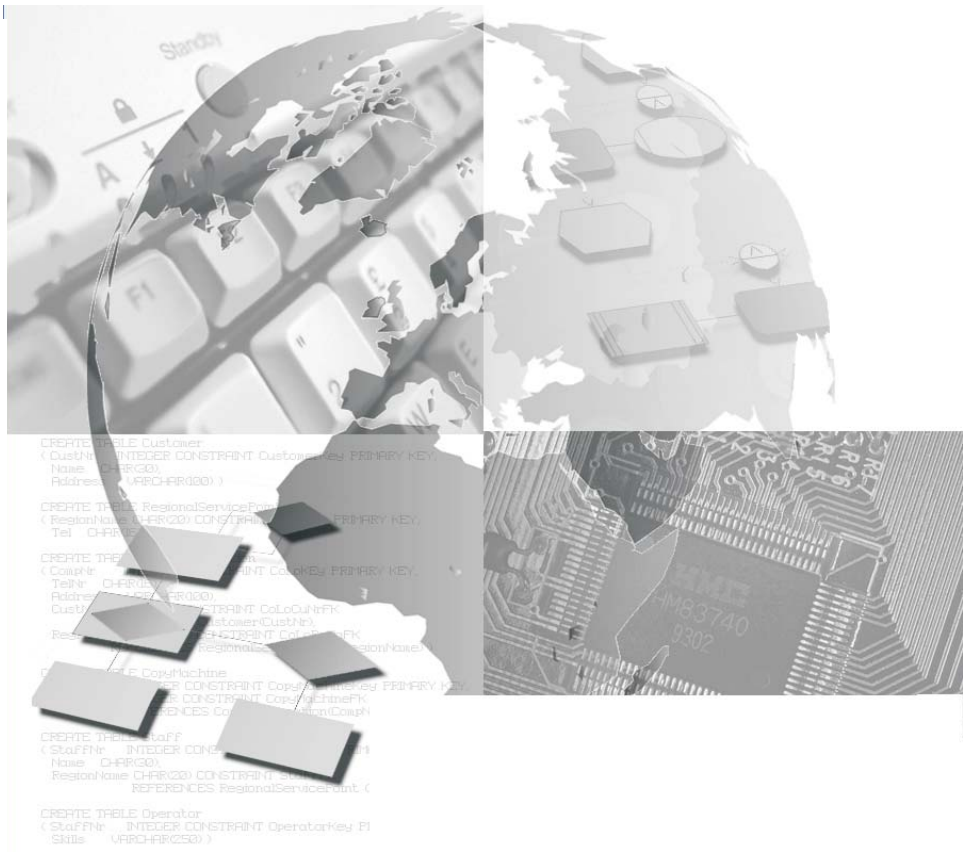
Westfälische
Wilhelms-Universität
Münster

WIRTSCHAFTS
INFORMATIK

Institut für Wirtschaftsinformatik

Arbeitsberichte



Arbeitsbericht Nr.112

Informations-Risiko-Management: Der Beitrag internationaler Normen und Standards

Rolf Alexander Teubner, Jan Terwey

Arbeitsberichte des Instituts für Wirtschaftsinformatik
Herausgeber: Prof. Dr. J. Becker, Prof. Dr. H. L. Grob, Prof. Dr. S. Klein,
Prof. Dr. H. Kuchen, Prof. Dr. U. Müller-Funk, Prof. Dr. G. Vossen

Arbeitsbericht Nr. 112

Informations-Risiko-Management: Der Beitrag internationaler Normen und Standards

Rolf Alexander Teubner, Jan Terwey

ISSN 1438-3985

Vorwort

Der Begriff „Information Management“ bzw. „Informationsmanagement“ (IM) hat bereits Anfang der 1980er Jahre Einzug in die Theorie und Praxis der Verwaltung und elektronischen Verarbeitung von Informationen gehalten. Während das Informationsmanagement im Laufe der Jahre zu einem anerkannten Schwerpunkt der Wirtschaftsinformatik – und in gewisser Hinsicht sogar zum Inbegriff der Disziplin – geworden ist, trägt es gleichwohl noch Merkmale eines Schlagwortes. Wissenschaftler und Praktiker thematisieren unter dem Begriff recht unterschiedliche Problem- und Aufgabenstellungen, ohne dass sich bisher allerdings eine einheitliche Sichtweise oder zumindest in den Interpretationen klare und anschlussfähige Begriffe herauskristallisiert haben. Damit sind die Bedingungen für den Austausch von Erkenntnissen im multipersonalen Forschungsprozess und letztlich für die Entwicklung allgemein anerkannter Bezugsrahmen und Theorien ungünstig. Darüber hinaus erschweren die sprachlichen Unklarheiten und das Fehlen möglicher Orientierungspunkte in Form von allgemein akzeptierten Konzepten auch Studierenden und interessierten Praktikern den Zugang zu diesem Themengebiet. Wir haben uns deshalb entschlossen, mit einer Reihe von Arbeitsberichten zur Systematisierung der Aufgaben und Probleme des Informationsmanagements sowie zur (Weiter-)Entwicklung von Lösungsansätzen beizutragen.

In einem ersten Beitrag (Nr. 82) haben wir die Entwicklung des IM in unterschiedlichen Disziplinen rekonstruiert und einen Überblick über den Stand der IM-Forschung im deutschsprachigen Raum gegeben. In einem zweiten Arbeitsbericht (Nr. 86) haben wir eine systematische Analyse und Bewertung einschlägiger deutscher Lehrbücher zum Informationsmanagement vorgenommen. Im Ergebnis zeigte sich, dass zwar einige viel versprechende Zugänge zum Arbeitsgebiet „Informationsmanagement“ existieren, ein einheitliches Fundament (Begriffe, Aufgabenfelder, Theorieansätze) bisher jedoch noch fehlt. An dieser Stelle setzt ein dritter Arbeitsbericht (Nr. 91) aus dieser Reihe an, in dem eine Terminologie für das IM erarbeitet und zur Diskussion gestellt wird. Eine gute Terminologie muss sich nicht für eine exakte und verständliche Beschreibung des Problembereichs eignen, sondern sich auch in der theoretischen Weiterentwicklung und praktischen Vermittlung von Erkenntnissen zum IM bewähren. Dabei stellen sich für das sowohl interdisziplinäre als auch internationale Arbeitsfeld „IM“ ganz besondere Herausforderungen. Zum einen müssen Begriffe und Erkenntnissen aus unterschiedlichen Nachbardisziplinen wie Betriebswirtschaftslehre, Informatik, Informations- und Kommunikationswissenschaften zusammengeführt werden. Forschungsergebnisse wiederum müssen so formuliert werden, dass sie an die Diskussion in diesen Nachbardisziplinen anschlussfähig sind. Zum anderen dürfen die Arbeiten begrifflich und inhaltlich nicht auf die deutsche Forschung beschränkt bleiben. Deshalb haben wir uns in einer Dokumentenanalyse

intensiv mit der Lehre und Forschung im englischen Sprachraum auseinandergesetzt. Ein vierter Arbeitsbericht (Nr. 95) stellt die Ergebnisse zur Diskussion.

Nachfolgende Arbeitsberichte zielen auf die Überwindung der angesprochenen Theoriedefizite. Zunächst geht es uns um ein Gesamtverständnis für die Objekte und Aufgaben der betrieblichen Informationsverarbeitung aus Sicht der Unternehmensführung. Wir haben diese in drei Arbeitsberichten behandelt, in deren Mittelpunkt jeweils ein wesentlicher Gestaltungsgegenstand steht: die Information als Ressource (AB 96), die Informationstechnologie (AB 104) und die Informationssysteme (AB 105).

Darauf aufbauend analysiert der vorliegende Arbeitsbericht die Risiken, denen die betriebliche Informationsverarbeitung ausgesetzt ist. Der Arbeitsbericht nutzt das im AB 91 vorgestellte und den in den AB 96, 104 und 105 ausgeführte Modell des Informationsmanagements, um Risikofelder zu identifizieren. Das Modell ist auch Grundlage für die Beurteilung des Beitrags, den aktuelle internationale Normen und Standards zur Bewältigung der Aufgaben des Informations-Risiko-Managements leisten.

Die vorgeschlagenen Konzepte und Systematisierungen werden von uns bereits seit längerem in der Ausbildung in Informationsmanagement an der Wirtschaftswissenschaftlichen Fakultät der Universität Münster verwendet. In diesen Veranstaltungen, die nicht nur von Wirtschaftsinformatikern, sondern auch von Betriebs- und Volkswirten besucht werden, zeigt sich bereits frühzeitig, ob Konzeptualisierungen – auch über disziplinäre Grenzen hinweg – verstanden werden und zum Verständnis der Probleme des Informationsmanagements und deren Lösung beitragen.

Alexander Teubner, Stefan Klein

Inhalt

1 Motivation

Dem betrieblichen Risikomanagement kommt heute in Anbetracht einer hochdynamischen, mit Unsicherheiten behafteten Umweltsituation bei gleichzeitig hoher interner Komplexität und Fehleranfälligkeit eine wichtige Rolle bei der Sicherstellung des Unternehmenserfolgs zu. Darüber hinaus ist es nicht nur im Interesse des Unternehmens, sich durch ein wirksames Risikomanagement gegen Fehler, Unwägbarkeiten und Wagnisse abzusichern. Auch für externe Anspruchsgruppen und insbesondere Kapitalgeber ist es wichtig, sich auf Einschätzungen und Informationen von Unternehmen verlassen zu können. Daher haben sich auch die gesetzlichen Rahmenbedingungen im Hinblick auf den Umgang mit Risiken verschärft, so etwa durch den Sarbanes-Oxley-Act in den USA oder das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) der Bundesrepublik Deutschland. Das KonTraG verpflichtet im § 91, Absatz 2, den Vorstand dazu „(…) geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“. Ähnlich wirkt auch die als „Basel II“ bekannte Eigenkapitalverordnung, die Kreditinstitute dazu anhält, die Kreditvergabe stärker an ökonomische Risiken zu knüpfen als bisher. Im Umkehrschluss bedeutet dies, dass sich die Einführung eines effektiven Risikomanagements als Antwort auf Unsicherheiten und Diskontinuitäten wiederum positiv auf die Bewertung der Bonität auswirkt.

Im Rahmen des betrieblichen Risikomanagements spielen Risiken, die sich aus dem betrieblichen Einsatz von Informationstechnologie (IT) ergeben, eine besondere Rolle. Alleine die Bedeutung von Investitionen in IT und die hohen Kosten für den IT-Einsatz, die in Dienstleistungsbranchen bei bis zu 10% des Umsatzes liegen können, sind ökonomisch Grund genug, sich sorgfältig mit den Risiken im IT-Bereich zu beschäftigen. Weit entscheidender ist jedoch die umfassende Durchdringung der Unternehmen mit Informationssystemen (IS). Daraus resultiert zum einen, dass der Ausfall der IS meist schwerwiegende Auswirkungen auf die laufende Geschäftstätigkeit hat. Zum anderen sind die betrieblichen IS heute zu solch komplexen Strukturen integriert, dass Fehler leicht unerkannt bleiben können und Systeme nur mit großem Aufwand umfassend vor unerlaubten Zugriffen oder sogar Sabotage geschützt werden können.

Aufgrund ihrer besonderen Bedeutung werden IT-Risiken inzwischen in einer ganzen Reihe von Normen und Standards behandelt. Für das Informationsmanagement sind diese eine wichtige Quelle breit akzeptierter Instrumente und Praktiken im Umgang mit Risiken. Allerdings ist das Angebot an verfügbaren Normen und Standards der Bedeutung des Problembereichs entsprechend inzwischen auf einen nur schwer überschaubaren Umfang angewachsen. Gleichzeitig unterscheiden sich die Standards nach Ursprung und Intention deutlich in den Problem-

stellungen, die sie behandeln, und den Handlungsempfehlungen, die sie geben. Für Praktiker und Wissenschaftler ist es daher gleichermaßen schwierig, einen Überblick über die Bedeutung und die inhaltlichen Beiträge der verfügbaren Normen und Standards zu gewinnen. An dieser Stelle soll der vorliegende Aufsatz einen Beitrag leisten. Zum einen werden die wichtigsten Normen und Standards zum Thema IT-Risikomanagement – in einem umfassenderen Verständnis wird auch von Informations-Risiko-Management (IRiM) gesprochen – identifiziert und im Hinblick auf ihre Akzeptanz in der Praxis beurteilt. Zum anderen werden die inhaltlichen Beiträge dieser Normen und Standards zu den Risiken der betrieblichen Informationsverarbeitung systematisch erfasst und dargestellt. Auf dieser Grundlage diskutieren wir abschließend den Beitrag, den diese Normen für die Ausgestaltung des betrieblichen IRiM leisten. Sowohl in die Beurteilung der Praxisakzeptanz als auch in die abschließende Diskussion fließen die Ergebnisse aus Gesprächen ein, die wir mit IT-Führungskräften aus zehn mittelständischen Unternehmen geführt haben[1)]. Bevor wir uns jedoch den Normen und Standards im Detail zuwenden, ist zu klären, was genau unter IT-Risikomanagement bzw. Informations-Risiko-Managements zu verstehen ist.

2 Informationssicherheit und Risikomanagement

Informationssicherheit bezeichnet einen Zustand der betrieblichen Informationsverarbeitung, in dem die Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit, Authentizität und Verlässlichkeit von Informationen und Daten in IK-technikgestützten Systemen gewährleistet ist[2)]. Der Begriff der Informationssicherheit geht damit weiter als der (im Alltagssprachgebrauch oft synonym verwendete) Begriff der IT-Sicherheit. Denn die Vertraulichkeit oder Verlässlichkeit von Informationen in informationsverarbeitenden Systemen sind nicht alleine durch technische Vorkehrungen zu gewährleisten, sondern erfordern auch organisatorische Regelungen, wie etwa zur Freigabe von Informationen oder deren regelmäßiger Überprüfung.

Sicherheit ist die Abwesenheit von Risiko. Ein Risiko bezeichnet eine Bedrohung (mögliche Schadensursache), sofern diese mit einer bestimmten Wahrscheinlichkeit eintreten und dabei einen Schaden verursachen kann. Letzteres kann ggf. durch entsprechende Schutzmaßnahmen abgewendet werden. Informationssicherheit bedeutet streng genommen die Abwesenheit von Informationsrisiken (alltagssprachlich auch „IT-Risiken“).

---

1) Wir danken der advantegy GmbH, die uns den Zugang zu Unternehmen aus der Region Niedersachsen und Nordhessen ermöglicht und bei der Durchführung der Interviews unterstützt hat, und den Mitabeitern, die uns als Gesprächspartner zur Verfügung standen.

2) Vgl. ISO / IEC (1996), S. 3 ff.

Ein Zustand absoluter Informationssicherheit ist aber praktisch kaum herzustellen und ist auch nicht immer notwendig und wünschenswert. Vielmehr muss sich der Umfang des Schutzes nach der Wahrscheinlichkeit des Eintretens von Bedrohungen und den damit verbundenen möglichen wirtschaftlichen Schäden richten. Deshalb kann anstatt von „Informationssicherheits-Management“ auch von „Informationsrisiko-Management“ (IRiM) gesprochen werden[3)]. IRiM bedeutet, mit Bedrohungen bewusst umzugehen, planmäßig Sicherheitsvorkehrungen herzustellen und diese zu überwachen, zu erhalten und weiterzuentwickeln.

3 Normen und Standards zum Informations-Risikomanagement

Ein Standard (engl. „standard“) bezeichnet eine Richtlinie, Vorgabe oder Konvention, die durch Autorität, Gewohnheit oder Konsens als Vorschrift für Beurteilungen oder das Handeln breit anerkannt wird. Unter einer Norm versteht man einen speziellen Standard, der von offiziell anerkannten Institutionen wie dem Deutschen Institut für Normung e. V. (DIN) oder der International Organization for Standardization (ISO) definiert wird und für jedermann zugänglich ist. Normen werden unter Mitarbeit und im Einvernehmen oder mit allgemeiner Zustimmung aller an dem behandelten Thema interessierten Kreise erstellt und sollten auf abgestimmten Ergebnissen von Wissenschaft, Technik und Praxis beruhen.

Im Bereich des IRiM gibt es eine Reihe von Standards bzw. Normen, die Best Practices, Leistungsniveaus, Richtlinien, Leitlinien, Kontrollvorgaben, etc. vorgeben. Für diese Untersuchung wurden solche Standards ausgewählt, die

- inhaltlich eine starken Bezug zum IRiM haben,
- eine über nationale Grenzen hinausgehende Bekanntheit und Anerkennung erfahren,
- die sich in der Diskussion in Wissenschaft und Praxis niederschlägt.

Tabelle 1 gibt einen Überblick über die Auswahl der Normen und Standards[4)]. Zwei Standards wurden trotz ihrer weiten Verbreitung nicht in die Analyse aufgenommen: Das US-amerikanische „Capability Maturity Model (CMM)“ des Software Engineering Institute und das Prozessmodell „Software Process Improvement and Capability Determination (SPICE)“ nach ISO/IEC TR 15504. Der Grund dafür ist, dass beide Modelle auf die Softwareentwicklung beschränkt sind und nicht speziell auf das Risikomanagement zielen. Zudem stellen sie

---

3) Vgl. dazu auch Teufel, Schlienger (2000); Heinrich (2002), S. 278 ff.

4) Zur Bekanntheit in der Praxis und zur wissenschaftlichen Diskussion vgl. KES (2004); Junginger, Krcmar (2003) und (2004); Kraft, Seidel (2004); Rausch, Disterer (2004); Thamm (2004).

den Reifegrad des Entwicklungsprozesses und dessen Messung in den Vordergrund, während Maßnahmen nur am Rande behandelt werden[5)]. Beide Standards können jedoch die nachfolgend besprochenen Normen und Standards in der Softwareentwicklung ergänzen.

Bezeichnung Herausgeber, Jahr der aktuellen Auflage	**Typ** **Sprache(n)**	**Begründung für die Auswahl**
CobiT – Control Objectives for Information and Related Technology ITGI – IT-Governance Institute, 2003.	Best Practice (mehrsprachig)	In Wissenschaft und Praxis diskutiert.
DIN ISO/IEC 15408 – IT-Sicherheitsverfahren – Evaluationskriterien für IT-Sicherheit Teil 1: Einführung und allgemeines Modell Teil 2: Funktionale Sicherheitsanforderungen Teil 3: Anforderungen an die Vertrauenswürdigkeit DIN - Deutsches Institut für Normung e. V., 2004.	Deutsche und internationale Norm (deutsch, englisch)	Häufige Berücksichtigung in Fachliteratur.
ISO/IEC 17799 – Information technology – Code of practice for information security management ISO/IEC – International Organization for Standardization, International Electrotechnical Commission, 2000.	Internationale Norm (englisch)	In Fachliteratur und Praxis international aufgenommen.
BS 7799-2 – Information security management systems – Specification with guidance for use BSI - British Standards Institution, 2002.	Britische Norm (englisch)	
ISO/IEC TR 13335 - Guidelines for the management of IT Security Part 1: Concepts and models for IT-Security Part 2: Managing and planning IT Security Part 3: Techniques for the management of IT-Security Part 4: Selection of safeguards Part 5: Management guidance on network security ISO/IEC – International Organization for Standardization, International Electrotechnical Commission, 1996-2001.	Internationaler Technischer Report (englisch)	In Fachliteratur stark diskutiert.
IT-Grundschutzhandbuch BSI – Bundesamt für Sicherheit in der Informationstechnik, 2003.	Standard (deutsch, englisch)	In Deutschland weithin bekannt und verbreitet.
ITIL – IT Infrastructure Library OGC – Office of Government Commerce, 2002.	Best / Commmon Practice (englisch)	In Praxis und Wissenschaft breit rezipierter und internationaler Standard.
VDI 5002 - Informationssicherheit in der Bürokommunikation VDI - Verein Deutscher Ingenieure e. V., 1993.	VDI-Richtlinie (deutsch)	In Praxis (noch) von Bedeutung.

Tabelle 1: Auswahl der Standards zum Informations-Risikomanagement

5) Vgl. Wallmüller (2004), S. 90 ff.

3.1 CobiT – Control Objectives for Information and Related Technology

Der CobiT-Standard ist ein Modell zur Steuerung und Kontrolle des unternehmensweiten IT-Einsatzes und adressiert insbesondere auch die Beherrschung von Risiken. Der Standard wurde 1996 von der „Information Systems Audit and Control Association (ISACA)“ entwickelt, einem Berufsverband, indem weltweit mehr als 35.000 Mitglieder v. a. aus dem Consulting, der Wirtschaftsprüfung und der Revision organisiert sind. CobiT ist eine Synthese aus insgesamt 41 internationalen Standards, die sich mit der Kontrolle, Revision, Sicherheit und Qualität von IT-Anwendungen befassen. Die derzeit aktuelle dritte Auflage von CobiT wurde in 2000 veröffentlicht und ist mehrsprachig verfügbar. Ziel des Standards ist es, die Überprüfbarkeit der IT-Prozesse und IT-Ressourcen zu verbessern. Dazu wird ein Prozessmodell zur umfassenden Kontrolle und Steuerung des IT-Einsatzes vorgegeben (Abbildung 1).

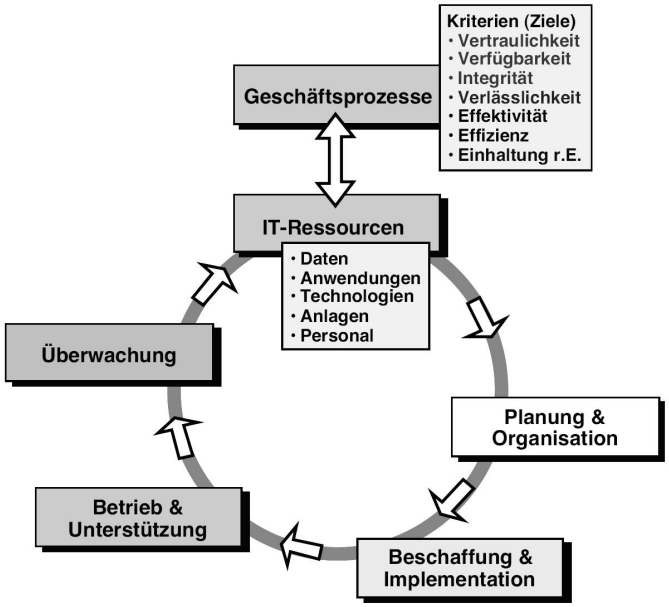


Abbildung 1: CobiT-Prozessmodell[6)]

Das CobiT-Modell der IT-Prozesse folgt dem Lebenszyklus für die sog. IT-Ressourcen „Daten“, „Anwendungen“, „Technologien“, „Anlagen“ und „Personal“. Der Zyklus umfasst die vier Phasen „Planung und Organisation“, „Beschaffung und Implementation“, „Betrieb und Unterstützung“ und „Überwachung“, die zu 34 Hauptprozessen und weiter zu 318 Teilprozessen verfeinert werden. Für jeden Haupt- und auch Teilprozess ist ein Idealzustand – recht abstrakt – durch Kontrollziele („Control Objectives“) formuliert, wodurch die Informationsver-

6) ISACA (2001).

sorgung der Geschäftsprozesse sichergestellt und damit ein Beitrag zur Erreichung der Geschäftsziele geleistet werden soll. Als zentrale Kriterien werden dabei die Qualität, Sicherheit und Ordnungsmäßigkeit der Informationsversorgung identifiziert (Tabelle 2). Für die Hauptprozesse werden zudem Indikatoren zur Messung der Zielerreichung angegeben. Das Maß, indem die Kontrollziele erreicht werden, wird auch als Reifegrad des Prozesses verstanden.

Die Kontrollziele für die Haupt und Teilprozesse („High-Level-" bzw. Detailed-Control Objective) werden weiter durch eine Anzahl von Kontrollpraktiken („Control Practice") operationalisiert. Darunter werden Mechanismen zur Realisierung und zielgerichteten Steuerung bzw. zur Vermeidung von Störungen der IT-Prozesse verstanden. Der CobiT-Standard enthält zusätzlich einen Leitfaden, der auf die Durchführung von Audits der vorbereitet [ITGI 2004].

Kategorie	Kriterium	Bedeutung
Qualität	Effektivität	Informationen sind für den Geschäftsprozess relevant und können rechtzeitig, fehlerfrei und konsistent bereitgestellt werden.
	Effizienz	Wirtschaftliche Informationsbereitstellung durch optimale Ressourcenverwendung muss gewährleistet sein.
Sicherheit	Vertraulichkeit	Sensitive Informationen sind vor unberechtigter Veröffentlichung zu schützen.
	Integrität	Richtigkeit, Vollständigkeit und Übereinstimmung mit betriebswirtschaftlichen Werten und Erwartungen von Informationen müssen sichergestellt werden.
	Verfügbarkeit	Schutz im Umgang mit Funktionen von Ressourcen, die Informationen für Geschäftsprozesse verfügbar machen.
Ordnungsmäßigkeit	Zuverlässigkeit	Geeignete Daten zum Betrieb und zur Verantwortung der regulativen und finanziellen Berichterstattung einer Geschäftseinheit müssen bereitgestellt werden.
	Einhaltung rechtlicher Erfordernisse	Externe Gesetze, regulative und vertragliche Abmachungen, denen der Geschäftsprozess unterlegen ist, müssen erfüllt werden.

Tabelle 2: Kriterien zur Bestimmung des Reifegrads von IT-Prozessen in CobiT

CobiT ist ein sehr umfassender, aber auch kompliziert aufgebauter Standard, der in der Praxis bisher kaum angenommen ist. Zwar ist CobiT in mehr als der Hälfte der mittelgroßen und großen Unternehmen bekannt[7)], wird jedoch nur in etwa jedem zehnten Unternehmen eingesetzt[8)]. In kleineren Unternehmen ist CobiT nach unseren Interviewerfahrungen dagegen kaum bekannt. Und wenn, dann bestehen Vorbehalte in der Anwendung aufgrund der Kom-

7) Vgl. KES (2004), S. 10.

8) Vgl. Junginger, Krcmar (2004), S. 23.

plexität des Standards. Mit „CobiT Quickstart“ gibt es allerdings, eine verschlankte Version des Standards, die die Barrieren des Einstiegs für KMU reduzieren soll[9)].

3.2 DIN ISO / IEC 15408 – Evaluationskriterien für IT-Sicherheit

Grundlage der DIN ISO / IEC 15408 sind die sog. „Common Criteria“ (CC), die ein Ergebnis der Vereinheitlichung nationaler Dokumente (z. B. ITSEC – Information Technology Security Evaluation Criteria) zur Evaluierung und Zertifizierung von IT-Sicherheit sind. Dieser Standard wurde in 1999/2000 in der Fassung 2.0 von der International Organization for Standardization (ISO) zur internationalen Norm erhoben und wird inzwischen vom Deutschen Institut für Normung auch in deutscher Fassung herausgegeben. Die DIN 15408 zielt auf die Entwicklung sicherer IT-Produkte und wendet sich damit vornehmlich an IT-Hersteller, die ihre Produkte nach dieser Norm zertifizieren lassen können. Die Zertifizierung wird jeweils für ein bestimmtes Produkt, dem sog. „Evaluierungsgegenstand (EVG)“, und wird auf einer bestimmten Vertrauenswürdigkeitsstufe („Evaluation Assurance Levels (EAL)“) vorgenommen. Insgesamt sind sieben EALs vorgesehen, die insbesondere spezielle Entwicklungs- und Testprozesse des EVG erfordern (Tabelle 3)[10)]. Die DIN ISO 15408 gibt zudem konkrete Prüfkriterien vor, nach denen Auditoren die Sicherheitsprüfungen bzw. eine Zertifizierung vornehmen können.

Aus Sicht der Kunden garantieren Systeme und Produkte, die nach DIN 15408 genormt sind, einen definierten Sicherheitsstandard, der je nach Einsatzbedingungen und -anforderungen zu wählen ist[11)]. Darüber hinaus unterstützt die Norm Anwender dabei, ihre Sicherheitsanforderungen an einzusetzende IT-Produkte implementierungsunabhängig in Form von sog. Schutzprofilen zu formulieren[12)].

---

9) Vgl. ITGI (2004), S. 11.
10) Vgl. DIN ISO/IEC 15408-3:2001, S. 35-44.
11) Vgl. Junginger, Krcmar (2002), S. 3.
12) Vgl. DIN ISO/IEC 15408-1:2001, S. 9.

EA Level	Anforderungen an die Entwicklung des EVG
EAL 1: funktionell getestet	Ist anwendbar, wenn der Anwender „ein gewisses Maß an Vertrauen“ in den korrekten Betrieb des EVG benötigt, jedoch keine ernsthaften Bedrohungen für den EVG zu erwarten sind. Gefordert ist eine konsistente Dokumentation der Funktion des EVG.
EAL 2: strukturell getestet	Erfordert die Lieferung von Entwurfsinformationen und Testergebnissen des EVG durch den Entwickler. Der Arbeitsaufwand für die Entwicklung soll nicht durch erhebliche zeitliche und finanzielle Zusatzinvestitionen erhöht werden. Wird angewendet wenn niedrige bis mittlere Sicherheitsanforderungen bestehen.
EAL 3: methodisch getestet und überprüft	Technische Sicherheitsmaßnahmen sollen einem gewissenhaften Entwickler erlauben eine maximale Vertrauenswürdigkeit zu erzielen, ohne bestehende, stimmige Entwicklungspraktiken wesentlich verändern zu müssen. Der Nachweis von Tests und Schwachstellenanalysen durch den Entwickler ist erforderlich.
EAL 4: methodisch entwickelt, getestet, durchgesehen	Vorhandene technische Sicherheitsmaßnahmen in der Entwicklung des EVG erlauben es maximale Vertrauenswürdigkeit zu erzielen. Diese Maßnahmen erfordern jedoch keine tiefgehenden Spezialkenntnisse, Fähigkeiten oder Betriebsmittel. Erwartet werden jedoch objektive Tests und Schwachstellenanalysen des EVG.
EAL 5: semiformal entworfen und getestet	Maximale Vertrauenswürdigkeit soll durch technische Sicherheitsmaßnahmen gewährleistet werden, die wiederum in scharfen betrieblichen Entwicklungspraktiken verankert sind. Erforderlich sind unabhängige Tests und Schwachstellenanalysen, die einen moderaten Widerstand gegen Angriffe auf den EVG berücksichtigen.
EAL 6: semiformal verifizierter Entwurf und getestet	Erfordert eine streng kontrollierte Entwicklungsumgebung, um einen erstklassigen EVG zum Schutz hoher Werte gegen signifikante Risiken zu entwickeln. Es sind ausführliche unabhängige Tests und Schwachstellenanalysen des EVG durchzuführen, die einen hohen Widerstand gegen Angriffe gewährleisten sollen.
EAL 7: formal verifizierter Entwurf und getestet	Entwicklung eines EVG für Situationen mit extrem hohem Risiko, in denen der hohe Wert des EVG die höheren Entwicklungskosten rechtfertigt. Es ist eine hochkonzentrierte Sicherheitsfunktionalität sicherzustellen und zu dokumentieren.

Tabelle 3: Evaluation Assurance Levels nach DIN ISO/IEC 15408

Die Norm hat für Entwickler von IT-Produkten eine hohe und wachsende Bedeutung. In 2004 war die DIN 15408 in drei von vier größeren Unternehmen bekannt und knapp 40% der Unternehmen setzten bewusst nach DIN 15408 zertifizierte IT-Produkte ein[13)]. Nach unseren Interviews wird die Norm allerdings, sofern sie überhaupt bekannt ist, dann lediglich als „Gütesiegel“ für Produkte verstanden, das aber nicht näher hinterfragt wird. In den befragten KMU wurde die Norm weder zur Erstellung von Schutzprofilen noch als Richtlinie für unternehmensinterne Soft- und Hardwareentwicklung eingesetzt.

13) Vgl. KES (2004), S. 9, 10. Durchschnittliche Mitarbeiteranzahl der befragten Unternehmen: 4600.

3.3 Code of Practice for Information Security Management – ISO / IEC 17799

Der Code of Practice for Information Security Management wurde zuerst von der British Standards Institution in der Norm BS 7799 festgeschrieben. Die Norm umfasst zwei Teile. Der erste Teil, BS 7799-1, definiert ein „Information Security Management System (ISMS)“ und ist inzwischen als internationale Norm ISO 17799 etabliert. Der zweite Teil, BS 7799-2, macht Vorgaben für die Einführung eines solchen ISMS. Unter „Information Security Management“ wird in diesen Normen die Erhaltung und Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen verstanden. Vertraulichkeit setzt voraus, dass nur berechtigte Personen Zugang haben. Integrität wird erreicht, indem Exaktheit und Vollständigkeit von Informationen und ihrer Verarbeitung gewährleistet werden. Zudem sollen Informationen und sie bereitstellende Anlagen für autorisierte Nutzer dann verfügbar sein, wenn sie benötigt werden[14)].

Unter einem ISMS wird der Teil des Managementsystems verstanden, der die Etablierung, Implementierung und Überwachung von Informationssicherheit gewährleisten soll[15)]. Die ISO / IEC 17799 schreibt nicht im Detail vor, wie ein ISMS auszugestalten ist. Sie identifiziert aber wesentliche Handlungsfelder, die ein ISMS adressieren muss, und schlägt dazu Maßnahmen zur Gewährleistung der Informationssicherheit vor (Tabelle 4).

---

14) Vgl. ISO/IEC TR 13335-4:2000, S. 1.

15) Vgl. BS 7799-2:2002, S. 4.

Handlungsfeld	Maßnahmenbündel
Security Policy	Etablierung einer Sicherheitspolitik
Organizational Security	Bildung von Organisationseinheiten mit Sicherheitsverantwortung; Regelung des Zugang von Dritten; Gestaltung von Outsourcingverträgen
Asset Classification and Control	Bestimmung von Verantwortlichen für Schäden an Inventar/Vermögenswerten; Klassifikation der Informationsbestände nach Schutzbedarf
Personnel Security	Sicherheitsverantwortung in Stellenbeschreibungen und bei Personalauswahl; Regelung von Zutrittsberechtigungen; Schulungen; Reporting von Vorfällen und Fehlfunktionen
Physical and Environmental Security	Sicherheitszonen; Schutzmaßnahmen für Betriebsmitteln; Schutz von Informationen und -trägern vor Diebstahl und Spionage („clear desk and clear screen“)
Communications and Operations Management	Zuteilung von Verantwortlichkeiten und Kommunikation von Betriebsabläufen; Systemkapazitätsplanung und Schaffung von Akzeptanz; Schutz gegen fehlerhafte Software; Durchführung von Backup und Logging; Netzwerkmanagement; sicherer Umgang mit Medien; Kontrolle des Austauschs von Informationen und Software
Access Control	Ableiten des Informationszugangsbedarfs anhand von Geschäfts- und Sicherheitsanforderungen; Management von Nutzerzugängen; Übertragung von Verantwortlichkeiten an Nutzer; Zugangskontrolle zu Netzwerken, Betriebssystemen und Anwendungen; Monitoring von Systemzugriffen und -gebrauch; Regelungen für den Zugriff bei „mobile computing“ und Telearbeit
Systems Development and Maintenance	Identifikation von Sicherheitsanforderungen von Informations- und Anwendungssystemen; Einrichtung sicherer Entwicklungs- und Supportprozesse; Einsatz von Kryptographie; Kontrolle des Zugriffs auf Systemdateien
Business Continuity Management	Identifikation von Störungsursachen; Ausarbeitung, Test und Weiterentwicklung von Notfall- und Wiederanlaufplänen
Compliance	Übereinstimmung mit rechtlichen Anforderungen schaffen; regelmäßige Überprüfung der Sicherheitspolitik und der technischen Sicherheitsanforderungen; Gewährleistung reibungsloser Systemaudits

Tabelle 4: Maßnahmenkatalog nach ISO/IEC 17799

ISO/IEC 17799 und BS 7799-2 haben nicht ausschließlich Organisationen einer bestimmten Art oder Größe als Zielgruppe. Stattdessen sollen die Empfehlungen an die spezifischen Gegebenheiten des Unternehmens angepasst werden[16)]. Die ISO 17799 ist in etwa 3/4 der mittelgroßen Unternehmen bekannt und wird in 38% der größeren Unternehmen eingesetzt[17)]. Auch in KMU ist die ISO 17799 nur vereinzelt bekannt und wird nur selten eingesetzt.

16) Vgl. Völker (2004), S. 103.

17) Vgl. KES (2004), S. 10; Junginger, Krcmar (2004), S. 23.

3.4 Guidelines for the Management of IT-Security – ISO/IEC TR 13335

Die Guidelines for the Management of IT-Security sind ein technischer Report (TR), der von der ISO und der IEC herausgegeben wird. Anders als klassische Normen geht der TR insbesondere auf aktuelle technologische Entwicklungen ein[18)]. Der Schwerpunkt liegt bisher auf den Datenverarbeitungstechnologien, allerdings wird bereits an einer Ausarbeitung in Richtung auf moderne Kommunikationstechnologien gearbeitet. Entwürfe hierzu werden bereits unter dem Thema „management of information and communication technology" diskutiert[19)].

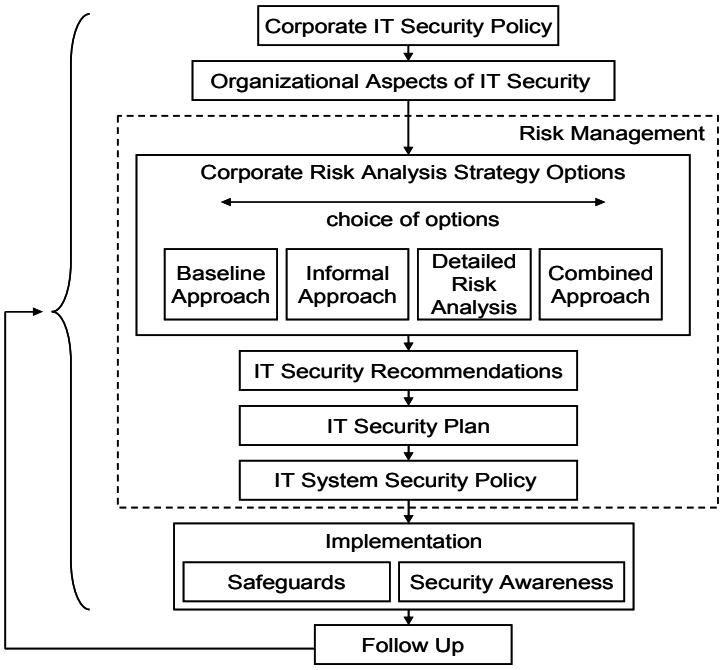


Abbildung 2: IT-Security Management Process[20)]

Der TR 13335 stellt ein allgemeines Konzept für das IT-Sicherheitsmanagement in insgesamt fünf Teilen dar. Nachdem in Teil eins grundlegende Begriffe des IT-Sicherheitsmanagements eingeführt wurden, wird in Teil 2 ein Gesamtüberblick über den „Planning and Management of IT Security" als Prozess gegeben (Abbildung 2). In Teil drei werden dann einzelne Schritte des Prozessmodells näher erläutert und wichtige Konzepte und Lösungsansätze vorgestellt. So wird etwa das Konzept einer „Security-Policy" durch ein umfassendes Template operationalisiert, und es werden je nach Schutzbedürfnis unterschiedliche Ansätze der Risikoanalyse und -vorsorge eingeführt. Die Risikoanalyse wird darüber hinaus durch eine systematische Zu-

---

18) Vgl. ISO/IEC TR 13335-1:1996, S. III.

19) Vgl. BSI (2004).

20) ISO/IEC TR 13335-2:1997, S. 2; ISO/IEC TR 13335-3:1998, S. 2.

sammenstellung potenzielle Bedrohungen nach Sicherheitsmerkmalen unterstützt (siehe Tabelle 3)[21)]. Der fünfte Teil geht auf spezielle Risiken bei externer Vernetzung ein.

S.-Merkmal	Bedrohungen
Vertraulichkeit	Lauschangriffe; elektromagnetische Strahlung; böswilliger Code; Maskierung von Nutzeridentitäten; Umleitung von Nachrichten; Softwarefehler; Diebstahl; unauthorisierter Zugang zu Computern, Daten, Diensten, Anwendungen und Speichermedien
Integrität	Zerfall von Speichermedien; Wartungsprobleme; böswilliger Code; Maskierung von Nutzeridentitäten; Umleitung von Nachrichten; Unleugbarkeit der Kommunikation; Softwarefehler; Versorgungsausfall (Energie, Klimatisierung); technische Fehler; Übertragungsfehler; Benutzung unberechtigter Software; unauthorisierter Zugang zu Computern, Daten, Diensten, Anwendungen und Speichermedien; Fehler von Nutzern
Verfügbarkeit	Zerstörerische Angriffe; Zerfall von Speichermedien; Fehler der IKT; Feuer, Wasser; Wartungsprobleme; böswilliger Code; Maskierung von Nutzeridentitäten; Umleitung von Nachrichten; Missbrauch von Ressourcen; Naturkatastrophen; Softwarefehler; Versorgungsausfall (Energie, Klimatisierung); technische Fehler; Diebstahl; Verkehrsüberlastung; Übertragungsfehler, Benutzung unberechtigter Software; unauthorisierter Zugang zu Computern, Daten, Diensten, Anwendungen und Speichermedien; Fehler von Nutzern
Zurechenbarkeit	Teilen von Nutzerzugängen; Nicht-Rückverfolgbarkeit von Handlungen; Maskierung von Nutzeridentitäten; Softwarefehler; unauthorisierter Zugang zu Computern, Daten, Diensten, Anwendungen und Speichermedien; schwache Authentifizierung von Identitäten
Authentizität	Unkontrollierte Datenmanipulation; unbekannter und unkontrollierter Ursprung von Daten
Verlässlichkeit	Inkonsistente Systemleistung; unzuverlässige Lieferanten

Tabelle 5: Sicherheitsmerkmale und Bedrohungen nach TR 13335

Der TR 13335 ist nicht auf bestimmte Unternehmen oder Branchen zugeschnitten, sondern weitestgehend allgemeingültig gehalten. Zuverlässiges Zahlenmaterial zur Verbreitung des TR in der Praxis liegt nach Wissen der Verfasser nicht vor. In den von uns befragten KMU war der TR 13335 kaum bekannt. Allerdings kann vermutet werden, dass der TR an Akzeptanz gewinnen wird, sobald er vollständig als Norm veröffentlicht ist[22)].

3.5 IT-Grundschutzhandbuch

Das IT-Grundschutzhandbuch (IT-GSHB) wurde erstmals 1996 vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben und ist seitdem laufend aktualisiert und erweitert worden. Das IT-GSHB ist in deutscher und englischer Sprache verfügbar; die deutsche Version ist zuletzt in 2004 aktualisiert und ergänzt worden.

---

21) Vgl. ISO/IEC (2000), S. 27 ff.

22) Der Teil eins ist bereits seit November 2004 als Norm ISO/IEC 13335-1 veröffentlicht.

Ziel des IT-GSHB ist es, „durch die geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmaßnahmen ein Sicherheitsniveau zu erreichen, das für den normalen Schutzbedarf angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und -Anwendungen dienen kann“[23)]. Das Handbuch schlägt also Maßnahmen vor, mit denen sich ein durchschnittliches (mittleres) Sicherheitsniveau in Unternehmen etablieren lässt.

Kapitel des IT-GSHB	Enthaltene Bausteine
Physische Infrastruktur	Gebäude; Verkabelung; Räume; Büroraum; Serverraum; Datenträgerarchiv; Raum für technische Infrastruktur; Schutzschränke; häuslicher Arbeitsplatz; Rechenzentrum
Nicht vernetzte Systeme und Clients	DOS-PC (ein Benutzer); Unix-System; Tragbarer PC; PCs mit wechselnden Benutzern; PC unter Windows NT; PC mit Windows 95; Windows 2000 Client; Internet-PC; allgemeines nicht vernetztes IT-System
Vernetzte Systeme und Server	Servergestütztes Netz; Unix-Server; Peer-to-Peer-Dienste; Windows NT Netz; Novell Netware 3.x; Novell Netware 4.x; Heterogene Netze; Netz- und Systemmanagement; Windows 2000 Server
Datenübertragungseinrichtungen	Datenträgeraustausch; Modem; Firewall; E-Mail; WWW-Server; Remote Access; Lotus Notes; Internet Information Server; Apache Webserver; Exchange/Outlook 2000
Telekommunikation	TK-Anlage; Faxgerät; Anrufbeantworter; LAN-Anbindung eines IT-Systems über ISDN; Faxserver; Mobiltelefon
Sonstige IT-Komponenten	Standardsoftware; Datenbanken; Telearbeit; Novell eDirectory; Archivierung
Übergeordnete Komponenten	IT-Sicherheitsmanagement; Organisation; Personal; Notfallvorsorge-Konzept; Datensicherungskonzept; Datenschutz; Computer-Virenschutzkonzept; Kryptokonzept; Behandlung von Sicherheitsvorfällen; Hard- und Software-Management; Outsourcing

Tabelle 6: Bausteine nach dem IT-Grundschutzhandbuch

Das IT-GSHB identifiziert sechs unterschiedliche Typen von IT-Komponenten, die spezifischen Bedrohungen ausgesetzt sind und jeweils in eigenständigen Kapiteln behandelt werden. In einem siebten Kapitel werden zudem übergeordnete Fragestellungen behandelt. Zu jedem thematischen Kapitel werden sog. „Bausteine“ identifiziert (Tabelle 6), die „die Gefährdungslage und die Maßnahmenempfehlungen für verschiedene Komponenten, Vorgehensweisen und IT-Systeme zusammenfassen“[24)]. Zu jedem Baustein wird auf Gefährdungen und auch auf Maßnahmenbündel verwiesen, die jeweils in zentralen Katalogen organisiert und dort ausführlich beschrieben sind.

---

23) BSI (2004), S. 14.

24) BSI (2004), S. 16.

Das IT-GSHB nimmt in seiner Verbreitung in Deutschland eine Spitzenreiterposition ein. Über 60% der Großunternehmen nutzen das GSHB[25)]. Aber auch in öffentlichen Organisationen und in KMU spielt das Handbuch eine wichtige Rolle. So sind über 30% der online registrierten Anwender Bundes-, Landes- und Kommunalbehörden[26)]. In unseren Gesprächen war das IT-GSHB in etwa der Hälfte der KMU bekannt und nahezu der einzige Standard, der wirklich auch in der praktischen Arbeit verwendet wurde. Dies bedeutet jedoch nicht, dass die Anwenderunternehmen in jedem Fall einen systematischen Grundschutz nach GSHB aufbauen. Die Mehrzahl der Unternehmen verwendet das GSHB punktuell, um sich über sichere IT-Lösungen zu informieren.

3.6 Information Technology Infrastructure Library

Die Information Technology Infrastructure Library (ITIL) ist eine mehrbändige Dokumentation von IT-Management-Prozessen, -Konzepten und -Methoden. Sie stellt damit ein Best- bzw. Common-Practice-Referenzmodell für das IT-Management dar. Ursprünglich von der britischen Central Computer and Telecommunications Agency Ende der 1980er Jahre für die Britische Regierung entwickelt, wird die ITIL inzwischen vom britischen Office of Government Commerce (OGC) herausgegeben. Das international tätige IT-Service-Management-Forum befasst sich zudem mit der Umsetzung des Standards in Prüfungsrichtlinien und dessen kontinuierlicher Weiterentwicklung[27)].

Motivation zur Entwicklung der ITIL war die Erkenntnis, dass Organisationen zunehmend von der IT abhängig sind und die Durchführung der Geschäftsprozesse dementsprechend klar definierte und zuverlässige IT-Dienstleistungen erfordern[28)]. Im Mittelpunkt der ITIL steht deshalb das IT-Servicemanagement mit den zwei Bereichen „Service-Delivery“ und „Service-Support“. Der erstere Bereich ist auf die Definition der Service Levels und den Entwurf der Services ausgerichtet. Er umfasst die Module „Capacity Management”, „Financial Management for IT Services”, „Availability Management“, „Service Level Management” und „IT Service Continuity Management”. Demgegenüber beschäftigt sich der zweite Bereich vor allem mit der Erbringung von IT-Dienstleistungen, dem „Incident Management / Service Desk“, dem „Problem Management“, dem „Configuration Management“, dem „Change Management“ und dem „Release Management“.

---

25) Vgl. Junginger, Krcmar (2004), S. 23.

26) Vgl. http://www.bsi.de/gshb/deutsch/etc/gshb_reg.htm, Abruf Dezember 2004.

27) URL: www.itsmf.de.

28) Vgl. ITSMF (2002), S. 31.

Das Service-Management wird ergänzt durch eine „Business Perspective“ auf die IT-Dienstleistungen, welche auch die Frage nach dem Sourcing der Services einschließt. Zudem beschäftigen sich die Aufgabenbereiche „Applications Management“ und „ICT Infrastructure Management“ mit der Entwicklung von Anwendungssystemen bzw. dem Aufbau der IK-technischen Infrastruktur (Abbildung 3).

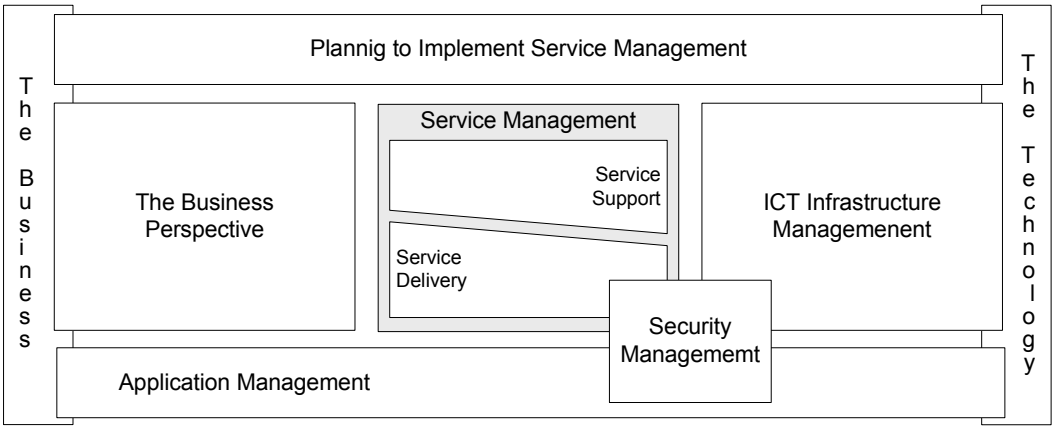


Abbildung 3: Aufgabenbereiche und Prozesse der ITIL[29)]

ITIL ist kein Standard, der primär auf Informationssicherheit bzw. Risikomanagement zielt. Jedes Modul der ITIL behandelt jedoch auch typische Probleme, aus denen sich Risiken und Bedrohungen für den jeweiligen Aufgabenbereich bzw. Serviceprozess ergeben können. Tabelle 7 zeigt exemplarisch Probleme der Planung und des Entwurfs einer Infrastruktur (Auszug aus dem Modul „ICT Infrastructure Management“).

Probleme in „Design and Planning”
• mangelhafte Selbstverpflichtung des Management • unzureichende(s) Ressourcen, Budget und Zeit • Mangel an Unternehmenszielen, Strategien, Politiken und Geschäftsausrichtung • ineffiziente Ressourcennutzung, dadurch Verschwendung von Zeit und Mitteln • Mangel an Kenntnissen über geschäftliche Wirkungen und Prioritäten • verschiedene und ungleiche Technologien und Anwendungen • Widerstand gegen Veränderungen • Mangel an Planung führt zu überstürzten Handlungen und ungeplanten Käufen • mangelhafter Abgleich zwischen der IKT und dem Geschäft • IKT diktiert dem Geschäft oder Geschäft diktiert die IKT • Mangel an Schulungen und fehlende Nachfolgeregelung beim Personalwechsel • Beschränkungen durch Altsysteme und -netzwerke • unrealistische Geschäftsanforderungen und zu hohe Erwartungen an die IKT

Tabelle 7: Entwurfs- und Planungsprobleme des „ICT Infrastructure Management“

29) Vgl. OGC (2002), Kap. 1.4.

Zur ITIL gehört zudem ein separates Dokument zum „Security Management“, welches einen Prozess für das IT Security Management mit den Phasen „Plan“, „Implement“, „Evaluate“ und „Maintain“ sowie einer kontinuierlichen Aktivität „Control“ sehr abstrakt beschreibt[30)]. Zudem werden, ebenfalls sehr allgemein gehalten, Beziehungen zwischen dem „Security Management“ und den einzelnen ITIL-Prozessen hergestellt. Da die Risiken in beiden Fällen sehr unspezifisch behandelt werden, leistet das „Security Management“ wenig konkrete Hilfestellung für das betriebliche IRiM.

Unternehmen können sich nach der Norm BS 15000 „Specification for IT-Servicemanagement“, die auf Inhalte von ITIL zugeschnitten ist, extern zertifizieren lassen. Die Akzeptanz von ITIL in der Praxis ist recht hoch. So fand ITIL nach einer Studie von 188 Unternehmen unterschiedlicher Größe und Branchen (vor allem IT- und Telekommunikation sowie produzierende Industrie) bereits 2003 in 36,7% der Unternehmen Anwendung[31)]. Auch in den KMU ist ITIL inzwischen als Trend erkannt, jedoch haben sich nur wenige der von uns befragten Unternehmen näher mit der ITIL befasst.

3.7 Informationssicherheit in der Bürokommunikation – VDI 5002

Die Richtlinie 5002 „Informationssicherheit in der Bürokommunikation“ (1993) ist Bestandteil des „Handbuch Bürokommunikation“ des Vereins Deutscher Ingenieure (VDI) e. V, dass in den neunziger Jahren mit dem Ziel entwickelt wurde, um „Unternehmen und die öffentliche Verwaltung bei Analyse, Planung und Einführung von Organisationskonzepten im Büro zu unterstützen“[32)]. Unter Informationssicherheit versteht der VDI den Zustand in dem die „Integrität“, „Verfügbarkeit“ und „Vertraulichkeit“ von Informationen und IT-Komponenten gewährleistet ist. Zielsetzung der VDI 5002 ist es, die Bedrohungen der Informationssicherheit von Bürokommunikationssystemen aufzuzeigen und die Erstellung eines Sicherheitskonzeptes zu unterstützen.

Als Gegenstand des Risiskomanagements identifiziert die VDI 5002 die sog. „IV-Landschaft“, die im Bürobereich vor allem Rechnersysteme mit Hard-, Software und Daten sowie Netzwerke mit eigenen Geräten und Leitungen umfasst. Bedrohungen resultieren jedoch nicht nur alleine aus dem Zusammenspiel dieser IK-technischen Komponenten, sondern auch aus deren Beziehungen zu Menschen, organisatorischem Umfeld, Ver- und Entsorgungs-

---

30) OGC (2002).

31) Kemper, Hadjicharalambous, Paschke (2004), S. 22-31.

32) VDI (1993), S. 2.

technik und der Umwelt (Natur)[33]. Die VDI 5002 empfiehlt dann ein „Phasenmodell für die Erarbeitung einer Sicherheitskonzeption“ für die IV-Landschaft[34]. Für die Phase der Maßnahmenentwicklung wird ein umfassender Maßnahmenkatalog aus den Bereichen Aufbau- und Ablauforganisation, IK-Technik (z. B. Verschlüsselung und Virenabwehr) und physische Sicherungsmaßnahmen (z. B. Schutz vor Einbruch und Diebstahl) vorgegeben.

Da die Richtlinie inzwischen sowohl IK-technisch als auch hinsichtlich der Anwendungsfelder überholt ist – insbesondere fehlt die gesamte Thematik interorganisatorischer Informationssysteme –, wird sie in der vorliegenden Form zukünftig immer weniger eine Rolle spielen. Allerdings sind VDI-Richtlinien in Deutschland, ähnlich wie DIN-Normen, im Allgemeinen hoch anerkannt[35]. Da sie VDI 5002 zudem vergleichsweise praxisverständlich geschrieben ist, ist davon auszugehen, dass sie heute durchaus (noch) verwendet wird. Über die Zahl der Anwendungen des liegen den Autoren allerdings keine Studienergebnisse vor. In den von uns befragten KMU war die VDI Richtlinie – wie die meisten anderen Normen – nur in Einzelfällen bekannt.

4 Inhaltliche Beiträge der Normen und Standards

4.1 Risikofelder der betrieblichen Informationsverarbeitung

Ein Vergleich der Inhalte der vorgestellten Normen und Standards macht deutlich, dass diese z. T. recht unterschiedliche Arten von Risiken thematisieren. Grundsätzlich lassen sich diese Risiken nach dem Bezugsobjekt in Betriebsrisiken und Entwicklungsrisiken unterscheiden[36]. Abbildung 4 stellt die Risikofelder grafisch dar. Die Informationsinfrastruktur (grau unterlegt) umfasst alle Voraussetzungen für eine effektive Information und Kommunikation im Unternehmen. Dazu zählen neben den Hardware- und Softwarekomponenten auch organisatorische Regeln und Anwenderqualifikationen. Die als weiße Rechtecke dargestellten Bereiche stellen Aufgaben dar, die in Zusammenhang mit der Aufrechterhaltung und Weiterentwicklung einer Informationsinfrastruktur (IIS) wahrzunehmen sind. Diese Aufgaben werden typischerweise vom betrieblichen IV-Bereich wahrgenommen. Ein Großteil der Aufgaben befasst sich mit dem laufenden Betrieb der IIS. Nicht zu unterschätzen sind jedoch auch die Planung und Wei-

---

33) Vgl. VDI (1993), S. 14 ff.

34) Vgl. VDI (1993), S. 19 ff.

35) Vgl. DIN (2000), S. 9 ff.

36) Zur hier vorgenommenen Abgrenzung und Identifikation der Risikofelder des Informationsmanagements vgl. Teubner (2003).

terentwicklung der IIS, um sicherzustellen, dass diese auch zukünftig den betrieblichen Herausforderungen gerecht wird.

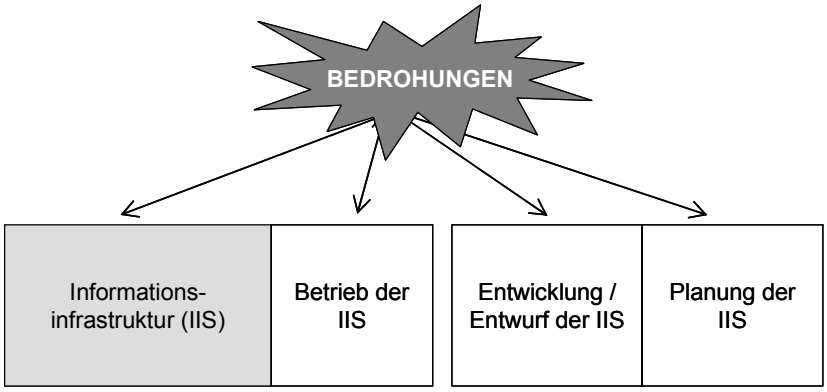


Abbildung 4: Risikofelder der betrieblichen Informationsverarbeitung

Die Betriebsrisiken beziehen sich auf Ausfälle oder Störungen der IIS. Diese können die Technik (z. B. Ausfall des Netzwerks), die Anwendungssysteme (z. B. Störungen durch fehlerhafte Bedienung) oder die Organisation (z. B. unerlaubter Zugriff auf Rechner oder Datenbestände) betreffen. Das Betriebsrisiko wird allerdings nicht alleine durch den Zustand der IIS bestimmt, sondern hängt auch von den laufenden Tätigkeiten in der Wartung und dem Betrieb ab. So kann etwa ein gutes User-Help-Desk zu einem reibungslosen Einsatz der Infrastruktur beitragen und Störungen durch Fehlbedienung vorbeugen. Auch eine regelmäßige Überprüfung und Wartung kann das Risiko von Fehlern und Störungen senken. Sofern Störungen auftreten ist zudem entscheidend, wie schnell diese behoben und welche Überbrückungsmaßnahmen in der Zwischenzeit durchgeführt werden.

Die Betriebsrisiken stehen oft im Mittelpunkt der Diskussion um Sicherheit und Bedrohungen der Informationsverarbeitung. Darüber hinaus ist allerdings auch die Weiterentwicklung der Infrastruktur mit Risiken behaftet. Die meiste Beachtung in der Fachliteratur finden hier wohl die Projektrisiken („doing the project right“)[37)]. Dagegen oft übersehen werden Risiken in der (strategischen) Planung der Infrastruktur („doing the right projects“). KRCMAR und JUNGINGER weisen hier insbesondere auf die Risiken hin, mit denen das Investitionsportfolio behaftet ist[38)]. Gerade die Planung einer zukunftsträchtigen IIS ist jedoch sowohl in Anbetracht der hohen Dynamik des betrieblichen Wandels als auch der schnellen Entwicklung und Komplexität der Informationstechnologie mit vielen Unsicherheiten behaftet.

---

37) Vgl. z. B. Wallmüller (2004); Krcmar, Junginger (2004).

38) Vgl. Krcmar, Junginger (2004).

In unserer Befragung wurde deutlich, dass sich die Mehrzahl der betrieblichen Sicherheitsmaßnahmen in KMU auf die Ausfallrisiken richtet. Als vorherrschende Bedrohungen sahen die von uns befragten Führungskräfte „Spam“, „Viren“ oder „unerlaubte Zugriffe“ an. Darüber hinaus wurden Betriebsrisiken sowohl organisatorischer Art als auch durch eigene Mitarbeiter, als wichtige Risikofaktoren identifiziert. Deutlich dahinter, aber auch noch als wichtig eingestuft wurden Bedrohungen durch Elementarschäden wie physikalische Zerstörung. Allerdings richtet sich auch ein gutes Viertel der Maßnahmen auf Risiken bei der Planung und Entwicklung der IIS. Als Risikofelder wurden die Technologieplanung, die Auswahl von Lieferanten, die Kooperation mit externen Dienstleistern, der Projektplanung und auch die Personalplanung genannt.

4.2 Ergebnisse

Ordnet man die inhaltlichen Beiträge der vorgestellten Normen und Standards den Risikofeldern aus Abbildung 4 zu, so ergibt sich die in Tabelle 8 dargestellte Schwerpunktsetzung.

Norm \ Teil der IT	Informations-infrastruktur	Betrieb	Entwicklung/ Entwurf	strategisches Management
CobiT	++ Technik, Systeme, Organisation	++	++	+
DIN ISO/IEC 15408	++ Technik, Systeme	-	o	-
ISO/IEC 17799	++ Technik, Systeme, Organisation	++	+	o
ISO/IEC TR 13335	++ Technik, Systeme	+	-	-
IT-Grundschutz-handbuch	++ Technik, Systeme, Organisation	+	-	-
ITIL	+ Systeme	++	++	+
VDI 5002	+ Technik, Systeme	+	-	-

Legende: (-) nicht berücksichtigt, (o) erwähnt, (+) partiell berücksichtigt, (++) umfassender berücksichtigt

Tabelle 8: Inhaltliche Schwerpunkte der analysierten Normen und Standards

Die Beiträge der analysierten Standards liegen eindeutig im Bereich der IIS und der Risiken des laufenden Betriebs. Die ISO/IEC 15408, der Technische Report 13335 und das IT-Grundschutzhandbuch legen ihren Fokus auf die IIS und die Sicherheit ihrer Komponenten. Während ersterer Standard sich ausschließlich auf Maßnahmen bei der Entwicklung von IT-Komponenten konzentriert, betrachten letztere auch deren Einsatz und den Betrieb der IIS.

Hierbei geht das IT-GSHB sehr viel detaillierter auf konkrete Sicherheitsmaßnahmen und Vorkehrungen ein als der TR 13335. Insbesondere werden im IT-GSHB auch organisatorische Risiken adressiert. Weniger konkret ist die ISO/IEC 17799, die jedoch in der Identifikation von Betriebsrisiken der IIS weiter geht als TR 13335 und IT-GSHB. Darüber hinaus werden auch die (technischen) Risiken der Systementwicklung betrachtet.

Überraschend breit ist der Beitrag der ITIL zur Risikoabdeckung: obwohl sie nicht primär auf die Ausgestaltung des Risikomanagements zielt, werden in der ITIL Risikoaspekte nicht nur des Betriebs der IIS, sondern auch Projektrisiken und z. T. auch Managementrisiken explizit angesprochen. Am umfassendsten werden die Risiken im CobiT-Standard berücksichtigt, der sowohl die IIS hinsichtlich Technik, Anwendungssystemen und Organisation als auch Risiken in Zusammenhang mit dem Betrieb, der Planung und Entwicklung der IIS gut abdeckt.

5 Fazit und Diskussion

Unsere Untersuchung führt uns zu dem Ergebnis, dass die vorliegenden Normen und Standards das IRiM bereits in wesentlichen Aufgabenfeldern adressieren. Erste wenn auch nicht repräsentative empirische Untersuchungen weisen auf eine gewisse Verbreitung der Standards in größeren Unternehmen hin. In unseren Interviews kommen wir allerdings zu dem Ergebnis, dass die Herausforderungen in KMUs anders wahrgenommen werden, als in den Normen und Standards niedergelegt [vgl. auch Kraft & Seidel 2004]. Bisher werden die vorliegenden Normen und Standards in KMUs nur wenig zu rezipiert. Demzufolge werden für das IRiM meist „hauseigene“ Konzepte eingesetzt. Allerdings ist ein Problembewusstsein ebenso vorhanden wie die generelle Bereitschaft, zukünftig das betriebliche IRiM systematischer zu betreiben.

In unsrer Befragung wurden allerdings auch einige Restriktionen für die Nutzung der Standards in der Praxis deutlich, die sich z. T. sicherlich auch auf größere Unternehmen übertragen lassen. So wurde von einigen Praktikern die Komplexität der Normen-Werke kritisiert. Schwierige Sprachregelungen und die oft abstrakten Maßnahmen und Modelle stellten weitere wesentliche Einstiegsbarrieren dar. Hinzu kommen die sehr unterschiedlichen Herangehensweisen der Standards an die Risikoproblematik, die es schwierig machten, diese zu vergleichen und die Vor- und Nachteile abzuschätzen. Auch wenn Unternehmen den Aufwand zum Aufbau eines normgerechten IRiM-Systems nicht scheuen, bleibt immer noch eine gewisse Unsicherheit darüber, wie effektiv ein nach diesen Standards aufgebautes IRiM letztlich sein wird.

Literatur

TSO, OGC: The Stationary Office, Office of Government Commerce (Hrsg.): Security Management. London 2002.

British Standards Institution (Hrsg.): Information Security management systems - Specification with guidance for use. BS 7799-2:2002. London 2002.

BSI – Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutzhandbuch. Bonn 2004.

DIN – Deutsches Institut für Normung e.V. (Hrsg.): IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit – Teil 1: Einführung und allgemeines Modell. DIN ISO/IEC 15408-1:2001. Berlin 2001.

DIN – Deutsches Institut für Normung e.V. (Hrsg.): IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit – Teil 2: Funktionale Sicherheitsanforderungen. DIN ISO/IEC 15408-2:2001. Berlin 2001.

DIN – Deutsches Institut für Normung e.V. (Hrsg.): IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit – Teil 3: Anforderungen an die Vertrauenswürdigkeit. DIN ISO/IEC 15408-3:2001. Berlin 2001.

ISACA – Information Systems Audit and Control Association / Switzerland Chapter (Hrsg.): COBIT 3rd edition – Der internationale Standard für IT-Governance. Zürich 2001.

ISO, IEC - International Organization for Standardization, International Electrotechnical Commission (Hrsg.): Information technology – Code of practice for information security management. ISO/IEC 17799:2000. Genf 2000.

ISO, IEC - International Organization for Standardization; International Electrotechnical Commission (Hrsg.): Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security. ISO/IEC TR 13335-1:1996. Genf 1996.

ISO, IEC - International Organization for Standardization, International Electrotechnical Commission (Hrsg.): Guidelines for the management of IT Security – Part 2: Managing and planning IT-Security. ISO/IEC TR 13335-2:1997. Genf 1997.

ISO, IEC - International Organization for Standardization, International Electrotechnical Commission (Hrsg.): Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security. ISO/IEC TR 13335-3:1998. Genf 1998.

ISO, IEC - International Organization for Standardization, International Electrotechnical Commission (Hrsg.): Guidelines for the management of IT Security – Part 4: Selection of Safeguards. ISO/IEC TR 13335-4:2000. Genf 2000.

ISO, IEC - International Organization for Standardization, International Electrotechnical Commission (Hrsg.): Guidelines for the management of IT Security – Part 5: Safeguards for external connections. ISO/IEC TR 13335-5:2001. Genf 2001.

ISO, IEC - International Organization for Standardization; International Electrotechnical Commission (Hrsg.): Information Technology Security Techniques – Management of Information and Communications Technology Security – Part 1: Concepts and models for Information and Communications Technology Security Management. ISO/IEC 13335-1:2004. Genf 2004.

ITGI - IT Governance Institute (Hrsg.): COBIT Mapping – Overview of international IT guidance. Rolling Meadows, IL 2004.

ITSMF – IT Service Management Forum (Hrsg.): IT Service Management – eine Einführung. Zaltbommel 2002.

Junginger, M., Krcmar, H.: Wahrnehmung und Steuerung von Risiken im Informationsmanagement – Eine Befragung deutscher IT-Führungskräfte. In: Studien des Lehrstuhl für Wirtschaftsinformatik, Technische Universität München, Nr. 1. Garching 2004.

Junginger, M., Krcmar, H.: Risikomanagement im Informationsmanagement – Eine spezifische Aufgabe des IV-Controllings. In: Information Management & Consulting 18 (2003) 2, S. 16-23.

Kemper, H.-G., Hadjicharalambous, E., Paschke, J.: IT-Servicemanagement in deutschen Unternehmen – Ergebnisse einer empirischen Studie zu ITIL. In: HMD – Praxis der Wirtschaftsinformatik 237 (2004) Juni, S. 21-31.

Kraft, R.; Seidel, J.: IT-Sicherheit für den Mittelstand. In: HMD Praxis der Wirtschaftsinformatik 240 (2004) Dezember, S. 57-66.

Rausch, T.; Disterer, G.: Indentifikation und Analyse von Risiken im IT-Bereich. In: HMD Praxis der Wirtschaftsinformatik 236 (2004) April, S. 19-32.

Teufl, S.; Schlienger, T.: Informationssicherheit – Wege zur kontrollierten Unsicherheit. In: HMD Praxis der Wirtschaftsinformatik, Heft 216 (2000) Dezember, S. 18-31.

Teubner, R. A.: Grundlegung Informationsmanagement. Arbeitsbericht Nr. 91 des Instituts für Wirtschaftsinformatik, Universität Münster, Februar 2003.

Thamm, J.: Assessments von IT-Organisationen. In: Information Management & Consulting (2004) 19, S. 65-71.

TSO, OGC - The Stationary Office, Office of Government Commerce (Hrsg.): Service Delivery. 2. Aufl., Norwich 2002.

VDI - Verein Deutscher Ingenieure (Hrsg.): Bürokommunikation: Informationssicherheit in der Bürokommunikation. VDI 5002. Düsseldorf 1993.

Wallmüller, E.: Risikomanagement für IT- und Softwareprojekte. Ein Leitfaden für die Umsetzung in der Praxis. München, Wien 2004.

Arbeitsberichte des Instituts für Wirtschaftsinformatik

Nr. 1 Bolte, Ch., Kurbel, K., Moazzami, M., Pietsch, W.: Erfahrungen bei der Entwicklung eines Informationssystems auf RDBMS- und 4GL-Basis; Februar 1991.

Nr. 2 Kurbel, K.: Das technologische Umfeld der Informationsverarbeitung - Ein subjektiver 'State of the Art'-Report über Hardware, Software und Paradigmen; März 1991.

Nr. 3 Kurbel, K.: CA-Techniken und CIM; Mai 1991.

Nr. 4 Nietsch, M., Nietsch, T., Rautenstrauch, C., Rinschede, M., Siedentopf, J.: Anforderungen mittelständischer Industriebetriebe an einen elektronischen Leitstand - Ergebnisse einer Untersuchung bei zwölf Unternehmen; Juli 1991.

Nr. 5 Becker, J., Prischmann, M.: Konnektionistische Modelle - Grundlagen und Konzepte; September 1991.

Nr. 6 Grob, H.L.: Ein produktivitätsorientierter Ansatz zur Evaluierung von Beratungserfolgen; September 1991.

Nr. 7 Becker, J.: CIM und Logistik; Oktober 1991.

Nr. 8 Burgholz, M., Kurbel, K., Nietsch, Th., Rautenstrauch, C.: Erfahrungen bei der Entwicklung und Portierung eines elektronischen Leitstands; Januar 1992.

Nr. 9 Becker, J., Prischmann, M.: Anwendung konnektionistischer Systeme; Februar 1992.

Nr. 10 Becker, J.: Computer Integrated Manufacturing aus Sicht der Betriebswirtschaftslehre und der Wirtschaftsinformatik; April 1992.

Nr. 11 Kurbel, K., Dornhoff, P.: A System for Case-Based Effort Estimation for Software-Development Projects; Juli 1992.

Nr. 12 Dornhoff, P.: Aufwandsplanung zur Unterstützung des Managements von Softwareentwicklungsprojekten; August 1992.

Nr. 13 Eicker, S., Schnieder, T.: Reengineering; August 1992.

Nr. 14 Erkelenz, F.: KVD2 - Ein integriertes wissensbasiertes Modul zur Bemessung von Krankenhausverweildauern - Problemstellung, Konzeption und Realisierung; Dezember 1992.

Nr. 15 Horster, B., Schneider, B., Siedentopf, J.: Kriterien zur Auswahl konnektionistischer Verfahren für betriebliche Probleme; März 1993.

Nr. 16 Jung, R.: Wirtschaftlichkeitsfaktoren beim integrationsorientierten Reengineering: Verteilungsarchitektur und Integrationsschritte aus ökonomischer Sicht; Juli 1993.

Nr. 17 Miller, C., Weiland, R.: Der Übergang von proprietären zu offenen Systemen aus Sicht der Transaktionskostentheorie; Juli 1993.

Nr. 18 Becker, J., Rosemann, M.: Design for Logistics - Ein Beispiel für die logistikgerechte Gestaltung des Computer Integrated Manufacturing; Juli 1993.

Nr. 19 Becker, J., Rosemann, M.: Informationswirtschaftliche Integrationsschwerpunkte innerhalb der logistischen Subsysteme - Ein Beitrag zu einem produktionsübergreifenden Verständnis von CIM; Juli 1993.

Nr. 20 Becker, J.: Neue Verfahren der entwurfs- und konstruktionsbegleitenden Kalkulation und ihre Grenzen in der praktischen Anwendung; Juli 1993.

Nr. 21 Becker, K.; Prischmann, M.: VESKONN - Prototypische Umsetzung eines modularen Konzepts zur Konstruktionsunterstützung mit konnektionistischen Methoden; November 1993

Nr. 22 Schneider, B.: Neuronale Netze für betriebliche Anwendungen: Anwendungspotentiale und existierende Systeme; November 1993.

Nr. 23 Nietsch, T.; Rautenstrauch, C.; Rehfeldt, M.; Rosemann, M.; Turowski, K.: Ansätze für die Verbesserung von PPS-Systemen durch Fuzzy-Logik; Dezember 1993.

Nr. 24 Nietsch, M.; Rinschede, M.; Rautenstrauch, C.: Werkzeuggestützte Individualisierung des objektorientierten Leitstands ooL; Dezember 1993.

Nr. 25 Meckenstock, A.; Unland, R.; Zimmer; D.: Flexible Unterstützung kooperativer Entwurfsumgebungen durch einen Transaktions-Baukasten; Dezember 1993.

Nr. 26 Grob, H. L.: Computer Assisted Learning (CAL) durch Berechnungsexperimente; Januar 1994.

Nr. 27 Kirn, St.; Unland, R. (Hrsg.): Tagungsband zum Workshop "Unterstützung Organisatorischer Prozesse durch CSCW". In Kooperation mit GI-Fachausschuß 5.5 "Betriebliche Kommunikations- und Informationssysteme" und Arbeitskreis 5.5.1 "Computer Supported Cooperative Work", Westfälische Wilhelms-Universität Münster, 4.-5. November 1993; März 1994.

Nr. 28 Kirn, St.; Unland, R.: Zur Verbundintelligenz integrierter Mensch-Computer-Teams: Ein organisationstheoretischer Ansatz; März 1994.

Nr. 29 Kirn, St.; Unland, R.: Workflow Management mit kooperativen Softwaresystemen: State of the Art und Problemabriß; März 1994.

Nr. 30 Unland, R.: Optimistic Concurrency Control Revisited; März 1994.

Nr. 31 Unland, R.: Semantics-Based Locking: From Isolation to Cooperation; März 1994.

Nr. 32 Meckenstock, A.; Unland, R.; Zimmer, D.: Controlling Cooperation and Recovery in Nested Transactions; März 1994.

Nr. 33 Kurbel, K.; Schnieder, T.: Integration Issues of Information Engineering Based I-CASE Tools; September 1994.

Nr. 34 Unland, R.: TOPAZ: A Tool Kit for the Construction of Application Specific Transaction; November 1994.

Nr. 35 Unland, R.: Organizational Intelligence and Negotiation Based DAI Systems - Theoretical Foundations and Experimental Results; November 1994.

Nr. 36 Unland, R.; Kirn, St.; Wanka, U.; O'Hare, G.M.P.; Abbas, S.: AEGIS: AGENT ORIENTED ORGANISATIONS; Februar 1995.

Nr. 37 Jung, R.; Rimpler, A.; Schnieder, T.; Teubner, A.: Eine empirische Untersuchung von Kosteneinflußfaktoren bei integrationsorientierten Reengineering-Projekten; März 1995.

Nr. 38 Kirn, St.: Organisatorische Flexibilität durch Workflow-Management-Systeme?; Juli 1995.

Nr. 39 Kirn, St.: Cooperative Knowledge Processing: The Key Technology for Future Organizations; Juli 1995.

Nr. 40 Kirn, St.: Organisational Intelligence and Distributed AI; Juli 1995.

Nr. 41 Fischer, K.; Kirn, St.; Weinhard, Ch. (Hrsg.): Organisationsaspekte in Multiagentensystemen; September 1995.

Nr. 42 Grob, H. L.; Lange, W.: Zum Wandel des Berufsbildes bei Wirtschaftsinformatikern, Eine empirische Analyse auf der Basis von Stellenanzeigen; Oktober 1995.

Nr. 43 Abu-Alwan, I.; Schlagheck, B.; Unland, R.: Evaluierung des objektorientierten Datenbankmanagementsystems ObjectStore, Dezember 1995.

Nr. 44 Winter, R., Using Formalized Invariant Properties of an Extended Conceptual Model to Generate Reusable Consistency Control for Information Systems; Dezember 1995.

Nr. 45 Winter, R., Design and Implementation of Derivation Rules in Information Systems; Februar 1996.

Nr. 46 Becker, J.: Eine Architektur für Handelsinformationssysteme; März 1996.

Nr. 47 Becker, J.; Rosemann, M. (Hrsg.): Workflowmanagement - State-of-the-Art aus Sicht von Theorie und Praxis, Proceedings zum Workshop vom 10. April 1996; April 1996.

Nr. 48 Rosemann, M.; zur Mühlen, M.: Der Lösungsbeitrag von Metadatenmodellen beim Vergleich von Workflowmanagementsystemen; Juni 1996.

Nr. 49 Rosemann, M.; Denecke, Th.; Püttmann, M.: Konzeption und prototypische Realisierung eines Informationssystems für das Prozeßmonitoring und -controlling; September 1996.

Nr. 50 Uthmann, C. v.; Turowski, K.; unter Mitarbeit von Rehfeldt, M.; Skall, M.: Workflowbasierte Geschäftsprozeßregelung als Konzept für das Management von Produktentwicklungs-prozessen; November 1996.

Nr. 51 Eicker, S.; Jung, R.; Nietsch, M.; Winter, R.: Entwicklung eines Data Warehouse für das Produktionscontrolling: Konzepte und Erfahrungen; November 1996.

Nr. 52 Becker, J.; Rosemann, M., Schütte, R. (Hrsg.): Entwicklungsstand und Entwicklungsperspektiven der Referenzmodellierung, Proceedings zur Veranstaltung vom 10. März 1997; März 1997.

Nr. 53 Loos, P.: Capture More Data Semantic Through The Expanded Entity-Relationship Model (PERM); Februar 1997.

Nr. 54 Becker, J., Rosemann, M. (Hrsg.): Organisatorische und technische Aspekte beim Einsatz von Workflowmanagementsystemen. Proceedings zur Veranstaltung vom 10. April 1997; April 1997.

Nr. 55 Holten, R., Knackstedt, R.: Führungsinformationssysteme - Historische Entwicklung und Konzeption; April 1997.

Nr. 56 Holten, R.: Die drei Dimensionen des Inhaltsaspektes von Führungsinformationssystemen; April 1997.

Nr. 57 Holten, R., Striemer, R., Weske, M.: Ansätze zur Entwicklung von Workflow-basierten Anwendungssystemen - Eine vergleichende Darstellung; April 1997.

Nr. 58 Kuchen, H.: Arbeitstagung Programmiersprachen, Tagungsband; Juli 1997.

Nr. 59 Vering, O.: Berücksichtigung von Unschärfe in betrieblichen Informationssystemen - Einsatzfelder und Nutzenpotentiale am Beispiel der PPS; September 1997.

Nr. 60 Schwegmann, A., Schlagheck, B.: Integration der Prozeßorientierung in das objektorientierte Paradigma: Klassenzuordnungsansatz vs. Prozessklassenansatz; Dezember 1997.

Nr. 62 Wiese, J.: Ein Entscheidungsmodell für die Auswahl von Standardanwendungssoftware am Beispiel von Warenwirtschaftssystemen; März 1998.

Nr. 63 Kuchen, H.: Workshop on Functional and Logic Programming, Proceedings; Juni 1998.

Nr. 64 Uthmann, C. v.; Becker, J.; Brödner, P.; Maucher, I.; Rosemann, M.: PPS meets Workflow. Proceedings zum Workshop vom 9. Juni 1998.

Nr. 65 Scheer, A.-W.; Rosemann, M.; Schütte, R. (Hrsg.): Integrationsmanagement; Januar 1999.

Nr. 66 zur Mühlen, M.: Internet - Technologie und Historie; Juni 1999.

Nr. 67 Holten R.: A Framework for Information Warehouse Development Processes; Mai 1999.

Nr. 68 Holten R.; Knackstedt, R.: Fachkonzeption von Führungsinformationssystemen - Instanziierung eines FIS-Metamodells am Beispiel eines Einzelhandelsunternehmens; Mai 1999.

Nr. 69 Holten, R.: Semantische Spezifikation Dispositiver Informationssysteme; Juli 1999.

Nr. 70 Becker, J.; zur Mühlen, M.; Rosemann, M. (Eds.): Workflow Management 1999. Proceedings of the 1999 Workflow Management Conference: Workflow-based Applications; November 1999.

Nr. 71 Klein, S.; Schneider, B.; Vossen, G.; Weske, M.; Projektgruppe PESS: Eine XML-basierte Systemarchitektur zur Realisierung flexibler Web-Applikationen; Juli 2000.

Nr. 72 Klein, S.; Schneider, B. (Hrsg): Negotiations and Interactions in Electronic Markets, Proceedings of the Sixth Research Symposium on Emerging Electronic Markets, Muenster, Germany, September 19 - 21, 1999; August 2000.

Nr. 73 Becker, J.; Bergerfurth, J.; Hansmann, H.; Neumann, S.; Serries, T.: Methoden zur Einführung Workflow-gestützter Architekturen von PPS-Systemen; November 2000.

Nr. 74 Terveer, I.: Die asymptotische Verteilung der Spannweite bei Zufallsgrößen mit paarweise identischer Korrelation; März 2002.

Nr. 75 Becker, J. (Ed.): Research Reports, Proceedings of the University Alliance Executive Directors Workshop – ECIS 2001; Juni 2001.

Nr. 76, Klein, S.; u.a. (Eds.): MOVE: Eine flexible Architektur zur Unterstützung des Außendienstes mit mobile devices (in Vorbereitung).

Nr. 77 Knackstedt, R.; Holten, R.; Hansmann, H.; Neumann, St.: Konstruktion von Methodiken: Vorschläge für eine begriffliche Grundlegung und domänenspezifische Anwendungsbeispiele; Juli 2001.

Nr. 78 Holten, R.: Konstruktion domänenspezifischer Modellierungstechniken für die Modellierung von Fachkonzepten; August 2001.

Nr. 79 Vossen, G.; Hüsemann, B.; Lechtenbörger, J.: XLX – Eine Lernplattform für den universitären Übungsbetrieb, August 2001.

Nr. 80 Knackstedt, R.; Serries, Th.: Gestaltung von Führungsinformationssystemen mittels Informationsportalen; Ansätze zur Integration von Data-Warehouse- und Content-Management-Systemen, November 2001.

Nr. 81 Holten, R.: Conceptual Models as Basis for the Integrated Information Warehouse Development, Oktober 2001.

Nr. 82 Teubner, R. A.: Informationsmanagement: Disziplinärer Kontext, Historie und Stand der Wissenschaft, Februar 2002.

Nr. 83 Vossen, G.: Vernetzte Hausinformationssysteme – Stand und Perspektive; Oktober 2001.

Nr. 84 Holten, R.: The MetaMIS Approach for the Specification of Management Views on Business Processes, November 2001.

Nr. 85 Becker, J.; Neumann, S.; Hansmann, H.: Workflow-integrierte Produktionsplanung und -steuerung: Ein Architekturmodell für die Koordination von Prozessen der industriellen Auftragsabwicklung; Januar 2002.

Nr. 86 Teubner, R. A.; Klein, S.: Bestandsaufnahme aktueller deutschsprachiger Lehrbücher zum Informationsmanagement; März 2002.

Nr. 87 Holten, R.: Specification of Management Views in Information Warehouse Projects; April 2002.

Nr. 88 Holten, R.; Dreiling, A.: Specification of Fact Calculations within the MetaMIS Approach; Juni 2002.

Nr. 89 Holten, R.: Metainformationssysteme – Backbone der Anwendungssystemkopplung; Juli 2002.

Nr.90 Becker, J.; Knackstedt, R.: Referenzmodellierung 2002. Methoden – Modelle – Erfahrungen; August 2002.

Nr. 91 Teubner, R. A.: Grundlegung Informationsmanagement; Februar 2003.

Nr. 92 Vossen, G.; Westerkamp, P.: E-Learning as a Web Service; Februar 2003

Nr. 93 Becker, J.; Holten, R.; Knackstedt, R.; Niehaves, B.: Forschungsmethodische Positionierung in der Wirtschaftsinformatik – epistemologische, ontologische und linguistische Leitfragen; Mai 2003.

Nr. 94 Algermissen, L.; Niehaves, B.: E-Government – State of the art and development perspectives; April 2003.

Nr. 95 Teubner, R. A.; Hübsch, T.: Is Information Management a Global Discipline? Assessing Anglo-American Teaching and Literature by a Web Contents Analysis; Oktober 2003.

Nr. 96 Teubner, R. A.: Information Resource Management; November 2003.

Nr. 97 Köhne, Frank; Klein, Stefan: Prosuming in der Telekommunikationsbranche: Eine Delphi-Studie; November 2003.

Nr. 98 Vossen, G.; Pankratius, V.: Towards E-Learning Grids: Using Grid Computing in Electronic Learning; September 2003.

Nr. 99 Vossen, G., Paul, H.: Tagungsband EMISA 2003: Auf dem Weg in die E-Gesellschaft; Oktober 2003.

Nr. 100 Vossen, G.; Vidyasankar K.: A Multi-Level Model for Web Service Composition; Oktober 2003.

Nr. 101 Becker, J.; Dreiling, A.; Serries, T.: Datenschutz als Rahmen für das Customer-Relationship-Management – Einfluss des geltenden Rechts auf die Spezifikation von Führungsinformationssystemen, November 2003.

Nr. 102 Müller, R.A.; Lembeck, C.; Kuchen, H.: A GlassTT – A Symbolic Java Virtual Machine using Constraint Solving Techniques; November 2003.

Nr. 103 Becker, J; Brelage C.; Crisandt J.; Dreiling A.; Holten R.; Ribbert M.; Seidel S.: Methodische und technische Integration von Daten- und Prozessmodellierungstechniken für Zwecke der Informationsbedarfsanalyse; März 2004.

Nr. 104 Teubner, R. A.: Information Technology Management; April 2004.

Nr. 105 Teubner, R. A.: Information Systems Management; August 2004.

Nr. 106 Becker, J.; Brelage, C.; Gebhardt, Hj.; Recker, J.; Müller-Wienbergen, F.: Fachkonzeptionelle Modellierung und Analyse web-basierter Informationssysteme mit der MW-KiD Modellierungstechnik am Beispiel von ASInfo, Mai 2004.

Nr. 107 Hagemann, S.; Rodewald, G.; Vossen, G.; Westerkamp, P.; Albers, F.; Voigt, H.: BoGSy - ein Informationssystem für Botanische Gärten, September 2004.

Nr. 108 Schneider, B.; Totz, C.: Web-gestützte Konfiguration komplexer Produkte und Dienstleistungen, September 2004.

Nr. 109 Algermissen, L; Büchel, N.; Delfmann, P.; Dümmer, S.; Drawe, S.; Falk, T.; Hinzen, M.; Meesters, S.; Müller, T.; Niehaves, B.; Niemeyer, G.; Pepping, M.; Robert, S.; Rosenkranz, C.; Stichnote, M.; Wienefoet, T.: Anforderungen an Virtuelle Rathäuser - Ein Leitfaden für die herstellerunabhängige Softwareauswahl, Oktober 2004.

Nr. 110 Algermissen, L; Büchel, N.; Delfmann, P.; Dümmer, S.; Drawe, S.; Falk, T.; Hinzen, M.; Meesters, S.; Müller, T.; Niehaves, B.; Niemeyer, G.; Pepping, M.; Robert, S.; Rosenkranz, C.; Stichnote, M.; Wienefoet, T.: Fachkonzeptionelle Spezifikation von Virtuellen Rathäusern - Ein Konzept zur Unterstützung der Implementierung, Oktober 2004.

Nr. 111 Becker, J.; Janiesch, C.; Pfeiffer, D.; Rieke, T.; Winkelmann, A.: Studie: Verteilte Publikationserstellung mit Microsoft Word und den Microsoft SharePoint Services, Dezember 2004.

Nr. 112 Teubner, R. A.; Terwey, J.: Informations-Risiko-Management: Der Beitrag aktueller internationaler Normen und Standards, April 2005.

Institut für Wirtschaftsinformatik
Leonardo-Campus 3
48149 Münster
http://www.wi.uni-muenster.de

ISSN 1438-3985