Ontologiebasierte Integration von Informations- und unternehmensweitem Risikomanagement. Motivation, Grundlagen, Vorgehen und erste Ergebnisse

Patrick Wolf, Matthias Goeken

Frankfurt School of Finance & Management
p.wolf | m.goeken@fs.de

Abstract: Das unternehmensweite Risikomanagement ist ein komplexer Aufgabenbereich, der in Unternehmen vielfach auf verschiedene Schultern verteilt ist. Aus dieser Aufgabenteilung erwächst die Herausforderung, die vorhandenen Risikoinformationen zu einem zutreffenden Bild der Gesamtrisikosituation zu integrieren. Ein geeignetes Hilfsmittel stellen Ontologien dar. Wie festzustellen ist, mangelt es aber an solchen Ontologien zur Unterstützung der Integration des unternehmensweiten Risikomanagements und seiner Teilsysteme. Der Beitrag präsentiert eine Methode zur Adressierung dieser Forschungslücke sowie erste Ergebnisse. Kern der Methode ist das Konzept stilisierter Fakten zur systematischen und nachvollziehbaren Generierung der Ontologieinhalte.

1 Einführung

Jede unternehmerische Tätigkeit ist in Anbetracht der Unsicherheit der Zukunft mit Risiken verbunden [COSO04] [IDW99] [ISO09]. Die Erkennung der Risiken und der angemessene Umgang mit ihnen ist eine inhaltlich und organisatorisch komplexe unternehmerische Aufgabe, die zum Teil ein hohes Maß an Spezialisierung im Vorgehen und den eingesetzten Methoden erfordert [St07] [Wi04] [Wo03]. Sie wird daher häufig von verschiedenen Aufgabenträgern mit jeweils unterschiedlichen inhaltlichen Schwerpunkten verantwortet (so z.B. Finanzrisiken durch die Finanzabteilung und Informationsrisiken durch die IT-Abteilung). Aus der Aufgabenteilung erwachsen die Herausforderungen, die verteilte Aufgabendurchführung zu koordinieren und die entstehenden Informationen zusammenzuführen, um ein zutreffendes Bild der Gesamtrisikosituation zu erhalten und Wechselwirkungen zwischen Risiken analysieren zu können.

Hiervon ausgehend betrachtet der Beitrag die Informationsintegration von unternehmensweitem Risikomanagement und Informationsrisikomanagement. Es wird angenommen, dass beide Systeme in starker gegenseitiger Abhängigkeit stehen und ihre jeweiligen Aufgaben nur dann wirksam erfüllen können, wenn die untereinander ausgetauschten Informationen vollständig sind und auf Basis einer einheitlichen Semantik interpretiert werden. Ontologien werden in diesem Zusammenhang als geeignetes Mittel zur expliziten Definition der Semantik der Informationsinhalte angesehen. Weil in der Literatur weder fundierte Ontologien zu den einzelnen Teilsystemen noch zur Informationsschnittstellen zwischen diesen existieren, wird eine Forschungslücke attestiert und eine Methode vorgestellt, um solche zu konstruieren. Deren Besonderheit ist die Ver-

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

wendung von „stilisierten Fakten“ zur Unterstützung der systematischen Wissensgewinnung. Der Einsatz der Methode wird damit begründet, dass umfangreiche Aussagen zum Informations- und unternehmensweitem Risikomanagement in Standards, Best-Practice-Referenzmodellen und wissenschaftlichen Veröffentlichungen vorliegen, die im Regelfall unsystematisch nebeneinander stehen. Mit Hilfe der Methode stilisierter Fakten sollen die durch Einzelaussagen breit gestützten Konzepte, Konzepteigenschaften und Konzeptbeziehungen des Informations- und unternehmensweiten Risikomanagements herausgearbeitet und die Ontologie somit fundiert werden.

Der Beitrag ist wie folgt strukturiert: Im zweiten Kapitel werden zunächst die grundlegenden Begriffe erörtert und der Einsatz von Ontologien zur Informationsintegration von Informations- und unternehmensweiten Risikomanagement diskutiert. Das dritte Kapitel diskutiert verwandte Arbeiten und stellt die Forschungslücke dar. Das vierte Kapitel präsentiert ein Vorgehen zur Ontologiekonstruktion. Im fünften Kapital werden Ergebnisse der Methodenanwendung vorgestellt. Fazit und Ausblick runden den Beitrag ab.

2 Grundlagen

Unter *Risiken* werden hier mögliche Ereignisse verstanden, die im Falle ihres Eintritts zu einer Abweichung von realisierten und geplanten Ergebnissen führen können [COSO04] [ISO09] [Wi04] [Wo03]. Die Abweichung kann positiver (Übererfüllung des Ziels) wie auch negativer Natur (Untererfüllung des Ziels) sein [COSO04] [ISO09]. Da Risiken grundsätzlich in allen Unternehmensbereichen (z.B. Tochtergesellschaften, Beteiligungen etc.) auftreten können und in der Regel vielschichtiger Natur sind (z.B. Finanz-/Informationsrisiken), besitzt das Risikomanagementsystem eines Unternehmens eine hohe Komplexität [IDW99] [ISO09]. Dieser Komplexität wird zumeist durch Zerlegung des Gesamtsystems in verschiedene Teilsysteme begegnet. Beispiele hierfür sind das Finanz- oder das Informationsrisikomanagement [St07]. Teilsysteme betrachteten jeweils bestimmte Risikoarten, was eine Spezialisierung von Methoden und Know-how und eine umfassendere Auseinandersetzung mit den betrachteten Risikoarten ermöglicht.

Die Koordination der Teilsysteme und ihrer Ergebnisse obliegt dem unternehmensweiten Risikomanagement [COSO04]. Hier fließen alle wesentlichen Risikoinformationen aus den Teilsystemen zusammen, werden übergreifend analysiert und bereinigt (z.B. Eliminierung von Dubletten), unter Berücksichtigung ihrer Wechselwirkungen aggregiert und an die relevanten internen bzw. externen Stakeholder kommuniziert (z.B. Unternehmensleitung, Kontrollorgan, Eigentümer). Weiterhin stellt es seinen Teilsystemen relevante Informationen u.a. zu erkannten Inkonsistenzen oder neu erkannte Risiken bereit. Der Fokus wird im Folgenden auf das Zusammenspiel Informations- (IRM) und unternehmensweiten Risikomanagement (URM) gelegt: Das IRM betrachtet die Risiken des betrieblichen Informationssystems und soll sicherstellen, dass dessen Wirtschaftlichkeit, Wirksamkeit und Angemessenheit nicht durch den Eintritt von Risiken beeinträchtigt und die Erreichung der Unternehmensziele damit gefährdet wird [Ju05].

Damit URM und IRM wirksam zusammenarbeiten können, müssen zwei wesentliche Anforderungen erfüllt sein: Einerseits ist die Informationsschnittstelle zwischen den

Systemen so zu gestalten, dass die ausgetauschten Informationen vollständig sind. Dies setzt bei der Schnittstellengestaltung Wissen darüber voraus, welche Informationen von den Systemen zur Erfüllung ihres Systemzwecks benötigt werden und welche davon das andere System infolge der Aufgabenteilung bereitstellen muss. Andererseits muss sichergestellt werden, dass die ausgetauschten Informationen von beiden Systemen inhaltlich gleich interpretiert werden. Da jedes der Systeme ein eigenes, am jeweiligen Systemzweck ausgerichtetes Informationsmodell besitzt, ist zusätzlich ein gemeinsames Informationsmodell erforderlich, das als Brücke zwischen beiden Systemen fungiert.

Als geeignetes Mittel zur Unterstützung der Informationsintegration zwischen Systemen und somit zur Erfüllung obiger Anforderungen werden in Anlehnung an [MM03] Ontologien angesehen. Eine Ontologie wird in der Literatur häufig nach [Gr93] als "an explicit specification of a conceptualization" angesehen. Häufig wird gefordert, dass eine gemeinsame und geteilte Konzeptualisierung („shared“) wiedergegeben wird [Gu09]. Diese ist eine für die Ontologiezwecke abstrahierte, vereinfachte Sicht auf einen bestimmten Gegenstandsbereich (z.B. IRM oder URM) [MM03] [Us96]. Mit expliziter Spezifikation ist in diesem Beitrag sowohl die semiformale Darstellung der relevanten Konzepte, Konzepteigenschaften und Konzeptbeziehungen von IRM und URM als auch die semiformale Darstellung der aus den Einzelontologien abgeleiteten, integrierten Konzepte, Konzepteigenschaften und Konzeptbeziehungen gemeint.

Die integrierte Ontologie soll in der Praxis als Referenz dienen, um eine bessere Integration von IRM und URM zu ermöglichen. Nach Analyse der Autoren existiert eine solche integrierte Ontologie bislang in der Literatur nicht (siehe Abschnitt 3). Dass aber in Bezug auf die Integration der beiden Teilsysteme Handlungsbedarf besteht, zeigt u.a. eine Studie von [JK04]. Auch das von der ISACA veröffentlichte RiskIT-Referenzmodell betont die Bedeutung einer wirksamen Integration [ISACA09].

Neben den beiden oben genannten allgemeinen Anforderungen sollen die betrachteten Ontologien folgende spezifischer Anforderungen erfüllen: (A1) Angemessene Fundierung der Ontologieelemente. Sämtliche Elemente der Ontologien (Konzepte, Konzepteigenschaften und Konzeptbeziehungen) sollen auf nachvollziehbaren Aussagen in relevanten Wissensquellen (z.B. Standards, wissenschaftlichen Veröffentlichungen, Best-Practice-Referenzmodellen) basieren, sofern vorhanden. Die Aussagen und daraus abgeleitete Folgerungen für die Ontologien sollen offengelegt werden. (A2) – Offenlegung widersprüchlicher Elementeaussagen. Sofern die Aussagen verschiedener Wissensquellen zu einem Ontologieelement in Widerspruch zueinander stehen, soll der Widerspruch offengelegt und angemessen gehandhabt werden. (A3) – Relevanz der Ontologieelemente. Die Elemente einer Ontologie sollen für die Erfüllung des jeweiligen Ontologiezwecks relevant sein. (A4) – Angemessene Spezifität der Ontologieelemente. Die Ontologieelemente sollen inhaltlich ausreichend spezifisch sein, damit sie die Erfüllung des jeweiligen Ontologiezwecks unterstützen. Im Folgenden werden insbesondere die Anforderungen A1 und A2 im Zusammenhang mit verwandten Arbeiten zum Themenbereich modell-/ontologiebasiertes Risikomanagement betrachtet.

ISBN 978-3-88579-286-4

3 Diskussion verwandter Arbeiten

In Bezug auf das *URM* existieren zahlreiche Standards, Best-Practice-Referenzmodelle und wissenschaftliche Veröffentlichungen. Sowohl Standards, wie z.B. ISO 31000:2009 oder IDW PS 340, als auch Best-Practice-Referenzmodelle, wie z.B. COSO ERM, beinhalten ausschließlich rein natürlich-sprachige Darstellungen, die Aussagen über Konzepte, Konzepteigenschaften und Konzeptbeziehungen des Risikomanagements treffen. Semi-formale oder formale Modelle konnten hingegen nicht identifiziert werden. Bei einzelnen Arbeiten, wie z.B. IDW PS 340, ist zum Verständnis des konzeptuellen Modells eine zeitintensive Analyse aller Einzelaussagen erforderlich; andere Arbeiten, wie ISO 31000 und COSO ERM, bieten ein Glossar, das wesentliche Konzepte auf einen Blick darstellt. Konzeptbeziehungen und -eigenschaften werden hier aber nur teilweise offengelegt. So stellt sich bzgl. ISO 31.000 beispielsweise die Frage, in welcher Beziehung die Konzepte "event", "risk" und "risk source" genau stehen.

In wissenschaftlichen Veröffentlichungen zum *URM*, die der BWL zuzuordnen sind, wie z.B. [St07], [Wi04], [Wo03] bietet sich ein vergleichbares Bild. Sie enthalten weitgehend natürlich-sprachige Modelle. Die Herausarbeitung der Modelle ist im Regelfall ein zeitaufwändiges Unterfangen, das einer Reihe von Interpretationen bedarf, da relevante Konzeptbeziehungen nicht immer explizit und konsistent erläutert sind. Als wissenschaftliche Veröffentlichungen zum URM, die der Wirtschaftsinformatik zuzuordnen sind, konnten mit [Si07] und [MR05] zwei stärker formalisierte konzeptuelle Modelle mit Bezug zum Risikomanagement identifiziert werden. [Si07] jedoch machen den Entstehungsprozess des Modells nicht transparent, da sie nicht auf ihre Literaturanalyse eingehen. Weiter explizieren sie ausschließlich den Gegenstandsbereich des Risikomanagementsystems und lassen andere RM-Elemente, wie z.B. die RM-Strategie, die Risikokultur oder RM-Aktivitäten, außer Acht. Zusätzlich ist das Modell nicht modular aufgebaut: Alle 27 Konzepte werden mitsamt ihrer vielfältigen Beziehungen auf der gleichen Ebene dargestellt. Dies wirkt sich negativ auf die Klarheit des Modells aus. In [MR05] präsentieren die Autoren ein konzeptuelles Risikomodell, das die Integration von Risikosachverhalten in Geschäftsprozessmodelle unterstützen soll. Somit scheint ebenfalls der Gegenstandsbereich zu begrenzt. Die dargestellten Konzepte und Beziehungen werden argumentativ begründet; eine weitergehende Fundierung durch Literaturaussagen und der Hinweis auf etwaige Widersprüche in der Literatur fehlen.

Insgesamt kann festgehalten werden, dass es an semi-formalen bzw. stärker formalisierten Modellen (Ontologien) mangelt, die die in 2 genannten Anforderungen erfüllen.

Auch zum Thema *IRM* sind zahlreiche Standards (z.B. ISO/IEC 27000 Serie, ISO/IEC 13335), Best-Practice-Referenzmodelle (z.B. RiskIT) und wissenschaftliche Veröffentlichungen (z.B. [Ju05], [WH07], [Pr08], [In09]), vorhanden. In der Vergangenheit fokussierte sich das Interesse hier insbesondere auf Risiken der Informationssicherheit [Ju05] [SHF10]. Das IRM wurde primär als eine technische, sicherheitszentrierte Aufgabe verstanden. Demzufolge wurden eher die kurzfristigen Auswirkungen von sicherheitsbezogenen Informationsrisiken auf die Grundwerte (z.B. Vertraulichkeit, Integrität, Verfügbarkeit) von wesentlichen Vermögenswerten (z.B. Informationen, IT-Systeme, IT-Infrastruktur) betrachtet [Ju05] [SHF10] [Pr08]. Andere Informationsrisiken (z.B. in

Bezug auf Qualität, Compliance, Agilität) und deren mittel- bis langfristigen Implikationen für die Unternehmensstrategie oder für die Wirksamkeit und Effizienz von Geschäftsprozessen wurde hingegen weniger Aufmerksamkeit geschenkt [SHF10] [In09]. Erst seit einigen Jahren ist ein Wandel festzustellen: Eine zunehmende Anzahl von Veröffentlichungen (z.B. [Ju05], [SHF10], [WH07], [ISACA09]) betont die Notwendigkeit einer ganzheitlichen und geschäftsbezogenen Betrachtung von Informationsrisiken.

Konzeptuelle Modelle und (stärker formalisierte) Ontologien lassen sich aufgrund der geschilderten Entwicklungen vor allem im Bereich der Informationssicherheit identifizieren. Ein systematischer Vergleich von existierenden Sicherheits-Ontologien findet sich beispielsweise bei [Bl08]. Allerdings besitzen die Ontologien einen für den hier verfolgten Zweck zu stark beschränkten Fokus.

Außerhalb des Bereichs der Informationssicherheit finden sich u.a. in den Arbeiten von [SHF10] und [ISACA09] konzeptuelle Modelle, die auf einem breiteren Verständnis von Informationsrisiken basieren. Im Hinblick auf [ISACA09] ist erneut die weitgehend natürlich-sprachige Darstellung des zugrunde liegenden konzeptuellen Modells zu kritisieren. Konzepte, Konzeptbeziehungen und Konzepteigenschaften müssen aus den Einzelaussagen mühsam extrahiert werden. In [SHF10] ist eine solche semi-formale Darstellung zwar enthalten, allerdings ist der Modellzweck auf die Abbildung des Gegenstandsbereichs des IRM für die Zwecke einer Modellierungsmethode eingeschränkt. Nicht dargestellt werden bspw. relevante kontextuelle Konzepte wie die IRM-Strategie, die Risikokultur oder die Organisationsstruktur und auch der Gegenstandsbereich erscheint nicht vollständig modelliert (z.B. fehlen Risikoindikatoren oder Möglichkeiten zur Unterscheidung von geplanten und realisierten Maßnahmen). Weiterhin werden die den Modellelementen zugrunde liegende Fundierung und der in der Literatur bestehende Konsens bzgl. der Interpretation der Modellelemente nur eingeschränkt offengelegt.

Als Ergebnis der Literaturauswertungen erscheint es gerechtfertigt, auch für das IRM einen Mangel an semi-formalen bzw. stärker formalisierten Modellen zu konstatieren.

Während zu URM und IRM zahlreiche Veröffentlichungen identifiziert werden konnten, stellt sich dieses bezüglich der *Integration* beider anders dar: Hier waren keine Veröffentlichungen auffindbar, weshalb die Thematik im wissenschaftlichen Schrifttum bislang nicht angemessen behandelt zu sein scheint. Im folgenden Abschnitt wird eine Forschungsmethode zur Adressierung dieser Lücke zur Diskussion gestellt.

4 Konstruktion einer integrierten Ontologie: Vorgehensmodell und stilisierten Fakten zur Wissensgewinnung

Zur Unterstützung der systematischen Entwicklung von Ontologien existieren in der Literatur verschiedene Vorgehensmodelle und Methoden. Übersichten finden sich u.a. bei [CFG03] und [FG02]. Als Basis für dieses Vorhaben wurde das „Methontology“ Framework [FGJ97] [Lo99] ausgewählt, da es von den verfügbaren als das ausgereifteste gilt [FGJ97]. Es unterscheidet Management-, Entwicklungs- und Unterstützungsaktivitäten [FGJ97] [FG02]. Aufgrund ihrer Relevanz stehen hier letztere im Fokus.

ISBN 978-3-88579-286-4

Die Entwicklungsaktivitäten von Methontology nehmen eine grundsätzliche Ontologiespezifikation vor und dienen der schrittweisen Formalisierung des Domänenwissens. Als Unterstützungsaktivitäten gelten die Wissensgewinnung, Integration, Evaluierung, Dokumentation und das Konfigurationsmanagement. Im Folgenden wird insbesondere die Aktivität "Wissensgewinnung" betrachtet, die von besonderer Bedeutung für die vorliegende Fragestellung ist: In ihr findet die auf den Ontologiezweck gerichtete Auswertung der in der Ontologie-Spezifikation festgelegten Wissensquellen (z.B. Standards, Best-Practice-Referenzmodelle) statt, um bedeutsame Konzepte, Konzeptbeziehungen und Konzepteigenschaften zu identifizieren. Die Wissensextraktion kann unterschiedlich erfolgen. An dieser Stelle wird die Methode stilisierter Fakten verwendet, die geeignet ist, große Mengen natürlich-sprachige Aussagen systematisch auszuwerten und breit gestützte Konzepte, Konzeptbeziehungen und Konzepteigenschaften zu identifizieren.

Da Ontologien eine geteilte Konzeptualisierung abbilden sollen, wird hier die Ansicht vertreten, dass Anwender die Qualität einer Ontologie umso höher einschätzen, je umfassender ihre Inhalte durch nachvollziehbare Aussagen von Domänenexperten gestützt sind und je mehr die Anwender der Fundiertheit dieser Aussagen vertrauen. Die Methode stilisierter Fakten wird in diesem Zusammenhang als geeignetes Mittel angesehen, um die auf verschiedene Quellen verteilen Aussagen unabhängiger Domänenexperten systematisch zu sammeln und sie unter Vernachlässigung einzelner Details zu einer gemeinsamen Sicht zu integrieren. Anders ausgedrückt "konzentriert sich [die Methode stilisierter Fakten] auf allgemeine Tendenzen [in den erkannten Aussagen] und ignoriert einzelne Details, um *gemeinsame Muster* über unterschiedliche Beobachtungen hinweg zu identifizieren" [HMS05]. Stilisierte Fakten sind als "breit gestützte und generalisierte Wissens- oder Erfahrungswerte [zu verstehen], die essentielle Eigenschaften eines Phänomens darstellen" [HFL09]. Die Methode ist in jüngerer Vergangenheit nicht nur in der Volkswirtschaftslehre, sondern auch in der Betriebswirtschaftslehre [WL07] und in der Wirtschaftsinformatik [HFL09] angewendet und diskutiert [Lo11] worden.

Damit erscheint sie für die Ontologiekonstruktion in hohem Maße geeignet, um aus vorhandenen Quellen "Bottom-Up" relevante Einzelaussagen zu Konzepten, Konzepteigenschaften und Konzeptbeziehungen zu extrahieren, diese Aussagen hinsichtlich ihrer inhaltlichen Übereinstimmungen zu analysieren, sie bei hinreichender Übereinstimmung zu aggregieren oder aber auf Widersprüche offen hinzuweisen [WL07]. Die Methode schafft Transparenz über die einer Ontologie zugrunde liegenden Wissensbasis und die Breite des Experten-Konsenses zu den einzelnen Ontologieinhalten. Die Aussagen können zusätzlich danach klassifiziert werden, ob sie rein argumentativer Natur oder durch empirische Studien gestützt sind (Evidenz der Aussagen [GP10]) und ob und welche Qualitätssicherung sie erfahren haben (z.B. Art und Ranking der Quelle). Damit kann die derzeitige Fundierung der Einzelaussagen offengelegt werden.

Die Generierung der stilisierten Fakten erfolgt im Rahmen eines induktiven Prozesses, der nicht frei von einigen subjektiven Elementen ist [HMS05]. Um die Nachvollziehbarkeit der Faktengenerierung zu gewährleisten, soll daher möglichst transparent vorgegangen werden. Zwei Aspekte scheinen hier besonders bedeutsam ([HMS05] [HFL09] [WL07]): Zum einen sollte dokumentiert werden, welche ursprünglichen Aussagen einem stilisierten Fakt zugrunde liegen, damit eine konstruktive Diskussion der Schluss-

folgerungen möglich ist [HMS05]. Bei der Generalisierung ist abzuwägen, "ob die vorliegenden Erkenntnisse durch ein hinreichendes Maß an Übereinstimmung und Repräsentativität gekennzeichnet sind und die Formulierung des Stylized Fact als Ausdruck einer stabilen Tendenz gerechtfertigt ist" [WL07]. Zum anderen müssen Qualitätskriterien definiert werden, die eine Unterscheidung zwischen gut gestützten, durchschnittlich gestützten und eher schwach gestützten stilisierten Fakten erlauben und dem Adressaten somit anschaulich darstellen, zu welchen den Ontologieinhalten zugrunde liegenden stilisierten Fakten bislang nur ein schwacher Konsens festzustellen ist.

Bei [HMS05] findet sich das nachstehende Vorgehensmodell zur Faktengenerierung. Die Vorgehensmodelle von [HFL09] und [WL07] bauen auf diesem Modell auf und nehmen Verfeinerungen einzelner Aktivitäten vor. Für das Forschungsvorhaben sind die Aktivitäten nach [HMS05] aber hinreichend detailliert:

Definition des untersuchten Phänomens. Zu Beginn ist das Phänomen klar abzugrenzen, über das vorhandene schriftliche Einzelaussagen gesammelt und stilisierte Fakten generiert werden sollen [HMS05]. Die zu untersuchenden Phänomene hier sind das URM, das IRM und deren Integration.

Quellensuche in Literaturdatenbanken. Auf Basis der Definition des untersuchten Phänomens sollen im zweiten Schritt Literaturquellen identifiziert werden, aus denen die Aussagen zum untersuchten Phänomen zu extrahieren sind. Die Auswahl soll einerseits möglichst umfassend und repräsentativ sein, andererseits sollen die identifizierten Quellen *"ein möglichst hohes Maß an Qualität aufweisen"* [HMS05]. Für das betrachtete Forschungsvorhaben erscheinen Veröffentlichungen zum URM, zum IRM und zu deren Schnittstellen relevant. Als zulässige Quellen werden wissenschaftliche Veröffentlichungen, Standards und Best-Practice-Modelle angesehen. Sie unterliegen Qualitätssicherungsmaßnahmen, so dass der Qualitätsaspekt angemessen berücksichtigt erscheint. Im ersten Schritt sollen aus Praktikabilitätsgründen zunächst nur jeweils maximal zehn wissenschaftliche Monografien, Standards und Best-Practice-Referenzmodelle betrachtet werden, die als möglichst repräsentativ bzw. weit verbreitet gelten können und jeweils eine umfassende Sichtweise auf das unternehmensweite Risikomanagement bzw. Informationsrisikomanagement einnehmen. Im Sinne eines für die Ontologiekonstruktion empfohlenen "Middle-Out"-Vorgehens sollen so Aussagen/Fakten zu den bedeutendsten Konzepten, Konzepteigenschaften und Konzeptbeziehungen je System extrahiert werden [ST05]. Durch die nachgelagerte Ausweitung der Analyse auf ggf. stärker fokussierte Veröffentlichungen (wie es z.B. bei Zeitschriften- und Konferenzartikeln zu erwarten ist) können weitere Verfeinerungen erfolgen. Es wird aber erwartet, dass hierdurch keine gänzlich neuen, zentralen Konzepte etc. erkannt werden.

Identifikation von Aussagen zum Phänomen. Gegenstand der dritten Aktivität ist es, aus den identifizierten Quellen die relevanten Einzelaussagen zum untersuchten Phänomen zusammenzutragen. Es wird empfohlen, zu jeder Aussage einen Kurztext zu formulieren, der auch ohne Kenntnis der Quelle verstanden werden kann [HMS05]. Dem beschriebenen Vorgehen zur Aussageidentifikation soll ohne Änderung gefolgt werden.

Gruppierung der Aussagen. Die extrahierten Einzelaussagen sollen im nächsten Schritt anhand ihrer Inhalte gruppiert werden. Genauere Ausführungen zur Durchführung finden sich allerdings weder bei [HMS05] noch z.B. bei [HFL09] oder [WL07]. Für das eigene Forschungsvorhaben soll hier ein zweigeteiltes Vorgehen angewendet werden: Zunächst sollen die Original-Einzelaussagen und der jeweils zugehörige, selbst formulierte Kurztext gesammelt werden. Je Einzelaussage sollen die angesprochenen Konzepte, Konzeptbeziehungen und -eigenschaften explizit genannt werden. Die Einzelaussagen jeder Quelle können dann nach angesprochenem Konzept, Konzeptbeziehung und -eigenschaft gruppiert werden. In einem zweiten Schritt können die Aussagen quellenübergreifend zusammengeführt und ebenfalls entsprechend gruppiert werden.

An die Gruppierung muss sich eine Überprüfung und Bereinigung der Zuordnungen anschließen. So kann es möglich sein, dass inkonsistente Bezeichnungen für Konzepte, Konzepteigenschaften und Konzeptbeziehungen über die einzelnen Quellen hinweg verwendet worden sind (z.B. Formulierung von Bezeichnungen teilweise in Plural, teilweise in Singular), dass sich Schreibfehler eingeschlichen haben oder dass Aussagen im Lichte anderer Aussagen ggf. anders zugeordnet werden sollten. Die Überprüfung und Bereinigung stellt somit eine bedeutsame Teilaktivität zur Qualitätssicherung dar.

Nach erfolgter Gruppierung empfehlen [HMS05] zu jeder Aussage eine entsprechende Folgerung zu formulieren. Aus den gruppierten Folgerungen können dann im nächsten Schritt die stilisierten Fakten abgeleitet werden. Die Folgerungen sollen den vom Forscher „für relevant erachteten Teil der entsprechenden Aussage wiedergeben. Dabei können unwesentliche Details der Aussage vernachlässigt werden“ [HMS05]. Folgerungen lassen sich gegenüber Kurztexten dahingehend abgrenzen, das letztere lediglich dem besseren Verständnis einer Einzelaussage dienen, während erstere den für die Faktengenerierung relevanten Kern einer Aussage herausarbeiten und hierbei den Kontext, d.h. die anderen identifizierten Aussagen zum gleichen Konzept, zur gleichen Konzeptbeziehung bzw. Konzepteigenschaft, beachten.

Ableitung der stilisierten Fakten. Im letzten Schritt sollen auf der Grundlage der Folgerungen die stilisierten Fakten abgeleitet werden. Zur Verdeutlichung der Fundierung der Fakten durch Einzelaussagen können Qualitätsstufen verwendet werden, z.B. gut, durchschnittlich oder schlecht gestützt [WL07]. Die Regeln zur Zuordnung eines Fakts zu einer bestimmten Klasse (z.B. "mindestens 5 Quellen, die den Fakt stützen") entziehen sich allerdings einer allgemeingültigen Begründbarkeit [WL07]. Bei der Regelgestaltung muss auch berücksichtigt werden, dass gleiche Aussagen desselben Autors bzw. einer Autorengruppe in unterschiedlichen Quellen nur einmal gezählt werden dürfen [HFL09].

5 Erste Ergebnisse

Ausgehend von der Forschungsmethode konzentrierten sich erste Forschungsaktivitäten auf den Bereich des unternehmensweiten Risikomanagements. Hier sollen Erkenntnisse gesammelt werden, ob die Forschungsmethode anwendbar ist und fundierte Ergebnisse entsprechend den Gestaltungs- und Erkenntniszielen zu produzieren vermag. Abbildung 1 zeigt das Ergebnis der ersten Phase, die Spezifikation der Ontologie für das URM.

ISBN 978-3-88579-286-4

Spezifikation der Ontologie zum unternehmensweiten Risikomanagement	
Domäne:	Unternehmensweites Risikomanagement (Gesamtheit aller organisatorischen Regelungen und Maßnahmen, welche die Erkennung von Unternehmensrisiken und den Umgang mit diesen Unternehmensrisiken betreffen)
Zweck:	Die Ontologie soll Auskunft über die wesentlichen Bestandteile des unternehmensweiten Risikomanagementsystems, deren Eigenschaften sowie deren Beziehungen untereinander geben. Sie soll dazu beitragen, dass sich ein einheitliches Verständnis in Bezug auf die relevanten Bestandteile eines Risikomanagementsystems entwickelt und sie soll ihre Adressaten bei Fragen der Gestaltung und Prüfung entsprechender (softwaregestützter) Systeme unterstützen.
Adressaten	Als primäre Adressaten der Ontologie gelten Unternehmensleiter, Risikomanager, Interne Revisoren, Wirtschaftsprüfer, Berater und Softwarehersteller.
Aufbau:	Die Ontologieinhalte sollen übersichtlich in Ebenen strukturiert sein, um eine Informationsüberflutung der Ontologienutzer zu verhindern. Auf oberster Ebene sollen nur wenige Top-Level Konzepte dargestellt werden und der Detailgrad der Inhalte dann auf den darunter liegenden Ebenen zunehmen. Die Anzahl der Ebenen soll maximal 3 betragen.
Formalisierungsgrad:	Die Formalisierungsgrad der Ontologie soll mindestens semi-formal sein. Inwieweit ein höherer Grad an Formalisierung möglich ist (z.B. im Hinblick auf "weiche" Elemente wie Risikomanagementstrategie oder Risikokultur), kann zum aktuellen Zeitpunkt nicht abschließend beurteilt werden. Wenn möglich, soll ein höherer Formalisierungsgrad angestrebt werden. Unter "semi-formal" wird verstanden, dass die Ontologieinhalte in einer künstlichen Sprache formuliert werden deren Sprachelemente in Syntax und Semantik formal definiert sind (z.B. ERM).
Primäre Wissensquellen:	(1) Standards: ISO/IEC 31000:2009; IDW Prüfungsstandard 340; Kommentar zum IDW PS 340 im WP-Handbuch 2006; usw. (2) Best-Practice-Referenzmodelle: COSO Enterprise Risk Management - Integrated Framework; usw. (3) Monografien Wieben, H. J. (2004), Credit Rating und Risikomanagement - Vergleich und Weiterentwicklung der Analysekonzepte, DUV; Wolf, K. (2004) - Risikomanagement im Kontext der Wertorientierten Unternehmensführung, DUV; Strohmeier, G. (2007), Ganzheitliches Risikomanagement in Industriebetrieben. Grundlagen, Gestaltungsmodell und praktische Anwendung, DUV; usw.
Kernkonzepte:	RM-Kontext, RM-Gegenstandsbereich, RM-Strategie, RM-Organisation, RM-Prozess, Risikokultur, RM-Informationssystem
...	...

Abbildung 1: Auszug aus der Ontologiespezifikation

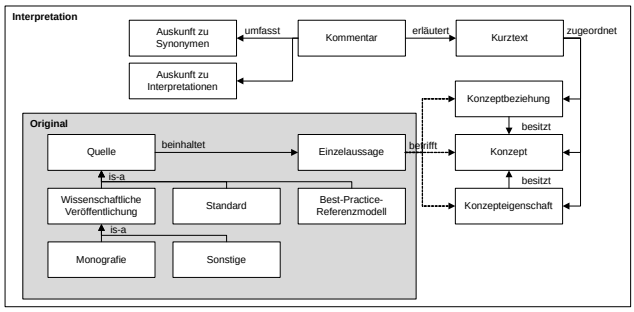

Abbildung 2: Metamodell der Aussagendokumentation

Parallel wurde mit der Wissensgenerierung begonnen. Gemäß den Ausführungen zur Quellensuche wurde der Fokus anfangs auf Standards und Best-Practice-Referenzmodelle zum Risikomanagement sowie auf ausgewählte Monografien gelegt, die unter dem Gesichtspunkt der ganzheitlichen Diskussion des unternehmensweiten Risikomanagements ausgewählt worden sind. In obiger Spezifikation sind die Quellen unter "Primäre Wissensquellen" angeführt. Die genannten Quellen wurden auf Einzelaussagen zu den Eigenschaften und Beziehungen der Elemente des unternehmensweiten Risikomanagementsystems analysiert. Die Ergebnisse wurden tabellarisch dokumentiert, wobei der Aufbau der Tabellen dem in Abbildung 2 dargestellten Metamodell entspricht.

- Als Wissensquellen gelten wissenschaftliche Veröffentlichungen, Standards und Best-Practice-Referenzmodelle.
- Die Wissensquellen beinhaltet Einzelaussagen zu den Eigenschaften und Beziehun-

gen der Elemente/Konzepte des unternehmensweiten Risikomanagementsystems. Die Eigenschaften (z.B. "Eintrittswahrscheinlichkeit"), Beziehungen (z.B. "Risiko betrifft Unternehmensbereich") und Konzepte (z.B. "Risiko") können entweder explizit in einer Einzelaussage benannt sein oder aber sich implizit aus dem weiteren Kontext der Aussage ergeben (repräsentiert durch die gestrichelten Linien). Eine Aussage kann mehrere Eigenschaften, Beziehungen und Konzepte ansprechen.

- Kurztexte besitzen eine subjektive Komponente, da sie vom Forscher formuliert sind. Sie dienen der Zerlegung von Einzelaussagen, die mehrere Eigenschaften oder Beziehungen eines oder mehrerer Konzepte ansprechen. Zu jeder angesprochenen Eigenschaft oder Beziehung geben sie den relevanten Teil der Einzelaussage wieder, d.h. sie vernachlässigen Aspekte, die nicht relevant erscheinen oder betonen Aspekte, die in der Einzelaussage nicht explizit enthalten sind, sich aber aus dem Kontext ergeben. Somit können zu jeder Einzelaussage mehrere Kurztexte existieren.
- Kommentare dienen dazu, eine bestimmte Interpretation innerhalb eines Kurztextes zu begründen (z.B. auf den Kontext hinzuweisen) und durchgeführte Begriffsersetzungen zu dokumentieren, um Transparenz über gleich interpretierte Begriffe zu schaffen und später Synonymlisten erstellen zu können.

Abbildung 3 zeigt einen Auszug aus der Auswertung der Quelle "IDW Prüfungsstandards 340" zur Veranschaulichung der Umsetzung und Anwendung des Metamodells.

ID	Original-Einzel-aussage	Kurztext	Auskunft zu Interpretationen	Begriffsersetzungen	Konzept	Konzept-eigen-schaft	Konzept-bezie-hung
1	Unter Risiko ist allgemein die Möglichkeit ungünstiger künftiger Entwicklungen zu verstehen.	Risiko ist mit Unsicherheit verbunden ("... Möglichkeit ungünstiger künftiger Entwicklungen ..."). Die Unsicherheit wird durch die Eintrittswahrscheinlichkeit eines Risikos ausgedrückt.	Das Konzept "Eintrittswahrscheinlichkeit" wird in Tz. 10 eingeführt. Es ist auch in anderen Quellen das gebräuchliche Konzept, um die Möglichkeit eines Risikos zum Ausdruck zu bringen und wird daher im Folgenden synonym zu "Möglichkeit" verwendet.	Möglichkeit <> Eintrittswahrscheinlichkeit	Risiko	Eintrittswahrscheinlichkeit	KEINE
26	Unter Risiko ist allgemein die Möglichkeit ungünstiger künftiger Entwicklungen zu verstehen.	Risiken besitzen negative Auswirkungen, wenn sie eintreten.	Für "ungünstige künftige Entwicklung" wird das Konzept "negative Auswirkung" eingeführt. Es wird auch im Standard (z.B. Tz. 10) entsprechend synonym verwendet. Das Konzept Auswirkung erscheint auch im Hinblick auf andere Quellen (z.B. ISO 31000) gebräuchlicher.	Negative Auswirkung <> ungünstige künftige Entwicklung	Risiko	KEINE	Auswirwirkung

Abbildung 3: Dokumentation der Einzelaussagen, Kurztexte und Zuordnungen (Auszug)

Nach der Auswertung der Quellen erfolgte die Gruppierung der extrahierten Einzelaussagen zunächst innerhalb der einzelnen Quellen zwecks Qualitätssicherung, anschließend quellenübergreifend. Zur Unterstützung der Gruppierung wurden die Tabellen in eine Datenbank eingelesen. Mittels Abfragen konnten die Einzelaussagen nach Konzept, Konzepteigenschaft oder -beziehung bzw. einer Kombination gruppiert und für die weiteren Analysen (z.B. Bereinigung inkonsistent verwendeter Konzeptbezeichnungen,

Ableitung stilisierter Fakten) aufbereitet werden. Den abschließenden Schritt der Wissensgenerierung stellt die Generierung der stilisierten Fakten dar. Dieser Schritt soll am Beispiel des Konzepts "Risiko" und der Eigenschaft "Restrisiko" veranschaulicht werden (Abbildung 4). Auf die Erläuterung des zugrunde liegenden Metamodell wird aus Platzgründen verzichtet, es geht aber implizit aus der Abbildung hervor.

Verdichtung bis Einzelaussagen (Fortsetzung folgende Seite, Gruppierung Einzelaussagen)						<= Einzelaussagen	
Konzept	**Eigenschaft**	**Stilisierter Fakt**	**Folgerung aus Kurztext**	**Auskunft zur Folgerung**	**Begriffsersetzungen in der Folgerung**	**Kurztext**	**Einzelaussage**	**ID**
Risiko	Restrisiko	Das Restrisiko ist der nicht-bewältigte Teil eines Risikos, der nach der Risikosteuerung verbleibt.	Das Restrisiko ist der nicht-bewältigte Teil eines Risikos.	Der Begriff "nicht bewältigtes Risiko" aus dem Kurztext wurde in der Folgerung mit dem Begriff "Restrisiko" ersetzt. Die Begriffe werden synonym zur Bezeichnung des gleichen Konzepts verwendet. Der Begriff "Restrisiko" erscheint verständlicher und eingängiger und wurde daher gewählt.	Restrisiko = Nicht bewältigtes Risiko	Ein Risiko kann vollständig oder in Teilen nicht bewältigt sein. Die zuständigen Entscheidungsträger im Unternehmen müssen über nicht-bewältigte Risiken informiert werden.	Soweit Risiken nicht bewältigt sind, muß schengesetzt werden, daß Informationen darüber in nachweisbarer Form an die zuständigen Entscheidungsträger weitergeleitet werden. Sie es grundsätzlich vorgesehen, daß eine nicht bewältigtes Risiko - ggf. in aggregierter Form– bis zum Vorstand berichtet wird.	1.16
			Das Restrisiko ist der nicht-bewältigte Teil eines Risikos, der nach der Risikosteuerung verbleibt.	Begründung zur Begriffsersetzung wie oben	Restrisiko = Residuales Risiko	Das residuale Risiko ist das Risiko, das nach der Risikosteuerung verbleibt.	residual risk = risk (2.1) remaining after risk treatment (2.25)	3.28
			Das Restrisiko ist der nicht-bewältigte Teil eines Risikos, der nach der Risikosteuerung verbleibt.	Begründung zur Begriffsersetzung wie oben	Restrisiko = Residuales Risiko	Das residuale Risiko ist das Risiko, das nach Durchführung der vom Management vorgesehenen Risiko-Steuerungs-maßnahmen verbleibt.	Residual risk is the risk that remains after management's response to the risk.	4.25
			Das Restrisiko ist der nicht-bewältigte Teil eines Risikos, der nach der Risikosteuerung verbleibt.	Begründung zur Ersetzung des Begriffs "Nettorisiko" durch "Restrisiko" wie oben. Auch der Begriff "Risikobewältigung" wurde aus vergleichbaren Gründen durch den Begriff "Risikosteuerung" ersetzt.	Restrisiko = Nettorisiko; Risikosteuerung = Risikobewältigung	Das Netto- bzw. Restrisiko ist das Risiko, das sich ergibt, wenn bei der Risikobewertung alle ergriffenen Maßnahmen zur Risikobewältigung berücksichtigt werden.	Erst daran anschließend sind die Risken zusätzlch netto zu bewerten. [...] Die Höhe des Restrisikos dient [..] als Entscheidungsgrundlage für den jeweiligen Entscheidungsträger, ob weitere Maßnahmen zur Risikobewältigung ergriffen werden müssen.	2.34
			Das Restrisiko ist der nicht-bewältigte Teil eines Risikos, der nach der Risikosteuerung verbleibt.	Begründung zur Ersetzung des Begriffs "Nettorisiko" durch "Restrisiko" wie oben. Auch der Begriff "Risikohandhabung" wurde aus vergleichbaren Gründen durch den Begriff "Risikosteuerung" ersetzt.	Restrisiko = Nettorisiko; Risikosteuerung = Risikohandhabung	Das Nettorisiko ist der nicht-bewältigte Teil eines Risikos, der nach den vom Management bisang eingeleiteten Risiko-Steuerungsmaßnahmen verbleibt und im Rahmen der Risikobewertung bestimmt wird.	Eine einheitliche Betrachtung von Brutto- oder Nettorisiken ist dabei (gemeint ist die Risikobewertung, PWO) sinnvoll. Die Nettobetrachtung bezieht die vom Unternehmen eingeleiteten Maßnahmen der Risikohandhabung in die Bewertung ein, während dies in der Bruttobetrachtung nicht der Fall ist. [RN entfernt, PWO]	7.41

Abbildung 4: Dokumentation der stilisierten Fakten zum URM (Auszug)

ISBN 978-3-88579-286-4

Auf der rechten Seite in Abbildung 4 sind jeweils die Originalaussagen und Kurztexte angegeben. In der Mitte ist je Einzelaussage und Kurztext die Folgerung dargestellt und kommentiert. Die Folgerungen zielen darauf ab, eine Aussagen-übergreifende Normierung der Begrifflichkeiten vorzunehmen und die Inhalte der Kurztexte/Einzelaussagen nochmals im Kontext der sonstigen Einzelaussagen zu interpretieren. So soll der Schluss von den Einzelaussagen auf die stilisierten Fakten transparent gemacht werden.

Auf der linken Seite ist schließlich der stilisierte Fakt zusammen mit dem Konzept und der Konzepteigenschaft dargestellt, auf die er sich bezieht. Das Konzept "Restrisiko" wird demnach in fünf von sieben Quellen angesprochen und inhaltlich definiert. Dies lässt vermuten, dass es sich um ein vergleichsweise relevantes Konzept handelt, das in der Ontologie enthalten sein sollte. Zwei der Einzelaussagen lassen sich auch dahingehend interpretieren, dass das Nettorisiko im Rahmen der Aktivität der Risikobewertung bestimmt werden sollte (nicht in oberer Grafik dargestellt) und das hier eine entsprechende Beziehung zwischen den zwei Konzepten besteht, die aber bislang weniger stark thematisiert wird.

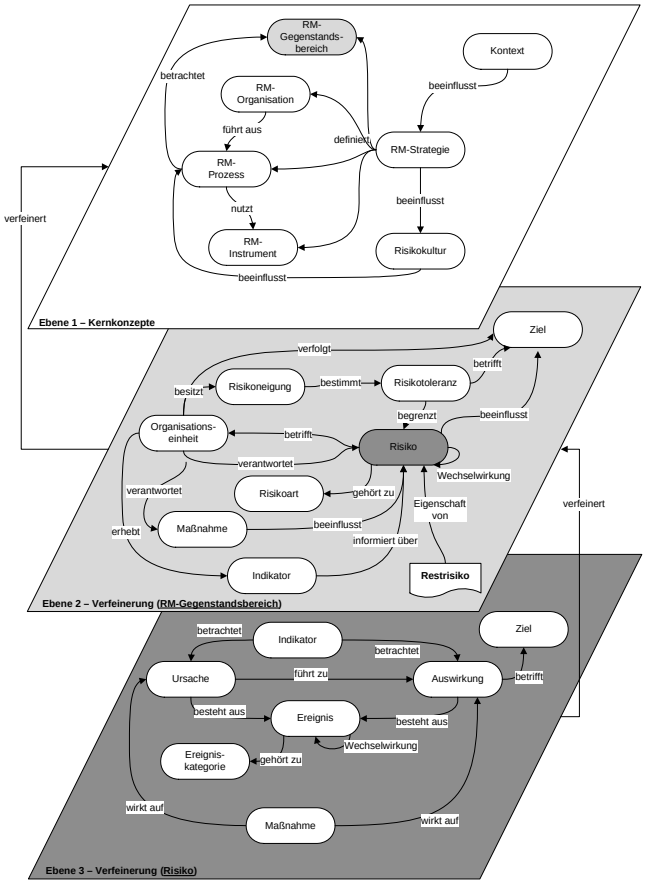

Abbildung 5: Auszug der Ontologie des URM

Die Ergebnisse der Faktengenerierung bildeten den Input für die Aktivitäten der Konzeptualisierung und Formalisierung der Ontologie zum URM. Abbildung 5 zeigt einen Ausschnitt der Ontologie. Die Konzepte sind, wie spezifiziert, auf drei Ebenen angeordnet: Ebene 1 weist dabei den geringsten und Ebene 3 den höchsten Detailgrad auf. Das Beispiel veranschaulicht für Ebene 2 die Verfeinerung des Konzepts "RM-Gegenstandsbereichs" und für Ebene 3 die Verfeinerung des Konzepts "Risiko". Wie zu sehen ist, wurde die in Abbildung 4 dargestellte Eigenschaft "Restrisiko" als Bestandteil des Konzepts "Risiko" auf Ebene 2 modelliert. Somit kann mittels der Konzepte auf Ebene 2 u.a. Auskunft über die Wirkung von Maßnahmen gegeben werden. Weiterhin ist z.B. eine Information darüber möglich, welche Ziele durch welche Risiken bedroht sind, da die entsprechende Ziel-Risiko-Beziehung hier ebenfalls explizit modelliert ist.

Auf der darunter liegenden Ebene 3 wird das Konzept "Risiko" in Ursachen und Auswirkungen verfeinert, die selbst wiederum aus (verschiedenen) Ereignissen bestehen können. Beispielsweise kann eine Ursache für das Unternehmensrisiko "Verfehlung der Umsatzziele" der tagelange Ausfall des Online-Shops sein, über den ein Großteil der Umsätze generiert wird. Ereignisse, die dieser Ursache zugrunde liegen, können z.B. "Brand im Rechenzentrum", "Nicht wirksamer Notfallplan" und "Fehlendes Ersatzrechenzentrum" sein. Der gemeinsame Eintritt der Ereignisse (Ursache) kann unmittelbar zum Ereignis "Ausfall der zentralen Online-Shop-Applikation" führen und mittelbar das Ereignis "Verlust von x% der geplanten Umsätze infolge des Online-Shop-Ausfalls" führen. Das Risiko stellt die aggregierte Sicht auf diese Einzelereignisse dar. Maßnahmen können an den Ursachen ansetzen und z.B. regelmäßige Brandschutzübungen sein oder der Aufbau eines Ersatzrechenzentrums. Sie können auch auf die Auswirkungen abzielen, z.B. Abschluss von Versicherungen. Die genannten Konzepte basieren auf den identifizierten Einzelaussagen und abgeleiteten Fakten. Aus Platzgründen muss an dieser Stelle auf eine weitergehende Erläuterung von Abbildung 5 verzichtet werden. Die Abbildung soll v.a. eine Vorstellung der Ergebnisse des Forschungsvorhabens vermitteln.

6 Fazit und Ausblick

Kern dieses Beitrags war die Präsentation einer Forschungsmethode zur Konstruktion fundierter Ontologien des URM, des IRM und der Informationsschnittstellen zwischen beiden Systemen sowie die Diskussion erster Ergebnisse. Die vorgeschlagene Forschungsmethode greift zur Gewinnung des erforderlichen Wissens für die Ontologiekonstruktion auf die Methode stilisierter Fakten zurück. Diese Methode ist bereits in verschiedenen Kontexten und Disziplinen erfolgreich eingesetzt wurden und wird auch hier als zweckmäßige, wenngleich sehr aufwändige Möglichkeit eingestuft, um die für erforderlich gehaltene Fundierung der Ontologieinhalte zu erreichen. Die Voraussetzung für die Anwendung der Methode stilisierter Fakten in Form einer umfassenden schriftlich fixierten Wissensbasis wird sowohl für das Informations- als auch das unternehmensweite Risikomanagement als erfüllt angesehen.

Das beschriebene Forschungsvorhaben soll intensiv weitergeführt werden, um die genannten Erkenntnis- und Gestaltungsziele zu erreichen. Mit diesem Beitrag soll der Grundstein für eine Diskussion des Vorgehens und der ersten Ergebnisse gelegt werden.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4
weitere Artikel online:
http://informatik2011.de/519.html

7 Literaturverzeichnis

[Bl08] Blanco, C.; Lasheras, J.; Valencia-García, R.; Fernández-Medina, E.; Toval, A.; Piattini, M.: A Systematic Review and Comparison of Security Ontologies. In *Proceedings of the 2008 Third international Conference on Availability, Reliability and Security* (March 04 - 07, 2008). ARES. IEEE Computer Society, Washington, DC, 2008.

[COSO04]Committee of Sponsoring Organizations of the Treadway Commision (COSO): *Enterprise Risk Management – Integrated Framework. Executive Summary*. 2004. http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf (10.08.2010).

[CFG03] Corcho, O.; Fernández-López, M.; Gómez-Pérez, A.: Methodologies, tools and languages for building ontologies: where is their meeting point?. *Data Knowl. Eng.* 46, 1 (Jul. 2003), S. 41-64.

[FGJ97] Fernández, M.; Gómez-Pérez, A.; Juristo, N.: *Methontology: From Ontological Art Towards Ontological Engineering*. Technical Report. AAAI Spring Symposium Series, Workshop on Ontological Engineering, 1997.

[FG02] Fernández-López, M.; Gómez-Pérez, A.: Overview and analysis of methodologies for building ontologies. *Knowl. Eng. Rev*. 17, 2 (Jun. 2002), S. 129-156.

[GP10] Goeken, M.; Patas, J.: Evidenzbasierte Strukturierung und Bewertung empirischer Forschung im Requirements Engineering. Grundlagen, Ordnungsrahmen, Forschungslandkarte. *Wirtschaftsinformatik* 52, 3 (2010), S. 173-184.

[Gr93] Gruber, T. R.: A translation approach to portable ontology specifications. *Knowl. Acquis*. 5, 2 (Jun. 1993), S. 199-220.

[Gu09] Guarino, N.; Oberle, D.; Staab, S.: What Is an Ontology? In: *Handbook on Ontologies.* Staab, S.; Studer, R. Hrsg. Berlin, 2009.

[HMS05] Heine, B.-O.; Meyer, M.; Strangfeld, O.: Stylised Facts als Konzept zur Messung und Bewertung wissenschaftlichen Fortschritts. In *Fortschrittskonzepte und Fortschrittsmessung in der Betriebswirtschaftslehre und der Wirtschaftsinformatik*, Zelewski, S. u. Akca, N. Hrsg., Essen, 2005, S. 119-138.

[HFL09] Houy, C.; Fettke, P.; Loos, P.: Stilisierte Fakten der Ereignisgesteuerten Prozesskette - Anwendung einer Methode zur Theoriebildung in der Wirtschaftsinformatik. In: *EPK 2009. GI-Workshop - AK "Geschäftsprozessmanagement mit Ereignisgesteuerten Prozessketten"* (Nov. 26-27, 2009). Nüttgens, M. et al. Hrsg. Berlin, 2009, S. 22-41.

[In09] Innerhofer-Oberperfler, F.: *A Framework for Rating IT Business Risks*. Dissertation. Leopold-Franzens-Universität, Innsbruck, Österreich, 2009.

[IDW99] Institut der Wirtschaftsprüfer (IDW): *IDW Prüfungsstandard: Die Prüfung des Risikofrüherkennungssystems nach § 317 Abs. 4 HGB (IDW PS 340) (Stand: 11.09.2000)*. In IDW –Fachnachrichten, 8 (1999), S. 350-357.

[ISACA09] ISACA: *The Risk IT Framework*, ISACA, RollingMeadows, IL, 2009.

[ISO09] ISO: *Risk Management – Principles and guidelines (ISO 31000)*. First Edition 2009-11-15, ISO, Genf, Schweiz, 2009.

[Ju05] Junginger, M.: *Wertorientierte Steuerung von Risiken im Informationsmanagement*. DUV, Wiesbaden, 2005.

[JK04] Junginger, M.; Krcmar, H.: *Wahrnehmung und Steuerung von Risiken im Informationsmanagement – Eine Befragung deutscher IT-Führungskräfte*. Studie. Lehrstuhl für Wirtschaftsinformatik. Technische Universität München, Garching, 2004.

[Lo11] Loos, P.: WI-Meinung/Dialog: Welche Rolle spielen eigentlich stilisierte Fakten in der Grundlagenforschung der WI? In: *Wirtschaftsinformatik* 2, 2011

[Lo99] López, M. F.; Gómez-Pérez, A.; Sierra, J. P.; Sierra, A. P.: Building a Chemical Ontology Using Methontology and the Ontology Design Environment. *IEEE Intelligent Systems* 14, 1 (1999), S. 37-46.

[MM03] Maedche, A; Motik, B.: Repräsentations- und Anfragesprachen für Ontologien – eine Übersicht. *Datenbank-Spektrum* 3, 6 (Juni 2003), S. 43-53.

[Pr08] Prokein, O.: *IT-Risikomanagement. Identifikation, Quantifizierung und wirtschaftliche Steuerung*. Gabler, GWV, Wiesbaden, 2008.

[ST05] Seedorf, S.; Tomczyk, P.: *Ein angepasstes Vorgehensmodell zur Entwicklung von Domänenontologien in der semantikbasierten Softwareentwicklung*.Arbeitspapier, 2 (März 2005), Universität Mannheim, FZI, Mannheim, 2005.

[Si07] Sienou, A.; Lamine, E.; Karduck, A.; Pingaud, H.: Conceptual model of risk: towards a risk modeling language. In *Proceedings of the 2007 international Conference on Web information Systems Engineering*. Lecture Notes In Computer Science. Springer, Berlin, Heidelberg, 2007, S. 118-129.

[SHF10] Strecker, S.; Heise, D.; Frank, U.: RiskM: A multi-perspective modeling method for IT risk assessment. *Information Systems Frontiers*, 2010. Online erschienen: 04.05.2010. DOI: 10.1007/s10796-010-9235-3.

[St07] Strohmeier, G.: *Ganzheitliches Risikomanagement in Industriebetrieben. Grundlagen, Gestaltungsmodell und praktische Anwendung*. DUV, GWV, Wiesbaden, 2007.

[Us96] Uschold, M.: Building ontologies: Towards a unified methodology. In *Proceedings of the Expert Systems, the 16th Annual Conf. of the British Computer Society Specialist Group on Expert Systems* (1996), Cambridge, UK, 1996.

[WL07] Weißenberger, B. E.; Löhr, B. W.: Planung und Unternehmenserfolg: Stylized Facts aus der empirischen Controllingforschung im deutschsprachigen Raum von 1990 – 2007. *Zeitschrift für Planung und Unternehmenssteuerung* 18, 4 (2007), S. 335-363. DOI=10.1007/s00187-007-0036-x.

[WH07] Westerman, G.; Hunter, R.: *Turning business threats into competitive advantage.* HBS Press, Boston, MA, 2007.

[Wi04] Wieben, H.-J.: *Credit Rating und Risikomanagement – Vergleich und Weiterentwicklung der Analysekonzepte*. DUV, GWV, Wiesbaden, 2004.

[Wo03] Wolf, K.: *Risikomanagement im Kontext der wertorientierten Unternehmensführung.* DUV, GWV, Wiesbaden, 2003.

[MR05] Zur Mühlen, M.; Rosemann, M.: Integrating Risk in Business Process Models. In *Proceedings der 16th Australasian Conference on Information Systems*, 2005. URL http://aisel.aisnet.org/acis2005/50 (23.08.2010).