Informationssicherheitsmanagement-System nach ISO 27000

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Nonnsen Vorname: Sönke

[redacted] [redacted]

Erstprüfer: Prof. Dr. Breitner

Hannover, den 13.11.2007

Inhaltsverzeichnis

1 Einleitung

Der Einsatz moderner Informationstechnologie (IT) in Unternehmen hat in der Vergangenheit einen immer größeren Stellenwert eingenommen. IT ersetzt und ergänzt klassische Technologien, z. B. das klassische Telefon durch Voice-over-IP (VoIP), und hebt auf diesem Weg unentdeckte Effizienzen. Die erfolgreiche Implementierung und Nutzung von IT ist ein allgemein gültiger Wettbewerbsfaktor geworden. Die Wandlung des Unternehmens, um zukünftigen Anforderungen gerecht zu werden, sowie die Gestaltung neuer, den Unternehmenswert steigernder, Produkte und Services, ist ohne den Einsatz moderner IT kaum vorstellbar. IT wird praktisch in sämtlichen Bereichen moderner Unternehmen eingesetzt. Die Kommunikation mit Kunden und Lieferanten wird über E-Mail und andere IT abhängige Kanäle realisiert. Viele Tätigkeiten können dank moderner IT-Infrastrukturen standortunabhängig ausgeübt werden. Somit kann IT zu Recht das Potenzial zugesprochen werden Haupttreiber des ökonomischen Wachstums im 21sten Jahrhundert zu werden [1]

Der Unternehmenswert setzt sich zu immer größeren Teilen aus immateriellen Vermögenswerten (Information, Wissen, Erfahrung, Image, Vertrauen, Patente, etc.) zusammen. Dieser Bedeutungszuwachs Immaterieller Vermögenswerte hätte ohne IT nicht stattgefunden, denn IT wird benötigt um diese Vermögenswerte speichern, verteilen und beschützen zu können. Hier liegt allerdings auch die größte Gefahr dieser Entwicklung begründet. Während Materielle Vermögenswerte sich durch Wegschließen oder ähnliche Verfah-

[1] Vgl. “IT Governance für Geschäftsführer und Vorstände“, IT Governance Institut (ITGI), 2003, Seite 15, http://www.isaca.org Anmerkungen: Das ITGI hat unter anderem die Control Objectives for Information and related Technology (COBIT) entwickelt, an denen sich weltweit führende Prüfungsgesellschaften orientieren.

ren schützen lassen, ist dies bei Immateriellen Vermögenswerten weitaus schwieriger. Je mehr der Unternehmenswe rt sich aus diesen schwer zu fassenden und kompliz iert abzugrenzenden Werten zusammensetzt, desto i n-stabiler ist das Unternehmen selbst. Um das Unternehmen und s eine Werte in einem solchen Szenario zu schützen, ist wirksames IT-Sicherheitsmanagement von besonderer Bedeutung.[2]

Die sich vergrößernde Abhängigk eit von IT bringt, wie oben schon angedeutet, neue und umfängliche Ris iken mit si ch. In der heutigen Geschäftswelt, die sich Global, 24 Stunden täglich und an 365 Tagen im Jahr abspielt, sind auch die Bedrohungen Global und stets Präsent. Der Angriff oder die Bedrohung kann von entfernten Länder n, z. B. üb er das Internet, zu Zeiten, an denen der Geschäftsbetrieb des bedrohten Unternehmens ruht und die Mitarbeiter selig schlafend zu Hause liegen, stattfinden.

IT wird aber nicht nur zum managen von Unternehmensressourcen genutz t sondern ist selbst Bestandteil dieser geworden. Informationen bilden nicht nur die Grundlage für die Vorbereit ung und Ausges taltung von Transaktionen, sondern stellen einen wichtigen Faktor im Wettbewerb zwischen Unternehmen dar. Unternehmerische Ideen und un ternehmerischer Erfolg resultieren aus einem Informationsvorsprung gegenüber anderen Wirtschaftssubjekten.“[3]

Die geschilderte Bedeutung moderner IT is t heutzuta ge nicht wirklich neu und wird auch nicht geleugnet. Leider is t vielen Verantwortlichen die Bedeu-

[2] Vgl. “IT Governance für Geschäftsführer und Vorstände“, IT Governance Institut (ITGI), 2003, Seite 15, http://www.isaca.org Anmerkungen: Das ITGI hat unter anderem die Control Objectives for Information and related Technology (COBIT) entwickelt, an denen sich weltweit führende Prüfungsgesellschaften orientieren.

[3] Vgl. Picot, Reichwald, Wigand, S. 29: Die grenzenlose Unternehmung: Information, Organisaiton und Management. Lehrbuch zur Unternehmensführung im Informationszeitalter. 2. Aufl., Gabler, Wiesbaden 1996.

tung einer sicheren IT und der damit verbundenen W erte nicht ganz so bewusst. Dies kann viele Gründe haben, es lä sst sich aber vermuten, dass die Verwundbarkeiten und die Gefa hren denen IT-Um gebungen g egenüber stehen, den Entscheidern nicht im nötigen Maße bekannt sind od er unterschätzt werden.

Jeder Eigentümer, der sein Haus in der Nähe eines F lusses errichtet, würde, die Bedrohung durch eine Flut vor Augen, seine „Verteidigungsanlagen“ verbessern, um sein Eigentum zu schütz en. Dabei würde es nicht reichen, einfach nur die Eingangstür zu versch ließen. Das Wass er würde durch jede auch noch so kleine Lücke in der Ve rteidigung dringen. Für einen wirkungsvollen Schutz müssten sämtliche bekannt en „Lücken“ abgedic htet und ein Wall rund um das Haus zu errichtet werden. Diesen Wall würde er wahrscheinlich höher bauen als nötig, um auch gegenüb er extremen und unv orhergesehenen Fluten geschützt zu sein . So wie es für den Hausbesitzer selbstverständlich ist, sein Eigentum gegen Bedrohungen und Naturgewalten zu schützen, so wichtig sollte der Schutz der Immateri ellen Werte sowie der IT in Unternehmungen genommen werden.

Gegen die gängigsten Gefahren wird, auf Grund von in der Vergangenheit liegenden Vorfällen, immer mehr getan. Firewall- und Virenschutzprogramme zählen zu den Standard Instrumenten der Gefahren Abwehr, gegenüber Angriffen von Außen. Auch Feuers chutz und physische Zugangsk ontrollen, zu sensiblen Bereichen der Information sverarbeitung, haben in modernen Unternehmen Einzug gefunden. Ein immer wichtiger werdenden Bereich stellt die Abwehr gegenüber inneren Gefahren dar. Der Schutz interner und sensibler Daten wird für viele Unternehm en, zu einem W ettbewerbsfaktor. Ein Aspekt der inneren Sicherheit sind auch Irrtum und Nachläss igkeit der e ige-

nen Mitarbeiter. Nicht umsonst rangiert dieser Bereich an erster Stelle, bei einer Umfrage der Zeitschrift KES aus dem Jahr 2006, unter IT Managern.

Abbildung 1-1Bedeutung der Gefahrenbereiche KES Studie 2006[4]

Bedeutung	**heute**	**Schäden**		
	Rang	Priorität	Rang	Ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,52	1	49 %
Malware (Viren, Würmer etc.)	2	1,06	4	35 %
Software-Mängel 3		0,6	2	46 %
Hardware-Mängel	4	0,55	3	45 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	5 0,5		7	12 %
Unbeabsichtigte Fehler von Externen	6	0,39	5	30 %
Mängel der Dokumentation	8	0,27	6	20 %

Irrtum und Nachlässigkeit der eigenen Mi tarbeiter rangiert bei den Befragten an erster Stelle, wenn es um IT-Sic herheit geht. Nicht nur das, bei jedem

[4]Leicht verändert und gekürzt übernommen aus KES – Die Zeitschrift für Informations-Sicherheit Nr. 2006 #4,5,6

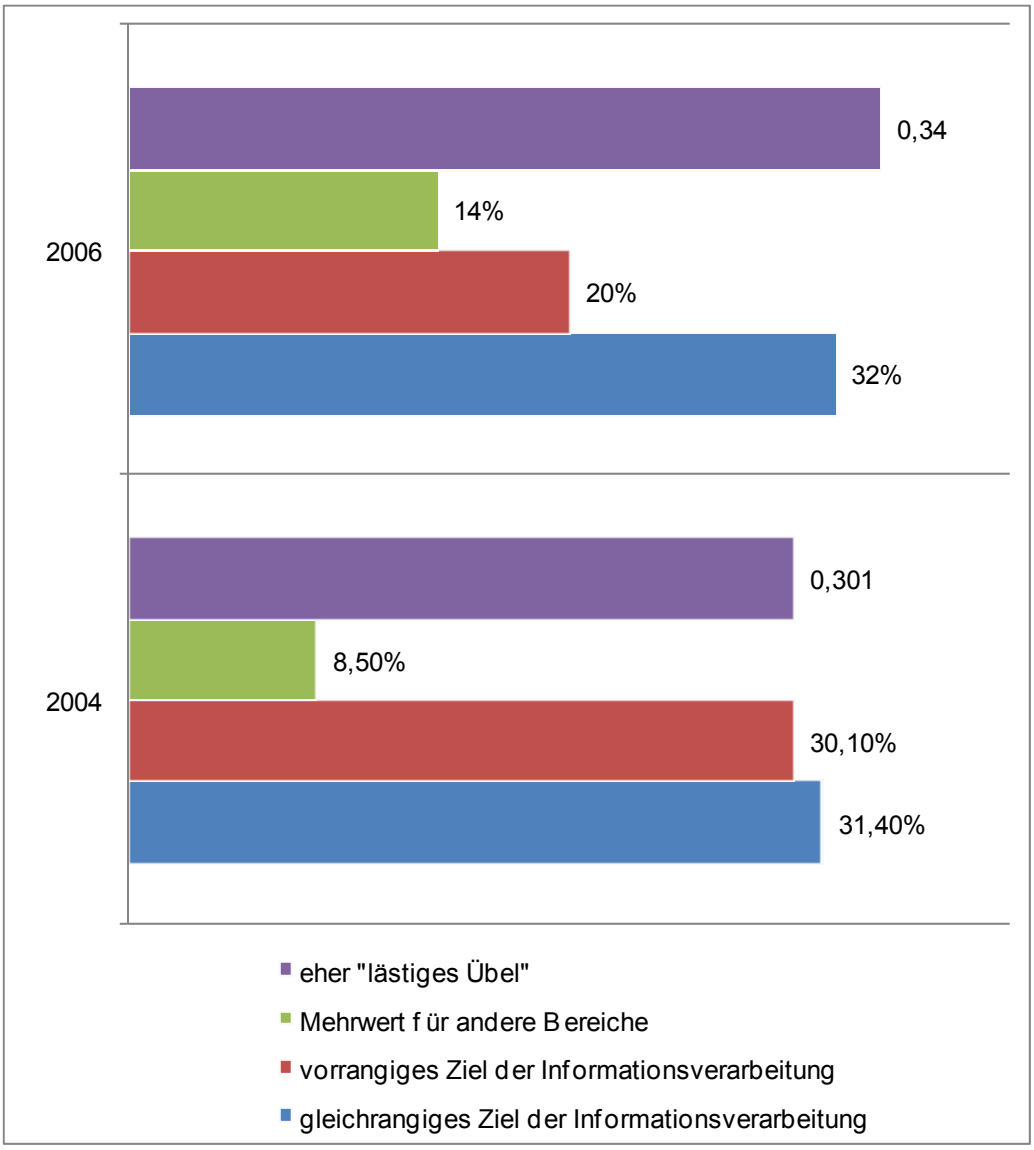
zweiten zog ein solcher Sicherheitsvorfall einen Schaden für das Unternehmen nach sich. Dies ist eine wichtige Erkenntnis. Während bei Angriffen von Malware nur 35 % der Befragten, trotz einer hohen Priorisierung und steigender Thematisierung des Themas, einen Schaden melden konnten. Daraus lässt sich schlussfolgern, dass die Häufigkeit bzw. die Präsenz eines Themas in der Öffentlichkeit, nicht gleichbedeutend mit den potenziellen und tatsächlichen Schäden, die entstehen können, ist. Software und Hardware defekte wiegen, bei Schadensereignissen, weitaus schwerer. Auch Mängel in der Dokumentation oder unbeabsichtigte Fehler von Externen machen in diesem Bereich einen hohen Stellenwert aus.

Das heißt, mit Firewall- und Virenschutzprogrammen, die hauptsächlich gegen Malware schützen, ist dem Thema Informationssicherheit in Unternehmen nicht genüge Getan. Eine ergänzende Schlussfolgerung der Umfrage Ergebnisse könnte sein, dass die eingesetzten Programme zur Gefahrenabwehr erfolgreich arbeiten und die Schadensquote trotz der hohen Angriffsquoten erfreulicherweise niedrig ist.

Dies würde mit Abbildung 1-2 korrespondieren, wonach IT-Sicherheit für viele ein eher lästiges Übel ist. Diese Sichtweise lässt auf ein „notwendiges“ Reagieren der Unternehmen auf Bedrohungen, wie z. B. Malware, schließen. Das Nutzen moderner Kommunikationsformen bedingt die beschriebenen Sicherheitsrisiken und erfordert den Einsatz entsprechender Maßnahmen.[5]

[5] Vgl. KES – Die Zeitschrift für Informations-Sicherheit Nr. 2006 #4,5,6 und 2004

Abbildung 1-2 KES/Microsoft Sicherheitsstudie 2004/06



Die Studie zeigt weiterhin, wie zwiespältig die Sichtweise auf IT-Sicherheit ausfällt. Während 2004 noch 30,1 % der Befragten IT-Sicherheit als vorrangiges Ziel der Informationsverarbeitung sahen sind es 2006 nur noch 20 %. Ein Erklärungsgrund mag die gleichzeitige Steigerung des Mehrwerts für andere Abteilungen sein. 14 % der Entscheider sehen IT-Sicherheit als Mehr-

wert generierenden F aktor. Dies könnte de r Teil der Manager sein, die IT-Sicherheit, über die bisherigen Grenzen der Malware Bekämpfung hinaus, zu einem Systemischen und ganzheitlichen An satz erweitern. Denn nur so kann IT-Sicherheit über die Grenzen des „l ästigen Übels“ hin aus e inen Beitrag zum Unternehmenserfolg leisten.

Einen weiteren Aspekt der IT-Sicherheit stellen di e regulatorischen Anforde - rungen an Unternehmen und Ihre Entschei der dar. Beispiels weise zählen dazu, der Sarbanes Oxley Act (SOX) aus den USA, das deutsc he KonTraG oder auch Basel II.

„Das KonTraG präzisiert und erweiter t dabei hauptsächlich Vors chriften des HGB (Handelsges etzbuch) und des Ak tG (Aktienges etz). Mit dem KonTra G wurde die Haftung von Vorstand, Aufsic htsrat und Wirtschaftsprüfern in Unternehmen erweitert. Kern des KonTra G ist eine Vorschrift, die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken (Risikofrüherkennungssystem) einzuführen und zu betreiben.“[6]

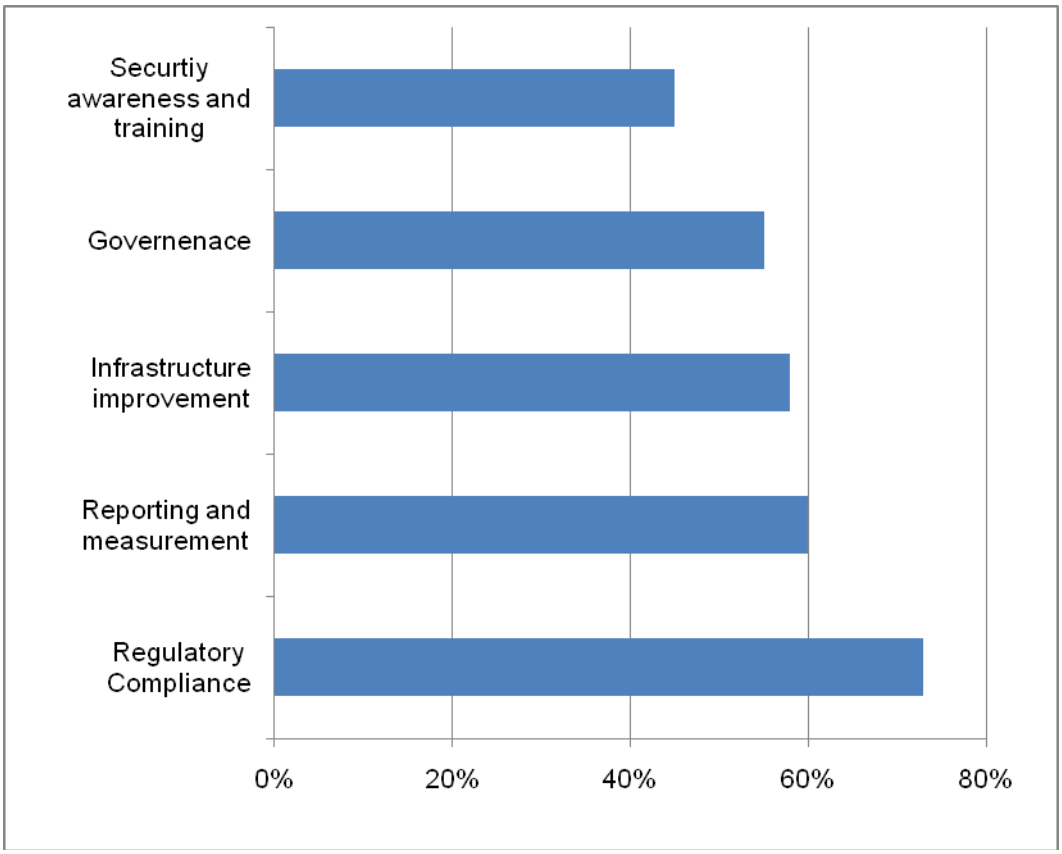
Der Rating Prozess, der mit Basel II von den Banken gefordert wird, berücksichtigt im Rahmen des Operationellen Risikos, unter anderem auch, die Wirksamkeit entsprechender Risiko-M anagementsysteme zu denen auch die IT-Sicherheit zählt.

Sarbanes Oxley wurde im Nachgang zu de r Enron Pleite in den USA 2002 eingeführt. Danach müssen alle bei der Securities and Exchange Commision (SEC) registrierten Unternehmen sowi e s ämtliche ausländische Niederlas - sungen dieser Firmen die Anforderungen des Acts erfüllen. Die s gilt expliz it

[6] Quelle Wikipedia: http://de. wikipedia.org/wiki/Gesetz_zur_Kontrolle_und_Transparenz_im_Unternehmensbereich, Zugriff am 4.11.2007

auch für nicht US-Firmen, die jedoch an amerikanischen Börsen gelistet sind. Eine nicht Befolgung kann empfindliche Strafen nach sich ziehen. Aufgrund dieser Ausgestaltung hatte die Einführung von SOX weltweit Konsequenzen. So ist es nicht verwunderlich, wenn das Thema IT-Sicherheit unter den führenden Finanzinstituten der Welt, nach einer Studie [7] der Wirtschaftsprüfungsgesellschaft Deloitte & Touche, von großer Bedeutung ist.

Abbildung 1-3 Top 5 Sicherheitsinitiativen[8]



Als wichtigsten Bereich haben die Befragten die Einhaltung und Erfüllung (Compliance) von Regeln und Gesetzen angegeben. Daraus lässt sich

[7] 2005 Global Security Survey

[8] Übernommen aus Deloitte Touche Global Securitiy Survey 2005

schlussfolgern, dass gerade für Finanzinstitute Sicherheit nicht mehr nur ein freiwilliges Thema ist, sondern eine vom Markt und den Stakeholdern geforderte Eigenschaft. Dies lässt sich vor allem mit den Forderungen des Sarbanes Oxley Acts hinsichtlich an amerikanischen Börsen und der SEC gelisteten Unternehmen begründen.

Des weiteren ist der Stellenwert den die Aufklärung und das Training der Mitarbeiter einnimmt mit 45% immer noch recht hoch und ein wesentlicher Aspekt des Sicherheitsmanagements.

Deloitte hat die Studie dabei in die fünf, international gebräuchliche, Regionen differenziert (s. h. Abbildung 1-4 auf der nächsten Seite)

- EMEA (Europa, mittlerer Osten und Afrika)
- APAC (Asien - Pazifik)
- LACRO (Latein Amerika und Karibik)
- Kanada
- USA

Hierbei fallen Regionale unterschiede ins Auge. Besonders auffällig ist, dass in der EMEA Region Standards und Prozeduren implementiert sind, aber der Bereich der Awareness-Schulung als Worst in Class herausfällt. Ein weiteres Ergebnis ist die anscheinend schwache Verbreitung der ISO Normen außerhalb Europas.

Abbildung 1-4 Regionale Unterschiede[9]

Finanzinstitute mit	EMEA	APAC	LACRO	CANADA	USA
eigener Sicherheitsstrategie	89%	70%	29%	70%	83%
genügend Engagement und finanziellen Mitteln um den regulatorischen Anforderungen gerecht zu werden	62%	56%	67%	78%	83%
Personalsicherheitsbewertungen bei IT-Mitarbeitern	43%	48%	50%	70%	52%
genügend Kompetenz und Qualifikationen um effektiv und effizient reagieren zu können	52%	31%	29%	50%	32%
ISO 17799:2000 Zertifikation oder Adaption	83%	65%	60%	60%	65%
Mindestens einer Schulungen für Mitarbeiter über Sicherheit und Datenschutz in den letzten 12 Monaten	36%	77%	57%	67%	76%

Best in Class **Worst in Class**

Dies könnte mit der Entwicklung und dem Ursprung der Norm 17799 als ehemaligem British Standard (BS) erklärt werden. Während der Rest der Welt, allem voran die Amerikaner, glauben genügend Ressourcen zur Verfügung zu haben, sehen die EMEA Regionen ihre Lage anders. Dort scheint Geld und das nötige Engagement nicht genügend vorhanden. Im Widerspruch dazu könnte die Einschätzung bzgl. der zur Verfügung stehenden personellen Kompetenz gesehen werden. Hier sehen sich die USA im Hintertreffen, was sich unter anderem in einem erheblichem Schulungsaufwand widerspiegelt.

[9] leicht verändert und gekürzt aus Deloitte Security Survey 2005

Diese Arbeit nimmt die regulatorischen und strategischen Herausforderungen, die mit dem verstärkten Einsatz moderner IT in der Gesellschaft und vor allem in Unternehmen einhergehen, zum Anlass, Standards und Methoden zu beleuchten, die geeignet erscheinen diesem Phänomen entgegen zu treten.

Dabei wird nach einem Überblick der Schwerpunkt auf die ISO/IEC 27000 Standardfamilie gelegt.

In Kapitel 5 wird die Implementation eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001 anhand eines Fallbeispiels exemplarisch betrachtet.

Das Ende der Arbeit bilden ein Fazit und ein Ausblick.

2 Informationssicherheit und Management

Information sind Daten, die analysiert, gemeinsam benutzt und interpretiert werden. Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.[10] Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird deshalb zunehmend verwendet. [11] IT-Sicherheit beschreibt den technischen Aspekt und ist als solcher in der Literatur jedoch

[10] [10] Vgl. BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise Seite 9

[11] Vgl. BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise Seite 9

6 Fazit und Ausblick

6.1 Ganzheitliches Konzept

Die Bedeutung moderner IT für Unternehmen kann nicht geleugnet werden. Die Sicherheit der damit verbundenen Werte stellt eine neue Herausforderung für Organisationen dar.

Best-Practices scheinen ein geeignetes Mittel zu sein, um Organisationen langfristig vor Bedrohungen zu schützen. In der heutigen Zeit ist es nicht mehr damit getan nur einen Virusscanner oder eine Firewall einzurichten. Sicherheit betrifft das gesamte Unternehmen und die Mitarbeiter.

Sicherheit ist somit auch keine Bestandsaufnahme sondern ein fortlaufender Prozess, der ständiger Anpassungen und Verbesserungen bedarf. Dies wird durch den kontinuierlichen Verbesserungsprozess eines ISMS gewährleistet. Die Implementation von Sicherheit in ein Managementsystem scheint nicht nur Zweckmäßig, sondern ideal, den Anforderungen der Zukunft zu begegnen. Die Verflechtung mit den strategischen Zielen der Unternehmung macht ein ISMS zu einem Nachhaltigen Konzept, das auf die Bedürfnisse der jeweiligen Geschäftsmodelle zugeschnitten ist.

Dennoch, so zeigen die Betrachtungen der anderen Standards, kann in bestimmten Gebieten die Integration weiterführender Standards Sinnvoll und nötig sein. Vor allem bei der Software Entwicklung bieten sich hier gute Möglichkeiten, die Anforderungen zu konkretisieren und in ein praktikables Modell zu überführen.

6.2 Aligning Cobit, ITIL und ISO 27001

Das IT-Governance Institute (ITGI) und OGC haben gemeinsam eine Studie zur Zusammenführung der verschiedenen Standards veröffentlicht. „*Aligning CobiT, ITIL and ISO 17799 for Business Benefit*“[41] Das itSMF unterstützte die Studie ebenfalls.

In der Studie wird CobiT aufgrund seiner breiten Aufstellung und Berücksichtigung mehrerer Standards eine Integrator Rolle zugeschrieben. CobiT soll die erwähnten Standards unter eine Regenschirm bringen.

Dies sehen die Autoren der Studie vor allem darin begründet, dass durch die wachsende Bedeutung regulatorischer Anforderungen, Unternehmen Best-Practices nicht mehr nur nach technischen Anforderungen ausrichten, sondern Governance Kriterien zukünftig berücksichtigen werden.

Das Modell sieht CobiT an höchster Stelle stehend. Aufbauend auf einem Prozessmodell liefert CobiT eine allgemeingültiges Maßnahmen und Kontroll Rahmenwerk, dass jeder Organisation passen sollte. Bestimmte, abgesonderte Bereiche könnnen durch ISO 27001 oder ITIL abgedeckt werden.

Diese Form der Verschmelzung wird im Kontext der hier gewonnenen Erkenntnisse Kritisch gesehen. Eine Verzahnung der verschiedenen Standards ist ein wünschenswertes Ziel dem voll und ganz zugestimmt werden kann. Dennoch scheint CobiT aufgrund der erlebten Spezifität nicht geeignet als Integrator zu dienen.

[41] Vgl. www.isaca.org

Der ISO 27001 scheint aufgrund der allgemeinen Orientierung und Fokussierung auf ein Managementsyste m viel eher dazu geeignet. Vor allem zwischen ITIL und ISO 27001 bestehen sehr gute Anknüpfungspunkte, an de nen die beiden Standards sich ideal ergänzen. CobiT wirkt dagegen wie ein von oben Aufgezwungenes Korsett, bei dem man sich an feste und bestimmte Vorgaben zu halten hat.

ITIL ergänzt und das ISMS um die prak tischen IT-Service orientierten Maßnahmen und erlaubt gleic hzeitig eine Ausrichtung der internen IT-Prozesse an Best-Practices. Denn IT-Service sollte nicht nur als externe Dienstleistung gesehen werden, für die internen Mitar beiter ist ein funktionierendes IT-Service Management mindestens genauso wichtig.

6.3 Ausblick

Generell werden sich die Standards we iter annähern, was für den Anwender nur gut sein kann. Sic herheit bleibt ein spannendes Thema und die Integration bzw. das Leben und Arbe iten mit Sic herheit wir d sich immer nahtloser gestalten. Gerade deshalb scheint ei ne st ändige Sensibilis ierung des Themas notwendig, denn eine der größt en Bedrohungen ist die menschlich e Nachlässigkeit.

Mit der Einführung der auch als EURO-SOX bezeichnete 8. EU-Richtlinie im Juli 2006 verschärfen sich auch die regulatorischen Anforderungen. Die nähe zu SOX wird durch die For derung der Einrichtung eines internen Kontrollsystems (IKS) deutlich. Diese Kont rollsystem soll die Wir ksamkeit von internen Kontrollen, Innenrevision und Risikomanagement überwachen.

Bis spätestens 29. Juni 2008 m uss EURO -SOX in nationales Vorschriften umgesetzt sein. Brauc hten sich Unter nehmen, die nic ht an der SEC gelist et

waren, bisher nicht mit den Anforderungen von SOX auseinander zusetzen, so sind von der EU-Regelung alle Kapitalgesellschaften betroffen. Damit werden auch kleinere und mittelständische Unternehmen gezwungen, sich mit den Themen Risikomanagement, IT-Security und Sicherheitsaudits intensiv zu beschäftigen[42] .

[42] Vgl. Bitkom, „Kompass der IT-Sicherheitsstandards“, Oktober 2007