Christoph Wildensee

Zugriffsberechtigungen / Access Management in rechnungslegungsrelevanten SAP ERP-Systemen

Exemplarische Rechtsgrundlagen, Risiken und Lösungsansätze für die kommunale deutsche Energiewirtschaft

Akademische Arbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783956368394

Christoph Wildensee

Zugriffsberechtigungen / Access Management in rechnungslegungsrelevanten SAP ERP-Systemen

Exemplarische Rechtsgrundlagen, Risiken und Lösungsansätze für die kommunale deutsche Energiewirtschaft

Diplom.de

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

ABSTRACT

„Zugriffsberechtigungen / Access Management in
rechnungslegungsrelevanten SAP ERP-Systemen
– Exemplarische Rechtsgrundlagen, Risiken und Lösungsansätze
für die kommunale deutsche Energiewirtschaft – “

by

Christoph Wildensee

2014

Access management is essential for ensuring, that accounting-related ERP systems run according to the rules. Basics of legitimation and application requirements are established by laws and court judgements. The standards are characterized in detail by accountants and the product manufacturers, especially access restrictions. The following thesis shows the legal and technical fundamentals and describes exemplary failings in the ERP system SAP. It turns out that recognized standard setters (e.g. ISACA, BSI), however, deploy a large number of regulations in information (systems) security management. But the german and EU administration are not able to set enough detailed regulation and unambiguity to force companies to do more than necessary against unauthorized data access, to implement effective authorization roles in accounting-related IT systems and finally to protect commercially sensitive data. Specifications exist, unambiguity and a graded threat of punishment is missing.

1. Einleitung

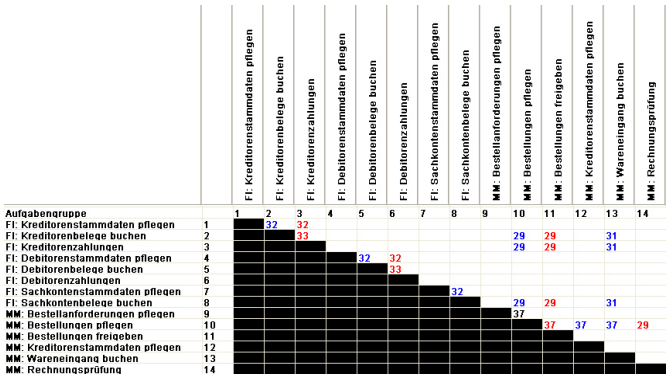
Informationen, ihre abgeleiteten Datenentsprechungen und die darauf fußenden Ablage- und Aufbereitungsstrukturen in den Systembestandteilen der Informationstechnologie (IT) stellen heute wesentliche Werte für Unternehmen dar und müssen daher folgerichtig adäquatem Schutz unterworfen sein. [1] „Sicherheitsvorfälle wie die Offenlegung oder Manipulation von Informationen können weitreichende geschäftsschädigende Auswirkungen haben oder die Erfüllung von Aufgaben behindern und somit hohe Kosten verursachen." [2] In der Öffentlichkeit diskutiert werden viele davon aus datenschutzrechtlicher Sicht, wenn es z.B. darum geht, dass dem Unternehmen personenbezogene Daten wie Kreditkartendaten oder ähnlich kritische, vom Kunden überlassene Informationen „verloren gehen", jedoch beginnt erst danach die notwendige Betrachtung der Grundlagen. Basis dafür ist das Bedürfnis, dass Daten, Prozesse, IT-Systeme, Vernetzung und die Prozessadressaten in einem Zustand der Kontinuität ohne störende Einflüsse agieren bzw. funktionieren, damit die Wertschöpfungs- und Ressourcenverwendungsketten reibungslos realisiert werden können.

„IT-Governance soll sicherstellen, dass die IT den optimalen Beitrag zur Wertschöpfung des Unternehmens in Bezug auf die Gewährleistung der Unternehmensstrategie und der Unternehmensziele liefert" [3] – wo im Detail möglich mit einer indikatorenorientierten Steuerungsausrichtung des IT-Einsatzes. Informations- und IT-Sicherheit als Teilaspekte des Sicherheitsmanagements im Unternehmen haben wiederum das Ziel, die Verfügbarkeit, die Vertraulichkeit, die Integrität und den vertrauenswürdigen Umgang mit den Informationen und abgeleiteten Daten, aber auch die Zuverlässigkeit, Unversehrtheit und Robustheit der Hard- und Software-Technologie zu gewährleisten. [4]

Weder die Wahl von Produkten noch einer Organisation zur Gewährleistung von IT-Sicherheit dürfen dabei aber – vornehmlich aus wirtschaftlichen Erwägungen heraus – die Prozesse im Unternehmen zu stark behindern, auch nicht, wenn Funktionstrennungen („Segregation of Duties" [SoD] [5]) systemseitig implementiert werden, weil mit bestimmten Funktionskombinationen ein natürliches Potential für Missbrauch assoziiert wird. [6]

---

[1] Vgl. HILDEBRAND/GEBAUER/HINRICHS/MIELKE(2011), S. 21, zur Information als Produktionsfaktor.
[2] BSI(2008), S. 5. Anzumerken als Herausforderung an ein Informationsmanagement und an die technische Lösungsbereitstellung, formuliert vom Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn.
[3] VOSSBEIN(2008), S. 77.
[4] Vgl. BSI(2008), S. 8 und BSI(2012), S. 3.
[5] SAP(I), Segregation of Duties Overview: "Segregation of Duties (SoD) is a control activity where an activity or set of activities are divided among several people in order to reduce the risk of fraud. Segregation of Duties is built around the idea that a critical or sensitive task be split from one person, thus reducing the likelihood of intentional fraud. Segregation of Duties represents a key internal control to help ensure no single person has too much control over a specific business operation. Segregation of duties is an essential component of a properly function internal controls environment within an organization.". Vgl. hierzu auch ASPRION(2013), S. 12ff.
[6] Vgl. auch ERWIN/MARLINGHAUS(2013), S. 21f.



Aufgabengruppe		1	2	3	4	5	6	7	8	9	10	11	12	13	14
FI: Kreditorenstammdaten pflegen	1		32	32											
FI: Kreditorenbelege buchen	2			33							29	29		31	
FI: Kreditorenzahlungen	3										29	29		31	
FI: Debitorenstammdaten pflegen	4					32	32								
FI: Debitorenbelege buchen	5						33								
FI: Debitorenzahlungen	6														
FI: Sachkontenstammdaten pflegen	7								32						
FI: Sachkontenbelege buchen	8										29	29		31	
MM: Bestellanforderungen pflegen	9										37				
MM: Bestellungen pflegen	10											37	37	37	29
MM: Bestellungen freigeben	11														
MM: Kreditorenstammdaten pflegen	12														
MM: Wareneingang buchen	13														
MM: Rechnungsprüfung	14														

Abb. 1-1: Beispiel einer zweidimensional-ausschließenden SAP-SoD-Matrix mit Berechtigtentrefferzahlen (Ausschnitt aus CheckAud). [7]

Investitionen in Informationstechnik und entsprechende IT-Sicherheitsprodukte, die alle Schichten inklusive der Basisinfrastruktur- (Betriebssystem, Datenbank, Netz) und Applikationsadministration überwachen bzw. einen Aktivitätsnachvollzug ermöglichen, haben nicht selten den Nebenaspekt, dass sie zu höherer Arbeits- und organisatorischer Ablaufqualität führen, wenn auch ein direkt messbarer Qualitätserhöhungsbeitrag in den Prozessen des Unternehmens nicht immer ermittelt werden kann. Eine optimierte Integration des Managements der Informationssicherheit in bestehende Strukturen ist zu erwarten. [8]

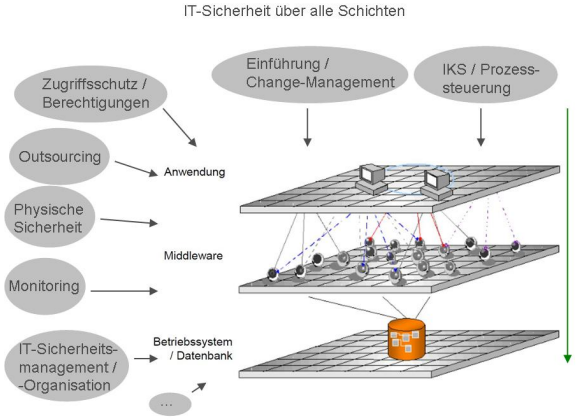


Abb. 1-2: Bestandteile eines IT-Sicherheitsmanagements über alle Schichten. [9]

Grundsätzlich gibt es kaum gesetzgeberische Klarheit, wenn es um die Frage geht, welche Maßnahmen ein Unternehmen zu ergreifen hat, um ein Mindestmaß an IT-Sicherheit herzustellen und wie stark hier auszuprägen ist, unter wirtschaftlichen Aspekten auch sanktionsfrei zu agieren. Dies ist verständlich, da neben der Aktualitätsfrage, die in Gesetzen kaum zu lösen ist, auch die unternehmerische Freiheit im Bereich der Organisations- und Prozessdefinition ggf. zu stark beschnitten wäre, insoweit können nur Maßstäbe zur Gewährleistung durch den Gesetzgeber allgemein formuliert und bestenfalls auf eine allgemeine Standardorientierung gesetzt werden.

---

[7] Eigene Darstellung mit dem Produkt CheckAud for SAP-Systems, Version 3.2, International Business Services for auditing and consulting (IBS) GmbH, Hamburg.
[8] Vgl. BSI(2008), S. 5.
[9] Einflussfaktoren auf die IT-Sicherheit in Anlehnung an BLEISE(2013), o.S.

Dies kann jedoch kaum zur Sanktionierung im Fall führen, dass Unternehmen gegen Sorgfaltspflichten aus diesen erwähnten Standards oder den Herstellerverlautbarungen zum IT-System verstoßen. Hierfür müsste neben der Initiierung einer juristischen Auseinandersetzung auch ein Verschulden im Sinne einer bewussten Untätigkeit, also einer Verletzung unternehmerischer Aufsichts- und Gestaltungspflichten, trotz besseren Wissens bewiesen (Vorsatzdelikt) oder zumindest grobe Fahrlässigkeit belegt werden, wenn es in einer persönlichen Haftung verantwortlich handelnder Personen gipfeln soll. [10] Auch müsste ein kausaler Zusammenhang zwischen Aktion oder Versäumnis und entstandenem Schaden herzuleiten sein. Sowohl die deliktische Haftung eines Unternehmens für seine Arbeitnehmer oder auch des verursachenden Arbeitnehmers selbst als auch die Haftung aus arbeitsvertraglicher Pflichtverletzung und Verantwortungsübernahme von leitenden Instanzen im Unternehmen im Sinne eines Organisationsverschuldens sind hier zu betrachten [11].

Strafrechtliche Vorschriften hinsichtlich des Ausspähens von Daten, definierten Computerbetrugs oder der Fälschung von Aufzeichnungen und beweiserheblicher Daten bzw. der Datenveränderung [12], die als Mischantragsdelikte (Mischung aus Antrags- und Offizialdelikt) erst einmal bekannt werden und somit aus dem Dunstkreis des Unternehmens heraustreten müssen, um verfolgt zu werden, helfen an dieser Stelle kaum. Nur wenn das Unternehmen Handlungsbedarf aufgrund eines unrechtmäßigen Handelns eines oder mehrerer Beschäftigter identifiziert, die Methoden verwenden, die unter die strafrechtlichen Vorschriften fallen (und dies wird regelmäßig nicht der Fall sein, wenn handelnde Personen im Auftrag des Unternehmens [13] die eigenen IT-Systeme [z.B. per Penetrationstests] folglich rechtmäßig auf Schwachstellen untersuchen [14]), wird es tätig und vornehmlich getrieben durch den potentiellen Imageschaden bei Innentätern die Abwicklung im Bereich des Arbeitsrechts und weniger über die schwierige Begründung aus dem Strafrecht – z.B. über einen Aufhebungsvertrag – vornehmen [15]. Hierbei ist diejenige Person, die die Handlung plante oder ausführte, im Fokus, weniger das dokumentierte und implementierte Berechtigungskonzept oder die verantwortlich handelnden

[10] Vgl. FEDERRATH(2010), S. 45., §§ 130, 30 OWiG ist in der Anwendung schwierig zu begründen.
[11] Vgl. GRIEGER(2010), S. 172f., im Zusammenhang mit übertragenem Aufgabenkreis und Schadenzuführung.
[12] Vgl. z.B. §§ 202, 202a, 202b, 202c, 263a, 268-271, 274, 303a Strafgesetzbuch (StGB).
[13] Vgl. WITT(2013), S. 26.
[14] Vgl. WELP(2007), S. 6.
[15] Michael Lörke ist der einhelligen Auffassung: „Speichert ein Angestellter beispielsweise Unternehmensdaten für eigene Zwecke, verhält er sich lediglich ungetreu. Er dringt jedoch nicht in einen von § 202a geschützten fremden Herrschaftsbereich ein. […] Erfasst werden soll von der Vorschrift nicht der „Insider“, sondern der in ein fremdes System Eindringende. Solange grundsätzlich ein Zugang zu den Daten gewährt wird, ist eine Zweckbindung der Zugangserlaubnis für die strafrechtliche Beurteilung unbeachtlich.“ […] „Ein strafbares Ausspähen von Daten kann nur stattfinden, wenn die Daten gegen unberechtigten Zugang besonders gesichert sind.“ LOERKE(2004), S. 20. Des Weiteren führt Frank Peter Schuster aus: „Auch bei dienstlichen Dateien erfolgt die unmittelbare Ausführung des Erstellens und Speicherns durch die Arbeitnehmer. Diese sind dabei allerdings den Weisungen des Arbeitgebers unterworfen; alle dienstlichen Vorgänge erfolgen auf seine Veranlassung. Deshalb wird man den Arbeitgeber als eigentlichen Urheber ansehen müssen; ihm ist der Skripturakt zuzurechnen.“ SCHUSTER(2010), S. 69. Ein Urteil aus München 2009 ergab: Der Missbrauch von Zugriffsrechten durch Administratoren bei vorherrschender Absicherung des IT-Systems rechtfertigt ohne vorherige Abmahnung durch den nicht wieder herzustellenden Vertrauensverlust die fristlose Kündigung. Vgl. Urteil des LAG München vom 08.07.2009 - 11 Sa 54/09.

Führungsfunktionen bzw. -personen des Unternehmens. Die Nutzung von Dienstleistern im Sinne einer Auftragsdatenverarbeitung kann allerdings zu strafrechtlichen Folgen führen. Softwareprodukte „zum Aufspüren von Sicherheitslücken sieht man nicht zwingend an, ob sein Zweck die Begehung einer solchen (Straf-) Tat ist.“ [16] In einem Missbrauchsfall wird es sicherlich zu einer zeitlich befristeten Verschärfung der Kontrollaktivitäten bzw. vielleicht sogar der stärkeren personellen Ressourcenausstattung der IT-Sicherheitsorganisation und des IT-Sicherheitsprodukteeinsatzes kommen. Detailvorgaben in Richtung Berechtigungskonzept werden aber folglich auch aus dem Strafgesetzbuch heraus nicht gemacht. Die Dokumentation des Willens, dass Daten abzusichern und Zugriffe zu reglementieren sind, ist nicht unwichtig. [17] Es ist jedoch nicht konkret ableitbar, z.B. Rollen, Berechtigungen und kritische Systemfunktionen in einer bestimmten Art und Weise auszuprägen und restriktiv Personen zuzuweisen bzw. auch nicht auszuprägen oder nicht zuzuweisen. Auch die Transparenzvorgaben aus dem Corporate Governance Kodex [18] – mit Verweis aus § 161 Aktiengesetz – sind nicht hilfreich [19]. Bei diesen geht es – als Empfehlungen und Anregungen formuliert – um Partizipations-, Prüf- und Transparenzvorgaben und -richtlinien hinsichtlich der Arbeit von Aufsichtsrat, Vorstand und Abschlussprüfer und deren Verhältnis zum Unternehmen.

Das Bundesdatenschutzgesetz (BDSG) findet über einen Sanktionskatalog nach §§ 43, 44 BDSG Wege, Unternehmen durch Prüfung der zuständigen Aufsichtsbehörde nach einem Verstoß oder aber auch nach Routineprüfungen der Verfahren gegen definierte Ordnungswidrigkeitstatbestände bzw. bei Vorsatz und „gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen“ [20] auch als Straftatbestand, mit „Strafzahlungen“ zu belegen, auch wenn diese nicht zwangsläufig zu einem Mehr an (IT-)Sicherheit führen müssen. Die Abdeckung von Formalismen wie z.B. das an bestimmte Rahmenbedingungen geknüpfte Vorhandensein und Bestellen eines betrieblichen Datenschutzbeauftragten, der Nachweis von Vorabkontrollen für bestimmte Verfahren (z.B. Videoaufzeichnung, häufig mit Erforderlichkeits- und Verhältnismäßigkeitsprüfung und -dokumentation als Erwägungsnachvollzug [21] des geringsten probaten Mitteleinsatzes) oder eine Prüf- und Dokumentationspflicht zu eingesetzten Dienstleistern (Auftragsdatenverarbeitung) im

---

[16] BITKOM(2008), S. 4.

[17] Interessant ist die Sichtweise „Durch § 202a StGB wird folglich nur der Dateninhaber geschützt, der nicht völlig sorglos mit seinen Daten umgeht. Durch die Einrichtung einer besonderen Zugriffssicherung muss er sein Interesse an einer Geheimhaltung der Daten dokumentieren.“ LOERKE(2004), S. 21.

[18] Vgl. DCGK(2013), o.S. zur Rollenwahrnehmung von Vorstand, Aufsichtsrat und Abschlussprüfer.

[19] § 161 AktG (Erklärung zum Corporate Governance Kodex): “(1) Vorstand und Aufsichtsrat der börsennotierten Gesellschaft erklären jährlich, dass den vom Bundesministerium der Justiz im amtlichen Teil des Bundesanzeigers bekannt gemachten Empfehlungen der „Regierungskommission Deutscher Corporate Governance Kodex“ entsprochen wurde und wird oder welche Empfehlungen nicht angewendet wurden oder werden und warum nicht. Gleiches gilt für Vorstand und Aufsichtsrat einer Gesellschaft, die ausschließlich andere Wertpapiere als Aktien zum Handel an einem organisierten Markt im Sinn des § 2 Abs. 5 des Wertpapierhandelsgesetzes ausgegeben hat und deren ausgegebene Aktien auf eigene Veranlassung über ein multilaterales Handelssystem im Sinn des § 2 Abs. 3 Satz 1 Nr. 8 des Wertpapierhandelsgesetzes gehandelt werden. (2) Die Erklärung ist auf der Internetseite […] dauerhaft öffentlich zugänglich zu machen.“

[20] § 44 Abs. 1 BDSG.

[21] Vgl. SCHOLZ, in: SIMITIS, BDSG, § 6b, Rn. 86-101.

Vorfeld einer Beauftragung und dann (undefiniert) regelmäßig wiederholend – durch die Novellierung des BDSG 2009 verschärft – ist denn auch vornehmlich das Ziel des BDSG an dieser Stelle. [22]

Der Gesetzgeber geht möglicherweise davon aus, dass bei Bekanntwerden eines Datenskandals der Imageschaden zu internen, qualitätserhöhenden Maßnahmen führt, dies ist aber aufgrund der Schnelllebigkeit von Nachrichten heute wohl kaum noch eine treibende Kraft.

Ein kausaler Zusammenhang zwischen seltener, gesetzlich geforderter Orientierung an Standards (z.B. nach BSI-Grundschutz [23] und den Herstellerverlautbarungen als „Soft Laws“) einerseits und dem tatsächlichen Umsetzungsstand in Unternehmen andererseits im Vergleich existiert ebenfalls nicht, ein unzureichendes „Matching“ im Untersuchungsfall ist kein sanktionsfähiger Tatbestand. Die wirtschaftliche Komponente spielt eine zu wichtige Rolle und kann vom Unternehmen immer als Karte ausgespielt werden. Auch die Diskussion um ein adäquates IT-Sicherheitsmanagement in Unternehmen, die zu kritischen Infrastrukturen zählen, führte nicht zu einer Beachtungsverpflichtung von Vorgaben z.B. des BSI. [24]

Es reicht insoweit, dass das Unternehmen im Bereich der IT-Sicherheit und auch der Berechtigungen als Teilaspekt die Aufgabenwahrnehmung definiert und darlegt, dass überhaupt Tätigkeit passiert. Häufig wird zwar hervorgebracht, dass „Vorstände und Geschäftsführer […] persönlich für Versäumnisse und mangelnde Risikovorsorge verantwortlich“ [25] sind, dies führt aber – auch im Sinne eines Organisationsverschuldens – bei Datenschutz- und Sicherheitsverstößen kaum zur persönlichen Haftung oder zu öffentlichkeitswirksamen Konsequenzen, wenn man vom gelegentlichen Jobverlust Einzelner aus vornehmlich politischen Erwägungen des Unternehmens heraus einmal absieht [26].

Es geht an dieser Stelle auch um eine vielbeschworene Panikmache, die nicht selten zur Aussage führt, dass ein beinahe uferloses IT-Risiko-Management gesetzliche Pflicht sei [27]. Es ist aber – und dies vor dem Hintergrund des steigenden Wettbewerbsdrucks als die gängige Begründung – in „der Praxis […] meistens schwierig, ein angemessenes Sicherheitsniveau zu erreichen und aufrecht zu erhalten. Die Gründe dafür sind vielfältig: fehlende Ressourcen, zu knappe Budgets und nicht zuletzt die steigende Komplexität der IT-Systeme.“ [28]

[22] Vgl. DATENSCHUTZ(2013), o.S., zum Ausspionieren von Beschäftigten im Aldi-Skandal.
[23] Vgl. RAHMEL(2007), S. 46ff.
[24] Vgl. KRITIS(2009), S. 13, zur Diskussion der IT-Risiken in kritischen Infrastrukturen.
[25] BSI(2012), S. 7.
[26] Vgl. BAHN(2009), o.S.
[27] Vgl. VONHOLLEBEN/WINTERS(2013), S. 16f., zur Maßnahmenableitung aus allgemeinen Pflichten.
[28] BSI(2012), S. 7.

Neben der Frage, wem Rechenschaft geschuldet wird, geht es also um die Frage der Intensität. Es reicht möglicherweise aus, Teile der IT-Sicherheits- und Datenschutzleitfäden der Hersteller oder anerkannter Institutionen umzusetzen. Eine Teilumsetzung dort, wo die Kosten als gering angenommen werden oder einplanbar sind, ein Ignorieren dort, wo erkennbar ist, dass erhebliche Kosten auf das Unternehmen zukommen – das ist ein durchaus probates Mittel, um Prüfinstanzen fernzuhalten, die aus Sicht des Unternehmens Kostentreiber sein können.

1.1 Problemstellung

Formulierungen in Gesetzen, Standards, Verlautbarungen und sicherheitsrelevanten Herstellerangaben sind nur dann als „scharfes Schwert“ zu sehen, wenn sie verbindlich und konkret in ihren Ansprüchen und Forderungen sind bzw. im Schadenfall auch von wertenden Instanzen als verbindlich zu befolgen angesehen werden. Ohne dies wird es auch in Zukunft zu Sicherheitsvorfällen – mit oder ohne Öffentlichkeitswirkung – ohne erkennbar am Schaden orientierte Konsequenzen für die Unternehmen oder für verantwortliche Personen kommen. Zur Organisation bzw. prozessualen Ausrichtung eines IT-Sicherheitsmanagements / -organisation im Unternehmen, ja sogar zur Gesamtausrichtung der unterschiedlichen Aufgaben der IT mit messbaren Steuerungsgrößen zur Risikominimierung im Kontext der Zielerreichung des Unternehmens, existieren nach DIN und ISO anerkannte und zertifizierbare Vorgehens-, Steuerungs- und Prüfmodelle, die allgemein formuliert Strukturelemente bereitstellen, die es erlauben, eine vergleichbare IT-Organisation mit allen Facetten auszugestalten. Die Frage steht aber im Raum, welche belastbaren Punkte sich aus Formulierungen ergeben, die Forderungen **im Detail der applikationsspezifischen Berechtigungsdefinition und -zuweisung mit entsprechenden „SoD“-Festlegungen** enthalten, die also folglich nicht ignoriert werden können. Auch diese sind ggf. interpretierbar, folgend ist aber eine Umsetzung nach „best practice“ [29] dann nicht abwendbar oder kann zumindest nicht vollumfänglich vernachlässigt werden.

Einzubeziehen ist dabei die betrieblich implementierte Funktion der Internen Revision als Überwachungsorgan der Unternehmensleitung und Teilaspekt des Internen Kontrollsystems und der Gewährleistung von Compliance – als durch die Unternehmensleitung geforderter Garant für Qualität und Aussagekraft vorhandener Kontrollaktivitäten. Die Aufgabenwahrnehmung erfolgt nach Vorgaben des Deutschen Instituts für Internen Revision e.V. (DIIR) und des „Institute of Internal Auditors“ (IIA), USA, die u.a. vorgeben, dass eine Interne Revision IT-Systeme risiko- und prozessorientiert [30] regelmäßig zu betrachten hat. Dies schließt auch den Aspekt des Berechtigungsmanagements ein.

---

[29] „Best practice“ soll nachfolgend definiert werden als von weitgehend fachkundigen Personen oder weithin anerkannten Institutionen bewährte, erprobte und begründete Methode, Interpretation und Sichtweise auf Detailaspekte im Bereich der technischen Ebene des Customizings von Zugriffsschutzdefinitionen in SAP-Systemen mit Herleitung technisch-juristischer Korrelationen, ohne dass diese in erster Linie justiziabel sind.

[30] Vgl. DIIR(2013), S. 35, 58.

Zusätzlich sind die Verlautbarungen und Prüfungsstandards der Wirtschaftsprüfer in Teilen wesentlich für die Arbeit der Internen Revision, denn hier werden mit Verweis auf handelsrechtliche Bestimmungen regelmäßig Vorgaben für den laufenden Betrieb rechnungslegungsrelevanter IT-Systeme kommuniziert. Speziell die Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie und von Archivierungssystemen gelten als essentiell, denn sie sind in großen Unternehmen immer vorhanden.

Die nachfolgende Arbeit versucht, über diese Frage anhand ausgesuchter Beispiele speziell zum Teilaspekt der Berechtigungsentwicklung, -steuerung und -zuweisung im rechnungslegungsrelevanten IT-Systemkomplex SAP ERP und speziell des SAP IS-U – ohne Beachtung der Betriebssystem- [31], Datenbank- [32] und Netzwerksicherheitsebene und vornehmlich mit Fokus auf Basis-Berechtigungen des ERP-Systems – Regelungsbedarf und Folgeabschätzungen für Unternehmen abzuleiten.

1.2 Aufbau der Arbeit

Die vorliegende Arbeit ist in fünf Bereiche aufgeteilt. Nach der Einleitung und Darlegung der Problemstellung in **Kapitel 1** werden zunächst in **Kapitel 2** die funktionalen Grundlagen, also die Bedeutung des Begriffs der Qualität, die auf SAP wirkenden Risiken und die Funktion der Internen Revision erläutert. In **Kapitel 3** werden exemplarisch die rechtlichen Grundlagen dargestellt, die auf Unternehmen der deutschen Energiewirtschaft wirken. **Kapitel 4** stellt wesentliche punktuell-kritische Aspekte des SAP-Berechtigungsmanagements unter Beachtung der zuvor besprochenen rechtlichen Grundlagen und ausgesuchte Besonderheiten des SAP IS-U dar. **Kapitel 5** offeriert eine abschließende Bewertung und ein Handlungsbedarf wird abgeleitet.

[31] Vgl. BSI(2013), M 4.257, S. 504.
[32] Zur Sicherheit auf der Datenbankebene: Vgl. z.B. auch HEIN(2002), o.S., auch BSI(2013), M4.269, S. 538.

2. Grundlagen

2.1 Die Funktion der Internen Revision

„Die Verantwortung für die Vermögenssicherung und für die Einhaltung der gesetzlichen Vorschriften liegt […] beim Vorstand oder bei der Geschäftsführung. Der Vorstand und die Geschäftsführung müssen ihre Organisationsverantwortung durch geeignete Überwachungsmaßnahmen (z.B. durch die Interne Revision) wahrnehmen.“ [33] Die Funktion der Internen Revision im Unternehmen kann als verlängerter Arm der Geschäftsführung gesehen werden, wenn es um die Aufgabenwahrnehmung der Überwachung der Organisation und eines ordnungsgemäßen Betriebs geht. Sie ist „Bestandteil des Internen Überwachungssystems.“ [34] Entsprechend gehört zum Aufgabengebiet „die Beurteilung der Effizienz und der Effektivität des Internen Kontrollsystems und die Prüfung und Beurteilung der Qualität, mit der die jeweiligen Aufgaben innerhalb des Unternehmens beachtet und erfüllt werden“. [35] Die Funktion und Aufgabenwahrnehmung der Internen Revision ist vom US-amerikanischen „Institute of Internal Auditors“ (IIA) definiert als: “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.“ [36] Das Deutsche Institut für Interne Revision (DIIR) stellt entsprechend heraus: “Die Interne Revision erbringt unabhängige und objektive Prüfungs- “assurance”- und Beratungsdienstleistungen, welche darauf ausgerichtet sind, Mehrwerte zu schaffen und die Geschäftsprozesse zu verbessern. Sie unterstützt die Organisation bei der Erreichung ihrer Ziele, indem sie mit einem systematischen und zielgerichteten Ansatz die Effektivität des Risikomanagements, der Kontrollen und der Führungs- und Überwachungsprozesse bewertet und diese verbessern hilft.“ [37] Sie unterstützt also die Geschäftsführung sicherzustellen, dass die Aufsichtsmaßnahmen getroffen und diese dauerhaft oder regelmäßig überprüft werden, „die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die den Inhaber treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist […], wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.“ [38] Aber diese Sicht reicht nicht aus, um das Aufgabenspektrum darzulegen, denn dieser Ansatz verkennt die Organisation und die Prozesssicht des Unternehmens. Die Interne Revision würde bei einem solchen Ansatz ausdrücklich nur eine Schutzschildfunktion ausüben gegenüber justiziablen Risiken und wäre somit zu stark mit der juristischen Beurteilung verkettet, dabei würde sie aber die Risiken des unternehmensgestalterischen

[33] LÜCK(2000), S. 6.
[34] LÜCK(2000), S. 1.
[35] LÜCK(2000), S. 1.
[36] LÜCK(2009), S. 20.
[37] DIIR(2012), S. 3.
[38] § 130 OWiG.

Organisationsprozesses und der systemunterstützenden Funktionen außerhalb der Betrachtung lassen. Abzugrenzen ist die Funktion des Controlling, das eine zumindest ähnliche Funktion darstellt, allerdings die zahlen- und wertorientierten Belange des Unternehmens im Fokus behält [39] und u.a. finanzorientiertes Forecasting [40], d.h. eine auf Nachhaltigkeit und Stabilität orientierte Finanzsicht, für das Unternehmen bereitstellt [41], ohne üblicherweise dabei Strukturen, Prozesse und die Aufgaben- und Verantwortungswahrnehmung durch explizite Prüfungstätigkeit in Frage zu stellen. Die Interne Revision hat ihre Ziele folglich im Bereich der Beurteilung der Ordnungsmäßigkeit, Zweckmäßigkeit und Angemessenheit, (Prozess-) Sicherheit und der Effizienz definierter Strukturen, Aktivitäten und Tätigkeiten der Unternehmensbereiche. [42] Man kann sie auch als unabhängig agierendes Inhouse-Consulting bezeichnen.[43] Auch das Risikomanagement ist Audit-Gegenstand der Internen Revision.[44] Sie nimmt darüber hinaus „die Funktion eines kritischen Gewissens im Unternehmen“ [45] mit der Notwendigkeit, fachlich fundiert zu argumentieren und zu dokumentieren, ein. Sie ist als interne Stelle oder Bereichsdefinition ausdrücklich bzw. üblich der Geschäftsleitung fachlich und disziplinarisch unterstellt und agiert auf deren Ansinnen hin, zielgerichtet Prüfungen, Beratungen und Projektbegleitungen durchzuführen. Die Interne Revision kann aber „aufgrund fehlender Anordnungs-befugnis nur eine Unterstützungsfunktion bei der Umsetzung von Verbesserungsvorschlägen übernehmen.“ [46] Sie ist also eher als prozessunabhängig zu bezeichnen. [47]

Die jährliche Aktivitätenplanung der Internen Revision erfolgt – ausgehend von einer immer stärkeren Bedeutung von Risikosichten in der Unternehmensleitung [48] – risikoorientiert [49], d.h. die Prozesse, Bereiche und Systeme werden nach Einschätzung der Revision in verschiedene Risikokategorien eingeteilt, beurteilt und in Beziehung gesetzt. [50] Zunächst erfolgt die Bindung von Kapazität für jährliche Pflichtprüfungen, dann die weitere Kapazitätsverteilung [51] auf Prüfgebiete der Prüflandkarte (Prüffelder des „Audit Universe“ [52]). In festgelegten Mehrjahresabständen (Mehrjahresplanung und Turnusbetrachtung) sollen folglich keine Prüffelder vorkommen, die noch nie geprüft wurden. [53]

---

[39] Vgl. FÜHRING(2009), S. 19, zum Verhältnis des Risikomanagements zur Unternehmens- und Risikokultur.
[40] Vgl. ANGELKORT/SANDT/WEIßENBERGER(2008), S. 6.
[41] Vgl. auch BECKER/BALTZER(2010), S. 13f., S. 18f.
[42] Vgl. LÜCK(2009), S. 19.
[43] Vgl. LÜCK(2000), S. 1.
[44] Vgl. MOHNIKE/EPKENHANS(2003), S. 9ff., zum Prüfungsvorgehen. Vgl. auch KREY(2001), S. 26f. Vgl. EULERICH/THEIS/VELTE/STIGLBAUER(2013), S. 59f., zum Modell „Three Lines of Defence“.
[45] LÜCK(2009), S. 19.
[46] HUNECKE(2003), S. 126.
[47] Vgl. LÜCK(2009), S. 19.
[48] Vgl. LÜCK(2000), S. 13.
[49] Vgl. MOHNIKE/EPKENHANS(2003), S. 11f.
[50] Vgl. WILDENSEE(2004), S. 34.
[51] Vgl. GEHRIG-EHRENZELLER(2011), S. 104f., zur Darlegung branchenspezifischer Personalressourcen.
[52] Vgl. WILDENSEE(2004), S. 34, zur Prüffelderdefinition und -bedeutung. Vgl. auch KREY(2001), S. 39.
[53] Vgl. WILDENSEE(2004), S. 35.

Es ist ersichtlich, dass die praxisnahe Beratung der Fachbereiche nicht unwesentlich an Aufmerksamkeit einnimmt. [54] Lück stellte bereits im Jahr 2000 heraus: „Der zunehmende Computereinsatz in den Unternehmen führt zu einer steigenden Komplexität der Prüfungsobjekte der Internen Revision. Die Vielzahl der Schnittstellen innerhalb der DV-Programme führt zu einer großen Komplexität des gesamten DV-Systems.“ [55] Dies bedeutet, dass die Interne Revision sowohl bei der Einführung, dem Customizing und der Änderung von unternehmensprozess- und funktionsunterstützenden Systemen als auch bei der Definition von Prozessen, der Betrachtung von Schnittstellenaspekten und dem übergeordneten Zusammenspiel der Fachbereiche und ihrer Prozesse im Sinne der Unternehmensziele Mehrwert schaffende Sichtweisen und Methodenansätze einbringt, „ohne dabei in den Prozessen des Unternehmens beteiligt zu sein.“ [56] Sie unterbreitet den geprüften und zuständigen Fachbereichen sowohl bei Prüfungen als auch bei Beratungen Empfehlungen, um identifizierte Schwachstellen zu beheben oder zumindest in ihrer Wirkung zu reduzieren, wenn denn eine Behebung nicht stattfinden kann oder soll. [57] Dabei stellt sie „die Realisierbarkeit in den Mittelpunkt – so berücksichtigt sie unternehmensspezifische Gegebenheiten im Allgemeinen sinnvoller, d.h. prozessnäher, während hier der Einbezug außerbetrieblicher Erfahrungen problematisch ist“. [58]
Zu sehen ist auch, dass die Interne Revision ein Gespür für Machbarkeit / Durchsetzbarkeit entwickeln muss, denn nicht immer werden unternehmerische Entscheidungen rational getroffen. Dies führt zu steigenden Anforderungen an den Leiter der Internen Revision, der neben einer fundierten Unternehmens- und Branchen- / Marktsicht die Strömungen im Unternehmen und speziell der Unternehmensleitung und der nächst tieferen Unternehmenshierarchieebene erkennen oder auch nur erahnen muss. Das Standing der Internen Revision steht und fällt mit der Akzeptanz des Leiters in diesen Ebenen. Steigende Anforderungen ergeben sich auch für die Revisionsbeschäftigten, u.a. im Bereich der Vorgehensmethodik, der IT-Systemkenntnisse (auch durchaus in speziellen Applikationen [wie z.B. bei Handelssystemen] und wesentlichen Anwendungen zur Abbildung des unternehmensweiten Ressourceneinsatzes), der Prozessmodellierung und der IT-Security. [59] Die Interne Revision verfügt über dokumentierte Berufsstandards und eine vorgegebene Berufsethik [60].

Ein wesentliches Element aktiver Revisionsarbeit ist ein üblicherweise uneingeschränktes aktives und passives Informationsrecht, d.h. sie kann in alle Unterlagen des Unternehmens Einblick nehmen, ebenso sind ihr wesentliche Unterlagen und Informationen, z.B. bei Veränderungen in der Organisation, den Prozessen, definierten IKS-Maßnahmen, in bestehenden Regelungen usw., proaktiv von verantwortlichen Stellen zur Verfügung zu stellen. [61]

---

[54] Vgl. z.B. GEHRIG-EHRENZELLER(2011), S. 106.
[55] LÜCK(2000), S. 11.
[56] GEHRIG-EHRENZELLER(2011), S. 99.
[57] Vgl. BARTA/GILLER/MILLA(2008), S. 219, zu mitigierenden (/ kompensierenden) Kontrollen.
[58] WILDENSEE(2004), S. 38.
[59] Vgl. auch BSI(2010), S. 23.
[60] Vgl. LÜCK(2009), S. 21ff., S. 40ff.
[61] Vgl. BSI(2010), S. 22.

Zuletzt ist die Interne Revision beteiligt an der Herstellung unternehmensinterner oder konzernweit gültiger Regelungen, tritt im Rahmen ihrer Nachweispflichten im „Audit Committee“ auf [62], sofern ein solches existiert, und auch die Sachverhaltsermittlung im Falle des dolosen Vorgehens von Beschäftigten gegen bestehende interne und externe / gesetzliche Regelungen gehört zu den Aufgaben. In diesem Zusammenhang nimmt sie die Funktion einer zentralen Koordinationsstelle in Richtung externer Anspruchsberechtigter ein, z.B. zur Kommunikation mit der Polizei und Staatsanwaltschaft. Gehrig-Ehrenzeller stellt denn auch das wesentliche Problem moderner Revisionsabteilungen heraus: „Eine Gefahr besteht durch die zunehmenden Anforderungen der vielen Regulierungen an das interne Kontrollsystem, dass die Interne Revision ihren Fokus zu stark auf Dokumentationsfragen legt und ihre Ressourcen weniger für unentdeckte, signifikante Risiken einsetzt.“ [63]

2.2 Spezialisierte Revision im Bereich der Informationsverarbeitung und ihre Aufgaben

In vielen Unternehmen der Energiewirtschaft existiert keine spezialisierte Revision mit dem Prüfungsschwerpunkt auf die Risiken der IT-Systeme und -Prozesse. Vielmehr werden diese Aufgaben häufig von IT-affinen kaufmännischen oder technischen Prüfer/-innen erledigt. Nicht selten ist auch die Leitungsebene mit diesen Inhalten wenig vertraut, so dass hier eine Betrachtungslücke entsteht und Prüfungen nur punktuell nach Priorität der prüfend Beschäftigten erfolgen. „Zentraler Gegenstand einer IT-Revision war in der Vergangenheit primär die Prüfung der IT-gestützten Buchführungssysteme. Diese Sichtweise wird heutzutage nicht mehr vertreten, da erkannt wurde, dass heutige Systeme stark vernetzt sind und viele Abhängigkeiten zwischen Systemen und Geschäftsprozessen existieren Daher wird inzwischen bei einer IT-Revision […] die gesamte IT-Infrastruktur einer Institution betrachtet.“ [64] Nach BSI stehen bei der klassischen IT-Revision „die drei Prüfkriterien Wirtschaftlichkeit (IT-Prozess, IT-Organisation, Sicherheitsmaßnahmen), Sicherheit und Ordnungsmäßigkeit (Einhaltung von Rechnungslegungsgrundsätzen wie Vollständigkeit, Richtigkeit, Zeitgerechtigkeit, Nachvollziehbarkeit, Ordnung) gleichwertig nebeneinander Die Gewichtung dieser drei Ziele bestimmt individuell die Institution bzw. der Revisor und ist abhängig von der Unternehmens- […] strategie sowie dem konkreten Prüfauftrag.“ [65] Die Weiterentwicklung der IT-Revision ist aus Sicht des BSI die Informationssicherheits-(IS-)Revision. „Die IS-Revision hingegen als „neue” Disziplin der Revision, legt den Schwerpunkt auf die ganzheitliche Prüfung der Informationssicherheit. Das bedeutet, dass hier vom Aufbau einer Informationssicherheitsorganisation über Personalaspekte bis zur Konfiguration von Systemen alle Ebenen geprüft werden. Die Prüfungskriterien Wirtschaftlichkeit und Ordnungsmäßigkeit werden nachrangig betrachtet. Die

[62] Vgl. GEHRIG-EHRENZELLER(2011), S. 106f.
[63] GEHRIG-EHRENZELLER(2011), S. 107.
[64] BSI(2010), S. 9f.
[65] BSI(2010), S. 10.

Sicherheit (einschließlich die Angemessenheit der Sicherheitsmaßnahmen) ist somit das wesentliche Prüfkriterium der IS-Revision.“ [66] So stellt das BSI auch fest: „Das Ziel einer IS-Revision ist es, das aktuelle Sicherheitsniveau innerhalb der Institution durch eine unabhängige Instanz festzustellen und Hinweise zu bestehenden Sicherheitslücken und -mängeln zu geben. Die IS-Revision ist ein Spezialfall der (allgemeinen) Revision. Ergebnis ist ein IS-Revisionsbericht mit Empfehlungen zur Verbesserung der Informationssicherheit.“ [67] Bedeutsam ist dabei, „dass die Prüfer, die eine IS-Revision durchführen, nicht unmittelbar bei der Konzeption, Entwicklung und Umsetzung der Maßnahmen zum untersuchten Objekt beteiligt waren.“ [68]

Dies führt wie oben erwähnt zu erheblich höheren Anforderungen an die Kompetenz der Prüfungsteams, als dies noch vor Jahren der Fall war und schlägt sich auch auf die Entlohnung nieder.[69] Dies ist naheliegend, denn sowohl der Ausbildungsstand als auch die Erfahrungen von Beschäftigten der Revision mit diesem Schwerpunkt im Umgang und in der Tiefe der IT-Systeme sind nur teuer am Markt zu substituieren. Beschäftigte aus dem Beratungsumfeld der IT-Produkte finden ebenfalls den Weg in das Audit-Umfeld großer Unternehmen und können dort mit ihren Produkt- und Technologieschwerpunkten häufig hohe Gehälter verhandeln. Insbesondere der produktspezifische Security-Aspekt, gepaart mit Methodenwissen auch aus dem Projektmanagement, ist eine begehrte Kombination.

„Die Hauptaufgabe der IS-Revision ist es, das Management […] und insbesondere den IT-Sicherheitsbeauftragten bei der Umsetzung und Optimierung der Informationssicherheit zu unterstützen und zu begleiten. Die Prüfungstätigkeit zielt darauf ab, die Informationssicherheit zu verbessern, Fehlentwicklungen auf diesem Gebiet zu vermeiden und die Wirtschaftlichkeit der Sicherheitsmaßnahmen und der Sicherheitsprozesse zu optimieren. Dies sichert die Handlungsfähigkeit, das Ansehen und die Vermögenswerte (Assets) der Institution.“ [70] Dies ist allerdings zu kurz gefasst, denn letztlich geht es auch darum, die verantwortlichen Bereiche für IT-Planung, IT-Bereitstellung, die Entwicklung und den Betrieb zu sensibilisieren und die Ordnungsmäßigkeit [71], die vor dem Hintergrund zunehmenden Regulation nach wie vor wichtig ist, im Blick zu behalten und regelmäßig punktuell auf Regularieneinhaltung zu auditieren. Dies betrifft insbesondere z.B. systemkritische Zustände des Customizings, die Kommunikationsmöglichkeiten und realisierten Schnittstellen zu anderen Systemen, das Change-Management, aber auch SoD-Konflikte und bekannte und anerkannte Sicherheitsaspekte der Anwendung wie vom Hersteller implementierte Funktionsfehler, Möglichkeiten der Eigenentwicklung, Nachvollzugs- und Protokollierungsaspekte, das Notfall-

[66] BSI(2010), S. 10.
[67] BSI(2010), S. 11.
[68] BSI(2010), S. 16.
[69] Vgl. GEHRIG-EHRENZELLER(2011), S. 102.
[70] BSI(2010), S. 7.
[71] Vgl. auch RÜTER/SCHRÖDER/GÖLDNER/NIEBUHR(2010), S. 214.

management, Automatisierungsmöglichkeiten, Belange der Wiederanlauf-Szenarien usw. [72] So ist der Ansatz, den Revisionsschwerpunkt auf technologische Belange zu reduzieren, ebenso unzutreffend wie die Sicherheitsbelange in den Vordergrund zu stellen. Insoweit ist eher für den Begriff der Informationsverarbeitungs-(IV-)Revision zu plädieren. Wenn nachfolgend von Interner Revision im Kontext dieser speziellen Fragestellungen gesprochen wird, ist die Aufgabenwahrnehmung der IV-Revision gemeint. Trotzdem wird die Begrifflichkeit der IT-Revision auch synonym verwendet. Die Analyse von applikationsspezifischen Berechtigungskonzepten auf Regularienkonformität ist nur ein kleiner Ausschnitt des Aufgabenspektrums.

2.3 SAP-Risiken

„Risiken stellen aus Sicht des Unternehmens grundsätzlich eine Aggregation vorhandener, vornehmlich monetär bewertbarer Faktoren dar, die auf die Ertragskraft und Handlungsfähigkeit des Unternehmens wirken – sowohl im Kerngeschäft als auch bei Innovationsprozessen im Sinne der Auswirkung einer Chance. Dabei spielt die Schadenhöhe und die Eintrittswahrscheinlichkeit eine entscheidende Rolle (Einbezug von mathematischen Bewertungsmethoden). Häufig wird nicht das Risiko selbst definiert, sondern auf eine Beschreibung der charakteristischen Risikoeigenschaften und deren Wirkung zurückgegriffen“. [73] Als Risiko wird auch der mangelnde Informationszustand gesehen. [74] „Die Risikoorientierung führt zu einer Strategie der Prüfung der wesentlichen Risikobereiche des Unternehmens. Risikoorientierung heißt in diesem Kontext: Ausrichtung von Prüfungsgegenstand und -umfang an den Fehlerquellen des Unternehmens […]“ [75] Die SAP-Systeme sind wesentliche IT-Systeme des Unternehmens, denn sie bilden die monetär bewerteten Werteflüsse und Ressourceneinsätze ab. Risiken ergeben sich aber nicht aus der Berechtigungssteuerung heraus. „Ein dokumentiertes Berechtigungskonzept beinhaltet […] meist lediglich Regelungen, die die Vergabe und Verwaltung von Berechtigungen betreffen. Dies ist jedoch beim Betrieb eines solch umfassenden DV-Konstrukts nicht ausreichend, um Revisionsstandards zu erfüllen. Notwendig ist eine Zusammenführung von Regelungen, die den gesamten Life-Cycle des SAP-Systems und aller Komponenten dokumentiert, um den Betrieb nachvollziehbar, nachhaltig und mit Soll-Vorgaben zu gewährleisten.“ [76] Entsprechend umfangreich ist die im Unternehmen zu implementierende Rahmengebung im Bereich der SAP-Risikobetrachtung. [77] Um zunächst relevante Risiken zu benennen, aber auch eine Eingrenzung vornehmen zu können über Risiken, die in der vorliegenden Arbeit nicht betrachtet werden sollen, muss der Betrachtungshorizont abgesteckt werden.

---

[72] Vgl. auch RÜTER/SCHRÖDER/GÖLDNER/NIEBUHR(2010), S. 123.
[73] WILDENSEE(2004), S. 34.
[74] Vgl. KREY(2001), S. 33, 35.
[75] KREY(2001), S. 41.
[76] WILDENSEE(2003c), S. 25.
[77] Vgl. WILDENSEE(2003c), S. 26ff.