

$$I_{op} = \begin{cases} 1, falls NOC = 0 \\ 0, falls \forall C_{\lambda i} = 0 \\ sonst, \end{cases} \tag{9}$$

Wichtig für die Effektivität ist die Frage ob tatsächlich alle kritischen Geschäftsprozesse hinsichtlich der Ressourcen mit einer Risikoanalyse, bezogen auf den Scope des ISMS, betrachtet wurden. Diese Betrachtung wird mit dem Indikator der Abdeckung beurteilt. Wenn sich innerhalb eines Betrachtungszeitraums die Anzahl der Assets ändert, haben sich die kritischen Geschäftsprozesse ebenfalls geändert. Zu den Assets gehören nach ISO 27001:2005 z. B. folgende Subjekte und Objekte: Schlüsselpersonen, Verträge, Applikation, Software, Image etc. Die Vollständigkeit hängt wiederum von der Qualität und Häufigkeit der Identifikation kritischer Geschäftsprozesse (*cBP*) ab. Durch regelmäßige Prüfungen (Audits) und unabhängige Audits (*external audits*) kann prinzipiell eine annähernde Abdeckung erzielt werden. Die Kennzahl der Gl.

(10) zeigt den Zusammenhang der (nicht) existierenden Policies (*NoSP*) zu kritischen Assets (*Asts*) und den kritischen Geschäftsprozessen (*cBP*):

$$I_{co} = \frac{\sum_{i=1}^{n} Asts(cBP)_i - \sum_{j=1}^{m} Asts(NoSP)_j}{\sum_{i=1}^{n} Asts(cBP)_i} \tag{10}$$

Die Gl. (10) setzt die kritischen Assets (*Asts)* die in der Risikoanalyse behandelt sein müssen mit den nicht vorhandenen Policies (*NoSP*) ins Verhältnis.

$$I_{co} = \begin{cases} 1, falls Asts(NoSP) = 0 \\ 0, falls \forall Asts(cBP) = 0 \\ sonst, \end{cases} \tag{11}$$

Der Indikator bewegt sich zwischen 0 und 1 und ist analog zur Gleichung 7 aufzufassen. Je weniger Risikoszenarien und Risikoanalysen für die kritischen Assets existieren, desto geringer ist der Abdeckungsgrad (I_{co}<1) der kritischen Prozesse und um so geringer fällt die Effektivität aus.

Abschließend kann aus den betrachteten Indikatoren die Effektivität (Efk) mit dem Kreuzprodukt der Gl. (12) berechnet werden.

$$Efk = I_{ex} \times I_{op} \times I_{co} \tag{12}$$

Die Schlüsselkennzahl (*Efk*) bewegt sich zwischen 0 und 1 und stellt einen Punkt in dem von den Indikatoren aufgespannten Raum (Kennzahlenraum) dar. Die Schlüsselkennzahl sagt etwas über die Wirksamkeit des ISMS und somit über die Risikoabwehr etwas aus. Die Schlüsselkennzahl liefert aufgrund der Indikatoren eine signifikante Aussage über einen Sachverhalt und erfüllt damit die 2. Definition. Diese Schlüsselkennzahl wird somit zu einer wertvollen Information für ein Unternehmen.

3.6 Bestimmung der Effizienz eines ISMS

Bei der Effizienz eines ISMS steht die Wirtschaftlichkeit der Absicherungen der kritischen Geschäftsprozesse bzw. deren Assets im Vordergrund. Die Wirtschaftlichkeit ist prinzipiell als Kosten/Nutzen-Relation zu bestimmen. Um für ein Unternehmen eine Planungssicherheit für das Budget der kritischen Prozesse zu bekommen, müssen sowohl die Infrastrukturkosten (Gl.14) als auch die Kosten zur Risikoabwehr (Gl. 15, Gl. 16, Gl. 17) betrachtet werden.
Einen geeigneten Blick auf die Kosten ermöglicht ein Total-Cost-of-Ownership Model (TCO-Modell). In dem TCO-Modell werden drei Kostenverursacher identifiziert. Zu nennen ist die Summe der direkten Kosten, die der indirekten Kosten und die der Betriebskosten.
Die drei erwähnten Kostenarten lassen sich wie folgt definieren:

- direkte Kosten ($\sum_i^n D_{ci}$): Mitarbeiter, Hardware, Software, Externe Services, physikalische Umgebungsbedingungen (Gebäude), in denen für eine

Organisation Informationsverarbeitung unter sicheren Bedingungen stattfinden soll. Außerdem ist neben der Anschaffung der Geräte, deren resultierender Werteverzehr zu beziffern.

- Betriebskosten ($\sum_j^m O_{cj}$): Unterhalt, Wartung Reparatur der unter direkten Kosten aufgezählten Komponenten.
- indirekte Kosten ($\sum_k^p I_{ck}$): Diese Kosten entstehen in Folge unproduktiver Nutzung durch den Endanwender. Dabei handelt es sich immer um Prozesse, Vorgänge oder Situationen, welche den Endanwender in seiner Produktivität hemmen. Hierunter fallen alle Ausbildungs- und Schulungskosten, Eigenentwicklungen (Excel-Tabellen).

Als Anpassung könnte das TCO-Modell, bezogen auf ein Fiskaljahr z. B. Fy_0, zum Zeitpunkt t_0, die Kosten bezogen auf die infrastrukturellen Maßnahmen der kritischen Geschäftsprozesse eines ISMS, bestimmt werden. Damit können für ein Fiskaljahr die infrastrukturellen Kosten wie folgt für ein ISMS ausgedrückt werden:

$$F_{y0} = \sum_i^n D_{ci} + \sum_j^m I_{cj} + \sum_k^p O_{ck} \tag{13}$$

Eine Veränderung (Iteration) lässt sich dann von einem Fiskaljahr Fy_0, zum Zeitpunkt t_0, bezogen auf das folgende Fiskaljahr (Fy_1), zum Zeitpunkt t_1, berechnen. Somit ergibt sich für die Kostenveränderung für die infrastrukturellen Maßnahmen eines ISMS der folgende Zusammenhang:

$$TCO_{I\,SMS} = \frac{F_{y1} - F_{y0}}{F_{y0}} \tag{14}$$

Neben den Infrastrukturkosten sind die Kosten für die Risikoabwehr zu betrachten. Denn ein wesentlicher Nutzen eines ISMS ist der gezielte Kostenumgang mit den erkannten Risiken. Es lassen sich zur Bestimmung der Wirtschaftlichkeit der Risikoabwehr eine Reihe von Fragen aufzeigen:

1. Welche der erkannten Risiken aus der Menge aller Risiken (R_G) lassen sich unter wirtschaftlichen Gesichtspunkten am ehesten vermeiden (R_{av})?
2. Welche der erkannten Risiken aus der Menge aller Risiken (R_G) lassen sich unter wirtschaftlichen Aspekten am ehesten vermindern (R_{mi})?
3. Welche der erkannten Risiken aus der Menge aller Risiken (R_G) lassen sich unter wirtschaftlichen Gesichtspunkten am ehesten transferieren (R_{tr})?
4. Welche der erkannten Risiken aus der Menge aller Risiken (R_G) lassen sich unter wirtschaftlichen Gesichtspunkten am ehesten akzeptieren (R_{ac})?

Es lassen sich für diese vier Fragen vier Handlungsalternativen aufzeigen, für die es gilt, Entscheidungen zu treffen. Somit ergeben sich gemäß den vier Handlungsalternativen die Kosten für R_{1cost}, R_{2cost} und R_{3cost}:

$$R_{1\cos t} = R_1 = \sum_{i=1}^n R_{av_i} \tag{15}$$

Die Gl. (15) beschreibt die Kosten (R_{1cost}),, die für die Vermeidung der Risiken veranschlagt werden.

$$R_{2cost} = R_2 = \sum_{j=1}^{m} R_{mij} \tag{16}$$

Die Gl. (16) beschreibt die Kosten (R_{2cost}), die für die Verminderung der Risiken veranschlagt werden.

$$R_{3cost} = R_3 = \sum_{k=1}^{p} R_{trk} \tag{17}$$

Die Gl. (17) beschreibt die Kosten (R_{3cost}), die für die Übertragung der Risiken veranschlagt werden. Für die akzeptierten Risiken (R_{ac}) lassen sich, solange diese nicht eingetreten sind, keine Kosten beziffern.

Im Abschnitt 3.4 wurde bereits eine obere Schranke definiert, die besagt, dass zumindest ein Kostengleichgewicht gemäß Gl. (5) bestehen muss, andernfalls wird das ISMS unwirtschaftlich betrieben. Diese einmalig festgestellte Wirtschaftlichkeit muss jedoch pro Fiskaljahr (*Fy*) neu bestimmt werden.

Für ein ISMS lässt sich das Gesamtrisiko (R_G) gemäß Gl. (4) aufgrund einer durchgeführten Risikoanalyse in einem Fiskaljahr z. B. (Fy_0) ableiten. Gemäß Gl. (4) eingeleitete Maßnahmen nach ISO/IEC 27002:2007 reduzieren dann die Risikosituation. Dieses Risikomanagement wird streng nach betriebswirtschaftlichen Konditionen vorgenommen. Wird im nächsten Fiskaljahr wiederum eine Risikoanalyse zum Zeitpunkt (Fy_1)durchgeführt, ergibt sich ggf. im Sinne der Schadensreduktion eine geringere Risikosituation. Hierfür kann es vielfältige Gründe geben. Einige sind nachfolgend aufgezählt:

- Die Prozesse zur Vermeidung der Risiken können optimiert werden.
- Die Prozesse und Maßnahmen zur Verminderung der Risiken können optimiert werden.
- Die Kosten für die Überwälzung des Risikos sind verändert (gestiegen, reduziert).

Hieraus ergibt sich ggf. eine Differenz für (RG), die mit einer Kostenveränderung für den Umgang der Risiken (mitigation, avoiding, transfer, accepting) zu erklären sind.

Die Kennzahl der Effizienz (Efz_k), die als wirtschaftliche Komponente bezogen auf einen Zeitraum (Δt) aufgefasst werden kann, kann im Vergleich von zwei Fiskaljahren ($\delta F \geq 0 = F_{y0} - F_{y1}$) für die Kosten der Risikoabwehr (R_{1cost}, R_{2cost} und R_{3cost}) und den infrastrukturellen Kosten Gl. (14) durch die Gl. 18 ausgedrückt werden.

$$Efz_k = \frac{\sum_{i=1}^{3} R_{icost} + F_{y0} - (\sum_{i=1}^{3} R_{icost} + F_{y1})}{\sum_{i=1}^{3} R_{icost} + F_{y0}} \tag{18}$$

Die Gl. (18) zeigt, dass die ($Efz_k \in R$) sowohl positive als auch negative Kennzahlen annehmen kann. Es wird jedoch in der Gl. (18) postuliert, dass im Fiskaljahr Fy_1 weniger Budget zur Risikoabwehr benötigt wird als im Fiskaljahr Fy_0, somit ist die Kennzahl i. d. R.. positiv. Wird mehr Budget ausgegeben als im Vorjahr, entsteht eine negative Kennzahl.
Aus diesem Abschnitt wird deutlich, dass Risikomanagement einem Kostenmanagement entspricht und ein Sicherheitsmanagement (ISMS) nach ISO 27001 ein Risikomanagement beinhaltet.

3.7 Balance-Matrix der Effektivität und Effizienz eines ISMS

Um die Güte bzw. die Key-Performance eines ISMS bestimmen zu können, müssen die Kennzahlen der Effektivität und die der Effizienz ins Verhältnis gesetzt werden. Damit wird neben der Wirksamkeit eines ISMS auch die Wirtschaftlichkeit gleichwertig berücksichtigt. Die effektive Absicherung der Informationswerte und dessen effiziente Durchführung können in einer Matrixdarstellung der Kennzahlen, bei der die eine Achse die Kennzahl der Effektivität des Informationssicherheitsmanagements und die andere Achse die Kennzahl der Effizienz des ISMS aufspannt, dargestellt werden. Die Kennzahlen der Effektivität und die der Effizienz bewegen sich jeweils zwischen $0 \leq Efk_k \leq 1$ und $-1 \leq Efz_k \leq 1$. Als erste lineare Näherung kann für die Effektivität definiert werden:

$$Efk_k = \begin{cases} ja = 0{,}5 < 1 \\ nein = 0 < 0{,}5 \end{cases} \tag{19}$$

Überschreitet die Kennzahl den Wert von 0,5 bewegt sich demzufolge das ISMS im positiven Bereich (Ja). Tritt der Fall ein, dass die Kennzahl unterhalb von 0,5 erreicht wird, wird ein (Nein) vergeben. Eine ähnliche Fallunterscheidung kann für die Kennzahl der Effizienz getroffen werden:

$$Efz_k = \begin{cases} ja = 0 < 1 \\ nein = -1 < 0 \end{cases} \tag{20}$$

Die Abschätzungen zu den Fallunterscheidungen müssen noch empirisch verifiziert werden. Vermutlich werden bei entsprechenden Untersuchungen in der Praxis prinzipiell alle möglichen Kombinationen der Gl. (19) und Gl. (20) beobachtbar sein. In der Abb. 3 sind die vier Fälle dargestellt.

Effektiv / Effizient	Ja	Nein
Ja	**IV: ISMS ist effektiv und effizient**	**I: ISMS ist effektiv und nicht effizient**
Nein	**III: ISMS ist nicht effektiv aber effizient**	**II: ISMS ist weder effektiv noch effizient**

Abbildung 3: Balance-Matrix eines ISMS

Die nachfolgenden Balance-Zustände sind in Anlehnung an den von (Heinrich und Lehner, 2005) entworfenen vier Feldern zur Zustandsbeschreibung eines IMS[5] definiert worden.
Als idealer ausbalancierter Zustand eines ISMS lässt sich der Zustand IV beschreiben.

- *Balance-Zustand IV*: Das ISMS ist effektiv und effizient, es ist in einem strategischen Gleichgewicht: Der Einsatz von Informationssicherheitsmaßnahmen unter dem Aspekt der Wirtschaftlichkeit befindet sich im strategischen Gleichgewicht, wenn der Einsatz der Absicherungsmaßnahmen effektiv und die Maßnahmen vollständig effizient erfolgen. Das ISMS-Leistungspotential unterstützt wirksam die IT-Strategie durch die richtigen Absicherungsmaßnahmen, während die Absicherungsmaßnahmen gleichzeitig durch ein optimales Kosten-/Leistungsverhältnis gekennzeichnet sind.

Neben dem strategischen Gleichgewicht existieren drei Arten des Ungleichgewichts, wie (Heinrich und Lehner, 2005, S.88 ff) für ein IMS definiert. Angewendet auf ein ISMS, wie in Abb. 3 dargestellt, bedeutet dies für ein ISMS, dass die Zustände II, III, und IV sich im Ungleichgewicht befinden:

- *Ungleichgewichtszustand I:* ISMS ist effektiv und nicht effizient, entspricht einer strategischen Verschwendung: Diese Unternehmenssituation ist dadurch gekennzeichnet, dass die Effektivität durch den Einsatz von Informationssicherheit hoch ist, die Effizienz der Informationssicherheit jedoch nicht erreicht wird.
- *Ungleichgewichtszustand II:* ISMS ist weder effektiv noch effizient, entspricht einem strategischen Dilemma (Heinrich und Lehner, 2005, S.88 ff): Der Einsatz eines ISMS sowie sein Leistungspotential sind beim strategischen Dilemma weder effektiv noch effizient.
- *Ungleichgewichtszustand III:* ISMS ist nicht effektiv aber effizient, entspricht einer strategischen Vergeudung: Bei der strategischen Vergeudung ist die Effizienz eines ISMS hoch, die Effektivität eines ISMS allerdings sehr tief. Das

[5]IMS ist die Abkürzung für ein Information Management System

Leistungspotential eines ISMS wird nicht genügend ausgeschöpft noch richtig erkannt.

Der Zustand IV ist der erwünschte Zustand, beim Zustand III muss von einer Scheinsicherheit ausgegangen werden, Zustand II ist der *worst case*, hohe Kosten bei ungenügender Sicherheit. Zustand I dürfte ebenso in der Realität vorkommen.

Es wird durch den Balance-Zustand IV deutlich, dass das Risikomanagement einem Kostenmanagement entspricht und ein Sicherheitsmanagement (ISMS) nach ISO 27001 einem Risikomanagement.

Aus Sicht der Effizienz (*Efz*) ist ein Minimum anzustreben, um das Budget eines Unternehmens, dass für die Risikoabwehr bereit gestellt werden muss, zu schonen. Denn jede Ausgabe reduziert den Gewinn des Unternehmens. Durch die Einführung einer Budgetgrenze müsste die Effektivität gegen die Effizienz optimiert werden. Es entsteht ein Zielkonflikt der im nächsten Abschnitt diskutiert wird.

4 Zielkonflikt zwischen Effektivität und Effizienz

Um die Wertschöpfungskette optimal abzusichern könnte nun die Forderung aufgestellt werden, die Effektivität zu maximieren. D.h. für alle Policies, die aus dem Statement of Applicability (SoA) abgeleitet wurden, ist die Anzahl der Prozeduren und Arbeitsanweisungen zu maximieren. Damit würde eine maximale Reduzierung der Gesamtrisiken (vgl. Gl. 4) erzielt werden. Diese Forderung überschreitet jedoch typischerweise das kalkulierte Budget nach Gl. (5). Das eingeführte Budgetlimit von 30% bezieht sich auf die in der Arbeit von Soo Hoo (Soo Hoo, 2000) empirisch ermittelte Obergrenze. Denn mittels der Effizienz wird versucht die Absicherung der Wertschöpfungskette hinsichtlich der Investitionen zu minimieren, um den Umsatz möglichst wenig zu reduzieren.

Dieser Zielkonflikt lässt sich als eine Variante des Knapsack Problems interpretieren wie Böhmer ausführt (Böhmer, 2009a). Dabei gehört das Knapsack Problem zu den ganzzahligen und kombinatorischen Problemtypen, den *NP–schweren* Problemen.

Der Darstellung des 0-1 Knapsack folgen Martello und Toth (vgl. Martello und Toth, S. 5). Übertragen auf den vorliegenden Zielkonflikt der Effektivität und Effizienz bedeutet dies, dass durch die vorgegebene Investitionsobergrenze ein Optimum der Absicherung der Wertschöpfungskette gefunden werden muss. In diesem 0-1 Knapsack Problem werden 1 bis n Policies, Prozeduren und Checklisten ausgesucht, die x_j (j = 1,…, n) die das Gesamtrisiko reduzieren.

$$x_j = \begin{cases} 1 = \forall j \\ 0 = sonst \end{cases} \tag{21}$$

Weiterhin gilt, in Anlehnung an Martello & Toth, dass pj die Policies beinhalten und wj die Reduktion von einem oder mehreren Risiken durch Gegenmaßnahmen (xj)aus dem SoA. Dabei sind diejenigen Polices, die mehr als ein Risiko reduzieren wertevoller gegenüber anderen. Unter c wird die Kostenobergrenze nach Soo Hoo verstanden. Es wird nun versucht von allen x diejenigen zu finden, für die gilt:

$$\sum_{j=1}^{n} = w_j x_j \leq c \tag{22}$$

Dabei wird die beste Ausnutzung der Policies zur Risikoreduzierung diejenige sein, die mehr als ein Risiko reduziert und gemäß Gl. (13) moderat ist, indem die Funktion

$$\max .z = \sum_{j=1}^{n} p_j x_j \tag{23}$$

gebildet wird. Unter p_j sind diejenigen Prozeduren und Checklisten zu verstehen, die den Risiken entgegen wirken. Der Wert w_j kann dahingehend auf den vorliegenden Sachverhalt interpretiert werden, dass der Wert derjenigen p_j steigt, wenn diese mehr als ein nur Risiko vermindern.
Wegen der Komplexität des 0-1 Knapsack Problems wird ein heuristisches Verfahren vorgeschlagen. Bei Martello & Toth werden verschiedene Heuristiken diskutiert. In diesem Beitrag wird in erster Näherung aus dem Branch-and-Bound (BB) Verfahren der Horowitz-Sahni Algorithums (HS) favorisiert. Das Branch-and-Bound Verfahren basiert im Wesentlichen auf einer Problem-Verzweigung und einer Beschränkung mittels eine unteren und oberen Grenze für die Teilmenge.

4.1 Verzweigung

Dabei beruht das Grundprinzip des Branch-and-Bound Verfahren auf einer Minimierung. Es wird eine Verzweigung des Problems (P_0) vorgenommen und hier in k=3 Teilprobleme P_i (i=1,…, k) verzweigt, so dass für die Mengen (x_j) der zulässigen Lösungen gilt:

$$x(P_0) = \bigcup_{i=1}^{k} x(P_i) \tag{24}$$

Als Teilprobleme bieten sich diejenigen Maßnahmen an, die den Risiken, wie in den Gleichungen 15, 16 und 17 beschrieben, entgegen wirken. Damit existieren die Teilprobleme $P_{1(avoid)}$, $P_{2(miti)}$, $P_{3(trans)}$.

4.2 Beschränkung

Weiterhin erfolgen Beschränkungen jeder Teilmenge durch eine untere Schranke (LB) und eine bekannte obere Schranke (UB). Gilt nun LB □ UB für eine Lösungsmenge, so wird diese Lösungsmenge nicht weiter betrachtet (Eliminierung uninteressanter Teilmengen). Für den Zielfunktionswert einer optimalen Lösung

von P0 bestimmt man heuristisch eine obere Schranke. Als obere Schranke könnte das eingeführte Budgetlimit von 30% des möglichen Schadens dienen. Dabei ist UB im Laufe des Verfahrens durch die jeweils beste bekannte Lösung von P0 gegeben und wird bis zum Minimum verringert. Ist nun LBi<UB und ggf. die optimale Lösung P'1 und ggf. zulässig für Pi bzw. P0, dann ist eine neue bisher beste Lösung für P_0 gefunden und es wird UB:=LBi gesetzt.

Abschließend wird exemplarisch ein HS Algorithmus gerechnet. Dieser wurde mit dem Fortran Programm, das dem Buch von Martello & Toth beiliegt, mit den nachfolgenden Daten berechnet. Es wurde der Horowitz-Sahni Algorithmus für eine Menge von Policies (P_{ol}) auf dem ersten Level $I_{\lambda 1}$ bestimmt. Die Menge der Policies besteht aus n=7 Richtlinien (x_j, j = 1,…, 7). Die aktuelle Lösung wird durch $\hat{z}$, $\hat{}$ dargestellt und die beste Lösung durch z^*. Für dieses gegebene Beispiel sieht die Berechnung wie folgt aus:

p= {70, 20, 39, 37, 7, 5, 10} mitigieren die Risiken. Es wird eine Risikoskala von 1,...,100 Einheiten verwendet. Um den Risiken mit Maßnahmen zu begegnen (vgl. Gl. 24), wird ebenfalls für die Maßnahmen eine Skala von 1,...,100 Einheiten verwendet. Es gilt somit

w= {31,10,20,19,4,3,6}.

c= {50} ist die Kapazität des Knapsack.

Es lässt sich für diesen Fall zeigen, dass die iterative Lösung gerade x_7 ist.

5 Diskussion der Ergebnisse, Zusammenfassung und weitere Untersuchungen

In diesem Beitrag wurde gezeigt, dass sich mittels Kennzahlen der Effektivität und der Effizienz die Performance eines ISMS gemäß ISO 27001 messen lässt. Dabei kann nur eine Messung vorgenommen werden, wenn eine definierte untere und obere Schranke eingehalten wird. Innerhalb dieser Schranken lässt sich die Performance messen. Für die Bestimmung der Kennzahlen der Effektivität und der Effizienz sind mehrere Parameter definiert worden. Jedoch werden Effektivität und Effizienz strikt getrennt betrachtet. Gemeinsam ist ihnen lediglich, dass jeweils der gleiche Betrachtungszeitraum zu Grunde gelegt wird. Dabei bewegt sich die Kennzahl der Effektivität zwischen $0 \leq Efk \leq 1$. Die der Effizienz zwischen $-1 \leq Efz \leq 1$. Es können aufgrund der Gl. (20) und der Gl. (19) vier Fälle unterschieden werden. Die Performance Matrix (Abb. 3) stellt die vier unterschiedlichen Fälle der Kennzahlkombination dar. Als idealer Fall lässt sich ein strategisches Gleichgewicht ermitteln, wenn der Einsatz der Sicherungsmaßnahmen nachgewiesen wirkungsvoll ist und die Kosten bezogen auf die Maßnahmen von Fiskaljahr zu Fiskaljahr abgenommen haben. Weiterhin wurde der Zielkonflikt zwischen der Effektivität und Effizienz untersucht. Es lässt sich für ein Beispiel

zeigen, dass eine iterative Lösung durch die Anwendung eines Knapsack-Problems erzielbar ist.

Literatur

Alemanni M, Alessia G, Tornincasa S, Vezzetti E (2008) "Key performance indicators for plm benefits evaluation: The alcatel alenia space case study," Comput. Ind., vol. 59, no. 8, pp. 833–841.

Blakley B, McDermott E ,Geer, D (2001) Information security is information risk management, in NSPW '01: Proceedings of the 2001 workshop on New security paradigms, (New York, NY, USA), pp. 97–104, ACM.

Böhmer W (2009) "Cost-benefit trade-off analysis of an ISMS based on ISO 27001," ARES Conference, The International Dependability Conference, pp. 392 –399, March, 16th. – 19th. Fokuoka, Japan.

Böhmer W (2008) "Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001," Emerging Security Information, Systems, and Technologies, The International Conference on (SECUWARE 2008), Nizza, France, Vol. 0, pp. 224–231.

Böhmer W (2009) "Survivability and business continuity management system according to bs 25999," Proceedings of the Emerging Security Information, Systems and Technologie, 2009. SECUWARE '09, Third International Conference on, pp. 142–147, June, 18-23, Athen, Greece.

Böhmer W, Brandt C, Groote J F (2009) "Evaluation of a business continuity plan using process algebra and modal logic," in 2009 IEEE Toronto International Conference – Science and Technology for Humanity TIC-STH 2009 - SIASP 2, pp. pp. 147–152, Ryerson University, 245 Church Street, Toronto, Ontario, Canada.

Böhmer W, Brandt C, Groote J F (2009) "Evaluation of a business continutiy plan using process algebra and modal logic," Computer Science Report CSR-09-12, Eindhoven University of Technology.

Brandt C, Engel T, Böhmer W, Roeltgen C (2008) "Diskussionsvorschlag einer Lösungsskizze zur Behandlung von operationellen IT-Sicherheitsrisken nach Basel II auf der Grundlage von Anforderungen der Credit Suisse," in Multikonferenz Wirtschaftsinformatik, MKWI München.

Calder A (2007), "PDCA cycle & documentation pyramid." IT Governance: a Manager's Guide to Data Security and ISO27001/27002, ISMS Toolkit.

Heinrich L, Lehner F (2005) Informationmanagement, Planung, Überwachung und Steuerung der Informationsinfrastruktur. Oldenbourg Verlag, 8. Auflage, S. 84-91, München.

Hoo, K S (2000) How Much is Enough? A Risk Management Approach to Computer Security; PhD. thesis. PhD thesis, Stanford University, CRISP.

Martello S, Toth P (1990) Knapsack Problems, Algorithms and Computer Implementations. ISBN 0471924201, John Wiley and Sons Ltd.

Rodriguez R R, Saiza J J A, Basa A O (2008), "Quantitative relationships between key performance indicators for supporting decision-making processes," Computer in Industry.

Schlüter S, Dunkhorst P (2001) ISO 9001:2000.: Qualitätsmanagement praxisgerecht einführen und weiterentwickeln. Behr's Verlag, , p. 13 – 15.

von Solms B and von Solms, R. (2005), "From information security to ... business security?," Computers & Security, vol. 24, pp. 271 – 273.

Sonnenreich W, Albanese J, Stout B (2008), "Return on security investment (ROSI) - a practical quantitative model," Journal of Research and Practice in Information Technology, vol. 38, Nr. 1, pp. p. 45–56.

Tsinas L, Trösken B, Sowa S (2009) "KPI-Framework für Informationssicherheit".