Klotz, Michael

Working Paper

Regelwerke der IT-Compliance - Klassifikation und Übersicht, Teil 2: Normen

SIMAT Arbeitspapiere, No. 05-13-024

Provided in Cooperation with:
Hochschule Stralsund, Stralsund Information Management Team (SIMAT)

Suggested Citation: Klotz, Michael (2013) : Regelwerke der IT-Compliance - Klassifikation und Übersicht, Teil 2: Normen, SIMAT Arbeitspapiere, No. 05-13-024, Fachhochschule Stralsund, Stralsund Information Management Team (SIMAT), Stralsund, https://nbn-resolving.de/urn:nbn:de:0226-simat05130240

This Version is available at:
https://hdl.handle.net/10419/88419

SIMAT Arbeitspapiere
Herausgeber: Prof. Dr. Michael Klotz

SIMAT AP 05-13-024

Regelwerke der IT-Compliance – Klassifikation und Übersicht Teil 2: Normen

Prof. Dr. Michael Klotz

Fachhochschule Stralsund
SIMAT Stralsund Information Management Team

August 2013

ISSN 1868-064X

Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2013 (SIMAT AP, 5 (2013), 24), ISSN 1868-064X

Download über URN vom Server der Deutschen Nationalbibliothek:
http://nbn-resolving.de/urn:nbn:de:0226-simat05130240

Impressum
Fachhochschule Stralsund
SIMAT Stralsund Information Management Team
Zur Schwedenschanze 15
18435 Stralsund
www.fh-stralsund.de
www.simat.fh-stralsund.de

Herausgeber
Prof. Dr. Michael Klotz
Fachbereich Wirtschaft
Zur Schwedenschanze 15
18435 Stralsund
E-Mail: michael.klotz@fh-stralsund.de

Autor

Prof. Dr. Michael Klotz lehrt und forscht am Fachbereich Wirtschaft der FH Stralsund auf den Gebieten der Unternehmensorganisation und des Informationsmanagements. Er ist u. a. Wissenschaftlicher Leiter des SIMAT, regionaler Ansprechpartner der gfo Gesellschaft für Organisation e.V., Mitglied des wissenschaftlichen Beirats und Academic Advocate der ISACA sowie Mitherausgeber der Zeitschrift „IT-Governance“.

Regelwerke der IT-Compliance – Klassifikation und Übersicht Teil 2: Normen

Prof. Dr. Michael Klotz[1]

Zusammenfassung: IT-Compliance bezeichnet einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden. Diese Vorgaben resultieren nicht zuletzt auch aus Normen. Eine Norm ist ein Standard, der von einer Normungsorganisation als Ergebnis eines systematischen, festgelegten Normungsverfahrens beschlossen und veröffentlicht wurde. Dieses Arbeitspapier richtet sich demgemäß auf aktuelle Normen, die für das IT-Management von Bedeutung sind. Als relevante Normungsorganisationen werden die International Organization for Standardization (ISO) und die International Electrotechnical Commission (IEC) sowie das Deutsche Institut für Normung (DIN) berücksichtigt. Die Spannbreite reicht von viel diskutierten ISO/IEC-Normen, beispielsweise der ISO/ IEC 270xx-Reihe oder der ISO/IEC 20000 über die IT-Governance-Norm ISO/IEC 38500 bis hin zu wenig bekannteren DIN-Normen, wie z. B. der DIN 66271 zum Umgang mit Softwarefehlern. Jede Beschreibung enthält eine prägnante Inhaltsangabe, den formellen Status der Norm und Links für die eigene Recherche. Auch dieses Arbeitspapier soll wieder eine Hilfestellung für den Praktiker sein, der sich schnell hinsichtlich relevanter IT-Normen orientieren will.

Gliederung

[1] Prof. Dr. Michael Klotz, FH Stralsund, Fachbereich Wirtschaft, Zur Schwedenschanze 15, 18435 Stralsund, michael.klotz@fh-stralsund.de

Schlüsselwörter: DIN – IEC – ISO – IT-Compliance – IT-Management – Normen – Standards

JEL-Klassifikation: L15, M10, M21, M42

Vorwort

Das Feld der managementrelevanten IT-Normen hat in den letzten Jahren eine beträchtliche Dynamik erfahren. Dies liegt zum einen selbstverständlich an der Anforderung der Praxis, sich auf verlässliche Vorgaben in wichtigen Handlungsbereichen, wie beispielsweise dem IT-Sicherheitsmanagement oder dem IT-Servicemanagement, stützen zu können. Zum anderen erlangen Normen dann an Verbindlichkeit, wenn in regulatorischen Vorgaben auf sie verwiesen wird, wie dies – derzeit allerdings noch als Ausnahme – in den „Mindestanforderungen an das Risikomanagement“ (MaRisk) der Fall ist, wo die Normenreihe ISO/IEC 270xx referenziert wird. Zum anderen sind Normen mittlerweile aber auch ein Instrument des internationalen Wettbewerbs. Staaten, die in der Normung führend sind, erlangen durch Erfahrungsvorsprünge einen Wettbewerbsvorteil für ihre Wirtschaftsteilnehmer. Nicht zuletzt stellen Normen damit auch einen Bereich dar, in dem durch Beratung, Schulung und Zertifizierung beträchtliche Umsätze erzielt werden.

Unternehmen sind somit gut beraten, sich mit Normen auseinanderzusetzen. Auch wenn das IT-Management einem geringeren Druck in der Anwendung von Normen als andere Unternehmensbereiche unterliegt, sollte bewusst entschieden werden, welchen Normen nachgekommen werden soll. Hierzu ist ein umfassender Überblick erforderlich. Diesen herzustellen ist Ziel dieses Arbeitspapiers.

Prof. Dr. Michael Klotz

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AS	Australian Standard
B2B	Business to Business
B2C	Business to Consumer
BS	British Standard
BSI	British Standard Institute
CEN	Comité Européen de Normalisation
CMMI	Capability Maturity Model Integration
COBIT	Control Objectives for Information and Related Technology
DIN	Deutsche Institut für Normung e. V.
DKE	Deutsche Kommission Elektrotechnik Elektronik Informations-technik im DIN und VDE
DR	Disaster Recovery
ECM	Enterprise Content Management
EN	Europäische Norm
EnEV	Energieeinsparverordnung
EU	Europäische Union
e. V.	eingetragener Verein
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IRBC	Information and communication technology readiness for business continuity
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnik / Informationstechnologie
ITIL	Information Technology Infrastructure Library
ITSM	IT-Service-Management
JTC	Joint Technical Comitee
MaRisk	Mindestanforderungen an das Risikomanagement
NIA	Normenausschuss Informationstechnik und Anwendungen
OECD	Organisation for Economic Co-operation and Development
SAM	Software Asset Management
SPICE	Software Process Improvement and Capability Determination
TR	Technical Report
TS	Technical Specification
VDE	VDE Verband der Elektrotechnik Elektronik Informations-technik e. V.
VOI	Verband Organisations- und Informationssysteme

1 IT-Compliance

IT-Compliance

Der Einsatz von Informationstechnologie (IT) in Unternehmen unterliegt vielfältigen unternehmensinternen und externen Anforderungen, denen in unterschiedlichem Ausmaß Folge zu leisten ist. Sowohl die IT-Funktion als auch die Nutzung der IT in den verschiedenen Fachabteilungen muss somit „compliant“ sein. Als Spezialisierung des allgemeinen Compliance-Begriffs (sog. „Corporate Compliance“) bezeichnet IT-Compliance einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden.[2] Hierbei ist es unerheblich, ob die IT-Leistungen ausschließlich unternehmensintern oder (ganz oder teilweise) durch externe IT-Dienstleister (im Rahmen von Entwicklungs-, Hosting-, Outsourcing-Verträgen o. Ä.) erbracht werden.

Regelwerke als Quelle von Compliance-Vorgaben

Eine grundlegende Aufgabe von IT-Compliance bzw. eines IT-Compliancemanagements ist die Festlegung, welche Vorgaben als relevant angesehen werden, d. h. welche Regelwerke mit IT-Bezug als Quelle von Vorgaben zu berücksichtigen sind. Es lassen sich grundsätzlich drei Gruppen von Regelwerken unterscheiden, die in ihrer Summe ein Grundgerüst für eine systematische Ableitung und Analyse von Compliance-Vorgaben darstellen, vgl. Abbildung 1:

- rechtliche Vorgaben aus Gesetzen anderer Staaten, Rechtsakten der Europäischen Union (EU), internationalen Abkommen, aus der Verfassung und aus Gesetzen sowie auf deren Grundlage von den Verwaltungen erlassenen Rechtsverordnungen oder Erlassen/Satzungen, Rechtsprechung sowie Verwaltungsvorschriften und weiteren Regelwerken, auf die in Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften verwiesen wird oder die von der Rechtsprechung zur Auslegung herangezogen werden; außerdem sind dieser Gruppe Verträge zuzurechnen, die ein Unternehmen mit Kunden, Lieferanten und sonstigen Marktpartnern abschließt und die IT-relevante Vereinbarungen enthalten;
- unternehmensexterne, auf die Unternehmens-IT bezogene Regelwerke, wie Deklarationen, Verhaltenskodizes, Normen und Standards vielfältiger Institutionen;

[2] Für vertiefende Ausführungen zu IT-Compliance siehe *Klotz 2012*, S. 12ff. und *Klotz 2013*.

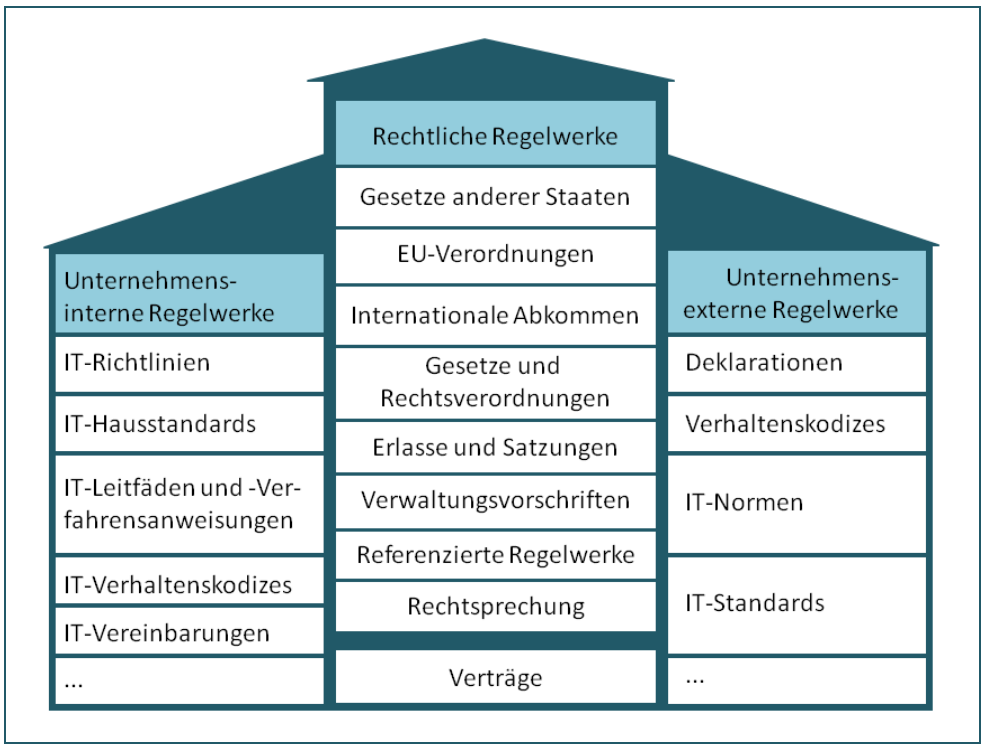


Abbildung 1
Das „House of IT-Compliance“[3]

- unternehmensinterne Regelwerke, wie z. B. IT-Richtlinien und -Hausstandards, IT-Leitfäden- oder -Verfahrensanweisungen, IT-Vereinbarungen und innerbetriebliche Verhaltenskodizes.

Unternehmens-externe Regelwerke

In die Gruppe der unternehmensexternen Regelwerke fallen viele derjenigen Regelwerke, die derzeit im IT-Management große Aufmerksamkeit erfahren, vor allem die als „Framework“, „Referenzmodell“ oder „Best-Practise-Modell“ gehandelten Standards, wie „Capability Maturity Model Integration“ (CMMI), „Information Technology Infrastructure Library“ (ITIL) und „Control Objectives for Information and Related Technology“ (COBIT). Insgesamt sind die in dieser Gruppe vertretenen Regelwerke höchst unterschiedlich. Die Spannbreite reicht von Deklarationen supranationaler Organisationen, wie der „Organisation for Economic Co-operation and Development“ (OECD), über nationale und internationale Normen, Standards internationaler und nationaler Verbandsorganisationen und behördlicher Einrichtungen bis hin zu Empfehlungen oder Konzepten, die sich über die Zeit durch Informations- und Erfahrungsaustausch in der Fachwelt herausgebildet haben.

[3] Entnommen aus *Klotz 2012*, S. 17.

2 Normen als compliance-relevante Regelwerke

Rolle von Normen

Normen, gleich in welchem Bereich sie zur Anwendung gelangen, werden nicht von einer isolierten Interessengruppe entwickelt, sondern entstehen vor dem Hintergrund einer breit geteilten Interessenlage, für die sie Antworten auf wichtige praktische Aufgabenstellungen bieten. Diese richten sich zumeist auf die Sicherstellung der Effektivität und der Effizienz des in Frage stehenden Anwendungsbereiches.

2.1 Standards und Normen

Die Begriffe „Normen“ und „Standards“ werden oftmals in einem Zuge genannt. Somit stellt sich die Frage, was unter „Norm“[4] zu verstehen ist und welcher Zusammenhang zwischen den beiden Begriffen „Standard“ und „Norm“ besteht. Da Normen eine Spezialisierung von Standards darstellen, hat die Begriffsklärung beim Begriff des Standards anzusetzen.[5]

Standards

Ein Standard ist zuerst einmal ein Regelwerk, das beschreibt, wie etwas zu tun, zu lösen oder handzuhaben ist. Nun stellt nicht jede Zusammenfassung von Richtlinien, Best Practices, Kontrollgrößen, Empfehlungen u. Ä. sofort einen Standard dar. Zur bloßen Existenz eines schriftlichen Regelwerkes muss hinzukommen, dass die als Standard beschriebenen Regeln breit akzeptiert und angewendet werden. Der Akzeptanzbereich kann dabei geographisch (z. B. auf einen Staat oder eine Staatengemeinschaft) oder auf eine nationale, internationale oder globale Anwendergruppe (z. B. Ingenieure, Projektmanager) beschränkt sein. Die Anwendergruppe muss zudem den Standard nicht nur kennen und akzeptieren, sondern auch wirklich praktisch nutzen. Aus dieser Nutzung muss sich zudem eine Rückkopplung für die Weiterentwicklung des Standards ergeben.

Normen

Normen beschreiben – ähnlich wie ein Standard – „wissenschaftlich begründete Arbeitsmethoden zur Bewältigung rationeller, meist wiederholbarer Arbeitsprozesse … bzw. Qualitäts- und Sicherheitsanforderungen“.[6] Im Unterschied zum Standard ist eine Norm nun ein Standard, der von einer offiziellen Normungsorganisation als Ergebnis eines systematischen, festgelegten Normungsverfahrens beschlossen und veröffentlicht wurde. Eine Norm

[4] Der Begriff „Norm“ ist bereits zu unterscheiden vom Begriff der Rechtsnorm, der die oben genannten rechtlichen Regelwerke bis hin zu den Verwaltungsvorschriften umfasst.
[5] Im Folgenden nach *Klotz 2013*, S. 739.
[6] *VOI 2008*, S. 18.

ist ein „Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird“.[7]

Verbindlichkeit von Normen

Aufgrund des formalisierten Erstellungsprozesses beinhalten in der Regel nicht den innovativsten Stand eines Anwendungsgebietes, sondern schreiben vielmehr die durch praktische Bewährung allgemein anerkannten Regeln eines (technischen) Anwendungsbereiches fest. Insofern werden Normen häufig – ggf. von externen Gutachtern – herangezogen um festzustellen, ob Sorgfaltspflichten eingehalten wurden. Die Einhaltung von Normen wird zudem mitunter in nationalen und internationalen Vorschriften, d. h. vor allem in Gesetzen und Verordnungen, verbindlich vorgeschrieben.[8] In diesen Fällen erlangt eine Norm eine unmittelbare rechtliche Bindungswirkung.[9]

Normungsorganisation

Normen stellen somit eine Teilmenge von Standards dar; sie werden mitunter auch als „de-jure-Standard“ bezeichnet. Eine Norm gewinnt dadurch einen offiziellen Charakter, dass die jeweilige Normungsorganisation dazu in der Lage ist, die Norm in ihrem Geltungsbereich (fachlich) durchzusetzen. Eine Normungsorganisation ist eine Institution, „die auf nationaler, regionaler oder internationaler Ebene anerkannt ist und als wesentliche Funktion, dank ihrer Statuten, die Erstellung, Anerkennung oder Annahme von Normen hat, welche der Öffentlichkeit zugänglich sind“.[10] Für die IT maßgebliche Normungsorganisationen, vgl. Tabelle 1, sind

- auf internationaler Ebene die „International Standardization Organization“ (ISO) und die „International Electrotechnical Commission“ (IEC), die beide gemeinsam für den Großteil der hier behandelten Normen verantwortlich zeichnen;
- auf europäischer Ebene das Europäische Komitee für Normung (Comité Européen de Normalisation – CEN);

---

[7] *DIN EN 45020*, S. 23.
[8] Für die IT lässt sich dafür allerdings derzeit kein Beispiel finden. Ein Beispiel aus der Energiewirtschaft bildet die Energieeinsparverordnung (EnEV), die an zahlreichen Stellen auf verschiedene DIN-Normen Bezug nimmt.
[9] Nach *VOI 2008*, S. 18.
[10] *DIN EN 45020*, S. 31.

Tabelle 1
Normungs-organisationen[11]

	ISO	IEC	CEN	DIN
Gründungsjahr	1947	1906	1961	1917
Sitz	Genf, Schweiz	Genf, Schweiz	Brüssel, Belgien	Berlin, Deutschland
Amtssprache	Englisch, Französisch	Englisch, Französisch, Russisch	Englisch, Französisch, Deutsch	Deutsch
Mitglieder	163 Länder	60 National Committees	33 National Members	1.934 juristische Personen
Dt. Vertretung	DIN e.V.	DKE	DIN e.V.	-
Homepage	www.iso.org	www.iec.ch	www.cen.eu	www.din.de

- in Deutschland das „DIN Deutsches Institut für Normung e. V." (DIN) mit Sitz in Berlin.

DIN

Mitglieder des DIN Deutsches Institut für Normung e. V. sind Unternehmen, Verbände, Behörden und andere Organisationen, gerade auch aus der Wissenschaft. Das DIN ist privatwirtschaftlich als Verein organisiert. Die offizielle Anerkennung als nationale Normungsorganisation ergibt sich Falle des DIN aus einem Vertrag zwischen der Bundesrepublik Deutschland und dem DIN, in dem diesem die Zuständigkeit für die nationalen, europäischen und internationalen Normungsaktivitäten übertragen wird. Damit ist das DIN dafür verantwortlich, den gesamten Prozess der Normung auf nationaler Ebene sowie die deutsche Beteiligung auf europäischer und internationaler Ebene zu organisieren.[12]

DIN – NIA

Innerhalb des DIN agiert der „Normenausschuss Informationstechnik und Anwendungen" (NIA) als nationales Gremium für die Normung in der Informationstechnik und in ausgewählten Anwendungsbereichen der Informationstechnik. Der NIA selbst ist wiederum in derzeit 19 Arbeitsausschüsse gegliedert. In der internationalen Normungsarbeit stellt der NIA das deutsche Spiegelgremium zur ISO/IEC JTC 1 dar. Auch in den entsprechenden Gremien des CEN ist der NIA vertreten.[13]

[11] Zahlenangaben gemäß Angaben auf der jeweiligen Webseite mit Stand 12.08.2013, Angabe des DIN mit Stand Dezember 2012.
[12] Nach *DIN 2013*.
[13] Nach *DIN-NIA 2013*.

ISO/IEC-Normen

ISO und IEC sind ebenfalls private Organisationen, deren Mitglieder sich aus den nationalen Normungsorganisationen zusammensetzen. Für die Normungsarbeit im Bereich der Informationstechnik haben ISO und IEC 1987 ein gemeinsames Gremium, das „ISO/IEC Joint Technical Committee 1“ (JTC1), eingerichtet. Dieser Einrichtung gehören derzeit 35 Länder an (unter ihnen Deutschland), weitere 57 befinden sich im Beobachtungsstatus „observing countries“.[14] Normen, die aus der Arbeit dieses Komitees resultieren, erhalten eine ISO/IEC-Kennung und stellen die Mehrheit der hier betrachteten Normen dar.

DIN – ISO – EN

ISO-Normen werden von den zuständigen Normenausschüssen des DIN kontinuierlich daraufhin geprüft, ob sie als „DIN ISO“-Norm übernommen werden sollen. Europäische EN-Normen werden vom DIN grundsätzlich als „DIN EN“-Norm übernommen. Normen, die sowohl vom DIN und der ISO als auch vom CEN verabschiedet wurden, werden als „DIN EN ISO“-Norm gekennzeichnet.

Weitere Normungsorganisationen

In jüngster Zeit treten zudem weitere nationale Normungsorganisationen auf den Plan, die für das IT-Management relevante Themen in ihrer Normungsarbeit adressieren. Ein für das IT-Management wichtiges Beispiel hierfür ist die australische Norm AS 8015: 2005, die im Jahr 2008 von der ISO/IEC als ISO/IEC 38500:2008 übernommen wurde und ein Referenzmodell für die IT-Governance beinhaltet. Auch aus Großbritannien stammen zahlreiche Normen (British Standards), die vom British Standard Institute (BSI) herausgegeben werden. Diese in der Praxis vielbeachteten Normen waren in der Vergangenheit häufig Basis für ISO-Normen und sind in diese ein- bzw. in diesen aufgegangen.

2.2 Auswahl der Normen

Managementorientierung

Normen im Bereich der Informations- und Kommunikationstechnologie gibt es viele. Entsprechend der gewählten Fokussierung werden im Folgenden prinzipiell nur solche Normen betrachtet, die das Management des IT-Einsatzes im Unternehmen relevant sind. Der Aspekt des leitungsbezogenen IT-Handelns, mithin die Managementorientierung, stellt somit das wesentliche Auswahlkriterium für die zu betrachtenden Normen dar. Damit scheiden rein informationstechnische Normen aus der Betrachtung aus (beispielsweise die zahlreichen ISO-Normen zu Programmiersprachen und technischer

[14] Vgl. *ISO 2013*.

Sicherheit oder DIN-Normen zu Datenkommunikation, graphischer Datenverarbeitung oder Codierung).

Herkunft

Bezüglich der Herkunft der Normen erfolgt eine Beschränkung auf die in Tabelle 1 aufgeführten Normungsorganisationen, also deutsche Normen des DIN sowie Normen der internationalen Normungseinrichtungen ISO und IEC.

IT-Spezialisierung

Hinsichtlich der inhaltlichen Ausrichtung scheiden Normen aus, die zwar mitunter Beachtung für das IT-Management finden, aber nicht spezifisch auf IT-Belange ausgerichtet sind. So können beispielsweise der ISO 22301[15] als Norm für das unternehmensweite Kontinuitätsmanagement durchaus auch wichtige Hinweise für das IT-Continuity Management entnommen werden. Da die Norm jedoch nicht speziell die IT fokussiert, wird sie hier nicht weiter betrachtet – im Gegensatz zur Norm ISO/IEC 27031, die IT-Continuity Management adressiert. Weitere Beispiele sind die weit verbreitete DIN EN ISO 9000[16], die ein allgemeines Rahmenwerk für das Qualitätsmanagement darstellt, und die ISO 31000[17], die grundlegende Konzepte und Richtlinien für ein allgemeines Risikomanagement beinhaltet. Gleichwohl erfährt die Norm ISO/ IEC 90003 Berücksichtigung, da sie spezialisierte Richtlinien für die Anwendung der ISO 9001 auf Computersoftware beinhaltet.

Aktualität

Als weiteres Auswahlkriterium wurde die Aktualität herangezogen, d. h. ältere Normen werden nicht weiter berücksichtigt, wenn diese nicht mehr gültig sind oder wenn sie in neueren Normen auf- oder in diese eingegangen sind, so wie im Falle der ISO 9000-3:1997, die in die ISO/IEC 90003:2004 überführt wurde. Auch die populäre Norm „BS 15000“ zum IT-Service-Management findet keine Berücksichtigung, da diese Norm des British Standard

---

[15] ISO 22301:2012-05 (E) Societal security - Business continuity management systems – Requirements, (dt.: Sicherheit und Schutz des Gemeinwesens – Managementsysteme für die Planung, Vorbereitung und operationelle Kontinuität – Anforderungen), vgl. http://www.fnfw.din.de/cmd?artid=154020739&contextid=fnfw&bcrumblevel=1&subcommitteeid=92707317&level=tpl-art-detailansicht&committeeid=54738903&languageid=de (Letzter Zugriff hier wir für alle in diesem Arbeitspapier angegebenen Links: 12.08.2013)

[16] DIN EN ISO 9000 Qualitätsmanagementsysteme - Grundlagen und Begriffe, vgl. http://www.nqsz.din.de/cmd?artid=82009580&contextid=nqsz&bcrumblevel=1&subcommitteeid=54748179&level=tpl-art-detailansicht&committeeid=54739099&languageid=de

[17] ISO 31000 Risikomanagement - Allgemeine Anleitung zu den Grundsätzen und zur Implementierung eines Risikomanagements, vgl. http://www.nasg.din.de/cmd?level=tpl-art-detailansicht&committeeid=54739031&artid=124279874&languageid=de&bcrumblevel=3&subcommitteeid=83621529

Institute (BSI) mittlerweile in die ISO/IEC 20000 eingegangen ist und als britische Norm zurückgezogen wurde.[18]

Die in diesem Arbeitspapier enthaltenen Daten zu den Normen wurden von den jeweiligen Webseiten der Normungsinstitute übernommen. Abbildung 2 zeigt als Beispiel die Angaben des DIN zur DIN ISO/IEC 15504-1 (Information technology - Process assessment - Part 1: Concepts and vocabulary (ISO/IEC 15504-1:2004). Neben formalen Angaben, z. B. zur Ausgabe und zur Sprache, finden sich eine kurze Inhaltsangabe, die Möglichkeit zum Download eines Inhaltsverzeichnisses (bei einer DIN ISO/IEC in Deutsch und Englisch, bei einer ISO/IEC nur in Englisch) und Kontaktdaten zu einem Ansprechpartner für diese Norm. Die Angabe der aktuellen Version ist unter der Bezeichnung der Norm zu finden. Weiterhin enthalten sind Angaben bzw. ein Link zu dem jeweils zuständigen nationalen Arbeitsgremium sowie die Möglichkeit zum Erwerb der Norm.

Abbildung 2
Webseite des DIN für die DIN ISO/IEC 15504-1[19]

[18] Vgl. http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030007551

[19] Quelle: http://www.nia.din.de/cmd?artid=141513167&bcrumblevel=2&level=tpl-art-detailansicht&committeeid=54738935&languageid=de

Abbildung 3 zeigt die entsprechende Webseite der ISO für die ISO/IEC 15504-1 (Information technology -- Process assessment -- Part 1: Concepts and vocabulary).

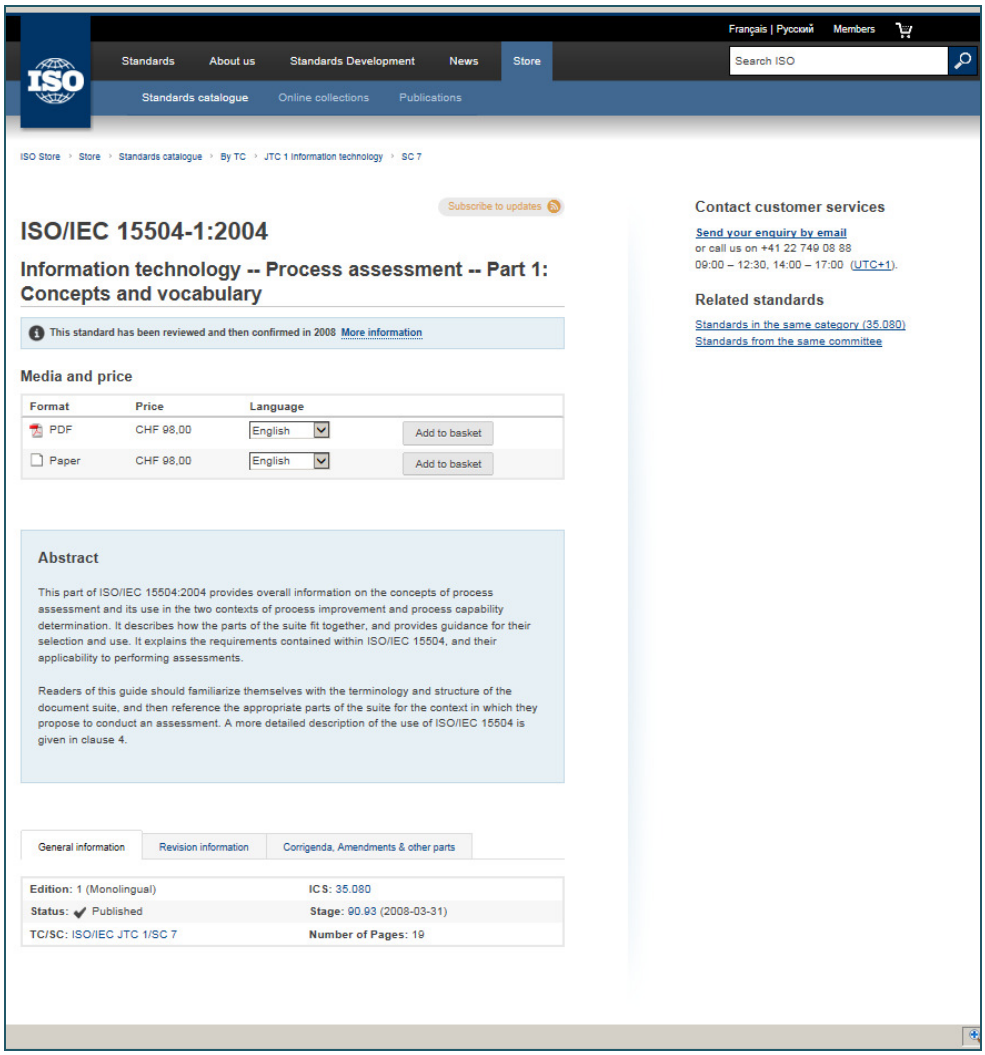
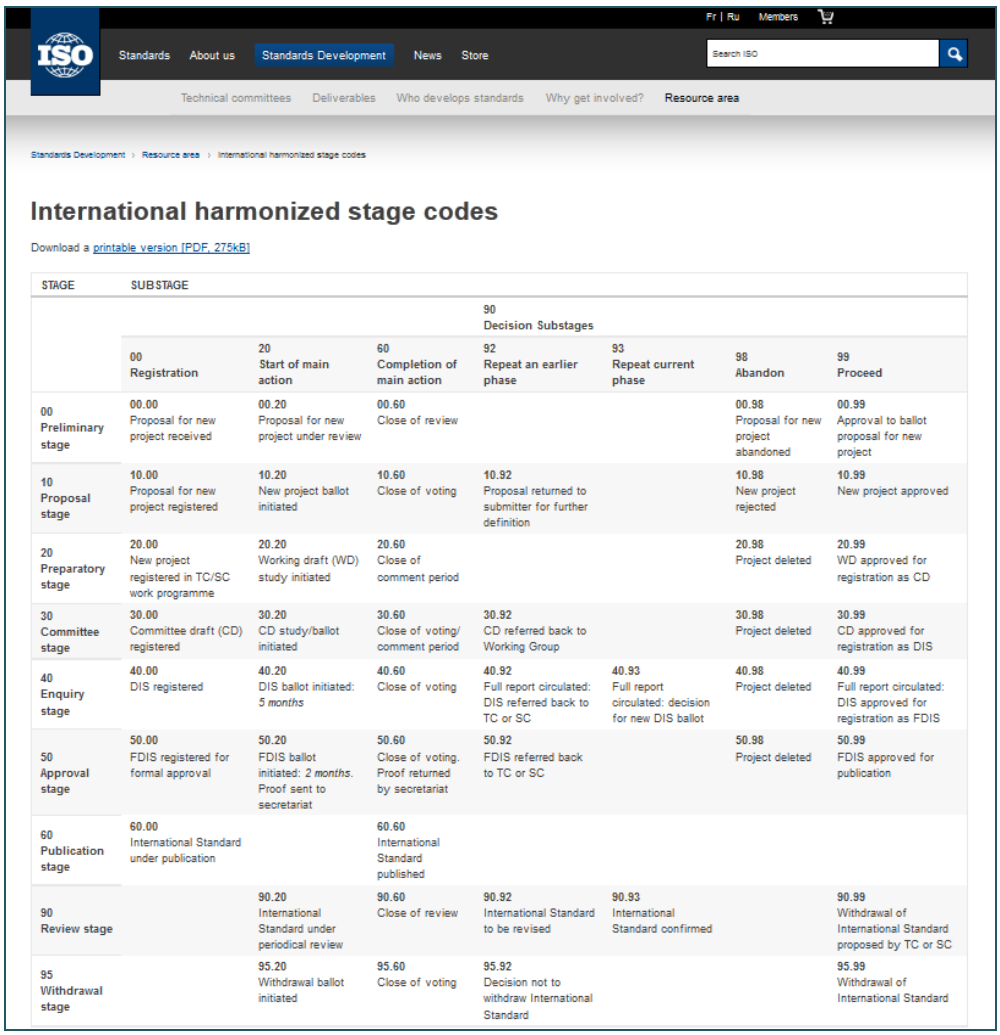


Abbildung 3
Webseite der ISO für die ISO/IEC 15504-1[20]

Die Zusammenfassung fällt hier und auch sonst für gewöhnlich etwas länger aus als auf der DIN-Webseite. Außerdem können zusätzliche Informationen zu Ergänzungen („Corrigenda, Amendments & other parts“) und Revisionsständen („Revision information“) angezeigt werden. Bei der ISO wird zudem das Jahr der Erstellung oder Überarbeitung der Norm als Teil der Normbezeichnung (hier: „ISO/IEC 15504-1:2004“) angegeben.

[20] Quelle:
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=38932

Zusätzlich werden verschiedene Codes vergeben, um die unterschiedlichen Stati der Normen genauer zu kennzeichnen. Abbildung 4 zeigt diese so genannten „stage codes“.



Fr | Ru Members

Standards About us Standards Development News Store

Search ISO

Technical committees Deliverables Who develops standards Why get involved? Resource area

Standards Development › Resource area › International harmonized stage codes

International harmonized stage codes

Download a printable version [PDF, 275kB]

STAGE	SUBSTAGE						
				90 Decision Substages			
	00 Registration	20 Start of main action	60 Completion of main action	92 Repeat an earlier phase	93 Repeat current phase	98 Abandon	99 Proceed
00 Preliminary stage	00.00 Proposal for new project received	00.20 Proposal for new project under review	00.60 Close of review			00.98 Proposal for new project abandoned	00.99 Approval to ballot proposal for new project
10 Proposal stage	10.00 Proposal for new project registered	10.20 New project ballot initiated	10.60 Close of voting	10.92 Proposal returned to submitter for further definition		10.98 New project rejected	10.99 New project approved
20 Preparatory stage	20.00 New project registered in TC/SC work programme	20.20 Working draft (WD) study initiated	20.60 Close of comment period			20.98 Project deleted	20.99 WD approved for registration as CD
30 Committee stage	30.00 Committee draft (CD) registered	30.20 CD study/ballot initiated	30.60 Close of voting/ comment period	30.92 CD referred back to Working Group		30.98 Project deleted	30.99 CD approved for registration as DIS
40 Enquiry stage	40.00 DIS registered	40.20 DIS ballot initiated: *5 months*	40.60 Close of voting	40.92 Full report circulated: DIS referred back to TC or SC	40.93 Full report circulated: decision for new DIS ballot	40.98 Project deleted	40.99 Full report circulated: DIS approved for registration as FDIS
50 Approval stage	50.00 FDIS registered for formal approval	50.20 FDIS ballot initiated: *2 months*. Proof sent to secretariat	50.60 Close of voting. Proof returned by secretariat	50.92 FDIS referred back to TC or SC		50.98 Project deleted	50.99 FDIS approved for publication
60 Publication stage	60.00 International Standard under publication		60.60 International Standard published				
90 Review stage		90.20 International Standard under periodical review	90.60 Close of review	90.92 International Standard to be revised	90.93 International Standard confirmed		90.99 Withdrawal of International Standard proposed by TC or SC
95 Withdrawal stage		95.20 Withdrawal ballot initiated	95.60 Close of voting	95.92 Decision not to withdraw International Standard			95.99 Withdrawal of International Standard

Abbildung 4
Angaben der ISO zu den International harmonized stage codes[21]

In diesem Arbeitspapier werden nur ISO-Normen berücksichtigt, deren stage code von 60.60 (International Standard published) bis 90.93 (International Standard confirmed) reicht.

[21] Quelle: http://www.iso.org/iso/home/standards_development/resources-for-technical-work/stages_table.htm#s90

3 Normen für das IT-Management

Im Folgenden werden die verschiedenen Normen im Einzelnen dargestellt. Hierzu werden zuerst einige grundlegende Basisdaten (zum Titel, zur aktuellen Version sowie ggf. zum aktuellen Status) genannt. Daran schließt sich eine kurze Inhaltsangabe an, bei der aber nicht alle Inhalte/Elemente einer Norm Erwähnung finden.

Die Auflistung der Normen wird in vier Gruppen gegliedert, DIN-Normen, DIN ISO-Normen, DIN ISO/IEC-Normen und ISO/IEC-Normen. Die berücksichtigten Normen sind in Tabelle 2 aufgeführt. In der Summe werden 38 Normen aufgelistet.

3.1 DIN-Normen

DIN-Normen

In der Gruppe der DIN-Normen sind diejenigen Normen enthalten, die vom DIN ohne Übernahme von einer anderen Normungsorganisation (ISO, IEC, CEN) selbst entwickelt wurden.

DIN 66271

Titel	**DIN 66271** **Softwarefehler und ihre Beurteilung durch Lieferanten und Kunden**
Aktuelle Version	Ausgabe 1995-06
Status	-
Inhalt	Die Norm definiert einen Softwarefehler als Nichterfüllung einer zwischen Kunden und Lieferanten festgelegten Forderung. Diese Abweichung von einem erwarteten Merkmalsergebnis führt i. d. R. zu Differenzen zwischen den Vertragsparteien. Zur Behebung dieser Differenzen ist eine transparente Fehlerklassifizierung notwendig. Diese wird in der DIN 66271 mit den drei Stufen „hoch“, „mittel“ und „niedrig“ dargestellt. Die zugrundeliegenden Kriterien sind die Beeinträchtigung des Einsatzes der Software und das Schadensrisiko, das aus dem Softwarefehler resultiert. Die daran anknüpfende Behebung des Fehlers, der Aufwand und die Priorität schließen sich im Umfang an die Fehlerklassifizierung an.
Link	Zur DIN-Website: http://www.nia.din.de/cmd?artid=2533281&bcrumblevel=1&contextid=nia&subcommitteeid=54770175&level=tpl-art-detailansicht&committeeid=54738935&languageid=de

Tabelle 2
Zuordnung der Normen

Gruppe		Anzahl
DIN-Normen	• DIN 66271 • DIN 66399-1 • DIN 66399-2	3
DIN ISO-Normen	• DIN ISO 15489-1	1
DIN ISO/IEC-Normen	• DIN ISO/IEC 15504-1 • DIN ISO/IEC 15504-2 • DIN ISO/IEC 15504-3 • DIN ISO/IEC 15504-4 • DIN ISO/IEC 15504-5 • DIN ISO/IEC 19770-1 • DIN ISO/IEC 27000 • DIN ISO/IEC 27001 • DIN ISO/IEC 27002	9
ISO/IEC-Normen	• ISO/IEC 2382-1 • ISO/IEC 12207 • ISO/IEC 15288 • ISO/IEC 15504-6 • ISO/IEC 18043 • ISO/IEC 20000-1 • ISO/IEC 20000-2 • ISO/IEC 20000-3 • ISO/IEC 24762 • ISO/IEC 27003 • ISO/IEC 27004 • ISO/IEC 27005 • ISO/IEC 27007 • ISO/IEC 27010 • ISO/IEC 27013 • ISO/IEC 27014 • ISO/IEC 27031 • ISO/IEC 27032 • ISO/IEC 27033-1 • ISO/IEC 27033-2 • ISO/IEC 27033-3 • ISO/IEC 27034-1 • ISO/IEC 27035 • ISO/IEC 38500 • ISO/IEC 90003	25
Insgesamt		38

Die Normenreihe DIN 66399 zur Vernichtung von Datenträgern richtet sich darauf, Informationsträger mit schutzbedürftigen Informationen so zu vernichten, dass die Reproduktion der auf ihnen wiedergegebenen Informationen entweder unmöglich ist oder weitgehend erschwert wird.[22] Die Norm besteht aus zwei Teilen:

DIN 66399-1

Titel	**DIN 66399-1** **Büro- und Datentechnik - Vernichten von Datenträgern – Teil 1: Grundlagen und Begriffe**
Aktuelle Version	Ausgabe 2012-10
Status	-
Inhalt	Die DIN 66399-1 beinhaltet die Grundlagen und Begriffe im Bereich der Datenträgervernichtung.
Link	Zur DIN-Website (mit Link auf das Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54771182&artid=155420083&bcrumblevel=2&languageid=de

DIN 66399-2

Titel	**DIN 66399-2** **Büro- und Datentechnik - Vernichten von Datenträgern – Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern**
Aktuelle Version	Ausgabe 2012-10
Status	-
Inhalt	Die DIN 66399-2 beinhaltet die Anforderungen an Maschinen zur sicheren Vernichtung von Datenträgern. Aus Sicht des IT-Managements sind hier die Vorgaben zu Kontrollen und Prüfungen der Vernichtung interessant.
Link	Zur DIN-Website (mit Link auf das Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54771182&artid=155420668&bcrumblevel=2&languageid=de

[22] Nach http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54771182&artid=155420083&bcrumblevel=2&languageid=de

3.2 DIN ISO-Normen

DIN ISO-Normen

In der Gruppe der DIN ISO-Normen sind diejenigen Normen der ISO enthalten, die vom DIN übernommen werden, also eine „DIN ISO“-Bezeichnung haben.

DIN ISO 15489-1

Titel	**DIN ISO 15489-1** **Information und Dokumentation – Schriftgutverwaltung – Teil 1: Allgemeines** **Information and documentation – Records management – Part 1: General**
Aktuelle Version	a) ISO/IEC 15489-1:2001 b) DIN-Ausgabe 2002-12
Status	ISO: Review Stage 90.92 (International Standard to be revised) 2012-07-13
Inhalt	Die DIN ISO 15489-1 beschreibt grundlegende Anforderungen an die rechtssichere Dokumenten- und Aktenverwaltung. Als Einführung in eine Normenreihe (zu der aber im Moment lediglich weitere technische Reports vorliegen) bietet die Norm einen guten Überblick über die Thematik der Schriftgutverwaltung bzw. des Records Management.[23]
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=31908 b) DIN-Website (mit Link zum deutschen Inhaltsverzeichnis): http://www.nabd.din.de/cmd?artid=53953792&contextid=nabd&bcrumblevel=1&subcommitteeid=112656096&level=tpl-art-detailansicht&committeeid=54738855&languageid=de

3.3 DIN ISO/IEC-Normen

DIN ISO/IEC-Normen

In der Gruppe der DIN ISO/IEC-Normen sind diejenigen Normen der ISO/IEC enthalten, die vom DIN übernommen werden, also eine „DIN ISO /IEC“-Bezeichnung haben.

Normenreihe DIN ISO/IEC 15504

Die im Folgenden aufgelistete Normenreihe „DIN ISO/IEC 15504-x“ beschreibt ein Modell zur Bewertung von Prozessen, das in der Fachdiskussion unter dem Namen „SPICE“ (Software Process Improvement and Capa-

[23] Nach *VOI 2008*, . 38f.

bility Determination) bekannt ist. Dieses Modell unterstützt mit den Zielen der Kostenreduktion und besserer Produktqualität das Management der Softwareentwicklung durch einen strukturierten Ansatz zur Verbesserung der Entwicklungsprozesse.[24]

DIN ISO/IEC 15504-1

Titel	**DIN ISO/IEC 15504-1** **Informationstechnik – Prozess-Assessment – Teil 1: Konzepte und Vokabular** **Information technology – Process assessment – Part 1: Concepts and vocabulary**
Aktuelle Version	c) ISO/IEC 15504-1:2004 d) DIN-Ausgabe 2011-04
Status	ISO: Review Stage 90.93 (International Standard confirmed) 2008-03-31
Inhalt	Die DIN ISO/IEC 15504-1 beinhaltet die grundlegenden Konzepte und Begriffe der Normenreihe.
Link	c) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=38932 d) DIN-Website (mit Link zum deutschen und englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=141513167&bcrumblevel=2&languageid=de

DIN ISO/IEC 15504-2

Titel	**DIN ISO/IEC 15504-2** **Informationstechnik – Prozess-Assessment – Teil 2: Durchführung eines Assessments** **Information technology – Process assessment – Part 2: Performing an assessment**
Aktuelle Version	a) ISO/IEC 15504-2:2003 b) ISO/IEC 15504-2:2003/Cor 1:2004 c) DIN-Ausgabe 2011-07
Status	a) Review Stage 90.93 (International Standard confirmed) 2008-03-31 b) Publication Stage 60.60 (International Standard published) 2004-02-11

[24] Wobei die Norm so allgemein gehalten ist, dass sie auf Prozesse auch anderer betrieblicher Funktionsbereiche angewendet werden kann und wird.

Inhalt	Die DIN ISO/IEC 15504-2 legt die einzuhaltenden Mindestanforderungen fest, um eine Prozessbewertung vergleich- und wiederholbar durchzuführen.
Link	a) ISO-Website : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=40192 b) DIN-Website (mit Link zum deutschen und englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=141757216&bcrumblevel=2&languageid=de

DIN ISO/IEC 15504-3

Titel	**DIN ISO/IEC 15504-3** **Informationstechnik – Prozess-Assessment – Teil 3: Richtlinien für die Durchführung von Assessments** **Information technology – Process assessment – Part 3: Guidance on performing an assessment**
Aktuelle Version	a) ISO/IEC 15504-3:2004 b) DIN-Ausgabe 2011-07
Status	a) Review Stage 90.20 (International Standard under periodical review) 2013-04-15
Inhalt	Die DIN ISO/IEC 15504-3 unterstützt den Anwender durch praktische Leitlinien zur Durchführung des Prozess-Assessments.
Link	a) ISO-Website : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=37454 b) DIN-Website (mit Link zum deutschen und englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=142202356&bcrumblevel=2&languageid=de

DIN ISO/IEC 15504-4

Titel	**DIN ISO/IEC 15504-4** **Informationstechnik – Prozess-Assessment – Teil 4: Anwendungsrichtlinien zur Prozessverbesserung und zur Bestimmung der Prozessfähigkeiten** **Information technology – Process assessment – Part 4: Guidance on use for process improvement and process capability determination**

Aktuelle Version	a) ISO/IEC 15504-4:2004 b) DIN-Ausgabe 2011-08
Status	a) Review Stage 90.93 (International Standard confirmed) 2009-12-31
Inhalt	Die informative DIN ISO/IEC 15504-4 beinhaltet Richtlinien dazu, wie ein konformes Prozess-Assessment innerhalb eines Prozessverbesserungsprogramms oder einer Bestimmung der Prozessfähigkeiten zu nutzen ist.[25]
Link	a) ISO-Website : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=37462 b) DIN-Website (mit Link zum deutschen und englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=142537720&bcrumblevel=2&languageid=de

DIN ISO/IEC 15504-5

Titel	**DIN ISO/IEC 15504-5** **Informationstechnik – Prozess-Assessment – Teil 5: Beispiel für ein Prozess-Assessmentmodell** **Information technology – Process assessment – Part 5: An exemplar software life cycle process assessment model**
Aktuelle Version	a) ISO/IEC 15504-5:2012 b) DIN-Ausgabe 2011-07
Status	a) Publication stage 60.60 (International Standard published) 2012-01-26
Inhalt	Die DIN ISO/IEC 15504-5, die noch auf der alten ISO/IEC 15504-5:2006 beruht, beschreibt ein exemplarisches Prozess-Assessmentmodell, das die Anforderungen aus DIN ISO/IEC 15504-2 erfüllt. Das Beispiel umfasst ein komplettes Assessmentmodell, das die Anwendung der DIN ISO/IEC 15504-2 konkretisiert und verdeutlicht.[26]
Link	a) ISO-Website : http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail

[25] Vgl. http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=142537720&bcrumblevel=2&languageid=de

[26] Nach http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=141787224&bcrumblevel=2&languageid=de

	_ics.htm?csnumber=60555 b) DIN-Website (mit Link zum deutschen und englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=141787224&bcrumblevel=2&languageid=de

Die folgende DIN ISO/IEC 19770-1 richtet sich auf das Software Asset Management. Es liegt zudem noch eine ISO/IEC 19770-2 bzw. eine BS ISO/IEC 19770-2, die sich mit Software-Identifikationskennzeichen („Tagging“) befassen. Wegen ihrer eher technischen Ausrichtung werden diese Normen jedoch nicht weiter berücksichtigt.

DIN ISO/IEC 19770-1

Titel	**DIN ISO/IEC 19770-1** **Informationstechnik – Management von Software-Assets – Teil 1: Prozesse** **Information technology – Software asset management – Part 1: Processes**
Aktuelle Version	a) ISO/IEC 19770-1:2012 b) DIN-Ausgabe 2009-08
Status	a) Publication stage 60.60 (International Standard published) 2012-06-13
Inhalt	Die DIN ISO/IEC 19770-1, die noch auf der alten ISO/IEC 19770-1:2006 beruht, richtet sich auf das Software Asset Management (SAM), d. h. die Verwaltung der genutzten Software-Ressourcen und der entsprechenden Lizenzen. Die Norm behandelt die grundlegenden Begriffe und die einzelnen SAM-Prozesse.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56000 b) DIN-Website (mit Link zum deutschen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=117319979&bcrumblevel=2&languageid=de

Normenreihe DIN ISO/IEC 2700x

Die ISO/IEC 270xx-Normenreihe beinhaltet wichtige Richtlinien und Empfehlungen für das Management der IT-Sicherheit, insbesondere für die Etablierung eines Informationssicherheits-Managementsystems (ISMS). Die Reihe weist eine hohe Entwicklungsgeschwindigkeit auf. So wurden die

ersten drei Normen bereits vom DIN übernommen, während die folgenden Normen (ab ISO/IEC 27003) lediglich als ISO/IEC-Normen vorliegen.

DIN ISO/IEC 27000

Titel	**DIN ISO/IEC 27000** **Informationstechnik – IT-Sicherheitsverfahren – Informations-sicherheits-Managementsysteme – Überblick und Terminologie** **Information technology – Security techniques – Information security management systems – Overview and vocabulary**
Aktuelle Version	a) ISO/IEC 27000:2012 b) DIN-Ausgabe 2011-07
Status	a) Review Stage 90.92 (International Standard to be revised) 2013-01-14
Inhalt	Die DIN ISO/IEC 27000, die auf der alten ISO/IEC 27000:2009 beruht, gibt einen Überblick über Informationssicherheits-Managementsysteme (ISMS) und ist der konzeptionelle Rahmen für die weiteren Normen der Reihe. Sie beinhaltet eine Einführung zu den Erfolgsfaktoren der Informationssicherheit, Hinweise zu Prozessverbesserungen und Best Practice-Empfehlungen. Der Schwerpunkt liegt jedoch entsprechend der Benennung der Norm auf der Definition von Fachbegriffen, die in den weiteren Normen der ISO 270xx-Reihe zur Anwendung gelangen.
Link	a) ISO International Organization for Standardization: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=56891 b) DIN-Website (mit Link zum deutschen und englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770248&artid=140845763&bcrumblevel=2&languageid=de

DIN ISO/IEC 27001

Titel	**DIN ISO/IEC 27001** **Informationstechnik – IT-Sicherheitsverfahren – Informations-sicherheits-Managementsysteme – Anforderungen** **Information Technology – Security techniques – Information security management systems – Requirements**
Aktuelle Version	a) ISO/IEC 27001:2005 b) DIN-Ausgabe 2008-09
Status	a) Review Stage 90.92 (International Standard to be revised) 2008-10-15
Inhalt	Die DIN ISO/IEC 27001, die auf der britischen Norm BS7799-2 beruht, beschreibt Anforderungen für eine systematische Erstellung,

	Umsetzung, Dokumentation, Ausführung, Überwachung und Weiterentwicklung eines Informationssicherheits-Managementsystems (ISMS). Die Verantwortung des Managements, z. B. für eine grundlegende Verpflichtung auf Informationssicherheit oder für die Bereitstellung von Ressourcen, wird in einem eigenen Kapitel herausgestellt. Die Norm legt Wert auf eine kontinuierliche Verbesserung des ISMS. Hierfür bilden ISMS-Audits und Managementbewertungen des ISMS die Grundlagen.
Link	a) ISO-Website : http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 b) DIN-Website (mit Link zum deutschem Inhaltsverzeichnis): http://www.nia.din.de/cmd?artid=103960154&bcrumblevel=1&contextid=nia&subcommitteeid=54770248&level=tpl-art-detailansicht&committeeid=54738935&languageid=de

DIN ISO/IEC 27002

Titel	**DIN ISO/IEC 27002** **Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-Management** **Information Technology – Security techniques – Code of practice for information security management**
Aktuelle Version	a) ISO/IEC 27002:2005 b) DIN-Ausgabe 2008-09
Status	• ISO: Review Stage 90.92 (International Standard to be revised) 2008-04-22
Inhalt	Die ISO/IEC 27002 beinhaltet einen umfangreichen Maßnahmenkatalog zur Umsetzung der DIN ISO/IEC 27001. Behandelt werden die Einschätzung von und der Umgang mit Sicherheitsrisiken, die Nutzung einer Sicherheitsrichtlinie, die Organisation der Informationssicherheit und das Asset Management, hier insbesondere die Klassifizierung von Information. Weitere Themen sind personelle Aspekte der Sicherheit, die physische Sicherheit, das Betriebs- und Kommunikationsmanagement, Zugangskontrolle, die Beschaffung, Entwicklung und Wartung von Informationssystemen, der Umgang mit Informationssicherheitsvorfällen, Umgang mit Informationssicherheitsvorfällen, Business Continuity Management und die Einhaltung von Vorgaben (Compliance).
Link	a) ISO-Website : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50297 b) DIN-Website (mit Link zum deutschem und englischem Inhaltsverzeichnis):

	http://www.beuth.de/de/norm/din-iso-iec-27002/110488964?SearchID=440388225

3.4 ISO/IEC-Normen

In dieser Gruppe werden Normen aufgelistet, die von der ISO und der IEC gemeinsam herausgegeben werden. Betrachtet werden lediglich aktuelle, verabschiedete Normen, die noch nicht zurückgezogen wurden. Auch ergänzende Dokumente, d. h. Technical Reports (TR) und Technical Specifications (TS), bleiben unberücksichtigt. Soweit ISO/IEC-Normen auch deutsche Normen darstellen, werden sie in diesem Abschnitt nicht erneut angegeben.

ISO/IEC 2382-1

Titel	**ISO/IEC 2382-1** **Information technology – Vocabulary – Part 1: Fundamental terms**
Aktuelle Version	ISO/IEC 2382-1:1993
Status	Review Stage 90.93 (International Standard confirmed) 2010-06-29
Inhalt	Die ISO/IEC 2382-1 enthält grundlegende Definitionen der IT, beispielsweise zur IT-Sicherheit, zu Anwendungen und Nutzern oder zum Datenmanagement.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=7229 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?artid=1369403&contextid=nia&bcrumblevel=1&subcommitteeid=54755362&level=tpl-art-detailansicht&committeeid=54738935&languageid=de

ISO/IEC 12207

Titel	**ISO/IEC 12207** **System and software engineering – Software life cycle processes**
Aktuelle Version	ISO/IEC 12207:2008
Status	Review Stage 90.92 (International Standard to be revised) 2013-02-26
Inhalt	Die ISO/IEC 12207 definiert einen Prozessstandard für die Entwicklung und das Management von Software. Hierfür beschreibt sie eine Architektur für den Lebenszyklus von Software, beginnend mit

	der ersten Bedarfs- und Anforderungsanalyse über Projektmanagement und Akquisition, Implementierung, Betrieb und Support bis hin zur Ablösung/Außerbetriebnahme. Die Norm gliedert die Architektur des Software-Lebenszyklus in sieben Prozessgruppen mit insgesamt 44 Prozessen. Sie ist insofern von grundlegender Bedeutung, als sie „weltweit für eine Vereinheitlichung von Begriffen und ein gemeinsames Verständnis von Konzepten“[27] bzgl. der Prozesse des Software-Lebenszyklus sorgt. Dies zeigt sich darin, dass sich andere Standards und Normen, wie z. B. CMMI oder die DIN ISO/IEC 15504, auf die ISO/IEC 12207 – insb. auf das Prozessmodell – beziehen.[28]
Link	a) ISO-Website: http://www.iso.org/iso/catalogue_detail?csnumber=43447 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=108283491&bcrumblevel=2&languageid=de

ISO/IEC 15288

Titel	**ISO/IEC 15288** **Systems and software engineering – System life cycle processes**
Aktuelle Version	ISO/IEC 15288:2008
Status	Review Stage 90.92 (International Standard to be revised) 2013-02-26
Inhalt	Die ISO/IEC 15288 enthält ein Lebenszyklusmodell und gliedert dieses in einzelne Prozesse (z. B. bezüglich Vereinbarung, Anschaffung, Management, Qualität, Personal, Projekt, Technik). Im Anhang wird die Integration mit ISO/IEC 12207 beschrieben.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43564 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=108283502&languageid=de&bcrumblevel=3&subcommitteeid=54770175

Normenreihe ISO/IEC 15504-x

Die folgende Norm ISO/IEC 15504-6 ergänzt die in Abschnitt 3.2 beschriebenen Normen DIN ISO/IEC 15504-1 bis DIN ISO/IEC 15504-5. Weitere

[27] *Liggesmeyer 2009*, S. 18.
[28] Vgl. *ebd.*

Dokumenten dieser Normenreihe bilden verschiedene Technical Reports und Technical Specifications.

ISO/IEC 15504-6

Titel	**DIN ISO/IEC 15504-6** **Information technology – Process assessment – Part 6: An exemplar system life cycle process assessment model**
Aktuelle Version	ISO/IEC 15504-6:2013
Status	Publication stage 60.60 (International Standard published) 2013-06-05
Inhalt	Die ISO/IEC 15504-6 ergänzt die ISO/IEC 15504-5 in denjenigen Fällen, wo Software- und Systemlebenszyklus integriert bewertet werden müssen. Anwendungsfelder im Bereich der IT sind große IT-Infrastrukturprojekte oder die Entwicklung und Lieferung von „embedded systems“.
Link	a) ISO-Website : http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61492 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=189652856&languageid=de&bcrumblevel=3&subcommitteeid=54770175

ISO/IEC 18043

Titel	**ISO/IEC 18043** **Information technology – Security techniques – Selection, deployment and operations of intrusion detection system**
Aktuelle Version	ISO/IEC 18043:2006
Status	Review Stage 90.92 (International Standard to be revised) 2010-04-23
Inhalt	Die ISO/IEC 18043 gibt Hinweise zur Auswahl, zum Einsatz und zum Betrieb von Intrusion Detection Systemen (IDS). Die Norm richtet sich an die Managementebene und Nutzer, die • den Nutzen und die Beschränkungen von IDS verstehen wollen, • eine IDS-Strategie und einen Einführungsplan zu entwickeln haben, • die Ergebnisse eines IDS managen müssen, • IDS in die Sicherheitsstrategie und -struktur des Unternehmens zu integrieren haben, • rechtliche Fragen beim Einsatz von IDS zu berücksichtigen haben.

Link	b) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=35394 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=92134614&languageid=de&bcrumblevel=3&subcommitteeid=146321440

Normenreihe ISO/IEC 20000-x

Die Normenreihe „ISO/IEC 20000-x“ richtet sich auf das IT-Servicemanagement. Sie kann durch die institutionelle Zertifizierungsmöglichkeit[29] als eine Ergänzung zum IT-Servicemanagementstandard „ITIL“ angesehen werden, der Zertifizierungen lediglich auf einer persönlichen Ebene erlaubt. Die Normenreihe besteht mittlerweile aus drei Normen, ergänzt um zwei Technische Reports.

ISO/IEC 20000-1

Titel	**ISO/IEC 20000-1** **Information technology – Service management – Part 1: Service management system requirements**
Aktuelle Version	ISO/IEC 20000-1:2011
Status	Publication Stage 60.60 (International Standard published) 2011-04-12
Inhalt	Die ISO/IEC 20000-1 beschreibt – ausgerichtet an den Prozessbeschreibungen der IT Infrastructure Library (ITIL) – Mindestanforderungen an ein professionelles IT-Service-Management (ITSM). Die Norm beinhaltet die Vorgaben, die ein Unternehmen erfüllen, sicherstellen und nachweislich dokumentieren muss, um eine entsprechende Zertifizierung zu erhalten. Die ISO/IEC 20000-1 stellt somit einen messbaren Qualitätsstandard für das IT-Service-Management dar.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=51986 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=142032964&bcrumblevel=2&languageid=de

[29] Für eine Diskussion der Vor- und Nachteile einer ISO 20000-Zertifizierung siehe *Dohle u.a. 2009*, S. 3ff.

ISO/IEC 20000-2

Titel	**ISO/IEC 20000-2** **Information technology – Service management – Part 2: Guidance on the application of service management systems**
Aktuelle Version	ISO/IEC 20000-2:2012
Status	Publication Stage 60.60 (International Standard published) 2012-02-14
Inhalt	Die ISO/IEC 20000-2 enthält Leitlinien für die Gestaltung von ITSM-Systemen entsprechend den Anforderungen der ISO/IEC 20000-1. Die Norm enthält Beispiele und Anregungen für die Umsetzung eines IT-Servicemanagements sowie Verweise auf andere Teile der ISO/IEC 20000-x und weitere relevante Normen.
Link	a) ISO-Website: http://www.iso.org/iso/catalogue_detail?csnumber=51987 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&subcommitteeid=54770175&artid=151262803&bcrumblevel=2&languageid=de

ISO/IEC 20000-3

Titel	**ISO/IEC 20000-3** **Information technology – Service management – Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1**
Aktuelle Version	ISO/IEC 20000-3:2012
Status	Publication Stage 60.60 (International Standard published) 2012-08-14
Inhalt	Die ISO/IEC 20000-3 beinhaltet als dritter Teil der ISO/IEC 20000 allgemeine praktische Anleitungen für die Umfangsdefinition (scope definition) unter Einbeziehung von Service Providern und sonstigen Lieferanten. Hierfür werden zahlreiche Beispiele (Szenarien) gegeben.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=60031 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=164911888&languageid=de&bcrumblevel=4&subcommitteeid=54770175

ISO/IEC 24762

Titel	**ISO/IEC 24762** **Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services**
Aktuelle Version	ISO/IEC 24762:2008
Status	Review Stage 90.92 (International Standard to be revised) 2011-04-19
Inhalt	Die ISO/IEC 24762 beschreibt Anforderungen an interne und externe Dienste zur Wiederherstellung (Disaster recovery – DR) von Informations- und Kommunikationstechnologien, wie z. B. Anforderungen an DR-Trainingsmaßnahmen, an die Identifikation und den Schutz der IT-Assets oder an die Dokumentation. „Der Standard definiert Anforderungen, die bei der Auswahl eines Dienstleisters von Wiederherstellungsdiensten durch eine Organisation oder bei der Gestaltung von Wiederherstellungsdiensten durch den Dienstleister selbst berücksichtigt werden sollen. Die Anforderungen adressieren interne wie externe Dienstleister.“[30]
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=41532 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=107020845&languageid=de&bcrumblevel=3&subcommitteeid=146321440

Normenreihe ISO/IEC 2700x

Die folgenden Normen ergänzen die in Abschnitt 3.3 beschriebenen Normen DIN ISO/IEC 27001 bis DIN ISO/IEC 27003. Außer Acht bleibt die ISO/IEC 27006, da diese Vorgaben für Zertifizierungsorganisationen trifft, die Informationssicherheits-Managementsysteme nach DIN ISO/IEC 27001 prüfen und zertifizieren wollen, und somit für Unternehmen weniger interessant ist.

ISO/IEC 270003

Titel	**ISO/IEC 27003** **Information technology – Security techniques – Information security management system implementation guidance**
Aktuelle Version	ISO/IEC 27003:2010

[30] *BITKOM 2009*, S. 27

Status	Review Stage 90.92 (International Standard to be revised) 2013-01-14
Inhalt	Die ISO/IEC 27003 ist als Implementierungsleitfaden der ISO/IEC 27001 einzustufen. Die Norm bietet im Wesentlichen eine Hilfestellung für die Planung und Einführung eines ISMS (Informationssicherheits-Managementsystems). Auch die wichtige Frage, wie die Zustimmung des Managements zu einem ISMS-Projekt zu erreichen ist, wird von der Norm adressiert.
Link	a) ISO-Website: http://www.iso.org/iso/catalogue_detail?csnumber=42105 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=126968584&languageid=de&bcrumblevel=3&subcommitteeid=54742877

ISO/IEC 270004

Titel	**ISO/IEC 27004** **Information technology – Security techniques – Information security management – Measurement**
Aktuelle Version	ISO/IEC 27004:2009
Status	Review Stage 90.92 (International Standard to be revised) 2013-06-11
Inhalt	Die ISO/IEC 27004 richtet sich auf die Bewertung der Effektivität eines nach ISO/IEC 27001 ausgestalteten ISMS. Die Norm setzt sich mit Messverfahren genauso auseinander wie mit Fragen der Managementverantwortlichkeit in Bezug auf die Bewertung des ISMS.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42106 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=125172607&languageid=de&bcrumblevel=3&subcommitteeid=54742877

ISO/IEC 270005

Titel	**ISO/IEC 27005** **Information technology – Security techniques – Information security risk management**
Aktuelle Version	ISO/IEC 27005:2011
Status	Review Stage 90.92 (International Standard to be revised) 2013-06-10

Inhalt	Die ISO/IEC 27005 unterstützt die generellen Konzepte der ISO/IEC 27001 und unterstützt die Implementierung eines entsprechend ausgerichteten ISMS durch ein adäquates Informationssicherheits-Risikomanagement. Die Norm bietet Hilfestellung für Informations-risikoanalyse und -bewertung sowie für die Einrichtung eines Infor-mationsrisiko-Managementprozesses.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=143000568&languageid=de&bcrumblevel=3&subcommitteeid=54742877

ISO/IEC 270007

Titel	**ISO/IEC 27007** **Information technology – Security techniques – Guidelines fpor information security management systems auditing**
Aktuelle Version	ISO/IEC 27007:2011
Status	Publication Stage 60.60 (International Standard published) 2011-11-14
Inhalt	Die ISO/IEC 27007 beinhaltet Richtlinien für diejenigen, die als unter-nehmensinterne oder -externe Prüfer ein Audit-Programm für ISMS aufstellen und Prüfungen vorbereiten und durchführen müssen. Auch erforderliche Fähigkeiten und die Auswahl von Auditoren werden be-schrieben.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42506 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=148250279&languageid=de&bcrumblevel=3&subcommitteeid=54742877

ISO/IEC 270010

Titel	**ISO/IEC 27010** **Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications**
Aktuelle Version	ISO/IEC 27010:2012
Status	Publication Stage 60.60 (International Standard published) 2012-03-20

Inhalt	Die ISO/IEC 27010 befasst sich mit Informationssicherheits-Management für organisationsübergreifende Kommunikation, z. B. im Rahmen von Communities. Neben technischen Aspekten werden auch Fragen der Informationssicherheitspolitik, die Organisation der Informationssicherheit, Asset Management, Informationssicherheits-Incident-Management oder Compliance erörtert.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42509 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=152467955&languageid=de&bcrumblevel=3&subcommitteeid=54742877

Die Normen ISO/IEC 27011ff. sollen branchenspezifische Spezialisierungen der ISO/IEC 27002 darstellen. Derzeit ist dies für Telekommunikationsunternehmen in der ISO/IEC 27011 umgesetzt, für weitere Branchen liegen Technische Reports vor (z. B. ISO/IEC TR 27019 für Energieunternehmen). Weitere für das IT-Management relevante Normen sind:

ISO/IEC 270013

Titel	**ISO/IEC 27013** **Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1**
Aktuelle Version	ISO/IEC 27013:2012
Status	Review Stage 90.92 (International Standard to be revised) 2013-06-10
Inhalt	Die ISO/IEC 27013 beinhaltet Hinweise für diejenigen Unternehmen, die die beiden Normen ISO/IEC 27001 und ISO/IEC 20000-1 gemeinsam oder nacheinander implementieren oder die beiden jeweils getrennt eingeführten Managementsysteme nachträglich integrieren wollen. Die Norm hebt diejenigen Managementprozesse hervor, bei denen Synergievorteile durch eine Integration von IT-Sicherheits- und IT-Servicemanagement zu realisieren sind (z. B. Service-Level-Management, Kontinuitätsmanagement oder Lieferantenmanagement).
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43753 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=167971026&languageid=de&bcrumblevel=3&subcommitteeid=54742877

ISO/IEC 270014

Titel	**ISO/IEC 27014** **Information technology – Security techniques – Governance of information security**
Aktuelle Version	ISO/IEC 27014:2013
Status	Publication Stage 60.60 (International Standard published) 2013-04-23
Inhalt	Die für das IT-Sicherheitsmanagement wichtige Norm ISO/IEC 27014 beschreibt Prinzipien und Prozesse für die IT Security Governance. Hierdurch sollen Unternehmen in die Lage versetzt werden, alle Aktivitäten die Informationssicherheit betreffend integriert steuern, bewerten, überwachen und kommunizieren zu können.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42506 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=148250279&languageid=de&bcrumblevel=3&subcommitteeid=54742877

ISO/IEC 270031

Titel	**ISO/IEC 27031** **Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity**
Aktuelle Version	ISO/IEC 27031:2011
Status	Publication Stage 60.60 (International Standard published) 2011-03-01
Inhalt	Die ISO/IEC 27031 beinhaltet basierend auf dem BS 25777 Ausführungen zur Rolle der IT im Rahmen des unternehmensweiten Kontinuitätsmanagements. Die Norm prägt hierfür den Begriff „Information and communication technology readiness for business continuity“ (IRBC). Die Ausführungen decken Managementverantwortlichkeiten, Planungs-, Implementierungs- und Betriebsaspekte sowie Überwachung und Review des IRBC ab.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=140332996&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 270032

Titel	**ISO/IEC 27032** **Information technology – Security techniques – Guidelines for cybersecurity**
Aktuelle Version	ISO/IEC 27032:2012
Status	Publication Stage 60.60 (International Standard published) 2012-07-16
Inhalt	Die ISO/IEC 27032 beinhaltet grundlegende Hinweise zur Sicherheit im Cyberspace. Die Beschreibungen beinhalten z. B. Stakeholder, Assets und Bedrohungen im Cyberspace. Die Richtlinien für Stakeholder richten sich an beliebige Organisationen, denen grundlegende Cybersecurity-Kontrollen empfohlen werden. Insgesamt bietet die Norm einen Überblick, der als Grundlage der Sensibilisierung für Cybersecurity im Unternehmen dienen kann.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44375 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=155835192&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 270033-1

Titel	**ISO/IEC 27033-1** **Information technology – Security techniques – Network security – Part 1: Overview and concepts**
Aktuelle Version	ISO/IEC 27033-1:2009
Status	Review Stage 90.92 (International Standard to be revised) 2013-01-11
Inhalt	Die ISO/IEC 27033-1 beinhaltet grundlegende Ausführungen zur Netzwerksicherheit, d. h. zu den verschiedenen Risiken, zur Risikoanalyse oder zu notwendigen Kontrollen. Für verschiedene Netzwerk-Anwendungsszenarien, z. B. Internetzugang für Mitarbeiter, B2B- oder B2C-Services oder mobile Kommunikation, werden Risiken, Sicherheitstechniken und Design sowie jeweilige Kontrollen diskutiert. Die Norm bietet damit eine Einführung, die als Grundlage für entsprechende Richtlinien im Unternehmen dienen kann.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51580 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-

	detailansicht&committeeid=54738935&artid=125172918&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 270033-2

Titel	**ISO/IEC 27033-2** **Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security**
Aktuelle Version	ISO/IEC 27033-2:2012
Status	Publication Stage 60.60 (International Standard published) 2012-07-27
Inhalt	Die ISO/IEC 27033-2 beinhaltet Richtlinien für die Vorbereitung, Gestaltung und Einführung von Maßnahmen zur Netzwerksicherheit. Zur Vorbereitung zählen eine Analyse u. a. der regulatorischen und der Geschäftsanforderungen. Ein Anhang enthält Muster für die Dokumentation der Netzwerksicherheitsarchitektur und der Sicherheitsanforderungen (z. B. Firewall-Konfiguration, physische Sicherheit, personelle Anforderungen).
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51581 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=164067612&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 270033-3

Titel	**ISO/IEC 27033-3** **Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues**
Aktuelle Version	ISO/IEC 27033-3:2010
Status	ISO: Review Stage 90.93 (International Standard confirmed) 2013-04-26
Inhalt	Die ISO/IEC 27033-3 detailliert die in ISO/IEC 27033-1 enthaltenen Netzwerk-Anwendungsszenarien. Die Beschreibung besteht jeweils aus einer Einführung, den spezifischen Bedrohungen, dem daraus resultierend erforderlichen Sicherheitsdesign und den erforderlichen Kontrollen.
Link	• ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51582

	b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=137802333&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 270034-1

Titel	**ISO/IEC 27034-1** **Information technology – Security techniques – Application security – Part 1: Overview and concepts**
Aktuelle Version	ISO/IEC 27034-1:2011
Status	Publication Stage 60.60 (International Standard published) 2011-11-21
Inhalt	Die ISO/IEC 27034-1 beinhaltet grundlegende Ausführungen zur Sicherheit von Anwendungen. Ausgeführt werden der Kontext der Sicherheit von Anwendungen (z. B. rechtlicher Rahmen, Applikations-Lebenszyklus, unterstützter Prozess, umgebende Organisation, verwendete Daten), Sicherheitsanforderungen, Risiken, Kosten der Sicherheit, Zielumgebung und Kontrollen bzw. Kontrollziele. Außerdem wird ein Sicherheits-Managementprozess beschrieben, der von der Spezifikation der Sicherheitsanforderungen über die anwendungsbezogene Risikobewertung letztlich bis hin zum Auditing der Anwendungssicherheit reicht. Den Kern bilden einzelne Konzepte, beispielsweise zur Sicherheitsbeurteilung oder zu einem Sicherheitsaudit, deren Anwendung den Unternehmen anempfohlen wird.
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44378 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=148454745&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 270035

Titel	**ISO/IEC 27035** **Information technology – Security techniques – Information security incident management**
Aktuelle Version	ISO/IEC 27035:2011
Status	Publication Stage 60.60 (International Standard published) 2011-08-17
Inhalt	Die ISO/IEC 27035 beinhaltet für Unternehmen aller Größenklassen „Hinweise und Anleitungen zur systematischen Erkennung, Evaluierung, Behandlung, Dokumentation, Reporting und Bewertung von IT-

	Sicherheitsvorfällen im Unternehmen“.[31]
Link	a) ISO-Website: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44379 b) DIN-Website (mit Link zum englischen Inhaltsverzeichnis): http://www.nia.din.de/cmd?level=tpl-art-detailansicht&committeeid=54738935&artid=145376936&languageid=de&bcrumblevel=3&subcommitteeid=146321440

ISO/IEC 38500

Titel	**ISO/IEC 38500** **Corporate governance of information technology**
Aktuelle Version	ISO/IEC 38500:2008
Status	Review Stage 90.92 (International Standard to be revised) 2012-09-21
Inhalt	Die für die Steuerung des IT-Einsatzes im Unternehmen zentrale Norm ISO/IEC 38500 beinhaltet ein Referenzmodell für die IT-Governance, das auf dem Corporate-Governance-Verständnis des Cadbury-Reports und den Corporate-Governance-Grundsätzen der OECD beruht. Dieses Verständnis wird von der Norm für IT-Belange spezialisiert. „Corporate governance of IT“ ist somit das System, durch das die aktuelle und künftige Nutzung der IT geleitet und bedarfsgerecht gesteuert wird. Im Vordergrund steht der planvolle Einsatz der IT, der an den Unternehmenszielen und der daraus abgeleiteten IT-Strategie ausgerichtet sein soll. Die Norm beschreibt ein grundlegendes Modell der IT-Governance, das im Rahmen von sechs Prinzipien (Verantwortlichkeit, Strategie, Beschaffung, Performanz, Konformität, Verhalten) Zielsetzungen guter IT-Governance postuliert. Diese Ziele werden erreicht, indem die oberen Entscheidungsträger und -gremien • den aktuellen und künftigen IT-Einsatz kontinuierlich bewerten (Bewertung), • sicherstellen, dass die Erstellung und die Umsetzung von IT-Planungen und Richtlinien für die Nutzung der IT den Geschäftsanforderungen entsprechen (Leitung), • die Einhaltung von externen Vorgaben, internen Richtlinien und Plänen sowie die Leistung der IT überwachen.[32]
Link	a) ISO-Website: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_deta

[31] *BITKOM 2009*, S. 25
[32] Im Wesentlichen übernommen aus *Klotz 2008*.

	il.htm?csnumber=51639 b) Teil-Download von der IEC-Website: http://webstore.iec.ch/preview/info_isoiec38500%7Bed1.0%7Den.pdf

ISO/IEC 90003

Titel	**ISO/IEC 90003** **Software engineering – Guidelines for the application of ISO 9001:2000 to computer software**
Aktuelle Version	ISO/IEC 90003-2004
Status	Review Stage 90.92 (International Standard to be revised) 2008-08-08
Inhalt	Die ISO/IEC 90003 unterstützt Unternehmen bei der Anwendung der ISO 9001 (Quality management systems – Requirements) in der Beschaffung, der Lieferung, der Entwicklung, dem Betrieb und der Wartung von Software und zugehörigen Support-Dienstleistungen.[33]
Link	ISO-Website: http://www.iso.org/iso/catalogue_detail?csnumber=35867

[33] Mittlerweile liegt die ISO 9001 in der Version ISO 9001:2008 vor, die als DIN EN ISO 9001:2008 übernommen wurde.

Quellenangaben

BITKOM 2009: Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (BITKOM); Deutsches Institut der Normung e.V. (DIN) Normenausschuss Informationstechnik und Anwendungen (NIA) (Hg.): Kompass der IT-Sicherheitsstandards – Leitfaden und Nachschlagewerk, 4. Aufl., online verfügbar unter: http://www.bitkom.org/files/documents/Kompass_der_IT-Sicherheitsstandards_web.pdf (letzter Zugriff am 12.08.2013)

DIN 2013: DIN Deutsches Institut für Normung e. V.: DIN e. V., http://www.din.de/cmd?cmsrubid=47514&menurubricid=47514&level=tpl-rubrik&menuid=47391&languageid=de&cmsareaid=47391 (letzter Zugriff am 12.08.2013)

DIN EN 45020: DIN EN 45020 – Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe (ISO/IEC Guide 2:2004), Entwurf, Juni 2004.

DIN – NIA 2013: DIN Deutsches Institut für Normung e. V.: Der NIA, http://www.nia.din.de/cmd?cmsrubid=57868&menurubricid=57868&level=tpl-rubrik&committeeid=54738935&menuid=46420&languageid=de&bcrumblevel=2&cmsareaid=46420 (letzter Zugriff am 12.08.2013)

Dohle u. a. 2009: Dohle, H.; Schmidt, R.; Zielke, F.; Schürman, T.: ISO 2000 – Eine Einführung für Manager und Projektleiter, Heidelberg: dpunkt 2009

ISO2013: International Organization for Standardization (ISO): JTC 1, http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45020 (letzter Zugriff am 12.08.2013)

ISO/IEC 12207:2008: ISO/IEC: System and software engineering – Software life cycle processes, ISO/IEC 12207:2008, Second Edition 2008.

ISO/IEC 38500:2008: ISO/IEC: Corporate governance of information technology, International Standard ISO/IEC 38500:2008, First Edition 2008.

Klotz 2008: Klotz, M.: IT-Governance genormt - die neue ISO/IEC 38500 In: IT-Governance, Jg. 2 (2008), Heft 4.

Klotz 2012: Klotz, Michael: Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke. In: SIMAT Arbeitspapiere. Hrsg. von Michael Klotz. 2., überarb. u. erw. Aufl. Stralsund: FH Stralsund, SIMAT Stralsund Information Management Team, 2012 (SIMAT AP, 4 (2012), 20).

Klotz 2013: IT-Compliance. In: Ernst Tiemeyer (Hg.): Handbuch IT-Management – Konzepte, Methoden, Lösungen und Arbeitshilfen für die Praxis, 5. Auflage, München: Hanser 2013, S. 707-763

Liggesmeyer 2009: Liggesmeyer, P.: Software-Qualität – Testen, Analysieren und Verifizieren von Software, 2. Aufl., Heidelberg: Spektrum Akademischer Verlag, 2009.

Singh 1996: Singh, R.: International Standard ISO/IEC 12207 Software Life Cycle Processes. In: Software Process – Improvement and Prctice, Jg. 2 (1996), S. 35-50; online verfügbar unter: http://www.abelia.com/docs/12207cpt.pdf (letzter Zugriff am 12.08.2013)

VOI 2008: VOI Verband Organisations- und Informationssysteme e. V. (Hg.): Standards und Normen im Umfeld ECM – Leitfaden für organisatorische und technische Anforderungen, Berlin: VOI 2008

Das Stralsund Information Management Team (SIMAT)

Das von Prof. Dr. Michael Klotz geleitete „Stralsund Information Management Team“ (SIMAT) ist am Fachbereich Wirtschaft der FH Stralsund angesiedelt. Es bündelt akademische Lehre und Forschung, Weiterbildungsangebote und Projekte im Themenbereich des betrieblichen Informationsmanagements. Informationsmanagement richtet sich auf die effektive und effiziente Nutzung der informationellen Ressourcen eines Unternehmens. Diese Zielsetzung wird heute von verschiedenen spezialisierten Fachrichtungen in der Informatik, der Wirtschaftsinformatik und der Betriebswirtschaftslehre verfolgt. Das SIMAT arbeitet insofern interdisziplinär, wobei die inhaltlichen Schwerpunkte in Kompetenzzentren (Competence Center) fokussiert werden. Im Rahmen des RD&D-Ansatzes (Research, Development and Demonstration) dienen Labore, die mit aktuellen Tools des Informationsmanagements ausgestattet sind, sowohl der fachlichen Arbeit als auch zu Demonstrationszwecken. Eine intensive Kooperation mit ausgewiesenen Expertinnen und Experten sowie mit privatwirtschaftlichen Unternehmen und die Mitarbeit in anwendungsnahen Fachorganisationen gewährleisten eine praxis- und lösungsorientierte Vorgehensweise. Die Zusammenarbeit mit Lehrstühlen anderer Hochschulen, wissenschaftlichen Einrichtungen und eine umfangreiche Publikationstätigkeit stellen sicher, dass sich das SIMAT am State-of-the-Art des Informationsmanagements orientiert und diesen mitprägt. Auf diese Weise sind die Mitarbeiterinnen und Mitarbeiter des SIMAT in der Lage, anspruchsvolle Konzepte und Lösungen zu konzipieren und zu realisieren.

Das SIMAT versteht sich als Mittler zwischen akademischer Forschung und Lehre auf der einen, und der Wirtschaftspraxis auf der anderen Seite. Diese Transferaufgabe, verankert im Landeshochschulgesetz Mecklenburg-Vorpommerns, bildet den Schwerpunkt der Arbeit des SIMAT. Forschung und Lehre werden nicht als Selbstzweck begriffen, sondern führen zu handlungsrelevanten, innovativen Konzepten und Lösungen, die in die Unternehmenspraxis transferiert werden. Die berufliche Weiterbildung bildet hierbei ein wesentliches Element.

Die anwendungsnahe Forschung am SIMAT ist auf eine ökonomische Verwertung hin orientiert. Es sollen Innovationen entwickelt und in Kooperation mit anderen wissenschaftlichen Einrichtungen, Fach-Institutionen und Unternehmen in eine nachhaltige und profitable Praxis umgesetzt werden. Hierzu werden eigene F&E-Projekte auf dem Gebiet des Informationsmanagements und Innovationsprojekte mit Partnern durchgeführt. Zudem hat sich das SIMAT auf die betriebswirtschaftliche Begleitberatung bei IT-nahen Technologieprojekten spezialisiert. Studierenden und wissenschaftlichen Mitarbeiterinnen und Mitarbeitern wird die Möglichkeit eröffnet, an

der Lösung praktischer Problemstellungen zu arbeiten und sich so optimal auf das spätere Berufsleben vorzubereiten.

Die studentischen Mitarbeiterinnen und Mitarbeiter erhalten im SIMAT Einblick in die Arbeitsmethodik sowohl auf wissenschaftlichem als auch auf wirtschaftlichem Gebiet. Aus den Projekten des SIMAT entstehen zahlreiche Abschlussarbeiten, die den Studierenden der FH Stralsund offen stehen. Das SIMAT bietet zudem eine berufliche Perspektive für Studierende, die sich als wissenschaftliche Mitarbeiter in der anwendungsnahen Forschung qualifizieren wollen.

Das SIMAT beteiligt sich zudem an der Diskussion der wissenschaftlichen Gemeinschaft. Hierzu werden regelmäßig Arbeitspapiere veröffentlicht, die den Stand der Arbeit des SIMAT in die Öffentlichkeit tragen und zur Diskussion anregen sollen. Das SIMAT lädt zudem andere Wissenschaftler, aber auch Referenten aus der Praxis als Vortragende ein. Auf diese Weise lernen die SIMAT-Mitarbeiterinnen und -Mitarbeiter sowie andere interessierte Studierende aktuelle Forschungsergebnisse und praktische Fragestellungen aus erster Hand kennen. Erkenntnisse aus diesen Aktivitäten sowie aus den verschiedenen F&E-Projekten werden systematisch in die Lehre überführt, so dass alle Studierenden von der Forschungsarbeit des SIMAT profitieren können.

Zum Zwecke des ökonomischen Transfers verfolgt das SIMAT den RD&D-Ansatz (Research, Development and Demonstration). Hierzu werden Labore als Demonstrationsbereiche unterhalten. In den Laboren werden Produkte und Lösungen von Kooperationspartnern des SIMAT in den Bereichen des Informations-, Projekt- und Prozessmanagements betrieben. Auf dieser technischen Grundlage werden im Rahmen von Projekten durch das SIMAT-Team prototypische Lösungen erarbeitet.

Kontakt

FH Stralsund • SIMAT • Zur Schwedenschanze 15 • 18435 Stralsund
Ansprechpartner: Prof. Dr. Michael Klotz (Wissenschaftlicher Leiter)
☎ +49 (0)3831 45-6946
✉ michael.klotz@fh-stralsund.de
www.simat-stralsund.de

Verzeichnis der SIMAT-Arbeitspapiere

AP	Datum	Autor	Titel
01-09-001	01.2009	M. Klotz	Datenschutz in KMU – Lehren für die IT-Compliance
01-09-002	02.2009	M. Klotz	Von der Informationsgesellschaft zum Informationsarbeiter
01-09-003	09.2009	L. Ramin M. Klotz	Aufgaben und Verantwortlichkeiten von IT-Nutzern anhand von COBIT
01-09-004	10.2009	S. Kubisch	Corporate Governance gemäß BilMoG und SOX
02-10-005	06.2010	M. Klotz	PMBOK-Compliance der Projektmanagement-Software Projektron BCS
02-10-006	07.2010	A. Woltering	Kontinuierliche Verbesserung von Desktop-Services mittels Benchmarking
02-10-007	09.2010	M. Klotz	Grundlagen der Projekt-Compliance
02-10-008	11.2010	I. Karminski	Grundlagen und aktuelle Entwicklungen der digitalen Betriebsprüfung
02-10-009	12.2010	D. Engel/ N. Zdrowomyslaw	Benchmarking-Studie Stralsund 2010
03-11-010	02.2011	E. Tiemeyer	Kennzahlengestütztes IT-Projektcontrolling – Projekt-Scorecards einführen und erfolgreich nutzen
03-11-011	05.2011	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke
03-11-012	06.2011	M. Klotz	Konzeption des persönlichen Informations-managements
03-11-013	08.2011	H. Auerbach/ N. Zdrowomyslaw	9. STeP-Kongress „Region gestalten! Gesundheitswirtschaft und Zukunftsmanagement“
03-11-014	08.2011	M. Klotz	Rollen der Information im Unternehmen
03-11-015	08.2011	Ahlfeldt	eGuides in kulturellen Einrichtungen – deutschsprachiger Museums-Apps
03-11-016	11.2011	S. J. Saatmann / I. Sulk / M. Klotz	Studie zu gewerblichen Strompreisen in Mecklenburg-Vorpommern – Strom als Wettbewerbsfaktor und Gegenstand der Standortvermarktung
04-12-017	02.2012	M. Klotz / I. Sulk / E. Wieck	GDPdU-Konformität von Projektmanagement-software – Exemplarische Konzeption und Umsetzung
04-12-018	07.2012	M. Horn-Vahlefeld	Projektdesign als organisatorischer Rahmen des Projektmanagements
04-12-019	08.2012	M. Klotz / J. Kriegel	ITIL und Datenschutz – Überlegungen für eine Integration des Datenschutzes in die IT-Prozesse nach ITIL
04-12-020	09.2012	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 1: Rechtliche Regelwerke, 2. Aufl.

04-12-021	10.2012	I. Sulk / M. Klotz	Einsatz von eGuides auf der Marienburg in Malbork (Polen) – Erhebung und Analyse einer Best Practice
04-12-022	12.2012	Witty, M. / C. Kliebisch	Die Versicherungsbranche unter FATCA
05-13-023	01.2013	S. J. Saatmann	The price-link in the natural gas market – The development of the oil price-link and alternative price mechanisms
05-13-024	02.2013	M. Klotz	Regelwerke der IT-Compliance – Klassifikation und Übersicht, Teil 2: Normen