Wissensabfluss und Wissensschutz bei (inter)nationalen IT-Projekten mit externen Dienstleistern

Empirische Analysen und Strategien zu einem Problem des Wissensmanagements

vorgelegt von

M. Sc.

André Karg

an der Fakultät I – Geistes- und Bildungswissenschaften

der Technischen Universität Berlin

zur Erlangung des akademischen Grades

Doktor der Philosophie

- Dr. phil. -

genehmigte Dissertation

Promotionsausschuss:

Vorsitzende: Prof. Dr. Silke Bartsch

Gutachter: Prof. Dr. Hans-Liudger Dienel

Gutachter: Prof. Dr. Andreas Schmietendorf

Tag der wissenschaftlichen Aussprache: 29. September 2020

Berlin 2020

„Eine Investition in Wissen bringt immer noch die besten Zinsen.“

Benjamin Franklin

Zusammenfassung

Die Forschungsarbeit beschreibt ein entwickeltes und evaluiertes Referenzmodell für den Wissensschutz bei IT-Projekten (Individual-Software-Entwicklung), um die erarbeiteten Wettbewerbsvorteile innerhalb einer IT-Beratung zu halten und damit auch die Existenz der Kunden zu sichern. Eine IT-Beratung soll in die Lage versetzt werden die Wissensrisiken vor und während der Zusammenarbeit mit externen Dienstleistern zu identifizieren und diese in die Dienstleisterauswahl einzubeziehen. Der ungewollte Wissenstransfer wird meist zu spät registriert, wenn bereits wirtschaftliche Folgen für die Wettbewerbsfähigkeit eingetreten sind. Es besteht Bedarf an umfassenderen Frameworks, um den Wissensverlust aus strategischer Perspektive zu adressieren. Zudem gibt es keinen Beweis für einen systematischen und umfassenden Managementansatz zur Identifikation und zum Schutz der Wissensressourcen. Für die Entwicklung des Referenzmodells und die Bearbeitung der Forschungslücke werden dazu die Methoden Literature Review, Prototyping, Experteninterviews, Inhaltsanalyse und Pilotierung genutzt.

Das Referenzmodell beschreibt in den etablierten Sourcing-Phasen, Strategie und Planung sowie Dienstleisterauswahl, die einzelnen Funktionen mit ihren Akteuren und den notwendigen Inputdaten, damit die Entscheidungen als resultierender Output getroffen werden können. Zudem kann eine IT-Beratung mit der Bewertung der Wissensgebiete ihre Identität bestimmen, auf denen ihr Wert beruht und diesen Wert im Unternehmen manifestieren. Die Projekt-Akteure einer IT-Beratung erhalten mit dem Modell Handlungsempfehlungen, um den Wissensschutz bei Prinzipal-Agenten-Beziehung umzusetzen. Die Entscheidungsfindung ist auf einen gemeinsamen Prozess zurückzuführen und damit nicht auf die Entscheidung von Einzelpersonen. In dem hier beschriebenen Referenzmodell werden dafür die folgenden Wissensschutzmechanismen genutzt: Identifizierung von wertvollen Wissensressourcen, Geheimhaltung, Beschränkung vom Dienstleisterzugriff durch zielgerichtete Dienstleisterauswahl und Überwachung der Wissensflüsse.

In der Arbeit wird empfohlen den Wissensschutz im Rahmen der ISO Norm 9001 umzusetzen, da diese Norm bereits das Wissensmanagement und damit auch das Risikomanagement von Unternehmen enthält. Zudem adressiert die Arbeit identifizierte Forschungslücken und zeigt zukünftige Forschungsfelder auf.

Abstract

The research work descripes a developed and evaluated reference model to protect the knowledge of IT projects (individual-software-development) in order to keep the competitive advantages elaborated within an IT consultancy and thus also to safeguard the existence of the customer financing the projects. IT consulting companies should be enabled to identify the knowledge risks before and when cooperating with external suppliers and to include them in the selection of external suppliers. In most cases the undesired knowledge transfer will be noticed too late when already economic consequences have arisen. More comprehensive frameworks are needed to address the knowledge loss from a strategic perspective. In addition there is no proof for a systemic and comprehensive management method to identify and protect the knowledge resources. For the development of the reference model and the processing of the research gap the following methods are being used: Literature Review, Prototyping, Expert Interviews, Content Analysis, and Pilot Testing.

In the established sourcing phases strategy and planning as well as selection of external suppliers the reference model describes the individual functions with their actors and the necessary input data so that the decisions can be taken as a resulting output. In addition an IT consultancy can determine their identity by evaluating the knowledge fields on which their value is based and manifest this value in the enterprise. The project actors of IT consultancies will receive recommendations for action with the [reference] model in order to be able to implement knowledge protection in case of principal-agent relations. Decision making is based on a common process and thus not on a decision of individuals. The following knowledge protection mechanisms are being used in the presently described reference model: Identification of valuable knowledge resources, secrecy, restriction of external supplier access through purposeful external supplier selection and the surveillance of the flow of knowledge.

The research work recommends to implement knowledge protection within the scope of ISO Standard 9001 as this standard already includes the knowledge management and thus also the risk management of companies. In addition the work addresses identified research gaps and shows future research fields.

Inhaltsverzeichnis

1 Einführung 1

1.1 Motivation 3

1.2 Forschungsziele 7

1.3 Aufbau der Forschungsarbeit 10

2 Grundlagen 13

2.1 Definitionen und Abgrenzung 13

2.1.1 Wissen 14
2.1.2 Wissensmanagement und -strategie 19
2.1.3 Wissensschutz und -strategie 22

2.2 IT-Beratung, Projekte und Software 30

2.2.1 Begriffsklärung und Merkmale 30
2.2.2 Softwareentwicklung in einer IT-Beratung 34
2.2.3 Wissensrisiken in einer IT-Beratung 38

2.3 Theoretische Fundierung 44

2.3.1 Prinzipal-Agent-Theorie 45
2.3.2 Weitere theoretische Ansatzpunkte 50

3 Forschungsmethoden und -vorgehen 58

3.1 Forschungsansatz und Forschungsprozess 58

3.1.1 Aktionsforschung 59
3.1.2 Design Science Research 60
3.1.3 Referenzmodellierungsprozess 62

3.2 Referenzmodellierung 67

3.2.1 Begriffsklärung und Anforderungen 67
3.2.2 Darstellungstechnik 74

3.3 Forschungsvorgehen 76

3.3.1 Prototypentwicklung mit Literature Review 76
3.3.2 Methodik der Experteninterviews und des Gruppeninterviews 78
3.3.3 Prototypevaluation mit Experteninterviews 81
3.3.4 Pilotierung mit Einzelinterviews und Gruppeninterview 88

4 Stand der Wissensschutzforschung 92

4.1 IT-Sourcing als Forschungsgegenstand 92

4.2 Sourcing-Phase 1: Strategie und Planung 97

4.2.1 Wissensschutzstrategien, -methoden und -mechanismen 97
4.2.2 Wissensschutzziele und effektive Wissensschutzmechanismen 102
4.2.3 Bestimmung der Unternehmensgrenze für den Wissensschutz 107
4.2.4 Risikomanagement und (Out-)Sourcing 111

4.3 Sourcing-Phase 2: Dienstleisterauswahl 117

4.3.1 Opportunismus und Vertrauen 117
4.3.2 Wissens-, Markt-, Wettbewerbsüberlappung 123

4.3.3 Absorptive Kapazität 126

5 Forschungsergebnis Wissensschutz-Referenzmodell 130

5.1 Überblick zum Referenzmodell 130

5.2 Referenzmodell-Phase 1: Strategie und Planung 137

5.2.1 Funktion 1: Strategische Planung für Wissensschutz durchführen 138

5.2.2 Funktion 2: Wissensschutz im Rahmen der Projektkategorisierung ermitteln 140

5.2.3 Funktion 3: Wissensgebiete auf Wissensschutz-Bedarf prüfen (Kategorisierung) 148

5.3 Referenzmodell-Phase 2: Dienstleisterauswahl 154

5.3.1 Funktion 4: Dienstleister kategorisieren 155

5.3.2 Funktion 5: Risikobewertung durchführen und Dienstleister auswählen 162

5.4 Evaluation 166

5.4.1 Modellevaluation im Rahmen der Pilotierung 166

5.4.2 Deployment Perspektive 173

5.4.3 Epistemologische Perspektive 176

5.4.4 Ökonomische Perspektive 179

6 Synthese und Ausblick 182

6.1 Beantwortung der Forschungsfragen 182

6.2 Reflexion: Erkenntnisse und Limitationen 184

6.2.1 Wissenschaftlicher Beitrag 185

6.2.2 Praktische Erkenntnisse 188

6.3 Anregung zur weiterführenden Forschung 191

7 Literaturverzeichnis 194

8 Anhang 217

8.1 Experten-Interviewleitfaden 217

Abkürzungsverzeichnis

AG	Auftraggeber
ARIS	Architektur integrierter Informationssysteme
BITKOM	Bundesverband Informationstechnologie Telekommunikation und neue Medien e.V.
BPS	Business Process Sourcing
CEO	Chief Executive Officer
CFO	Chief Financial Officer
COO	Chief Opperating Officer
CPO	Chief Purchase Officer / Chief Procurement Officer
DL	Dienstleister
DS	Design Science
DSR	Design Science Research
FZD	Funktionszuordnungsdiagramm
eEPK	erweiterte ereignisgesteuerte Prozesskette
EPK	ereignisgesteuerte Prozesskette
EU	Europäische Union
F&E	Forschung und Entwicklung
GUI	Graphical User Interface
IKS	Informations und Kommunikationssystem
IKT	Informations- und Kommunikationstechnologie
IP	Interviewpartner
IPP	Intellectual Property
IPMA	Internationale Project Management Association
IPR	Intellectual Property Rights
IS	Informationssystem
ISE	Individual-Software-Entwicklung
ISR	Information Systems Research
IT	Informationstechnologie
ITS	Informationstechnologie Sourcing
IV	Interview
KIBS	Knowledge-intensive Business Services
KPS	Knowledge Process Sourcing
PA	Prinzipal-Agenten

p.a.	per annum
PT	Personentage
TAK	Transaktionskosten
USP	Unique Selling Proposition
WI	Wirtschaftsinformatik
WM	Wissensmanagement
WMS	Wissensmanagementsystem
WS	Wissensschutz

Abbildungsverzeichnis

Abbildung 1: Übersicht zum Forschungsobjekt 1

Abbildung 2: Forschungsobjekt sind IT-Projekte mit externen IT-Dienstleistern 10

Abbildung 3: Aufbau der Dissertationsschrift 11

Abbildung 4: Die Wissenstreppe 20

Abbildung 5: Wissenssicherheit und überlappende Theorien 24

Abbildung 6: Wissenssicherheit und angrenzende Konzepte 24

Abbildung 7: Spannungsfeld vom Wissen-Teilen und Wissensschutz 28

Abbildung 8: Rahmen- und Einzelprojektorganisation 32

Abbildung 9: Einordnung der Individualsoftware in IKT 37

Abbildung 10: Klassifikation von Software nach dem Grad der Kundenindividualität 38

Abbildung 11: Bedrohungen, Werte und Risiken 40

Abbildung 12: Grundstruktur einer Risikoanalyse 40

Abbildung 13: Übersicht zum Spannungsfeld der IT-Dienstleistungen und dem Wissensschutz 41

Abbildung 14: Beispiele für Leistungsbeziehungen im Schichtenmodell der betrieblichen Informationsstruktur 42

Abbildung 15: Einteilung betrieblicher Anwendungssysteme nach dem Verwendungszweck 43

Abbildung 16: Verhaltensrisiken vor und nach Vertragsschließung bei Prinzipal-Agenten-Beziehungen 48

Abbildung 17: Die durch die Vertrauensbeziehung begründeten Verhaltensrisiken 54

Abbildung 18: Klassifikation von Ressourcen innerhalb der Knowledge-based view 55

Abbildung 19: Angewendete Methoden in der Arbeit 59

Abbildung 20: Informationssystem DSR-Forschungs-Framework 61

Abbildung 21: Einordnung des Referenzmodells in den Design Science Prozess 62

Abbildung 22: Phasen des Forschungsvorgehens 63

Abbildung 23: Einsatzhäufigkeit der primären Methode in den Jahren 2007-2012 67

Abbildung 24: Transformation des „Ist“ zum „Soll“ mittels eines Vorgehensmodells 72

Abbildung 25: Iterative Prozesse der Referenzmodell-Entwicklung und -Anwendung 73

Abbildung 26: Darstellungsform eines Funktionszuordnungsdiagramms 76

Abbildung 27: Ablauf von qualitativen Interviews 82

Abbildung 28: Wissensschutzmethoden 98

Abbildung 29: Die branchenspezifischen Unterschiede beim IP-Schutz in drei KIBS-Branchen 104

Abbildung 30: Proximationsanalyse 110

Abbildung 31: Weltklasse Ressourcen / Fähigkeiten 114

Abbildung 32: Sourcing Alternativen 115

Abbildung 33: Transitivität der Partnerauswahlentscheidungen 121

Abbildung 34: Erweiterte ereignisgesteuerte Prozesskette des Wissensschutz-Referenzmodells 133

Abbildung 35: Ereignisgesteuerte Prozesskette des Wissensschutz-Referenzmodells 134

Abbildung 36: Funktion Strategische Planung für Wissensschutz durchführen 139

Abbildung 37: Funktion Wissensschutz für IT-Projekt ermitteln (Kategorisierung) 141

Abbildung 38: Funktion Wissensgebiete auf Wissensschutzbedarf prüfen 148

Abbildung 39: Funktion Dienstleister kategorisieren 156

Abbildung 40: Dienstleisterkategorisierung nach Gefahrenpotential 158

Abbildung 41: Funktion Risikobewertung durchführen und Dienstleister auswählen 163

Abbildung 42: Risikobewertung für das Technologie-/Fachwissen im IT-Projekt 164

Abbildung 43: Risikobewertung für das Technologie-/Fachwissen im IT-Projekt α 172

Abbildung 44: Projektsteckbrief für Ist-Projekte 221

Abbildung 45: Projektkategorisierung nach Technologie- / Fachwissen im IT-Projekt 221

Abbildung 46: Projektsteckbrief für Beispiel 1 221

Abbildung 47: Projektsteckbrief für Beispiel 2 222

Abbildung 48: Projektkategorisierung für Beispiel 1 222

Abbildung 49: Projektkategorisierung für Beispiel 2 222

Abbildung 50: Kategorisierungsmatrix des Fachwissens / Technologiewissens Template ... 223

Abbildung 51: Kategorisierungsmatrix des Technologiewissens für Beispiel 1 und 2 224

Abbildung 52: Kategorisierungsmatrix des Fachwissens für Beispiel 1 und 2 224

Abbildung 53: Projektkategorisierung für Beispiel 1 225

Abbildung 54: Projektkategorisierung für Beispiel 2 225

Abbildung 55: Bsp. Wissenskategorisierung der IT-Beratung mit Projektbezug 225

Abbildung 56: Dienstleisterkategorisierung nach Gefahrenpotential für Beispiel 1 und 2 ... 227

Abbildung 57: Kategorisierungsmatrix nach Dienstleister Fachwissen/Technologiewissen Template 228

Abbildung 58: Kategorisierungsmatrix Fachwissen für Dienstleister Meyer 228

Abbildung 59: Kategorisierungsmatrix Technologiewissen für Dienstleister Meyer 229

Abbildung 60: Kategorisierungsmatrix Fachwissen für Dienstleister Schmidt 229

Abbildung 61: Kategorisierungsmatrix Technologiewissen für Dienstleister Schmidt 229

Abbildung 62: Dienstleisterkategorisierung Template 230

Abbildung 63: Dienstleisterkategorisierung Beispiel 1 230

Abbildung 64: Dienstleisterkategorisierung Beispiel 2 231

Abbildung 65: Projektsteckbrief für Beispiel 1 232

Abbildung 66: Risikobewertung Vertriebssystem 232

Abbildung 67: Projektsteckbrief für Beispiel 2 233

Abbildung 68: Risikobewertung Logistiksystem 233

Tabellenverzeichnis

Tabelle 1: Wissensarten und ihre Autoren 15

Tabelle 2: Einteilung in Wissensträger 17

Tabelle 3: Verwendete Einteilung von Wissensinhalten 18

Tabelle 4: Äquivalente Bezeichnungen für Knowledge Protection 26

Tabelle 5: Beschreibung der Projektmanagementphasen nach DIN 69901-5: 2009 33

Tabelle 6: Grundtypen der Verhaltensunsicherheit 46

Tabelle 7: Grundtypen von Agenturproblemen 47

Tabelle 8: Aktivitäten der Referenzmodell-Entwicklung und -Anwendung 73

Tabelle 9: Notation der Elemente der EPK und des FZD 75

Tabelle 10: Suchworte und relevante Autoren aus der Initialrecherche 77

Tabelle 11: Arten von Befragungen beim qualitativen Paradigma 79

Tabelle 12: Interviewleitfaden - Überblick 83

Tabelle 13: Stichprobendesign und Ist-Durchführung der Interviews 85

Tabelle 14: Teilnehmer an den qualitativen Experteninterviews 86

Tabelle 15: Auswahl eines IT-Projektes für das Gruppeninterview 90

Tabelle 16: Gruppeninterviewleitfaden - Überblick 91

Tabelle 17: Etablierte Phasen beim IT-Sourcing 95

Tabelle 18: Wissensschutz tangiert die Literatur zur Dienstleisterauswahl 96

Tabelle 19: Klassifizierungsrahmen von Wissensschutzmechanismen 99

Tabelle 20: Synthese von Wissensschutzgebieten und -mechanismen 101

Tabelle 21: Einflussfaktoren auf die Wissensschutzziele 102

Tabelle 22: Verwendung der Begriffe im Zusammenhang mit Wissensschutz 109

Tabelle 23: Phasen und Stufen beim strategischen Outsourcing 116

Tabelle 24: Exploitative Allianzen vs. Explorative Allianzen 126

Tabelle 25: Wissensschutz-Referenzmodell bei der ISE 132

Tabelle 26: IT-Projektabhängige und –unabhängige Funktionen 135

Tabelle 27: Modellerweiterungen im Interviewprozess 136

Tabelle 28: Tabellarische Darstellung des Projektumfeldes 139

Tabelle 29: Relevante Wissensschutz Informationen im IT-Projektsteckbrief 143

Tabelle 30: IV-Ergebnis Verhältnis Fachwissen Technologiewissen 146

Tabelle 31: Projektkategorisierung nach Technologie-/Fachwissen im IT-Projekt 147

Tabelle 32: Ergebnisse vom Experteninterview: Akteursgruppen für die Wissenskategorisierung 151

Tabelle 33: Wissenskategorisierung vom Technologie-/Fachwissen in der IT-Beratung 153

Tabelle 34: Bestimmung der absorptiven Kapazität für die Dienstleisterkategorisierung..... 159

Tabelle 35: Bestimmung der Wissensüberlappung für die Dienstleisterkategorisierung 160

Tabelle 36: Kategorisierung des Technologie-/Fachwissens vom Dienstleister..... 161

Tabelle 37: Risikobewertung zum Wissensschutz in einer IT-Beratung 162

Tabelle 38: Erweiterte Projektsteckbrief Projekt α – Fachwissens- und Technologiewissenskombination 166

Tabelle 39: Projekt α - Wissenskategorisierung des Fachwissens 167

Tabelle 40: Projekt α - Wissenskategorisierung des Technologiewissens 168

Tabelle 41: Kombination vom Fachwissen und Technologiewissen im Projekt α 168

Tabelle 42: Projekt α - Dienstleisterkategorisierung nach Gefahrenpotential 168

Tabelle 43: Projekt α - Dienstleisterkategorisierung zum Fachwissen 169

Tabelle 44: Projekt α - Dienstleisterkategorisierung zum Technologiewissen 170

Tabelle 45: Evaluation aus der deployment Perspektive 173

Tabelle 46: Evaluation aus der epistemologischen Perspektive..... 177

Tabelle 47: Evaluation aus der ökonomischen Perspektive - Leistungen 180

Tabelle 48: Funktionen und Akteure beim Wissensschutz 220

1 Einführung

IT-Beratungen unterstützen Unternehmen beim Einführen, Warten und Weiterentwickeln von Informationssystemen. Durch die rasant wachsende Digitalisierung ist nahezu jedes Unternehmen auf Informations- und Kommunikationstechnik angewiesen. Diese Konstellation bringt Chancen wie auch Risiken mit sich. In diesem Zusammenhang beauftragen Wirtschaftsunternehmen IT[1]-Beratungen mit der Digitalisierung der Arbeits- und Geschäftsprozesse im Rahmen von Individual-Software-Entwicklung (ISE)[2], damit sie im Wettbewerb auf den globalen Märkten weiterhin bestehen können. Nur die wenigsten Unternehmen haben das Potenzial diese Herausforderungen im Alleingang und ohne Kooperation zu lösen und die gesamte Vielfalt mit Fach- und Technologiewissen abzudecken.[3]

Ausgehend von der Situation in Abbildung 1, dass ein Wirtschaftsunternehmen (Kunde / Endkunde) eine IT-Beratung mit einem innovativen, wettbewerbsrelevanten und strategisch bedeutenden IT-Projekt beauftragt, um seine Arbeits- und Geschäftsprozesse in Informationssystemen abzubilden, wird notwendigerweise wertvolles organisationales Wissen geteilt. Dieses Wissen basiert auf Informationen und diese wiederum auf Daten. Um diese Informationssysteme bei dieser Projektart für die Auftraggeber zu realisieren, sourct die IT-Beratung Projektaufgaben aus Kostengründen, Flexibilität, limitierten Personalressourcen und Wissenskompetenzen an zum Teil größere, branchenübergreifende, internationale, innovative, lernbereite, lernfähige externe IT-Dienstleister aus.

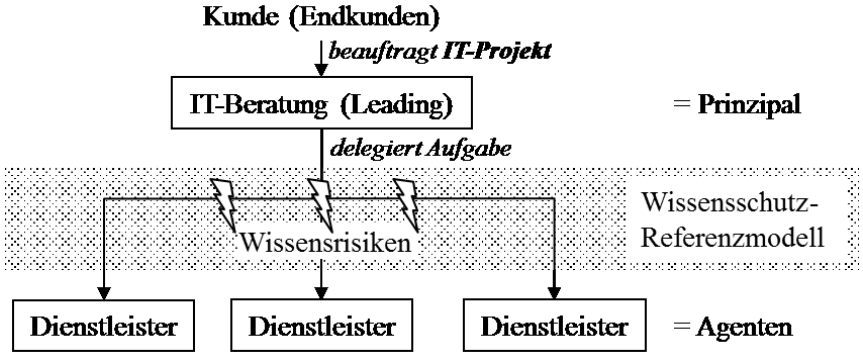

Abbildung 1: Übersicht zum Forschungsobjekt[4]

In einer Agentenbeziehung führen ein oder mehrere Prinzipal(e) mit einem anderen Agenten zusammen eine Dienstleistung aus, die Entscheidungsbefugnisse für den Agenten beinhaltet.[5] Bei dieser Prinzipal-Agenten-Beziehung zwischen IT-Beratung und externen IT-Dienstleister

[1] In der vorliegenden Arbeit wird der Begriff Informationstechnologie (IT) verwendet, da nach Fink et al. (2005, S. 3) „eine Kommunikation (ein Informations- oder Datenaustausch) zwischen Systemen bzw. Systemelementen in der Regel systemimmanent ist." Demnach können die Begriffe Informationstechnologie (IT) und Informations- und Kommunikations-Technologie (IKT) als synonym verwendet werden.
[2] Nach ISO/IEC 2382 wird Software in Systemsoftware, Unterstützungssoftware und Anwendungssoftware gegliedert sowie nach dem Grad der Individualität in Standardsoftware und Individualsoftware.
[3] Vgl. Quintas et al. 1997, S. 389.
[4] Eigene Darstellung.
[5] Vgl. Jensen & Meckling 1976, S. 308.

entstehen Wissensrisiken, die reduziert werden müssen. Sollte die IT-Beratung nicht verantwortungsvoll mit dem wertvollen und schützenswerten Wissen umgehen, wird ihre Wettbewerbsfähigkeit und die des beauftragenden Wirtschaftsunternehmens bedroht und riskiert. Das Risikomanagement und Wissensmanagement einer IT-Beratung sollte die Wissensrisiken erkennen, analysieren, bewerten, überwachen und kontrollieren. Die Prinzipal-Agent-Theorie offeriert im Status Quo keine Antworten auf die Fragen zum Wissensschutz, weshalb das Ziel dieser Arbeit ist, diesen theoretischen Mehrwert herauszuarbeiten.

Ein klassisches Beispiel für diese Art von Wissensrisiko ist die Kooperation von *Apple* und *Microsoft* von 1982 bis 1984. *Apple* beauftragte *Microsoft* mit der Entwicklung von Tabellen, Datenbanken und graphischen Anwendung für den *Mac*. *Microsoft* war vermutlich dadurch in die Lage versetzt sich das wertvolle Wissen zu der GUI (*Graphical User Interface*) anzueignen. Später hat *Microsoft* die Marke *Windows* gegründet.[6] Die von *Apple* eingeleiteten rechtlichen Schritte gegen *Microsoft* waren nicht erfolgreich, weil die Nachweisbarkeit zur Wiederverwendung vom Wissen schwierig möglich ist.

Bei einer Wiederverwendung des aufgenommenen beziehungsweise absorbierten Wissens kombiniert und entwickelt der Dienstleister das Wissen mit seiner Wissensbasis und seinen Erkenntnissen weiter. Durch diese Veränderung und Weiterentwicklung des ursprünglichen Wissens werden die Nachverfolgbarkeit und damit rechtliche Schritte diffizil. Wenn der Prinzipal den Wert seines Wissens nicht kennt und das Wissen leichtfertig mit einem Agenten teilt, dann trägt der Prinzipal zum Wissensfortschritt des Agenten bei.[7] Der ungewollte Wissenstransfer wird vom Prinzipal meist zu spät registriert, wenn bereits wirtschaftliche Folgen für die Wettbewerbsfähigkeit beim Prinzipal oder seiner Auftraggeber eingetreten sind, wie das oben aufgeführte Beispiel *Apple* und *Microsoft* zeigt.

In der oben charakterisierten Geschäftsbeziehung versucht der externe Dienstleister das ergänzende Wissen so schnell wie möglich zu erhalten,[8] denn einzigartiges Wissen ist die wertvollste Ressource eines Unternehmens. Diese Ressource ermöglicht es dem Unternehmen, alle anderen Ressourcen zu entwickeln, einzusetzen und zu verwerfen.[9] An dieser Stelle setzt die vorliegende Arbeit an, indem aus der Perspektive der IT-Beratung ein Wissensschutz-Referenzmodell entwickelt wird, damit diese nicht in eine ähnliche Situation wie beispielsweise *Apple* geraten. Ihr Ziel ist folglich das Entwickeln eines Risikoinformationssystems für den Schutz des wertvollen organisationalen Wissens einer IT-Beratung bei bestehender und zukünftiger ISE mit externen nationalen und internationalen IT-Dienstleistern (Outsourcing[10]).

Wissen, insbesondere technisches Wissen und das Humankapital, ist das wertvollste und schützenswerteste Vermögen einer IT-Beratung, die das Unternehmen befähigen, beim Wettbewerb

[6] Vgl. Norman 2001, S. 51.
[7] Vgl. IP_3, IP_11.
[8] Vgl. Hamel 1991, S. 86.
[9] Vgl. Sofka & Shehu 2009, S. 2, Grant 1996.
[10] Vgl. Abschnitt 4.2.4.

in Führung zu bleiben.[11] Um in diesem Wettbewerb zu bestehen, muss eine IT-Beratung nach außen offen sein, um Informationen und Wissen aus dem Umfeld und dem Markt zu erhalten.[12] Zeitgleich muss eine IT-Beratung ihre Wissensbasis durch Wissensmanagement-Methoden schützen und pflegen.[13] Wenn mit dem organisationalen Wissen leichtfertig umgegangen wird, gefährdet das die Existenz der IT-Beratung.

Im Rahmen dieser Einführung wird die Motivation, die Relevanz, die Forschungslücke und das Forschungsziel detailliert dargestellt. Darauf folgt die Ableitung der Forschungsfragen. Die Einführung schließt mit einem Überblick über den weiteren Aufbau der Promotionsschrift ab (Unterkapitel 1.3).

1.1 Motivation

Die BITKOM-Studie (2015) zum Wirtschaftsschutz, in der der Wissensschutz als eine Teilmenge angesehen werden kann, beziffert den jährlichen wirtschaftlichen Schaden in Deutschland durch mangelnden Wirtschaftsschutz auf 51 Milliarden Euro.[14] In der gleichen Studie wird dokumentiert, dass die IT in allen Unternehmensgrößen mit 34% das zentrale Angriffsziel ist.[15] IT-Beratungen mit mangelndem Wissensschutz riskieren unter anderem Umsatzeinbußen (Verlust von Wettbewerbsvorteilen), Imageschäden bei Kunden oder Lieferanten (negative Medienberichterstattung) und das Abwerben von Mitarbeitern (Mitarbeiterfluktuation).[16] Das Bundesamt für Verfassungsschutz dokumentiert ein unterschätztes Risiko von Innentätern, zu dem auch die Mitarbeiter der externen Dienstleister gehören, da diese oft Vertrauenspositionen innehaben und die Kenntnisse über das wertvolle organisationale Wissen besitzen und nutzen können.[17] Die Arbeit versucht einen Beitrag für diese Problemstellung zu leisten, da der Stand der Forschung hierzu evident unzureichend ist.

Wie bei der oben erwähnten Studie herausgekommen, hat die IT-Branche im Vergleich zu anderen Branchen Besonderheiten. Sie ist hoch komplex und das Potential für radikale Innovation ist wegen der dynamischen Umwelteinflüsse und kurzen Produktlebenszyklen höher.[18] Denn IT-Beratungen befinden sich in einer rapid entwickelnden Umgebung mit marginalen Einstiegskosten für neue Mitbewerber.[19] Im Vergleich zu anderen Branchen besteht eine Besonderheit darin, dass die Konkurrenz keine großen Investitionen in Maschinen tätigen muss. Besonders in der IT-Branche ist es entscheidend, sich im Vorfeld bei Dienstleisterbeziehungen zu reflektieren, welches Wissen mit den externen Dienstleistern geteilt werden kann und welches Wissen in der IT-Beratung verbleiben sollte.[20] Dieses Teilen und Zurückhalten von Wissen

---

[11] Vgl. Olander et al. 2011, S. 606.
[12] Vgl. Quintas et al. 1997, S. 389.
[13] Vgl. Quintas et al. 1997, S. 389.
[14] Vgl. BITKOM 2015, S. 17, alle befragten Unternehmen, die in den letzten zwei Jahren von Datendiebstahl, Wirtschaftsspionage oder Sabotage betroffen waren (n=550).
[15] Vgl. BITKOM 2015, S. 13.
[16] Vgl. BITKOM 2015, S. 17.
[17] Vgl. BfV 2015, S. 18.
[18] Vgl. Olander et al. 2011, S. 597, Koberg et al. 2003, S. 26.
[19] Vgl. Olander et al. 2011, S. 606.
[20] Vgl. Liebeskind 1996, S. 102 ff.

wird in der Literatur als die Unternehmensgrenze[21] definiert. Gleichzeitig sollten laut LIEBESKIND Unternehmen (in Bezug auf diese Arbeit: IT-Beratungen) nur ihr wertvolles Wissen schützen, dass den Schutzaufwand rechtfertigt und die Aufwandskosten amortisiert.[22] Die Zielstellung nur das wertvolle Wissen zu schützen, ist ein Balanceakt für Unternehmen, die mit dem entwickelten Wissensschutz-Referenzmodell adressiert wird. Denn eine IT-Beratung kann nur begrenzt zukünftige Entscheidungen bei den radikalen Innovationen, der dynamischen Umwelt und den kurzen Software-Lebenszyklen treffen.

Das Forschungsobjekt dieser Arbeit ist die IT-Beratung eines internationalen Mobilitätsdienstleisters, die das wertvolle organisationale Projektwissen schützen muss, um seine Wettbewerbsvorteile zu sichern und auszubauen. IT-Beratungen entwickeln unter anderem Individualsoftware und betreuen Informationssysteme für ihre Auftraggeber, um die Arbeits- und Geschäftsprozesse der Auftraggeber mittels IT-Lösungen zu realisieren. Jeder dieser Auftraggeber hat analoge und ebenso differenzierte Anforderungen an seine Informationssysteme. Diese Anforderungen werden in der ISE definiert und umgesetzt. In diesem Zusammenhang sourct die IT-Beratung Projektaufgaben an externe nationale und internationale IT-Dienstleister[23] aus, um unter anderem Kosten zu reduzieren, flexibel zu sein und auf neue Technologien, Kompetenzen, Märkte zuzugreifen.[24] Bei diesem Outsourcen von Projektaufgaben in IT-Projekten wird das Wissen überwiegend unkontrolliert mit dem externen IT-Dienstleister geteilt, da die Projektverantwortlichen kaum Sensibilisierung für den Wissensschutz und damit für den kontrollierten Wissensaustausch haben.

Die Mitarbeiter der externen Dienstleister werden von der IT-Beratung nach dem Tagessatz, der verfügbaren Kapazität, nach den aufgebauten Projekterfahrungen und der Arbeitsqualität ausgewählt. Eine Dienstleisterauswahl auf der Grundlage von Wissensrisiken um Wettbewerbsvorteile für die IT-Beratung und ihre Auftraggeber zu sichern erfolgt nicht, da kaum Wissenssensibilität präsent ist. Das organisationale Wissen ist rar, wertvoll und unersetzlich, deshalb ist sicherzustellen, wie es vernetzt, bewahrt und eingesetzt wird.[25]

Beim Vergleich des Daten-, Informations- und Wissensschutzes nehmen IT-Beratungen umfangreiche Aktivitäten auf sich, um ihre Daten und Informationen zu schützen und investieren Kapital und Ressourcen zur Implementierung von Frameworks zum IT-Service-Management,

---

[21] Vgl. Abschnitt 2.1.3, Abschnitt 4.2.3, Bolisani et al. 2013, Liebeskind 1996, Quintas et al. 1997, Olander et al. 2009, Hamel 1991.
[22] Vgl. Liebeskind 1996, S. 102.
[23] In dem untersuchten Forschungsobjekt (IT-Beratung) werden die Dienstleister auch als Partner bezeichnet. Diese Bezeichnung korrigierte Interviewpartner_10 und verwies auf die korrekte Bezeichnung externe Dienstleister. In der Forschungsliteratur sind ebenso die Begriffe Supplier, Vendor, Lieferant, Partner, Sourcingpartner, Servicepartner und Allianzpartner in diesem Kontext zu finden.
[24] Vgl. Nassimbeni et al. 2012, S. 405.
[25] Vgl. Desouza & Awazu 2004, S. 10.

so zum Beispiel die Zertifizierung nach *Control Objectives for Information and Related Technology* (COBIT[26]) oder *Information Technology Infrastructure Library* (ITIL[27]).[28] Der Daten- und Informationsschutz ist damit strukturiert und unterliegt strengen Kontrollen und Überprüfungen in den IT-Beratungen. Hingegen wird der Wissensschutz in der Praxis und in der Literatur wenig fokussiert.[29] In der Forschungsliteratur orientieren sich die meisten Arbeiten auf einzelne Aspekte des Wissensschutzproblems.[30]

Einerseits ist Wissensschutz aus der Wissensmanagement-Perspektive nach THALMANN & MANHART eine Barriere für den Wissensaustausch. Die empirische Forschung bestätigt jedoch andererseits, dass der erfolgreiche Wissensschutz die organisationale Effizienz signifikant steigert.[31] Diese Sichtweise postulieren HURMELINNA-LAUKKANEN und ELCHE-HOTELANO explizit mit der Aussage, dass die strategische Anwendung von diesen Mechanismen den Wissensaustausch und die Innovations-Performance verbessert.[32]

Der gezielte Einsatz von Wissensschutzmechanismen in Unternehmen mit wissensintensiven Dienstleistungen[33] (*Knowledge-intensive Business Services* - KIBS) wie einer IT-Beratung ist notwendig. Denn diesen KIBS mangelt es an einer geplanten Wissensschutzstrategie, weshalb die Effektivität des Wissensschutzes reduziert wird.[34] Mögliche risikominimierende Maßnahmen sind Wissensschutzmechanismen.[35] Ein wesentlicher Ansatz sind die informellen Wissensschutzmechanismen für KIBS, jedoch sind ihre Auswirkungen auf operative Prozesse und ihre Beziehungen zu Wissensmanagementpraktiken noch wenig erforscht.[36] Im Großen und Ganzen scheint es KIBS-Unternehmen an einer geplanten Wissensschutzstrategie zu fehlen, das die Gesamteffektivität des Wissensschutzes vermindert.[37] Die Verwendung von informellen Wissensschutzmechanismen sollte deshalb durch Analysen genauer untersucht werden, um ihre Reliabilität zu sichern.

Das Forschungsdesiderat reflektiert sich auch in der Forschungsagenda von MANHART & THALMANN.[38] Diese entwickeln auf der Basis eines systematischen *Literature Reviews* eine Forschungsagenda, die sich auf die folgenden fünf Wissensschutz-Themenfelder bezieht:

---

[26] Control Objectives for Information and Related Technology ist ein international anerkanntes Framework zur Information Technology (IT)-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives.
[27] IT Infrastructure Library ist eine Sammlung von Best Practices in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements und gilt inzwischen als internationaler De-facto-Standard im Bereich IT-Geschäftsprozesse.
[28] Vgl. Thalmann & Manhart 2013, S. 1, Thalmann et al. 2012, S. 5487, Manhart & Thalmann 2015, S. 190, Ahmad et al. 2014, S. 38.
[29] Vgl. Väyrynen et al. 2013, S. 34, Thalmann & Manhart 2013, S. 3.
[30] Vgl. Nassimbeni et al. 2012, S. 409.
[31] Vgl. Thalmann & Manhart 2013, S. 2.
[32] Vgl. Hurmelinna-Laukkanen 2011, S. 303, Elche-Hotelano 2011, S. 220.
[33] Im englischen Sprachraum werden diese wissensintensiven Unternehmensdienstleistungen als knowledge-intensive business services (KIBS) bezeichnet. Vgl. Amara et al. 2008, Bolisani et al. 2013. In der Arbeit wird diese Kurzbezeichnung verwendet.
[34] Vgl. Thalmann & Manhart 2013, S. 2, Olander et al. 2011, S. 605, Bolisani et al. 2013, S. 208.
[35] Vgl. Abschnitt 4.2.1.
[36] Vgl. Bolisani et al. 2013, S. 209.
[37] Vgl. Bolisani et al. 2013, S. 208.
[38] Vgl. Manhart & Thalmann 2015, S. 204 f.

- "Opening the black box around the protection of tacit knowledge
- Analysing the phenomena in-depth
- Designing supportive IT
- Viewing knowledge protection through a theoretical lens
- Managing the portfolio of knowledge protection measures more systematically"[39]

Diese sollen in Zukunft von Forschern fokussiert werden, da bisher wenig Veröffentlichungen hierzu existieren. Die Arbeit konzentriert sich hauptsächlich auf das dritte Thema, jedoch existieren auch Ansatzpunkte zu dem ersten und zweiten Punkt. Der konkrete Bezug zu den drei Themenfeldern wird folgend beschrieben. Die vorliegende Arbeit fokussiert den Schutz des *tacit* / impliziten Wissens, das in den IT-Projekten bei der ISE entsteht. Das implizite Wissen ist im hohen Maße personengebunden, in Aktionen verankert, besteht aus Denkmodellen, Überzeugungen und eigenen Perspektiven und ist deshalb für eine Person schwer vermittelbares Wissen.[40] Diese Arbeit analysiert den Wissensschutz in der Tiefe, speziell in einer IT-Beratung, um Erkenntnisse für ein Referenzmodell zu generieren. Ein Referenzmodell kann idealtypisch für die Gestaltungsbeschreibung aller relevanten Prozesse und Strukturen appliziert werden.[41] Mit diesem Wissensschutz-Referenzmodell, das auf dem *Design Science Research* (DSR) Ansatz[42] basiert, werden diese Prozesse und Strukturen deskribiert. Auf der Basis des Referenzmodells könnte ein Risikoinformationssystem als unterstützende IT konstruiert werden. Jedoch empfiehlt es sich, diese Erkenntnisse in die bestehenden Risikoinformationssysteme vom Projektgeschäft zu integrieren.

Des Weiteren wird von TRKMAN & DESOUZA hingewiesen, dass die Risikomanagementforschung[43] beim *Wissen-Teilen* bisher eine geringe Bedeutung hat.[44] Der ungewollte Wissensverlust entsteht häufig bei getroffenen Entscheidungen von Mitarbeitern, die täglich zusammenarbeiten und regelmäßig Kontakt mit Dienstleistern haben. IT-Beratungen müssen den Wissensfluss ihres wertvollen Wissens deshalb überwachen und schützen, damit sie ihre Wettbewerbsposition langfristig sichern und erhalten.[45] Diese Wettbewerbsposition einer IT-Beratung basiert auf dem Fach-, Technologiewissen und den Lösungsideen. Dieses wertvolle Wissen kann für die externen Dienstleister hilfreich sein, damit sie ihre Wissenslücken in Projekten schließen und auf ihrer Roadmap Fortschritte machen.[46] Wenn somit zwei oder mehr Unternehmen bei der zunehmenden und notwendigen Zusammenarbeit Wissen teilen, besteht die Wahrscheinlichkeit einer Wissensschutzverletzung.[47]

---

[39] Manhart & Thalmann 2015, S. 204 f.
[40] Vgl. Chan & Lee 2011, S. 104, Olander et al. 2011, S. 596.
[41] Vgl. Schneider et al. 2008, S. 96.
[42] Der Design Science Research Ansatz von Hevner et al. 2004 wird im Unterkapitel 3.1 beschrieben. Die Anforderungen vom Design Science nach Hevner et al. sind, ein anwendbares, nutzenstiftendes, verständlich aufgearbeitetes Forschungsergebnis zu erarbeiten, das ein relevantes Problem adressiert und einen wissenschaftlichen Beitrag liefert. Vgl. Hevner et al. 2004, S. 82 f.
[43] Vgl. Abschnitt 4.2.4.
[44] Vgl. Trkman & Desouza 2012, S. 2.
[45] Vgl. Trkman & Desouza 2012, S. 5.
[46] Vgl. Drechsler & Natter 2012, S. 440.
[47] Vgl. Trkman & Desouza 2012, S. 5.

1.2 Forschungsziele

Die Fragestellungen der Arbeit schließen genau an dieser Forschungslücke an, da nur wenige und vereinzelte wissenschaftliche Arbeiten zum Wissensschutz auf den Gebieten Referenzmodellierung, KIBS, ISE, implizites Wissen und Risikomanagement existieren.[48] Mit dem Referenzmodell sollen IT-Beratungen mit ihren Projektakteuren befähigt werden, Wissensrisiken bei ISE zu identifizieren und zu erkennen, welche Mechanismen sie einsetzen und nutzen können. Die Leitfrage dieser Arbeit lautet daher:

Wie muss ein Risikoinformationssystem einer IT-Beratung zur Unterstützung des Wissensschutzes bei der ISE mit externen IT-Dienstleistern gestaltet sein?

Die Untersuchungen zum Wissensschutz in der IT-Beratung sind der Wirtschaftsinformatik[49] (WI) zuzuordnen. „Gegenstand der Wirtschaftsinformatik sind Informations- und Kommunikationssysteme in Wirtschaft und Verwaltung (kurz: „Informationssysteme“).“[50] Nach ULRICH wird die WI als angewandte und handlungsorientierte Wissenschaft verstanden, deren Betrachtungsgegenstände aus der betrieblichen Wirklichkeit entnommen werden. Das Ergebnis soll dem Menschen in der täglichen Praxis ein akademisch begründetes Verhalten erlauben.[51] Die WI ist somit eine Wissenschaftsdisziplin, die realwissenschaftliche, formalwissenschaftliche und ingenieurwissenschaftliche Perspektiven integriert.[52]

Die WI verfolgt laut SCHÜTTE „sowohl ein theoretisches Erkenntnis- als auch ein pragmatisches Gestaltungsziel“.[53] Ausgehend von dem identifizierten Defizit und den abgeleiteten Forschungsfragen werden diese zwei Ziele genauer erörtert. Das Erkenntnisziel ist zum einen das theoretische Fundament und stützt das grundlegende Verständnis für die Methoden und die Techniken der Informationssystemgestaltung.[54] Die Arbeit verfolgt das Erkenntnisziel, eine identifizierte Forschungslücke bei der Prinzipal-Agent-Theorie zu bearbeiten. Beim Auswahlprozess (*Signalisieren* und *Screening*) und beim *Monitoring* eines Agenten durch den Prinzipal werden bisher keine Wissensrisiken fokussiert. Dieses Defizit vom mangelnden Wissensschutz beim Prinzipal wird mit *Literature Reviews*, Experteninterviews, Gruppeninterviews und der praktischen Erfahrung des Verfassers genauer untersucht und bearbeitet. Der wissenschaftliche Mehrwert liegt darin, dass die Dienstleisterauswahl, das *Monitoring* und die Risikobewertung bei einer Prinzipal-Agenten-Beziehung im Detail geprüft und weiterentwickelt wird. Der entwickelte Dienstleister-Auswahlprozess bezieht die Wissensrisiken ein und erweitert mit diesem Lösungsansatz die Prinzipal-Agent-Theorie.

---

[48] Vgl. Manhart & Thalmann 2015, S. 204.
[49] Die Information System (IS-) Forschung ist im englischsprachigen Raum das Pendant zu der Wirtschaftsinformatik die hauptsächlich durch behavioristische / verhaltenswissenschaftliche Forschung charakterisiert ist. (Vgl. Palvia et al. 2003, Steininger et al. 2009)
[50] WKWI 1994, S. 80.
[51] Vgl. Ulrich 1984.
[52] Vgl. Lehner et al. 1995, S. 6.
[53] Schütte 2007, S. 63.
[54] Vgl. Becker et al. 2003, S. 11.

Das Gestaltungsziel besteht in der Entwicklung konkreter IT-Artefakte für ein Risikoinformationssystem zur Unterstützung des Wissensschutzes bei der ISE in IT-Beratungen mit externen Dienstleistern. Die Artefakte werden in der gestaltungsorientierten WI als Konstrukte (Konzepte, Terminologien, Sprachen), Modelle, Methoden und Instanzen (Implementierungen als Prototypen oder produktive Informationssysteme) definiert.[55] Um solche Artefakte in der konstruktionsorientierten Forschung zu entwickeln, werden beispielsweise die konstruktivistischen Forschungsmethoden wie die Aktionsforschung, das Prototyping, die Referenzmodellierung und die Simulation angewendet.[56] Das zu konstruierende Wissensschutz-Referenzmodell[57] (Langbezeichnung: Referenzinformationssystemmodell) soll die Zusammenarbeit in IT-Projekten mit nationalen und internationalen IT-Dienstleistern langfristig unterstützen, indem der zu kontrollierende Wissensaustausch sichergestellt wird. Die zu entwickelnden Gestaltungsempfehlungen sollen dabei theoretisch fundiert sein, ebenso sollen die praktischen Erfahrungen des Verfassers in die Arbeit aufgenommen sowie durch Experteninterviews erweitert und durch ein Gruppeninterview validiert werden. Die Zielgruppe des innovativen Artefaktes sind zum einen die Wissenschaftsgemeinschaft, die Interesse an Informationssystemunterstützung hat, und zum anderen IT-Beratungen, die mit externen Dienstleistern in der ISE zusammenarbeiten. Konkrete Personenkreise sind die Führungskräfte, Manager und Projektmanager, die die IT-Projektleistungen in einer IT-Beratung verantworten.

Der Abstraktionsgrad des Referenzmodelles muss so detailliert sein, dass alle grundlegenden Perspektiven des Wissensschutzes in der ISE mit externen Dienstleistern erfüllt werden und sich an die vorliegenden individuellen Bedingungen von IT-Beratungen adaptieren lassen. Das Referenzmodell hat den Anspruch nicht statisch zu sein, sondern dynamisch, flexibel und offen für neue empirische und wissenschaftliche Erkenntnisse.

Die vorliegende Arbeit leistet einen Beitrag zur Bearbeitung dieser Forschungslücke, damit IT-Beratungen und ihre Akteure wissen, wie sie den Wissensschutz in der ISE mit externen nationalen und internationalen Dienstleistern sicherstellen können. Es besteht Bedarf an umfassenderen Frameworks, um den Wissensverlust aus strategischer Perspektive zu adressieren.[58] Zudem gibt es keinen Beweis für einen systematischen und umfassenden Managementansatz zur Identifikation und zum Schutz der Wissensressourcen.[59] Aus diesem Grund erhöhen sich die Bedeutung und die Bedrohungen des Wissens, da solide Planungsmodelle für den Wissensschutz fehlen.[60] Auf der Grundlage des Wissensschutz-Referenzmodells könnte ein Planungsmodell deriviert werden. Dazu müsste die jeweilige IT-Beratung das Referenzmodell in die

[55] Vgl. Österle et al. 2010, S. 4.
[56] Vgl. König et al. 1996, S. 45 f., Wilde & Hess 2007, S. 284.
[57] Unter einem Referenzmodell wird in dieser Arbeit ein Modell verstanden, das „für Anwendungssysteme- und Organisations[system]gestalter Informationen über allgemeingültige zu modellierende Elemente eines Systems zu einer Zeit als Empfehlungen mit einer Sprache deklariert, so dass ein Bezugspunkt für ein Informationssystem geschaffen wird“ (Schütte 1998, S. 69).
[58] Vgl. Ahmad et al. 2014, S. 27.
[59] Vgl. Ahmad et al. 2014, S. 27.
[60] Vgl. Manhart & Thalmann 2013, S. 1, Manhart & Thalmann 2015, S. 191.

etablierten Informationssysteme der strategischen Planung, der Projektplanung, der Dienstleisterauswahl und dem Risikomanagement integrieren. Das Referenzmodell liefert damit eine Empfehlung für die Informationsflüsse und die -verarbeitung in IT-Beratungen.

Damit schließen sich folgende Fragestellungen an.[61] Auf der einen Seite muss eine IT-Beratung für die Erkenntnisse von externen Quellen offen sein und gleichzeitig muss das wertvolle Wissen geschützt werden.[62] Sie muss demnach das wertvolle und schützenswerte Wissen[63] identifizieren, um die Unternehmensgrenze für den Wissensschutz zu definieren.[64]

*Forschungsfrage 1: Wie identifiziert eine IT-Beratung die **Unternehmensgrenze** beim Wissen-Teilen und -Zurückhalten, um den Wissensschutz in der ISE mit externen Dienstleistern sicherzustellen?*

Um zum Beispiel Kosten zu reduzieren, flexibel zu sein und auf neue Technologien, Kompetenzen, Märkte zuzugreifen,[65] werden IT-Projektleistungen an externe nationale und internationale Dienstleister ausgelagert. An der Schnittstelle zwischen der IT-Beratung und dem externen Dienstleister soll das Wissensschutz-Referenzmodell ansetzen, damit das aufgebaute oder aufzubauende Wissen nicht unkontrolliert von den IT-Projekten[66] zum nationalen oder internationalen Dienstleister diffundiert. Diese Forschungsfrage adressiert die erörterte Lücke bei der Prinzipal-Agent-Theorie in Bezug auf den Dienstleister-Auswahlprozess (*Signalisieren*, *Screening* und *Monitoring*).

*Forschungsfrage 2: Mit welchen **externen Dienstleistern** kann eine IT-Beratung in der ISE **zusammenarbeiten,** ohne ihre **Wettbewerbsfähigkeit** oder die ihrer Auftraggeber zu riskieren?*

Die Akteure in einer IT-Beratung sollen befähigt werden, den Wissensschutz anzuwenden. Das heißt, dass die Schlüsselrollen identifiziert werden müssen um den Wissensschutz / Wissensverlust zu überwachen.[67]

*Forschungsfrage 3: Welche **Funktionen** werden den **Akteuren** in einer IT-Beratung beim Wissensschutz **zugeordnet**, damit wertvolles Wissen geschützt werden kann?*

Ist das wertvolle Wissen identifiziert und die Akteure zum Wissensschutz befähigt, können die externen Dienstleister in den ISE-Projekten bewusst eingesetzt werden. In IT-Projekten mit externen Dienstleistern sind die Kosten für den Schutz des wertvollen organisationalen Wissens

---

[61] Vgl. Leitfrage.
[62] Vgl. Norman 2002, S. 178.
[63] Die Definition des wertvollen und schützenswerten Wissens erfolgt im Abschnitt 2.1.1.
[64] Vgl. Abschnitt 4.2.1.
[65] Vgl. Nassimbeni et al. 2012.
[66] Ein Projekt ist ein „Vorhaben, das im Wesentlichen durch Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist, wie zum Beispiel Zielvorgabe, zeitliche, finanzielle, personelle oder andere Begrenzungen, projektspezifische Organisation.“ DIN 69901.
[67] Vgl. Ahmad et al. 2014, S. 31.

gegeben. Diese eingesetzten Aufwände amortisieren sich langfristig und sichern Wettbewerbsvorteile.

Diese Forschungsfragen sind instruktiv für das methodische Vorgehen und das Forschungsziel. Das auf dieser Basis entwickelte Wissensschutz-Referenzmodell soll die Akteure befähigen, das wertvolle organisationale Wissen in einer IT-Beratung zu schützen.

Zum Verständnis sind in der weiterentwickelten Abbildung 2 zusätzlich zu den Beziehungen der IT-Beratung mit ihren Akteuren für die ISE, der Fokus der vorliegenden Arbeit, der steuerbare Wissensschutz und der nicht steuerbare Wissenstransfer visualisiert. Die internen Projektakteure der IT-Beratung, die mit den externen Dienstleistern kollaborieren, können zum Beispiel Projektmanager, Entwickler, fachliche und technische Softwarearchitekten und Testmanager sein. Abhängig davon welchen Qualifikationsbedarf das Projektteam hat, kann der externe IT-Dienstleister verschiedene Rollen im IT-Projekt einnehmen. Der kritische Bereich der Kooperation ist hervorgehoben und ist als *steuerbarer Wissensschutz* gekennzeichnet. Dadurch soll verdeutlicht werden, dass das Wissen das einmal die Unternehmensgrenze verlassen hat, *nicht* mehr von der IT-Beratung *steuerbar* ist. Zu beachten ist, dass sich der *Auftraggeber* (Kunde / Endkunde) der IT-Beratung und andere Auftraggeber der IT-Dienstleister im gegenseitigen Wettbewerb befinden können. Der Einzige, dem diese mögliche Wettbewerbssituation zwischen den Auftraggebern bewusst und bekannt ist, ist der externe Dienstleister, da die anderen Akteure in dieser Konstellation von den Kooperationen oder den Dienstleistungsaufträgen keine direkte Kenntnis besitzen.

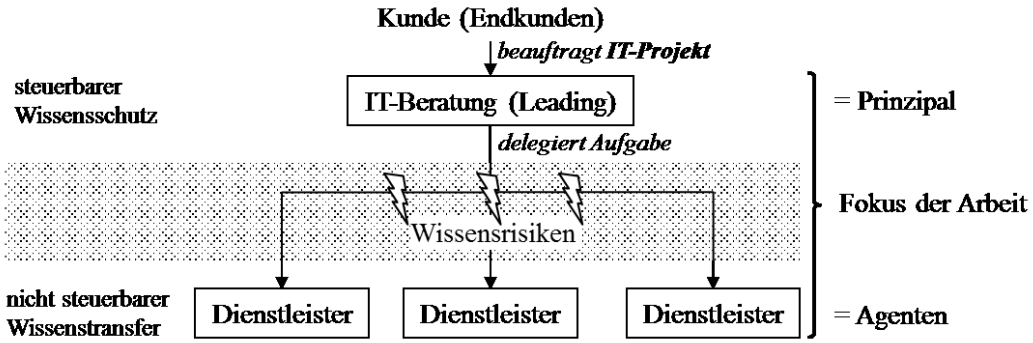

Abbildung 2: Forschungsobjekt sind IT-Projekte mit externen IT-Dienstleistern[68]

An der Schnittstelle *IT-Beratung und externe Dienstleister* setzt das Wissensschutz-Referenzmodell an. Bei der ISE kann Wissen unkontrolliert zum nationalen oder internationalen IT-Dienstleistern diffundieren. Deswegen ist Wissensschutz in IT-Beratungen hoch relevant, jedoch weitestgehend unerforscht.[69]

1.3 Aufbau der Forschungsarbeit

Die Arbeit strukturiert sich in sechs Kapitel (Abbildung 3). Das einleitende erste Kapitel stellt die Motivation, die Forschungsziele und den Aufbau der Arbeit dar. Bestandteil des zweiten

[68] Eigene Darstellung.
[69] Vgl. Kapitel 1.

Kapitels sind die Grundlagen wie Begriffsabgrenzungen zum Wissen, Wissensschutz und die Herleitung einer Wissensschutzstrategiedefinition. Darüber hinaus beschreibt das Kapitel die IT-Beratung, ihre Projektorganisation und setzt sie in Bezug zum Wissensschutz. Zudem wird die theoretische Fundierung des Themas erörtert.

Das dritte Kapitel charakterisiert das Forschungsvorgehen und die -methodik. Dazu gehören die Besonderheiten der Referenzmodellierung von Organisationsgestaltung[70], die methodische Beschreibung der Experteninterviews, des Gruppeninterviews sowie die Datenerhebung der qualitativen Interviews.

Das vierte Kapitel befasst sich mit dem Forschungsstand zum Wissensschutz basierend auf einem *Literature Review* auf. Weiterhin fokussiert dieses Kapitel die relevanten Bereiche der Arbeit wie die Strategie und Planung des Wissensschutzes und die Dienstleisterauswahl.

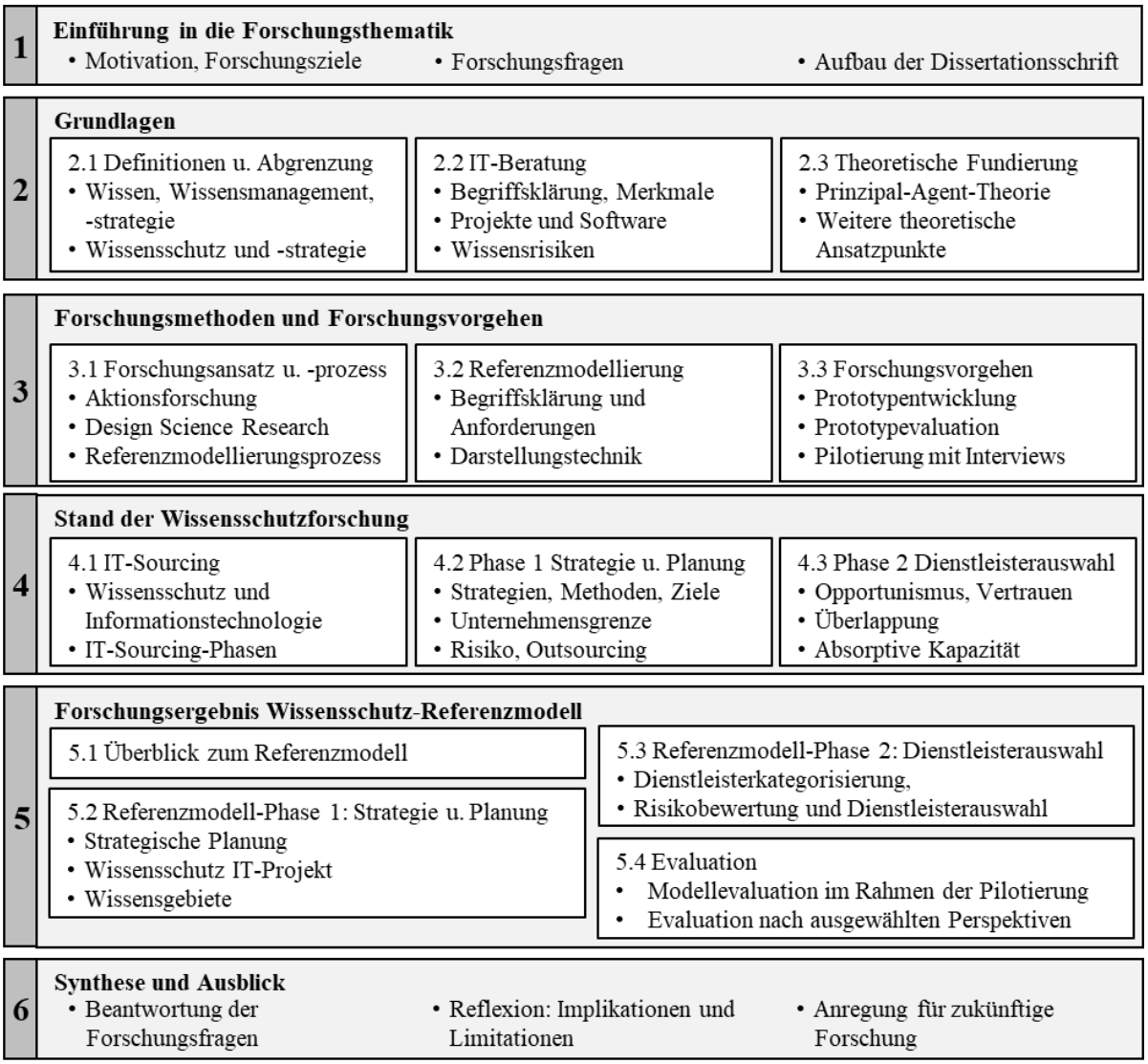

Abbildung 3: Aufbau der Dissertationsschrift[71]

[70] Vgl. Schütte 1998, S. 309 ff., Rosemann & Schütte 1999, S. 23 ff., Schlagheck 2000, S. 201.
[71] Eigene Darstellung.

Im fünften Kapitel erfolgt die Darstellung des entwickelten Wissensschutz-Modells. Dazu gehören alle relevanten Hinweise und Anmerkungen aus der Theorie und Praxis. Die Zusammenfassung und Reflexion des Forschungsvorgehens ist der Inhalt des sechsten Kapitels. Im Rahmen der Dokumentation und Reflexion der erzielten Ergebnisse schließt sich ein Ausblick und Diskussion auf weitere Forschungspotentiale an.

2 Grundlagen

Das Untersuchungsobjekt dieser Arbeit ist eine IT-Beratung eines internationalen Mobilitätsdienstleisters. Die theoretische Fundierung bildet die Referenzmodellierung im DSR. Die inhaltlichen Grundlagen für die Arbeit werden in den folgenden Unterkapiteln und Abschnitten beschrieben.

Zunächst beschreibt und grenzt Unterkapitel 2.1 die Begriffe Daten, Information, Wissen, Wissensarten, organisationales Wissen, wertvolles / schützenswertes Wissen sowie die Wissensträger und die Wissensinhalte ab. Anschließend wird die Definition der Wissensschutzstrategie für die Arbeit herausgearbeitet und die verschiedenen Ansätze zu den Wissensmanagement-Theorien, dem Datenschutz, dem Informationsschutz, der Wissenssicherheit und dem *Intellectual Property (Rights Protection)* dargestellt und diskutiert.

Das Unterkapitel 2.2 ordnet die IT-Beratung als Untersuchungsobjekt der KIBS-Branche zu, deskribiert ihre Merkmale und grenzt sie gegenüber anderen Branchen ab. Anschließend wird eine IT-Beratung definiert und ihre spezifische Projektorganisation beschrieben, mit der das Projektteam die beauftragten Informationssysteme / Anwendungssysteme für ihre Auftraggeber entwickeln kann. Damit sollen die Strukturen und Prozesse transparent werden, in die das Wissensschutz-Referenzmodell integriert wird. Um die ISE für die Auftraggeber in einen Kontext einzuordnen werden die Dimensionen von Dienstleistungen aus der Literatur dargestellt, die IT-Dienstleistungsausprägungen herausgearbeitet und der Individualisierungsgrad beschreibt. Anschließend folgt die Eingrenzung der fokussierten IT-Leistungsbeziehung auf die Anwendungssystemebene und die infrage kommenden betrieblichen Anwendungssysteme auf die sich der Wissensschutz beziehen kann. Ferner wird das Wissensrisiko bei den in der Arbeit relevanten IT-Dienstleistungen unter Beteiligung von externen Beratern dargestellt und transparent gemacht. Die Relevanz des Wissensschutzes und seine Anwendung in IT-Beratungen wird beschrieben. Das letzte Unterkapitel 2.3 elaboriert die besondere Rolle der Prinzipal-Agenten-Beziehung, die den IT-Projekten mit externen Dienstleistern zugrunde gelegt werden kann. Zudem dokumentiert der letzte Abschnitt die weiteren theoretischen Ansatzpunkte der Arbeit.

2.1 Definitionen und Abgrenzung

Zum Grundverständnis werden die Begriffe Daten, Information und Wissen gegeneinander abgegrenzt sowie die Wissensarten (explizites / implizites Wissen) und speziell das organisationale Wissen definiert, da diese Voraussetzung für die Herleitung der Wissensschutz-Definition für diese Arbeit sind. Die Aussagen zum Wissensschutz und der Abgrenzung zu *Intellectual Property (Rights) Protection* werden dokumentiert. Das Unterkapitel schließt mit der Definition zur Wissensschutzstrategie ab.

2.1.1 Wissen

Zeichen, die in einem regelbasierten Kontext stehen, sind Daten.[72] Daten sind wiederum aufgezeichnete, unverarbeitete, unanalysierte und ungetrennte Muster ohne Bedeutung, sie leisten jedoch einen Beitrag zu Auswertungsverfahren.[73] Durch die Datenaggregation mittels der Anwendung von mathematischen, statistischen oder logischen Prozess-Techniken werden Informationen erschaffen.[74] Infolge der Verknüpfung von Informationen und Erfahrungen entsteht Wissen, das dazu verwendet wird Situationen zu interpretieren und Handlungen abzuleiten.[75]

Für die Arbeit wird die Wissensdefinition von DAVENPORT & PRUSAK zugrunde gelegt, weil diese mit ihren Verweisen auf Erfahrungen, Fachkenntnisse und Strukturrahmen indirekt auf das erarbeitete wertvolle Fach- und Technologiewissen eingeht, das in den IT-Projekten zur ISE verwendet wird:

> „Wissen ist eine fließende Mischung aus strukturierten Erfahrungen, Wertvorstellungen, Kontextinformationen und Fachkenntnissen, die in ihrer Gesamtheit einen Strukturrahmen zur Beurteilung und Eingliederung neuer Erfahrungen und Informationen bietet.“[76]

In Unternehmen mit KIBS ist Wissen eine zentrale Ressource. Wissen ist nach FRIED & BAITSCH die einzige Ressource, die sich durch Gebrauch vermehrt, die die Einzigartigkeit eines Produktes beziehungsweise eines Unternehmens begründen kann und weitere Innovationen hervorbringt.[77] Wissen wird immer schneller generiert und im Verhältnis zu natürlichen Ressourcen nicht knapp. Das Wissen ist personengebunden und erfordert die ganzheitliche Fähigkeit von Personen, die es interpretieren, in einem Kontext anwenden und in Handlungen umsetzen.[78] Die Fähigkeit, Daten in Wissen zu transformieren und dieses für das Unternehmen vorteilhaft einzusetzen, macht das Individuum zum zentralen Träger der organisationalen Wissensbasis. Es reicht nicht aus, ausschließlich die Wissensbasis zu betrachten. Viele der Prozesse, die die Grundlage für das erfolgreiche Agieren von Unternehmen schaffen, beinhalten Elemente kollektiven Wissens. Denn Wissen ist nicht greifbar, grenzenlos und dynamisch und kann nicht gelagert werden. Es muss benutzt werden, wenn es Wert erzeugen soll.[79] Daten, Information und Wissen sind die Vorrausetzung für die Abwicklung der Geschäfts- und Produktionsprozesse. Ebenso bilden sie die Basis für Management-Entscheidungen, Kundenbeziehungen und auch für den Erfolg im Wettbewerb. Denn Mitarbeiter wenden circa sechzig bis neunzig Prozent ihrer Zeit mit dem Umgang von Daten, Informationen und Wissen auf.[80]

---

[72] Vgl. Krcmar 2015, S. 11.
[73] Vgl. Trkman & Desouza 2012, S. 3.
[74] Vgl. Trkman & Desouza 2012, S. 3.
[75] Vgl. Maier 2007, S. 64 f., Krcmar 2015, S. 15.
[76] Vgl. Davenport & Prusak 1998, S. 32.
[77] Vgl. Fried & Baitsch 2000, S. 33.
[78] Vgl. Stelzer 2014.
[79] Vgl. Nonaka 2001.
[80] Vgl. Ballod 2009, S. 4.

Wissensarten

Das Wissen lässt sich in explizites und implizites Wissen (*Tacit Knowledge*) kategorisieren.[81] *Tacit Knowledge*[82] ist in hohem Maße personengebunden, in Aktionen verankert und besteht aus Denkmodellen, Überzeugungen und eigenen Perspektiven und ist deshalb für eine Person schwer vermittelbares Wissen.[83] Explizites Wissen ist formal, systematisch und kann leicht innerhalb von Gemeinschaften kommuniziert und geteilt werden.[84] Dieses Wissen befindet sich in Dokumenten und Datenbanken mit anderen abgelegten Informationen.[85] Der Fokus der vorliegenden Arbeit wird auf den Schutz des impliziten Wissens gelegt. Weitere unterschiedliche Wissensarten und ihre Autoren sind in der Tabelle 1 vergleichend dargestellt.

Tabelle 1: Wissensarten und ihre Autoren[86]

Wissensarten	Autor(en) / Studien
1. Tacit 2. Explicit	Polanyi 1968, Nonaka & Takeuchi 1995
1. Individual 2. Collective	von Krogh 2009
1. Individual 2. Social	Russell 1948
1. Embrained 2. Embodied 3. Encultured 4. Embedded 5. Encoded	Blackler 1995
1. Codified 2. Personalised	Hansen et al. 1999
1. Information 2. Know-how	Kogut & Zander 1992
1. Know-what 2. Know-how 3. Know-why 4. Care-why	Quinn et al. 1996

Organisationales Wissen

In der bestehenden Literatur wird organisationales und individuelles Wissen voneinander abgegrenzt. „Dabei liegen verschiedene ebenso konstruktivistisch geprägte und beeinflusste Verständnisse zum organisationalen Wissen und organisationalen Lernen vor.“[87] So definiert NONAKA, als ein Vertreter der *Knowledge-based View*[88], organisationales Wissen als Wissen,

[81] Vgl. Chan & Lee 2011, S. 100.
[82] "We can know more than we can tell." (Polanyi 1966, S. 4). Vgl. Polanyi 1958 und Gelwick 1977.
[83] Vgl. Chan & Lee 2011, S. 104, Olander et al. 2011, S. 596.
[84] Vgl. Olander et al. 2011, S. 596.
[85] Vgl. Olander et al. 2011, S. 596.
[86] Ilvonen 2013, S. 23.
[87] Bouncken 2003, S. 3.
[88] Vgl. Abschnitt 2.3.2.

das durch den kontinuierlichen Dialog zwischen *tacit* Wissen und explizitem Wissen entsteht.[89] Für BLOODGOOD & SALISBURY hingegen kann organisationales Wissen in Individuen und Personengruppen existieren, oder es kann ein organisationsweites Phänomen wie eine organisationale Routine sein.[90]

Die Arbeit folgt dem Ansatz, dass das organisationale Wissen in einer Personengruppe existiert und damit kollektiv sein kann. Die Organisationsmitglieder oder technischen Systeme können die verschiedenen Wissensträger laut BOUNCKEN sein, die geteilte Repräsentationen besitzen. Weiterhin entsteht dieses organisationale Wissen mit Referenz auf eine Organisation, das heißt „bei dem die Organisation den Kontext und den Modus bildet, in dem organisationales Wissen entsteht".[91] Für die Arbeit bedeutet das, dass die IT-Projektakteure und die technischen Systeme in Form von ISE die Wissensträger vom organisationalen Wissen sind. Die Systeme, die im Rahmen der ISE aus den IT-Projekten entstanden sind, prägen eine IT-Beratung.

Das organisationale Wissen bildet sich nach GRANT durch die Interaktionen zwischen Individuen heraus. Somit entsteht es bei der Kollaboration zwischen dem Projekt-Auftraggeber und den IT-Projektakteuren in den fünf Projektphasen[92]. Zu diesem organisationalen Wissen gibt es bisher wenig Hinweise, wie Manager diese Interaktionsprozesse beeinflussen können.[93] Für die Führungskraft einer IT-Beratung dokumentiert das Modell ein Vorgehen, um das wertvolle und schützenswerte organisationale Fach- und Technologiewissen in der ISE zu identifizieren und zu schützen. Damit kann sichergestellt werden, dass dieses Wissen von den internen IT-Projektakteuren bearbeitet und nicht an externe Dienstleister weitergegeben wird.

Wertvolles und schützenswertes Wissen

Das *valuable organizational knowledge*[94], so bezeichnet es LIEBESKIND, muss vor äußeren Fremdinteressen geschützt werden.[95] Denn Unternehmen müssen in einer Netzwerkbeziehung, wie es eine Prinzipal-Agenten-Beziehung ist, ihr *valuable organizational knowledge* schützen, indem sie ihre Wissensflüsse überwachen, wenn sie langfristig ihre Wettbewerbsposition erhalten und ausbauen wollen.[96] Das sicherzustellen ist ein bedeutsames Ziel des Wissensschutz-Referenzmodells. Damit die IT-Beratung identifizieren kann, welches Wissen wertvoll und schützenswert ist, gibt es verschiedene Ansätze. Für SOFKA & SHEHU ist Wissen nur wertvoll, wenn es in gewissen Kontexten repliziert werden kann. Dieses komplexe Wissen ist schwieriger zu transferieren, da es den gleichzeitigen Transfer von Zusatzwissen erfordert.[97] Wenn ein Dienstleister in einem IT-Projekt beteiligt wird, erhält er dieses notwendige Zusatzwissen. Einen weiter gefassten Ansatz verfolgen OLANDER et al. Nach ihnen ist das technische Wissen

[89] Vgl. Nonaka 1994, S. 14 f.
[90] Vgl. Bloodgood & Salisbury 2001, S. 58, Cohen et al. 1996, Nelson & Winter 1982, Nonaka & Takeuchi 1995.
[91] Bouncken 2003, S. 4.
[92] Vgl. Tabelle 5.
[93] Vgl. Grant 1996, S. 113.
[94] Vgl. Liebeskind 1997, S. 650.
[95] Vgl. Desouza & Awazu 2004, S. 11.
[96] Vgl. Trkman & Desouza 2012, S. 5.
[97] Vgl. Sofka & Shehu 2009, S. 3 f.

und das Humankapital das wertvollste und schützenswerteste Vermögen, die das Unternehmen befähigen, beim Wettbewerb in Führung zu bleiben.[98] Auf den Grundgedanken von OLANDER et al. stützt sich ein Kernelement des entwickelten Referenzmodells, in dem das Fachwissen und Technologiewissen der IT-Projekte identifiziert und bewertet wird.

Die Forschungsliteratur und deren verschiedenen Autoren zum Wissensschutz verwenden die Begriffe wertvolles (Kern-)Wissen[99] und wertvolle Ressource[100] im Zusammenhang mit Kernkompetenzen[101] oder ebenso Kern-(wettbewerbs)Ressource[102] als Synonym für schützenswertes Wissen. Aus diesem Grund wurde ebenso die Literatur zum Schutz von Kernkompetenzen geprüft, um domänenübergreifend Erkenntnisse in das Referenzmodell aufzunehmen.[103] In der Praxis stellt es sich so dar, dass schützenswertes Wissen zu einer Kernkompetenz gehören kann.

Wissensträger, Wissensinhalte und Wissenstransfer

LINDEMANN et al. untergliedern Wissen in Wissensträger und -inhalte. In den Wissensträgern kann sich Wissen manifestieren, Wissensträger sind stofflicher Natur und sie transportieren Wissensinhalte. Die Wissensinhalte definieren sich über den Sachverhalt über den das Wissen besteht.[104] In der Tabelle werden die unterscheidbaren Wissensträger definiert. Die für diese Arbeit relevanten Wissensträger (Tabelle 2) und Wissensinhalte (Tabelle 3) sind hervorgehoben.

Tabelle 2: Einteilung in Wissensträger105

Wissensträger	Erläuterung
Kollaboratives Wissen	nur in der Zusammenarbeit mehrerer Personen nutzbares Wissen
Persönliches Wissen	bestehendes Wissen einer Person, das unter Einbeziehung und Übernahme neuer Informationen laufend weiter entwickelt wird
Dokumentiertes Wissen	tritt in der Investitionsgüterindustrie in elektronischen Dateien oder papiergebunden auf
Produktgebundenes Wissen	ist in Produkten/Komponenten hinterlegt und an diese Artefakte gebunden

Die zu entwickelnden Informationssysteme, die in den IT-Projekten entstehen, beinhalten das kollaborative, persönliche und produktgebundene Wissen. Das dokumentierte Wissen steht nicht im Fokus dieser Arbeit, da es sich im Vergleich zu den anderen Wissensträgern (implizites Wissen) um explizites Wissen handelt.

Hervorzuheben ist, dass sich LINDEMANN et al. auf den Schutz von Technologiewissen fokussieren und sie definieren diesen als eine Ansammlung heterogener Wissensinhalte. Die verschiedenen Arten von Wissensinhalten sind in der folgenden Tabelle 3 detailliert dargestellt.

[98] Vgl. Olander et al. 2011, S. 606.
[99] Vgl. Bloodgood & Salisbury 2001, Belsis et al. 2005, Jennex & Zyngier 2007, Hurmelinna-Laukkanen 2011.
[100] Vgl. Grant 1996, Gold et al. 2001.
[101] Vgl. Kale et al. 2000, Desouza & Vanapalli 2005, Chan & Lee 2011.
[102] Vgl. Bolisani et al. 2013.
[103] Vgl. Abschnitt 4.2.3.
[104] Vgl. Lindemann et al. 2012, S. 17.
[105] Lindemann et al. 2012, S. 17.

Diese lassen sich dem relevanten Technologiewissen und Fachwissen in den IT-Projekten der IT-Beratungen zuordnen. Sekundären Fokus hat die letzte Kategorie der übergeordneten Wissensinhalte (Lebenszyklus und Betrieb), da diese erst in der Wartung und Weiterentwicklung relevant wird und die ISE bereits abgeschlossen ist. In den IT-Projekten werden zum Beispiel die konkreten Technologiewissensgebiete *Java*, *C++*, *Big Data*, *Software as a Service*, Cloud-, Datenbank-, Mobile- und Firewall-Technologien verwendet.

Tabelle 3: Verwendete Einteilung von Wissensinhalten[106]

Einordnung in übergeordnete Wissensinhalte	Einteilung in detaillierte Wissensinhalte
Produktgestalt und Produkteigenschaften	• Gestalt oder Softwarecode • Eigenschaften und Modelle • Kombination von Komponenten oder Materialien • Komponenten- und Materialwahl • Stück- und Materiallisten
Prozessabläufe	• Dokumentation • Normung • Messungen, Tests oder Überprüfungen • Handwerkliche Grundlagen • Fertigung und Montage • Software-Programmierung • Handhabung der Arbeitsumgebung • Werkzeuge und deren Einsatz • Beschaffung von Kompetenzen und Materialien • Informationsgewinnung • Ressourcenmanagement
Gründe für Gestaltungsentscheidungen (Design Rationale)	• Demontage und Zusammenbau • Versagensarten (Produkt) • Eigenschaftsvorhersage, Simulation • Versagensarten (Komponenten, Material) • Mathematisches, technisches und naturwissenschaftliches Hintergrundwissen • Gestaltungsphilosophie • Frühere Konstruktion ähnlicher Produkte
Produktfunktion	• Kundenbedürfnisse • Versagenssymptome • Funktionale Modelle
Organisatorische Zusammenhänge und Ansprechpartner	• Vorhersagen menschlichen Verhaltens • Quellen für Ingenieurwissen und -fähigkeiten
Lebenszyklus und Betrieb	• Verkauf • Anwendungen • Betrieb • Instandhaltung • Reparatur oder Modifizierung • Diagnose • Verpackung, Lagerung, Transport

„Die Wissensübermittlung von einem Wissensgeber an einen Wissensempfänger wird als Wissenstransfer bezeichnet. […] Wissenstransfersituationen sind betrieblicher, persönlicher, orga-

[106] Lindemann et al. 2012, S. 18 f.

nisatorischer oder produktbezogener Natur und beinhalten einen Mechanismus des Wissenstransfers."[107] Bei der Beteiligung von externen Beratern in den IT-Projekten kommt es zu einer Wissenstransfersituation. Mit Hilfe der Darstellung der Wissensträger wird deutlich, wo das *Tacit Knowledge* von der ISE präsent ist. Die Wissensinhalte in der Tabelle 3 geben erste Hinweise auf die Wissenskomplexität des Wissensschutzes in der betrieblichen Praxis.

Zusammenfassend ist auf der Grundlage der Wissensabgrenzung und den Definitionen zum organisationalen Wissen herauszustellen, dass das Wissen als bedeutender Produktionsfaktor angesehen wird. Zudem ist hervorzuheben, dass die Literatur das wertvolle und schützenswerte organisationale Wissen im Zusammenhang mit Kernkompetenzen verwendet.

2.1.2 Wissensmanagement und -strategie

Unternehmen organisieren immer schon den Umgang mit Wissen, ohne dass der Begriff Wissensmanagement[108] (WM) verwendet wurde. Beispiele sind Weiterbildung oder Unternehmensentwicklung und ebenso Aktenpläne oder Ablagesysteme. Ebenso sind Teile des Qualitätsmanagements oder der Einführung elektronischer Informationssysteme als Wissensprozesse zu nennen. Das WM unterstützt das strategische Management bei IT-Entscheidungen. Für Entscheidungen werden leicht zugängliche Informationen benötigt. Der Zugriff auf die Informationen muss zur richtigen Zeit am richtigen Ort erfolgen.[109] Jeder Mitarbeiter braucht zudem Zugang zu Organisationseinheiten übergreifendem Wissen, das für ihn relevant ist. Eine lange Suche und umständliche Beschaffungswege wirken hemmend auf die Motivation und die Arbeitsatmosphäre. Die Führungskräfte und Mitarbeiter benutzen zur Erfüllung ihrer Aufgaben bereits das persönliche Wissen, kollektive Wissen, das Wissen der Lieferanten, Dienstleister, Partner und Kunden. In der täglichen Zusammenarbeit ist Wissen daher nichts Neues. WM ist kein Selbstzweck, sondern wird für den Ausbau des Unternehmenserfolges gebraucht. Wissen stellt ebenso einen immateriellen Vermögenswert von Unternehmen dar. In wissensintensiven Dienstleistungsunternehmen[110] kann dem Wissen aus der ISE demzufolge eine bedeutende Rolle zugeordnet werden.

Weltweit gibt es über 150 WM-Konzepte, die empirische Forschung und praktische Erfahrung beinhalten.[111] Hinzuweisen ist auf die vielfach zitierten Prozesse des Wissensmanagements wie die Spirale der Wissensschaffung im Unternehmen von NONAKA & TAKEUCHI[112] und die Bausteine des Wissensmanagements von PROBST et al.[113]. Ein für die Arbeit relevantes WM-Modell, die Wissenstreppe, wird folgend beschrieben, weil es für die Arbeit die Begrifflichkeiten

---

[107] Lindemann et al. 2012, S. 20.
[108] Wissensmanagement ist seit der DIN EN ISO Norm 9001:2015 verpflichtend für Unternehmen: http://www.community-of-knowledge.de/beitrag/wissensmanagement-im-kontext-mit-der-neuen-iso-norm-90012015/.
[109] Vgl. Mertins et al. 2009, S. 18.
[110] Vgl. Abschnitt 2.2.1.
[111] CEN / ISSS Knowledge Management Workshop 2004, S. 13.
[112] Nonaka & Takeuchi 1997, S. 87.
[113] Probst et al. 1999, S. 58.

visuell abgrenzt. Die ersten Stufen, Daten, Information und Wissen (siehe Wissenstreppe) wurden bereits im vorangegangenen Unterkapitel genauer erläutert. Die nächste Stufe nach dem Wissen ist Handeln. Erst, wenn das Wissen *Know-how* in die Praxis umgesetzt werden kann, hat das Wissen einen Wert für das Unternehmen. Die Wissenstreppe wird vom strategischen WM von oben nach unten durchlaufen. Bei diesen Schritten ist zu klären, welches Wissen und welche Kompetenzen gebraucht werden, um die Wettbewerbsziele des Unternehmens zu erreichen. Im Zusammenhang damit steht das operative Geschäft, dass die Koordinierung von Daten, Informationen und Wissen beinhaltet.[114] Zu dem operativen Geschäft gehört ebenso die Realisierung der IT-Projekte.

NORTH & REINHARDT weisen darauf hin, dass alle Stufen der Wissenstreppe zu gestalten sind. Sollte eine Stufe der Treppe nicht realisiert sein, so *stolpert* das Unternehmen.[115]

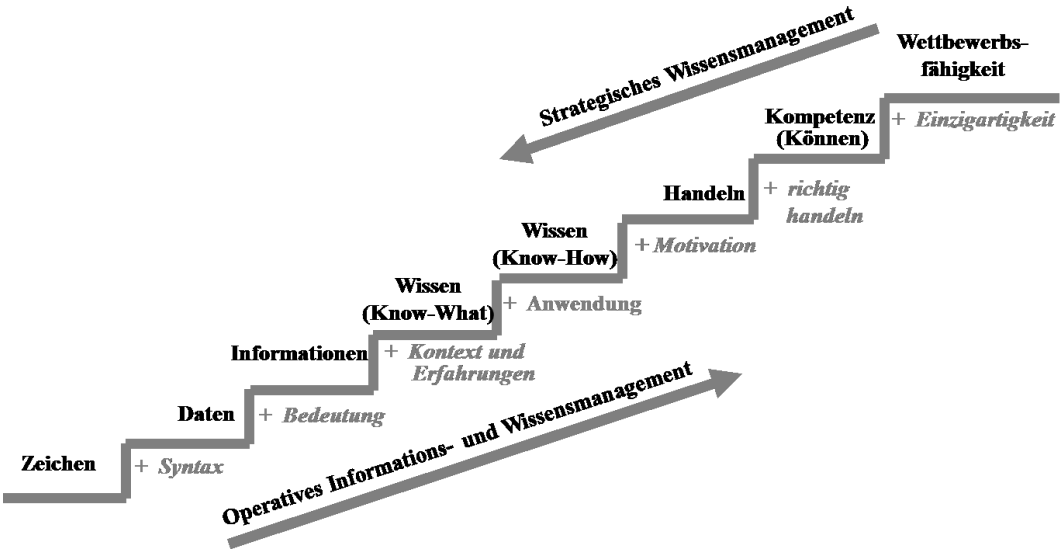

Abbildung 4: Die Wissenstreppe[116]

Ein strategisches WM verbessert die übergreifende Zusammenarbeit in Teams, Abteilungen, Geschäftsbereichen sowie der Projektabwicklung in bereichsübergreifenden Großprojekten. Ein WM-System „funktioniert dann richtig, wenn der Anwender praktisch davon nichts merkt."[117]

WM ist ein relativ junges Forschungsfeld, das viele verschiedene Definitionen umfasst.[118] Nach MAIER wird WM wie folgt definiert.

> "Knowledge management is defined as the management function responsible for the regular selection, implementation and evaluation of goal-oriented knowledge strategies that aim at improving an organization's way of handling knowledge internal and external to the organization in order to improve organizational performance. The implementation of knowledge strategies

[114] Vgl. North & Reinhardt 2005, S. 31.
[115] Vgl. North & Reinhardt 2005, S. 32.
[116] North & Güldenberg 2008, S. 25.
[117] Kampffmeyer 2014, S. 3.
[118] Vgl. Manhart & Thalmann 2015, S. 192.

> comprises all person-oriented, organizational and technological instruments suitable to dynamically optimize the organization-wide level of competencies, education an ability to learn of the members of the organization as well as to develop collective intelligence." [119]

Demnach ist es die Aufgabe von Managern regelmäßig eine Auswahl, Umsetzung und Evaluierung von geeigneten Wissensstrategien vorzunehmen, um eine höhere organisatorische Leistungsfähigkeit zu erzielen, da der interne und externe Wissensumgang optimiert wird. Nach SCHULTZE & LEIDNER beinhaltet WM die Generierung, Darstellung, Speicherung, Übertragung, Transformation, Anwendung, Einbettung und Schutz von organisationalem Wissen.[120] Wissen muss nach dieser WM-Definition geteilt und geschützt werden. DESOUZA & AWAZU beschreiben diese Konfliktsituation und konkretisieren sie:

> "Knowledge needs to be shared and protected. It needs to be shared with the right agents within and without the organization and, by the same token, must be protected from an organization's competitors." [121]

Demnach kommt es darauf an, dass Wissen mit den richtigen Dienstleistern außerhalb der IT-Beratung zu teilen, um es gleichzeitig vor Wettbewerbern zu schützen.

Wissensmanagement-Strategie

Die Entwicklung einer präventiven Strategie hilft dem Unternehmen zu erkennen, was zu tun ist, wohin es gehen soll und was zu planen ist, um zum Ziel zu gelangen.[122] Eine Strategie definiert den Umfang der Absichten eines Unternehmens, insbesondere in Bezug auf die Mobilisierung von Fachwissen, um die Innovationsfähigkeit auszubauen.[123] Dieses Fachwissen und damit die Innovationsfähigkeit werden in den Auftraggeber IT-Projekten generiert und aufgebaut. Unternehmen ohne eine präventive Strategie reagieren auf kurzfristige Chancen, ohne die mittel- und langfristige Ziele zu erreichen.[124] Basierend auf dieser Aussage nehmen AMARA et al. an, dass KIBS-Unternehmen[125] mit einer Strategie auf wettbewerbsorientierte Herausforderungen reagieren, indem sie WM-Strategien hinsichtlich des Einsatzes von Wissen entwickeln, das in fortschrittlichen Technologien und Wertschöpfungspraktiken verkörpert ist. Diese WM-Strategien können die Wahrscheinlichkeit erhöhen unterschiedliche Innovationsformen zu entwickeln.[126]

BLOODGOOD & SALISBURY weisen darauf hin, dass Unternehmen identifizieren sollten, wo sich das Wissen befindet, wenn sie über ihre Strategien nachdenken, um ebenso sicherzustellen, dass

---

[119] Maier 2007, S. 57.
[120] Vgl. Manhart & Thalmann 2015, S. 192, Schultze & Leidner 2002.
[121] Desouza & Awazu 2005, S. 29.
[122] Vgl. Amara et al. 2009, S. 414.
[123] Vgl. Amara et al. 2009, S. 414.
[124] Vgl. Amara et al. 2009, S. 414, Miles & Snow 1978.
[125] Vgl. Abschnitt 2.2.1.
[126] Vgl. Amara et al. 2009, S. 414.

das Wissen in der richtigen Weise und mit den richtigen Personen erstellt, übertragen und geschützt wird.[127] Um den Ort des Wissens im Unternehmen zu identifizieren werden im Abschnitt 4.2.3 die bestehende Literatur analysiert und die relevanten Modelle und Algorithmen für das Referenzmodell herangezogen.

Im Jahr 2005 haben JENNEX & OLFMAN zwölf kritische Erfolgsfaktoren für WM und -systeme aus 17 Studien mit über zweihundert WM-Projekten zusammengefasst und synthetisiert. Die Sicherheit und der Schutz des Wissens sind auf dieser Liste der kritischen Erfolgsfaktoren an zwölfter und damit letzter Stelle zu finden.[128] Für LEE et al. ist der Wissensschutz sogar genauso kritisch und bedeutsam zu sehen wie die Rolle von Innovationen in Unternehmen.[129] Jedoch zeigt die Wissensschutzforschung von 2014 auf, dass die komplexe Frage des Wissensschutzes häufig im Management übersehen wird und die Wissensschutzverantwortung beim Wissenseigentümer liegt.[130] Die internen Projektakteure, die Wissenseigentümer sind, brauchen die strategischen Zielvorgaben des Managements, damit der Wissensschutz im IT-Projekt mit externen Beratern funktionieren kann. Nach MANHART & THALMANN besteht die Notwendigkeit, dass der Wissensschutz in die WM-Strategie mit den strategischen Schutzzielen integriert wird.[131] Die WM-Strategie bezieht sich demnach auf eine Reihe von Entscheidungen und Aktionen, die überlegene Leistungen zum Ziel haben und als Ergebnis soll sie einen Wettbewerbsvorteil gegenüber den Mitbewerbern erarbeiten.[132]

Zusammenfassend ist darzulegen, dass aufbauend auf verschiedenen WM-Definitionen auf die WM-Strategie und ihren Erfolgsfaktor Wissensschutz verwiesen wird. Damit ist für die Arbeit belegt, dass der Wissensschutz Bestandteil der WM-Strategie sein sollte.

2.1.3 Wissensschutz und -strategie

Aufbauend auf der Wissensabgrenzung, den Wissensarten und dem WM folgen die für die Arbeit relevanten abgrenzenden Aussagen zum Daten-, Informationsschutz, Wissenssicherheit und *Intellectual Property (Rights Protection)*, die im Vergleich zum Wissensschutz nicht im Fokus der Arbeit sind.

Datenschutz und Schutz von Daten

Der Datenschutz hat das Ziel den „Schutz des Persönlichkeitsrechts des Einzelnen vor einer Beeinträchtigung durch die Verwendung von ihn betreffenden Daten. Die Geheimhaltung betrieblicher Daten ist also keine Frage des Datenschutzes.“[133] Der Schutz von Daten hingegen

[127] Vgl. Bloodgood & Salisbury 2001, S. 58.
[128] Vgl. Jennex & Zyngier 2007, S. 49, Jennex & Olfman 2005.
[129] Vgl. Lee et al. 2007, S. 58.
[130] Vgl. Ahmad et al. 2014, S. 28.
[131] Vgl. Manhart & Thalmann 2015, S. 192.
[132] Vgl. Amara et al. 2009, S. 414, Porter 1996.
[133] Mertens et al. 1997, S. 120.

bedeutet den Schutz vor Verlust, Manipulation, Missbrauch und Nicht-Verfügbarkeit von Daten.[134] Um diese Schutzvoraussetzungen zu gewährleisten, liegt der Fokus auf Computer- und Netzwerksicherheitsmaßnahmen.[135]

Informationsschutz und Schutz von Informationen

DESOUZA sieht Wissensschutz als den Übergang zwischen WM und Informationsschutz.[136] Nach VÄYRYNEN et al. ist Informationsschutz die Basis für den Wissensschutz. Die beiden Begriffe werden oft im Austausch verwendet, da nach ihren Untersuchungen nur wenige Autoren deutlich zwischen beiden Begriffen unterscheiden.[137] Der Informationsschutz ist ein Teilgebiet der Informationssicherheit.[138] Im Fokus stehen elektronische, schriftliche und verbale kommunizierte Informationen.[139] Dabei sollen bewusst oder unbewusst menschliches Fehlverhalten und technische Unzulänglichkeiten vermieden werden. Das Ziel ist der Schutz von technischen Systemen, organisatorischen Methoden und Prozessen. Der Schutz von Informationen hingegen gehört zum IT-Sicherheitsmanagement sowie dem IT-Grundschutz-Katalog.[140] Dieser erfordert die gleichen Aktivitäten, die für den Schutz eines Produktes notwendig sind.[141] Die Produkte können zum Beispiel Finanzreports oder Produktionsfaktor sein, die zur Entscheidungsvorbereitung von Aktionen erforderlich sind.[142]

Wissenssicherheit

Der Wissensschutz muss vom umfassenden Wissenssicherheits-Konzept differenziert werden, welches die externe und interne Vertraulichkeit, Integrität und Zugänglichkeit von Wissen beinhaltet.[143] Die Wissenssicherheit wird von DESOUZA als die Überlappung vom WM und der Informationssicherheit angesehen,[144] da nach diesem Konzept das Unternehmen eine Sicherheitsperspektive auf den Wissenstransfer anwenden sollte.[145] Diese Sichtweise zu den überlappenden Theorien ist in Abbildung 5 visualisiert und wurde von ILVONEN in ihrer Arbeit übernommen.

[134] Vgl. Levitin & Redman 1998, S. 90, Maier et al. 2005, S. 127 f.
[135] Vgl. Schneier 2001, S. 113.
[136] Vgl. Desouza 2006, S. 2.
[137] Vgl. Väyrynen et al. 2013, S. 36.
[138] Vgl. Holthaus 2000, S. 45.
[139] Vgl. BSI 2016a, S. 102.
[140] Vgl. BSI 2016b.
[141] Vgl. Desouza & Awazu 2004, S. 2.
[142] Vgl. Maier 2007, S. 42.
[143] Vgl. Manhart & Thalmann 2015, S. 192, Ilvonen 2013.
[144] Vgl. Manhart & Thalmann 2015, S. 192, Desouza 2006.
[145] Vgl. Manhart & Thalmann 2015, S. 192, Gerber & von Solms 2005.

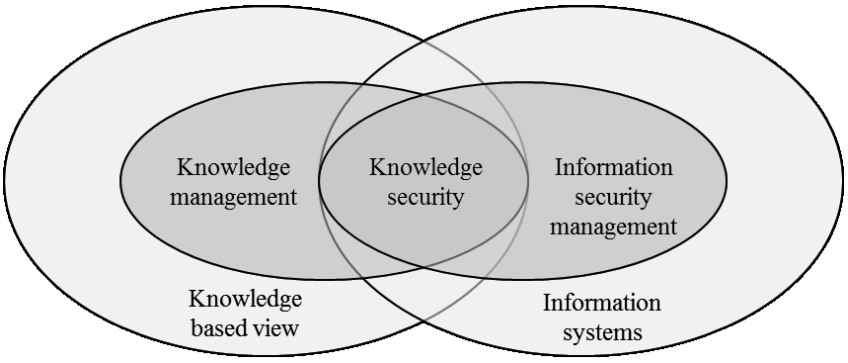

Abbildung 5: Wissenssicherheit und überlappende Theorien[146]

Zum Wissenssicherheits-Konzept existieren nach ILVONEN parallele Konzepte und Theorien, die untereinander zum Teil nicht wie dargestellt, vergleichbar sind. Die Abbildung 6 illustriert die Schnittstellen zur Wissenssicherheit und setzt die antiparallelen Konzepte in Beziehung zueinander.[147]

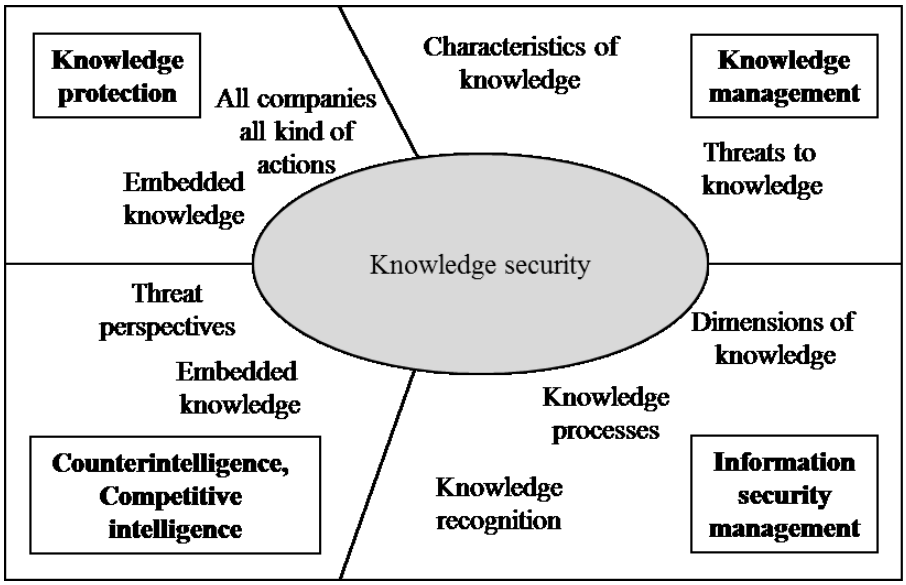

Abbildung 6: Wissenssicherheit und angrenzende Konzepte[148]

Intellectual Property (Rights Protection)

Das *Intellectual Property* (IPP) wird nach BOLISANI et al. im Vergleich zum Wissensschutz als die gesetzlichen Rechte definiert, die in Bezug auf das intellektuelle Kapital und seine Produkte geltend gemacht werden. IPP wird in der Regel auf das Eigentum an Ideen[149] angewendet, darunter fallen literarische und künstlerische Werke die urheberrechtlich geschützt sind, Erfindungen die patentrechtlich geschützt sind und Zeichen für die Unterscheidung von Waren eines Unternehmens, wie zum Beispiel Marken.[150] Nur einige Formen des intellektuellen Kapitals

[146] Modifiziert nach: Ilvonen 2013, S. 161.
[147] Vgl. Ilvonen 2013, S. 162.
[148] Modifiziert nach: Ilvonen 2013, S. 162.
[149] OECD 2008, S. 276.
[150] Vgl. Bolisani et al. 2013, S. 194.

können als IPP geschützt werden und nicht alle Produkte oder Arbeitsweisen, in denen sie eingebettet sind.[151] IPP *Proctection*[152] und IPP *Rights Protection*[153] fokussieren im Vergleich zum Wissensschutz auf formale Wissensschutzmechanismen[154] (vertragliche, gesetzliche) von Innovationswissen.[155] Der Wissensschutz hingegen betrachtet die formalen und informalen Schutzmechanismen. IPP *(Rights) Protection* ist nach dieser Definition eine Teilmenge des Wissensschutzes, auf der diese Arbeit aufbaut. Der Fokus der vorliegenden Arbeit liegt auf dem informalen Schutzmechanismus der Geheimhaltung, deshalb wird nicht weiter auf IPP oder IPP *(Rights) Protection* eingegangen.

Wissensschutz

Der Wissensschutz hat das Ziel, dass kein Wissen ohne Kenntnis der Verantwortlichen die Unternehmensgrenzen verlässt. Dadurch soll Wissen zurückgehalten werden, um dessen Enteignung von anderen Unternehmen zu verhindern.[156] Damit wird die Exklusivität des Wissens für das Unternehmen sichergestellt. Zum anderen sollen Imitationen durch Wettbewerber verhindert werden,[157] mit denen die IT-Beratung und ihre Auftraggeber im Wettbewerb stehen. In der englischsprachigen Literatur werden für den Wissensschutz anstatt *Knowledge Protecion*[158] andere äquivalente Bezeichnungen verwendet (Tabelle 4).

[151] Vgl. Bolisani et al. 2013, S. 194.
[152] Hertzfeld et al. 2006, S. 825 f., Amara et al. 2008, S. 1530.
[153] Zhao 2006, S. 1186.
[154] Vgl. Abschnitt 4.2.1.
[155] Vgl. Howells et al. 2003, S. 21.
[156] Vgl. Tongo 2013, S. 710.
[157] Vgl. Kogut & Zander 1992, S. 383 f., Liebeskind 1997, S. 624.
[158] Sofka & Shehu 2009, Bloodgood & Salisbury 2001, Bolisani et al. 2013, Carlsson 2004, Chai et al. 2011, de Faria & Sofka 2010, Hurmelinna-Laukkanen 2011, Lee et al. 2007, Manhart & Thalmann 2013, Thalmann & Manhart 2013, Manhart & Thalmann 2015, Monteiro et al. 2011, Nassimbeni et al. 2012, Norman 2001, 2002, Väyrynen et al. 2013, Perri & Andersson 2014, Olander & Hurmelinna-Laukkanen 2010, Olander et al. 2011.

Tabelle 4: Äquivalente Bezeichnungen für Knowledge Protection[159]

Inhalte	Autor(en) / Studien
Protecting knowledge	Liebeskind 1996
Protection of knowledge	Gold et al. 2001
Protecting of organizational knowledge	Schultze & Leidner 2002
Intellectual property protection	Drechsler & Natter 2012
Formal and informal protection	Elch-Hotelano 2011
Protecting intellectual property	Howells et al. 2003, Arrow 1974, Heiman & Nickerson 2002, 2004
Protection of intellectual assets	Olander et al. 2009
Intellectual asset protection	Manton 2006
Protect valuable technological assets	Li et al. 2008
protection of proprietary assets	Kale et al. 2000
protecting trade secrets	Barrier 2004
Protection of / protecting knowledge assets	Alstete 2003
Knowledge security	Desouza 2006, Ilvonen 2013
Security / protection of knowledge	Sage & Rouse 1999, Jennex & Olfman 2000, Jennex & Olfman 2005, Jennex & Zyngier 2007

Einige der angelsächsischen Äquivalente werden im Kontext mit Patentierung geistigen Eigentums, Daten- und Informationsschutz genutzt. Das wird der hier verwendeten Wissensschutz-Definition nicht gerecht. Diesen eingegrenzten Perspektiven auf *Knowledge Protecion* mangelt es am WM-Bezug für ein komplexes Unternehmen mit Einflussfaktoren wie Mitarbeiter, Prozesse und Technik. Die Arbeit legt somit ihren Fokus auf die Einflussfaktoren Mensch und Unternehmensprozesse.

Der Wissensschutz definiert nach LIEBESKIND die Grenze eines Unternehmens.[160] Diese Grenze beschreibt, welches Wissen geteilt und welches Wissen zurückgehalten wird. In diesem Zusammenhang prägen QUINTAS et al. den Begriff des *Boundary Paradox* und definieren, wie bereits weiter oben geschrieben, dass ein Unternehmen nach außen offen sein muss um Informationen und Wissen aus dem Umfeld und dem Markt zu erhalten. Zeitgleich muss das Unternehmen seine Wissensbasis schützen und pflegen.[161] Das *Boundary Paradox* beschreiben OLANDER et al. und BOLISANI et al. als *Knowledge Sharing - Knowledge Protection Dilemma*.[162] BOLISANI et al. definieren Wissensschutz als:

> "a broader concept that includes intellectual property rights protection and also 'softer' protection methods that can be used to deal with the intangible nature of knowledge."[163]

[159] Eigene Darstellung.
[160] Vgl. Liebeskind 1996, S. 104.
[161] Vgl. Quintas et al. 1997, S. 389.
[162] Vgl. Olander et al. 2009, S. 355, Bolisani et al. 2013, S. 193.
[163] Bolisani et al. 2013, S. 194.

Während sich diese Definiton auf IPP *Rights Protection* bezieht und auf die weichen Schutzmethoden verweist, fokussiert die Begriffsklärung von MANHART et al. den Bezug auf erfolgreiches Wissensmanagement:

> "Knowledge protection is an important contributor to successful knowledge management and concerns the prevention of unwanted knowledge spill-overs, knowledge loss and the reduction of knowledge visibility".[164]

Ein weiteres Ziel des Wissensschutzes ist es, Wettbewerbsvorteile für das Unternehmen zu generieren. Bezugnehmend auf BLOODGOOD & SALISBURY können Unternehmen mit der Unterstützung von drei WM-Strategien Wettbewerbsvorteile aufbauen, diese sind Wissensgenerierung, Wissenstransfer und Wissensschutz.[165] Nach diesem Strategiekonzept soll der Wissensschutz verhindern, dass Wissen geändert, zu anderen Unternehmen verlagert, verloren oder obsolet wird.[166] Der Autor stützt die Sichtweise von BLOODGOOD & SALISBURY[167] und MANHART et al. zum Wissensschutz und nimmt diese in die Arbeit auf.

Nach dem Modell von BOGERS zum *Knowledge Sharing and Protection*, das in Abbildung 7 dargestellt ist, kann Wissen als exogen und endogen gestaltet werden. Wissen ist endogen, wenn es ein Ergebnis des kodifizierten Forschungs- und Entwicklungsprozesses ist. Exogenes Wissen wird in der Zusammenarbeit mit dem Dienstleister aufgenommen und muss von der IT-Beratung für selbstverständlich gehalten werden. Das exogene Wissen bestimmt das Spannungsfeld des Wissensaustausches und des -schutzes in Forschungs- und Entwicklungskooperationen.[168] Das Modell von BOGERS basiert auf einer gleichberechtigten partnerschaftlichen Beziehung, die zum Beispiel bei (strategischen) Allianzen, Joint Ventures und F&E existiert. Diese gleichberechtigte Partnerschaft beschreiben TRKMAN & DESOUZA als symmetrische Kollaboration.[169] Diese Sichtweise unterscheidet sich vom intendierten Forschungsziel, das die Prinzipal-Agenten-Beziehung und damit eine abhängige Dienstleisterbeziehung fokussiert. Die folgende Abbildung visualisiert dieses Spannungsfeld einer gleichberechtigten Partnerbeziehung, das ebenso für die Prinzipal-Agenten-Beziehung anwendbar ist.

---

[164] Manhart et al. 2015, S. 2.
[165] Vgl. Väyrynen et al. 2013, S. 36.
[166] Vgl. Manhart & Thalmann 2013, S. 2.
[167] Bloodgood & Salisbury 2001.
[168] Vgl. Bogers 2011, S. 106.
[169] Vgl. Trkman & Desouza 2012, S. 7, Mentzer et al. 2000.

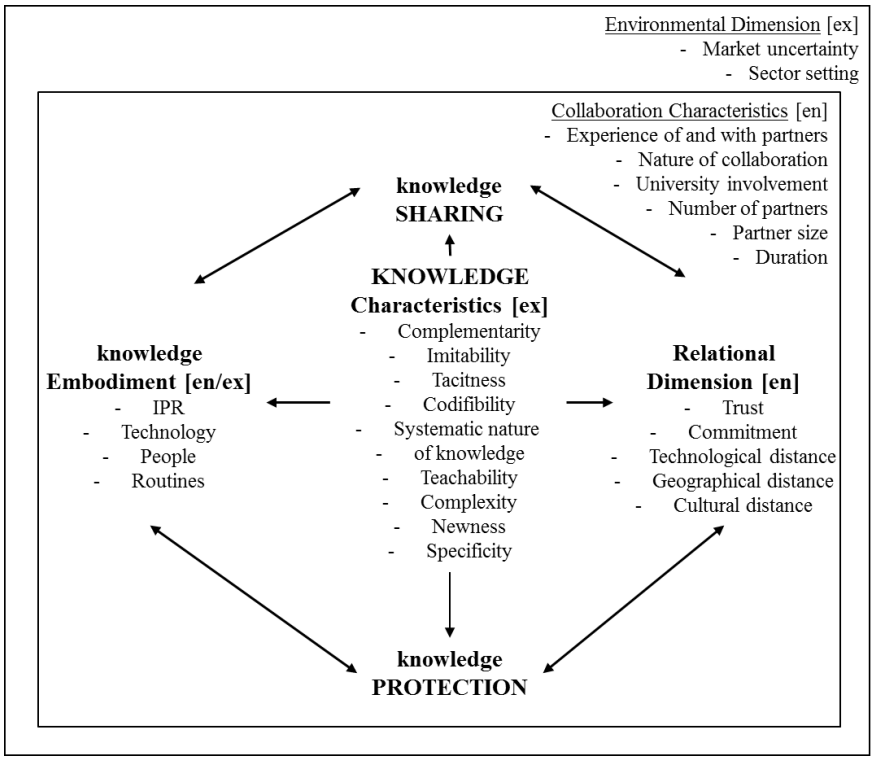

Abbildung 7: Spannungsfeld vom Wissen-Teilen und Wissensschutz[170]

Wissensschutzstrategie

Um die Wirksamkeit der verschiedenen Schutzstrategien besser zu verstehen, ist zunächst zu klären, welche Vermögenswerte ein Unternehmen vor Mitbewerbern, Auftraggebern und anderen Akteuren auf dem Markt schützen will. Das Problem besteht darin, dass Wissen von Natur aus frei beweglich ist, weil es sich in den Köpfen von Individuen befindet,[171] und insbesondere, weil die *Festlegung der Eigentumsrechte*[172] an Wissen schwach, teuer und aufwändig ist. Im Vergleich zu materiellen Ressourcen sind die Eigentumsrechte über Wissen schwer zu spezifizieren und durchzusetzen.[173] Deshalb müssen Unternehmen eine Reihe von organisatorischen Regelungen verwenden, um den Wert des Wissens zu schützen. So können Unternehmen,

(a) die Enteignung von Wissen vermeiden und
(b) die differenzierte Beobachtbarkeit von Wissen und ihren Produkten reduzieren

und das schützt gegen die Imitation.[174] Jedoch muss jedes Unternehmen seine spezifische Strategie erarbeiten, damit sein Wissensvermögen geschützt wird.[175] Mit dem Wissensschutz-Referenzmodell sollen IT-Beratungen eine Unterstützung für die Entwicklung der Wissensschutzstrategie bei der ISE mit externen IT-Dienstleistern erhalten.

[170] Bogers 2011, S. 106.
[171] Vgl. Lee et al. 2007, S. 60, Grant 1996, S. 112, Simon 1991, S. 125.
[172] Vgl. Liebeskind 1996, S. 95, Lee et al. 2007, S. 60.
[173] Vgl. Pawlowsky 2019, S. 16.
[174] Vgl. Lee et al. 2007, S. 60.
[175] Vgl. Song 2008, S. 61.

Nach HOWELLS et al. ist der Schutz der internen Prozesskenntnisse zuerst zu fokussieren, da sie für die Bereitstellung von Dienstleistungen von entscheidender Bedeutung sind. Die Bereitstellung von vielen Diensten ist auf IT angewiesen, so ist die Software für sie der zweitbedeutendste zu schützende Vermögenswert. Für die Mehrheit aller Unternehmen ist es essentiell, die einzigartigen Fähigkeiten ihrer Mitarbeiter zu sichern.[176] Zu diesen einzigartigen Fähigkeiten gehören das Fachwissen und das Technologiewissen einer IT-Beratung, mit der die IT-Projekte erfolgreich realisiert werden. Diese aufgebauten einzigartigen Fähigkeiten der Mitarbeiter sind in dem Referenzmodell als Fachwissen und Technologiewissen bezeichnet. Diese schützenswerten Wissensgebiete sollen mit Hilfe des Referenzmodells identifiziert und geschützt werden.

Eine Wissensschutzstrategie zu entwickeln hilft dem Unternehmen, was zu tun ist und wie das gesetzte Ziel erreicht werden kann.[177] AMARA et al. und DE FARIA & SOFKA weisen nach, dass die Wissensschutzstrategie mehrere einschränkende Schutzformen umfasst, wenn die Absicht eines höheren Präventionsgrades von dem abgehenden Wissenstransfer besteht. Ein höherer Einschränkungsgrad stammt von einer größeren Kombinationsauswahl der Schutzmethoden, um von ihren einzigartigen Eigenschaften zu profitieren (zum Beispiel Umfang der Wissensschutzstrategie).[178] VÄYRYNEN et al. und BLOODGOOD & SALISBURY definieren Wissensschutzstrategie als die Erhaltung seines ursprünglichen und schöpferischen Zustandes und die Verwahrung vor unberechtigten Wissenstransfer zu anderen Unternehmen.[179]

Für die Arbeit wird die Definition zur Wissensschutzstrategie von AMARA et al. und DE FARIA & SOFKA zugrunde gelegt und die folgende Wissensschutzstrategie Definition aufgestellt. Diese Definition wurde in den Experteninterviews mit den Interviewpartnern und ihren praktischen Erfahrungen besprochen, diskutiert, erweitert und validiert:

> Wissensschutzstrategie schützt wertvolles organisationales Wissen eines Unternehmens um Wissensvorsprung zu sichern und setzt Schutzmethoden (formale / informale Mechanismen) nach dem bewerteten Präventionsgrad des abgehenden Wissenstransfers zu anderen Unternehmen ein. Um die Wettbewerbsfähigkeit zu erhalten, werden organisationale Wissensflüsse zur Prävention von ungewollter Wissensdiffusion geprüft. Zu definieren ist, welches Wissen die „Grenze“ vom Unternehmen verlassen darf und welches Wissen im Unternehmen verbleiben soll.

MONTEIRO et al. forschten zum Wissensschutz und der Innovations-Performance, für sie behindert der strategische Wissensschutz die Gegenseitigkeit, die Erwartung, dass ein Gefallen eines Tages zurückkommt und sich damit die implizite moralische Verpflichtung dieses Abkommens zu wahren, verlängert.[180] Diese Sichtweise ist für F&E-Partnerschaften und damit für bidirektionale Kooperation anwendbar. Jedoch stellt der Autor die Validität dieser Aussage für eine Prinzipal-Agenten-Beziehung[181] (Auftraggeber - Auftragnehmer) in Frage. Für den Prinzipal

---

[176] Vgl. Howells et al. 2003, S. 4.
[177] Vgl. Amara et al. 2008, S. 1534.
[178] Vgl. Amara et al. 2008, S. 1534, Faria & Sofka 2010, S. 958.
[179] Vgl. Bloodgood & Salisbury 2001, S. 59, Väyrynen et al. 2013, S. 36 f.
[180] Vgl. Monteiro et al. 2011, S. 2.
[181] Vgl. Unterkapitel 2.3.

ist schwer zu erkennen, ob dieses organisationale Wissen aus dem IT-Projekt für den Agenten und seinen IT-Projekten bei anderen Auftraggebern von Nutzen ist. Zudem ist es diffizil die Enteignung oder die Imitation des Wissens nachzuweisen.[182]

Bei den Wissensschutzstrategien gibt es nach SOFKA & SHEHU Unterschiede zwischen national und international agierenden Unternehmen. Nach ihren Untersuchungen nehmen internationale Unternehmen eher eine passive Rolle ein und haben keine eindeutige Wissensschutzstrategie.[183]

Zusammenfassend ist darzulegen, dass basierend auf der Abgrenzung des Wissensschutzes zum Datenschutz, Informationsschutz und zur Wissenssicherheit eine Wissensschutzstrategie Definition für die Arbeit abgeleitet wird. Besonders hervorgehoben werden soll, dass sich die aktuelle Wissensschutzforschung überwiegend auf die bidirektionale Kollaboration bezieht. Die unidirektionale Kommunikation, wie bei einer Prinzipal-Agenten-Beziehung, findet in der Forschung zum Wissensschutz kaum Beachtung.

2.2 IT-Beratung, Projekte und Software

Zum Grundverständnis wird die IT-Beratung als Forschungsobjekt charakterisiert sowie das Projektgeschäft mit dem Ziel Informationssysteme für die Auftraggeber zu implementieren beschrieben. Im Abschnitt 2.2.1 werden die Begrifflichkeiten, seine Merkmale und Besonderheiten erläutert. Anschließend erfolgt im Abschnitt 2.2.2 die Beschreibung der IT-Beratung als Forschungsgegenstand. Im letzten Abschnitt dieses Unterkapitels wird auf den Wissensschutz in einer IT-Beratung eingegangen.

2.2.1 Begriffsklärung und Merkmale

Die IT-Beratung ist mit ihren wissensintensiven und schnelllebigen Produkten und Dienstleistungen auf WM angewiesen. ALAVI & LEIDNER definieren WM-Systeme in Unternehmen als:

> "IT-based systems developed to support and enhance the organizational processes of knowledge creation, storage / retrieval, transfer, and application."[184]

Sie stellten fest, dass nicht durch alle WM-Initiativen eine Information Technologie (IT)-Lösung implementiert wird, aber die IT unterstützt das WM als *Enabler*. MAIER erweitert das IT-Konzept für das WM-System indem er es als ein Informations- und Kommunikationstechnologie (IKT)-System bezeichnet, das die Funktionen der Wissensbildung, -konstruktion, -identifikation, -erfassung, -akquisition, -auswahl, -bewertung, -organisation, -verknüpfung, -strukturierung, -formalisierung, -visualisierung, -verteilung, -retention, -wartung, -verfeinerung, -evolution, -zugriff, -suche und -anwendung besitzt.[185] Im Allgemeinen wird IKT in der Wissensgesellschaft eingesetzt, um mit Ertragssteigerung, Diversifikationsvorteilen und Wissensvorteilen die Wettbewerbsvorteile eines Unternehmens zu ermöglichen und zu unterstützen.[186]

---

[182] Vgl. Liebeskind 1996, S. 93 ff.
[183] Vgl. Sofka & Shehu 2009.
[184] Alavi & Leidner 2001, S. 114.
[185] Vgl. Maier 2007, S. 86.
[186] Vgl. Carlsson 2004, S. 640.

In der vorliegenden Arbeit wird der Begriff IT und IS verwendet, da nach FINK et al. „eine Kommunikation (ein Informations- oder Datenaustausch) zwischen Systemen bzw. Systemelementen in der Regel systemimmanent ist“.[187] Demnach können die Begriffe IT und IKT sowie IS und IKS als synonyme verwendet werden.

Nach den zugrunde gelegten Definitionen liegt der Ursprung von IT-Lösungen, die IT-Beratungen in ihren Projekten konzipieren und konstruieren, in dem Zyklus von WM-Systemen. Projekte sind nach DIN 69901:

> „ein Vorhaben, das im Wesentlichen durch Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist, wie zum Beispiel Zielvorgabe, zeitliche, finanzielle, personelle oder andere Begrenzungen, projektspezifische Organisation“.[188]

In den IT-Projekten und damit der ISE werden betriebliche Informationssysteme oder auch Anwendungssysteme[189] für die Auftraggeber realisiert.

Damit eine IT-Beratung Projekte realisieren kann, ist eine Projektorganisation notwendig. Eine Projektorganisation beschäftigt sich mit dem Kooperieren von Projektmitarbeitern innerhalb eines oder mehrerer Projekte.[190] Die *International Project Management Association* (IPMA) definiert die Projektorganisation wie folgt:

> „Die Projektorganisation besteht aus einer Gruppe von Menschen und der dazugehörigen Infrastruktur, für die Vereinbarungen bezüglich Autorität, Beziehungen und Zuständigkeiten unter Ausrichtung auf die Geschäfts- und Funktionsprozesse getroffen wurde. Dieses Kompetenzelement umfasst die Entwicklung und Aufrechterhaltung von geeigneten Rollen, Organisationsstrukturen, Zuständigkeiten und Fähigkeiten für das Projekt.“[191]

Diese Menschengruppe oder Stakeholder versuchen das Projekt zu beeinflussen und teilen sich in unmittelbare (zum Beispiel Projektmanager, Projektmitarbeiter) und mittelbare (zum Beispiel Projektbeeinflusser) Projektbeteiligte auf.

In der Abbildung 8 ist eine exemplarische Rahmen- und Einzelprojektorganisation abgebildet. Für einzelne und projektübergreifende Projekte können die Rollen, Verfahren und Prozesse definiert werden. Eine IT-Beratung, die mehrere Auftraggeber betreut, wird sich im Vergleich zu einer Einzelprojektorganisation, in einer Projektrahmenorganisation organisieren, um die verschiedenen Auftraggeber zu bedienen.[192] Der untere linke gestrichelte Abbildungsbereich kennzeichnet die risikobehaftete Wissensschnittstelle des Projektteams zum externen Berater. Zudem ist mit der modifizierten Darstellung angedeutet, dass der externe Berater auch außerhalb der Projektorganisation Aktivitäten durchführt. Diesen Bereich fokussiert die vorliegende Arbeit.

---

[187] Fink et al. 2005, S. 3.
[188] DIN 69901.
[189] Vgl. Disterer et al. 2003, S. 21.
[190] Vgl. Kremer & Rohde 2009, S. 297.
[191] Kremer & Rohde 2009, S. 297.
[192] Vgl. Kremer & Rohde 2009, S. 297.

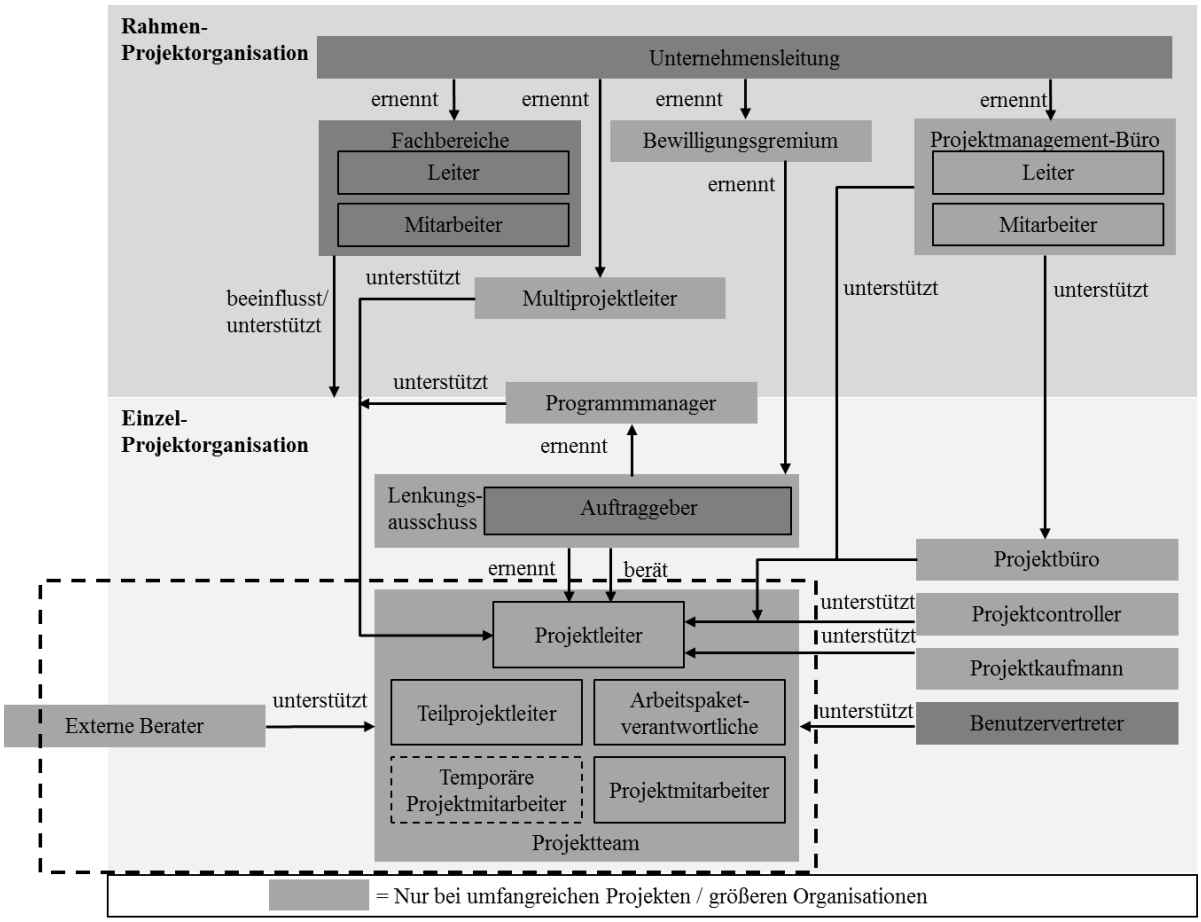

Abbildung 8: Rahmen- und Einzelprojektorganisation[193]

Die folgenden Projektrollen können zum Beispiel innerhalb eines IT-Projektes existieren und von einem externen Berater / Dienstleister eingenommen werden. Der Projektleiter oder Projektmanager, der das Projekt verantwortet, ist hier nicht aufgeführt und sollte *by default* nicht durch einen externen Berater / Dienstleister besetzt werden.[194] Die Projektrollen sind:

- Fachliche / Technische Berater
- Fachliche / Technische Architekten
- Implementierungsverantwortlicher
- Entwickler
- Testmanager, Tester

Um die IT-Projekte einer IT-Beratung zu realisieren, können diese nach der DIN 69901 in fünf Projektmanagementphasen[195] gegliedert werden. Diese Phasen sind in der Tabelle 5 beschrieben:

[193] Modifiziert nach: Pfetzing & Rohde 2006, S. 50, Kremer 2005, S. 76.
[194] Vgl. Feeny & Willcocks 1998, S. 15 f.
[195] Siehe Definition der Projektmanagementphasen nach DIN 69901-5: 2009: Initialisierungsphase - Definitionsphase – Planungsphase – Steuerungsphase – Abschlussphase. Im Vergleich dazu die Definition der Projektphasen nach DIN69901-2:2009 = ISO 21500:2012: Initiating, Planning, Implementing, Controlling, Closing.

Tabelle 5: Beschreibung der Projektmanagementphasen nach DIN 69901-5: 2009[196]

Projektphase	Beschreibung
1. Initialisierungsphase	• Projektidee konkretisieren, analysieren, bewerten und Zielvision skizzieren • Relevante Prozesse für die Projektabwicklung vorbereiten • Freigabe der Prozessergebnisse durch die Führung
2. Definitionsphase	• Kernteam bilden • Projektziele spezifisch und messbar definieren und formulieren • Konkrete Projektinhalte festlegen und strukturieren • Meilensteine definieren und Projektaufwand abschätzen • Umfeldanalyse durchführen und Machbarkeit bewerten
3. Planungsphase	• Projektstrukturplan erstellen • Im iterativen Prozess die Termin-, Ressourcen- und Kostenplan erarbeiten • Risikobetrachtung • Abstimmung mit Lieferanten • Freigabe durch den Auftraggeber
4. Steuerungsphase	• Kickoff mit Commitment zu Zielen, Planung und Organisationsform • Teambildung und Teamentwicklung • Projektumsetzung • Reporting und Steuerung (Ziele, Termine, Kosten, Ressourcen, Qualität, Risiken etc.) • Änderungsmanagement • Abnahmeerklärung durch Auftraggeber
5. Abschlussphase	• Nachkalkulation • Durchführung einer Abschlussbesprechung inkl. Abschlussbericht • Lessons Learned • Archivierung von Unterlagen zur Wissensdokumentation

PAI & BASU berichten von sechs IKT-Entwicklungsprojektphasen, diese sind: „project initiation, analysis, logic design, physical design, implementation and maintenance".[197] Für das Modell werden die fünf Projektmanagementphasen der DIN und ISO Norm zugrunde gelegt. AMORIBIETA et al. empfehlen beim Offshore-Outsourcing erst ab der Design-Phase Aufgaben abzugeben.[198] Diese Sichtweise adaptiert das entwickelte Modell. Die Positionierung zum strategischen Wissensschutz bei der ISE sollte in den ersten beiden Projektmanagementphasen, der Initialisierungsphase und der Definitionsphase, etabliert werden. In diesen Projektmanagementphasen müssen die strategischen Entscheidungen zum Wissensschutz und zum externen Dienstleistereinsatz getroffen werden.[199]

Zusammenfassend ist festzustellen, dass in der Arbeit die Begriffe IT und IS als Synonyme für IKT und IKS verwendet werden können. Im folgenden Abschnitt wird deutlich, dass die ISE für die das Wissensschutz-Referenzmodell entwickelt wird, der Informationstechnik und nicht

[196] Vgl. Wagner et al. 2009, S. 49 f.
[197] Vgl. Pai & Basu 2007, S. 27.
[198] Vgl. Pai & Basu 2007, S. 27.
[199] Vgl. Abschnitt 5.2.2.

der Kommunikationstechnologie zuzuordnen ist.[200] Die spezifische Projektorganisation mit dem Spannungsfeld des externen Beratereinsatzes wird skizziert und visualisiert. Die strategischen Entscheidungen zum Wissensschutz sind in die ersten beiden Projektmanagementphasen zu legen.

2.2.2 Softwareentwicklung in einer IT-Beratung

Die Informationstechnologie nimmt mit ihren Berührungspunkten zu allen Unternehmensbereichen und -funktionen eine Querschnittsfunktion ein.[201] Nach FINK & KNOBLACH gehört eine IT-Beratung zu der Gruppe der Unternehmensberatung.[202] Eine IT-Beratung definiert WAMSTEKER als, die Unterstützung von privatwirtschaftlichen oder öffentlichen Organisationen im Bereich der Planung, Entwicklung, Implementierung und Betrieb von IT-Systemen.[203] Weiterhin wird eine IT-Beratung in die Branche der KIBS eingeordnet. Nach MULLER & DOLOREUX beschäftigen sich KIBS vor allem mit wissensintensiven Inputs für Geschäftsprozesse von anderen Unternehmen, das beinhaltet private und öffentliche Auftraggeber.[204] Eingeführt wurde der KIBS-Begriff von MILES et al.[205] KIBS-Unternehmen erzeugen Wissen und Innovationen und verkaufen ihre Dienstleistungen, wie zum Beispiel die ISE für andere Unternehmen.[206]

Die folgende Definition von LEHRER et al. beschreibt den KIBS-Grundgedanken und bestätigt, dass die Informationstechnologie Bestandteil von KIBS ist:

> "Knowledge-intensive business services encompass a particular service category founded upon technical knowledge and/or professional knowledge applied to solve a strategic task of the client, e.g., R&D services, marketing, strategic consultancy, and information technology."[207]

Im Rahmen des Wissensmanagements sind KIBS-Unternehmen bestrebt das bereits aufgebaute Wissen für neue Projekte und Auftraggeber wieder zu verwenden.[208] Gerade im Dienstleistungssektor und besonders bei KIBS besteht häufig die Notwendigkeit, maßgeschneiderte Lösungen für jeden neuen Auftraggeber anzubieten, da diese Lösungen effektiver und kostengünstiger sind, wenn die Unternehmen in der Lage sind, ihre Erfahrungen aus früheren Projekten zu nutzen.[209] Die Ergebnisse von BOLISANI et al.[210] zu KIBS-Unternehmen stehen im Einklang mit den allgemeinen Forschungserkenntnissen von BETTENCOURT et al.[211] und KUUSISTO[212]. Demnach haben KIBS-Unternehmen eine enge Verbindung zu ihren Auftraggebern, die nicht nur

[200] Vgl. Abbildung 9.
[201] Vgl. Lippold 2016, S. 57.
[202] Vgl. Fink & Knoblach 2003.
[203] Vgl. Wamsteker 2012.
[204] Vgl. Muller & Doloreux 2007, S. 5, Amara et al. 2009, S. 407.
[205] Vgl. Alvisi 2012, Miles et al. 1995.
[206] Vgl. Miles et al. 1995, S. 28.
[207] Lehrer et al. 2012, S. 500.
[208] Vgl. Bolisani et al. 2013, S. 204.
[209] Vgl. Bolisani et al. 2013, S. 204.
[210] Vgl. Bolisani et al. 2013, S. 203.
[211] Bettencourt et al. 2002.
[212] Kuusisto 2008.

als KIBS-Empfänger, sondern ebenso als wertvolle Wissensquellen fungieren, um neue Dienstleistungen zu entwerfen und umzusetzen.[213] Diese wertvollen Wissensquellen gilt es zu identifizieren und zu schützen, damit die Wettbewerbsfähigkeit einer IT-Beratung und die der Auftraggeber unter der Projektbeteiligung von externen Beratern gesichert wird.

Folgend der existierenden Literatur von MILES et al., STRAMBACH, MULLER & DOLOREUX und BOLISANI et al. sind die Funktionsfähigkeit und die Innovationsfähigkeit von KIBS strikt mit den kognitiven Vermögenswerten verbunden, die sie besitzen:[214]

1. Ihr bedeutendster Produktionsfaktor und bedeutendstes Produktionsergebnis besteht aus Wissen, der direkt an Kunden in Form von Beratung geliefert wird oder in Artefakte und Dienstleistungen eingebettet ist.
2. Ihre Tätigkeit beruht hauptsächlich auf den Spezialisierungen, der Fertigkeiten und der Kenntnisse ihrer gewonnenen Mitarbeiter.
3. Die Bereitstellung wissensintensiver Dienstleistungen erfordert eine vertiefte Interaktion zwischen Dienstleister und Nutzer, die sowohl an kognitiven Austausch- und Lernprozessen beteiligt sind.[215]
4. Die Bereitstellung solcher Dienste beinhaltet ein Problemlösungsverfahren, bei dem die KIBS-Unternehmen ihr Wissen an die spezifischen Bedürfnisse der einzelnen Kunden anpasst.
5. Sie sind häufig Schnittstellen zwischen globalen Wissensquellen und Endbenutzern.[216]
6. Ihre Innovationsfähigkeit ist direkt mit der Akquisition, der Verarbeitung, der Kapitalisierung und der Lieferung neuen Wissens verbunden.[217]

Demzufolge sehen sich KIBS-Unternehmen häufig zwei kontrastierenden Zielen gegenüber, die an das Wissensaustausch-Wissensschutz-Dilemma erinnern, das in der Regel mit Innovationsaktivitäten zusammenhängt:[218]

- Einerseits müssen sie für externe Beziehungen offen sein und einen effektiven Wissensaustausch mit Dienstleistern und Auftraggebern bewältigen.
- Andererseits müssen sie die Entwicklung und Aktivierung von internen kognitiven Vermögenswerten, die ihre Kernkompetenzen darstellen, schützen.

Aufbauend auf den erarbeiteten theoretischen Grundlagen zu KIBS, IT-Beratung, WM und Wissensschutz kann eine IT-Beratung für die vorliegende Arbeit wie folgt definiert werden:

> Die IT-Beratung unterstützt privatwirtschaftliche oder öffentliche Unternehmen im Bereich der Planung, Entwicklung, Implementierung und Betrieb von IT-Systemen. Im Beratungsprozess und der Interaktion müssen der Wissensaustausch und der Wissensschutz mit Dienstleistern und Auftraggebern sichergestellt werden, weil Wissen und damit das Wissensmanagement ihr bedeutendster Produktionsfaktor ist und ihre Innovationsfähigkeit davon abhängt.

Nach MILES et al. verkaufen KIBS-Unternehmen ihre Dienstleistungen an andere Unternehmen.[219] Dienstleistungen lassen sich nach der Literatur anhand von drei Dimensionen erkennen:

- Potenzialdimension: Der Leistungserbringer offeriert das Potenzial.
- Prozessdimension: Der Leistungsabnehmer bringt den externen Faktor in den Prozess der gemeinsamen Leistungserbringung ein (uno-actu-Prinzip).

---

[213] Vgl. Bolisani et al. 2013, S. 203.
[214] Vgl. Bolisani et al. 2013, S. 193, Miles et al. 1995, Strambach 2008, Muller & Doloreux 2009.
[215] Vgl. Bettencourt et al. 2002.
[216] Vgl. Smedlund 2006.
[217] Vgl. Amara et al. 2009.
[218] Vgl. Bolisani et al. 2013, S. 193, Olander et al. 2009.
[219] Vgl. Miles et al. 1995, S. 28.

- Ergebnisdimension: Das Ergebnis ist nutzbringend.[220]

Gegenüber Sachgütern weisen die Dienstleistungen drei charakteristische Merkmale auf:

- Leistungsfähigkeit des Dienstleistungsanbieters (zum Beispiel *Know-how*),
- Integration eines externen Faktors des Leistungsabnehmers (zum Beispiel Geschäftsprozesswissen) und
- Immaterialität des Dienstleistungsergebnisses.[221]

Die Begriffsdefinition der IT-Dienstleistung basiert auf diesem Dienstleistungsverständnis. Nach KNOTHE et al.[222] und RUDOLPH[223] charakterisieren sich IT-Dienstleistungen neben dem Bezug zur Informationstechnologie durch Immaterialität, das uno-actu-Prinzip und die Integration eines externen Faktors. Der Begriff IT-Dienstleistung oder das englische Pendant der IT-Service ist in der Literatur divers definiert.

Im Rahmen von Marktanalysen beinhalten IT-Dienstleistungen den laufenden Betrieb, die Wartung, die Implementierung / die Entwicklung, weitere Projektgeschäfte, Schulung und Beratung.[224] BÖHMANN unterscheidet auf der Basis des Einsatzumfanges von IT-Systemen und IT-Aktivitäten zur Leistungserstellung zwischen IT-Dienstleistungen und IT-basierten Dienstleistungen.[225] Die vorliegende Arbeit folgt dieser IT-Dienstleistungsdefinition. Eine Dienstleistung ergibt sich,

> „wenn IT-Systeme oder IT-Aktivitäten wesentlicher Bestandteil des Leistungsergebnisses sind und zusätzlich IT-Systeme oder andere IT-bezogene Faktoren sowohl als Potenzialfaktoren für die Sicherstellung der Leistungsbereitschaft bedeutsam als auch als externe Faktoren in den Leistungserstellungsprozess eingebunden sind".[226]

MEFFERT & BRUHN[227] und ZARNEKOW[228] unterscheiden dabei zwischen personell erzeugten und automatisiert / industriell erzeugten IT-Dienstleistungen. Die industriellen IT-Dienstleistungen definieren sich durch IT-Systeme die für den laufenden Betrieb essentiell sind. Die personell erzeugten IT-Dienstleistungen charakterisieren sich durch einen hohen Personaleinsatz und sind Bestandteil der Softwareentwicklung, Systemintegration, IT-spezifische Schulung und Beratung.

Die Arbeit fokussiert sich auf den IT-Dienstleistungsbegriff der personell erzeugten Dienstleistungen, da diese die Softwareentwicklung beinhaltet. Das Ergebnis der Softwareentwicklung ist eine Software, die sich nach BALZERT wie folgt charakterisieren lässt:

- „Software ist ein immaterielles Produkt
- Software unterliegt keinem Verschleiß
- Software wird nicht durch physikalische Gesetze begrenzt
- Software ist im Allgemeinen leichter und schneller änderbar als ein technisches Produkt
- Für Software gibt es keine Ersatzteile

---

[220] Vgl. Meffert & Bruhn 2006, S. 28 ff.
[221] Vgl. Corsten & Gössinger 2007, S. 26 ff., Meffert & Bruhn 2006, S. 28 ff., Hilke 1989, S. 15.
[222] Vgl. Knothe et al. 2004, S. 11.
[223] Vgl. Rudolph 2009, S. 22 f.
[224] EITO 2007, S. 256, Hradilak 2007, S. 20.
[225] Vgl. Böhmann 2004, S. 30 ff.
[226] Böhmann 2004, S. 32.
[227] Meffert & Bruhn 2006, S. 42.
[228] Zarnekow 2007, S. 11.

- Software altert
- Software ist schwer zu vermessen“[229]

Software wird nach ISO / IEC 2382 in System-, Unterstützungs- und Anwendungssoftware gegliedert. Zudem kann Software nach dem Grad der Individualität in Standard- und Individualsoftware gegliedert werden. Diese Arbeit fokussiert sich beim Wissensschutz auf die ISE, da für die Auftraggeber individuelle und innovative Informationssysteme entwickelt werden. Die Standardsoftware hingegen wird für mehrere Kunden erstellt und ist nicht Untersuchungsbestandteil dieser Arbeit. In der Abbildung 9 von TEUBNER wird die Einordnung von Individualsoftware grau hervorgehoben.

Informationstechnik (Computertechnik)											**(Tele-) Kommunikationstechnik**						
Hardware						**Software**					**Netze**				**Dienste**		
Rechner			Peripherie			System-software			**Anwend-ungs-software**		private Netze		öffentliche Netze		private Dienste		öffentliche Dienste
Zentralprozessor	Interne Speicher	Schnittstellen	Eingangsgeräte	Ausgangsgeräte	Externe Speicher	Betriebssysteme	Übersetzer	Dienstprogramme	Standardsoftware	**Individualsoftware**	PBX	LAN	WAN	Internet	Kommunikations-dienste		Mehrwertdienste

Abbildung 9: Einordnung der Individualsoftware in IKT[230]

Bei der innerbetrieblichen erstellten Software ist davon auszugehen, dass es sich um einmalig verwendbare Individualsoftware handelt, die das Ziel hat den innerbetrieblichen Leistungserstellungsprozess zu unterstützen.[231] Jedoch sind die Anforderungen an die innerbetriebliche Leistungserstellung bei den Unternehmen einer Branche simultan, die den Einsatz des Wissensschutzes notwendig macht, um die Wettbewerbsvorteile einer IT-Beratung und die der Auftraggeber beim externen Dienstleistereinsatz zu schützen.

Der Grad der Individualisierung von Software wird in der Abbildung 10 dargestellt. Die relevante Information von HERZWURM ist, dass der Kunde bei der Individualsoftware (Einzelsoftware) den gesamten Produktentwicklungsauftrag auslöst. Bei der Variantensoftware (individualisierte Standardsoftware) wird vom Kunden die Anpassungsentwicklung beauftragt und bei der standardisierten Variante (Massensoftware, Marktsoftware) wird bereits vor dem Kundenauftrag gestartet.[232]

[229] Balzert 1999, S. 26 ff.
[230] Modifiziert nach: Teubner 1999, S. 22.
[231] Vgl. Herzwurm 2000, S. 80.
[232] Vgl. Herzwurm 2000, S. 80.

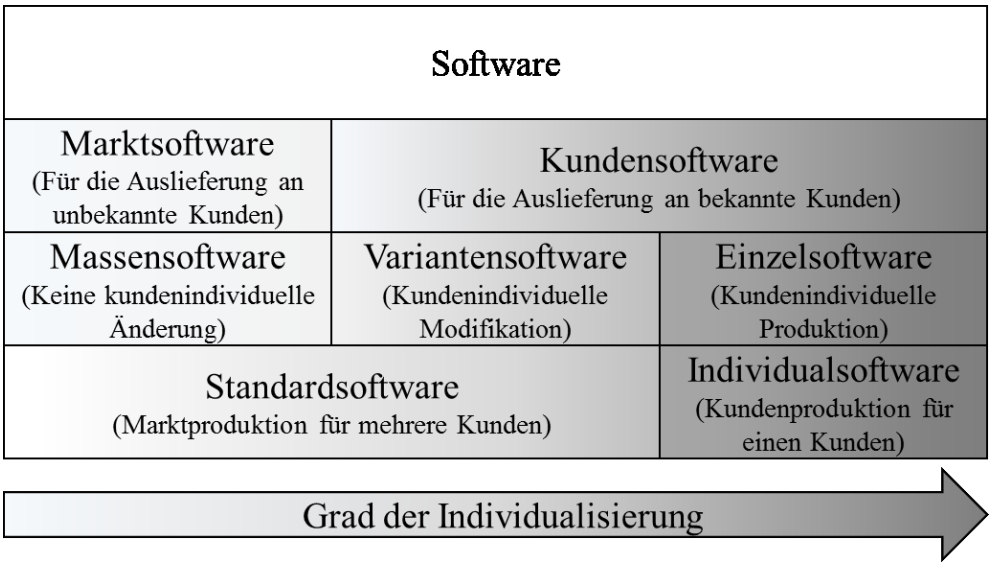

Abbildung 10: Klassifikation von Software nach dem Grad der Kundenindividualität[233]

HERZWURM weist darauf hin, dass „die Unterscheidung zwischen dem Zusammenbau von Softwaremodulen mit entsprechender Parametrisierung und der Anpassungsprogrammierung von Standardsoftware […] eher technischer Natur [ist] und zum Zwecke der Untersuchung der Kundenorientierung ohne besondere Bedeutung“.[234]

Zusammenfassend werden in diesem Abschnitt Dienstleistungen im Allgemeinen und IT-Dienstleistungen im spezifischen charakterisiert. Das basiert auf der Relation von IT-Beratungen zu der KIBS-Branche. Die Individualsoftware als ein Ergebnis einer IT-Dienstleistung wird mit ihrem Individualisierungsgrad nach Kundenanforderungen präzisiert. Fokus der vorliegenden Arbeit sind die Softwareentwicklungsprojekte, die einen individuellen Kundenbezug aufweisen. Die Softwareentwicklung von Standardsoftware wird somit ausgeschlossen.

2.2.3 Wissensrisiken in einer IT-Beratung

Dem griechischen Philosophen PLATON wird der Ausspruch zugeschrieben: „Wenn zwei Knaben jeder einen Apfel haben und sie diese tauschen, hat am Ende auch nur jeder einen Apfel. Wenn aber zwei Menschen je einen Gedanken haben und diese tauschen, hat am Ende jeder zwei neue Gedanken“. Somit befördert das *Wissen-Teilen* die Innovationskraft und kann Wettbewerbsvorteile sichern. Wird erfolgskritisches oder schützenswertes Wissen mit einem externen IT-Dienstleister geteilt, so kann das die Zukunftsfähigkeit einer IT-Beratung beeinflussen.

In dem innovationsreichen und rapiden Umfeld der sich besonders die IT-Beratungen stellen müssen, um sich kurzfristig und langfristig auf dem Markt etablieren und behaupten zu können, müssen Kompetenzen outgesourct werden. Eine IT-Beratung muss sich auf ihre Kernprozesse und damit auf ihr Kernwissen konzentrieren. Der Wettbewerbsdruck und die Notwendigkeit

[233] Modifiziert nach: Herzwurm 2000, S. 81.
[234] Herzwurm 2000, S. 80.

einer besseren finanziellen Leistungsfähigkeit sind die treibende Kraft für die Zunahme an Outsourcingbestreben[235] und -umfang in allen Branchen weltweit.[236] Aufbauend auf diesen Bestrebungen sollte validiert werden, ob Nicht-Kernwissen an Dienstleister abgegeben wird. Nach GHODESWAR & VAIDYANATHAN und FARRELL kann das Outsourcing ein Unternehmen befähigen, die globalen Fähigkeiten effektiv und effizient zu nutzen, indem sie die *Best Practices* der Branche für die Verbesserung ihrer Wertschöpfungskette einsetzen und damit neue Märkte erschließen und gründen können.[237]

Risiko, Risikoanalyse und Wissensrisiko

Zum Begriff Risiko gibt es verschiedene Definitionen.[238] Nach ISO 31000 wird Risiko als die Auswirkung von Unsicherheit auf Ziele definiert[239] und ist eine Folge von Ereignissen oder von Entwicklungen.[240] Nach dieser Norm können die Auswirkungen positiv oder negativ sein. Die Unsicherheit oder Ungewissheit auf Ziele wird mit der Eintrittswahrscheinlichkeit geschätzt. Nach den Untersuchungen von HEINRICH et al. ist Risiko „sowohl etwas Negatives, Bedrohliches bzw. Gefährliches als auch Zukünftiges und daher Ungewisses".[241] Zu den folgenden Risiken-Elementen sind sich die Autoren einig. Sie enthalten:

- „die zu erwartende Häufigkeit bzw. Eintrittswahrscheinlichkeit eines gefährdenden Ereignisses und
- das beim Ereigniseintritt zu erwartende Schadensausmaß."[242]

In der Abbildung 11 ist ein etabliertes Modell zu den Zusammenhängen der Risikoanalyse mit seinen Einflussfaktoren abgebildet. DAMM et al. erklären, dass wenn eine Bedrohung auf eine Unternehmensschwachstelle (organisatorisch, menschlich, technisch) trifft, dann entwickelt sich für das Unternehmen eine Gefahr.[243] Zur Ermittlung der Schadenspotentiale müssen die zu schützenden Werte / Assets identifiziert und quantifiziert werden.[244] Wie in der Abbildung 11 skizziert, bildet sich aus der Gefahr, dem Schadenspotential und der bewerteten Eintrittswahrscheinlichkeit das Risiko.[245]

---

[235] Vgl. Nassimbeni et al. 2012, S. 407.
[236] Vgl. Ghodeswar & Vaidyanathan 2008, S. 23.
[237] Vgl. Ghodeswar & Vaidyanathan 2008, S. 31, Farrell 2004.
[238] Vgl. Heinrich et al. 2014, S. 512.
[239] Vgl. ISO 31000.
[240] Vgl. ISO 31000:2009, Clause 2.1.
[241] Heinrich et al. 2014, S. 512.
[242] Heinrich et al. 2014, S. 512.
[243] Vgl. Damm et al. 1999, S. 23, Devargas 1993, S. 46.
[244] Vgl. Eckert 2004, S. 15.
[245] Vgl. Damm 1999, S. 24.

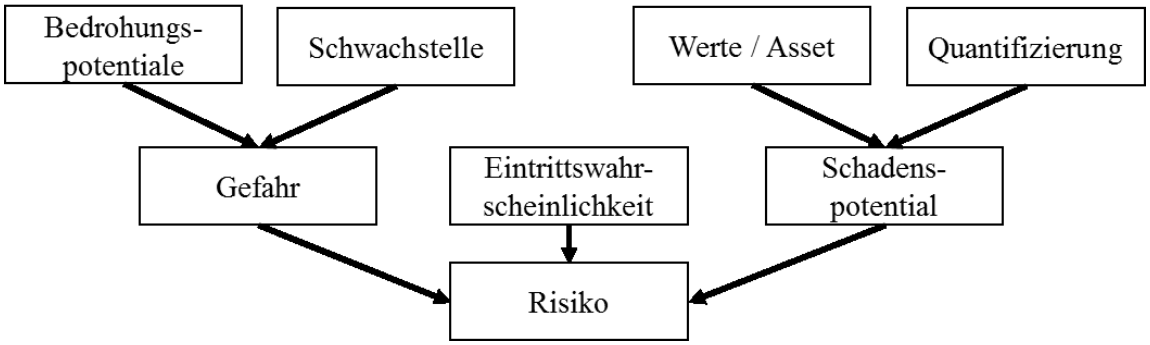

Abbildung 11: Bedrohungen, Werte und Risiken[246]

ISO/IEC 27000 definiert Risikoanalysen als systematischen Prozess zur Identifikation und Einschätzung des Umfangs von Risiken. „Im Rahmen einer Risikoanalyse werden Ursachen und Konsequenzen von gefährdenden Ereignissen untersucht und bewertet.“[247] Die Grundstruktur einer Risikoanalyse ist in Abbildung 12 illustriert und eine detaillierte Beschreibung kann bei HEINRICH et al.[248] eingesehen werden.

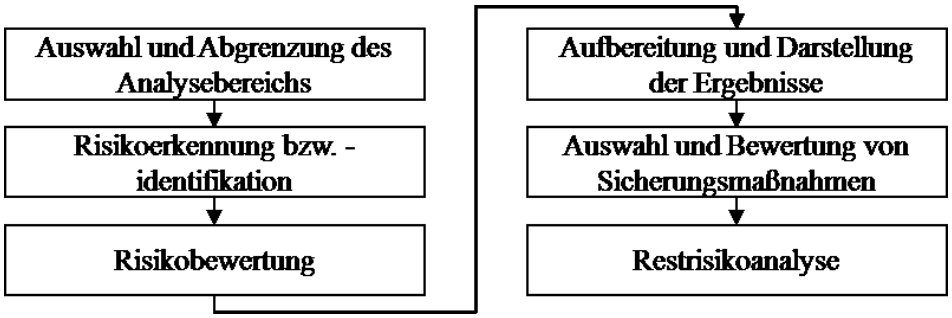

Abbildung 12: Grundstruktur einer Risikoanalyse[249]

Eine Aussage von DESOUZA & AWAZU verdeutlicht, dass wenn hingegen die Signifikanz der Bedrohung hoch und der Wissenswert gering ist, macht es aus wirtschaftlichen Gründen wenig Sinn in den Wissensschutz und damit in eine Risikoanalyse zu investieren.[250] Damit eine IT-Beratung die Wissensrisiken erkennen und analysieren kann, ist dem Gestaltungsziel folgend ein Risikoinformationssystem in Form eines Wissensschutz-Referenzmodells zu entwickeln.

Dieses Wissensrisiko bei der Leistungserbringung mit externen nationalen und internationalen IT-Dienstleistern ist in der Abbildung 13 hervorgehoben und soll durch entsprechende vorbeugende Maßnahmen auf ein vertretbares Restrisiko reduziert werden.[251] Das Restrisiko ist ein Risiko, dass nicht durch gezielte Maßnahmen reduziert werden kann oder von den Verantwortlichen akzeptiert wird.[252]

---

[246] Modifiziert nach: Devargas 1993, S. 54, Damm et al. 1999, S. 24, Yapp 2003, S. 174, Eckert 2004, S. 16.
[247] Heinrich et al. 2014, S. 512.
[248] Heinrich et al. 2014, S. 512 ff.
[249] Heinrich et al. 2014, S. 513.
[250] Vgl. Desouza & Awazu 2005, S. 32.
[251] Vgl. Devargas 1993, S. 54.
[252] Vgl. Heinrich et al. 2014, S. 509.

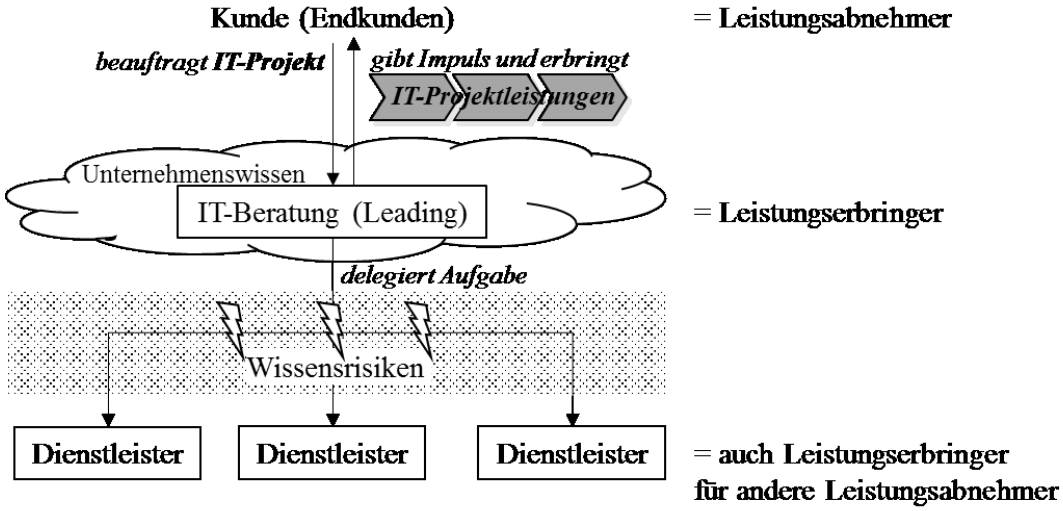

Abbildung 13: Übersicht zum Spannungsfeld der IT-Dienstleistungen und dem Wissensschutz[253]

Alle in- und ausländischen Dienstleister bedeuten für eine IT-Beratung ein Wissensrisiko und damit ein Risiko für die Wettbewerbsfähigkeit. Bei der strategischen Planung einer Dienstleisterbeziehung sind umfassende Kenntnisse über den Dienstleister und seine Mitarbeiter erforderlich. TRKMAN & DESOUZA weisen darauf hin, dass der unkontrollierte Wissensaustausch und die unkontrollierte Wissensübertragung zu katastrophalen Ergebnissen führen können.[254]

IT-Dienstleistungen und Anwendungssysteme

Bei der IT-Leistungsbeziehung wird zwischen Leistungserbringer und Leistungsabnehmer oder Auftraggeber differenziert. In der Literatur werden ebenso die Beziehungen Prinzipal-Agent[255], Client-Vendor[256] und Netzwerk[257] in diesem Zusammenhang erwähnt. Der Agent wird in der Literatur und in der Praxis ebenso als Dienstleister, Vendor, Supplier, Lieferant, (externe) Partner, Sourcing-Partner, Allianzpartner[258] oder Erfüllungsgehilfe bezeichnet. In der Arbeit wird der Begriff (externe IT-) Dienstleister verwendet, da es sich bei der Geschäftsbeziehung um eine IT-Dienstleistung handelt.[259]

In Abbildung 14 ist dargestellt, dass dependent von der Betrachtungsperspektive in der Wertschöpfungskette eine IT-Beratung als Leistungserbringer (Agent) als auch als Auftraggeber (Prinzipal) gegenüber den vorgelagerten Leistungserbringern agiert.[260] Diese verschiedenen

---

[253] Eigene Darstellung.
[254] Vgl. Trkman & Desouza 2012, S. 2, Hackney et al. 2008.
[255] Vgl. Desouza & Awazu 2004.
[256] Vgl. Nassimbeni et al. 2012.
[257] "The term 'network' is often used casually (Cova et al., 2010). Various kinds of networks are postulated (Cova et al., 2010), such as alliance network (Baum et al., 2000); alliance partners (Becerra et al., 2008); business net (Möller and Svahn, 2006); cluster (Liao, 2010); collaborative or cooperative arrangement (Provan et al., 2007); co-opetition (Li et al., 2011); external knowledge sourcing (Carayannopoulos and Auster, 2010); innovation outsourcing (Baloh et al., 2008); inter-organizational knowledge network (Dawes et al., 2009; Hackney et al., 2008); knowledge-sharing network (Dyer and Nobeoka, 2000); network of practice (Agterberg et al., 2010); strategic alliance (Connell and Voola, 2007); supply network (Kärkkäinen et al., 2003; Straub et al., 2004), and vertical partnership (Kotabe et al., 2003) - to mention just a few." Trkman & Desouza 2012, S. 2.
[258] Vgl. Trkman & Desouza 2012, S. 2, Becerra et al. 2008.
[259] Vgl. Abschnitt 2.2.2.
[260] Vgl. Zarnekow 2007, S. 54.

Wertschöpfungsstufen bzw. -tiefen visualisiert TEUBNER in einem Schichtenmodell der betrieblichen Informationsstruktur.[261] An dieser Stelle soll darauf hingewiesen werden, dass sich dieses Schichtenmodell auf das IT-Service Management fokussiert und damit auf die IT-Dienstleistungen, die ein breites Leistungsspektrum neben der Umsetzung von der ISE beinhaltet. In der vorliegenden Arbeit wird der ausschließliche Fokus auf die Anwendungssystemschicht[262] gelegt, bei der eine IT-Beratung (Leistungsabnehmer) mit einem oder mehreren externen IT-Dienstleister(n) (Leistungserbringer) aufgabenspezifische / punktuelle Projektunterstützung in der ISE vereinbart.

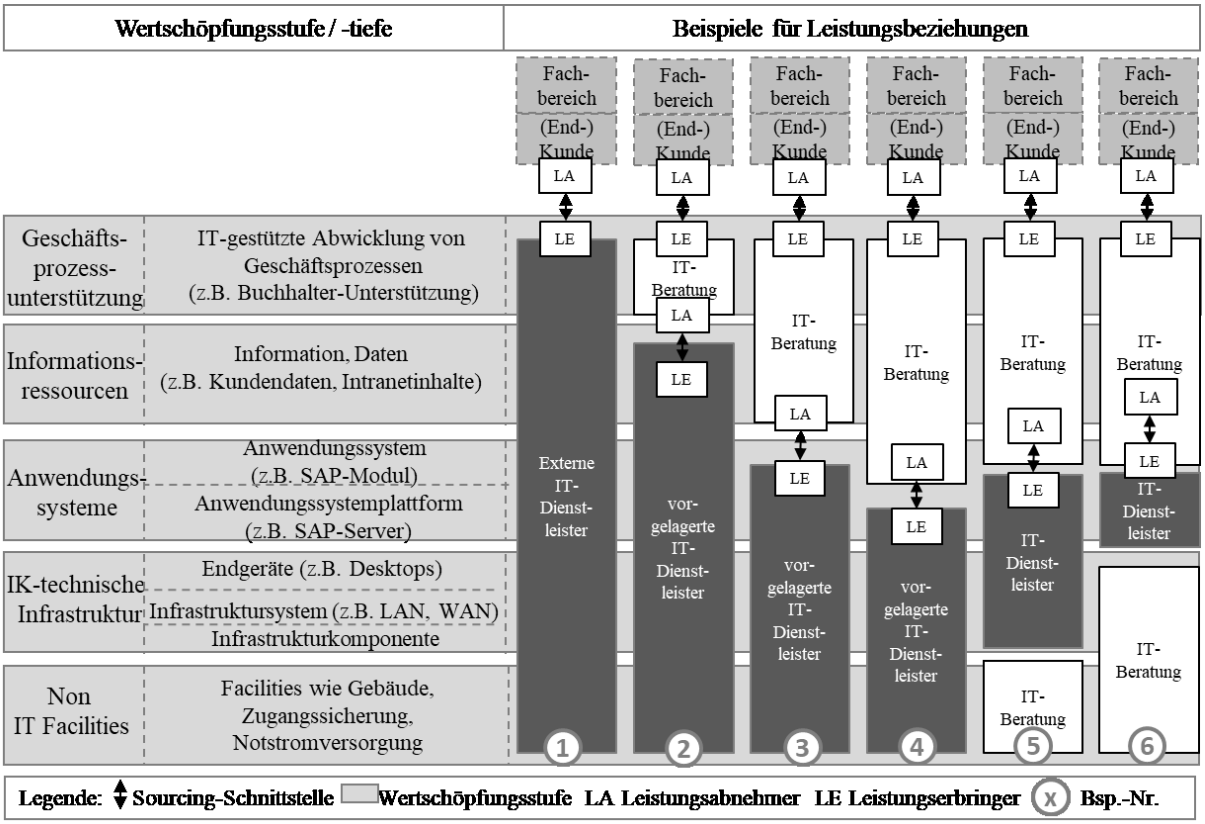

Abbildung 14: Beispiele für Leistungsbeziehungen im Schichtenmodell der betrieblichen Informationsstruktur[263]

Diese IT-Anwendungssysteme, kurz auch Anwendungssysteme, werden von STAHLKNECHT & HASENKAMP wie folgt definiert. Anwendungssysteme sind:

- „im engeren Sinne die Gesamtheit aller Programme, das heißt die Anwendungssoftware, und die zugehörigen Daten für ein konkretes betriebliches Anwendungsgebiet und
- im weiteren Sinne zusätzlich die für die Nutzung der Anwendungssoftware benötigte Hardware und Systemsoftware, die erforderlichen Kommunikationseinrichtungen und – je nach Betrachtungsweise - auch die Benutzer“. [264]

[261] Vgl. Brocke 2011, S. 14, Teubner 2008, S. 42.
[262] Siehe Beispiel Nr. 6 in der Abbildung 14.
[263] Modifiziert nach: Brocke 2011, S. 15, in Anlehnung an Teubner 2008, S. 42.
[264] Stahlknecht & Hasenkamp 2005, S. 326.

Diese Anwendungssysteme können für alle betrieblichen Arbeitsgebiete eingesetzt werden.[265] STAHLKNECHT & HASENKAMP unterteilen betriebliche Anwendungssysteme nach ihrem Verwendungszweck in operative Systeme, Systeme für den elektronischen Informationsaustausch, Führungssysteme und Querschnittssysteme.[266] Die weiteren Details sind in Abbildung 15 visualisiert.

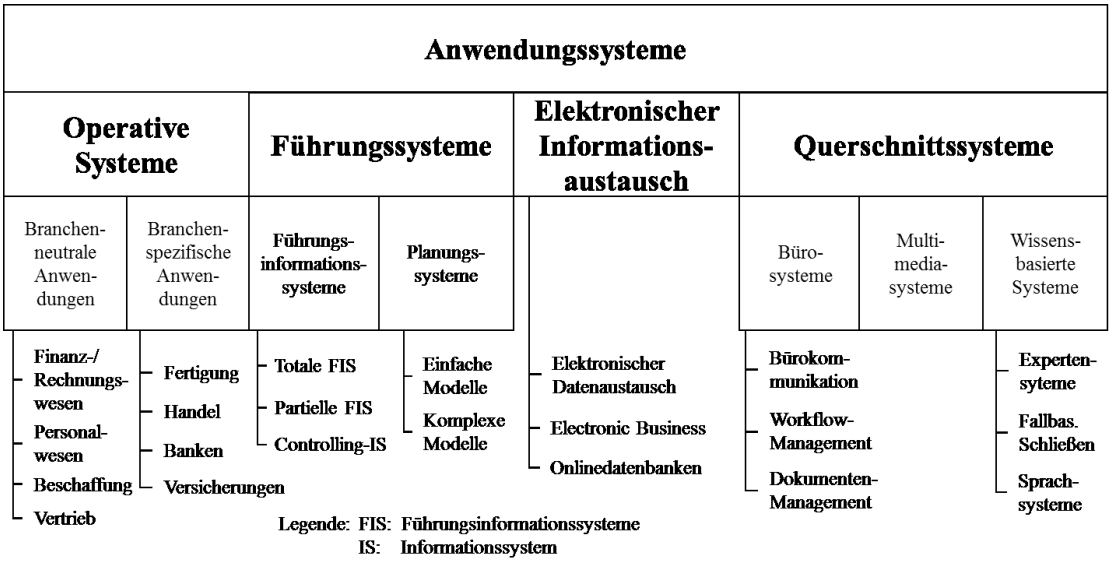

Abbildung 15: Einteilung betrieblicher Anwendungssysteme nach dem Verwendungszweck[267]

An dieser Stelle wird noch einmal auf Abschnitt 2.2.2 verwiesen. Die Individualsoftware ist der Fokus der vorliegenden Untersuchung und dazu gehören alle Anwendungssysteme, die individuell von einer IT-Beratung entwickelt werden. Der Wissensschutz in der vorliegenden Arbeit konzentriert sich besonders auf die Querschnittssysteme (wissensbasierte Systeme), da diese einen hohen individuellen Grad für die Kunden aufweisen und für diese Anwendungszwecke kaum Standardsoftware existiert. Für die anderen beiden betrieblichen Anwendungssysteme wie Administrations- und Dispositionssysteme sowie Führungssysteme ist ein hoher Individualisierungsgrad abhängig vom Branchenumfeld.

Wissensschutz bei KIBS / IT-Beratungen[268]

Die Untersuchungen von MILES et al., AMARA et al. und PÄÄLLYSAHO & KUUSISTO zeigen, dass hoch-technologisierte KIBS und besonders IKTs die intensivsten Anwender von Wissensschutzmechanismen sind.[269] Die Studie von BOLISANI et al. bestätigt, dass größere Unternehmen eher geneigt sind Wissensschutzmechanismen zu verwenden. Die Vielfalt der verwendeten Wissensschutzmechanismen ändert sich jedoch nicht mit der Unternehmensgröße.[270] Nach den Untersuchungen von BOLISANI et al. sind Unternehmen, die mit Auftraggebern und Dienstleistern zusammenarbeiten und diese als eine wesentliche Wissensquelle betrachten, die die auf

[265] Vgl. Stahlknecht & Hasenkamp 2005, S. 326.
[266] Vgl. Stahlknecht & Hasenkamp 2005, S. 326.
[267] Modifiziert nach: Stahlknecht & Hasenkamp 2005, S. 327
[268] Weitere Erkenntnisse zum Wissensschutz mit IT-Bezug sind im Unterkapitel 4.1 aufgeführt.
[269] Vgl. Bolisani et al. 2013, S. 206, Miles et al. 2000, Amara et al. 2008, Päällysaho & Kuusisto 2008a, b.
[270] Vgl. Bolisani et al. 2013, S. 206.

Wissensschutzmechanismen zurückgreifen. Diese Unternehmen nutzen eher eine Kombination von Wissensschutzmechanismen.[271]

BOLISANI et al. aggregieren die Erkenntnisse von AMARA et al. zum Wissensschutz und KIBS-Unternehmen, die die Beziehung zwischen Wissensschutz- und WM-Strategien neben den anderen Problemfeldern adressieren. Diese sind:

- KIBS-Unternehmen verwenden meist informelle Wissensschutzmechanismen.
- KIBS-Unternehmen wenden verschiedene Alternative Wissensschutzmechanismen an, die sich gegenseitig ergänzen und verstärken.
- Der immaterielle Charakter der KIBS-Aktivitäten kann diese Unternehmen veranlassen, auf eine Kombination von Wissensschutzmechanismen zu vertrauen.
- Es besteht ein Zusammenhang zwischen Wissensschutz und Forschungs- und Entwicklungsintensität.
- Zwischen den verschiedenen Branchen gibt es einige signifikante Unterschiede bei der Verwendung der Wissensschutzmechanismen.
- Die Verwendung der Wissensschutzmechanismen nimmt mit zunehmender Unternehmensgröße zu, vor allem bei den formalen Schutzmechanismen (wie Urheberrechten, Patenten usw.).[272]

BOLISANI et al. postulieren zudem, dass Unternehmen mit angepassten Dienstleistungen eine höhere Neigung haben Wissensschutz anzuwenden als Organisationen mit Standarddienstleistungen.[273] Die ISE für die Auftraggeber kann zu diesen angepassten Dienstleistungen zugeordnet werden.

Zusammenfassend ist festzuhalten, dass das Wissensrisiko bei den in der Arbeit fokussierten IT-Dienstleistungen unter Beteiligung von externen Beratern dargestellt und transparent gemacht ist. Die Relevanz des Wissensschutzes und seine Anwendung in IT-Beratungen ist dargestellt.[274] Herausgearbeitet und eingegrenzt wird die fokussierte IT-Leistungsbeziehung auf die Anwendungssystemebene. Die infrage kommenden betrieblichen Anwendungssysteme sind beschrieben, auf die sich der Wissensschutz des Referenzmodells beziehen kann.

2.3 Theoretische Fundierung

Zur theoretischen Fundierung werden in diesem Unterkapitel die Grundlagen deskribiert. Die Prinzipal-Agent-Theorie bildet die Haupttheorie für diese Arbeit. DESOUZA & AWAZU haben die Prinzipal-Agenten-Beziehung mit den Schwerpunkten auf Transaktionskosten, WM, organisationalem Wissen und Managementperspektive genauer untersucht.[275] In diesem Zusammenhang wird auch der Wissensschutz aufgeführt. Ihre Erkenntnisse sind Grundlage für die Arbeit und werden deshalb hier dargestellt. MANHART & THALMANN identifizieren bei ihrem *Literature Review* zum Wissensschutz die theoretischen Perspektiven der Transaktionskostentheorie, die *relationale Perspektive* und die *Resource-based view*.[276] Die vorliegende Arbeit

[271] Vgl. Bolisani et al. 2013, S. 203.
[272] Vgl. Bolisani et al. 2013, S. 197, Amara et al. 2008.
[273] Vgl. Bolisani et al. 2013, S. 208.
[274] Weitere Präzisierung im Unterkapitel 4.1.
[275] Vgl. Desouza & Awazu 2004, S. 10 f.
[276] Vgl. Manhart & Thalmann 2015, S. 199 ff.

weist ebenso Schnittmengen zu diesen drei Perspektiven auf. Die betreffenden Schnittmengen werden beschrieben.

2.3.1 Prinzipal-Agent-Theorie

Die Theorie betrachtet die Relation zwischen einem Auftragnehmer (Agent) und einem Auftraggeber (Prinzipal), bei der eine Verhaltensunsicherheit des Agenten vorliegt.[277] Grundgedanke ist, dass der Prinzipal mit Hilfe von Lösungsansätzen seine Ziele entgegen der vorliegenden Informationsasymmetrie erreicht. Wegen des opportunistischen Verhaltens eines Agenten ist davon auszugehen, dass er bestrebt ist seinen Nutzen bei dieser Beziehung zu maximieren.[278] Aufbauend auf dem Werk von COASE[279] begründen JENSEN & MECKLING die Theorie und definieren eine Agentenbeziehung als Vertrag, bei dem ein oder mehrere Prinzipal(e) mit einem anderen Agenten zusammen eine Dienstleistung durchführen, die Entscheidungsbefugnis für den Agenten beinhaltet.[280]

Diese Arbeit fokussiert diese Prinzipal-Agenten-Beziehung aus der Projektmanagement-Perspektive mit externen IT-Dienstleistern und strebt die Unsicherheitsvermeidung für den Prinzipal an. Die Forschungsliteratur bezeichnet diese Beziehungsart ebenso als Client-Vendor[281]. GHODESWAR & VAIDYANATHAN verwenden den Vendor[282] Begriff im Zusammenhang mit Prinzipal und Client. In der vorliegenden Arbeit wird die Bezeichnung Prinzipal und Agent genutzt.

Nach DESOUZA & AWAZU entstand die Prinzipal-Agent-Theorie ursprünglich aus dem *risk-sharing* Verhalten zwischen Agenten, die unter Unsicherheitsbedingungen handelten. Sie basiert auf den drei Annahmen, die nachfolgend beschrieben werden:

- beschränkter Rationalität,
- Informationskosten und
- Heterogenität der Risikopräferenzen.

Jeder Prinzipal ist rational beschränkt, das erschwert die Beobachtung des Agenten-Verhaltens. Die Verhaltensinformationen sind immer mit Kosten verbunden. Nützliche Informationen erhält der Prinzipal nicht ohne entsprechenden Aufwand. Diese Informationen und damit die Aufwandskosten sind erforderlich, um das Verhalten eines Agenten zu überwachen. Zwischen dem Prinzipal und dem Agenten besteht dadurch immer eine Risikopräferenzlücke. Ein Prinzipal gilt in der Regel als risikoneutral und ein Agent ist normalerweise als riskant anzusehen.[283]

Die Probleme, die bei der Beziehung zwischen Prinzipal und Agent entstehen, werden auch Agenturprobleme genannt. Die Agenturprobleme ergeben sich aus Informationsasymmetrie

[277] Jensen & Meckling 1976.
[278] Vgl. Desouza & Awazu 2004, S. 8.
[279] Coase 1937.
[280] Vgl. Jensen & Meckling 1976, S. 308.
[281] Nassimbeni et al. 2012.
[282] Ghodeswar & Vaidyanathan 2008.
[283] Vgl. Desouza & Awazu 2004, S. 10.

und opportunistischem Verhalten. Zunächst wird auf die Probleme bei der Informationsasymmetrie eingegangen. Auch das opportunistische[284] Verhalten ist bei einer IT-Beratung bei der ISE mit externen Dienstleistern gegeben und wird weiter unten deskribiert. In der Tabelle 6 sind die Grundtypen der Verhaltensunsicherheiten *Hidden Characteristics*, *Hidden Intentions, Hidden Knowledge*[285] / *Hidden Information*[286] und *Hidden Actions* beschrieben, die mit der traditionellen Bezeichnung der Agenturprobleme *Adverse Selection*, *Hold-up* und *Moral Hazard* verbunden werden.[287]

Tabelle 6: Grundtypen der Verhaltensunsicherheit[288]

Informations-asymmetrie	Beschreibung der Situationsmerkmale
Hidden Characteristics (Adverse Selection)	Vor Vertragsschluss hat der Agent private Information über seine Merkmale, z. B. seine Qualifikation. Der Agent kann dem Prinzipal Qualifikationen vorspiegeln, über die er gar nicht verfügt. Für den Prinzipal ergibt sich das Problem der Qualitätsunsicherheit. Er wird erst nach Vertragsabschluss erfahren, welche Qualifikationen der Agent tatsächlich besitzt.
Hidden Intentions (Hold-up)	Nach Vertragsschluss hat der Agent aufgrund der vertraglichen Bindung zwischen dem Prinzipal und ihm die Gelegenheit, verborgene Absichten umzusetzen. Er kann willentlich unfair gegen den Prinzipal handeln. Der Prinzipal kann nicht einfach aus dem Vertragsverhältnis austreten, weil ihm dadurch Kosten entstehen. Er verliert die Investitionskosten, die er ausgab, um den Vertrag mit dem Agenten abzuschließen (sunk costs).
Hidden Knowledge/ Information (Moral Hazard)	Nach Vertragsabschluss kann der Agent privates Wissen über exogene Einflussfaktoren erlangen, das zur Beurteilung seiner Tätigkeit und des Ergebnisses relevant ist. Es kann sich dabei um Expertenwissen über Umwelteinflüsse, Informationen über die Erfolgsaussichten von Handlungsalternativen oder um Wissen und die Ergebnisse gewählter Handlungen handeln. Er kann dieses Wissen opportunistisch ausnutzen.
Hidden Actions (Moral Hazard)	Nach Vertragsabschluss kann der Agent aufgrund der Ressourcenplastizität Handlungsalternativen auswählen. Dabei kann er ein geringeres Arbeitsvolumen wählen oder ein größeres Arbeitsvolumen vortäuschen, ohne dass der Prinzipal dies beobachten oder beurteilen kann.

Diese verborgenen Verhaltensmuster sind ebenso bei einer Wissenstransaktion zwischen IT-Beratung und externen Dienstleister gegenwärtig. Dadurch entstehen für den Auftraggeber Risiken und Probleme. Die möglichen Risiken bei einer Outsourcingbeziehung, die ebenso zugrunde gelegt werden können, fassen NASSIMBENI et al. aus der Forschungsliteratur zusammen, diese sind:

- Kontrollverlust,
- schlechtere Servicequalität,
- opportunistisches Dienstleister-/Lieferantenverhalten,
- Verlust von internem Fachwissen,
- Kosteneskalation,

[284] Vgl. Abschnitt 4.3.1.
[285] Weiershäuser 1996.
[286] Wolff 1995.
[287] Vgl. Saam 2002, S. 29.
[288] In Anlehnung an Saam 2002, S. 30.

- Dienstleister-/Lieferantenabhängigkeit,
- Fehlende erforderliche Dienstleisterressourcen,
- Verlust vertraulicher Daten und
- Verletzung von Intellectual Property Rechten.[289]

SAAM fasst die Grundtypen von Agenturproblemen zusammen und charakterisiert sie (Tabelle 7). In der Tabelle sind die Lösungsansätze hervorgehoben, die das Modell adressiert und erweitert.

Tabelle 7: Grundtypen von Agenturproblemen[290]

Agentur-Problem	**adverse selection**	**hold-up**	**moral hazard**	**moral hazard**
Informations-asymmetrie	hidden characteristics	hidden intentions	hidden knowledge / hidden information	hidden action
Informations-problem des Prinzipals	Qualifikation des Agenten unbekannt	Absicht des Agenten unbekannt	Fach-/Prozesswissen des Agenten unbekannt	Anstrengung und Arbeitseinsatz des Agenten nicht beobachtbar oder beurteilbar
Zeitpunkt	vor Vertragsabschluss	nach Vertragsabschluss	nach Vertragsabschluss	nach Vertragsabschluss
Verhaltens-formen (Interpretation)	exogen gegeben (Qualifikation)	willensabhängig (Fairness)	exogen gegeben (Fach-/Prozesswissen)	willensabhängig (Anstrengung)
Verhaltens-transparenz	ex post bekannt	ex post bekannt	ex post verborgen	ex post verborgen
Rahmen-bedingung	Informations-ineffizienz	sunk costs	Informations-ineffizienz	Ressourcen-plastizität
Lösungs-ansätze	Selbstwahlschemata, **Signalisieren**, **Screening**	Autoritätssysteme, Spieltheoretische Lösungsdesigns	Anreizsysteme, Selbstwahlsysteme, **Signalisieren**, **Screening**	Anreizsysteme, Selbstbindung, **Kontrollsystem**

Infolge der genannten Probleme und Risiken kann ein Zielkonflikt zwischen dem Prinzipal und einem Agenten entstehen und es ist zu validieren, was für eine IT-Beratung am effektivsten ist.[291] Das Ziel vom Prinzipal ist es nach DESOUZA & AWAZU, diese Konflikte zu lösen und das Agentenverhalten auszurichten, indem die mit dem Konflikt verbundenen Kosten minimiert werden. Zu den Prinzipal-Kosten gehören die Monitoring-, Bindungs- und die Opportunitätskosten. Sollten die Monitoringkosten entsprechend hoch sein, dann ist es für den Prinzipal besser die Transaktion ohne den Agenten Einsatz durchzuführen. Ein Prinzipal wird nur einen

[289] Vgl. Nassimbeni et al. 2012, S. 407, Bounfour 1999, Ellram et al. 2008, Embleton & Wright 1998, Gonzalez et al. 2006, Rebernik & Bradac 2006.
[290] Saam 2002, S. 30, in Anlehnung an Spremann 1990, Picot & Neuburger 1995, Weiershäuser 1996; zu ähnlichen Klassifizierungsansätzen vgl. Breid 1995, S. 824, Dietl 1993, S. 125, Kiener 1989, S. 25, Strong & Walter 1987, S. 178 f.
[291] Vgl. Desouza & Awazu 2004, S. 10, Jensen & Meckling 1976.

Agenten involvieren, wenn die Transaktionsvorteile die -kosten überwiegen.[292] Diese drei Kostenarten sind demnach zu prüfen:

- Monitoringkosten: „includes measurement cost of an agent's behavior and an incentive cost that lets the agent's behavior reflects principal's goal".
- Bindungskosten: „is the cost of sharing risk between agents".
- Opportunitätskosten: "is associated with a transaction being locked or committed to a given agent".[293]

In der Abbildung 16 sind die Agenturprobleme und die möglichen Lösungsansätze vor und nach Vertragsabschluss visualisiert dargestellt. Die identifizierte Forschungslücke legt zugrunde, dass selbst wenn die Verträge alle relevanten Wissensschutzklauseln enthalten, wäre der Nachweis einer Vertragsverletzung in Bezug auf implizites Wissen nicht oder diffizil nachweisbar. Darauffolgend werden die adressierten und zu erweiternden Lösungsansätze beschrieben.

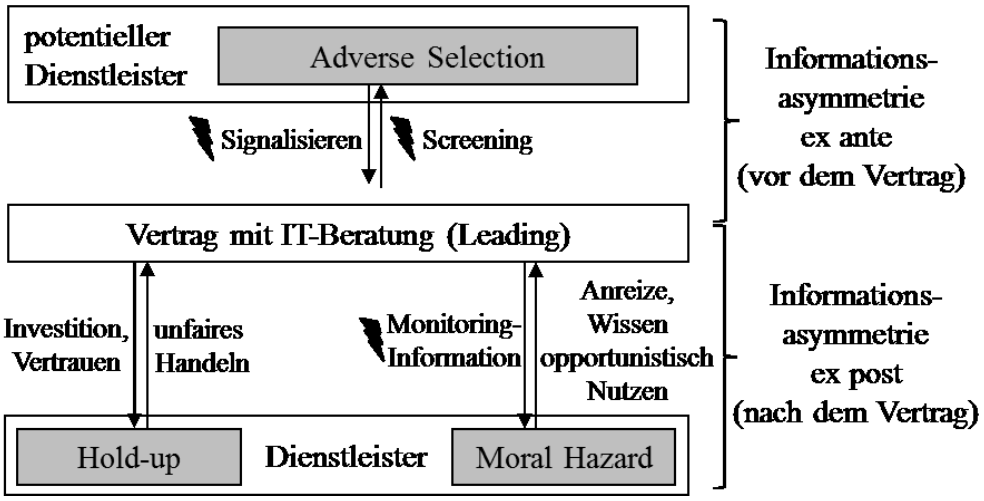

Abbildung 16: Verhaltensrisiken vor und nach Vertragsschließung bei Prinzipal-Agenten-Beziehungen[294]

Die Lösungsansätze *Signalisieren* und *Screening* vor der vertraglichen Vereinbarung sollen die Eignung des Dienstleisters verifizieren. Zum *Signalisieren* eines Dienstleisters (Agenten) gehören alle Mittel, die seine Dienstleistungsqualität von potentiellen Mitbewerbern differenziert, dazu gehören zum Beispiel Zertifikate, Zeugnisse, Garantien oder Referenzen.[295]

Der Prinzipal versucht beim *Screening* alle nicht gefilterten Informationen des Agenten zu erhalten, um die potentielle Leistungsqualität zu validieren.[296] Um die Eigenschaften und Qualifikationen eines Agenten zu bestimmen, recherchiert der Prinzipal valide Quellen.[297] Relevante

[292] Vgl. Desouza & Awazu 2004, S. 10.
[293] Vgl. Desouza & Awazu 2004, S. 10.
[294] Modifziert nach: http://www.daswirtschaftslexikon.com/d/vertragstheorie/vertragstheorie.htm, zuletzt abgerufen 10.10.2018.
[295] Vgl. Milgrom & Roberts 1992, S. 154 f., Backes-Gellner et al. 2001, S. 121 ff.
[296] Vgl. Großmann 2010, S. 92 ff.
[297] Vgl. Fritsch 2005, S. 298.

Informationen können zum Beispiel auch mit Assessment Center, Probezeiten, Gutachter-Verfahren und Selbst-Selektion bei Vertragsangeboten eruiert werden.[298] Diese Informationen sollen die Grundlage für eine fundierte *Dienstleisterauswahlentscheidung* bilden.

Das *Monitoring* des Agenten während des Projekteinsatzes soll die Informationsasymmetrien zum Prinzipal reduzieren.[299] Zu der systematischen Beobachtung eines Agenteneinsatzes gehören alle zweckgebundenen Aktivitäten, um die Einhaltung der vertraglichen Verpflichtungen zu prüfen.[300] Wie weiter oben erwähnt entstehen beim *Monitoring* Aufwandskosten.

Wegen dieser nicht zu unterschätzenden Aufwände und unter anderem dem opportunistischen Agentenverhalten sollten die Sourcingvorhaben nach DESOUZA von Beginn an bis zur Beendigung aus einer Schutzperspektive untersucht werden. Das beinhaltet zum Bespiel, dass bereits beim *Signalisieren* und *Screening* und damit bei der Bedarfsanalyse die möglichen Risiken und Probleme identifiziert werden, wenn eine konkrete Projektaufgabe durch einen Agenten erbracht werden soll. In dieser Anfangsphase ist die Schutzdimension zu reflektieren und zu validieren, wer für das Projektmanagement-Team benannt wird, um die Leistungen und deren Erfüllung vom Agenten zu evaluieren.[301] Wenn es um den Schutz des organisationalen Wissens geht, postulieren DESOUZA & AWAZU, dass die vertraglichen Beziehungen mit einem Agenten zu aufwendig sind. Für die Aufgabenerfüllung braucht der Agent Wissen und gleichzeitig muss das wertvolle organisationale Wissen definitiv präventiv gegenüber äußeren Interessen geschützt werden.[302] Das organisationale Wissen ist rar, wertvoll und unersetzlich, deshalb sollte der Auftraggeber sicherstellen, für welchen Zweck es eingesetzt wird.[303] Für den Prinzipal ist Wissen als eine Machtposition[304] zu sehen, die zu einer endogenen Transition für den Agenten führen kann.[305] Der Wissenstransfer vom Prinzipal an den Agenten verringert somit den Wissenswert für den vormaligen Besitzer.

Bei der ISE müssen zum Teil Agenten mit spezifischem Wissen involviert werden. Denn ein Agent mit evident effektiveren Dienstleistungen in der Wertschöpfungskette kann nicht so leicht durch einen anderen Agenten ersetzt werden.[306] Gewisses Fachwissen und Technologiewissen ist spezifisch, schwer verfügbar und kann damit Alleinstellungsmerkmale aufweisen. Die dyadische Beziehung zwischen dem Prinzipal und dem Agenten basiert hauptsächlich auf einer Austauschperspektive bei der beide in Synergie arbeiten, um einen neuen Wert zu schaffen, der höher ist als wie sie ihn individuell erreichen könnten.[307] Um diesen neuen Wert in der untersuchten ISE zu generieren sind externe Dienstleister mit spezifischen Wissen zu involvieren.

---

[298] In Anlehnung an daswirtschaftslexikon 2016
[299] Vgl. Arrow 1991, S. 45 f., Milgrom & Roberts 1992, S. 186 f.
[300] Vgl. Ripperger 2005, S. 66.
[301] Vgl. Desouza 2008, S. 291.
[302] Vgl. Desouza & Awazu 2004, S. 11.
[303] Vgl. Desouza & Awazu 2004, S. 10.
[304] Vgl. Crozier & Friedberg 1979, S. 51, Scott 1986, S. 367.
[305] Vgl. Kräkel 2002, S. 222.
[306] Vgl. Ghodeswar & Vaidyanathan 2008, S. 30.
[307] Vgl. Ghodeswar & Vaidyanathan 2008, S. 30.

Bei der Prinzipal-Agenten-Beziehung zwischen einer IT-Beratung und den externen IT-Dienstleistern, die IT-Projekte unterstützen, handelt es sich um eine asymmetrische Beziehung. Nach MENTZER et al. und TRKMAN & DESOUZA sind asymmetrische Kollaborationen im Vergleich zu einer symmetrischen Kollaboration, bei der beide gleichermaßen voneinander abhängig sind, dysfunktionaler, weniger stabil, weniger engagiert und weniger vertrauensvoll. Bei der symmetrischen Kollaboration besteht eine relative Abhängigkeit und diese Interdependenz hat eine positive Korrelation auf den Informationsaustausch und die allgemeine strategische Orientierung.[308]

In dieser asymmetrischen Beziehung agiert die Logik des kollektiven Handelns, da rationale selbstinteressierte Individuen nicht freiwillig handeln um ihre gemeinsamen oder Gruppeninteressen zu erreichen.[309] Dieser Zustand liegt vor, wenn dem Agenten andere Anreize bedeutender sind als das Gemeinwohl des Prinzipals. Diese Konstellation ist bei der ISE präsent, sie profitiert durch die Wiederverwendung und baut auf dem Erprobtem auf.[310] Von dieser Wiederverwendbarkeit können die eingesetzten externen Berater und damit die Dienstleister profitieren. DESOUZA & AWAZU heben hervor, dass wenn ein Agent Zugriff auf wertvolle Wissensobjekte erhält und diese vorteilhaft außerhalb vom Prinzipal anwendet, ist eine wahrscheinliche Konsequenz, dass der Prinzipal keine Aufträge mehr erhält und damit in Konkurs geht.[311]

Zusammenfassend werden in diesem Abschnitt die vorliegende Relation zwischen einer IT-Beratung und den externen Dienstleistern erörtert. Dazu gehören die damit verbundenen möglichen Risiken, (Interessens-)Konflikte, Probleme und Aufwände die bei einer asymmetrischen Prinzipal-Agenten-Kollaboration entstehen können.

2.3.2 Weitere theoretische Ansatzpunkte

Aufgrund der Interdisziplinarität des Modells liegen ebenso Ansatzpunkte zu weiteren Theorien vor. Die betreffenden Schnittmengen der Arbeit zur Transaktionskostentheorie, *relationalen Perspektive*, *Resource-based view* und *Knowledge-based view* werden im Folgenden deskribiert.

Transaktionskostentheorie[312]

Die weiter oben erwähnten Transaktionskosten basieren auf der Transaktionskostentheorie (TAK-Theorie), die ein Teilgebiet der Institutionenökonomie ist. Die Theorie wurde von COASE zum ersten Mal erwähnt und dessen Vorstellungen von WILLIAMSON fortentwickelt. Beide adressierten die Frage, wann es sinnvoll ist, Transaktionen innerhalb einer Institution durchzuführen oder über den Markt abzuwickeln. Alternativ formuliert befasst sich die TAK-Theorie

[308] Vgl. Trkman & Desouza 2012, S. 7, Mentzer et al. 2000.
[309] Vgl. Desouza & Awazu 2004, S. 10, Olson 1971.
[310] Vgl. Desouza & Awazu 2004, S. 10 f.
[311] Vgl. Desouza & Awazu 2004, S. 11.
[312] Coase 1937, Williamson 1975.

mit den Kosten, die bei der Koordination einer Geschäftsbeziehung entstehen.[313] Eine Transaktion wird von WILLIAMSON wie folgt definiert:

> „Eine Transaktion findet statt, wenn ein Gut oder eine Leistung über eine technisch trennbare Schnittstelle hinweg übertragen wird. Eine Tätigkeitsphase wird beendet; eine andere beginnt.“[314]

Dabei werden alle auftretenden Transaktionen in einer Institution und die über den Markt laufenden spezifiziert. Demnach sind die Transaktionskosten Marktbenutzungs- oder Hirarchiekosten. Im Vergleich zur neoklassischen Sichtweise, dass der vollkommene Markt keine Institutionen braucht und dadurch nur relevante Transaktionskosten entstehen, war die neue Erkenntnis, die Betriebskosten oder die Reibungskosten des Wirtschaftssystems in die Untersuchung von wirtschaftlichen Zusammenhängen miteinzubeziehen.[315]

Die TAK-Theorie bezieht sich auch auf die Property-Rights-Theorie, da auch bei der Definition und Übertragung von Verfügungsrechten Transaktionskosten entstehen. Diese Aufwandskosten entstehen zum Beispiel bei einer Patentanmeldung mit seinen bürokratischen Verfahren und der vorausgehenden weltweiten Recherche.[316] Die rechtliche Genehmigung zur Festschreibung von bestimmten Eigenschaften wie auch der Aufwand für die Umsetzung des Wissensschutz-Referenzmodell gehören damit zu den Transaktionskosten. Vor einer Transaktion und damit vor der Beauftragung einer IT-Projektdienstleistung muss folglich geprüft werden, ob erstens das Risiko mit dem Markt oder zweitens einer dem Unternehmen bekannten Institution eingegangen werden sollte. Drittens sollte die Realisierung eines IT-Projektes innerhalb einer IT-Beratung bevorzugt werden, wenn sie kosteneffizienter als die Marktlösung umgesetzt werden kann. COASE und WILLIAMSON fokussieren sich bei der TAK-Theorie weniger auf die Kosten der unternehmensinternen Koordination. Aus diesem Grund konzentrieren andere wissenschaftliche Arbeiten diesen Forschungsbereich und definieren Aktivitäten mit immateriellen und wissensintensiven Gütern als Transaktionen, die definitiv innerhalb einer IT-Beratung realisiert werden sollten.[317] Entscheidet eine IT-Beratung, den Markt nicht zu internalisieren, entstehen vor und nach dem Vertragsabschluss Kosten für eine Transaktion:

- Ex-ante Transaktionskosten (Such-, Anbahnungs- und Einigungskosten) und
- Ex-post Transaktionskosten (Abwicklungs-, Kontroll-, Steuerungs- und Anpassungskosten).[318]

Die Höhe der TAK wird, ausgehend von der beschränkten Rationalität, der Annahme opportunistischen Verhaltens und der Unterstellung der Risikoneutralität der Akteure, durch die folgenden drei Charakteristika determiniert:

1. Spezifität der für eine Transaktion notwendigen Investitionen
2. Unsicherheit in der Handlungsumwelt

---

[313] Vgl. Kutschker & Schmid 2011, S. 454 f.
[314] Williamson 1985, 1990, S. 1.
[315] Vgl. Göbel 2002, S. 132.
[316] Vgl. Richter & Furubotn 1996, S. 46 ff.
[317] Das Arrow-Paradox in der Wissensschaft diskutiert die Gründe für eine notwendige Internalisierung von wissensintensiven Gütern. Vgl. Arrow 1974, Kutschker & Schmid 2011, S. 456.
[318] Vgl. Kaas 1995a, S. 4.

3. Häufigkeit der Transaktion[319]

Erstens, umso spezifischer oder individualisierter eine Transaktion ist, desto höher ist die Interdependenz des Nachfragers zum Leistungsanbieter, da weniger Optionen für geeignete Transaktionspartner existieren. Zudem ist ein Anbieterwechsel wiederum mit Aufwänden und Kosten verbunden. Zweitens, die Unsicherheit beim Nachfrager besteht bei den möglichen Umweltveränderungen und dem zukünftigen Verhalten des Vertragspartners. Unsicherheit kann auch nach dieser Theorie (siehe 2.3.1) durch das opportunistische Verhalten des Leistungsanbieters exploitiert werden.[320] Drittens, umso häufiger eine Transaktion durchgeführt wird, desto geringer sind die TAK vom Nachfrager und Leistungsanbieter, da die individuellen Rahmenbedingungen wie Informationsstände und Bedürfnisse bekannt sind und keine zusätzlichen Beschaffungsaufwände entstehen.[321] Zudem werden bei einer wiederholten Transaktion die Kontrollaufwände durch das gegenseitige Vertrauen reduziert.[322] Zusammenfassend bestimmen die Häufigkeit der Transaktion, die Höhe der Spezifizität sowie der Unsicherheit, ob eine Transaktion besser organisationsintern oder im Markt kosteneffizienter durchzuführen ist.[323]

Für DIBBERN & HEINZEL sind Transaktionskosten in der IT-Domäne die Kosten, die zur „Planung, Anpassung und Kontrolle der Aufgabenerfüllung in den einzelnen Funktionen der Informationsverarbeitung“[324] dienen. Dennoch schließen sie die IT-Güter (Hardware, Standardsoftware) wegen ihrer Unspezifität aus. Gleichwohl begründen die Autoren die TAK-Theorie mit Relation auf spezifisches und organisationsinternes Wissen der Mitarbeiter. Dieses Wissen erarbeiten sich die Mitarbeiter über einen langen Zeitraum durch Erkenntnisse und aufgebaute Fähigkeiten. Im Zusammenhang mit Wissenstransaktionen betrachtete LIEBESKIND die TAK.[325] Sie argumentiert, dass Unternehmen die entscheidende Rolle für das Schaffen und Erhalten der Wettbewerbsvorteile darstellen, wenn sie ihr wertvolles Wissen schützen können.[326] Die Arbeit nutzt die von LIEBESKIND dokumentierten Zusammenhänge und stützt sich auf ihre Erkenntnisse. Damit soll eine IT-Beratung mit dem Wissensschutz-Referenzmodell befähigt werden, eine Transaktion aus der Wissensperspektive zu bewerten.

Nach den Literaturerkenntnissen von MANHART & THALMANN konzentrieren sich bisherige Veröffentlichungen zu dieser Theorie auf die Untersuchung von formalen Wissensschutzmechanismen, jedoch nicht auf die informalen Wissensschutzmechanismen auf die sich diese Arbeit fokussiert.[327]

---

[319] Vgl. Kutschker & Schmid 2011, S. 454 f.
[320] Vgl. Kaas 1995b, S. 34 f.
[321] Vgl. Meffert & Bruhn 2009, S. 62.
[322] Vgl. Grund 1998, S. 93 f.
[323] Vgl. Kutschker & Schmid 2011, S. 454 f.
[324] Dibbern & Heinzel 2009, S. 120.
[325] Vgl. Liebeskind 1996, S. 97.
[326] Vgl. Liebeskind 1996, S. 93.
[327] Vgl. Manhart & Thalmann 2015, S. 200.

Relationale Perspektive

Um die entstehenden opportunistischen Probleme bei einer Prinzipal-Agenten-Beziehung zu lösen, nimmt das Vertrauen und damit die *relationale Perspektive* eine entscheidende Rolle ein. Damit das Wissensschutz-Referenzmodell aktionsfähig ist, muss die *relationale Perspektive* aufgenommen werden. Die *relationale Perspektive* konzentriert sich hauptsächlich darauf, wie das *relationale Kapital*, das heißt das gegenseitige Vertrauen, der Respekt und die Freundschaft in interorganisationalen Beziehungen das *Learning Paradox* beeinflusst.[328] Das *relationale Kapital* wird dafür genutzt:

- die externen Strukturen darzustellen,
- die Beziehungen zu Kunden, Dienstleistern, Lieferanten, Partnern und weiteren Interessensgruppen abzubilden und
- die Bedeutung des externen Umfeldes zu dokumentieren.[329]

Für LI et al. zeigt sich ein Defizit von *relationalem Kapital* in der Anwendung von formalen Wissensschutzmechanismen, da diese ein Zeichen für einen Vertrauensmangel zwischen den Unternehmen ist.[330] Sollten die formalen Mechanismen von einem Prinzipal nicht ausgeschöpft werden, dann vergibt dieser leichtfertig seine erarbeiteten Wettbewerbsvorteil und könnte bei einer Wissensschutzverletzung keine rechtlichen Schritte einleiten. Wie bereits geschrieben sind die formalen Wissensschutzmechanismen eine Voraussetzung für das Referenzmodell. Die Arbeit fokussiert die informalen Wissensschutzmechanismen bei denen umso mehr die Vertrauenssituation maßgebend ist und diesen Aspekt nimmt das Referenzmodell auf.

Die durch eine Vertrauensbeziehung belegten Verhaltensrisiken eines Agenten sind in zeitlicher Abhängigkeit in Abbildung 17 von RIPPERGER visualisiert. Wegen der diffizilen Nachweisbarkeit, dass implizites Wissen vom Vertrauensnehmer (Agent) selbst oder für andere Auftraggeber wiederverwendet wird, nehmen das Vertrauensverhältnis und die eruierten Erfahrungen des Vertrauensgebers (Prinzipal) eine zentrale Funktion ein. Vor einer Projektbeteiligung des Agenten sind die Handlungsabsichten und das Umfeld auf potentielle Risiken zu antizipieren.[331]

[328] Vgl. Manhart & Thalmann 2015, S. 200, Kale et al. 2000, Jordan & Lowe 2004.
[329] Vgl. Chan & Lee 2011, S. 101.
[330] Vgl. Li et al. 2008, S. 328.
[331] Vgl. Ripperger 2005, S. 76.

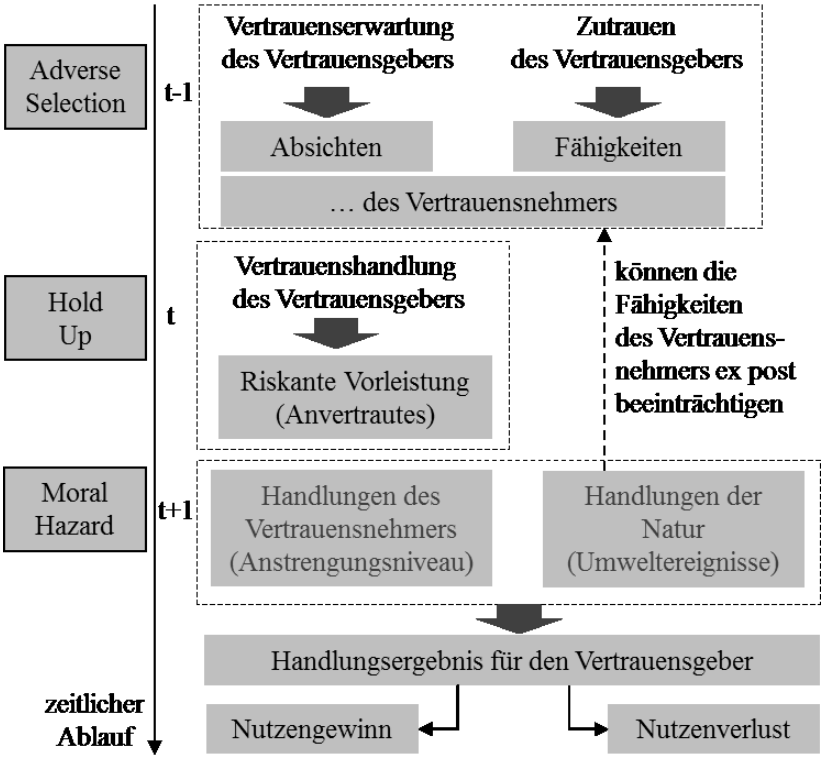

Abbildung 17: Die durch die Vertrauensbeziehung begründeten Verhaltensrisiken[332]

Nach NORMAN führt ein höheres Vertrauen zu einem niedrigeren Schutzniveau zwischen den kooperierenden Unternehmen.[333] Zudem weisen KALE et al. darauf hin, dass die Beziehungen der Unternehmen mehr Aufmerksamkeit bekommen müssen, da sie eine erhebliche Rolle bei der Lösung des *Boundary Paradox*[334] einnehmen.[335] Sie umschreiben diese Grenzsituation, das Unternehmen bei Kooperation mit der herausfordernden Aufgabe konfrontiert sind, die Balance zwischen *trying to learn and trying to protect*[336] zu finden.

Resource-based view und Knowledge-based view

Das wertvolle und schützenswerte Wissen als Kerngedanke der Arbeit basiert auf der Annahme das Wissen eine Ressource ist. Somit begründet sich Wissen als Ressource aus strategischer Sicht in der *Resource-based view* beziehungsweise in der darauf aufbauenden *Knowledge-based view*.[337] Der *Resource-based view* Leitgedanke besteht darin, dass der Organisationserfolg durch das Vorliegen einzigartiger organisationsspezifischer Ressourcen definiert wird. Nach dieser Theorie sind Ressourcen die Voraussetzung um verschiedene Produkte und Dienstleistungen zu entwickeln.[338] Ressourcen lassen sich in materielle und immaterielle aufteilen. In der Abbildung 18 von MAIER werden die Klassifikationen der Ressource Wissen dargestellt. Die

[332] Ripperger 2005, S. 76.
[333] Vgl. Norman 2004, S. 612.
[334] Vgl. Abschnitt 4.2.1.
[335] Vgl. Manhart & Thalmann 2015, S. 200, Kale et al. 2000.
[336] Kale et al. 2000, S. 219.
[337] Vgl. Maier 2007, S. 64, Grant 1996, Spender 1996.
[338] Vgl. Maier 2007, S. 96.

zwei für die Arbeit relevanten Formen von Wissen, *tacit* und explizit, werden in diesem Abschnitt nicht weiter erörtert, da bereits im Abschnitt 2.1.1 dokumentiert.

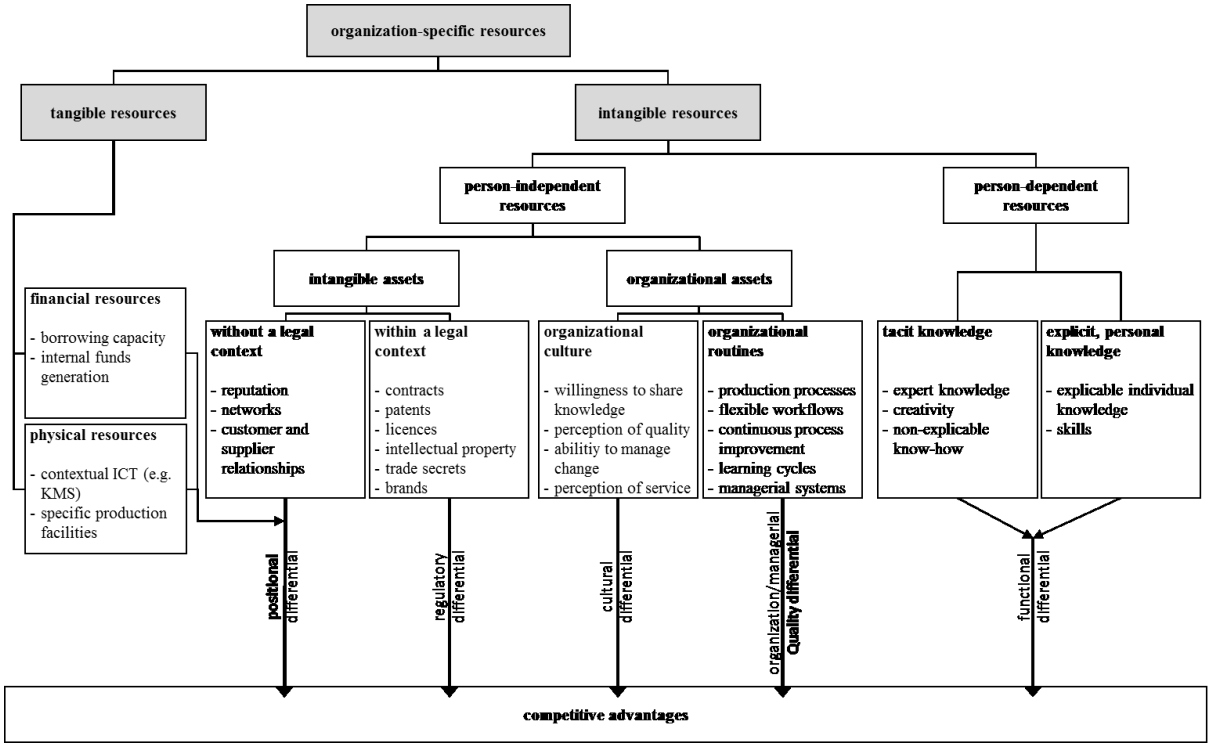

Abbildung 18: Klassifikation von Ressourcen innerhalb der Knowledge-based view[339]

In den neunziger Jahren wurde die Schlüsselressource Wissen in der Strategieliteratur[340] von mehreren Autoren[341] mit der *Knowledge-based view* begründet.[342] Nach MAIER verbindet die *Knowledge-based view* das WM und das strategische Management.[343] Die Konzepte der *Knowledge-based view* lassen sich nach TSOUKAS in taxonomische und konnektionistische Ansätze unterteilen.[344] Die Autoren der taxonomischen Ansätze konzentrieren sich mehrheitlich auf eine klassifizierende Wissens-Typologisierung in und durch Unternehmen.[345] Die zweite Forschergruppe, der konnektionistischen Ansätze, untersuchen Unternehmen und ihr Wissen überwiegend nach dem metaphorischen Aufbau vom menschlichen Gehirn.[346]

Mit der Schlüsselressource sollen die Wettbewerbsvorteile erarbeitet und gesichert werden. Die Wettbewerbsvorteile eines Unternehmens sind nach der *Knowledge-based view* abhängig von der Nutzung, Anwendung und Integration seiner vorhandenen Fähigkeiten sowie diese für die

[339] Maier 2007, S. 99.
[340] Vgl. Carlsson 2004, S. 628.
[341] Zum Beispiel: Leonard-Barton 1992, Quinn 1992, Spender 1994, 1996, Grant 1996, Zahn et al. 2000.
[342] Vgl. Maier 2007, S. 102.
[343] Vgl. Maier 2007, S. 103.
[344] Vgl. Tsoukas 1996, S. 13.
[345] Vgl. Tsoukas 1996, S. 14.
[346] Vgl. Tsoukas 1996, S. 14 f.

Erforschung neuer Fähigkeiten zu nutzen und zu entwickeln.[347] Des Weiteren brauchen Unternehmen spezifische Kombinationen von Fähigkeiten, um ihre Wettbewerbsvorteile zu sichern und eine Geschäftsstrategie, die die Ressourcen und Fähigkeiten nutzt.[348]

Unter der Annahme von DESOUZA, dass die wissensbasierten Ressourcen der bedeutsamste Ausgangspunkt für die Wettbewerbsvorteile sind,[349] diskutiert die Wissensschutzliteratur den Wissensschutz als Unternehmensfähigkeit[350] sowie eine Reihe von Unternehmensmaßnahmen[351] oder Einflussfaktoren[352], um externe Dienstleister daran zu hindern, das Wissen eines Unternehmens zu absorbieren.[353] Es kann nicht generalisiert werden, dass die wissensbasierten Ressourcen der bedeutsamste Ausgangspunkt für die Wettbewerbsvorteile sind. Die Wissensbasis einer IT-Beratung stellt ein Aspekt unter vielen Einflussfaktoren für den Unternehmenserfolg dar. Für die Reihe der oben erwähnten Unternehmensmaßnahmen sind Theorien wie die *absorptive Kapazität*[354], organisationales Lernen und der Wissensaustausch von Bedeutung, besonders um das *Boundary Paradox*[355] zu erklären.[356] Im Rahmen der Arbeit werden diese Theorien charakterisiert und deren zu beachtenden Funktionen in das Referenzmodell integriert.

Damit der *Prinzipal* und damit die IT-Beratung strategisch planen und seine wettbewerbsrelevanten Wissensressourcen identifizieren kann, wird die fünfstufige strategische Vorgehensanalyse der *Resource-based view* in das Referenzmodell integriert. Die originären Schritte sind:

1. Identify and classify the firm‘s resources. Appraise strengths and weakness relative to competitors. Identify opportunities for better utilization of resources.
2. Identify the firm‘s capabilities: What can the firm do more effectively than its rivals? Identify the resources inputs to each capability, and the complexity of each capability.
3. Appraise the rent generating potential of resources and capabilities in terms of
    a. their potential for sustainable competitive advantage, and
    b. the appropriability of their returns
4. Select a strategy which best exploits the firm‘s resources and capabilities relative to external opportunities.
5. Identify resource gaps which need to be filled. Invest in replenishing, augmenting and upgrading the firm‘s resource base.[357]

Für das Modell heißt das, dass eine IT-Beratung seine Ressourcen identifizieren, Fähigkeiten kennen und Wettbewerbsvorteile aufgrund der Ressourcen und Fähigkeiten bewerten muss. Anschließend muss eine Strategie auf der Grundlage der Ressourcen und Fähigkeiten des Unternehmens, unter Einbeziehung der externen Möglichkeiten, festgelegt werden.

---

[347] Vgl. Maier 2007, S. 102.
[348] Vgl. Manhart & Thalmann 2015, S. 200, Grant 1991.
[349] Vgl. DeSouza 2006, S. 1.
[350] Vgl. Gold et al. 2001, S. 186.
[351] Vgl. Baughn et al. 1997.
[352] Vgl. Norman 2002.
[353] Vgl. Manhart & Thalmann 2015, S. 200.
[354] Vgl. Abschnitt 4.3.3
[355] Vgl. Abschnitt 4.2.3.
[356] Vgl. Manhart & Thalmann 2015, S. 200.
[357] Maier 2007, S. 103, vgl. Grant 1991, S. 115, Grant 1998, S. 113.

Zusammenfassend ist festzuhalten, dass eine IT-Beratung mit dem Referenzmodell in die Lage versetzt wird, eine Transaktion in Bezug auf den Wissensschutz für ein IT-Projekt zu bewerten. Das *relationale Kapital* und damit das Vertrauen ein zentraler Aspekt bei der Dienstleister-Auswahl für ein IT-Projekt mit schützenswerten Wissensgebieten ist. Nach der *Resource-based view* und *Knowledge-based view* muss eine IT-Beratung aufbauend auf seinen Ressourcen und Fähigkeiten seine Wettbewerbsvorteile bewerten und eine Strategie festlegen.

3 Forschungsmethoden und -vorgehen

Dieses Kapitel charakterisiert die Forschungsmethoden und das -vorgehen. Im Unterkapitel 3.1 erfolgt die Einordnung zum konstruktionsorientierten Forschungsansatz und der Darstellung vom Forschungsprozess mit dem spezifischen iterativen Referenzmodellierungsprozess zwischen *Literature Review*, der Kollaboration mit Praktikern und der Modellierung.

Im Unterkapitel 3.2 wird die Referenzmodellierung beschrieben. Zum Grundverständnis werden die Begriffe Modell, Vorgehensmodell und Referenzmodell definiert. Besonders eingegangen wird auf die allgemeinen Anforderungen an Referenzmodelle sowie die Grundsätze ordnungsmäßiger Modellierung.

Das Unterkapitel 3.3 präzisiert das Forschungsvorgehen. Dazu gehören die Methodenbeschreibung vom *Literature Review* um einen Prototypen zu entwickeln. Im Abschnitt 3.3.2 werden die Interview-Methodik für die Experteninterviews und das Gruppeninterview deskribiert. Im Abschnitt 3.3.3 der Prototypevaluation mit Experteninterviews werden die Leitfadenentwicklung, die Expertenauswahl mit der Samplingstrategie, die Interviewdurchführung, die Transkription und die Auswertung mittels qualitativer Inhaltsanalyse beschrieben. Die Darstellung des Pilotierungsprojektes mit den Einzelinterviews und dem Gruppeninterview bildet den Abschluss dieses Kapitels (Abschnitt 3.3.4).

3.1 Forschungsansatz und Forschungsprozess

Die vorliegende Arbeit orientiert sich an dem forschungsmethodischen Verständnis des DSR[358]-Ansatzes von HEVNER et al.[359]. Mit der genannten Konstruktion eines Referenzmodells und damit der Erarbeitung eines neuen Artefakts basiert das Forschungsvorgehen auf den konstruktivistischen Forschungsmethoden, wie der Aktionsforschung, dem Prototyping, der Pilotierung und der Referenzmodellierung.[360] Aus der Sichtweise vom DSR, die ihren Ursprung bei den Ingenieurswissenschaften und den konstruktivistischen Wissenschaften haben,[361] sind ebenso empirische Forschungsmethoden (Querschnittsanalysen, Experimente) ein wertvolles Element des Erkenntnisprozesses.[362] Der Forschungsprozess folgt dem DSR-Ansatz und der Aktionsforschung. In der Abbildung 19 sind neben dem Forschungsansatz auch die angewendeten Forschungsmethoden visualisiert dargestellt, die in den folgenden Abschnitten beschrieben werden.

---

[358] Vgl. Ostrowski & Helfert 2012.
[359] Hevner et al. 2004.
[360] Vgl. König et al. 1996, S. 45 f., Wilde & Hess 2007, S. 284.
[361] Vgl. Hevner & Chatterjee 2010, S. 11.
[362] Vgl. König et al. 1996, S. 44 f., Hevner et al. 2004, S. 86, Loos & Fettke 2007, S. 36, S. 39, Wilde & Hess 2007, S. 284.

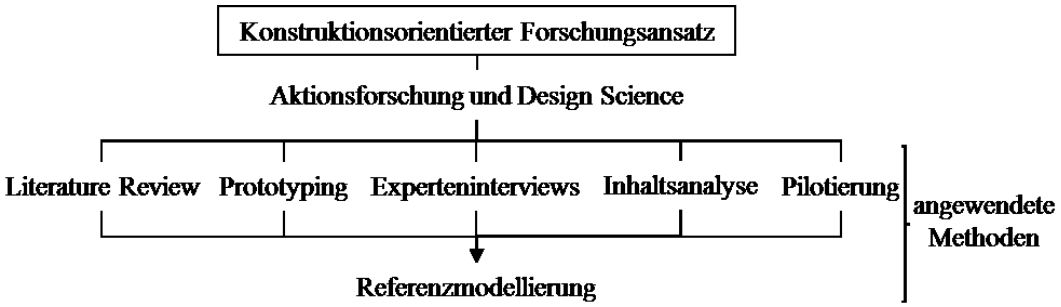

Abbildung 19: Angewendete Methoden in der Arbeit[363]

3.1.1 Aktionsforschung

Die Entwicklung des Referenzmodells durch den Autor kann der Aktionsforschung[364] zugeordnet werden, da der Forscher aktiv am untersuchten Forschungsprozess beteiligt ist[365] und gestalterisch Einfluss nimmt[366]. Um die differenzierten Kriterien von Wissenschaft und Praxis in der Aktionsforschung zu gewährleisten, werden ergänzende Forschungsmethoden im Forschungsprozess genutzt.[367] Diese sind das *Literature Review*, das Prototyping, die qualitativen Experteninterviews, die qualitative Inhaltsanalyse (Zusammenfassung), die Pilotierung und die Referenzmodellierung. Die Erkenntnisse der Arbeit basieren im Wesentlichen auf der mehrjährigen gemeinsamen Aktionsforschung in einer IT-Beratung und der langjährigen Projektexpertise des Autors mit externen IT-Dienstleistern. Die Aktionsforschung ist ein von LEWIN[368] geprägter Begriff und wird wegen ihrem Fokus auf die praktische Realisierbarkeit in der konstruktionsorientierten Wirtschaftsinformatik verwendet.[369] Nach FRANK et al. hat die Aktionsforschung eine große Bedeutung für die WI, denn sie „eröffnet […] den direkten Zugang zu Prozessen der Analyse, Planung, Entwicklung und Einführung von IKS[370], die ein zentraler Erkenntnisgegenstand der WI sind".[371] Nach WHYTE et al. ist das Ziel der Aktionsforschung die Transparenz, Realitätshaltigkeit, Praxisrelevanz und Interaktionen. Die Generalisierung der Ergebnisse ist eher sekundär.[372] Mit dieser Methode ist ein vielfältiger Ansatz in der Forschung möglich. Für das angestrebte Forschungsziel ist eine Bandbreite an Vorgehensweisen möglich. Jedoch erfordert es einen definierten prozessualen und zyklischen Ablauf.[373]

Zusammenfassend ist der Forscher bei der Aktionsforschung in das Forschungsobjekt integriert und wirkt bei der Realisierung der Forschungsziele aktiv mit. Die von dem Forscher durch

---

[363] Eigene Darstellung.
[364] Die Aktionsforschung ist „eine Forschungsmethode der angewendeten Sozialwissenschaften, welche die strikte Trennung zwischen Forscher und Forschungsobjekt aufhebt." Büren et al. 2003, S. 521 und vgl. Whyte et al. 1991, S. 20.
[365] Vgl. Whyte et al. 1991, S. 20.
[366] Vgl. Checkland & Holwell 1998, S. 11.
[367] Vgl. Mingers 2001, S. 243, Chiasson et al. 2008, S. 37, Österle et al. 2010, S. 4 f.
[368] Vgl. Lewin 1946.
[369] Vgl. Lau 1997, S. 34, Baskerville & Wood-Harper 1998.
[370] IKS steht für Informations- und Kommunikationssysteme.
[371] Frank et al. 1998, S. 87.
[372] Vgl. Whyte et al. 1991.
[373] Vgl. Checkland & Holwell 1998, S. 14, S. 16, Fleisch 2001, S. 291.

Aktivitäten, Beobachtungen, Analysen gewonnen Erkenntnisse und weitere relevante Praxisergebnisse fließen in die Forschungsarbeit ein (Abbildung 22). Die subjektive Auffassung des Forschers wird im Prozess der Lösung des Forschungszieles mit einbezogen und reflektiert.

3.1.2 Design Science Research

Die Anforderungen der DS nach HEVNER et al. sind ein anwendbares, nutzenstiftendes, verständlich aufgearbeitetes Forschungsergebnis zu erarbeiten, das ein relevantes Problem adressiert und einen wissenschaftlichen Beitrag liefert.[374] Aufbauend auf diesem Gestaltungsziel werden entwickelte Artefakte mit entsprechender Problemlösungskraft konstruktivistisch erstellt, getestet, modifiziert und erweitert.[375] Die vorliegende Arbeit konstruiert basierend auf den wissenschaftlichen Erkenntnissen und der Praxiserfahrung des Autors ein Referenzmodell, das in Experteninterviews (Prototypevaluation) und einer Pilotierung getestet, modifiziert und erweitert wird. Mit dem Referenzmodell wird eine IT-Beratung befähigt, den strategischen Wissensschutz in ihren IT-Projekten mit ISE zu etablieren. Die zu entwickelnden Artefakte werden in der gestaltungsorientierten Wirtschaftsinformatik als Konstrukte (Konzepte, Terminologien, Sprachen), Modelle, Methoden und Instanzen (Implementierungen als Prototypen oder produktive Informationssysteme) definiert.[376] Um solche Artefakte in der konstruktionsorientierten Forschung zu entwickeln, finden die beschriebenen Forschungsmethoden Anwendung. Die von HEVNER et al. gestellten Anforderungen an die DS-Forschung sind:

- 1. Design as an Artifact: Die Ergebnisse müssen anwendbare Artefakte in Form von Konstrukten, Modellen, Methoden oder Instanzen sein.
- 2. Problem Relevance: Das Handlungsziel ist die Entwicklung von Lösungen für bedeutende und relevante Probleme.
- 3. Design Evaluation: Der Nutzen, die Qualität und die Wirksamkeit des Artefaktes müssen bewertet bzw. demonstriert werden.
- 4. Research Contributions: Der wissenschaftliche Beitrag durch die Schaffung des Artefaktes oder die Erweiterung der Wissensbasis muss nachvollziehbar sein.
- 5. Research Rigor: Die stringente Anwendung von Methoden bei der Konstruktion und Bewertung des Artefaktes.
- 6. Design as a Search Process: Die Entwicklung der Ergebnisse soll durch einen iterativen Suchprozess gekennzeichnet sein.
- 7. Communication of Research: Die Ergebnisse müssen sowohl für Fach- und ebenso für Führungskräfte aufbereitet und kommuniziert werden.[377]

Diese sieben aufgeführten Publikationsrichtlinien wurden in den Forschungsprozess einbezogen und die Forschungsergebnisse werden bei der Reflexion (Unterkapitel 6.2) nach diesen Anforderungen diskutiert.

In der folgenden Abbildung ist das Informationssystem Forschungs-Framework von HEVNER et al. dargestellt, das die gestellten DS-Anforderungen adressiert. Nach OSTROWSKI & HELFERT gibt es eine umfangreiche Diskussion zu dem Rigor und der Relevanz in der DS-Forschung.[378]

---

[374] Vgl. Hevner et al. 2004, S. 82 f.
[375] Vgl. Ulrich 2001, S. 225 ff., König et al. 2002, S. 6 f., Hevner et al. 2004.
[376] Vgl. Österle et al. 2010, S. 4.
[377] Vgl. Hevner et al. 2004, S. 82 ff.
[378] Vgl. Ostrowski & Helfert 2012, S. 1. Iivari et al. 2009, Winter 2008.

BASKERVILLE et al. und PEFFERS et al. stellen heraus, dass die Auffassungen und Empfehlungen zur DS-Forschung zwischen den Autoren variieren. Das beruht auf dem Umstand, dass die methodischen Leitlinien der DS selten angewendet werden. Was wiederrum darauf hindeutet, dass die bestehende Methodik immer noch zu abstrahiert dokumentiert ist.[379]

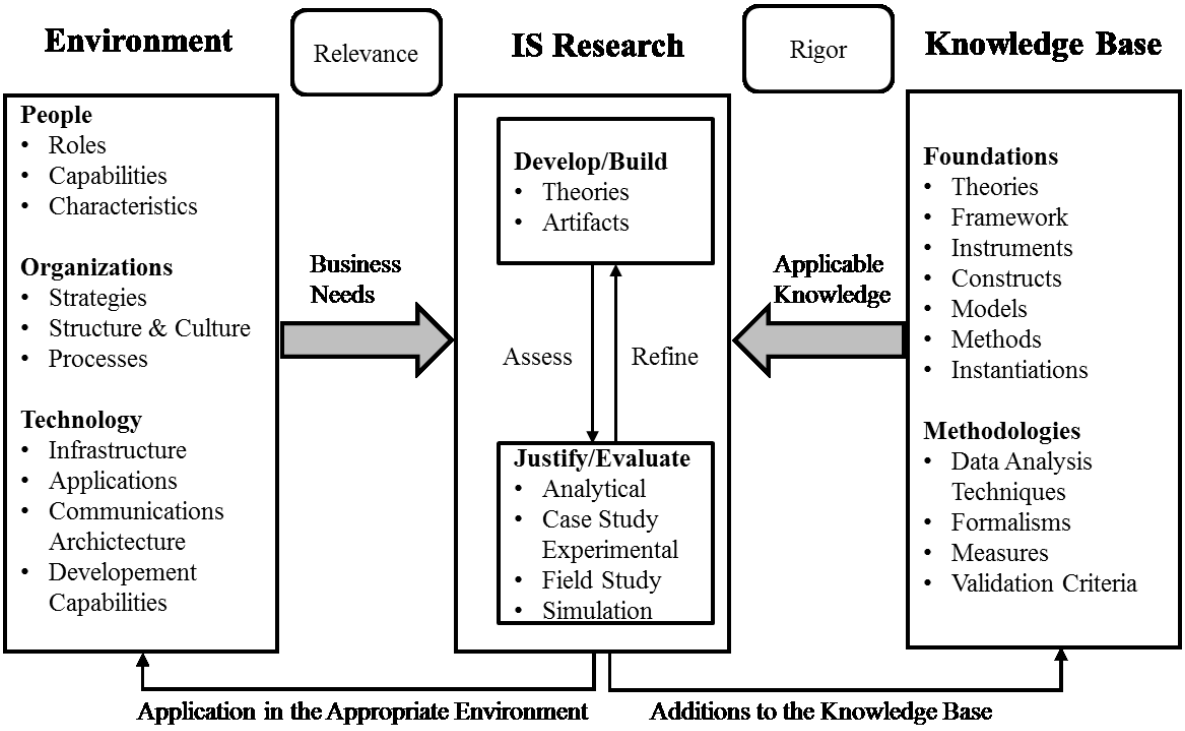

Abbildung 20: Informationssystem DSR-Forschungs-Framework[380]

Um die Referenzmodellierung visuell und prozessual in die DS-Methodik einzuordnen, haben OSTROWSKI & HELFERT eine Übersichtsdarstellung entwickelt.[381] Sie gliedern den Prozess in acht Phasen (Abbildung 21). Nach der Problemidentifikation und der Zielstellung findet in der dritten Phase, dem Meta-Design[382], die Entwicklung des Referenzmodells statt. Diese Meta-Design Phase kann mit der Konstruktionsphase (Abbildung 22) von SCHLAGHECK gleichgesetzt werden.[383]

[379] Vgl. Ostrowski & Helfert 2012, S. 2, Baskerville et al. 2009, Peffers et al. 2007.
[380] Hevner et al. 2004, S. 80. Bildunterschrift: „The goal of behavioral science is truth. The goal of design-science research is utility. As argued above, our position is that truth and utility are inseparable."
[381] Vgl. Ostrowski & Helfert 2012, S. 2.
[382] Vgl. Walls et al. 1992.
[383] Vgl. Schlagheck 2000, S. 77 ff.

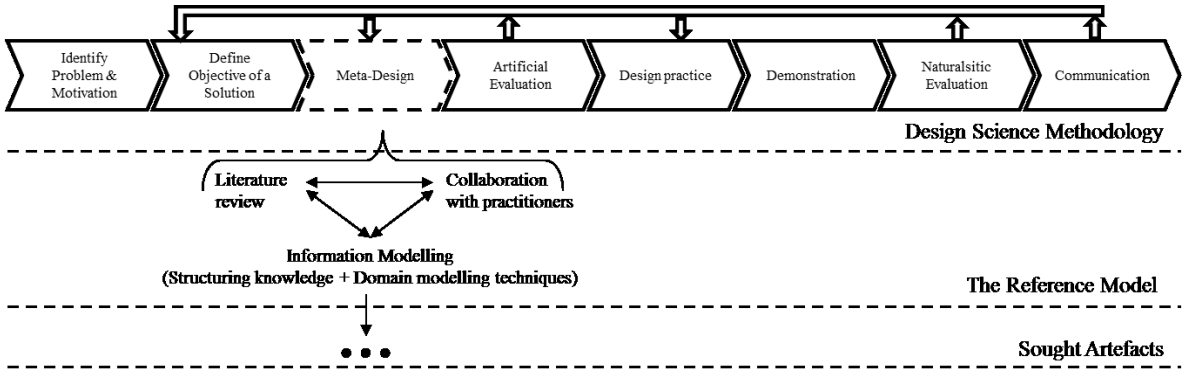

Abbildung 21: Einordnung des Referenzmodells in den Design Science Prozess[384]

OSTROWSKI & HELFERT heben hervor, dass die DS-Methodik wegen des hohen Abstraktionsgrades noch zu selten angewendet wird.[385] Aus diesem Grund modellieren sie die detaillierten Aktivitäten (Verfahren, Werkzeuge, Techniken) zur Referenzmodellierung. Sie beschreiben den iterativen Prozess zwischen dem *Literature Review*, der Kollaboration mit Praktikern und der finalen Modellierung. Unter gesicherten Umständen könnte der Forscher nur einen dieser Prozesse verwenden, um ein vollständig modelliertes und beschriebenes Artefakt für die Meta-Design-Phase zu liefern. Der iterative Referenzmodellierungsprozess von OSTROWSKI & HELFERT präzisiert die Doppelkreisdarstellung von SCHLAGHECK in der Abbildung 25.[386] Die Arbeit nimmt den beschriebenen iterativen Prozess zwischen *Literature Review*, Kollaboration mit Praktikern und Modellierung für die Referenzmodellentwicklung auf. Der angewendete Prozess wird im folgenden Abschnitt beschrieben.

Zusammenfassend muss nach der DS ein mehrwertstiftendes und relevantes Forschungsergebnis vorliegen. Die sieben aufgestellten Anforderungen an die DS-Forschung wurden beschrieben und werden bei der Reflexion mit Bezug auf die Erkenntnisse zum entwickelten Referenzmodell diskutiert.

3.1.3 Referenzmodellierungsprozess

Die Referenzmodellierung soll wiederverwendbare Modelle konstruieren und zur Anwendung bringen.[387] Mit der Wiederverwendbarkeit sollen „Effektivitäts- als auch Effizienzsteigerung in der Modellierung“ erzielt werden.[388] Nach DELFMANN kann ein Referenzmodell einen Empfehlungscharakter haben oder als ein Modell verstanden werden auf das Bezug genommen wird.[389] Die generierte Expertise dieser Arbeit manifestiert sich in der dokumentierten Modellierung der strukturierten Aktivitäten in den Funktionen, der ausführenden Projekteakteure, der Definition der Unternehmensgrenze vom *Wissen-Teilen und -Zurückhalten*, der Risikoanalyse von Dienstleistern und deren Zusammenfassung in einem Risikoinformationssystem. Das entwickelte Modell hat das Ziel Basis für eine effiziente und effektive Wissensschutz-Anwendung

[384] Ostrowski & Helfert 2012, S. 2.
[385] Vgl. Ostrowski & Helfert 2012, S. 1, Peffers et al. 2007.
[386] Vgl. Abschnitt 3.2.1.
[387] Vgl. Fettke & Loos 2004, S. 331.
[388] Vgl. vom Brocke & Fettke 2018.
[389] Vgl. Delfmann 2006, S. 45.

in IT-Beratungen zu sein.[390] Des Weiteren kann es zur Analyse, Diskussion und Schulung verwendet werden.[391] Basierend auf dem Referenzmodellierungsvorgehen nach SCHLAGHECK erfolgte eine primäre Anwendung und Anpassung innerhalb eines Prototyping- und Pilotierungsprojektes.[392]

Referenzmodellierung in fünf Phasen

In Anlehnung an die Phaseneinteilung von SCHLAGHECK unterteilt sich das Forschungsvorgehen zur Referenzmodellierung in fünf Phasen, die *Definitionsphase*, die *Analysephase*, die *Konstruktionsphase*, die *Evaluationsphase* und die *Disseminationsphase* (Abbildung 22).[393] Die Details der Phasen mit dem Bezug zu der Arbeit werden in den folgenden Absätzen beschrieben.

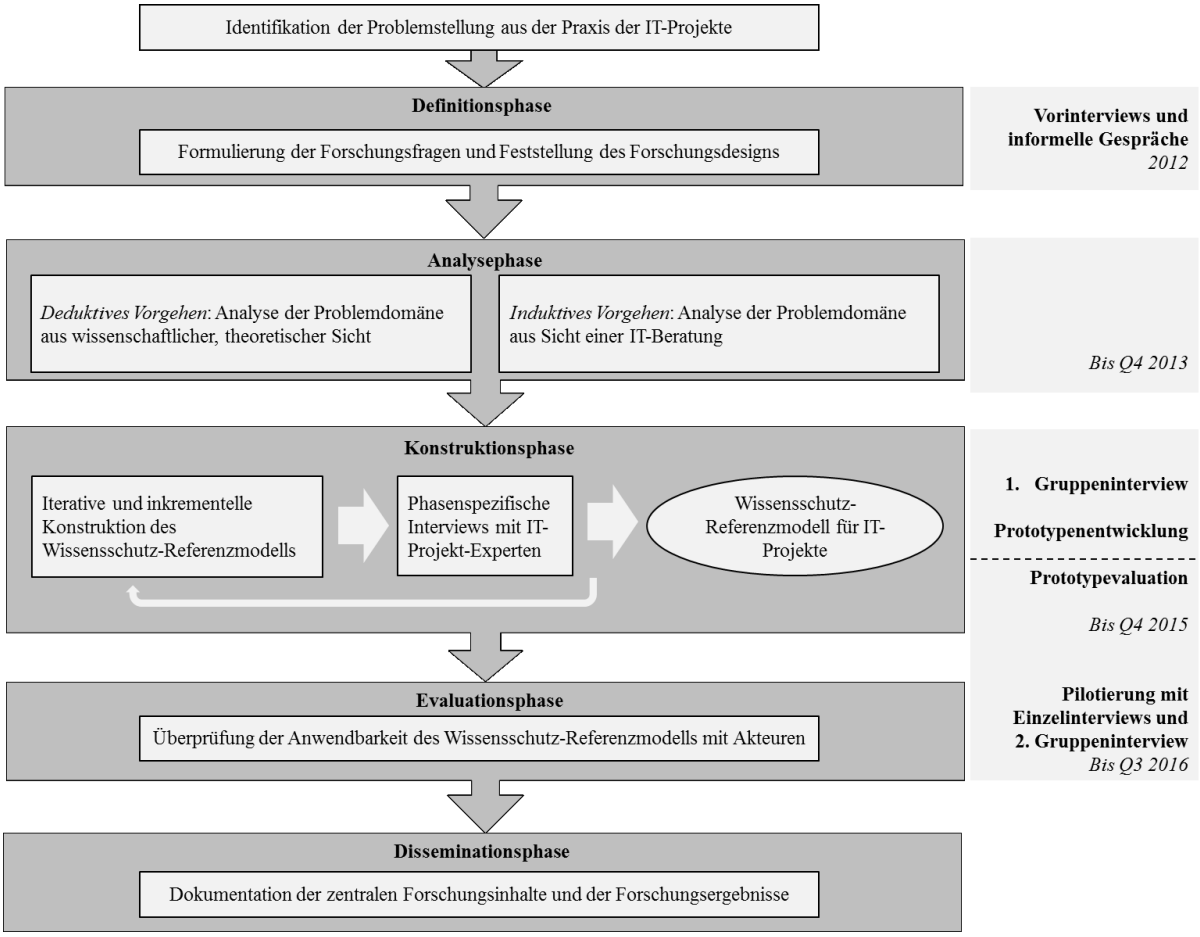

Abbildung 22: Phasen des Forschungsvorgehens[394]

Die identifizierte Problemstellung, der Schutz des wertvollen organisationalen Wissens einer IT-Beratung in der ISE mit externen nationalen und internationalen IT-Dienstleistern, stellt die Ausgangssituation für das Forschungsvorgehen dar. Die Forschungsfragen und das Forschungsdesign sind auf der Basis dieses Praxisproblems in der *Definitionsphase* formuliert.

---

[390] Vgl. Schütte 1998, S. 74 ff., Becker et al. 2004, S. 251.
[391] Vgl. Leist 2002, S. 8 f.
[392] Vgl. Schlagheck 2000, S. 78.
[393] Vgl. Schlagheck 2000, S. 77 ff.
[394] In Anlehnung an Schlagheck 2000, S. 77 ff.

In der anschließenden *Analysephase* erfolgen die Identifikation wesentlicher Informationsquellen und die Informationsbeschaffung, um die Wissensbasis über die Problemdomäne aufzubauen. Diese Phase ist nach BECKER et al. durch das Kombinieren des induktiven und des deduktiven Vorgehens gekennzeichnet. Beim induktiven Vorgehen wird die Praxiserfahrung des Verfassers zugrunde gelegt. Die Literaturrecherche der zur Referenzmodellierung relevanten Informationen bildet die Basis des deduktiven Vorgehens.[395] Ein Schwerpunkt der relevanten Literaturrecherche zum Wissensschutz sind die Wissensschutzmechanismen und die angrenzenden Disziplinen der Arbeit wie Outsourcing, organisationales Wissen, IT, KIBS und Prinzipal-Agent.

Auf der Basis des induktiven und deduktiven Vorgehens erfolgt die *Konstruktionsphase* mit der iterativen und inkrementellen Konstruktion eines Prototyps, der die Grundlage für den Interviewleitfaden darstellt. Um das neu entwickelte Artefakt zu validieren und im iterativen Prozess zu überarbeiten,[396] werden mit IT-Sicherheitsexperten, Akteuren des Managements, der Unternehmensstrategie, des IT-Sourcing Managements und des Projektmanagements Interviews durchgeführt (Abbildung 22). Mit Hilfe von einem entwickelten Leitfaden bekommen die Experteninterviews einen inhaltlich strukturierten Rahmen und behalten dadurch eine gewisse Offenheit.[397] Um die Hinweise und Erweiterungen in den folgenden Interviews zu diskutieren und zu validieren, wurden diese nach dem jeweiligen Interview in den IV-Leitfaden aufgenommen. Bei der Zusammenfassung (qualitative Inhaltsanalyse) der transkribierten Experteninterviews wurde der entwickelte Prototyp nochmals validiert, erweitert und aktualisiert. Ziel ist es die praktische Expertise der Projektakteure in den Prototypen zu integrieren und die aus der Literatur abgeleiteten Wissensschutzerkenntnisse zu verifizieren. In dieser Konstruktionsphase werden die Forschungsfragen 1, 2 und 3 adressiert. Zudem enhält diese Phase auch Evaluationselemente, weshalb die Linie zur Evaluationsphase gestrichelt ist.

Die Überprüfung der Anwendbarkeit des Referenzmodells erfolgt anschließend in der *Evaluationsphase* innerhalb eines Pilotierungsprojektes. Die Perspektiven und Nutzersichten des Evaluationsprozesses werden im nächsten Absatz dokumentiert. Für die Pilotierung stellt das Management einer IT-Beratung drei Projekte zur Validierung, die nach ihrer Bewertung einen hohen Wissensschutzbedarf haben. Nach den Vorabgesprächen mit den verantwortlichen Projektmanagern zu deren Pilotierungseignung wird ein IT-Projekt für die Pilotierung ausgewählt. Mit den zentralen Projektakteuren führt der Autor im Rahmen der Pilotierung Einzelinterviews durch, um für das IT-Projekt eine exemplarische Wissens- und Risikobewertung vorzunehmen. In einem Gruppeninterview mit den zentralen Projektakteuren werden die Ergebnisse der Einzelinterviews präsentiert und diskutiert. Die finale Phase der Referenzmodellierung ist die *Disseminationsphase*, in der die zentralen Forschungsinhalte und Forschungsergebnisse zu dokumentieren sind.

---

[395] Vgl. Becker et al. 2002.
[396] Vgl. Österle et al. 2010, S. 5.
[397] Vgl. Gläser & Laudel 2004.

Evaluationsprozess – Perspektiven und Nutzersicht

Neben der Dokumentation des Modells sind auch die empirischen Nachweise zu erbringen, dass die angestrebten Ziele und der Nutzen erreicht werden.[398] Der mit dem Modell verfolgte Nutzen ist damit zu evaluieren sowie die grundsätzliche Gültigkeit, die bis zur ersten tatsächlichen Anwendung offen ist.[399] Beim Referenzmodellierungsvorgehen von SCHLAGHECK ist die Evaluation und Evolution eine entscheidende Phase und diese zeichnet sich durch eine praktische Anwendung aus.[400] Jedoch haben eine große Anzahl der entwickelten Referenzmodelle keine Anwendung durchlaufen.[401] Nach FRANK sind Evaluationen aufwendige Vorhaben, für die Forschungseinrichtungen nicht die notwendige Ressourcen besitzen.[402] Die vorgenommene Evaluation im Rahmen der Interviews ist deshalb ein erster Schritt, die nach einer Modelleinführung in einer IT-Beratung in einem zyklischen Prozess weiterverfolgt werden muss. Der Referenzmodellbeitrag zeichnet sich durch seine erste praktische Anwendung aus, der im Rahmen dieser Arbeit in der zyklischen Evaluation des Prototyps mit seiner Weiterentwicklung und der anschließenden Pilotierung realisiert wurde. Die Beschreibung der Prototypevaluation und der Pilotierung erfolgt in den beiden Abschnitten (3.3.3 und 3.3.4).

Laut FRANK ist der Evaluationsprozess eine herausfordernde Aufgabe, bei der das entwickelte Modell aus verschiedenen Perspektiven (z. B. ökonomisch, technische, deployment, epistemologisch) bewertet werden kann. Jeder dieser Perspektiven wird von ihm durch Aspekte ergänzt und diese werden wiederrum durch Kriterien präzisiert. Diese Perspektiven besitzen die folgende Charakteristik:

- Ökonomische Perspektive: verfolgt das Ziel, das Verhältnis von Kosten und Nutzen bei der Anwendung vom Referenzmodell zu bewerten. Dazu gehören der Investitionsschutz, die Auswirkungen auf die Informationsqualität und die Wettbewerbsfähigkeit.
- Deployment Perspektive: fokussiert sich auf die Akteure, die das Modell realisieren. Dabei werden unter anderem die Kriterien Verständlichkeit, Kompatibilität mit anderen in dem Unternehmen etablierten Vorgehensweisen und die Verfügbarkeit von Hilfsmitteln bewertet.
- Technische Perspektive: zielt auf die Bewertung des konstruierten Artefaktes ab. Dazu gehören die Erfüllung der Spezifikationen sowie die Unterstützung für Analyse und Transformation.
- Epistemologische Perspektive: bewertet das Referenzmodell im Kontext der wissenschaftlichen Forschung. Der Fokus dabei liegt auf den Kriterien, die für wissenschaftlichen Theorien verwendet werden.[403]

[398] Vgl. Schwabe 2008, S. 149 f.
[399] Vgl. Schütte 1998, S. 70.
[400] Vgl. Schlagheck 2000, S. 78.
[401] Vgl. Fettke & Loos 2004b, S. 23 ff.
[402] Vgl. Frank 2006, S. 138.
[403] Vgl. Frank 2006, S. 123.

Die Evaluation der Ergebnisse stützt sich auf diese Erkenntnisse von FRANK. Bevor eine Evaluation vorgenommen werden kann, müssen auf der Grundlage der angestrebten Spezifikationen und dem Forschungsziel[404] relevante Perspektiven ausgewählt werden.[405] Die zu erfüllenden Spezifikationen sind zum einen die aufgestellten Forschungsfragen[406], die sieben Anforderungen der DSR[407] und die Anforderungen an die Referenzmodellierung[408].

Ein Schwerpunkt bei den Interviews (Prototypevaluation und Pilotierung) liegt auf der deployment Perspektive, weil das Referenzmodell verständlich sein muss, damit es in einer IT-Beratung angewendet werden kann. Auch die ökonomische Perspektive (Fokus auf Leistungen) mit dem Bezug zum Wissensmanagement und zur Koordination wird in den Interviews diskutiert und bewertet. In der Arbeit wird zudem die epistemologische Perspektive mit dem Schwerpunkt zur Prinzipal-Agent-Theorie (Evaluation von Theorien) evaluiert.[409] Die technische Perspektive wird bei der Evaluation nicht untersucht. Die Ergebnisse für die ausgewählten Perspektiven und deren Evaluation erfolgt im Unterkapitel 5.4. Neben den vier Perspektiven unterscheidet FRANK in die drei Nutzersicht-Typen:

1. Pre-development use: als Grundlage für die Entwicklung von Software.
2. Post-development use: als Dokumentation von bestehender Software.
3. Business (re-) design: zur Lösung von organisationalen und strategischen Problemen.[410]

In besonderen Fällen können verschiedene Sichten kombiniert werden, wie es das vorliegende Referenzmodell mit der ersten und dritten Sicht anvisiert. IT-Beratungen die noch keine Software oder Prozess für den strategischen Wissensschutz in IT-Projekten verwenden, können das Referenzmodell mit seinen Funktionen und den Kategorien für die Softwareentwicklung nutzen. In den meisten IT-Beratungen werden bereits etablierte Prozesse mit Softwareunterstützung vorliegen. In diesem Fall wird empfohlen diese nach dem Referenzmodell anzupassen, damit der Wissensschutz in den IT-Projekten umgesetzt werden kann.

Häufigkeit: Referenzmodellierung, Prototyping und Aktionsforschung

SCHREINER et al. merken an, dass ein Großteil der deutschsprachigen WI Publikationen den konstruktiven Methoden zugeordnet werden kann, „während das (anglo-amerikanische) Pendant Information Systems Research mit vornehmlich verhaltenswissenschaftlicher Forschung assoziiert wird".[411] Die Abbildung 23 zeigt, dass die Referenzmodellierung im untersuchten und verfügbaren Zeitraum 2007-2012 mit einer sechsprozentigen relativen Häufigkeit eher selten vorkommt.[412] Das Prototyping (drei Prozent) und die Aktionsforschung (1 Prozent) sind zudem noch geringer vertreten.

---

[404] Vgl. Unterkapitel 1.2.
[405] Vgl. Frank 2006, S. 136.
[406] Vgl. Unterkapitel 1.2.
[407] Vgl. Abschnitt 3.1.2.
[408] Vgl. Abschnitt 3.2.1.
[409] Vgl. Abschnitt 2.3.1, Kapitel 5 und Abschnitt 6.2.1.
[410] Vgl. Frank 2006, S. 124.
[411] Frank 2006, Goeken 2003, Herzwurm & Stelzer 2008, zitiert nach Schreiner et al. 2015, S. 1.
[412] Abbildung 23 zeigt die Einsatzhäufigkeit der primären Methoden in den Jahren 2007-2012 der (deutschsprachigen) Wirtschaftsinformatik. Die Darstellung vom angegebenen Zeitraum basiert auf 108 Beiträgen, die in der

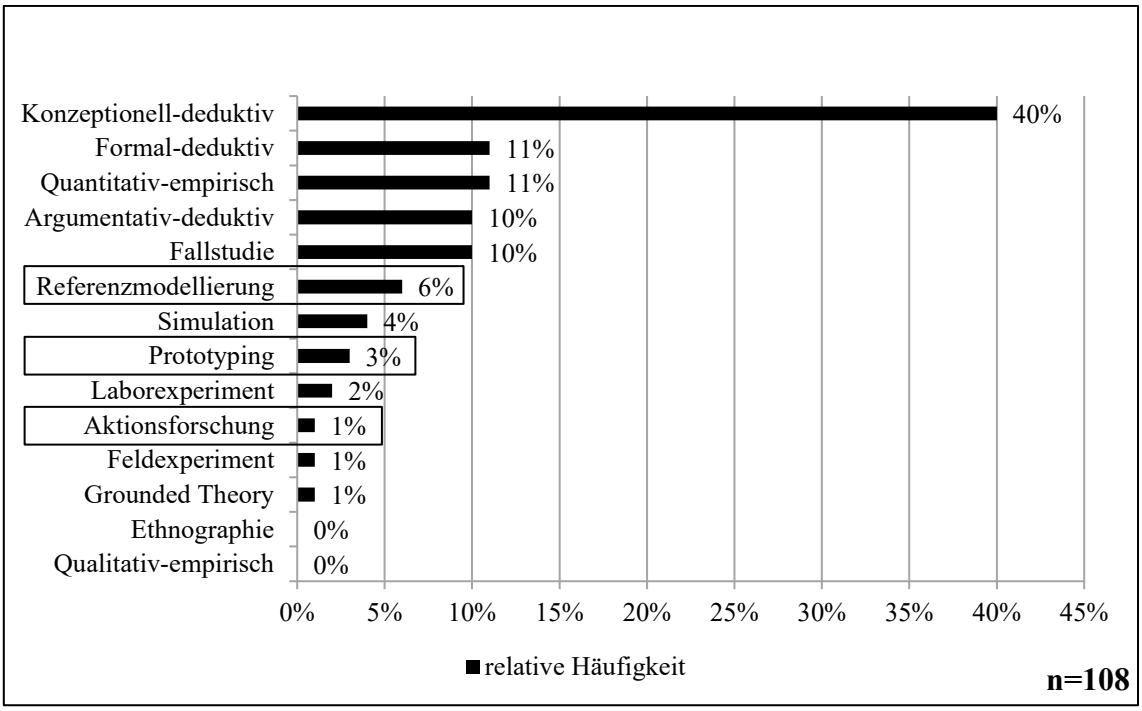

Abbildung 23: Einsatzhäufigkeit der primären Methode in den Jahren 2007-2012[413]

Zusammenfassend nutzt diese Arbeit die dargestellten Methoden zur Gestaltung eines Referenzmodells für den Wissensschutz bei der ISE mit externen Dienstleistern. Diese Methode versteht sich wegen des branchenspezifischen Allgemeingültigkeitsanspruches und dem Empfehlungscharakter als Referenzmodell und hat das Anwendungsziel in der Praxis Kosten-, Zeit-, Qualitäts-, Risiko- und Wettbewerbssituations-Parameter zu optimieren.[414]

3.2 Referenzmodellierung

In diesem Unterkapitel wird die Referenzmodellierung beschrieben. Dazu werden im Abschnitt 3.2.1 die Begriffe Modell, Vorgehensmodell und Referenzmodell definiert. Des Weiteren wird auf die allgemeinen Anforderungen an Referenzmodelle sowie die Grundsätze ordnungsmäßiger Modellierung eingegangen. Der Abschnitt 3.2.2 dient zur Beschreibung der verwendeten Darstellungstechnik des Referenzmodells.

3.2.1 Begriffsklärung und Anforderungen

In der Literatur wird der Begriff Modell dependent von dem jeweiligen Kontext definiert. Die Modelltheorie von STACHOWIAK[415] ist prinzipiell akzeptiert und strebt eine disziplinübergreifende Verwendung des Modellbegriffs an. Spezifischer unterscheidet die Wirtschaftsinformatik (WI) zwischen dem abbildungsorientierten und konstruktionsorientierten Modellbegriff.[416]

Zeitschrift Wirtschaftsinformatik veröffentlicht wurden. Die Prozentzahlen zeigen die relative Häufigkeit, mit der die jeweilige Methode angewendet wurde.

[413] Schreiner et al. 2015, S. 8.

[414] Vgl. Fettke & Loos 2004a, S. 333.

[415] Stachowiak 1973.

[416] Vgl. vom Brocke 2003, S. 9 ff.

Der konstruktionsorientierte Modellbegriff beachtet im Vergleich zum abbildungsorientierten Modellbegriff die Subjektivität der Wahrnehmung.[417] Der konstruktionsorientierte Modellbegriff nimmt in der WI eine bedeutende Rolle ein, denn in der WI stellen Modelle „kein (vereinfachtes) Abbild der Realität dar […], sondern sind als (Re-) Konstruktionen der Realität aufzufassen".[418] Als Grundlage für den Begriff Modell wird eine für die Arbeit zuordenbare Modelldefinition von SCHÜTTE verwendet. Ein Modell ist:

> „das Ergebnis einer Konstruktion eines Modellierers, der für Modellnutzer eine Repräsentation eines Originals zu einer Zeit als relevant mithilfe einer Sprache deklariert. Ein Modell setzt sich somit aus der Konstruktion des Modellierers, dem Modellnutzer, einem Original, der Zeit und einer Sprache zusammen".[419]

Aufbauend auf der eingenommenen wissenschaftlichen Positionierung[420] nutzt die Arbeit den konstruktionsorientierten Modellbegriff.

Parallel zum Modellbegriff nehmen die beiden synonym verwendeten Begriffe des Informationsmodells / Informationssystemmodells[421] im Kontext der Referenzmodellierung eine bedeutsame Rolle ein. Informationsmodelle sind nach DELFMANN „spezielle Modelle, die für die Gestaltung von Informationssystemen verwendet werden."[422] SCHÜTTE definiert ein Informationsmodell als:

> „das Ergebnis einer Konstruktion eines Modellierers, der für Anwendungssystem- und Organisations[system]gestalter Informationen über zu modellierende Elemente eines Systems zu einer Zeit als relevant mit Hilfe einer Sprache deklariert".[423]

Die Adressatenfokussierung dieser Definition auf Anwendungssystem- sowie Organisationssystemgestalter ist mit der in dieser Arbeit vorliegenden Positionierung mit einem Informationssystem kongruent. Entsprechende Übersichten zu Informationsmodellklassen hat unter anderem SCHÜTTE zusammengestellt.[424] Zu den Informationsmodellen mit anderen Anwendungskontexten ordnen sich die Referenzmodelle ein.[425]

Beim Referenzmodell handelt es sich ursprünglich um ein Informationsmodell,[426] ebenso als Referenzinformationsmodell bezeichnet.[427] Basierend auf dem etymologischen Ursprung des Referenzbegriffs hat ein Referenzmodell einen Empfehlungscharakter und es ist ein Modell auf das Bezug genommen werden kann.[428] SCHÜTTE definiert das Referenzmodell als ein Modell, das:

---

[417] Vgl. vom Brocke 2003, S. 10.
[418] Dresbach 1999, S. 73.
[419] Schütte 1998, S. 59.
[420] Vgl. Unterkapitel 2.3.
[421] Vgl. vom Brocke 2003, S. 29.
[422] Delfmann 2006, S. 40.
[423] Schütte 1998, S. 63.
[424] Schütte 1998, S. 64.
[425] Vgl. Delfmann 2006, S. 47.
[426] Vgl. Fettke 2006, S. 26.
[427] Vgl. Schütte 1998, S. 69.
[428] Vgl. Delfmann 2006, S. 45.

> „für Anwendungssystem- und Organisations[system]gestalter Informationen über allgemeingültige zu modellierende Elemente eines Systems zu einer Zeit als Empfehlungen mit einer Sprache deklariert, so dass ein Bezugspunkt für ein Informationssystem geschaffen wird".[429]

Das Referenzmodell in dieser Arbeit fokussiert diese Definition. Idealtypisch kann ein Referenzmodell für die Gestaltungsbeschreibung aller relevanten Prozesse und Strukturen appliziert werden.[430] Der Referenzmodell-Grundgedanke in der WI, mit ihrem Ziel der Datenverarbeitungs-Unterstützung, ist die systematische Strukturierung betriebswirtschaftlicher Aufgaben.[431] Damit reduziert der Einsatz von Referenzmodellen das Risiko einer Fehlgestaltung[432] und führt zur Kostenreduktion, da sie die Unternehmensfunktionen, -daten und -prozesse strukturieren und vereinfachen.[433] Weiterhin können durch Referenzmodelle die organisatorischen Konzepte umgehend implementiert werden und verkürzen somit die Einführungszeit der Softwareimplementierung.[434]

Der Fokus bei der Referenzmodell-Konstruktion liegt auf der Anwendungsfunktion und deckt damit die fachkonzeptionelle Ebene ab.[435] Von den technischen Details sollte abstrahiert werden, um einen unabhängigen Einsatz von der etablierten Software in der IT-Beratung zu ermöglichen. Allgemeine Anforderungen an ein Referenzmodell werden bei DELFMANN[436] und KNACKSTEDT[437] formuliert, diese sind:

- Allgemeingültigkeit
- Wiederverwendbarkeit
- Vollständigkeit
- Adaptierbarkeit

Bei der Anforderung der Allgemeingültigkeit ist die Frage nach Objektivität zu beantworten. Das erfolgt bei DELFMANN[438] nicht. DELFMANN legt fest, „Allgemeingültigkeit wird […] als optimale Eigenschaft von Referenzmodellen angesehen".[439] Die Wiederverwendbarkeit liegt nach SCHLAGHECK vor, „wenn eine hinreichende Abstraktion oder eine Berücksichtigung verschiedener Varianten eine Einsetzbarkeit in einem anderen Kontext erlauben".[440] DELFMANN beschreibt die Vollständigkeit, „wenn mindestens ein Anwendungskontext existiert, den eine Wiederverwendung des Referenzmodells erfordert".[441] Die Adaptierbarkeit eines Modells ist erfüllt, wenn die individuellen Bedürfnisse der Anwender erfüllt sind.[442]

---

[429] Schütte 1998, S. 69.
[430] Vgl. Schneider et al. 2008, S. 96.
[431] Vgl. Schütte 1998, S. 82.
[432] Vgl. Weiber 2002, S. 93.
[433] Vgl. Speck & Schnetgöke 2005, S. 217.
[434] Vgl. Becker & Schütte 2004, S. 80. Zu den Vorteilen des Einsatzes von Referenzmodellen vgl. auch Schütte 1998, S. 75 f.
[435] Vgl. Schütte 1998, S. 72.
[436] Vgl. Delfmann 2006, S. 46 f.
[437] Vgl. Knackstedt 2006, 57 f.
[438] Vgl. Delfmann 2006, S. 46 f.
[439] Delfmann 2006, S. 46.
[440] Schlagheck 2000.
[441] Delfmann 2006, S. 47.
[442] Vgl. Delfmann 2006, S. 47.

Der Modellrahmen und der modulare Aufbau ermöglichen es die Komplexität eines Referenzmodells einzugrenzen, überschaubar zu gestalten und ebenso eine Wiederverwendbarkeit zu ermöglichen. Der Nutzen und die Anwendbarkeit eines Modells sind durch den Inhalt, seine inhaltliche Qualität bestimmt. Deshalb sind Qualitätsanforderungen von jedem Modellentwickler zu erfüllen. „Die Qualität des Modells ist umso höher zu bewerten, je geringer die Differenz zwischen den Anforderungen des Modell-adressaten und der tatsächlichen Eignung des Modells zur Problemlösung ist."[443]

Nach DELFMANNS zahlreichen Analysen von Referenzmodellen, die in der Literatur zu finden sind, weisen diese einen konkreten Branchenbezug auf, der ebenso von einigen Autoren explizit gefordert wird.[444] Mit dieser „Forderung wird das Einsatzgebiet von Referenzmodellen auf konkrete betriebswirtschaftliche Domänen beschränkt".[445] DELFMANN unterstützt als Option den Branchenbezug ausdrücklich.[446] Grundsätzlich teilt der Autor diese Auffassung und sieht in seiner Arbeit einen konkreten empirischen Beweis.

Die Grundsätze ordnungsgemäßer Modellierung sichern durch ihre Anwendung die Qualität des Referenzmodells. Modelle sind subjektgestaltete Abbildungen von Prozessen und Sachverhalten, die es erlauben, einen unternehmensspezifischen Ablauf zu konstruieren.[447] Die Anwendung einheitlicher Grundsätze vermindert die Subjektivität eines Referenzmodells. SCHÜTTE schlägt sechs allgemeine Grundsätze vor, die anschließend erläutert werden:

- Grundsatz der Konstruktionsadäquanz
- Grundsatz der Sprachadäquanz
- Grundsatz der Wirtschaftlichkeit
- Grundsatz des Systematischen Aufbaus
- Grundsatz der Klarheit
- Grundsatz der Vergleichbarkeit[448]

Grundsatz der Konstruktionsadäquanz

Nach SCHÜTTE ist Konstruktionsadäquanz gegeben, wenn das Modell nachvollziehbar mit einem realem Gegenstand und geeigneten Kriterien ausgestattet ist.[449] Dabei sieht SCHÜTTE als ein Kriterium die Übereinstimmung zwischen Modellherstellern und Modellnutzern an, unter anderem in Bezug auf repräsentierende Probleme und Modelldarstellungen.[450] „Die Konstruktionsadäquanz bringt zum Ausdruck, dass Modelle nie gegen die Realität geprüft werden können."[451] Die einheitliche und eindeutige Benennung von Sachverhalten und damit die Namenskonvention sind unverzichtbar.

---

[443] Schütte 1998, S. 113.
[444] Vgl. Delfmann 2006, S. 47.
[445] Delfmann 2006, S. 47.
[446] Vgl. Delfmann 2006, S. 47.
[447] Vgl. Schütte 1998, S. 60.
[448] Vgl. Schütte 1998, S. 112 ff.
[449] Vgl. Schütte 1998, S. 113.
[450] Vgl. Schütte 1998, S. 114.
[451] Schütte 1998, S. 114.

Grundsatz der Sprachadäquanz

Die Bedingungen der Grammatik, der Syntax sind zu beachten.[452] Die zur Verfügung stehenden Modellsprachen werden nach dem Grundsatz der Sprachadäquanz untersucht und nach dem Objekt der Modellierung ausgewählt. Für das Referenzmodell dieser Arbeit eignet sich die ereignisgesteuerte Prozesskette (EPK), das für Organisationsdarstellung zu nutzen ist.

Grundsatz der Wirtschaftlichkeit

Die Wirtschaftlichkeit eines Modells muss sich an seinen Erstellungskosten und der Nutzeffektivität messen lassen. Die Adaption und Veränderbarkeit bei neuen Anforderungen muss gegeben sein sowie die Plausibilität. Das heißt, dass adaptive Referenzmodellierungen den Grundsatz der Wirtschaftlichkeit erfüllen müssen.[453]

Grundsatz des Systematischen Aufbaus

Der Systematische Aufbau bei der Entwicklung eines Modells fordert das eine „ganzheitliche konsistente perspektivisch motivierte Sichtweise angewandt werden muss".[454] DELFMANN postuliert hierzu, das dieser Grundsatz „im Allgemeinen auf die in methodischen Informationssystemarchitekturen häufig verfolgte Sichtentrennung ab[zielt], die eine Komplexitätsreduktion der resultierenden Modellsysteme verspricht".[455] Verschiedene Modelladaptionen sind zu validieren, „um eine kombinierte Anwendung der Mechanismen zu ermöglichen".[456]

Grundsatz der Klarheit

Ein Modell erfüllt den Grundsatz der Klarheit durch die Nachvollziehbarkeit und die Verständlichkeit. Die Sicherung dieses Grundsatzes erfolgt ebenso durch die Hierarchisierung, die Layoutgestaltung und die Filterung. Der Aspekt der Hierarchisierung wird erreicht durch die Klarheit der Kriterien zum Beispiel bei einer Betrachtung des Organisationssystems. Die Gestaltung des Layouts ist dependent von den erforderlichen Objekten des Modells, die in der grafischen Darstellung in Anzahl und Komplexität aufgenommen werden.[457] Nach DELFMANN steht dieses Kriterium „eng mit den Grundsätzen der Richtigkeit, Relevanz und Wirtschaftlichkeit zusammen da durch mangelnde Klarheit im Rahmen der Adaption erstens Fehler in den Modellen entstehen können, zweitens gegebenenfalls Modellteile falschen Adaptionsparameterausprägungen zugeordnet werden und drittens durch diese Fehler Zusatzaufwand zur Beseitigung der Fehler entsteht".[458] Die Filterung sollte sich nach SCHÜTTE bei einem Modell auf inhaltliche und sprachliche Aspekte orientieren, um eine ziel- und zweckgerichtete Klarheit zu erreichen.[459]

---

[452] Vgl. Schütte 1998, S. 114.
[453] Vgl. Schütte 1998, S. 114, Delfmann 2006, S. 61.
[454] Schlagheck 2000, S. 59.
[455] Delfmann 2006, S. 61.
[456] Delfmann 2006, S. 61.
[457] Vgl. Schütte 1998, S. 132.
[458] Delfmann 2006, S. 60.
[459] Vgl. Schütte 1998, S. 132.

Grundsatz der Vergleichbarkeit

Die Vergleichbarkeit der Modelle kann durch den Bezug auf organisationsgenutzte Modelle mit dem Referenzmodell erreicht werden. Damit ist eine Überprüfung sowie Fehlersuche in dem entwickelten Modell gegeben. Das Ziel ist die Erreichung der Realitätsnähe und Validität eines Modells. Dabei sind die Konsistenz von genutzten Modellen mit vergleichbaren Sachverhalten, Techniken sowie die Modellierungssprachen einzubeziehen.[460] DELFMANN betont, „dass Adaptionsmechanismen auf unterschiedliche Modellierungssprachen bzw. Ergebnismodelle dieser Modellierungssprachen äquivalente Auswirkungen haben".[461]

Der Verfasser nutzt die oben aufgeführten Hinweise bei der Modellierung seines Referenzmodelles und in den Expertengesprächen über die Gestaltung des Referenzmodelles für die organisationale Nutzung. Um das Referenzmodell zu konstruieren und anzuwenden, ist die Orientierung an einem Vorgehensmodell essenziell.

Vorgehens- und Referenzmodell

Der Begriff Vorgehensmodell kommt ursprünglich aus der Softwareentwicklung[462] und legt die zeitliche Abfolge der Phasen mit ihren Aktivitäten fest[463]. Im Allgemeinen wird das Vorgehensmodell von HEINRICH & LEHNER wie folgt definiert: „der als Modell abgebildete Prozess zum Lösen eines Problems".[464] BRUGGER illustriert diesen Lösungstransformationsprozess als Vorgehensmodell vom gegebenen Istzustand zum angestrebten Sollzustand. Die definierten Schritte des Vorgehensmodells stellen somit eine Orientierungshilfe dar und können situativ angepasst werden.[465]

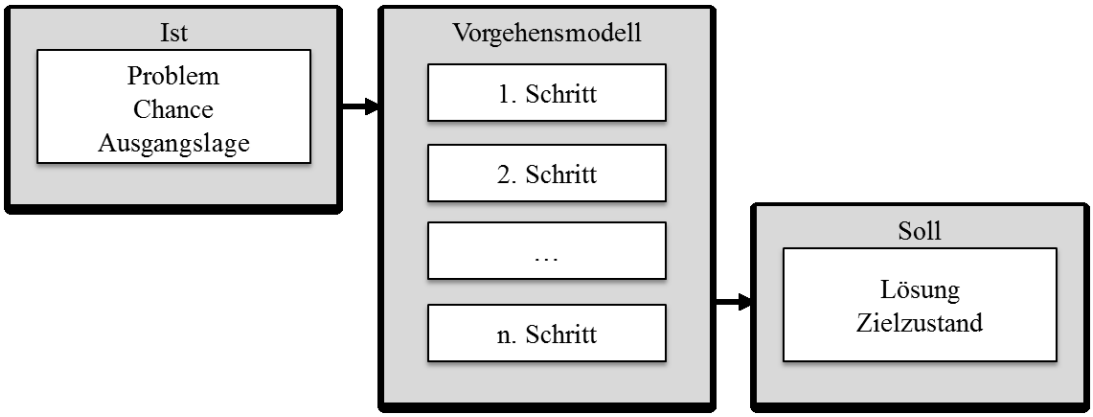

Abbildung 24: Transformation des „Ist" zum „Soll" mittels eines Vorgehensmodells[466]

Um ein Referenzmodell zu entwickeln und anzuwenden existieren mehrere Vorgehensmodelle mit gleichartiger Grundstruktur. Aus der Sicht des Verfassers stellt das Vorgehensmodell von

[460] Vgl. Delfmann 2006, S. 60.
[461] Delfmann 2006, S. 61.
[462] Vgl. Bullinger & Fähnrich 1997, S. 11.
[463] Vgl. Gutzwiller 1994, S. 14.
[464] Heinrich & Lehner 2005, S. 404.
[465] Vgl. Brugger 2005, S.161.
[466] Brugger 2005, S.161.

SCHLAGHECK den umfassendsten Entwicklungs- und Anwendungsansatz dar. Der iterative Prozess der gleichberechtigten und miteinander gekoppelten Referenzmodell-Entwicklungsphase und -anwendungsphase ist in Abbildung 25 skizziert.[467] Die Entwicklungs- und Anwendungsphase beinhalten die folgenden Aktivitäten:

Tabelle 8: Aktivitäten der Referenzmodell-Entwicklung und -Anwendung[468]

Entwicklungsphase	Anwendungsphase
• Problemdefinition • Analyse und Zerlegung der Problemdomäne • iterative und inkrementell Konstruktion des Referenzmodells • Evaluation und Evolution	• Problemdefinition • Anforderungsermittlung • Suche und Selektion • Konstruktion bzw. Anwendung

Für die vorliegende Arbeit ist das Ergebnis vom iterativen Prozess das spezifische Wissensschutz-Referenzmodell für eine IT-Beratung.

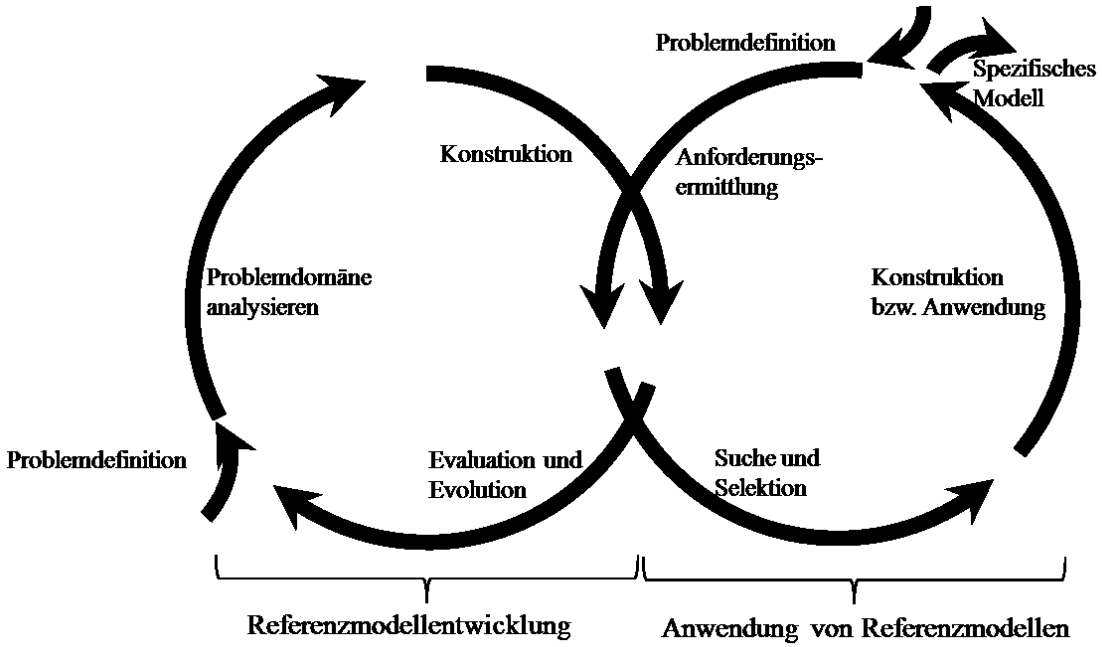

Abbildung 25: Iterative Prozesse der Referenzmodell-Entwicklung und -Anwendung[469]

Zusammenfassend sind diese allgemeinen Anforderungen und Grundsätze ordnungsmäßiger Modellierung Grundlage für das zu gestaltende Referenzmodell. Zu entwickeln sind konkrete Artefakte für ein Risikoinformationssystem zur Unterstützung des Wissensschutzes bei der ISE in IT-Beratungen mit externen Dienstleistern. Mit diesem Referenzmodell wird ein Gestaltungsmodell entwickelt, das die Projektakteure bei ihren zu treffenden Entscheidungen unterstützen soll. „Gestaltungsmodelle sind Entscheidungsmodelle, die aus der Kombination von Zielen mit Erklärungsmodellen und Lösungsalgorithmen hervorgehen.“[470]

[467] Vgl. Schlagheck 2000, S. 78.
[468] Eigene Darstellung.
[469] Schlagheck 2000, S. 78.
[470] Peritsch 2000, S. 136 f.

3.2.2 Darstellungstechnik

Um die Modellierungskomplexität zu reduzieren werden Informationssysteme in verschiedene Sichten unterteilt.[471] In dem ARIS-Modell[472] werden die Daten-, Funktions-, Organisations- und Prozesssicht für die Modellierung der Informationssysteme verwendet. Die Prozesssicht demonstriert die dynamischen Aspekte des Modells, und die statischen Aspekte werden in der Daten-, Funktions- und Organisationssicht präsentiert.[473] ARIS bietet für die Modellierung der Sichten diverse Modelltypen an. „Ein Modelltyp repräsentiert eine bestimmte Notation, die für die Modellierung eines oder mehrerer Aspekte von Prozessen genutzt werden kann.“[474] Jedem Modelltyp ist eine begrenzte Anzahl von Objekttypen mit einer dezidierten Bedeutung und visualisierten Präsentation zugewiesen.[475] Ein Objekttyp kann dagegen mehreren Modelltypen zugewiesen sein. Die Relationen zwischen den Objekttypausprägungen werden mittels gerichteter oder ungerichteter Kanten illustriert.

Damit die Zusammenhänge deutlich werden, modelliert die Arbeit die Steuerungssicht bzw. die Prozesssicht. Dazu werden die Darstellungsweisen der ereignisgesteuerten Prozesskette (EPK) genutzt. EPKs haben die Grundelemente Funktion, Ereignis und Konnektor. Diese Grundelemente verbinden gerichtete Kanten, um den Kontrollfluss abzubilden. Funktionen in einem EPK sind aktive Elemente, die bei dem Vorliegen mehrerer Prozesswege Entscheidungskompetenz besitzen. Ereignisse haben keine Entscheidungskompetenz und sind daher passive Elemente, die einen eingetretenen Zustand zum Start und zum Ende einer EPK beschreiben.[476] Konnektoren sind Verknüpfungsknoten von Funktion und Ereignis in nicht sequentiellen EPKs, die die logischen Operatoren „und“, „inklusives oder“ und „exklusives oder“ sein können.

Zu dieser Prozesssicht gehören auch Funktionszuordnungsdiagramme (FZD) die Input- und die Outputdaten von Funktionen abbilden. Sie verbinden damit die Daten- und Funktionssicht und können um Objekttypen[477] ergänzt werden. Die EPK könnte auch direkt um diese Zuordnungen erweitert werden und würde dann als erweiterte ereignisgesteuerte Prozesskette (eEPK) bezeichnet werden. Um die Übersichtlichkeit in der Prozesssicht sicherzustellen werden die EPK und das FZD verwendet. Die verwendeten Objekttypen in der EPK und FZD sind in der Tabelle 9 beschrieben.

---

[471] Vgl. Delfmann 2006, S. 43.
[472] Für eine Gesamtheit der ARIS-Modelltypen siehe vgl. Lehmann 2008, S. 29-60.
[473] Vgl. Gabriel et al. 2002, S. 290.
[474] Lehmann 2008, S. 26.
[475] Vgl. Lehmann 2008, S. 27 f.
[476] Vgl. Lehmann 2008, S. 52, S. 65.
[477] Zum Beispiel Organisationseinheiten, Personentypen und Anwendungstypen.

Tabelle 9: Notation der Elemente der EPK und des FZD[478]

Symbol	Benennung	Bedeutung
	Ereignis	Beschreibung eines eingetretenen Zustandes, von dem der weitere Verlauf des Prozesses abhängt.
	Funktion	Beschreibung der Transformation von einem Inputzustand zu einem Outputzustand.
	Cluster	Sammlung zusammengehörender Entitytypen
	DV-Funktionstyp	Typisierung von DV-Funktionen. Sie stellen die kleinste Einheit dar, die vollständig ausgeführt werden muss.
⊗ ∨ ∧	Logischer Operator „exklusives oder“ Logischer Operator „oder“ Logischer Operator „und“	Logische Verknüpfungsoperatoren beschreiben die logische Verknüpfung von Ereignissen und Funktion.
- - - - - - - - - - - - →	Kontrollfluss	Zeitlich-logischer Zusammenhang von Ereignissen und Funktionen.
→ ←	Datenfluss	Beschreibung, ob Daten von einer Funktion gelesen, erstellt oder aktualisiert werden.
———	Zuordnung	Zuordnung von Ressourcen.

Der Fokus der Arbeit liegt auf der Detaillierung der Funktionen, um das bestehende Phasenmodell zum (Out-) Sourcing für den Wissensschutz in der ISE zu präzisieren. Um die einzelnen Funktionen im Referenzmodell im Detail zu erläutern, werden die Darstellungskonventionen zum FZD in Abbildung 26 festgelegt. Die jeweilige Funktion, der alle möglichen Elemente zugeordnet sind, befindet sich im Zentrum. Im linken oberen Bereich sind die Inputdaten und im rechten oberen Bereich die Outputdaten für die Funktion. Die ausführende Rolle ist im linken unteren Bereich abgebildet. Rechts unten befinden sich die Funktionalität, die die informationstechnische Unterstützung der Funktion beschreibt. Der Anwendungstyp ist bei allen Modell-Funktionen des Wissensschutz-Referenzmodells das Risikoinformationssystem und wird deshalb hier nicht aufgenommen.

[478] Modifiziert nach: Gadatsch 2008, S. 147, S. 192, S. 217.

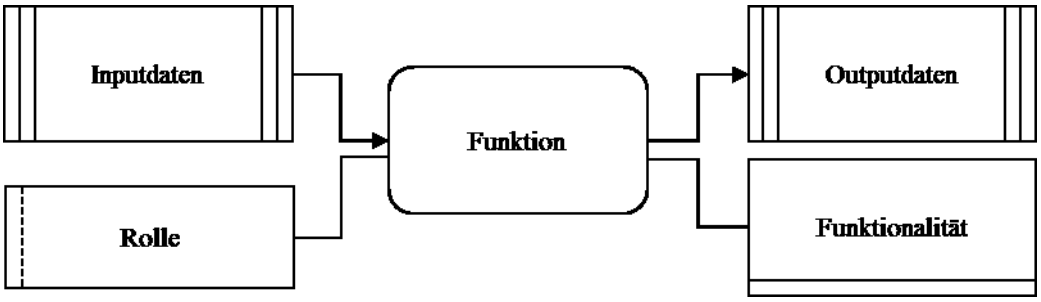

Abbildung 26: Darstellungsform eines Funktionszuordnungsdiagramms

3.3 Forschungsvorgehen

Dieses Unterkapitel präzisiert den skizzierten Forschungsprozess. Im Abschnitt 3.3.1 werden dazu die Methodik des *Literature Reviews* beschrieben, um einen Prototypen zu entwickeln. Der folgende Abschnitt deskribiert die Interview-Methodik für die Experteninterviews und das zweite Gruppeninterview. Die Schritte Leitfadenentwicklung, Expertenauswahl mit der Samplingstrategie, die Interviewdurchführung, die Transkription und die Auswertung der Interviews mit der qualitativen Inhaltsanalyse sind Bestandteil der Prototypevaluation mit Hilfe der Experteninterviews (Abschnitt 3.3.3). Der letzte Abschnitt des Kapitels schließt mit der Beschreibung des Pilotprojektes ab, zu den Einzelinterviews und ein Gruppeninterview gehören.

3.3.1 Prototypentwicklung mit Literature Review

Um einen Prototypen zu entwickeln wurden die Erkenntnisse aus einer initialen und kontinuierlichen Literaturanalyse genutzt. Die Literaturrecherche zum Wissensschutz orientiert sich methodisch an WEBSTER & WATSON[479] und damit an den für die WI zugrundgelegten Regeln. Die methodischen Stufen sind:

- Identifizierung der relevanten Literatur,
- Strukturierung des Reviews und
- die Konzeptentwicklung (Prototypentwicklung).

Die relevanten Quellen werden durch Schlagwort-, Rückwärts- und Vorwärtssuche identifiziert.[480] Mit dem *Literature Review* wird einerseits auf der etablierten Wissensbasis[481] zu den Themenfeldern Wissensschutz, -mechanismen und zu den angrenzenden Disziplinen recherchiert. Andererseits wird mit dem *Literature Review* die Neuwertigkeit der eigenen Arbeit überprüft.[482]

Identifizierung der relevanten Literatur

Die Literaturrecherche umfasste die Identifizierung der relevanten Literatur und damit die Suche nach Journal-Artikeln in den folgenden Datenbanken: *EBSCO* (Business Source Complete), *Elsevier ScienceDirect*, *JSTOR*, *Emerald Insight* und *EconBiz*. Mit Hilfe der Suchmaschine *Association for Information Systems Electronic Library* (AISeL)[483] wurden die Tagungsbände

[479] Webster & Watson 2002.
[480] Vgl. Webster & Watson 2002.
[481] Vgl. Hevner et al. 2004, S. 88.
[482] Vgl. Baker 2000, S. 219.
[483] Vgl. http://aisel.aisnet.org/ zum Beispiel: AMCIS, ECIS, ICIS, PACIS, HICSS, ACIS, DIGIT, BLED.

von Konferenzen durchsucht, die für die Wirtschaftsinformatik und IS-Forschung relevant sind. In jeder dieser Datenbanken wurde in Abhängigkeit von der Suchmaske in den Feldern nach *Title, Abstract, Subject, Topic* und *Keywords* nach dezidierten Schlagworten recherchiert.

Im Jahr 2013 fand die Initialrecherche in der Datenbank EBSCO mit der Suchzeit ab dem Jahr 2000 statt. Zuletzt wurde Anfang 2015 recherchiert und dabei konnten vier weitere relevante Artikel identifiziert werden. Dazu wurden die Suchworte und deren Kombinationen unter Berücksichtigung der angrenzenden Disziplinen der Arbeit festgelegt, die identifizierten relevanten Autoren sind in der Tabelle 10 dokumentiert.

Tabelle 10: Suchworte und relevante Autoren aus der Initialrecherche

Suchworte	Autoren
knowledge protection (and) mechanism	Ahmad et al. 2014, Amara et al. 2008, Drechsler & Natter 2012, Jiang 2002, Lawson et al. 2012, Norman 2001, Olander et al. 2009, 2010, 2011, 2012, 2014, Olander & Hurmelinna-Laukkanen 2010, Oxley & Sampson 2004, Perri & Andersson 2014, Subramanayam & Susarla 2007
knowledge protection (and) outsourcing	Ilvonen 2013, Nassimbeni et al. 2012, Perri & Andersson 2014, Subramanayam & Susarla 2007
knowledge protection (and) organizational knowledge	Ahmad et al. 2014, Birasnav et al. 2012, Desouza & Awazu 2004, Manhart & Thalmann 2015, Olander et al. 2014, Subramanayam & Susarla 2007, Tongo 2013
knowledge protection (and) information technology	Mayer 2006, Manhart & Thalmann 2015, Berčič & George 2009, Subramanayam & Susarla 2007, Desouza & Awazu 2004, Erickson et al. 2003, Olander et al. 2009, Desouza & Wazu 2005, Desouza 2006
knowledge protection (and) knowledge intensive	Ahmad et al. 2014, Amara et al. 2008, Birasnav et al. 2012, Co 2007, Olander et al. 2012, Steyn & Kahn 2008
knowledge protection (and) principal agent	Desouza & Awazu 2004

Die zum Teil evident geringe Ergebnisliste der wissenschaftlichen Beiträge wurden geprüft. Anzumerken ist, dass für *Knowledge Protection* in der englischen Literatur äquivalente Bezeichnungen[484] verwendet werden. Die Veröffentlichungen mit dem Bezug zu den formalen Schutzmechanismen, auf die sich die *Intellectual Property (Protection)* bezieht, fanden keine Berücksichtigung. Die Artikel mit einem geringen Anteil am Wissensschutz wurden ausgeschlossen.

Die in den Suchergebnissen angezeigten Artikel wurden nach Schlüsselworten gefiltert. Daraufhin folgte die Validierung der *Abstracts* in den identifizierten Artikeln, um die Relevanz und Priorität für das Thema zu ermitteln. Das Durcharbeiten der *Abstracts* ist nach WEBSTER & WATSON ein Qualitätskriterium, um die relevanten Artikel zu identifizieren. Ein spezieller Fokus ist auf Artikel zur IT-Branche gelegt worden. Explizit erfolgte die Literaturorientierung auf das Themengebiet der informalen Wissensschutzmechanismen. Die referenzierte Literatur von

[484] Vgl. Tabelle 4.

hochrelevanten Artikeln wurde recherchiert, selektiv ausgewählt und analysiert. Dadurch konnten weitere Artikel identifiziert werden, die nicht in der Suchmaschine indiziert waren.

Strukturierung des Reviews

Im zweiten Schritt erfolgte die Strukturierung der ausgewählten Artikel nach den für die Forschungsarbeit relevanten Themen und Kategorien. Weitere relevante Artikel sind im Kapitel 4 dokumentiert und in inhaltliche Themen eingeordnet. Diese Themen sind die Theorien mit strategischen Wissensschutzbezug und Positionierung zur Dienstleisterauswahl. Diese Kategorien sind die Voraussetzung um den Status Quo der wissenschaftlichen Artikel zu erfassen.

Konzeptentwicklung: Prototypentwicklung

Um einen Prototypen für ein theoretisches Wissensschutz-Referenzmodell zu konstruieren, wird auf den identifizierten inhaltlichen Themen und Kategorien aus den wissenschaftlichen Artikeln aufgebaut. Diese Erkenntnisse ergeben mit der langjährigen Praxiserfahrung des Verfassers, den Vorinterviews, informellen Gesprächen und einem Gruppeninterview den Input für das entwickelte Wissensschutz-Referenzmodell, das im Kapitel 5 charakterisiert wird. Mit einer konstruierten Vorabversion des prototypischen Artefakts wird im Forschungsprozess experimentiert.[485] Der Prototyp hat das Ziel neue Erkenntnisse zu erhalten[486] sowie Adäquanz und Umsetzbarkeit im Sinne eines *Proof of Concepts* zu prüfen und zu evaluieren[487]. Nach BECKER et al. wird der Prototyp in der WI vielfach als Hauptergebnis eines Forschungsansatzes verstanden.[488] Der entwickelte Prototyp wird für zwei exemplarische IT-Projekte in den Experteninterviews genutzt, um den Interviewpartnern das Referenzmodell zu erläutern.

3.3.2 Methodik der Experteninterviews und des Gruppeninterviews

Eine der bedeutsamsten Erhebungsmethoden der empirischen Sozialforschung stellt das Interview dar. Bei einem Interview wird bewusst und gezielt eine Gesprächssituation hergestellt, was ein allgemeiner Kritikpunkt ist, weil die ermittelten Daten des Dialogs durch ein Bias charakterisiert sind.[489] Um diesem Kritikpunkt entgegenzuwirken wurden die Interviews in der Arbeitsumgebung der Befragten durchgeführt und bei mangelnder Nachvollziehbarkeit der Argumentation direkt nachgefragt. Die Befragungsarten vom qualitativen Paradigma lassen sich nach den Dimensionen in der Tabelle 11 differenzieren. Die für diese Arbeit charakterisierenden relevanten Formen des Interviews sind hervorgehoben.

[485] Vgl. Stahlknecht & Hasenkamp 2005, S. 219.
[486] Vgl. Wilde & Hess 2007, S. 282.
[487] Vgl. Dumke 2003, S. 116, Frank 2006, S. 42.
[488] Vgl. Becker et al. 2009, S. 16.
[489] Vgl. Wrona 2005, S. 24.

Tabelle 11: Arten von Befragungen beim qualitativen Paradigma[490]

Dimensionen der Differenzierung	Formen des Interviews

1. Intention des Interviews	• **Vermittelnd, evtl. Aktionsforschung**
	• **Ermittelnd**
	  o **Informatorisches Interview**
	  o Analytisches Interview
	  o Diagnostisches Interview

2. Standardisierung	• **Halb-standardisiert** • Nicht-standardisiert
3. Struktur der zu Befragenden	• **Einzelinterview** • **Gruppeninterview, evtl. Gruppendiskussion**
4. Form der Kommunikation	• **Mündlich**
5. Stil der Kommunikation, Interviewverhalten	• **Weich** • Neutral
6. Art der Fragen	• **Offen**
7. Kommunikationsmedium bei mündlichen Interviews	• **Face-to-Face, persönlich** • Telefonisch

Damit mit verdeutlicht, dass die differierenden Interviewformen verschieden charakterisiert werden,[491] zum Beispiel in Intention, Standardisierung, Struktur, Kommunikationsstil und -medium. Bei der ersten und dritten Dimension in der Tabelle 11 sind mehrere Formen hervorgehoben, da die vermittelnde und ermittelnde Interviewform wie auch die Befragungsstrukturen des Einzel- und Gruppeninterviews angewendet wurden. Die Details dazu werden nach der Beschreibung der *Methodologischen Kriterien und qualitative Interviewformen* unter *Methodik der Experteninterviews* bzw. des *Gruppeninterviews* dokumentiert.

Methodologische Kriterien und qualitative Interviewformen

Unabhängig vom qualitativen Interviewtyp müssen nach LAMNEK vornehmlich methodologische Kriterien genügen, die die Grundlage bilden:

- „Explikation und Prozesscharakter des qualitativen Interviews manifestieren sich im Prinzip der Reflexivität von Gegenstand und Analyse.
- Qualitative Interviews versuchen, den Charakter des Alltagsgesprächs zu realisieren.
- Prinzip der Zurückhaltung durch den Forscher. Qualitative Interviews lassen den Befragten zu Wort kommen: Er ist nicht nur Datenlieferant, sondern er determiniert als Subjekt das Gespräch qualitativ und quantitativ.
- Prinzip der Relevanzsysteme der Betroffenen. Es erfolgt keine Prädetermination durch den Forscher, sondern eine Wirklichkeitsdefinition durch den Befragten.
- Prinzip der Kommunikativität. Es gilt das kommunikative Regelsystem des Befragten; der Interviewer hat sich daran anzupassen.
- Prinzip der Offenheit. Das Interview ist für unerwartete Informationen zugänglich.
- Prinzip der Flexibilität. In der Interviewsituation reagiert der Forscher variabel auf die Bedürfnisse des Befragten.

[490] Modifiziert nach: Lamnek & Krell 2016, S. 315.
[491] Vgl. Wrona 2005, S. 24.

- Prinzip der Prozesshaftigkeit. Das qualitative Interview ermittelt bevorzugt Deutungs- und Handlungsmuster der Befragten, die sich im Verlauf des Interviews entwickeln.
- Prinzip der datenbasierten Theorie. Das qualitative Interview dient eher der Genese als der Prüfung von Theorien.
- Prinzip der Explikation. Die Aussagen im Interview emergieren dadurch zur Theorie (Typenbildung), indem sie im Interviewprozess interpretiert werden."[492]

Auf ähnliche oben aufgeführte Prinzipien verweisen MAYRING[493] und FLICK et al.[494]. Unter Einhaltung dieser Merkmale ist das Ziel eine *anwendungsorientierte Handlungsempfehlung*[495] im Rahmen der Referenzmodellierung zu entwickeln. Um das angestrebte Ziel zu erreichen, wurden qualitative Experteninterviews mit IT-Projektakteuren zum Wissensschutz als Datenerhebungsinstrument durchgeführt, da sie für die Beantwortung der Forschungsfragen zielführend sind. Experteninterviews finden speziell im Zusammenhang von multimethodischen Forschungsdesigns Anwendung, um den Forschungsgegenstand eines Themas zu gliedern.[496] Die Experteninterviews stellen nach MEUSER & NAGEL eine Sonderform des problemzentrierten Interviews dar,[497] da sie besonders im Umfeld eines heuristischen Bezugsrahmens verwendet werden.[498] Die verschiedenen Formen qualitativer Interviews vergleichen LAMNEK & KRELL bezüglich ihrer methodologischen Prämissen.[499] Das problemzentrierte Interview fasst alle Formen einer offenen, halbstrukturierten Befragung zusammen und stellt eine Variante des narrativen Interviews dar, die nach Möglichkeit ein offenes Gespräch anvisiert.[500] Der Interviewer muss bei dieser Interviewform sein erarbeitetes Vorwissen im Rahmen seiner Analysen zur speziellen Problemstellung darlegen. Somit wird angestrebt, das Spannungsfeld zwischen Theoriegeleitetheit und Offenheit aufzulösen.[501] Das Vorwissen reflektiert sich im Interviewleitfaden und wird als heuristisch-analytischer Rahmen zur Anregung von Interviewfragen appliziert.

Methodik der Experteninterviews

Die Experteninterviews differenzieren sich in eine vermittelnde und ermittelnde Komponente. Der erste Interviewbestandteil fokussiert die Modellvorstellung und bezieht sich auf die vermittelnden Aspekte mit der Aktionsforschung. Die Modellvorstellung wurde für den Interviewleitfaden mit zwei praxisnahen IT-Projekt-Beispielen aufgearbeitet. Diese basieren auf dem theoretischen Modell, die den entwickelten Prototypen darstellen. Der zweite Interviewbestandteil konzentriert sich auf das informatorische Interview. Zu den informatorischen Interviews gehören die Experteninterviews, die Bestandteil vom Referenzmodell-Entwicklungsprozess sind. Experteninterviews ordnen sich in die qualitativen Einzelbefragungen ein.[502] Diese sind

[492] Lamnek & Krell 2016, S. 332 f.
[493] Mayring 2016, S. 24 ff.
[494] Flick et al. 2003, S. 24.
[495] Vgl. Wrona 2005, S. 9.
[496] Vgl. Bogner & Menz 2002.
[497] Vgl. Lamnek & Krell 2016, S. 338, Meuser & Nagel 1991, S. 443 f.
[498] Vgl. Wrona 2005, S. 25.
[499] Vgl. Lamnek & Krell 2016, S. 362.
[500] Vgl. Wrona 2005, S. 25.
[501] Vgl. Wrona 2005, S. 25.
[502] Vgl. Bortz & Döring 2006, S. 313.

weitgehend leitfadenunterstützt, um sich an einer Struktur zu orientieren.[503] Um die Vergleichbarkeit der Experteninterviews zu gewährleisten sind Interviewleitfäden als Gedächtnisstütze und Orientierungsrahmen für den Forscher effektiv, im Vergleich zu einer reinen Frage-Antwort-Schablone.[504] Der Forschende kann damit sicherstellen, dass im Gesprächsverlauf alle Aspekte und Fragenkategorien besprochen werden.[505]

Eine besondere Bedeutung für den Autor hat die kritische Reflexion des Modells. Um diese zu fördern und die dezidierte Expertise der Interviewten im Interviewverlauf offenzulegen, war die nicht prädeterminierte Interviewdurchführung hilfreich.[506] Dependent des jeweiligen Kompetenzbereiches des Experten (Tabelle 13) wurde die Diskussionstiefe thematisch fokussiert.

Die vorliegende Studie erhebt die qualitativen Daten mit Hilfe von halb-standardisierten, leitfadengestützten Interviews. Nachdem die Experteninterviews in transkribierter Form vorliegen, wird das theoretische Modell im iterativen Prozess weiterentwickelt, korrigiert und validiert. Diese Prozessvalidierung, -erweiterung, -vertiefung und -aktualisierung vom theoretischen Modell dienen der Beantwortung der Forschungsfragen. Das erweiterte Wissensschutz-Referenzmodell aus den Experteninterviews bildet die Grundlage für das durchgeführte Gruppeninterview.

Methodik des Gruppeninterviews

Zur Vorbereitung des halb-standardisierten Gruppeninterviews wurden in vermittelnden Einzelinterviews die Wissensgebiete des untersuchten IT-Projekts begleitend kategorisiert. Diese Einzelinterviews dienten zur Vorbereitung vom Gruppeninterview und um praktische Erfahrung im Rahmen der Aktionsforschung zu generieren. Auf der Grundlage der Einzelinterviews wurde das Gruppeninterview mit der vermittelnden und ermittelnden Komponente vorbereitet. Die Struktur und damit die Leitfadenunterstützung liefert eine erstellte Präsentation mit Agenda. Nachdem das Gruppeninterview in transkribierter Form vorliegt, wird das Modell weiterentwickelt, korrigiert und validiert.

3.3.3 Prototypevaluation mit Experteninterviews

Der Prozess von qualitativen Interviews folgt dem Phasenablauf nach BORTZ & DÖRING, der in Abbildung 27 visualisiert ist. Die Datenerhebung startet mit der inhaltlichen Vorbereitung und der Planung des Interviewkonzeptes. Zuerst ist zu definieren, in welchem Umfeld geforscht werden soll, wie umfangreich die Forschungsfragen sind und ob eine offene, halb-standardisierte oder standardisierte Methodik verfolgt wird.[507]

[503] Vgl. Flick 2005.
[504] Vgl. Wrona 2005, S. 26.
[505] Vgl. Wrona 2005, S. 26.
[506] Vgl. Lamnek & Krell 2016, S. 332.
[507] Vgl. Bortz & Döring 2006, S. 310 f.

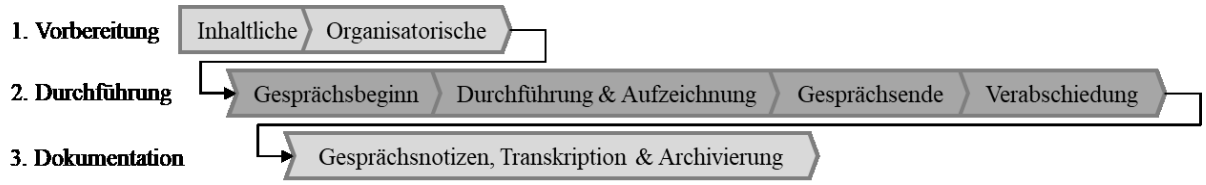

Abbildung 27: Ablauf von qualitativen Interviews[508]

Leitfadenentwicklung und Interviewunterlage

Auf der Grundlage des theoretischen Wissensschutz-Modells (Prototyp) wurde ein Interviewleitfaden mit zwei praxisnahen IT-Projekten entwickelt, die zur Erläuterung des Modells, der Funktionen und Illustration der Praxistauglichkeit dienten. Dazu kam ein exemplarisches Skalensystem zum Einsatz, das sich an etablierten Unternehmensskalen orientierte. So erfolgte die Vorstellung des Prototyps mit dem Bezug zur betrieblichen Praxis und die Demonstration der Anwendbarkeit des Modells. Der entwickelte Experteninterviewleitfaden mit dem Prototyp im Prozessdesign konnte in Vorgesprächen mit wissenschaftlichen Mitarbeitern und IT-Projektakteuren immer weiterentwickelt und validiert werden. Der betriebliche Ansprechpartner, mit dem das erste Experteninterview durchgeführt wurde, erteilte die Genehmigung für weitere Interviews. Der Leitfaden der qualitativen Untersuchung wird überblicksweise in Tabelle 12 visualisiert und beinhaltet fünf Phasen, die wie dargestellt chronologisch besprochen wurden. In den Phasen drei und vier gab es teils Variationen. Diese beziehen sich auf die Verständnisfragen, Fragen und Diskussion.

[508] Vgl. Bortz & Döring 2006, S. 310 f.

Tabelle 12: Interviewleitfaden - Überblick[509]

Phase / Agendapunkt	Detailbeschreibung
1. Gesprächsbeginn	• Vorstellung • Ziel des Forschungsprojekts • Interviewaufzeichnung beginnt • Dokumentation der Vertraulichkeit und Anonymität
2. Themenvorstellung, Begriffsklärung und offene Eingangsfrage	• Wissensschutz Beispielszenario • Was verstehen Sie unter Wissensschutz in IT-Projekten mit externen Dienstleistern? • gemeinsame Begriffsabgrenzung • Persönliche Berufspraxis und Erfahrungen
3. Modellvorstellung ggf. Verständnisfragen und Diskussion	Vorstellung der zu betrachtenden Funktionen mit den identifizierten Bewertungskategorien anhand von zwei Praxisbeispielen: 1. Strategische Planung 2. Projektkategorisierung 3. Wissenskategorisierung 4. Dienstleisterkategorisierung 5. Risikobewertung und Auswahlentscheidung
4. Modell-Validierung Fragen und Diskussion	Fragen und Diskussion zu den fünf identifizierten Funktionen: • Bewertungskategorien und deren Definitionen • Kategoriegewichtungen • Bewertungsskala • Wissenskombinationen • Akteure • Verantwortlichkeiten • Visualisierung • praktische Erfahrung und Anwendbarkeit
5. Gesprächsende	• Praxiserfahrung in der IT-Branche • Studienfach • Interesse an Forschungsergebnissen • Dank und Verabschiedung

Wie dem Interviewleitfaden zu entnehmen ist, erfolgte eine kurze persönliche Vorstellung, dann die Zielstellung des Vorhabens und das Einverständnis zur Aufzeichnung. Gesondert erfolgte ein Hinweis, dass die Fragen und Anmerkungen aus der persönlichen Sicht und der beruflichen Erfahrung beantwortet werden sollten. Ein gemeinsames Verständnis für die Begrifflichkeiten und die für das Vorhaben entwickelte Definition zum Wissensschutz sicherte die anschließende Diskussionsgrundlage. Das entstandene Prozessdesign des Wissensschutz-Modells mit seinen Funktionen, Akteuren, Definitionen und Beispielszenarien wurde folgend Schritt für Schritt erläutert und diskutiert. Anschließend wurde der entwickelte Fragenkatalog für jede Funktion mit den Experten erörtert. Mit Hilfe des erarbeiteten Fragenkatalogs sollten die designten Prozesse des Prototyps weiterentwickelt, korrigiert und validiert werden.

Jedem interviewten Experten wurde als vertrauensbildende Maßnahme die Anonymität zu den Interviewaussagen zugesichert, indem vor dem Interview unter anderem kommuniziert wurde,

[509] Eigene Darstellung.

dass die Transkription durch den Autor durchgeführt wird. Dieses Vorgehen war im Vorfeld mit dem betrieblichen Ansprechpartner abgestimmt, damit diese sensitiven Informationen offeriert werden. Alle vertraulichen Informationen wie Personennamen, Organisationsbezeichnungen und Internas, um konkrete Rückschlüsse auf Unternehmen ziehen zu können, wurden vom Transkriptor deshalb extrahiert.

In den Experteninterviews bezeichneten die Befragten die externen Dienstleister zum Teil als Partner, weil diese in der untersuchten IT-Beratung als Synonyme deklariert werden. Ein Interviewpartner merkte an, dass die richtige Bezeichnung Dienstleister ist, da mit ihnen kein partnerschaftliches Verhältnis positioniert wird.[510] Dennoch existieren in anderen Unternehmensbereichen der untersuchten IT-Beratung Partnerschaftsverträge, die nicht der ISE für Auftraggeber zuzuordnen sind.

Expertenauswahl und Sampling

Bei qualitativen Samplingstrategien stehen im Vergleich zu den quantitativen (Ziel der Repräsentativität) die Angemessenheit für die jeweiligen Forschungsfragen im Vordergrund. Damit steht die Eignung der Fälle für die Aufdeckung der zu erforschenden Strukturen und Zusammenhänge im Fokus und nicht die Fallzahl.[511] Infolgedessen hängt die Qualität des qualitativen Samplings hauptsächlich von den folgenden Punkten ab:

- zu welchen Vergleichen es anregt,
- welche Eckpunkte es aufzeigt und
- inwieweit es Elemente für eine Theorieneuentwicklung oder -weiterentwicklung bereitstellen kann.[512]

Bei der Expertenwahl findet im Vorfeld grundsätzlich eine theoretische Samplingstrategie statt. Für diese Samplingstrategie gibt es die minimale und maximale Kontrastierung, wobei bei ersteren ein ähnlicher Fall bzw. Interviewpartner und bei zweitem ein sehr verschiedener Interviewpartner ausgewählt wird.[513] In der vorliegenden Expertenbefragung fand in Bezug auf die Projektakteure einer IT-Beratung die theoretische Samplingstrategie der maximalen Kontrastierung Anwendung. Damit wird in der Arbeit das Ziel verfolgt, die identifizierten Wissensschutzkategorien im entwickelten Prototypen auf Relevanz zu untersuchen und die unterschiedlichen Akteursgruppen, die bei dem Referenzmodell agieren sollen, zu befragen.[514] Alle Experten kommen aus dem IT-Umfeld und ihre verschiedenen Akteurs- und Rollensichtweisen können den Prototypen mit seinen Kategorien weiterentwickeln und evaluieren. Die Auswahl der Experten erfolgte nach definierten Kriterien.[515] Das Ziel war es, zu jeder der drei Hauptakteursgruppen, Projektmanagement, Strategie- / Kunden- / Management und IT-Sourcing Management jeweils drei Vertreter zu gewinnen. In der Tabelle 13 ist das Stichprobendesign und die

[510] Vgl. IP_10.
[511] Vgl. Lamnek & Krell 2016, S. 186.
[512] Vgl. Brüsemeister 2000, S. 24.
[513] Vgl. Wrona 2005, S. 23.
[514] Vgl. Wrona 2005, S. 23.
[515] Vgl. Bortz & Döring 2006.

durchgeführten halb-standardisierten Experteninterviews mit den IT-Projektakteuren visualisiert gegenübergestellt. Dazu ist anzumerken, dass in der Hauptakteursgruppe Strategie- / Kunden- / Management insgesamt fünf Experten befragt wurden, weil diese als Top-Management Vertreter eine zentrale Akteursrolle in dem Modell einnehmen. Zudem sind die Akzeptanz und Realisierung des Modells von ihnen abhängig.

Tabelle 13: Stichprobendesign und Ist-Durchführung der Interviews[516]

Stichprobendesign	Interviewdurchführung im Ist-Zustand
Drei Projektmanagement-Vertreter: • grundlegenden Erfahrungen im Projektmanagement • erfahrene Projektmanager • Senior Projektmanager	Drei Projektmanagement-Vertreter: • Projektmanager • Projektmanager / Management • Senior Projektmanager
Drei Strategie- / Kunden- / Management Vertreter: • Abteilungsleiter / Bereichsleiter • Top-Manager • Kundenmanager / Strategiemanager	Fünf Strategie- / Kunden- / Management Vertreter: • Abteilungsleiter / Management • Top-Manager (Pretest-Interview) • Kundenmanager • Strategiemanager • Strategiemanager
Drei IT-Sourcing Management Vertreter: • IT-Sourcing Mitarbeiter • IT-Sourcing Abteilungsleiter • Suppliermanager	Drei IT-Sourcing Management Vertreter: • IT-Sourcing Mitarbeiter • IT-Sourcing Abteilungsleiter • Suppliermanager

Alle in der Tabelle 14 aufgeführten Befragten sind männlich und hatten im Durchschnitt 20,1 Jahre Berufserfahrung und davon im Durchschnitt 7,5 Jahre Berufserfahrung in anderen Unternehmen. Die elf Interviews hatten eine durchschnittliche Länge von 99 Minuten. Dabei dauerte die Modellvorstellung durchschnittlich 46 Minuten und die Diskussion im Durchschnitt 53 Minuten.

[516] Eigene Darstellung.

Tabelle 14: Teilnehmer an den qualitativen Experteninterviews[517]

Name	Expertise / Rolle	Berufs-erfahr-ung	Erfahrung in an-deren Unterneh-men	Ort	Datum	Dauer in Minuten
IP_1	Top-Manager	29	3	Berlin	08.06.15	89'
IP_2	IT-Sourcing M.	25	22	Frankfurt	14.07.15	121'
IP_3	Abteilungsl. / M.	17	10	Frankfurt	15.07.15	92'
IP_4	Projektm. / M.	21	5	Frankfurt	29.07.15	127'
IP_5	Strategiemanager	15	2	Frankfurt	10.08.15	95'
IP_6	IT-Sourcing A.	4	0	Frankfurt	11.08.15	89'
IP_7	Senior Projektm.	22	5	Frankfurt	12.08.15	84'
IP_8	Kundenmanager.	25	7	Frankfurt	01.09.15	80'
IP_9	Strategiemanager	23	5	Frankfurt	02.09.15	97'
IP_10	Suppliermanager	25	12	Frankfurt	02.09.15	110'
IP_11	Projektmanager	15	12	Berlin	14.09.15	103'
		Ø 20,1 Jahre	Ø 7,5 Jahre			Ø 99‘ Minuten

Nach dem achten Experteninterview stellte sich eine erste theoretische Sättigung ein. Diese Sättigung besagt nach GLASER & STRAUSS[518], dass der Prototyp durch die Befragungen hinreichend validiert wurde. Mit Hilfe des zyklischen Prozesses von Interview zu Interview wurden neue Kategorien und Hinweise stets in Folgeinterviews diskutiert und validiert. Damit konnte der Prototyp sukzessive erweitert und bis zur erwähnten Sättigung weiterentwickelt werden. Um das zu bestätigen, wurde nach dem achten Interview mit jeweils einem Experten der drei Vertretergruppen ein Interview durchgeführt. Auf der Interviewunterlage wurden die Anmerkungen der Experten dokumentiert und anschließend kritisch reflektiert und die konkreten Anpassungen im Experten-Interviewleitfaden[519] für das Folgeinterview aktualisiert. Die hauptsächlichen Modifikationen am Modell im Interviewverlauf sind im Kapitel 5 dokumentiert und gekennzeichnet.

Interviewdurchführung und Transkription

Jedes der Experteninterviews wurde mit den Projektakteuren einzeln und in einem geschlossenen Meetingraum durchgeführt, dadurch konnten Störungen vermieden werden und die Vertraulichkeit war gewährleistet. Die Interviews dauerten zwischen 80 und 127 Minuten und fanden in deutscher Sprache statt. Grundlage der Interviews bildete der Experten-Interviewleitfaden (Unterkapitel 8.1) und zwei exemplarische praxisnahe IT-Projekte die zur Veranschaulichung des Prototyps dienten. Die Aufnahme erfolgte mit einem digitalen Aufnahmegerät. Hinzuweisen ist, dass bei dem ersten Interview mit dem betrieblichen Ansprechpartner lediglich der ermittelnde Interviewbestandteil aufgezeichnet wurde. Ab dem zweiten Interview wurden die komplette Befragung aufgezeichnet, da auch beim vermittelnden Interviewbestandteil wertvolle Verständnisfragen zum Modell zur Diskussion und Hinweisen führten. Die anschließende

[517] Eigene Darstellung.
[518] Vgl. Glaser & Strauss 1967.
[519] Vgl. Anhang.

Transkription der Experteninterviews wurde mit der Software f4transkript[520] durchgeführt, damit alle Hinweise und Anpassungen nachvollziehbar dokumentiert und keine Aspekte übersehen werden.

Auswertung der Experteninterviews mittels qualitativer Inhaltsanalyse

Im Anschluss an die Interviewdurchführung und deren Transkription erfolgte die Auswertung. Qualitative Daten in textueller Form können auf verschiedene Weise analysiert werden. Die Inhaltsanalyse verfolgt das Ziel (fixierte) Kommunikation zu analysieren, dabei systematisch, regelgeleitet und theoriegeleitet vorzugehen, um damit Implikationen auf gewisse Aspekte der Kommunikation zu ziehen.[521] Die qualitative Inhaltsanalyse entstand aus der Kritik an der quantitativen Inhaltsanalyse mit ihrem relativ begrenztem Spektrum, der Vernachlässigung der Kontextabhängigkeit und dem ausschließlichen Wörter zählen, da damit einzig deskriptive Resultate mit geringer Reichweite möglich sind.[522] Hingegen versucht die qualitative Inhaltsanalyse die Strukturen von Texten zu erkennen und zu verstehen, das wiederrum das Ziel hat, deskriptive und interpretative Ergebnisse herzuleiten. Laut MAYRING lässt sich die von ihm weiterentwickelte Methode in die drei Techniken der Interpretationsformen *Zusammenfassung*, *Explikation* und *Strukturierung* einteilen. In Abhängigkeit von der zu beantwortenden Forschungsfrage ist die Verwendung einer oder der aufeinander aufbauenden Techniken denkbar. MAYRING definiert die drei Interpretationstechniken wie folgt:

- „Zusammenfassung: Ziel der Analyse ist es, das Material so zu reduzieren, dass die wesentlichen Inhalte erhalten bleiben, durch Abstraktion einen überschaubaren Corpus zu schaffen, der immer noch Abbild des Grundmaterials ist.“
- Explikation: Ziel der Analyse ist es, zu einzelnen fraglichen Textteilen (Begriffen, Sätzen, ...) zusätzliches Material heranzutragen, das das Verständnis erweitert, das die Textstelle erläutert, erklärt, ausdeutet.
- Strukturierung: Ziel der Analyse ist es, bestimmte Aspekte aus dem Material herauszufiltern, unter vorher festgelegten Ordnungskriterien einen Querschnitt durch das Material zu legen oder das Material aufgrund bestimmter Kriterien einzuschätzen.“[523]

Aufbauend auf diesen Darlegungen wird die Technik *Zusammenfassung* für diese Arbeit ausgewählt, um die Forschungsfragen zu beantworten. Zuerst wurden in den Interviews die Interviewfragen und deren Antworten gekennzeichnet. Danach wurden herausragende Antworten und Diskussionen beim vermittelnden Interviewbestandteil markiert. Anschließend erfolgte eine Übernahme in eine zentrale Übersicht und in die Zusammenfassung. Damit wurde zum einen sichergestellt, dass keine Hinweise zu weiteren praktischen Kategorien der interviewten Experten bei der kritischen Reflexion des Autors zwischen den Interviews unbeachtet blieben. Des Weiteren enthält das theoretisch entwickelte Referenzmodell etablierte Kategorien, die zum Teil von mehreren Autoren validiert wurden, weshalb sich die anderen beiden Techniken nicht für diese Arbeit eignen. Ebenso beziehen sich die Interviewfragen auf die entwickelten

[520] Software siehe Webseite: www.audiotranskription.de.
[521] Vgl. Mayring 2015, S. 12 f.
[522] Vgl. Diekmann 1995, S. 578 ff.
[523] Mayring 2015, S. 67.

Funktionen des Referenzmodells, womit keine weiteren Klassifikations-, Bedeutungs- oder Strukturanalysen notwendig sind.

Vertiefende Experteninterviews zum Dienstleister-Gefahrenpotential

Bei den elf Experteninterviews zum Prototypen hat sich herausgestellt, dass die Komplexität der Dienstleisterkategorisierung (Funktion 4)[524] mit den IT-Sourcing Vertretern weiter untersucht werden sollte, um diese Funktion noch detaillierter zu entwickeln und zu validieren. Aus diesem Grund nehmen diese vertiefenden Experteninterviews eine besondere Rolle ein. Ein weiteres Ziel dieser Experteninterviews war die Diskussion zu der möglichen Gewichtung der Einflussfaktoren in der *Dienstleister-Gefahrenpotential-Bestimmung* und der Bedarf aus den Experteninterviews reale Dienstleister nach dem Modell zu kategorisieren. Damit sollte die Validität der theoretisch entwickelten Funktion des Modells geprüft und auf Anwendbarkeit validiert werden. Deshalb wurden zwei weitere vertiefende Experteninterviews zur Dienstleisterkategorisierung geplant, vorbereitet und durchgeführt. Bei einem Experteninterview wurde im Vorfeld der Wunsch geäußert, einen weiteren Experten hinzuzunehmen, damit bei der exemplarischen Bewertung der Dienstleister die subjektive Meinung eliminiert werden konnte. Insgesamt wurden mit den folgenden drei Experten die vertiefenden Interviews durchgeführt.

- 1. vertiefendes Paar-Experteninterview: Zwei IT-Sourcing Mitarbeiter (Dauer: 92 Minuten)
- 2. vertiefendes Experteninterview: IT-Sourcing Abteilungsleiter (Dauer: 50 Minuten)

Bei dem ersten vertiefenden Paar-Experteninterview befindet sich ein Paar auf der Seite der Befragten.[525] Insgesamt wurden fünf reale Dienstleister nach einem *Dienstleister-Gefahrenpotential* kategorisiert und das Ergebnis mit der eigenen Einschätzung verglichen. Diese Untersuchung kann damit auch zu der im nächsten Abschnitt beschriebenen Pilotierung zugeordnet werden, da für existierende Dienstleister das Gefahrenpotential bestimmt und diese Modell-Funktion pilotiert wurde. Die Details zu diesen Interviews sind in das Kapitel 5 eingearbeitet.

Den gewonnenen Erkenntnissen eines Prototyps mangelt es jedoch an der Einbettung in ein Aktionssystem.[526] Für ÖSTERLE et al. wird die Einbettung mit Hilfe der Weiterentwicklung und Pilotierung eines Artefaktes vorgenommen.[527] Die Pilotierung im Rahmen dieser Arbeit erfolgte in den oben beschriebenen vertiefenden Experteninterviews, den anschließenden Einzelinterviews und dem Gruppeninterview (Abbildung 22), die im Folgenden Abschnitt beschrieben werden.

3.3.4 Pilotierung mit Einzelinterviews und Gruppeninterview

Um das Wissensschutz-Referenzmodell in einem Piloten zu erproben, wurden über den betrieblichen Ansprechpartner potenziell zu prüfende IT-Projekte angefragt, die nach der Einschätzung des Managements schützenswertes Wissen beinhalten und auf den Wissensschutz hin untersucht werden sollten. Das Management benannte daraufhin drei IT-Projekte. Mit den drei

[524] Vgl. Abschnitt 5.3.1.
[525] Vgl. Lamnek & Krell 2016, S. 338, Helfferich 2005.
[526] Vgl. Frank 2006, S. 42.
[527] Vgl. Österle et al. 2010, S. 5.

Projektmanagern wurde in Einzelinterviews der erweiterte Projektsteckbrief im Hinblick auf den Wissensschutz begleitend ausgefüllt. Im Vorfeld skizzierte der Autor jeweils die Zielsetzung der Pilotierung sowie das bereits beschrittene Forschungsvorgehen zur Sicherung der Transparenz.

Den Projektmanagern wurde jeweils der Mehrwert für ihr Projekt aufgezeigt, wenn die Pilotierung mit ihrem Projektteam durchgeführt wird. Der Mehrwert für die Projekte stellt sich wie folgt dar:

- Der Projektmanager erkennt, wie die Wissensgebiete (Fach- / Technologiewissen) von den Projektverantwortlichen bewertet werden und schützenswertes / wertvolles Wissen wird identifiziert.
- Für die zukünftige Ressourcenplanung von externen und internen Mitarbeitern in Bezug auf den Wissensschutz kann aufgrund fundierter Bewertungen eine Risikoeinschätzung durchgeführt werden.
- Die aktuelle Ressourcenplanung wird in Bezug auf Wissensrisiken überprüft, um den ungewollten Wissenstransfer zu externen Dienstleistern zu reduzieren.

Beim Ausfüllen des erweiterten Projektsteckbriefs wurden zuerst alle Projektansprechpartner notiert. Dazu gehören der Vertriebsbereich sowie die fachlichen und technischen Ansprechpartner. Den Interviewten stand ebenso ein ausgefüllter Beispiel-Projektsteckbrief zur Verfügung. Zu jeder Kategorie wurde die Beschreibung expliziert.

IT-Projekt-Auswahlprozess

Zum Auswahlprozess für das Gruppeninterview-Projekt wurden die Projektsteckbriefe sowie die persönliche Einstellung des Projektmanagers zum Wissensschutz dokumentiert. Die Projekte werden nachfolgend als *Projekt alpha, beta* oder *gamma* bezeichnet, da hier der Bezug zu den realen Projekten aus Compliance-Gründen nicht hergestellt werden kann.

Tabelle 15: Auswahl eines IT-Projektes für das Gruppeninterview[528]

Kategorien	IT-Projekt alpha	IT-Projekt beta	IT-Projekt gamma
Projekttyp	Weiterentwicklungsprojekt	Neuentwicklungsprojekt	Neuentwicklungsprojekt
Innovationsgrad	hoch	sehr hoch	hoch
Marktattraktivität	sehr hoch	sehr hoch	hoch
strategische Relevanz	hoch	niedrig	hoch
Projekt unterstützt die Wettbewerbsfähigkeit	mittel	mittel	hoch
eingesetzte externe Dienstleister mit Projektrolle	vier verschiedene externe Dienstleister	zwei verschiedene externe Dienstleister, 1 Lieferant für 3D Modelle	ein externer Dienstleister
Projektsituation (Umfeldanalyse für Risikobewertung)	beim Softwareentwicklungsprozess muss eine Norm eingehalten und muss unabhängig begutachtet werden.	Projekterfolg vom externen Dienstleisterbeitrag abhängig, hohe Anforderungen an Qualität	abzubildende Prozesse sind zum Teil neu. Arbeitsabläufe ändern sich und Ergebnisse werden anders erreicht wegen Ablösung von Papierprozessen.
Fachwissen im Projekt (Geschäftsprozesswissen in der Branche)	ein Fachwissensgebiet	zwei Fachwissensgebiete	vier Fachwissensgebiete
Technologiewissen im Projekt (Technologiewissen der IT-Beratung)	vier Technologiewissensgebiete	ein Technologiewissensgebiet	zwei Technologiewissensgebiete
erbrachte Leistung durch externe Dienstleister	ca. 1450 Personentage / Jahr durch externe Dienstleister	60% der Aufwände werden durch externe Dienstleister erbracht	nicht bekannt / noch zu ermitteln
Zugänglichkeit des Projektmanagers für den Wissensschutz	hoch	hoch	gering

Das *Projekt alpha (α)* hat ein Projektbudget von ca. 1.5 Millionen Euro und wurde ausgewählt, weil vier verschiedene Dienstleister mit einem hohen externen Berateranteil involviert sind, eine sehr hohe Marktattraktivität vorliegt und eine gewisse Komplexität der Wissensgebiete vorhanden ist. Zwei der drei Projektmanager zeigten sich offen gegenüber dem Wissensschutz beim Ausfüllen des erweiterten Projektsteckbriefes.

Vorbereitung und Durchführung

Zur Vorbereitung des Gruppeninterviews bewertete der Kundenmanager sowie die fachlichen und technischen Ansprechpartner die identifizierten Fach- und Technologiewissensgebiete in Einzelinterviews. Insgesamt wurden fünf Schlüsselpersonen des *Projektes α* zu der Bewertung

[528] Eigene Darstellung.

der Wissenskategorisierung begleitend inquiriert. Jedes der Einzelinterviews dauerte 45 Minuten, um die Wissenskategorisierung (Funktion 3)[529] auszufüllen und die Historie vom Vorhaben zu skizzieren. Die Bewertungen wurden aufbereitet und in eine erstellte Präsentation eingearbeitet. Zu dem Gruppeninterview waren die Interviewten und alle weiteren erfassten Projektansprechpartner sowie das IT-Sourcing Management eingeladen. Die Agenda der Präsentation ist in Tabelle 16 dargestellt.

Tabelle 16: Gruppeninterviewleitfaden - Überblick [530]

Phase / Agendapunkt	Detailbeschreibung
1. Gesprächsbeginn	• Vorstellung • Ziel des Forschungsprojekts • Interviewaufzeichnung beginnt • Dokumentation der Vertraulichkeit und Anonymität
2. Relevanz des Wissensschutzes	• Forschungsgegenstand, -fragen • Modellentwicklung • Experteninterviews • Referenzmodell
3. Auswertung der Einzelinterviews	• Projektkategorisierung • Einzelsichten auf das Fach-/Technologiewissen für Projekt α • Gesamtsicht auf die Risikobewertung

4. Fragen und Diskussion zu den Ergebnissen	• Fragen zu den präsentierten Ergebnissen
	• Einstiegsfragen zur Diskussion:
	  ○ Wie bewerten sie das Ergebnis im Vergleich zu ihrer Erwartungshaltung?
	  ○ Wo sehen sie die Grenzen vom Wissen-Teilen und Wissen-Zurückhalten am Beispiel-Projekt α?
	  ○ Wird für Sie sichtbar, welche externen Dienstleister das Potential haben, die Wettbewerbsfähigkeit der IT-Beratung und/oder die unserer Auftraggeber zu gefährden?
	  ○ Welche besonderen Verantwortlichkeiten sehen Sie, damit das Wissensschutz-Modell funktioniert?

5. Gesprächsende	• Interesse an den Forschungsergebnissen • Dank und Verabschiedung

Das Gruppeninterview dauerte 95 Minuten (geplant 90 Minuten). Dieses unterteilt sich in eine Präsentation der Erkenntnisse (20 Minuten) und einer anschließenden Fragen- und Diskussionsrunde (75 Minuten). Die Rückmeldungen aus den Einzelinterviews und die Analyseergebnisse wurden bei den Fragen und in der Diskussion thematisiert.

[529] Vgl. Abschnitt 5.2.3.
[530] Eigene Darstellung.

4 Stand der Wissensschutzforschung

Nachdem im Kapitel 2 und 3 die Basis zum Wissensbegriff, der IT-Beratung und der Referenzmodellierung gelegt wurden, wird in diesem Kapitel der Forschungsstand zum Wissensschutz, seine strategische Relevanz und die Literatur zur Dienstleisterauswahl dokumentiert und diskutiert. Die Struktur dieses Kapitels sowie das *Literature Review* orientiert sich an den zwei für das Modell relevanten (Out-)Sourcing-Phasen von MONCZKA et al.[531] und NASSIMBENI et al.[532]. Diese sind die Strategie und Planung sowie die Dienstleisterauswahl. Der folgende Forschungsstand orientiert sich wesentlich an diesen Phasen, bis auf die Themen die mehreren Phasen zugeordnet werden können, wie dem Risikomanagement und dem (Out-) Sourcing (Abschnitt 4.2.4).

Zunächst konzentriert sich das erste Unterkapitel 4.1 auf einen Überblick zur Wissensschutzforschung mit Informationstechnologiebezug und der Identifizierung der IT-Sourcing-Phasen. Im Unterkapitel 4.2 wird die relevante strategische Wissensschutzliteratur zu den Wissensschutzstrategien, den Einflussfaktoren auf die Wissensschutzziele, die effektivsten Wissensschutzmechanismen und die Bestimmung der Unternehmensgrenze erarbeitet, um den Wissensschutz sicherzustellen. Damit wird die erste Forschungsfrage[533] fokussiert. Dieses Unterkapitel schließt mit der Risikomanagementbetrachtung im Zusammenhang mit (Out-)Souring ab und es folgen Hinweise für die Beantwortung der dritten Forschungsfrage[534].

Das dritte Unterkapitel 4.3 widmet sich hauptsächlich der zweiten Forschungsfrage[535]. Der erste Abschnitt geht auf das Vertrauen und das opportunistische Verhalten vom externen Dienstleister ein. Die Behandlung von Wissens-, Markt- und Wettbewerbsüberlappung folgen. Abschließend wird die *absorptive Kapazität* untersucht.

4.1 IT-Sourcing als Forschungsgegenstand

Zuerst sind die relevanten Wissensschutzveröffentlichungen mit Informationstechnologiebezug absatzweise beschrieben und resümiert, dass diese Erkenntnisse einen geringen Beitrag für das Referenzmodell liefern. Durch den Input der Praxisvertreter und weitere Literaturanalysen konnten bestehende IT-Sourcing Modelle identifiziert werden, die Basis für die theoretische Konzeptentwicklung (Prototyp) sind. Die relevante Forschungsliteratur wird deshalb nach den IT-Sourcing-Phasen Strategie und Planung sowie Dienstleisterauswahl gegliedert.

Artikel zum Wissensschutz mit einem IT- / IKT-Fokus

Im Folgenden sind ausgewählte Forschungsartikel zum Wissensschutz mit einem IT-Fokus identifiziert und kategorisiert. Die Forschungsinhalte und die Forschungsschwerpunkte zu jedem Artikel werden resümiert und im Vergleich zu der vorliegenden Arbeit abgegrenzt. Das

[531] Monczka et al. 2005.
[532] Nassimbeni et al. 2012.
[533] Vgl. Unterkapitel 1.2.
[534] Vgl. Unterkapitel 1.2.
[535] Vgl. Unterkapitel 1.2.

Themengebiet des Wissensschutzes in Verbindung mit der Informationstechnologie bietet Potential für weitere Forschung, da bei den Recherchen wenige Publikationen mit dieser Ausrichtung identifiziert werden konnten. Von den bei EBSCO identifizierten 26 Veröffentlichungen, bei denen Informationstechnologie zum großen Teil nur erwähnt und nicht untersucht wurde, weisen die folgenden sieben Arbeiten einen konkreten IT-Bezug auf.

BOGERS[536] betrachtet das *Knowledge Paradox* bei der F&E in einer offenen Innovationspartnerschaft. Er erörtert zwei konkrete Strategien zur Bewältigung des Spannungsfeldes vom *Wissen-Teilen und -Zurückhalten*. Er wertet dazu acht Fallstudien aus. Sieben von diesen Fallstudien untersuchen Unternehmen, die in der IKT-Branche agieren. Er spezifiziert die Rolle und die Auswirkung des Wissensschutzmechanismus Lizenzierung. Die informalen Wissensschutzmechanismen sind bei BOGERS nicht relevant.

BOLISANI et al.[537] klassifiziert die Arten von Wissensschutzmechanismen und untersucht Ähnlichkeiten und Unterschiede im Wissensschutz zwischen KIBS[538], die in verschiedenen Sektoren tätig sind, diverse Größen haben und unterschiedliche WM-Strategien verfolgen. Dazu werden in einer Umfrage 471 wissensintensive Dienstleistungsunternehmen inquiriert. Eine von den drei fokussierten Branchen ist die IT-Dienstleistung. Der Aspekt fehlt, wie die Wissensschutzstrategie umgesetzt werden kann.

ELCHE-HOTELANO[539] postuliert, das interne Wissensressourcen (zum Beispiel Mitarbeiter), der Erwerb von externen Technologien, die interne Konstruktion und strategische Schutz einen positiven Einfluss auf die Innovations-Performance haben. Seine empirische Analyse basiert auf Untersuchungen in spanischen Dienstleistungsunternehmen. Er bezieht seine gefundenen Ergebnisse auf andere wissenschaftliche Arbeiten aus der IKT-Branche und konkludiert, dass die Technologieanpassung einen evident positiven Einfluss auf die Innovationsentwicklung hat. Von ihm werden keine Wissensschutzmechanismen und Wissensschutzstrategien elaboriert.

HURMELINNA-LAUKKANNEN[540] verifiziert, dass ein breites Spektrum an Wissensschutzmechanismen eingesetzt werden kann und dass die strategische Anwendung den Wissensaustausch und die Innovations-Performance verbessert. Wissensschutz Handlungsempfehlungen für die Akteure werden nicht untersucht. An der empirischen Analyse der 242 finnischen Unternehmen beteiligten sich 18,6 Prozent der Unternehmen aus der IKT-Branche.

NORMAN[541] referiert, dass Strukturen und Prozesse genutzt werden können, damit der (strategische) Partner das kritische Wissen und die kritischen Ressourcen des Unternehmens nicht bemerkt, versteht, aneignet oder imitiert. Sie kategorisiert die Wissensschutzmechanismen und

---

[536] Vgl. Bogers 2011, S. 93.
[537] Vgl. Bolisani et al. 2013, S. 192.
[538] „wissensintensive unternehmensorientierte Dienstleistungen“, Übersetzung von der englischen Bezeichnung: „knowledge intensive business services (KIBS)“ Amara et al. 2008.
[539] Vgl. Elche-Hotelano 2011, S. 220.
[540] Vgl. Hurmelinna-Laukkannen 2011, S. 303.
[541] Vgl. Norman 2001, S. 51.

lässt die einzelnen Mechanismen in qualitativen und quantitativen Befragungen nach ihrer Effektivität bewerten. Die Erhebung verifiziert, dass die Effektivität von Wissensschutzmechanismen evident von der Branche abhängig ist. Hervorzuheben ist, dass sie dem Management und den Mitarbeitern eines Unternehmens Kompetenzen im Wissensschutz zuordnet. Die Untersuchungen basieren auf der Computer-, Elektronik-, Pharmazie- und Telekommunikationsbranche.

OLANDER et al.[542] untersuchen und validieren empirisch fünf Personalmanagement Wissensschutzmechanismen in einer Fallstudie. Diese sind die Rekrutierung, Aus- und Weiterbildung zur Geheimhaltung, Mitarbeiterbindung, Erfassen und Verbreiten von Wissen im Unternehmen und ihre Kontrolle. Untersucht wurden 15 klein- und mittelständische finnische Unternehmen aus den Branchen: Ingenieurswissenschaften, Informationstechnologie und Dienstleistungserbringung.

SUBRAMANYAM & SUSARLA[543] betrachten die Vertragsgestaltung zwischen Auftraggeber und Auftragnehmer beim IT-Outsourcing in Bezug auf den Wissensaustausch und Wissensschutz. Sie fokussieren die Beziehung zwischen dem Auftraggeber und dem Auftragnehmer in Bezug auf die Wissensasymmetrien, die Wissensaustausch-Mechanismen und die eingeführten Anreize zum Austausch. Die Vertragsgestaltung und somit die Anwendung der formalen Wissensschutzmechanismen wird bei der vorliegenden Arbeit vorausgesetzt und wird deshalb nicht recherchiert.

Als Ergebnis der initialen Literaturanalyse ist zu postulieren, dass wie bereits im *Literature Review* von THALMANN & MANHART[544] festgestellt, gibt es einzelne Ansätze in den Artikeln zur IT-Branche. Jedoch liegen keine Betrachtungen und Hinweise vor, die den Wissensschutz des wertvollen organisationalen impliziten Wissens[545] einer IT-Beratung untersuchen. Ebenso wenig wird die Rolle des IT-Artefakts[546] und die Entwicklung von Informationssystemen[547] exploriert.[548]

IT-Sourcing-Phasen

Der Wissensschutz und seine verschiedenen Termini[549] sind interdisziplinär und tangieren verschiedene Forschungsrichtungen und -theorien. Im *Literature Review* identifizierte der Verfasser das bestehende Modell von MONCZKA et al. als Phasenmodell für das onshore/offshore von

[542] Vgl. Olander et al. 2011, S. 593.
[543] Vgl. Subramanyam & Susarla 2007, S. 1.
[544] Thalmann & Manhart 2015.
[545] Vgl. Manhart & Thalmann 2015, S. 195.
[546] Vgl. Manhart & Thalmann 2015, S. 199.
[547] Vgl. Manhart & Thalmann 2015, S. 201.
[548] Vgl. Unterkapitel 1.2.
[549] Vgl. Tabelle 4.

IT-Service Outsourcing.[550] NASSIMBENI et al. erweiterte das etablierte Modell um die Hauptrisiken beim Outsourcing in den drei Phasen.[551] Die Betrachtung des Wissensschutzes fehlt jedoch in diesen Phasen. Das entwickelte Wissensschutz-Modell setzt auf diesem existierenden und erweiterten Modell zum Outsourcing auf.[552] Die drei Phasen von dem etablierten Modell sind (Tabelle 17):

Tabelle 17: Etablierte Phasen beim IT-Sourcing[553]

Phase	Nach MONCZKA et al.	Nach NASSIMBENI et al.
1	Strategy and Planning	Strategic Planning
2	Contracting and Relationship Development	Supplier Selection and Contracting
3	Implementation	Implementation and Monitoring

Hinzuweisen ist, dass die Phasenbestandteile *Contracting* und *Implementation and Monitoring* nicht Fokus dieser Arbeit sind. Aufbauend auf den Modellen von MONCZKA et al.[554] und NASSIMBENI et al.[555] zum (Out-)Sourcing wird die aktuelle Wissensschutzliteratur nach den ersten beiden Modellphasen in *Strategie und Planung* sowie *Dienstleisterauswahl* unterteilt.

Einige Forschungsarbeiten befassen sich mit der theoretischen *Strategie und Planung*. Jedoch fehlen Untersuchungen zu den relevanten Schritten oder Funktionen, um eine konkrete Strategie insbesondere für ein IT-Projekt zu entwickeln. Die Arbeiten zum strategischen Wissensschutz und damit zur Lösung des *Boundary Paradox* tangieren zum Beispiel die Themen Wissensschutzmethoden, (effektive) -mechanismen, Risikoeinschätzung und Abhängigkeit zu den Unternehmenszielen. Im Unterkapitel 4.2 wird der Forschungsstand für die *Strategie und Planung* im Hinblick auf die zu entwickelnden Modell-Funktionen erörtert.

Für die Sourcing-Phase der Dienstleisterauswahl gibt die vorliegende Literatur zur Partnerauswahl Hinweise für die IT-Projekte. Zudem stellen MANHART & THALMANN heraus, dass der Wissensschutz bei der Partnerauswahl bisher weitgehend vernachlässigt wurde.[556] Um die existierenden Erkenntnisse zu nutzen, recherchierte der Autor in anderen angrenzenden Forschungsrichtungen wie dem *Intellectual Property Protection*, Risikomanagement, Allianzen, F&E-Partnerschaften und Outsourcing. Die identifizierten Inhalte sind in der folgenden Tabelle 18 dargestellt:

[550] Vgl. Monczka et al. 2005.
[551] Vgl. Nassimbeni et al. 2012.
[552] Anmerkungen vom Autor: In der existierenden Forschungsliteratur zum Wissensschutz konnte zum recherchierten Zeitpunkt kein Modell oder Framework identifiziert werden, auf denen das Wissensschutz-Referenzmodell aufbauen konnte, deshalb wurde unter anderem in der angrenzenden Forschungsrichtung vom Outsourcing recherchiert.
[553] Eigene Darstellung.
[554] Monczka et al. 2005.
[555] Nassimbeni et al. 2012.
[556] Vgl. Manhart & Thalmann 2015, S. 198.

Tabelle 18: Wissensschutz tangiert die Literatur zur Dienstleisterauswahl[557]

Inhaltliche Themen	Autor(en) / Studien
Partnerauswahl	Li et al. 2008
Wissens- /Markt- / Wettbewerbsüberlappung	Bogers 2011, Jiang 2002, Jordan & Lowe 2004, Kale et al. 2000, Li et al. 2008, Maier 2007, Norman 2001, 2002, 2004
Vertrauen	de Faria & Sofka 2010, Ghodeswar & Vaidyanathan 2008, Hoecht & Trott 2005, Lee et al. 2007, Li et al. 2008, Monteiro et al. 2011, Norman 2002, 2004, Sofka & Shehu 2009, Trkman & Desouza 2012
Opportunismus	Kale et al. 2000, Maier 2007, Majchrzak & Jarvenpaa 2010, Walter et al. 2010
Absorptive Kapazität	de Faria & Sofka 2010, Drechsler & Natter 2012, Li et al. 2008, Liebeskind 1997, Manhart & Thalmann 2015, Norman 2002, 2004, Olander et al. 2010, Sofka & Shehu 2009, Schultze & Leidner 2002

Wie zu erkennen ist, fehlen Untersuchungen zu der Auswahl von Partnern beziehungsweise Dienstleistern. LI et al. weisen in ihren Untersuchungslimitationen explizit daraufhin, dass ihre Erkenntnisse nicht auf das Projektgeschäft und die damit notwendigen Managemententscheidungen transferiert werden können. Hier wird weiterer Forschungsbedarf gesehen.[558] Der Wissensschutz-Forschungsstand zur Dienstleisterauswahl und die für die Arbeit relevanten Erkenntnisse zu Wissens-, Markt-, Wettbewerbsüberlappung, Opportunismus, Vertrauen sowie die *absorptive Kapazität* werden im Unterkapitel 4.3 erörtert.

Die weiteren identifizierten tangierenden Forschungsrichtungen zum Wissensschutz haben eine untergeordnete Relevanz für die Arbeit und dienten dem entwickelten Referenzmodell als Informationsbasis. Diese sind:

- Intellectual Property
- (Wissens-)Sicherheit
- IT-Sicherheit
- F&E
- Innovationsmanagement
- Multinationale Unternehmen
- (Strategische) Allianz
- Netzwerk
- Koopetition

Weitere *Literature Reviews* zum Wissensschutz wurden im Bearbeitungsprozess der Arbeit von AHMAD et al.[559] und THALMANN & MANHART[560] veröffentlicht. Diese Veröffentlichungen liefern einen wertvollen Beitrag für diese Arbeit und bestätigen zudem nachweislich die identifizierte Forschungslücke.[561]

[557] Eigene Darstellung.
[558] Vgl. Li et al. 2008, S. 329.
[559] Ahmad et al. 2014.
[560] Thalmann & Manhart 2015.
[561] Vgl. Unterkapitel 1.2.

4.2 Sourcing-Phase 1: Strategie und Planung

In diesem Unterkapitel wird der Forschungsstand im strategischen Wissensschutz erörtert. Weiterhin werden in den Abschnitten 4.2.1 und 4.2.2 die Wissensschutzstrategien sowie die darauf aufbauenden Erkenntnisse der Einflussfaktoren auf die Wissensschutzziele und die effektivsten Wissensschutzmechanismen nach Branchen beschrieben. Der Abschnitt 4.2.3 elaboriert den Stand der bisherigen Forschung zur Identifizierung der Unternehmensgrenze für den Wissensschutz. Im letzten Abschnitt dieses Unterkapitels wird auf die Risikomanagementforschung im Zusammenhang mit dem (Out-)Sourcing eingegangen.

4.2.1 Wissensschutzstrategien, -methoden und -mechanismen

Um das wertvolle organisationale Wissen vor ungewollter Wissensdiffusion zu schützen, müssen Wissensschutzstrategien[562], -methoden und -mechanismen angewendet werden. In der Literatur sind zahlreiche Übersichten dazu erstellt und veröffentlicht. Die Begriffe Wissensschutzstrategie, -methode und -mechanismen werden zum Teil analog in der Forschungsliteratur verwendet. Die vorliegende Arbeit fokussiert speziell die Literatur zur strategischen Planung und der methodischen Unterstützung für eine IT-Beratung. Nach LEE et al. können die Wissensschutzmechanismen dazu beitragen, dass das *relationale Kapital*[563] einer IT-Beratung aufgebaut und der Wissensaneignung von Dienstleistern vorgebeugt wird.[564]

Wissensschutzstrategie

Nach DE FARIA & SOFKA lässt sich die Forschung in zwei Wissensschutzstrategie-Paradigmen unterteilen.[565] Das eine Paradigma basiert nach ENCAOUA et al.[566] und LAURSEN & SALTER[567] auf den gesetzlichen Schutzformen[568], ebenso bekannt als der formale Wissensschutz nach HARABI[569], wie zum Beispiel Patente oder Urheberschutz. Das andere Paradigma beruht auf organisatorischen Prozessen der Unternehmen um den ungewollten Wissensabfluss zu verhindern und seine negativen Konsequenzen zu begrenzen.[570] Dieses Paradigma wird von HARABI als strategisch, von ENCAOUA et al. als *Market-based* und von LAURSEN & SALTER als Pionier-Methode bezeichnet.[571]

Wissensschutzmethoden

Aufbauend auf den zwei Wissensschutzstrategien wird die Unterteilung der Schutzmethoden aufgeführt, die sich neben den organisatorischen Prozessen und gesetzlichen Schutzformen

---

[562] Vgl. Wissensschutzstrategie Definition im Abschnitt 2.1.3.
[563] Vgl. Abschnitt 2.3.2.
[564] Vgl. Lee et al. 2007, S. 67.
[565] Vgl. de Faria & Sofka 2010, S. 957.
[566] Encaoua et al. 2006.
[567] Laursen & Salter 2005.
[568] In der englischen Literatur als „legal knowledge protection strategies“ bezeichnet.
[569] Harabi 1995.
[570] Vgl. Sofka & Shehu 2009, S. 3.
[571] Vgl. de Faria & Sofka 2010, S. 957.

weiter detaillieren. Einen Überblick zu den Schutzmethoden liefern BOLISANI et al. und PÄÄLLYSAHO & KUUSISTO. Wie bereits im Abschnitt 2.2.3 beschrieben, fokussieren BOLISANI et al. in ihren Untersuchungen den Wissensschutz in KIBS und haben deshalb für diese Arbeit eine hohe Relevanz. Ihre Erkenntnisse sind in der Abbildung 28 illustriert und die relevanten Wissensschutzmethoden sind für die Arbeit hervorgehoben.

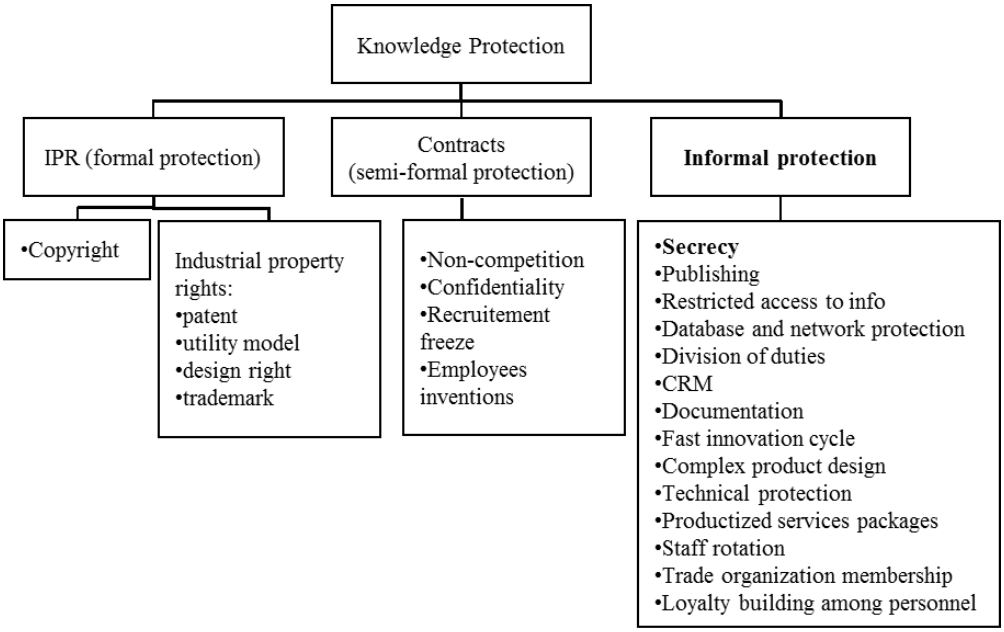

Abbildung 28: Wissensschutzmethoden[572]

Die vorliegende Arbeit konzentriert sich auf die *Informal Protection* Methoden und damit nicht auf die *Formal / Semi-formal Protection* Methoden. Die Anwendung der formellen Schutzmethoden ist Prämisse bei Verwendung des Wissensschutz-Referenzmodelles. Gesondert darauf hingewiesen werden soll, dass die ISE nur einen dezidierten Ausschnitt der Arbeits- und Geschäftsprozesse einer IT-Beratung darstellen. Um den strategischen Wissensschutz in den IT-Projekten zu etablieren, wurde der informale Wissensschutzmechanismus der Geheimhaltung[573] als einer der effektivsten Schutzmechanismen für das Referenzmodell ausgewählt.

Wissensschutzmechanismen

Nach OLANDER et al. wird die Steuerung der Wissensflüsse oft in formelle (Verträge, ipr, Geschäftsgeheimnisse) und informelle (Personalmanagement, Vorsprung, Geheimhaltung) Schutzmechanismen vorgenommen.[574] Diese Einteilung und Sichtweise zu den Wissensschutzmechanismen überlappt sich mit der oben genannten Wissensschutz-Methodendifferenzierung.

Wie bereits angeführt können nach NORMAN Strukturen und Prozesse genutzt werden, damit der Dienstleister das kritische Wissen und die kritischen Ressourcen von der IT-Beratung nicht bemerkt, versteht, aneignet oder imitiert.[575] NORMAN unterteilt die Wissensschutzmechanismen

[572] Bolisani et al. 2013, S. 195, Päällysaho & Kuusisto 2008a, S. 7.
[573] In der englischen Forschungsliteratur wird die Geheimhaltung als "secrecy" oder „isolating mechanism" bezeichnet.
[574] Vgl. Olander et al. 2011, S. 594.
[575] Vgl. Norman 2001, S. 51.

in *Human Resources, Legal Structure* und *Processes*[576] und lässt die Mechanismen in ausgewählten Unternehmen aus mehreren Branchen nach ihrer Effektivität bewerten. In der Tabelle 19 sind die einzelnen Mechanismen strukturiert dargestellt und die für die Arbeit relevanten hervorgehoben, weil diese dem informalen Wissensschutz zuzuordnen sind.

Tabelle 19: Klassifizierungsrahmen von Wissensschutzmechanismen[577]

Areas	Categories	Knowledge Protection Mechanisms
Human Resources	**Top Management Support**	Actions by top management • **Identify core capabilities** • **Stress protection of core capabilities** • **Provide resource for protection core capabilities**
	Alliance Management	Actions by focal firm managers in alliance • **Stress protection of core capabilities** • Appoint a focal firm information manager
	Human Resource Management	Human resource management in focal firm • **Educate personnel about proprietary data** • **Establish** reward/**evaluation program for protection of core capabilities** • **Consult designated individuals when circumstances are unclear** • Report contacts with partner employees
Legal Structure	Patents	• Obtain patent to prevent imitation
	Contractual Mechanisms	• Specify proprietary information • Specify what information and capabilities can be shared • Specify what information and capabilities cannot be shared • Provide consequences if a partner accesses off-limits information • Provide consequences if a partner uses proprietary information in the wrong way • Sign nondisclosure agreements (NDAs) • Bar employment to partner employees • Ensure that information or technology shared with partner is covered by patents
Processes	**Information Flows**	• Limit to one person (gatekeeper) • **Limit to a few people (communication stars)** • **Exclude certain information deemed off-limits**
	Partner Access	• **Perform certain alliance activities separately from partner** • **Limit partner's access to facilities** • **Limit partner's access to non-alliance personnel**

Das entwickelte Modell im folgenden Hauptkapitel adressiert damit die Mechanismen aus der Prozesssicht mit der Überwachung der Informationsflüsse und Partnereinsicht bzw. dem Dienstleisterzugriff auf schützenswerte Wissensgebiete wie auch die *Human Ressource* Sicht mit Managementunterstützung, Dienstleistermanagement und Ressourcenmanagement. Die Beschränkung vom Dienstleisterzugriff fließt in das Modell mit der Dienstleisterauswahl ein,

[576] Vgl. Norman 2001, S. 52.
[577] Norman 2001, S. 52.

der für die Forschungsarbeit eine hohe Relevanz besitzt. LI et al. argumentieren, dass die Partnerauswahl (in Bezug auf diese Arbeit: Dienstleisterauswahl) ein weiterer alternativer Wissensschutzmechanismus bei Kooperationen ist, um die Bedrohung vom Wissensverlust zu kontrollieren.[578] Der Abschnitt 4.2.4 erörtert diesen Mechanismus auf der Grundlage vom *relationalen Kapital* Vertrauen und Opportunismus, der Wissens-, Markt-, Wettbewerbsüberlappung und von der *absorptiven Kapazität*.

Die oben aufgeführten *Human Ressources* Wissensschutzmechanismen präzisieren OLANDER et al. Sie postulieren, dass zu den bedeutsamsten Personalmanagement-Kategorien in Bezug auf den Wissensschutz die folgenden Bereiche gehören:

- das Recruiting und damit die Auswahl der richtigen Mitarbeiter,
- die Weiterbildung und Schulung von Mitarbeitern, insbesondere die Verantwortung im Zusammenhang mit Wissensschutz und Organisationsgeheimnissen,
- das Halten von Mitarbeitern im Unternehmen, in dem das Commitment zum Unternehmen durch verschiedene Mechanismen gelebt wird, diese Mechanismen können Weiterbildungsmöglichkeiten, Karrieremöglichkeiten und Aktionärsvereinbarungen sein,
- das Erfassen und Verbreiten von Wissen durch die Speicherung von expliziten Kenntnissen in Datenbanken und die Förderung der informellen Kommunikation zur Verbreiterung des impliziten Wissens und
- Überwachung der Mitarbeiterkommunikation und Mobilität.[579]

Diese Mechanismen helfen die personenbezogenen Wissensrisiken zu reduzieren. Dazu gehören der Verlust von vertraulichem Wissen zu anderen Unternehmen, Arbeiten für einen anderen Mitbewerber oder selbst ein Unternehmen zu gründen.[580] Die untersuchten IT-Beratungen von OLANDER et al. identifizierten die bedeutende Rolle des Festhaltens an Wissensarbeitern und deshalb intensivieren sie ihre Bindung zu ihnen. Das Verlieren eines Keyplayers an ein konkurrierendes Unternehmen wäre das *worst-case* Szenario.[581] So hebt auch NORMAN hervor, dass der schwierigste Aspekt beim Wissensschutz das Wissen ist, das von Individuen und Gruppen in einem Unternehmen gehalten wird.[582]

In einem *Literature Review* analysieren AHMAD et al. die bekannten Wissensschutzmechanismen und bereiten diese in einer Übersicht auf. Die Wissensschutzmechanismen werden im Vergleich zu NORMAN in strategische, operationale, technische und formale unterteilt (Tabelle 20).[583] Die für die Arbeit relevanten Mechanismen sind hervorgehoben.

[578] Li et al. 2008, S. 315 f.
[579] Vgl. Olander et al. 2011, S. 598.
[580] Vgl. Olander et al. 2011, S. 598.
[581] Olander et al. 2011, S. 608.
[582] Vgl. Norman 2001, S. 58.
[583] Vgl. Ahmad et al. 2014, S. 30.

Tabelle 20: Synthese von Wissensschutzgebieten und -mechanismen[584]

Knowledge protection area	Mechanisms
Strategic-level Management Initiatives	**1. Identifying Valuable, Rare, Inimitable and Non-Substitutable knowledge assets** **a) Key firm knowledge resources to be identified and associated sensitivity risks assessed and considered** **2. Developing, implementing and resourcing policies, procedures and guidelines on Knowledge Protection** **a) Identifying knowledge protection roles** **b) Implementing protection processes and mechanisms** **c) Developing policies, procedures and guidelines** **d) Developing a security culture** **e) Resourcing security initiatives** f) Identification of relevant intellectual property rights and laws for knowledge protection policies
Operational-level Knowledge Protection Processes	**1. Compartmentalization to protect sensitive knowledge** 2. Classification and handling knowledge 3. Making knowledge explicit to prevent loss 4. Deliberately keeping knowledge tacit to mitigate leakage
Supporting Technology Infrastructure	Identification, configuration and deployment of tools and technologies to authenticate, control and track access to sensitive information
Legal Structures for Knowledge Protection	Legal frameworks and mechanisms to protect sensitive knowledge

Durch diese Hervorhebungen wird verdeutlicht, dass die Arbeit den strategischen Wissensschutz fokussiert, da in der Projektinitialisierungsphase und -definitionsphase die strategische Entscheidung zum *Wissen-Teilen* und *-Zurückhalten* in Bezug auf den Dienstleistereinsatz getroffen wird. Zu den Entscheidungen gehören auch die Identifizierung von wertvollen Wissensressourcen und die Entwicklung eines Vorgehens zum Wissensschutz. Für diese Arbeit bedeutet das, dass ein Vorgehen für den Schutz von wertvollen Wissensgebieten einer IT-Beratung entwickelt wird. Ebenso hingewiesen werden muss, dass die Mechanismen zum Schutz des impliziten Wissens im Fokus sind und damit nicht das explizite Wissen in Dokumenten oder IT-Systemen.

LINDEMANN et al. fokussieren sich auf den Schutz von Technologiewissen und stellen die verschiedenen Arten von Wissensschutzmechanismen zusammen. Die für diese Arbeit relevanten Wissensschutzmechanismen sind die *Steuerung des eigeninitiierten Wissenstansfers*, weil die IT-Beratung selbst und bewusst entscheidet welche Dienstleister in den Projekten involviert werden. Diese Mechanismen sind:

- Anteil Eigenleistung bei wichtigen Technologien hoch halten
- Wissen im Zweifel nicht ohne Rücksprache preisgeben
- Regeln für Herausgabe von Dokumenten und Komponenten definieren
- Entscheider für externe Freigabe von Wissen definieren
- Fernwartung einsetzen
- Outsourcing auf technologisch oder kommerziell unwichtige Leistungen beschränken

[584] In Anlehnung an Ahmad et al. 2014, S. 30.

- Wertschöpfung mit Kernwissen selbst im Heimatmarkt tätigen
- Offshoring auf Technologien mit limitiertem Leistungsspektrum beschränken
- Vertriebsleistung nicht outsourcen
- Schaden durch Wissenspreisgabe bei Entscheidungen berücksichtigen[585]

LEE et al., wie auch die vorliegende Arbeit konzentrieren sich auf die informellen Schutzmechanismen und empfehlen die Wissensschutzmechanismen als organisationale Fähigkeit zu sehen. Diese beinhaltet die folgenden vier Bereiche und optimieren zum Beispiel die Organisationsfähigkeiten um die Wettbewerbsvorteile zu sichern:

- Top-Management-Unterstützung
- Human Resource
- Informationsflüsse
- Partnerzugang[586]

Im entwickelten Referenzmodell[587] werden diese vier Bereiche adressiert. Zusammenfassend ist darzulegen, dass die Begriffe Wissensschutzstrategie, -methode und -mechanismus auf der Basis der Literatur abgegrenzt sind. Es wurde herausgearbeitet, dass die Arbeit die informalen Mechanismen fokussiert. Dazu gehören die identifizierten strategischen Mechanismen, die vor einer Projektkooperation mit einem Dienstleister etabliert werden müssen.

4.2.2 Wissensschutzziele und effektive Wissensschutzmechanismen

Die Wissensschutzziele, die sich eine IT-Beratung beim (Out-)Sourcing stellt, sind dependent von den in der Tabelle 21 aufgeführten Einflussfaktoren. Diese Einflussfaktoren sind die Erkenntnisse aus der bisherigen Forschungsliteratur,[588] welche in den folgenden Absätzen erörtert werden.

Tabelle 21: Einflussfaktoren auf die Wissensschutzziele[589]

Einflussfaktoren	Autor(en) / Studien
Unternehmensgröße / -art	Arundel 2001, Hanel 2001, Traoré 2005, Subramanyam & Susarla 2007, Amara et al. 2008, Bolisani et al. 2013
Branchenabhängigkeit	Howells et al. 2003
Wissensfähigkeiten (Marktaktivitäten[590])	Gold et al. 2001;
Rechtssystem	de Faria & Sofka 2010, Nassimbeni et al. 2012
Wissensart	Harabi 1995
Organisationale Kultur	Goldman 1998, Gold et al. 2001, Neville et al. 2003, Ahmad et al. 2014
Individueller Hintergrund	Link & Ruhm 2009

585 Lindemann et al. 2012, S. 87 f.
586 Vgl. Lee et al. 2007, S. 60.
587 Vgl. Kapitel 5.
588 Vgl. Thalmann & Manhart 2014, S. 13, Manhart & Thalmann 2015, S. 197 f.
589 Eigene Darstellung in Anlehnung an Thalmann & Manhart 2014, S. 13, Manhart & Thalmann 2015, S. 197 f.
590 Gold et al. 2001, S. 186 f.

Einflussfaktor: Unternehmensgröße / Unternehmensart

BOLISANI et al. verweist auf die Erkenntnisse von AMARA et al. zu der Korrelation von Wissensschutz und Unternehmensgröße. Die Verwendung der Wissensschutzmechanismen nimmt mit zunehmender Unternehmensgröße zu, vor allem bei den formalen Schutzmechanismen (wie Urheberrechten, Patenten usw.).[591] Größere produzierende Unternehmen (zum Beispiel Biotechnologie) setzen im Vergleich zu kleinen und mittelständischen Unternehmen eher auf Patente, um ihre Innovationen zu schützen.[592] Das geht mit den Erkenntnissen von ARUNDEL einher, dass die relative Bedeutung der Geheimhaltung im Vergleich zu Patenten bei größeren Unternehmen abnimmt.[593] Nach HANEL stützen sich herstellende Unternehmen umso mehr auf Schutzmethoden, umso größer sie sind.[594]

Einflussfaktor: Branchenabhängigkeit[595]

Verschiedene Autoren postulieren die Wirksamkeit des Wissensschutzmechanismus in Abhängigkeit von Branchen. AMARA et al. identifizieren bei ihren Untersuchungen zum Wissensschutz zwischen den Branchen signifikante Unterschiede. Hoch-technologisierte Branchen sind eher mit den formalen Schutzmethoden vertraut und KIBS-Unternehmen wird eher eine Tendenz zur Geheimhaltung und zu den informalen Methoden zugeordnet.[596] So werden bei Computer-Service-Organisationen mehr Wissensschutzmechanismen verwendet als bei Ingenieursdienstleistungen und Managementberatungsleistungen.[597] NORMAN eruiert bei komparativen Analysen einen Wissensschutz-Methodenmixansatz. Zum Beispiel sind Patente ein viel effektiverer Wissensschutz für die Pharmaindustrie als für die Elektronikindustrie.[598] Des Weiteren berichten andere Studien von einer viel höheren Patentneigung in der verarbeitenden Industrie als im Dienstleistungssektor.[599] Die Metallindustrie zum Beispiel nutzt diese Schutzformen schon seit langem, möglicherweise wegen ihrer Eigenständigkeit.[600] Bei informellen Gesprächen wurde zum Beispiel erwähnt, dass eine einmal gebaute Kraftwerksturbine nicht patentiert wird, weil die Informationen und das Wissen bei einer Patentierung beim Patentamt dokumentiert und damit offengelegt werden müssten.

Die Literaturrecherchen von PÄÄLLYSAHO & KUUSISTO demonstrieren, dass der Schutz von Service Innovationen, die ebenso mit IKTs umgesetzt werden können, durch ipr‘s äußerst schwierig und daher von untergeordneter Bedeutung sind.[601] In der Abbildung 29 ist ihre Übersicht zu drei KIBS-Branchen vergleichend dargestellt und dem formalen und informalen Wissensschutz zugeordnet. Die in dieser Arbeit fokussierte ISE beruht auf Beratungsleistungen, die

---

[591] Vgl. Bolisani et al. 2013, S. 197, Amara et al. 2008.
[592] Vgl. Amara et al. 2008, S. 1536, Traoré 2005.
[593] Vgl. Amara et al. 2008, S. 1536, Arundel 2001.
[594] Vgl. Amara et al. 2008, S. 1536, Hanel 2001.
[595] Im Abschnitt 2.2.3 wird der Wissensschutz und die Besonderheit der KIBS-Branche beschrieben.
[596] Vgl. Bolisani et al. 2013, S. 198.
[597] Vgl. Bolisani et al. 2013, S. 197, Amara et al. 2008.
[598] Vgl. Norman 2001, S. 55.
[599] Vgl. Olander et al. 2011, S. 597, Taylor & Silberston 1973, Cohen et al. 2000, Arundel & Kabla 1998.
[600] Vgl. Olander et al. 2011, S. 597, Hall 2005.
[601] Vgl. Päällysaho & Kuusisto 2011, S. 65.

dem KIBS-Zweig *Business / management consultancy* zugewiesen werden. Die externen Berater sind am individuellen Softwarelösungsprozess beteiligt. Im Vergleich zu der hier betrachteten ISE kann die von mehreren Kunden genutzte Standardsoftware zum *Software sector* gezählt werden. Für diese Standardsoftware werden eher die formalen Schutzmethoden verwendet.

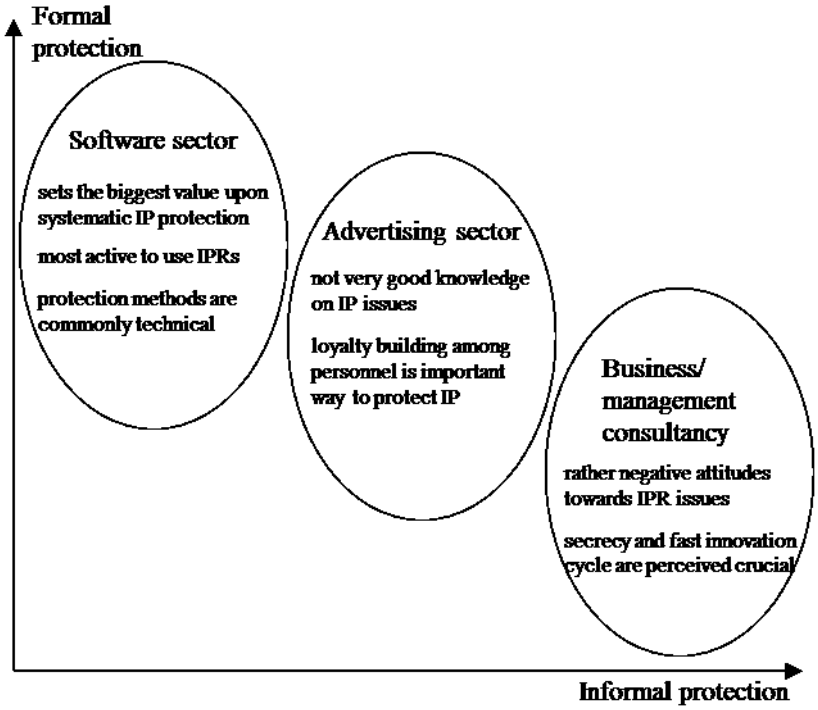

Abbildung 29: Die branchenspezifischen Unterschiede beim IP-Schutz in drei KIBS-Branchen[602]

Für die vorliegende Arbeit bedeutet das, dass der Fokus auf den informalen Wissensschutzmechanismus gesetzt wird.

Einflussfaktor: Wissensfähigkeiten (Marktaktivitäten)

GOLD et al. eruieren, dass der Wissensschutz zu einem effektiven WM der organisationalen Fähigkeiten gehört.[603] Sie bestätigen, dass nur das wertvolle Wissen geschützt werden muss, das die Wettbewerbsfähigkeit erhält.[604] Gleichzeitig sollten Unternehmen ihr vorhandenes Wissen ausschöpfen und neues Wissen schaffen, dass sie in ihren ausgewählten Märkten zielgerichtet positionieren.[605] Dieser Einflussfaktor implementiert sich im Modell mit der Bewertung der Wissensgebiete einer IT-Beratung und die der externen Dienstleister.

Einflussfaktor: Rechtssystem

Die nationalen oder internationalen Rechtssysteme in denen die kooperierenden Unternehmen agieren, haben auf das vorliegende Referenzmodell mit dem Fokus auf die informalen Wissensschutzmechanismen einen untergeordneten Einfluss.[606] Ein Rechtssystem hat beim Einsatz der

[602] Päällysaho & Kuusisto 2011, S. 74.
[603] Vgl. Gold et al. 2001, S. 186.
[604] Vgl. Gold et al. 2001, S. 192.
[605] Vgl. Gold et al. 2001, S. 186 f.
[606] Vgl. Abschnitt 4.2.1.

formalen Wissensschutzmechanismen eine Relevanz und bestimmt die Durchsetzbarkeit der gesetzlichen Regelungen. Die rechtlichen Rahmenbedingungen unterscheiden sich aufgrund der Vielfalt der wirtschaftlichen Entwicklung und der Handelspolitik in den Ländern.[607] Damit verbunden sind die Durchsetzung der Rechte am geistigem Eigentum.

Einflussfaktor: Wissensart

HARABI postuliert, dass für Produkt- und Prozessinnovationen die Patentierung der am wenigsten wirksame Wissensschutzmechanismus ist.[608] In der ISE werden unter anderem branchenspezifische Informationssysteme entwickelt, die die Prozesse vom Auftraggeber optimieren. Diese Aussage bestätigt die getroffene Modell-Entscheidung für die informalen Wissensschutzmechanismen um das Fach- und Technologiewissen der IT-Beratung zu schützen.

Einflussfaktor: organisationale Kultur

Die organisationale Kultur ist eine Voraussetzung damit die Akteure das notwendige Wissensschutzbewusstsein entwickeln um das Wissen der IT-Beratung zu schützen.[609] Für diese Arbeit bedeutet das, dass den Projektakteuren bewusst ist, welche Wettbewerbsfolgen eine nicht Berücksichtigung des Wissensschutzes haben kann. Die Wissensschutzkultur ist neben der entwickelten Wissensschutzstrategie essentiell zur Reduzierung der Risiken.[610]

Einflussfaktor: individueller Hintergrund

LINK & RUHM eruieren, dass Unternehmer mit einem akademischen Hintergrund ihr Wissen eher veröffentlichen als Unternehmen mit geschäftlichem Hintergrund, die eher ihr Wissen patentieren.[611] Eine IT-Beratung verfolgt ein geschäftliches Ergebnisziel und muss sich gegenüber Mitbewerbern, Auftraggebern und auch den eigenen Dienstleistern behaupten, wenn sie langfristig bestehen will.

Effektive Wissensschutzmechanismen und Geheimhaltung

Nach NEUHÄUSLER sollte die präferierte Strategie eine Kombination aus informalen und formalen Mechanismen sein oder das Unternehmen sollte nur informale Mechanismen anwenden.[612] Ebenso empfehlen MONTEIRO et al. nach ihren Wissensschutz-Untersuchungen den Schwerpunkt von den gesetzlichen auf die organisatorischen und verhaltensbezogenen Gesichtspunkte zu konzentrieren sowie strategische Wissensschutzmechanismen einzusetzen.[613]

Nach den Erhebungen von NORMAN basieren die effektivsten Wissensschutzmechanismen auf den folgenden zwei Kriterien. Erstens müssen die Mitarbeiter für den Wissensschutz sensibilisiert und zweitens muss das schützenswerte Wissen identifiziert werden. Eine hervorzuhebende

[607] Vgl. de Faria & Sofka 2010, S. 959, Yang & Kuo 2008.
[608] Vgl. Harabi 1995, S. 981.
[609] Vgl. Neville et al. 2003, S. 2041, Goldman 1998.
[610] Vgl. Neville et al. 2003, S. 2041.
[611] Vgl. Link & Ruhm 2009, S. 1.
[612] Vgl. Neuhäusler 2012, S. 688.
[613] Vgl. Monteiro et al. 2011, S. 1.

Eigenschaft dieser effektiven Methoden ist es, dass sie einem Unternehmen erlauben, nach außen offen zu sein und die Vorteile vom *Wissen-Teilen* zu nutzen. Zudem bewahren sie sich dadurch die Möglichkeit des spontanen Lernens und der Veränderung.[614]

Des Weiteren gehört nach den Untersuchungen von NORMAN das Abschotten und damit die Geheimhaltung von wertvollem Wissen ebenso zu den effektivsten Wissensschutzmechanismen. Ein Geheimnis ist nach SCHEPPLE eine Information, die von einem oder mehreren sozialen Akteuren absichtlich von einem oder mehreren anderen Akteuren zurückgehalten wird.[615] Mit der Geheimhaltung sind ebenso die Internalisierung und die Isolierung des wertvollen organisationalen Wissens verbunden. Die Geheimhaltung[616] und der Wissensvorsprung[617] werden in einigen Studien als die effizientesten Wissensschutzmechanismen erwähnt, und ebenso evident sind implizites Wissen und Komplexität beim Schutz des Kernwissens[618]. Die inquirierten Unternehmen bei NEUHÄUSLER bestätigen die Geheimhaltung und den Wissensvorsprung als relevante Wissensschutzmechanismen.[619]

Ein effektiver Mechanismus ist, festgelegte Aktivitäten ohne einen Dienstleister auszuführen. Das erlaubt einem Unternehmen oder einer IT-Beratung wertvolles schützenswertes Wissen vom Einflussbereich ihres Dienstleisters abzuschotten.[620] ROEHL & TRUITT haben eine ähnliche Strategie vorgeschlagen, die besonders bei Technologiewissen anwendbar ist.[621] Nach PÄÄLLYSAHO & KUUSISTO kann Schlüsselwissen oder *Know-how* unkompliziert vor einigen Mitarbeitern und/oder von externen Mitarbeitern wie Geschäftspartnern oder Kunden geheim gehalten werden. Viele Unternehmen definieren und klassifizieren sorgfältig das explizite Wissen nach Informationstypen. Generisch kann jedoch die Geheimhaltung einen negativen Einfluss auf die Innovationskraft und die Qualität der Interaktion haben.[622] Aufbauend auf der Literaturrecherche wird die Geheimhaltung als eine der effektivsten Wissensschutzmechanismen für das anvisierte Wissensschutz-Referenzmodell selektiert.

Zusammenfassend ist darzulegen, dass die bekannten Einflussfaktoren auf die Wissensschutzziele erörtert und die Erkenntnisse für die KIBS-Branche herausgestellt sind. Der informale und effektive Wissensschutzmechanismus der Geheimhaltung wird für die KIBS-Branche von mehreren Autoren verifiziert. Damit die Projektakteure die Geheimhaltung etablieren, müssen sie das wertvolle und schützenswerte Wissen im IT-Unternehmen identifizieren können. Der folgende Abschnitt verfolgt dieses Ziel.

---

[614] Vgl. Norman 2001, S. 55.
[615] Vgl. Hannah 2005, S. 71 f., Scheppele 1988, S. 12.
[616] Vgl. Olander et al. 2014, S. 2, Arundel 2001.
[617] Vgl. Olander et al. 2014, S. 2, Leiponen & Byma 2009, Lieberman & Montgomery 1988.
[618] Vgl. Olander et al. 2014, S. 2, Norman 2002.
[619] Vgl. Neuhäusler 2012, S. 692.
[620] Vgl. Norman 2001, S. 56.
[621] Vgl. Norman 2001, S. 56, Roehl & Truitt 1987.
[622] Vgl. Päällysaho & Kuusisto 2011, S. 68.

4.2.3 Bestimmung der Unternehmensgrenze für den Wissensschutz

Die erste[623] Forschungsfrage hat das Ziel, die Grenze beim *Wissen-Teilen und -Zurückhalten* in einer IT-Beratung zu identifizieren. LIEBESKIND theoretisiert, dass der Wissensschutz als die *boundary* eines Unternehmens beschrieben werden könnte und damit die Grenze vom *Wissen-Teilen und -Zurückhalten*.[624] Diese Grenze wird von HAMEL als *Openess / Transparency*[625], von QUINTAS et al. als das *Boundary Paradox*[626], von OLANDER et al. und BOLISANI et al. als das *Knowledge Sharing – Knowledge Protection Dilemma*[627] umschrieben.

Um die Grenze vom Unternehmen zu bestimmen stellt LIEBESKIND zwei Entscheidungsfragen auf, da IT-Beratungen nur das einzigartige und wertvolle Wissen schützen sollten, das den Schutzaufwand amortisiert:[628]

1. Welches Wissen soll geschützt werden und welches nicht?
2. Welchen Wissensschutzmechanismus oder welche Wissensschutzmechanismus-Kombinationen sollen verwendet werden, um das wertvolle Wissen zu schützen?

Die Anwendung von gleichzeitig mehreren Wissensschutzmechanismen kann zu überhöhten Kosten führen, wobei unzureichender Wissensschutz zu erheblichen Wissensverlust führt. Wie weiter oben geschrieben, sind situationsbedingt einige Wissensschutzmechanismen effektiver als andere. Diese Erkenntnisse sollten bei der Auswahlentscheidung der Mechanismen hinzugezogen werden. Auch müssen Unternehmen nach LIEBESKIND schwierige Kompromissentscheidungen in Bezug auf *Wissen-Teilen* treffen, weil der Wissensschutz die für die Innovation notwendigen Wissensströme hemmen kann. Aus diesem Grund muss zwischen Wissensschutz und Innovation taxiert werden. Dieser Innovationsschutz-Kompromiss kann je nach verwendetem Wissensschutzmechanismus mehr oder weniger intensiv ausgeprägt sein.[629]

Offenheit und Transparenz

DRECHSLER & NATTER und auch der Autor folgen der Definition des Konzepts der *Openness* von LAURSEN & SALTER. Sie definieren *Openness* als die gemeinsame Entwicklung von Wissen durch Beziehungen zu externen Partnern, einschließlich Wettbewerbern, Lieferanten, Dienstleistern, Auftraggebern, Universitäten und Forschungsinstitutionen.[630] Insbesondere ist der Offenheitsgrad die gewichtete Summe der verschiedenen Kooperationsarten, die von den Partnern in der Operationalisierung der Innovation verwendet werden, während die eingebrachten Ideen die Bedeutung des jeweiligen Partners wiederspiegeln.[631] Bezugnehmend auf die Kontingenztheorie von HAMBRICK können die Haupteinflussfaktoren des Offenheitsgrades in die organi-

[623] Siehe Forschungsfrage 1.
[624] Vgl. Liebeskind 1996, S. 93.
[625] Hamel 1991, S. 85.
[626] Quintas et al. 1997, S. 389.
[627] Olander et al. 2009, S. 355, Bolisani et al. 2013, S. 193.
[628] Vgl. Liebeskind 1996, S. 102.
[629] Vgl. Liebeskind 1996, S. 104.
[630] Vgl. Drechsler & Natter 2012, S. 439, Laursen & Salter 2006.
[631] Vgl. Drechsler & Natter 2012, S. 439.

sationsspezifischen (intern) und die umweltbezogenen (externe) Faktoren strukturiert werden.[632] JIANG definiert nach den Erkenntnissen von HAMEL die *Transparency* als die Offenheit und Durchlässigkeit vom Unternehmen, also wie problemlos der Dienstleister auf die Informationen, Kenntnisse und Fähigkeiten zugreifen kann.[633]

Boundary Paradox

NORMAN umschreibt den von QUINTAS et al. geprägten Begriff vom *Boundary Paradox* wie folgt.[634] Die gemeinsamen Entwicklungsbemühungen profitieren von einem hohen Maße an Interaktion und Kooperation zwischen den Unternehmen. Durch das Teilen stellt eine IT-Beratung ihr wertvolles und schützenswertes Wissen sowie ihre kritischen Fähigkeiten den Dienstleistern zur Verfügung. Das kann zur Aneignung von Wissen und deren Imitation[635] führen. Dadurch erkennen die Unternehmen das *Boundary Paradox* und sind für die Erkenntnisse von externen Quellen offen und schützen gleichzeitig das organisationsspezifische Wissen. KALE et al. umschreiben diese Grenzsituation wie bereits aufgeführt, als die Balance zwischen *trying to learn and trying to protect*[636]. Im Lernprozess zwischen Prinzipal und Agent entsteht der Zielkonflikt, dass Wissen der IT-Beratung an den Dienstleister diffundiert. Die Preisgabe von Wissen, das den Lernprozess zwischen den kooperierenden Unternehmen erleichtert, könnte eine IT-Beratung in Gefahr bringen.[637]

Bestimmung der Unternehmensgrenze für den Wissensschutz

Um die Grenze eines Unternehmens zu bestimmen, verweisen HOECHT & TROTT auf HAMEL & PRAHALAD. Um die Kernkompetenzen zu identifizieren, haben sie für die kritischen Geschäftsprozesse einen dreistufigen Test entwickelt.[638] Dieser dreistufige Analysetest der Kernkompetenz besteht aus der Bewertung des *Kundennutzens*, der *Mitbewerberabgrenzung* und der *Übertragbarkeit*. QUINN bestätigt dieses Vorgehen und weist gleichzeitig daraufhin, dass niemals die Kernkompetenzen oder ebenso bezeichnet als *best in world competencies* outgesourct werden dürfen.[639] Neben der von NORMAN identifizierten *Strategie*-Kategorie werden diese drei Bewertungskategorien in dem entwickelten Referenzmodell für die Bewertung des Fach- und Technologiewissens wieder verwendet.[640] Nach OLANDER et al. sind das technische Wissen und das Humankapital das wertvollste und schützenswerteste Vermögen einer IT-Beratung, die das Unternehmen befähigen, beim Wettbewerb in Führung zu bleiben.[641]

---

[632] Vgl. Drechsler & Natter 2012, S. 439, Hambrick 1983.
[633] Vgl. Jiang 2002, S. 14.
[634] Vgl. Norman 2002, S. 178.
[635] Eine Erklärung, welche Voraussetzung für die Imitation vorliegen muss, erfolgt im Abschnitt 4.2.4.
[636] Kale et al. 2000, S. 219.
[637] Vgl. Kale et al. 2000, S. 219.
[638] Vgl. Hoecht & Trott 2005, S. 403, Hamel & Prahalad 1994.
[639] Vgl. Hoecht & Trott 2005, S. 403, Quinn 1999.
[640] Siehe Abschnitt 5.2.3.
[641] Vgl. Olander et al. 2011, S. 606.

In der Forschungsliteratur werden die Begriffe Kernkompetenz, Kernressourcen, -fähigkeiten und wertvolles, einzigartiges, kritisches (Kern-)Wissen von mehreren Autoren im Zusammenhang mit Wissensschutz oder Schutz von Wissen verwendet. Nachfolgend sind die unterschiedlichen Begriffe und deren gemeinsame Verwendung in der Tabelle 22 hervorgehoben dargestellt.

Tabelle 22: Verwendung der Begriffe im Zusammenhang mit Wissensschutz[642]

Autor	Wertvolles Wissen	Einzigartiges Wissen	Kritisches Wissen	Kernwissen	Kernkompetenz	Kernressourcen / -fähigkeit
Ahmad et al. 2014	X					
Alstete 2003	X					
Belsis et al. 2005	X					
Bloodgood & Salisbury 2001	X					
Bolisani et al. 2013						X
Chan & Lee 2011					X	
Desouza & Vanapalli 2005	**X**				**X**	
Gold et al. 2001						X
Hurmelinna-Laukkanen 2011	X					
Howells et al. 2003	**X**				**X**	
Jennex & Zyngier 2007	X					
Jiang 2002		**X**			**X**	**X**
Kale et al. 2000	**X**				**X**	
Li et al. 2008	**X**			**X**	**X**	
Lee et al. 2007	**X**					**X**
Liebeskind 1996	X	X				
Luoma et al. 2010			**X**		**X**	
Manhart & Thalmann 2015	X		X			
Mayer 2006	**X**				**X**	
Nassimbeni et al. 2012					**X**	
Neville et al. 2003	X					
Nonaka 2007				X		
Norman 2001			**X**	**X**	**X**	**X**
Norman 2002				**X**		**X**
Olander et al. 2009	**X**			**X**	**X**	
Olander & Hurmelinna-Laukkanen 2010				X		
Olander et al. 2011				**X**	**X**	
Olander et al. 2014	**X**	**X**		**X**	**X**	
Thalmann & Manhart 2013			X			
Tongo 2013	X	X				
Trkman & Desouza 2012	**X**				**X**	
Väyrynen et al. 2013	X					

Daraus lässt sich schlussfolgern, dass das wertvolle / einzigartige / kritische (Kern-) Wissen von den verschiedenen Autoren zum Wissensschutz im Zusammenhang mit Kernkompetenz /

[642] Eigene Darstellung.

Kernressource / -fähigkeit verwendet wird und auf den Analysemethoden zu den Kernkompetenzen aufgebaut werden kann. An dieser Stelle soll ebenso auf die bereits erwähnte Wissenstreppe[643] nach NORTH hingewiesen werden. Bei dieser ist dokumentiert, dass die Kompetenz (Können) in Bezug auf die Wettbewerbsfähigkeit *über* dem Wissen (*Know-What* und *Know-How*) eingeordnet ist. Das Wissen stellt damit eine Voraussetzung für die Kompetenz dar.

Ebenso verwenden LINDEMANN et al. den Kernkompetenzbegriff im Zusammenhang mit wertvollem schützenswerten Wissen, wobei sich ihre Untersuchung auf den Schutz von Technologiewissen konzentriert.[644] Ihre Vorgehensempfehlung zur Definition des wertvollen Wissens umfasst die Beantwortung der drei Entscheidungsfragen:

- „Was kann unser Unternehmen bzw. unser Unternehmensbereich besonders gut?
- Warum kauft der Kunde unser Produkt?
- Was kann der Wettbewerb nicht?“[645]

Als Analyseergebnis sollen den wertvollen Wissenselementen mögliche Wissensträger im Arbeitsumfeld zugeordnet werden. Die Inhalte der drei postulierten Fragen sind bereits in den identifizierten Bewertungskategorien[646] integriert und werden deshalb nicht weiterverfolgt.

Ein weiterer Ansatz um die Unternehmensgrenze für den Wissensschutz zu bestimmen ist die Proximationsanalyse von GRONAU & BAHRS. Bei dieser soll verdeutlicht werden, auf welche Kritizitätsniveauinhalte die Akteure Zugriff haben.[647] Bei der Änderung des Zugangsniveaus der Akteure, Vorgabe von Risikogrenzwerten und durch die Definition von Mindestschutzanforderungen werden Anforderungen für die zukünftige Gestaltung der Informations- und Wissensschnittstellen definiert. Ebenso sehen GRONAU & BAHRS als primäres Mittel die Geheimhaltung, die das Wissen nur für einzelne Akteure zugänglich macht und keine kritischen Inhalte geteilt werden.[648]

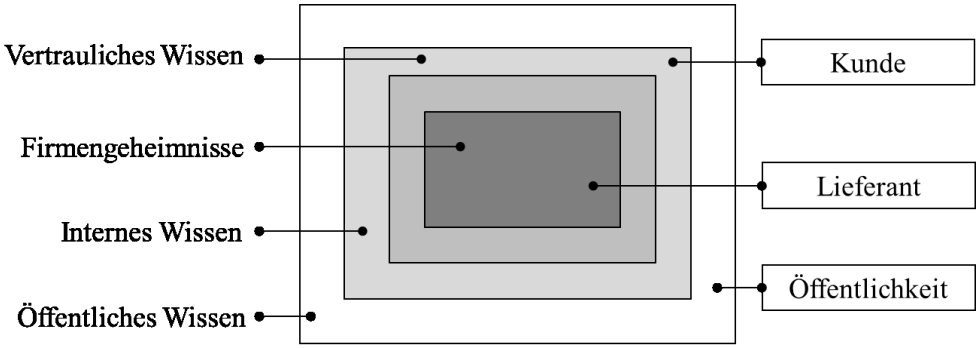

Abbildung 30: Proximationsanalyse[649]

[643] Vgl. Abschnitt 2.1.2.
[644] Vgl. Lindemann et al. 2012, S. 33.
[645] Lindemann et al. 2012, S. 33.
[646] Vgl. Hoecht & Trott 2005, S. 403, Quinn 1999, Norman 2001.
[647] Vgl. Gronau & Bahrs 2010, S. 410.
[648] Vgl. Gronau & Bahrs 2010, S. 411.
[649] Gronau & Bahrs 2010, S. 411, Systematische Risikoanalyse zur Verhinderung ungewollten Know-how Abflusses, 15.09.2010, http://knowledge-firewall.de/.

Zusammenfassend ist festzustellen, dass die diversen theoretischen Ansätze zur Bestimmung der Unternehmensgrenze vom *Wissen-Teilen und -Zurückhalten* erörtert wurden. Um diese Unternehmensgrenze zu bestimmen, wurde der Autor auf die Literatur zur Kernkompetenz aufmerksam und adaptiert diese Vorgehensweise für den Wissensbegriff. Hervorzuheben ist, dass keiner der Autoren erwähnt hat, dass ihre theoretischen Ansätze praktisch verifiziert sind. Für das theoretische Referenzmodell und damit für den Prototypen werden deshalb die Bewertungsansätze (*Strategie*, *Kundennutzen*, *Mitbewerberabgrenzung*, *Übertragbarkeit*) zur Kategorisierung der Wissensgebiete in Kombination mit der Geheimhaltung ausgewählt, da diese ebenso die praktische Erfahrung des Autors reflektieren.

4.2.4 Risikomanagement und (Out-)Sourcing

Dieser Abschnitt baut auf der Definition und den Grundlagen zum Risikobegriff aus Abschnitt 2.2.3 auf. NORMAN und TRKMAN & DESOUZA eruieren, dass die Mitarbeiteraufklärung ein Schlüsselfaktor für den effektiven Wissensschutz ist, um die einzelnen Wissensrisiken zu verringern.[650] Ein inquirierter Manager von NORMAN merkte an, dass der Schutz des wertvollen Wissens von den Entscheidungen der Mitarbeiter eines Unternehmens abhängig ist.[651] Die größte Herausforderung besteht darin, die Mitarbeiter zur Teilnahme an der Mitarbeiteraufklärung zu motivieren und offen wertvolles Wissen zu vermitteln und dabei unerwünschte Überläufe zu Mitbewerbern zu verhindern.[652] Das Bewusstsein für den Bedarf an Wissensschutz beginnt in der Führungsebene. Somit sollte die Führungsebene die Voraussetzungen für einen effektiven Wissensschutz schaffen, um das wertvolle Wissen einer IT-Beratung zu identifizieren. Ohne diese eindeutige Identifikation würden die unterschiedlichen Individuen differenzierte Entscheidungen treffen.[653] Mitarbeiter wissen oft nicht, welches Wissen für die IT-Beratung wertvoll ist, deshalb sollte eine mögliche Aktion sein, allen Mitarbeitern bewusst zu machen, dass schützenswertes Wissen unter keinen Umständen außerhalb der Arbeitsumgebung besprochen werden darf.[654] In Bezug auf Projekte stellen JORDAN & LOWE bei ihrer Studie heraus, je komplexer das Projekt ist,

- desto größer die Anzahl der Partner,
- desto breiter der Projektumfang,
- desto innovativer das anvisierte Ergebnis,
- desto größer ist die Notwendigkeit die institutionellen Vereinbarungen eng miteinander zu verbinden.[655]

Diese Aussage wird in das theoretische Referenzmodell integriert.

---

[650] Vgl. Trkman & Desouza 2012, S. 10, Norman 2001.
[651] Vgl. Norman 2001, S. 55 f.
[652] Vgl. Trkman & Desouza 2012, S. 10.
[653] Vgl. Norman 2001, S. 55 f.
[654] Vgl. Trkman & Desouza 2012, S. 10.
[655] Vgl. Jordan & Lowe 2004, S. 253.

Risikomanagement

Das Wissensrisikomanagement muss ökonomisch sein,[656] der investierte Aufwand sollte sich deshalb amortisieren. Nach den Analysen von TRKMAN & DESOUZA haben viele Unternehmen enorme Zeit und Ressourcen aufgewendet, um ihre Wissensressourcen besser zu organisieren und das kann sich wiederum evident auf die Wissensnetzwerke auswirken. Ein Unternehmen kann über den Markt, das Netzwerk und durch den internen Aufbau Wissen erwerben. Bei diesen drei Wissensakquirierungen sollten die Risiken und die aufzuwendenden Kosten evaluiert werden.[657] TRKMAN & DESOUZA definieren Wissensrisiken als:

> "a likelihood of any loss from an event connected with the identification, storage or protection of knowledge that may decrease the operational or strategic benefit of any party involved in the network (cf., Perrot, 2007)."[658]

Sie stellen dar, dass zum Beispiel bei einer asymmetrischen Kooperation, die bei einer Prinzipal-Agenten-Beziehung vorliegt, dass erkannte Risiko höher ist, als bei einer symmetrischen Beziehung.[659] Das Wissensschutzlevel des organisationalen Wissens ist deshalb mit Hilfe des Referenzmodells zu bestimmen, damit die Verantwortlichen in die Lage versetzt werden nachvollziehbare Entscheidungen in Bezug auf den Wissensschutz zu treffen. IT-Beratungen, die von Kooperationen profitieren können und gleichzeitig ihr wertvolles Wissen schützen, erhöhen die Wahrscheinlichkeit, ihre Wettbewerbsvorteile als Grundlage für ihren Markterfolg zu erhalten.[660]

HOECHT & TROTT postulieren, dass hochriskante Wissensgebiete im Kontext Risikomanagement identifiziert werden sollen und die Auswahl und der Wissenszugriff der Externen überwacht werden muss. Für sie ist die zunehmende vernetzte Wirtschaft der Preis der *Offenheit nach außen*, den die IT-Beratungen beim externen Dienstleistereinsatz eingehen. Sie empfehlen gegen den ungewollten Wissensverlust an externe Berater die bewährten Wissensschutzmaßnahmen zu verwenden.[661] Für HOECHT & TROTT stellt sich die Frage, ob die sozialen Kontrollinstrumente stark genug sind, um *Betrayal Acts* durch externe Berater zu verhindern. Die sozialen Kontrollinstrumente sind zum Beispiel die Selbstregulierung von verinnerlichten Normen zu professionellem Verhalten und der Reputationsverlust.[662]

Im Vergleich zu einem Berater eines externen Dienstleisters, der erheblich weniger von der netzwerkbasierten sozialen Kontrolle dependent ist, agiert ein akademischer Forscher in der eng verzahnten wissenschaftlichen Gemeinschaft. Seine Arbeit ist von Natur aus auf Kollaboration ausgerichtet und seine soziale Stellung entscheidend für das alternierende Vertrauen.[663] Externe Berater dagegen arbeiten für konkurrierende Unternehmen und haben keine etablierten

---

[656] Vgl. Trkman & Desouza 2012, S. 4.
[657] Vgl. Trkman & Desouza 2012, S. 4.
[658] Trkman & Desouza 2012, S. 5.
[659] Vgl. Trkman & Desouza 2012, S. 11.
[660] Vgl. Li et al. 2008, S. 328.
[661] Vgl. Hoecht & Trott 2005, S. 406 f.
[662] Vgl. Hoecht & Trott 2005, S. 406.
[663] Vgl. Hoecht & Trott 2005, S. 406 f.

Berufsverbände, die in der Lage und bereit sind, dass Geschäftsverhalten ihrer Mitglieder zu regulieren.[664]

Das Unternehmen kann nach HOECHT & TROTT externe Dienstleister durch eingesetzte übergreifende Experten (Gatekeeper) kontrollieren, da beim strategischen Outsourcing die gesetzlichen Mittel eine begrenzte Wirksamkeit haben und die Voraussetzung für den Aufbau von Vertrauen evident schlechter sind als in traditionellen Outsourcing-Beziehungen. Diese übergreifenden Experten müssen in ihrem Aufgabenbereich hoch angesehen sein, damit sie die identifizierten Hochrisikobereiche innerhalb ihres Unternehmens definieren, abgrenzen und überwachen können. Mit dem übergreifenden Experten kann ein bewusster Wissensverlust an den externen Berater verhindert werden, aber es besteht weiterhin das Risiko, dass versehentlich Wissen offen gelegt wird und das führt zu Wettbewerbsdefiziten in der Branche.[665] Einen übergreifenden Experten bei der ISE einzusetzen wird in dem vorliegenden Referenzmodell nicht verfolgt. Diese kontrollierende Funktion sollte eine Gemeinschaftsentscheidung der IT-Projektakteure sein, wie sie das Modell fokussiert. Nach HOECHT & TROTT ist es für externe Berater diffizil die Vertraulichkeit gegenüber seinen Auftraggebern zu gewährleisten und zeitgleich weltbeste Geschäftsmethoden zu vermitteln.[666] Zu diesen Weltklasse-Fähigkeiten haben GHODESWAR & VAIDYANATHAN eine Übersichtsgrafik erstellt, auf die jedes Unternehmen mit Outsourcing zugreifen kann (Abbildung 31). Die Informationstechnologie und Softwareentwicklung ist eine der acht identifizierten Fähigkeiten.

[664] Vgl. Hoecht & Trott 2005, S. 407.
[665] Vgl. Hoecht & Trott 2005, S. 407.
[666] Vgl. Hoecht & Trott 2005, S. 407.

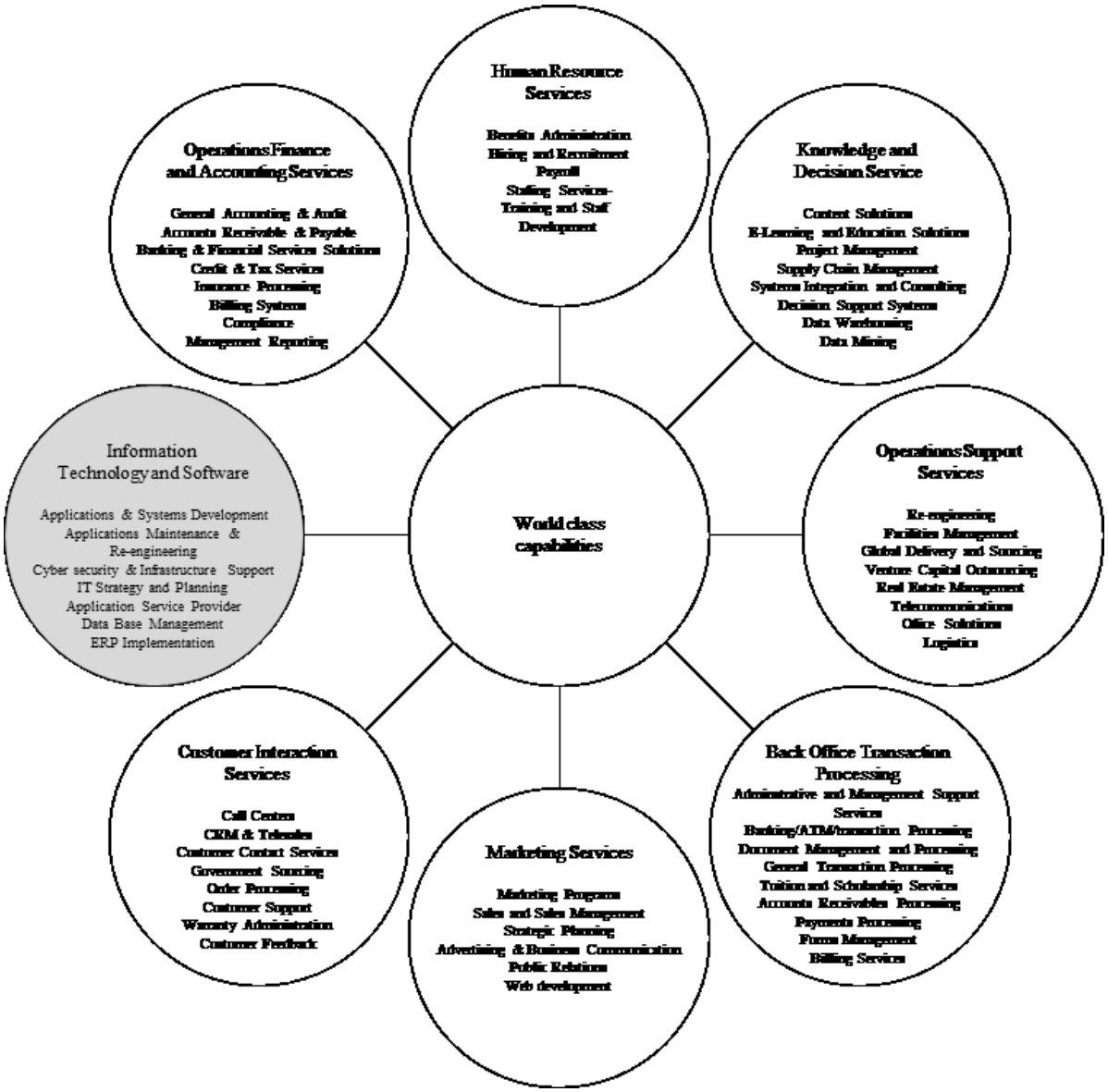

Abbildung 31: Weltklasse Ressourcen / Fähigkeiten[667]

(IT-) Outsourcing

Basierend auf einer umfangreichen Auswahl an Outsourcingdefinitionen fokussiert die Arbeit eine Definition mit IT-Bezug. Das Outsourcing definieren KARABULUT et al. als:

> "ongoing administration, management and possibly subcontracting by an external party, of specific client's (IT) processes to enhance their efficiency and effectiveness".[668]

NASSIMBENI et al. grenzen die Begriffe Outsourcing und Offshoring gegeneinander ab, da einige Autoren diese zwei Termini oft konfus und überlappend verwenden.[669] Die untersuchten Sourcing-Studien zeigen, dass eine Unterscheidung in die zwei Variablen Eigentum an Unternehmenswerten (facilities) und Lokation vom Dienstleistungsanbieter sinnvoll ist.[670] Diese

[667] Ghodeswar & Vaidyanathan 2008, S. 33, Brown & Wilson 2005.
[668] Karabulut et al. 2007, S. 48.
[669] Vgl. Nassimbeni et al. 2012, S. 406, Monczka et al. 2005, Jagersma & Gorp 2007, Elango 2008, Manning et al. 2008.
[670] Vgl. Nassimbeni et al. 2012, S. 406, Olsen 2006, Metters 2008, Aksin & Masini 2008.

zwei Variablen sind in der Abbildung 32 visualisiert und beide Begriffe lassen sich wie folgt abgrenzen:

- Outsourcing: bezieht sich auf die Verlagerung von Prozessen an externe Dienstleister unabhängig vom Standort des Dienstleisters.
- Offshoring: bezieht sich auf die Verlagerung von Prozessen in jedes fremde Land, unabhängig davon, ob der Dienstleister extern oder mit dem Unternehmen verbunden ist.[671]

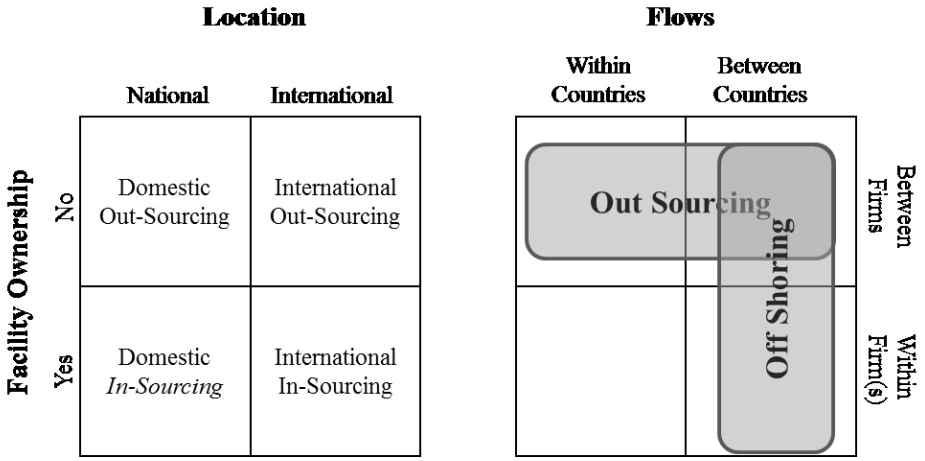

Abbildung 32: Sourcing Alternativen[672]

Outsourcing kann sich auf die Verlagerung innerhalb und zwischen Ländern beziehen, wobei sich Offshoring nur auf internationale Verlagerung orientieren kann. Offshoring inkludiert daher nur die Verlagerung von Arbeitsplätzen oder Prozessen an einen externen und international ansässigen Dienstleister.[673]

GHODESWAR & VAIDYANATHAN unterscheiden in drei verschiedene Outsourcinglevel:

- Taktisches Outsourcing: ist eine Form des traditionellen Outsourcings und basiert auf dem Kostenvergleich und der make-or-buy Entscheidung. Die Vorteile beziehen sich auf finanzielle Einsparungen und lösen von Personalproblemen. Zudem kann es sich auf periphere Aktivitäten erstrecken um branchenspezifische Fähigkeiten zu erwerben, indem mit ausgewählten Dienstleistern zusammengearbeitet wird.
- Strategisches Outsourcing: wird für die Neudefinition der Unternehmen verwendet, damit sich das Management auf die Kerngeschäftsfunktionen konzentrieren kann.
- Transformationales Outsourcing: wird häufig dazu verwendet, um das Geschäft neu zu definieren. Das Unternehmen wird befähigt ihre Führungsposition zu behalten, einen nachhaltigen Wettbewerbsvorteil zu schaffen und für ein Unternehmen den höchsten Wert zu schaffen.[674]

Die Risiken beim strategischen und transformationalen Outsourcing sind höher als beim taktischen und werden gemeinsam mit dem Outsourcingpartner geteilt. Bevor eine Outsourcingvereinbarung getroffen wird, müssen geprüfte Risikominimierungspläne, Hochsicherheitsniveaus, reife Projektmanagementkompetenzen und bewährte Business Kontinuitätspläne deployt werden.[675] Obwohl die Risiken bei einem taktischen Outsourcing von GHODESWAR &

[671] Vgl. Nassimbeni et al. 2012, S. 406.
[672] Nassimbeni et al. 2012, S. 407.
[673] Vgl. Nassimbeni et al. 2012, S. 406, Olsen 2006.
[674] Vgl. Ghodeswar & Vaidyanathan 2008, S. 25 f.
[675] Vgl. Ghodeswar & Vaidyanathan 2008, S. 26.

VAIDYANATHAN geringer im Vergleich zu den anderen beiden Outsourcingleveln eingestuft werden, fokussiert diese Arbeit das taktische Outsourcing und ihre Risikobewertung.

NASSIMBENI et al. differenzieren zwischen dem *Information Technology Sourcing* (ITS), *Business Process Sourcing* (BPS) und dem *Knowledge Process Sourcing* (KPS).

- ITS betrachtet die Externalisierung von Prozessen, die mit der technologischen Infrastruktur des Auftraggeberunternehmens verbunden sind, wie Softwareentwicklung, Webentwicklung und dem Helpdesk.[676]
- BPS bezieht sich auf die Beschaffung von Unterstützungsaktivitäten wie zum Beispiel Finanzierung, Rechnungswesen und Personal.[677]
- KPS-Dienste beinhalten hochkomplexe, wissensintensive und beurteilungsorientierte Prozesse wie die medizinische Diagnostik und die Politikverwaltung.[678]

Das Outsourcen von Tätigkeiten im Rahmen von IT-Projekten kann nach diesen Definitionen dem ITS zugeordnet werden. Das vorliegende Modell basiert auf dem ITS, da IT-Softwareentwicklung und Webentwicklung externalisiert werden.[679]

MONCZKA et al. haben ein Modell für das onshore/offshore IT-Service Outsourcing entwickelt, das NASSIMBENI et al. um die Hauptrisiken ergänzen.[680] In der Tabelle 23 sind die Outsourcing Phasen mit der Beschreibung der Stufen visualisiert. Das entwickelte Referenzmodell basiert auf den Erkenntnissen von MONCZKA et al. und NASSIMBENI et al.

Tabelle 23: Phasen und Stufen beim strategischen Outsourcing[681]

	Stage			
Phase	I	II	III	IV
Strategy and Planning	Reactive, opportunistic approach toward identifying and deciding to act on opportunities	Informal process to evaluate whether an individual activity should be considered for outsourcing	Formal process applied periodically to identify and evaluate candidate activities across the company for outsourcing opportunities	Ongoing systematic process to identify and evaluate candidate activities, business units, functions across the company for outsourcing opportunities
Contracting and Relationship Development	For each situation, ad-hoc approach is used for defining requirements, negotiating and selecting suppliers and shaping relationships	Informal and inconsistently applied process exists for defining requirements, negotiating and selecting suppliers and shaping relationships	Formal, consistently applied process used to define requirements, negotiate and select suppliers and shape relationships	Formal process extends to include early identification of relationships growth opportunities and paths/milestone to realize them
Implementation	Ad-hoc approach is used for transition planning; „Arms-length“ management of the relationship driven by adherence to contract terms	Informal and inconsistently applied process exists for transition planning and relationship management	Formal, repeatable process used to govern the transition and manage the ongoing relationship for mutual benefit	Proactive process used to identify untapped opportunities and develop new relationships with current and potential outsourcing partners

676 Vgl. Nassimbeni et al. 2012, S. 407, Bhalla et al. 2008, Ghodeswar & Vaidyanathan 2008.
677 Vgl. Nassimbeni et al. 2012, S. 407, Sen & Shiel 2006.
678 Vgl. Nassimbeni et al. 2012, S. 407, Currie et al. 2008, Sen & Shiel 2006.
679 Vgl. Nassimbeni et al. 2012, S. 405 f.
680 Vgl. Monczka et al. 2005, Nassimbeni et al. 2012.
681 Monczka et al. 2005, S. 53.

LOH & VENKATRAMAN definieren IT-Outsourcing als:

> ''the significant contribution by external vendors in the physical and/or human resources associated with the entire or specific components of the IT infrastructure in the user organization''.[682]

IT-Outsourcing kann als eine bedeutende administrative Innovation angesehen werden, bei der es eine signifikante Verschiebung der Unternehmensführung, Veränderung der internen Prozesse der Anwenderorganisationen und Veränderung der organisatorischen Routinen zur Bewältigung der externen Umwelteinflüsse gibt.[683] FARRELL hebt hervor, dass das IT- / IKT-Outsourcing Geschäft exponentiell expandiert, da die Unternehmen immense Kosten und technologische Vorteile erwarten.[684]

Zusammenfassend festzuhalten ist, dass das Wissensrisikomanagement essentiell ist, jedoch müssen sich die investierten Aufwände amortisieren. Das Wissensrisiko ist bei einer asymmetrischen Sourcing-Kooperation (Prinzipal-Agenten-Beziehung) höher, da die externen Berater von keiner sozialen Kontrolle dependent sind. Auf der Grundlage der Abgrenzung vom Outsourcing und Offshoring wird die vorliegende Arbeit dem taktischen Outsourcinglevel und dem ITS zugeordnet. Einige hier aufgeführte Arbeiten sind auch relevant für die nachfolgende Dienstleisterauswahl (Unterkapitel 4.3).

4.3 Sourcing-Phase 2: Dienstleisterauswahl

In den folgenden Abschnitten wird die bestehende Literatur mit Bezug auf Partnerbeziehungen erörtert. Dabei wird die originäre Bezeichnung Partner verwendet und die Erkenntnisse auf die Dienstleisterbeziehung adaptiert.

Damit der Agent das vom Prinzipal geteilte Wissen nutzbringend für sich deployen kann, gibt es nach ZHAO drei Voraussetzungen:

- die Motivation zu imitieren,
- die Fähigkeit zu imitieren und
- die Möglichkeit der Umgehung rechtlicher Restriktionen.[685]

Die Motivation zu imitieren ist auf das *opportunistische Verhalten*[686] vom externen Dienstleister zurückzuführen (Abschnitt 4.3.1). Die Wissensüberlappung (Abschnitt 4.3.2) und *absorptive Kapazität* (Abschnitt 4.3.3) sind die Voraussetzungen für die Fähigkeit zu imitieren. Diese drei Themengebiete werden deshalb in diesem Unterkapitel untersucht.

4.3.1 Opportunismus und Vertrauen

Einer der Hauptgründe warum Unternehmen an Kooperationen teilnehmen besteht darin, dass sie Wissen und Fähigkeiten vom Partner erlernen möchten und gleichzeitig wollen sie sich vor

[682] Loh & Venkatraman 1992, S. 336.
[683] Vgl. Khalfan 2004, S. 30, Loh & Venkatraman 1992.
[684] Vgl. Farrell 2010, S. 3.
[685] Vgl. Zhao 2006, S. 1186.
[686] Vgl. Abschnitt 4.3.1.

dem opportunistischen Verhalten des Partners schützen, um ihr wertvolles Wissen zu behalten.[687] Jedoch handelt ein opportunistischer Partner per Definition bewusst und vorsätzlich, so dass sich opportunistisches Verhalten als intendierte Dysfunktionen bezeichnen lässt.[688] WILLIAMSON ordnet dem Begriff „Guile" (Arglist) die aufgeführten intendierten Verhaltensweisen zu[689] und definiert Opportunismus als:

> "[…] opportunistic agents are given to self-interest seeking with guile. This includes but is scarcely limited to more blatant forms, such as lying, stealing, and cheating. More generally, opportunism refers to the incomplete or distorted disclosure of information, especially to calculated efforts to mislead, distort, disguise, obfuscate, or otherwise confuse."[690]

Opportunistisches Verhalten und Risiko

Die Reduktion der Informationsasymmetrie erhöht die Anfälligkeit einer IT-Beratung gegenüber dem opportunistischen Verhalten durch einen früheren Dienstleister, was ein opportunistisches Risiko für das fokale[691] Unternehmen darstellt.[692] Denn in Netzwerken versuchen Dienstleister so viel Wissen wie möglich von anderen Unternehmen zu extrahieren, während sie so wenig wie möglich selbst beitragen.[693] Das führt zu einem suboptimalen Zustand der Zusammenarbeit, wobei jedes Unternehmen auf der Suche nach einem lokalen statt nach einem globalen Optimum ist.[694]

MAJCHRZAK & JARVENPAA heben hervor, dass in vielen Unternehmen, wo einzelne Mitarbeiter kollaborieren und in Situation mit opportunistischen Risiken beteiligt sind, das Management Regeln vorgibt, was geteilt werden darf und was nicht.[695] Die Verantwortlichkeit für die Definition der Unternehmensgrenze[696] wird aufgrund dieser Aussage im theoretischen Referenzmodell dem Management zugeordnet.

Vertrauen

Bei der Recherche zum Wissensschutz und seiner angrenzenden Forschungsdisziplinen[697] wird schnell deutlich, dass das Vertrauen eine entscheidende Position in der partnerschaftlichen Zusammenarbeit einnimmt. Für Vertrauen gibt es unzählige Definitionen. Der Autor folgt der Definitionen von MAYER et al. und HUMPHREY & SCHMITZ, die Vertrauen folgendermaßen definieren:

---

[687] Vgl. Kale et al. 2000, S. 217.
[688] Vgl. Walter et al. 2010, S. 137.
[689] Vgl. Walter et al. 2010, S. 136, Williamson 1975, S. 6, 1985, S. 47.
[690] Williamson 1985, S. 47.
[691] Nach dem Gabler Wirtschaftslexikon ist ein fokales Unternehmen ein zentrales Unternehmen in einem strategischen Netzwerk, dem die Aufgabe der Selektion bei der Aufnahme von Unternehmen in das Netzwerk, die Koordination der spezialisierten Aktivitäten der Netzwerkunternehmen sowie die Steuerung des Wissenstransfers und die Evaluierung der erbrachten Leistungen innerhalb des Netzwerkes zufällt. Siehe: http://wirtschaftslexikon.gabler.de/Definition/fokales-unternehmen.html.
[692] Vgl. Li et al. 2008, S. 319.
[693] Vgl. Trkman & Desouza 2012, S. 10, Baum et al. 2000.
[694] Vgl. Trkman & Desouza 2012, S. 10.
[695] Vgl. Majchrzak & Jarvenpaa 2010, S. 78.
[696] Vgl. Abschnitt 4.2.3
[697] Vgl. Tabelle 18.

> "[T]he willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party."[698]

> "[…] an agent exhibits trust when he/she exposes herself/himself to the risk of opportunistic behaviour by others and when he/she has no reason to believe that the trusted other will exploit this opportunity."[699]

Nach HOECHT & TROTT ist eine zentrale Erkenntnis, dass das Vertrauen den Treuegeber (Prinzipal) anfällig für das Verhalten des Treuenehmers (Agent) macht, aber der Treuegeber diese Chance ignoriert. Diese gewählte Unwissenheit macht soziale Interaktion möglich.[700] ZUCKER postuliert, dass Vertrauen auch auf die Zugehörigkeit zu einer gemeinsamen Gruppe beruht, es kann prozessbasiert und institutionalisiert sein.[701] SAKO unterscheidet zwischen folgenden Vertrauensformen:

- Kompetenzvertrauen: ist das Vertrauen in die Fähigkeiten des anderen, etwas ordnungsgemäß durchzuführen.
- Vertragliches Vertrauen: ist das anerkennen der vereinbarten Austauschregeln.
- Wohlwollendes Vertrauen: ist die gegenseitige Erwartungshaltung zur Zusage über die vertraglichen Verpflichtungen hinaus.[702]

Der Fokus der vorliegenden Arbeit liegt auf dem wohlwollenden Vertrauen, weil das Wissensschutz-Modell die Anwendung der formalen Wissensschutzmechanismen und damit auch die vertraglichen Vereinbarungen voraussetzt. Zudem kann wegen der schwierigen Nachweisbarkeit vom wiederverwendeten Wissen durch den Dienstleister und dem vorliegenden opportunistischen Verhalten des Dienstleisters nicht ausschließlich auf die Verträge vertraut werden. Dennoch kann sich durch gemeinschaftliche Erfahrungen der Kooperationspartner Vertrauen generieren und durch das Vertrauen können sich wiederum die Transaktionskosten und die Unsicherheit beim Wissensaustausch und -transfer reduzieren.[703]

TRKMAN & DESOUZA fassen zusammen, dass das Vertrauen zwischen Dienstleistungspartnern und der Vertrauensaufbau die bedeutsamste Voraussetzung für einen Wissenstransfer in einer Netzwerkbeziehung ist.[704] Wenn IT-Beratungen Informationen oder Maßnahmen vor einem Dienstleister verbergen, ist die organisationsübergreifende Zusammenarbeit zurückhaltend.[705] Der langsame Aufbau von stabilem Vertrauen und die zügige Reduzierung von Informationsasymmetrie zwischen den kooperierenden Unternehmen erleichtern die Weiterentwicklung des Wissens und den Wissenstransfer zwischen ihnen.[706]

---

[698] Mayer et al. 1995, S. 712.
[699] Humphrey & Schmitz 1996, S. 4.
[700] Vgl. Hoecht & Trott 2005, S. 408 f.
[701] Vgl. Hoecht & Trott 2005, S. 408 f., Zucker 1986.
[702] Vgl. Hoecht & Trott 2005, S. 408 f., Sako 1992.
[703] Vgl. Li et al. 2008, S. 317, Gulati 1995, Barney & Hansen 1994, Beckman et al. 2004, Dyer & Chu 2003, McEvily et al. 2003, Parkhe 1993.
[704] Vgl. Trkman & Desouza 2012, S. 11, Bönte 2008, Dawes et al. 2009, Easterby-Smith et al. 2008, Rosenbaum 2000, van Wijk et al. 2008.
[705] Vgl. Trkman & Desouza 2012, S. 11 f., Yeung et al. 2009.
[706] Vgl. Li et al. 2008, S. 318.

Vertrauen verringert das opportunistische Verhalten

DYER & SINGH stellen heraus, dass eine Vertrauensbasis eine wesentliche Voraussetzung für interorganisatorische Zusammenarbeit ist, um dem Dienstleister einen angemessenen Anreiz für das Teilen vom wertvollen Wissen zu geben.[707] Das Vertrauen beeinflusst offensichtlich erheblich die wahrgenommenen Risiken in dem die wesentlichen Widersprüche zwischen den kooperierenden Unternehmen reduziert werden, die aufgrund von gegenseitigem Misstrauen und Beziehungsproblemen vor und während der Zusammenarbeit auftreten können.[708] HUMPHREYS et al. deuten darauf hin, dass Vertrauen das Potenzial für opportunistisches Verhalten zwischen den kollaborierenden Parteien senkt und damit die Transaktionskosten des Austausches, da weniger Kontrollmechanismen benötigt werden.[709] Nach KE & WEI hat die Unfähigkeit die Handlungen beim zukünftigen Wissensaustausch der Partner vorherzusagen den entgegengesetzten Effekt in Bezug auf den Einsatz von Kontrollmechanismen.[710]

Nach HAUSLER et al. ist Vertrauen zwischen Unternehmen vor allem in technologischen Kooperationen kritisch.[711] Vertrauen reduziert die Ängste vor dem Opportunismus des Dienstleisters und senkt damit die Transaktionskosten[712].[713] Durch das Vertrauen wird nach INKPEN & LI die Notwendigkeit von Überwachung und anderen Kontrollmechanismen reduziert.[714] Für CURRALL & JUDGE fördert das Vertrauen Verhaltensweisen wie die offene Kommunikation und die Bereitschaft Informationen zu teilen.[715] Auf der Grundlage dieser Erkenntnisse sollten IT-Beratungen mit vertrauenswürdigen Dienstleistern weniger Wissensschutz brauchen.[716]

Andererseits heben MONTEIRO et al. hervor, dass wenn bei innovativen Entwicklungspartnerschaften gleichzeitig strategische Wissensschutzmechanismen eingesetzt werden, vermittelt das eine konfuse Nachricht an die aktuellen und potenziellen Partner, da dieses die Vertrauensentwicklung hemmt.[717] In Beziehungen mit wenig Vertrauen werden deshalb strukturelle Mechanismen verwendet, um zum einen die Möglichkeiten des opportunistischen Verhaltens zu begrenzen oder opportunistisches Verhalten durch Strafen zu verhindern, die so schwerwiegend sind, dass sie eigennützigem Verhalten zuvorkommen.[718]

---

[707] Vgl. Lee et al. 2007, S. 67, Dyer & Singh 1998.
[708] Vgl. Trkman & Desouza 2012, S. 11, Simatupang & Sridharan 2002.
[709] Vgl. Trkman & Desouza 2012, S. 11, Humphreys et al. 2004.
[710] Vgl. Trkman & Desouza 2012, S. 11, Ke & Wei 2007.
[711] Vgl. Norman 2004, S. 612, Hausler et al. 1994.
[712] Vgl. Williamson 1991.
[713] Vgl. Norman 2004, S. 612, Williamson 1991.
[714] Vgl. Norman 2004, S. 612, Inkpen & Li 1999.
[715] Vgl. Norman 2004, S. 612, Currall & Judge 1995.
[716] Vgl. Norman 2004, S. 612.
[717] Vgl. Monteiro et al. 2011, S. 2.
[718] Norman 2004, S. 611.

Partnerauswahlentscheidungen auf Basis von Interaktionen und Reputation

LI et al. fanden heraus, dass frühere Dienstleisterpartnerschaften das Opportunismuspotential reduzieren können.[719] Sie heben hervor, dass bei bekannten Dienstleistern mit denen bereits vorherige Interaktionen stattgefunden haben eine höhere Wahrscheinlichkeit besteht, gegenseitig das Wissen, die Betriebsroutinen und die Managemententscheidungen zu verstehen.[720] Mit diesem Vorwissen können frühere Partner die informellen Wissensschutzmechanismen leichter überwinden.[721] In bestehenden Partnerschaften, wo sich die Geschäftspartner kennen und ein opportunistisches Verhalten anstreben, ist es aus diesen Gründen leichter das wertvolle Wissen des Geschäftspartners aufzunehmen, als für neue Geschäftspartner.[722]

Für LI et al. lassen sich die Partner aufgrund bisheriger Interaktionen in drei Arten unterteilen, diese sind in Freunde, Bekannte und Unbekannte.[723] Die Visualisierung der bisherigen Interaktionen in Beziehung zum getragenen Risiko und dem Mehrwert der Partnerschaft erfolgt in Abbildung 33.

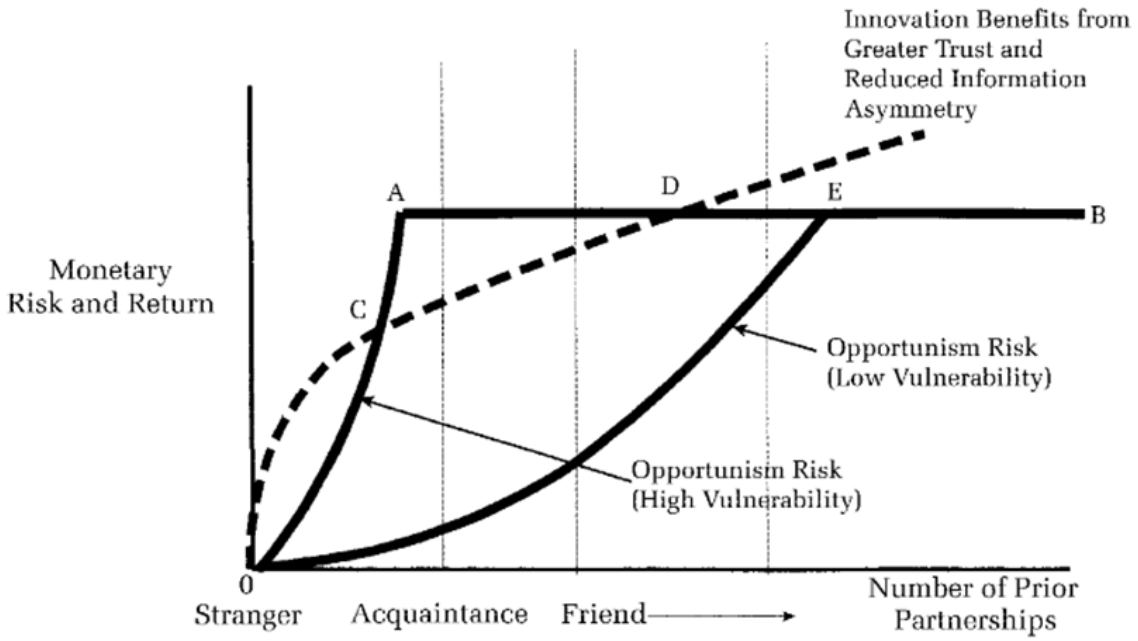

Abbildung 33: Transitivität der Partnerauswahlentscheidungen[724]

Der formale Wissensschutz kann in einigen Partnersituationen unwirksam oder weniger wirksam sein als angestrebt, weshalb der verbleibende Opportunismus durch eine sorgfältige Auswahl von Partnern reduziert werden kann.[725] Die Partnerauswahl ist ein essentieller Bestandteil vom Sourcingmanagement. Die bisherige Forschung und auch die befragten Interviewpartner

[719] Vgl. Li et al. 2008, S. 320, Gulati 1995, Sabel 1993.
[720] Vgl. Li et al. 2008, S. 318.
[721] Vgl. Li et al. 2008, S. 318, Arrow 1974, Heiman & Nickerson 2002, 2004.
[722] Vgl. Li et al. 2008, S. 318.
[723] Li et al. 2008, S. 315 f.
[724] Li et al. 2008, S. 319.
[725] Vgl. Li et al. 2008, S. 320.

weisen darauf hin, dass Unternehmen Partner aufgrund ihrer Ressourcen und Fähigkeiten auswählen.[726] Unternehmen können zum Beispiel ihre Partnerauswahlentscheidung anpassen, um ihr wertvolles Wissen zu schützen.[727] Das ist ein Grundgedanke des entwickelten Referenzmodells. Die Partnerauswahl ist eine der richtungsweisenden Entscheidungen eines Unternehmens.[728]

Der Erfolg oder Misserfolg von früheren Kooperationen kann bei zukünftigen Entscheidungen erhebliche Auswirkungen auf die Partnerauswahl haben.[729] In der Regel werden bei Misserfolg einer Kooperation keine negativen Nachrichten publiziert, es sei denn rechtliche Aspekte wurden verletzt.

TRKMAN & DESOUZA stellen heraus, dass die wahrgenommene Reputation von anderen Unternehmen ein entscheidender Antrieb bei jeder Entscheidung Wissen zu teilen oder zurückzuhalten ist, denn eine längere Interaktionsdauer wirkt sich positiv auf die Reputation aus.[730] Das heißt, bei einem geringen Erfahrungsschatz gibt es wenige Reputationsinformationen über den Dienstleistungspartner, was den Wissensaustausch riskanter macht.[731] Daher ist zu Beginn jeder Dienstleistungspartnerschaft ein anfängliches Vertrauensniveau erforderlich, um den Wissensaustausch aufzunehmen und die erwarteten langfristigen Vorteile müssen die wahrgenommen Risiken überwiegen.[732] Ebenso bestätigen JORDAN & LOWE, dass ein Unternehmen das Problem vom wissensabsorbierenden Dienstleister mildern kann, indem es die gemachte Dienstleistererfahrung dokumentiert und das Vertrauen zu diesem prüft.[733] Im Referenzmodell wird deshalb die von den Projektakteuren erworbene Dienstleistererfahrung aus vorherigen Projekten und Beziehungen in die Dienstleisterauswahl einbezogen. Dieses Erfahrungswissen wird in die Bewertung des *Gefahrenpotentials* vom externen Dienstleister integriert.

Höheres Risiko bei Partnern aus verschiedenen Ländern

Nach LI et al. bilden die Komplexität des globalen Geschäftsumfeldes und die mangelnde Vertrautheit zwischen den Allianzpartnern aus verschiedenen Ländern zusammen ein höheres wahrgenommenes Opportunitätsrisiko als in inländischen Allianzen.[734] Infolgedessen sind die Allianzpartner vermutlich mehr über den Wissensverlust in internationalen Allianzen besorgt, als sie es bei inländischen sind. Diese Bedenken können sich in einer vorsichtigen Auswahl von Allianzpartnern widerspiegeln. Daher ist die Erforschung der Partnerauswahl für internationale F&E-Allianzen als Mechanismus zum Schutz der technologischen Vermögenswerte der Allianz-Teilnehmer erforderlich.[735]

---

[726] Vgl. Li et al. 2008, S. 327 f.
[727] Vgl. Li et al. 2008, S. 329.
[728] Vgl. Li et al. 2008, S. 315.
[729] Vgl. Li et al. 2008, S. 329.
[730] Vgl. Trkman & Desouza 2012, S. 11, Ensign & Hébert 2010.
[731] Vgl. Trkman & Desouza 2012, S. 11, Carayannopoulos & Auster 2010.
[732] Vgl. Trkman & Desouza 2012, S. 11.
[733] Vgl. Jordan & Lowe 2004, S. 247.
[734] Vgl. Li et al. 2008, S. 331, McCutchen et al. 2004.
[735] Vgl. Li et al. 2008, S. 331.

Vertrauensaufbau zwischen Prinzipal und Vendor/Agent

Für den Prinzipal ist es vorteilhaft eine langfristige Beziehung mit dem Vendor zu betrachten und zu etablieren, um die Unsicherheiten zu eliminieren.[736] Wie bereits weiter oben geschrieben, verwenden GHODESWAR & VAIDYANATHAN den Vendor Begriff im Zusammenhang mit Prinzipal und Client. Ihre Erkenntnisse können einer Prinzipal-Agenten-Beziehung zugeordnet werden und fließen deshalb in das Wissensschutz-Modell ein. Das Teilen von Erkenntnissen, Erfahrungen und Wissen erleichtern es oft bei Prinzipal-Vendor-Beziehungen ein höheres Maß an Vertrauen aufzubauen und eine bessere Atmosphäre für den Aufbau der laufenden strategischen Geschäftsbeziehung zu schaffen.[737]

Nach MONTEIRO et al. ermöglichen formelle Kooperationen und informelles Sourcing das Wissen von kooperierenden Unternehmen für Innovationen zu kombinieren,[738] jedoch scheint genau das mit dem Begriff des strategischen Wissensschutzes unvereinbar zu sein.[739]

Zusammenfassend ist darzulegen, dass es sich beim opportunistischen Verhalten um eine intendierte Dysfunktion handelt und jedes Unternehmen ein lokales anstatt ein globales Optimum anvisiert. Das gegenseitige Vertrauen kann sich aus gemeinsam realisierten Projekten etablieren. Aus der Literatur wird das wohlwollende Vertrauen für die vorliegende Arbeit abgeleitet. Mit dem Vertrauensaufbau kann das opportunistische Verhalten reduziert werden. Bei der ISE mit wertvollem und schützenswerten Wissen sind nur Dienstleister einzusetzen, denen ein hohes Vertrauen durch generierte Projekterfahrung zugewiesen werden kann.

4.3.2 Wissens-, Markt-, Wettbewerbsüberlappung

In der vorliegenden Partnerauswahlliteratur werden die Wissens-, Markt- und Wettbewerbsüberlappung von verschiedenen Autoren angeführt. Ein Dienstleister, der die Vermögenswerte einer IT-Beratung ergänzt, anstatt das sich die Vermögenswerte überlappen, kann die Aneignungsgefahr nach JORDAN & LOWE vermindern, aber nicht vollständig vermeiden. Das Konzept der *absorptiven Kapazität* im folgenden Abschnitt baut darauf auf, dass sich einige Kenntnisse notwendigerweise überlappen um neues Wissen für die Unternehmen zu generieren.[740] Für das entwickelte Referenzmodell wird damit transparent gemacht, dass die Feststellung der überlappenden Bereiche ein zentrales Kriterium ist, um die *absorptive Kapazität*[741]des Dienstleisters zu bewerten.

Wissensüberlappung

Eine gewisse Wissensüberlappung zwischen den Partnern ist erforderlich und Voraussetzung damit sie sich gegenseitig verstehen und effektiv miteinander zusammenarbeiten können. Ein fokales Unternehmen wird wahrscheinlich mehr auf den Wissensschutz bei einem Partner mit

---

[736] Vgl. Ghodeswar & Vaidyanathan 2008, S. 30.
[737] Vgl. Ghodeswar & Vaidyanathan 2008, S. 30.
[738] Vgl. Monteiro et al. 2011, S. 6, Kogut & Zander 1992.
[739] Vgl. Monteiro et al. 2011, S. 6.
[740] Vgl. Jordan & Lowe 2004, S. 247.
[741] Vgl. Abschnitt 4.3.3.

umfangreicheren Fähigkeiten achten, als bei einem Partner mit geringeren Fähigkeiten.[742] Ebenso stellen OLANDER et al. fest, dass bei gemeinsamer F&E für neue Innovationen ein gewisses Maß an komplementärem Wissen notwendig ist. Jedoch darf das wertvolle Wissen nicht mit dem Partner geteilt werden.[743] Nach NORMAN ist die Feststellung der Wissensüberlappung eine Voraussetzung um die *absorptive Kapazität*[744] festzustellen.[745] Diese Aussagen weisen darauf hin, dass das Wissen einer IT-Beratung und die der potentiellen Dienstleister kategorisiert werden müssen, damit eine Risikobewertung erfolgen kann.

GHODESWAR & VAIDYANATHAN empfehlen, dass bei der Auswahl eines Dienstleisters für ein IT-Projekt, die angebotene Leistung des Dienstleisters im Rahmen eines Pilotprojektes demonstriert und beurteilt werden sollte.[746] Damit erhält das Unternehmen Informationen zu der vorliegenden Wissensüberlappung beim Dienstleistungspartner. Um die Technologiewissensüberlappung von zwei Unternehmen zu bewerten haben LI et al. die hinterlegten Patente untersucht.[747]

Wettbewerbsüberlappung

Unternehmen, die mit Partnern zusammenarbeiten, die gleichzeitig eine hohe Wettbewerbsüberlappung aufweisen, müssen aus Wettbewerbsgründen ihr wertvolles Wissen intensiver schützen.[748] Wenn Wissen an einen Partner oder einen Wettbewerber transferiert wird, dann ist es dependent, ob dieser das Wissen effektiv nutzen kann. Das heißt, wenn dem Wettbewerber ergänzendes Wissen fehlt, dann kann es sein das auch dieses transferierte Wissen ihm nicht weiterhilft.[749]

Bei den Untersuchungen stellte NORMAN fest, dass das Bedürfnis nach Wissensschutz bei einem Dienstleister auf den folgenden Konstellationen basiert: der Wettbewerbsüberlappung, dem entwickelten Vertrauen[750] und dem Umstand ob das obligatorische Wissen zum wertvollen und schützenswerten Wissen einer IT-Beratung gehört.[751] Die Wettbewerbs- und Marktüberlappung haben analoge Inhalte und werden deshalb für den Referenzmodell-Beitrag im nächsten Absatz zusammengefasst.

Marktüberlappung

Die Überlappung der Marktbereiche wird folgend beschrieben. JIANG definiert bezugnehmend auf KHANNA den Marktbereich als:

---

[742] Vgl. Norman 2004, S. 612.
[743] Vgl. Olander et al. 2011, S. 595.
[744] Vgl. Abschnitt 4.3.3.
[745] Vgl. Norman 2002, S. 181.
[746] Vgl. Ghodeswar & Vaidyanathan 2008, S. 30.
[747] Vgl. Li et al. 2008, S. 324.
[748] Vgl. Inkpen 1998, S. 73.
[749] Vgl. Liebeskind 1997, S. 629.
[750] Vgl. Abschnitt 4.3.1.
[751] Vgl. Norman 2001, S. 58.

> "A firm's market scope is defined by both its product and geographic scope, and it determines a firm's areas of economic interest."[752]

Die Marktüberlappung gibt an, inwieweit die zugrundeliegende Einstellung des Unternehmens gegenüber der Allianz wettbewerbsfähig ist.[753] Partnerunternehmen, die in unterschiedlichen Geschäftsbereichen arbeiten, tendieren eher zu komplementären als zu konkurrierenden Interessen, daher ist das Konfliktpotential zu Interessensphären weniger wahrscheinlich.[754]

Haben die Partner im Gegensatz dazu einen hohen Überlappungsgrad in ihren Marktbereichen, dann wird es für einen oder ebenso für beide Unternehmen möglich sein, mit der *absorptiven Kapazität* die Fähigkeiten des jeweils anderen zu erlernen.[755] Wenn die Unternehmen eine Nähe in Produkt und/oder geographischen Märkten haben, wird es für sie leichter sein die erworbenen Kompetenzen des anderen Unternehmens anzueignen.[756] Eine hohe Marktüberlappung bedeutet mehr Wettbewerb und eine höhere *absorptive Kapazität* des Dienstleisters. Damit ist das Unternehmen für das nicht autorisierte Lernen des Dienstleisters anfälliger und der Schutz vor ungewolltem Wissensabfluss sollte eine hohe Priorität für das Unternehmen haben. JIANG schlussfolgert deshalb, dass das Transparenzniveau von einem Unternehmen wahrscheinlich geringer sein wird, umso höher der Grad der Marktüberlappung zwischen den Marktbereichen des Unternehmens und seiner Partner ist.

Nach MARCH sind zwei Arten von Allianzaktivität zu unterscheiden, die Exploitation (Ausbeutung) im Vergleich zur Exploration (Erforschung).[757] Bei ausbeutenden Aktionen nutzen Unternehmen ihre bestehenden Vermögenswerte und Technologien, um Einnahmen zu erzielen und die Produktivität zu erhöhen.[758] Bei explorativen Aktivitäten streben die Unternehmen nach neuen Ressourcen, Technologien oder Produkten.[759] Jeder der beiden Strategien sind für Unternehmen notwendig. Das zeichnet sich durch die erfolgreiche Exploitation aus und sichert die Rentabilität des Unternehmens, während die kontinuierliche Erforschung hilft, die Zukunftsfähigkeit zu sichern. In der Tabelle 24 sind die einzelnen Ausprägungen gegenübergestellt.

---

[752] Jiang 2002, S. 15, Vgl. Khanna et al. 1998, S. 195.
[753] Vgl. Jiang 2002, S. 15, Bleeke & Ernst 1993, Khanna et al. 1998.
[754] Vgl. Jiang 2002, S. 15, Lei et al. 1997.
[755] Vgl. Jiang 2002, S. 16, Cohen & Levinthal 1990, Mowery et al. 1996, 1998.
[756] Vgl. Jiang 2002, S. 16, Hamel 1991.
[757] Vgl. Jiang 2002, S. 16, March 1991.
[758] Vgl. Jiang 2002, S. 16, Koza & Lewin 1998.
[759] Vgl. Jiang 2002, S. 16, Levinthal & March 1993.

Tabelle 24: Exploitative Allianzen vs. Explorative Allianzen[760]

	Exploitative	Explorative
Goal	Efficiency, value-adding, rent-maximization	Innovation, new knowledge generation
Preferred information flow	Pre-defined, controlled	Free, open
Need for knowledge sharing	lower	higher
Learning focus	Learn *from* the partner	Leran *with* the partner
Expected pay-off	Certain and proximal	Uncertain and distant
Incentive for opportunism	Higher	Lower
Need for knowledge protection	Higher	Lower

Folgende Behauptungen ergeben sich daraus. Unternehmen haben eher ein höheres Transparenzniveau bei *explorativen* Allianzen als bei *exploitativen* Allianzen. Die Art der Allianzaktivitäten ergibt sich aus der Überlappung der Marktbereiche auf das Transparenzniveau derart, dass der negative Zusammenhang weniger stark bei *explorativen* Allianzen als bei *exploitative* Allianzen ist.[761] Bei der untersuchten Dienstleisterbeziehung von Prinzipal und Agent liegt eine *exploitative* Beziehung vor.

Nach BOSCHMA kann nach der kognitiven, organisatorischen, sozialen, institutionellen und geographischen Nähe zwischen zwei Unternehmen differenziert werden.[762] Diese fünf Arten sind miteinander verbunden. Die organisatorische Nähe basiert im Vergleich zu der geografischen Nähe auf der Zugehörigkeit und der Ähnlichkeit.[763] Diese Aussagen weisen darauf hin, dass die Wettbewerbs- / Marktaktivitäten und der Marktumfang von einer IT-Beratung und dem potentiellen Dienstleister für die Risikobewertung kategorisiert und in Relation zueinander gesetzt werden müssen.

Zusammenfassend ist festzustellen, dass die Wissens- und die Wettbewerbs- / Marktüberlappung zwischen einer IT-Beratung und dem externen Dienstleister für die Risikobewertung herangezogen werden muss. Zudem sind externe Dienstleister mit umfangreicheren Fähigkeiten im Vergleich zu der beauftragenden IT-Beratung mit einem höheren Risiko bei der Zusammenarbeit einzustufen. Das Referenzmodell stützt sich auf diese Aussage.

4.3.3 Absorptive Kapazität

Die Voraussetzung für den Wissenstransfer und die bildende Wertschöpfung ist die *absorptive Kapazität* des Dienstleisters. Das beinhaltet die Fähigkeit neues Wissen von einer IT-Beratung

[760] Jiang 2002, S. 18.
[761] Vgl. Jiang 2002, S. 17.
[762] Vgl. Trkman & Desouza 2012, S. 9, Boschma 2005.
[763] Vgl. Trkman & Desouza 2012, S. 9, Davenport 2005, Lemarie et al. 2001.

zu bewerten, zu assimilieren und anzuwenden.[764] Die *absorptive Kapazität* wird als die Fähigkeit eines Unternehmens definiert, die den Wert neuen Wissens erkennen kann und das Wissen für kommerzielle Zwecke aufnimmt.[765]

Vom theoretischen Standpunkt impliziert das Konzept der *absorptiven Kapazität* von COHEN & LEVINTHAL die Offenheit von Unternehmen bei Innovationen.[766] Die *absorptive Kapazität* eines Unternehmens bezieht sich auf seine Kompetenz um auf externe Ideen, Wissenschaften und andere Wissensquellen für Innovationen zuzugreifen, diese aufzunehmen und zu integrieren.[767] COHEN & LEVINTHAL verbinden die *absorptive Kapazität* mit der Lernbereitschaft und Innovationsfähigkeit.[768] Diese beiden Eigenschaften geben Hinweise wie ausgeprägt die *absorptive Kapazität* vom externen Dienstleister ist. Diese Eigenschaften werden in die Bewertung des *Dienstleister-Gefahrenpotentials* des Referenzmodells integriert.

Eine erstellte prozessbasierte Definition regt an, dass die *absorptive Kapazität* als die Fähigkeit des Dienstleisters gesehen werden kann, externes Wissen durch sequentielle explorative und transformative Prozesse sowie *exploitatives* Lernen zu nutzen. Diese Sichtweise impliziert, dass IT-Beratungen mit externen Dienstleistern interagieren um die Effizienz und Effektivität ihrer Innovationsprozesse zu erhöhen.[769] In Bezug auf den Grad der Offenheit sollte einer IT-Beratung, die gewillt ist zu Lernen und ihr Wissen zu teilen, das strategische Ausmaß der Zusammenarbeit bewusst sein.[770]

Die *absorptive Kapazität* hängt von der individuellen und organisationalen Ebene des Wissensempfängers ab, da dem vorhandenen Wissen neues Wissen hinzugefügt werden muss.[771] Das Wissen, das bei der ISE aufgebaut wird, ist ebenso dem idiosynkratischen[772] Wissen zuzuordnen, das nicht an einem einzigen Ort aggregiert werden kann.[773]

Frühere Interaktionen zwischen Partnern

Forschungsarbeiten zur *absorptiven Kapazität* befassen sich damit, dass frühere Interaktionen zwischen den beteiligten Unternehmen die kausale *Ambiguität* beim Wissenstransfer reduzieren, weil der Technologietransfer zwischen den Unternehmen effizienter und effektiver durchgeführt werden kann.[774] Im Umkehrschluss heißt das, dass umso länger und so öfter die Unternehmen bereits zusammengearbeitet haben, umso besser funktioniert der Wissens- und Tech-

---

[764] Vgl. Olander & Hurmelinna-Laukkanen 2010, S. 416.
[765] Vgl. Inkpen 1998, S. 75.
[766] Vgl. Drechsler & Natter 2012, S. 439.
[767] Vgl. Drechsler & Natter 2012, S. 439.
[768] Vgl. Cohen & Levinthal 1990, S. 128.
[769] Vgl. Drechsler & Natter 2012, S. 439.
[770] Vgl. Drechsler & Natter 2012, S. 439.
[771] Vgl. Grant 1996, S. 111.
[772] Das idiosynkratische Wissen wird von Hayek (1945, S. 521) als „knowledge of the particular circumstances of time and place" und von Jensen & Meckling (1992) als „specific knowledge" bezeichnet. Zitiert nach Grant 1996, S. 111.
[773] Vgl. Grant 1996, S. 111.
[774] Vgl. Li et al. 2008, S. 317, Cohen & Levinthal 1990, Kale et al. 2000, Kogut & Zander 1992, Mowery et al. 1998, Szulanski 1996, von Hippel 1994, Zahra & George 2002.

nologietransfer zwischen den Unternehmen, weil die kausale *Ambiguität* beim Transfer reduziert wird. Die Fähigkeit eines Dienstleisters Kenntnisse von einer IT-Beratung zu absorbieren, ist dependent von ihrer historischen Beziehung, damit ist die *absorptive Kapazität* unternehmensspezifisch und pfadabhängig.[775] Diese Bestimmung der unternehmensspezifischen *absorptiven Dienstleisterkapazität* wird im Referenzmodell implementiert.

COHEN & LEVINTHAL weisen darauf hin, dass der Zugriff auf Wissen der anderen Unternehmen nicht das Gleiche ist, wie die Fähigkeit, seinen Wert zu erkennen, zu assimilieren und effizient in die Prozesse zu integrieren. Genau diese Fähigkeit ist von der *absorptiven Kapazität* des Unternehmens und damit von der aufgebauten Wissensbasis abhängig.[776] Aufgrund dieser Aussage werden in der Dienstleisterauswahl im Referenzmodell Informationen abgefragt, die den Dienstleister kategorisieren.

Die *absorptive Kapazität* eines Dienstleisters in Bezug auf externe Technologien ist dependent von den technischen Fähigkeiten und der Managementkompetenz des Kommunikationsempfängers. Damit ist die *absorptive Kapazität* am größten, wenn das was gelernt werden soll im Zusammenhang mit dem bereits Bekannten steht.[777] In diesem Zusammenhang erläutert MOWERY, ein Unternehmen ist weit besser ausgestattet, wenn es ein gewisses Maß an interner F&E selbst durchführt, um die Ergebnisse von externer F&E aufzunehmen.[778] Zusammenfassend lässt sich festellen, das interne und externe F&E sich nicht ersetzen sondern ergänzen.[779]

Ähnlichkeit der Qualifikation, Ressourcen und Fähigkeiten

Umso ähnlicher die Qualifikationen, Ressourcen, Fähigkeiten, organisationale Strukturen und Prozesse von Unternehmen, desto größer ist die *absorptive Kapazität*.[780] Während diese Ähnlichkeiten die Zusammenarbeit erleichtern kann, erhöht sich das Risiko des Wissensverlustes.[781] Aus der Ressourcensicht bedeutet das für das Referenzmodell, dass die Anzahl der Mitarbeiter und die Anzahl der Länderaktivitäten des Dienstleisterunternehmens erfasst werden sollten. Zum Beispiel haben größere Unternehmen nachvollziehbarerweise ein umfangreicheres Technologieportfolio und damit eher eine Technologie, die für die intendierte Kooperation relevant ist.[782]

Ein ähnlicher Dienstleister kann leichter den Wert des Wissens einer IT-Beratung erkennen und hat eine bessere Möglichkeit das Wissen zu replizieren und zu nutzen. Aus diesem Grund sollten IT-Beratungen ihr Wissen in einem größeren Ausmaß schützen, wenn sie eine höhere Ressourcenüberlappung mit ihrem Dienstleister haben.[783] Das führt zu der Erkenntnis, dass bei

[775] Vgl. Mowery et al. 1996, S. 89.
[776] Vgl. Davis 2004, S. 407, Cohen & Levinthal 1990.
[777] Vgl. Teece 1998, S. 22.
[778] Vgl. Teece 1998, S. 22, Mowery 1984.
[779] Vgl. Teece 1998, S. 22.
[780] Vgl. Norman 2004, S. 612.
[781] Vgl. Norman 2002, S. 183.
[782] Vgl. Mowery et al. 1996, S. 81.
[783] Vgl. Norman 2002, S. 183.

einem Dienstleister mit umfangreicheren Fähigkeiten als die IT-Beratung der Wissensschutz erforderlicher ist, als bei einem mit geringeren Fähigkeiten.[784]

Bestimmung von Dienstleisterart, Dienstleisterbranche (Marktumfang)

Die gegenwärtige *absorptive Kapazität* eines Dienstleisters wird durch seine historische Beteiligung an bestimmten Produktmärkten, Forschungs- und Entwicklungsbeteiligungen und seiner technischen Aktivitäten beeinflusst.[785] Für das Referenzmodell bedeutet das, dass die Dienstleisterart zu bestimmen ist.

Ohne die notwendige *absorptive Aufnahmekapazität*, den offenen Zugang zu Wissen und den Fähigkeiten ist es weniger wahrscheinlich, dass es sich auf das fokale Unternehmen auswirkt, weil der Partner weniger fähig ist, die Informationen kommerziell zu nutzen.[786] Für das Referenzmodell bedeutet das, dass die Dienstleisterbranchen ermittelt werden und damit der Marktumfang.

Zusammenfassend werden in diesem Abschnitt die *absorptive Kapazität* und ihre in der Forschung aufgezeigten dependenten Faktoren aufgeführt. Für das Referenzmodell sind die Dienstleistergröße (Mitarbeiter), Länderaktivitäten (Länder), Dienstleisterart, Dienstleisterbranche (Marktumfang), Lernbereitschaft und Innovationsfähigkeit zur Bestimmung der *absorptiven Dienstleisterkapazität* wesentliche Merkmale.

[784] Vgl. Norman 2004, S. 612.
[785] Vgl. Cohen & Levinthal 1990, S. 135 f., Mowery et al. 1996, S. 81.
[786] Vgl. Norman 2002, S. 192.

5 Forschungsergebnis Wissensschutz-Referenzmodell

Nachdem im Kapitel 4 der Forschungsstand zum relevanten Wissensschutz gelegt wurde, beschreibt dieses Kapitel das auf dieser Basis entwickelte theoretische (Prototyp) und in den Interviews weiterentwickelte und evaluierte Wissensschutz-Referenzmodell. Zunächst konzentriert sich das erste Unterkapitel auf einen Modellüberblick. Die Unterkapitel 5.2 und 5.3 deskribieren die zwei Referenzmodell-Phasen mit den fünf identifizierten Funktionen und den Akteuren. Diese Funktionen werden aus der Theorie und durch die Auswertung der Interviews ergänzt. Das letzte Unterkapitel fokussiert die Pilotierung an einem ausgwählten IT-Projekt und die Evaluation nach der deployment, epistemologischen und ökonomischen Perspektive.

5.1 Überblick zum Referenzmodell

Das entwickelte Modell gibt einen Bezugsrahmen für IT-Beratungen. Dennoch muss sich jede IT-Beratung dem Wissensschutz selbst stellen und in Abhängigkeit der Wissensbasis und der definierten Strategie Regelungen festlegen. Das Modell fokussiert den strategischen Wissensschutz vom impliziten Wissen in IT-Projekten. Nach der Vielzahl der aufgeführten Wissensschutzmechanismen (Abschnitt 4.2.1) nimmt das Modell die folgenden Mechanismen auf:

- Identifizierung von wertvollen Wissensressourcen mit dem Ziel der Geheimhaltung,
- Beschränkung vom Dienstleisterzugriff durch
    - zielgerichtete Dienstleisterauswahl und
    - Überwachung der Wissens- / Informationsflüsse.

Zu den aufgenommenen Mechanismen ist zu bemerken, dass die Überwachung der Wissens- / Informationsflüsse einen Bezug zum operativen Geschäft und strategischen Wissensschutz haben. Wenn sich Rahmenbedingungen ändern, muss strategisch entschieden werden, wie mit den Auswirkungen auf das operative Geschäft und damit den Wissens- / Informationsflüssen umgegangen wird.

Das theoretisch entwickelte Wissensschutz-Modell mit den Mechanismen konnte auf der Grundlage der Vorinterviews zur Themenfokussierung, einem Gruppeninterview, dem *Literature Review*, der Teilnahme an Arbeitskreisen und den informellen Gesprächen entwickelt werden, das in Experteninterviews validiert und weiterentwickelt wurde. Das im *Literature Review* identifizierte Phasenmodell von MONCZKA et al. und NASSIMBENI et al. bildet den Gestaltungsrahmen des Wissensschutz-Referenzmodells für die Individual-Software-Entwicklung. Die ersten beiden Phasen, *Strategie und Planung* (Funktion 1 bis 3) sowie *Dienstleisterauswahl* (Funktion 4 und 5), sind die Basis für das Wissensschutz-Modell. MONCZKA et al. haben den drei Phasen (Tabelle 23) bereits verantwortliche Instanzen in einem Unternehmen zugeordnet.[787] Die Betrachtung des Wissensschutzes und die Funktionszuordnung auf Projektakteure fehlt jedoch in diesen Phasen. Den zwei relevanten bestehenden Phasen (erste Spalte in der Tabelle)

[787] Monczka et al. 2005 haben keine Betrachtung der Wissensgebiete, weder technisch noch fachlich, durchgeführt, auch wurden keine IT-Projekte mit externen Dienstleistern untersucht. Ebenso zu beachten ist, dass onshore oder offshore IT-Service Outsourcing ein anderes Ziel haben als die untersuchte Prinzipal-Agenten Beziehung. Die durchzuführenden Phasen sind kongruent.

werden in der Tabelle 25 die neu identifizierten Funktionen und Akteure in einer Übersicht zugeordnet. Diese im Rahmen der Arbeit neu entwickelten Funktionen werden in den folgenden Unterkapiteln detailliert beschrieben. Abweichungen und Erweiterungen zum theoretisch entwickelten Modell, die aus den Interviews in das Modell aufgenommen wurden, sind in diesem Kapitel 5 zusätzlich mit einem Stern vor dem Wort (*) gekennzeichnet.

Des Weiteren unterscheidet das Modell zwischen neuen und existierenden IT-Projekten. Eine *Dienstleisterauswahlentscheidung* in der fünften Funktion wird bei neuen IT-Projekten getroffen, bei denen ein externer Dienstleister eingesetzt werden soll. Die dritte grau dargestellte Modellphase der IT-Projektrealisierung ist nicht mehr für den strategischen Wissensschutz relevant. Sie wird deshalb bei der Modellbeschreibung nicht weiter betrachtet. IT-Beratungen haben jedoch existierende IT-Projekte, die sich in der IT-Projektrealisierung befinden. In dieser Phase *Implementierung und Monitoring* werden nach dem Modell die *Dienstleisterauswahlentscheidungen* verifiziert, indem die Informationen zu jeder Funktion (1 bis 4) erörtert werden. In der anschließenden Funktion 5 erfolgt beim Vorliegen identifizierter Risiken gegebenenfalls eine Korrektur. So kann ein anderer Dienstleister ausgewählt werden, der der Wissensschutzvorgabe der IT-Beratung entspricht.

Der Referenzmodell-Prozess mit seinen Funktionszuordnungsdiagrammen[788] wird in der Abbildung 34 in einer erweiterten ereignisgesteuerten Prozesskette (eEPK)[789] in projektunabhängige (weiß) und projektabhängige Funktionen (orange) modelliert. Damit wird die prozessuale Abfolge verdeutlicht und die zu Beginn gestellte Leitfrage beantwortet. Zudem sind rechts oberhalb, von jeder der fünf Funktionen, die adressierten Forschungsfragen (F1, F2, F3) notiert.

[788] Funktionszuordnungsdiagramme enthalten Inputdaten und Rolle (auf der linken Seite) sowie Outputdaten und Funktionalität (auf der rechten Seite).

[789] EPKs haben die Grundelemente Funktion, Ereignis und Konnektor. Diese Grundelemente verbinden gerichtete Kanten, um den Kontrollfluss abzubilden. Funktionen in einem EPK sind aktive Elemente, die bei dem Vorliegen mehrerer Prozesswege Entscheidungskompetenz besitzen. Ereignisse haben keine Entscheidungskompetenz und sind daher passive Elemente, die einen eingetretenen Zustand zum Start und zum Ende einer EPK beschreiben. Konnektoren sind Verknüpfungsknoten von Funktion und Ereignis in nicht sequentiellen EPKs, die die logischen Operatoren „und“, „inklusives oder“ und „exklusives oder“ sein können. Vgl. Lehmann 2008, S. 52, S. 65.

Tabelle 25: Wissensschutz-Referenzmodell bei der ISE[790]

Phasen (Verantwortung)	Funktionen	Akteure
1 Strategie und Planung (Aufsichtsrat, CEO, CFO)	1 Strategische Planung für Wissensschutz durchführen • IT-Projekt-Wissensschutzstrategie in Abhängigkeit von den Wissensschutzzielen und auf der Grundlage der IT-Strategie, Umfeldanalyse (Auftraggeber, Dienstleister, Mitbewerber) generieren	Strategie-manager
	2 Wissensschutz im Rahmen der Projektkategorisierung ermitteln • Informationen vom IT-Projektsteckbrief (Projekttyp, **Innovationsgrad, *Marktattraktivität, *Strategische Relevanz, *Auftraggeber Wettbewerbsfähigkeit,* Projektsituation, **Wissensschutzkategorie oder -grad* bewerten und **KO-Kriterien prüfen* • Fach- und Technologiewissensgebiete abfragen und in Matrix mit **Aufwandsbewertung in Personentagen* dokumentieren	Projekt-manager mit Führungs-kraft (Ressourcen-manager)
	3 Wissensgebiete auf Wissensschutzbedarf prüfen • Fach- und Technologiewissensbewertung nach den Kategorien (Strategie, Kundennutzen, Mitbewerberabgrenzung, Übertragbarkeit) vornehmen • Weitere Bewertungskategorien sind: Verlinkung vom Wissensgebiet zu den IT-Projekten, **Gesamtauftragsvolumen in Personentagen, *interne Expertise im Wissensgebiet, *Kernkompetenz*	Management mit Strategie-, **Kunden-management*, **fachliche und *technische Architekten*
2 Dienstleister-auswahl[791] (COO, CPO)	4 Dienstleister kategorisieren • Dienstleister-Gefahrenpotential bestimmen (Dienstleister-steckbriefe, Kategorisierung: absorptive Kapazität, Dienst-leistererfahrung (Vertrauen) • Fach- und Technologiewissensgebiete der Dienstleister nach **interner Expertise* u. externer Marktstellung bewerten	IT-Sourcing Manager mit Ressourcen-management
	5 Risikobewertung durchführen u. Dienstleister auswählen • **Risikomatrix* mit bewerteten Wissenskombinationen, IT-Projekten, Dienstleistern • Treffen der Auswahlentscheidung	**IT-Sourcing Manager,* Ressourcen-manager mit Projekt-manager
3 Implementierung und Monitoring (CPO, Führungskraft, Projekt- und Fachverantwortliche)	6 IT-Projekt umsetzen	IT-Sourcing Manager, Projekt-manager und Projektteam

[790] Eigene Darstellung.
[791] Diese Phase wurde im Arbeitsprozess von Partnerauswahl in Dienstleisterauswahl umbenannt, da es sich bei einer Prinzipal-Agenten-Beziehung nicht um gleichberechtigte Partner handelt.

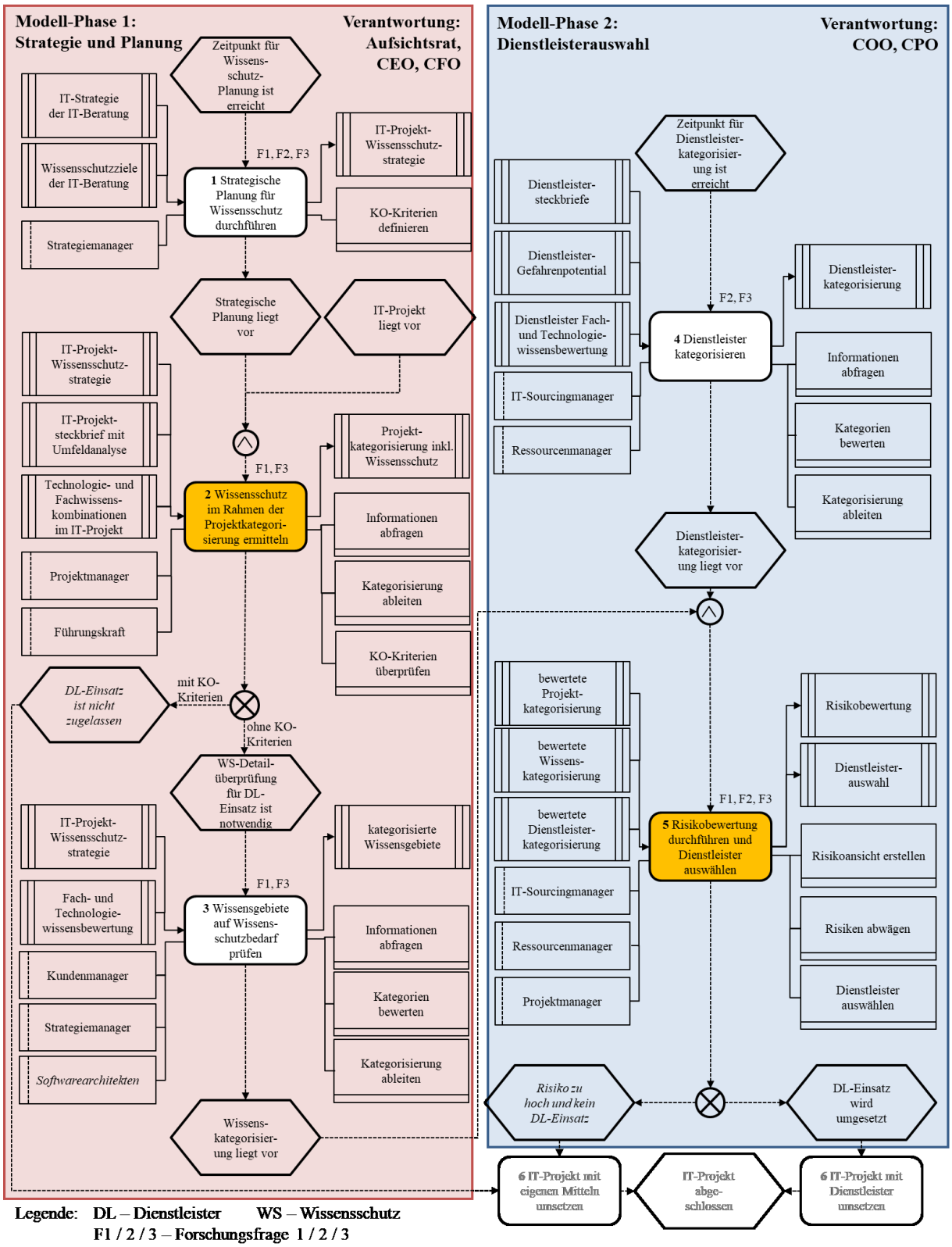

Abbildung 34: Erweiterte ereignisgesteuerte Prozesskette des Wissensschutz-Referenzmodells[792]

[792] Eigene Darstellung.

Nachdem den Phasen die Funktionen und die Akteure in Tabelle 25 und in Abbildung 34 zugeordnet wurden, wird in der Abbildung 35 der Referenzmodell-Prozess in einer EPK in projektunabhängige und projektabhängige Prozesse modelliert. Damit wird aus einer anderen Perspektive die prozessuale Abfolge verdeutlicht, die anschließend beschrieben wird.

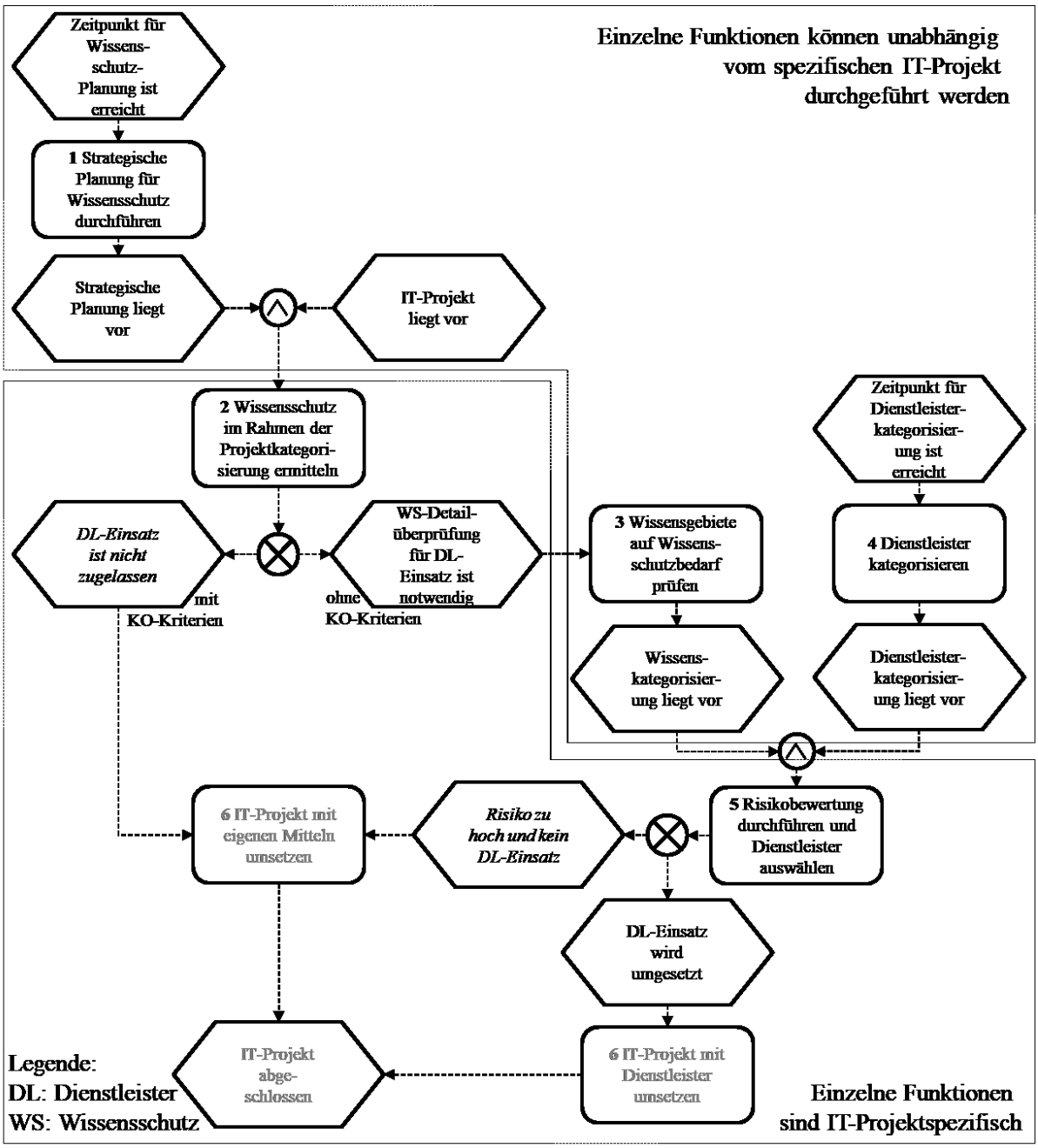

Abbildung 35: Ereignisgesteuerte Prozesskette des Wissensschutz-Referenzmodells[793]

Zu Beginn ist die *Strategische Planung* mit der IT-Projekt-Wissensschutzstrategie zu ermitteln. Die zweite Funktion stellt die Projektkategorisierung dar, bei der das IT-Projekt *mit* oder *ohne KO-Kriterien* bezogen auf den Wissensschutz kategorisiert wird. Diese *KO-Kriterien* sind in der *Strategischen Planung* von einer IT-Beratung zu definieren. Der logische Verknüpfungs-

[793] Eigene Darstellung.

operator **exklusives oder* mit den zwei möglichen Prozesswegen wurde im Rahmen der Expertenhinweise in das Modell aufgenommen und bestätigt. Bei den Projekten **mit KO-Kriterien* kann mit der IT-Projektumsetzung begonnen werden, da nach Unternehmensvorgaben keine externen Dienstleister zu involvieren sind.

Bei den IT-Projekten *ohne KO-Kriterien* sind die gegebenenfalls noch nicht erfassten Wissensgebiete in der Wissenskategorisierung zu bewerten. Parallel dazu erfolgt die Dienstleisterkategorisierung. Alle ermittelten Informationen aus den Funktionen (1 bis 4) fasst die fünfte Funktion mit der Risikobewertung und Auswahlentscheidung zusammen und visualisiert diese in einer Identifikationsmatrix. Nachdem die Risiken der möglichen Dienstleister abgewogen wurden, erfolgt eine *Auswahlentscheidung* für oder gegen den externen Dienstleistereinsatz. Im Anschluss an diese Funktion startet die IT-Projektumsetzung.

Damit die Nachvollziehbarkeit und die Abhängigkeit zwischen den Funktionen verdeutlicht wird, werden die IT-Projektabhängigen bzw. -unabhängigen Funktionen in einer tabellarischen Übersicht dargestellt (Tabelle 26).

Tabelle 26: IT-Projektabhängige und –unabhängige Funktionen[794]

IT-Projektunabhängige Funktionen	IT-Projektabhängige Funktionen
• 1 Strategische Planung für Wissensschutz durchführen →	• 2 Wissensschutz für IT-Projekt ermitteln (Kategorisierung)
• 3 Wissensgebiete auf Wissensschutz-Bedarf prüfen (Kategorisierung)	
• 4 Dienstleister kategorisieren →	• 5 Risikobewertung durchführen und Dienstleister auswählen
	• 6 IT-Projekt umsetzen

Aufgenommene Hinweise der Interviewpartner in das Modell

Im Rahmen der Interviews und der Evaluation vom entwickelten Modell, wie bereits weiter oben dokumentiert, wurde das Modell bei jedem Interview bewertet und nach jedem Interview der Leitfaden um Änderungshinweise und relevant erachtete Kategorien erweitert. In der Tabelle 27 sind die aufgenommenen Hinweise aufgeführt, die in den Folgeinterviews besprochen und validiert wurden. Alle anderen Modellbestandteile bestätigten die Interviewpartner und sind in dieser Tabelle nicht aufgeführt. Auch die Anpassungen an den Akteuren für die Wissenskategorisierung (Funktion 3) sind in der Tabelle 27 nicht aufgeführt, weil jeder Interviewpartner seine Expertise zu den Bewertungskategorien äußern sollte, bevor eine Anpassung erfolgen konnte. Die Rückmeldungen zu den Akteuren sind in der Tabelle 32 dokumentiert und wurden nach dem Abschluss der Interviews ausgewertet, damit die Akteure präzisiert werden konnten. Die Zuordnung zu den fünf Funktionen ist vor jedem Punkt mit F1 bis F5 abgekürzt. In den folgenden Unterkapiteln 5.2 und 5.3 ist das Modell mit seinen Änderungen im Detail beschrieben.

[794] Eigene Darstellung.

Tabelle 27: Modellerweiterungen im Interviewprozess[795]

IP	Aufgenommene Modell-Hinweise der Interviewpartner
1	• F3: Begriffsdefinition Übertragbarkeit um Erfahrungswissen der Mitarbeiter erweitern • F3: Begriffsdefinition Kundennutzen um Endanwendernutzen erweitern • F3: Akteur Personalmanagement durch Kundenmanagement ersetzen • F4: Auftragsvolumen des Dienstleisters zum Wissensgebiet in Personentagen aufnehmen • F4: Wirtschaftliche Lage des Dienstleisters im Steckbrief dokumentieren
2	• F3: Kennzeichnung von schützenswerten Wissensgebieten für die keine Sourcing-Anfragen gestellt werden dürfen • F4: 360° Feedback zur Bewertung des Dienstleisters (Lernbereitschaft, -fähigkeit, Innovationsfähigkeit, Erfahrung) heranziehen
3	• F2: um Marktattraktivität / Marktwachstum / Innovationsgrad erweitern • F3: Kundenbeitrag in der Definition Kundennutzen konkretisieren • F4: Zeitdauer der Zusammenarbeit mit dem Dienstleister in den Steckbrief aufnehmen • F5: Hinweis auf notwendige Anpassung der Risikobewertung für die Managersicht
4	• F2: Kombinationen der Technologiewissensgebiete macht das Alleinstellungsmerkmal aus • F2: Weitere Projektart aufnehmen: prototypische Entwicklung • F2: Hinweis auf KO-Kriterien zum Einsatz des Wissensschutzmodells, zum Beispiel strategische Bedeutung des IT-Projektes • F3: Interne Expertise zum Wissensgebiet und die Ressourcenverfügbarkeit, die dieses Wissensgebiet hat, aufnehmen • F4: Definition Dienstleistererfahrung um Qualität / Arbeitsqualität im Vergleich zum Vertrauen erweitern • F4: Besondere Vertragskonstrukte mit dem Auftraggeber in den Dienstleistersteckbrief aufnehmen
5	• F3: Zur Bewertung der internen Expertise des Wissensgebietes aufnehmen, wie viele interne Mitarbeiter können das Wissensgebiet bearbeiten • F5: Wertschöpfungstiefe der IT-Beratung (Eigenfertigung) und des Dienstleisters mit prozentualem Anteil am Projekt dokumentieren • F5: Interpretationshilfe für Risikobewertung entwickeln
6	• F3: Analysen zu den Wissensgebieten können auch für den zukünftigen Ressourcenaufbau genutzt werden • F3: Abgleich, ob das Wissensgebiet zu einer Kernkompetenz gehört • F4: Dienstleistergröße in Zwischenstufen einteilen: Global Player, Mittelständler, Fachkraftvermittler • F4: Mischformen der Dienstleister berücksichtigen • F4: Umbenennung der Projektrolle vom Dienstleister in interne Expertise
7	• F2: In der Projektkategorisierung kennzeichnen, ob es eine unternehmenskritische Anwendung betrifft • F3: Kennzeichnen, ob das Fach- oder Technologiewissensgebiet zukunftsweisend ist – Strategiedefinition (Bewertungskategorie) erweitert
8	• F2: Anstatt die konkreten IT-Projekte könnten auch die IT-Programme bewertet werden • F2: Bestätigung zu Projektsteckbrief erweitern um Innovationsgrad, Vertraulichkeit und Schutzbedarf • F4: Dienstleister-Auftragsvolumen mit Angabe der Jahreszahl dokumentieren
9	• F2: Bestätigung der KO-Kriterien und Hinweis auf Nogo-Projekte mit Dienstleistereinsatz

[795] Eigene Darstellung.

10	• F2: Wissensgebiete in unternehmensspezifisches / branchenspezifisches Wissen kategorisieren. Fachwissen in spezifisches Know-how und allgemeingültiges unterteilen. • F3: Definition Kundennutzen um die Wirksamkeit auf Endkunden erweitern • F4: Im Dienstleistersteckbrief Interesse an bestimmten Wissensgebieten dokumentieren • F5: Bestätigung zu Handlungsbedarf kennzeichnen und Steuerungsgrößen festlegen
11	• F2: Alleinstellungsmerkmal als Projektkriterium aufnehmen • F4: In den Dienstleistersteckbrief aufnehmen, ob die Dienstleistung an einen Subauftragnehmer weitergegeben werden darf und Wachstum des Dienstleisters in den letzten Jahren dokumentieren

Modellbeschreibung ohne Skalen

Das im folgenden beschriebene Referenzmodell wird ohne Skalen beschrieben. Für die zwei praxisnahen konstruierten IT-Projekte im IV-Leitfaden wurde eine fünfer Likert-Skala zu Illustrationszwecken eingesetzt, da sich in der IT-Beratung fünfer und siebener Skalen bei anderen Unternehmensbewertungen etabliert haben. Einige Experten stimmten der Skala der Wissenskategorisierung zu. Andere Interviewpartner hatten eine höhere oder eine geringere Likert-Skala empfohlen und bevorzugten zum Teil eine gerade Skala, damit sich der ausfüllende Bewerter in der Mitte der Skala für eine Tendenz entscheiden muss. Aus diesem Grund wird empfohlen, dass jede IT-Beratung ihre Skalen für die Bewertungskategorien selbst festlegt und diese an die bestehenden Bewertungsskalen in der jeweiligen IT-Beratung angleicht. Die Projektakteure sollten die gleichen Maßstäbe wie bei anderen Bewertungen innerhalb der IT-Beratung ansetzen. Hingewiesen wurde auf die einheitlichen Skalen für die Bewertenden, damit nicht unterschiedliche Annahmen vorliegen.

Ein Anliegen einiger Interviewpartner[796] bezog sich auf den pragmatischen Ansatz des Modells und die Berechnung. Die Aussagen dazu sind im Folgenden zusammengefasst:

- Die Interviewpartner avisierten eine gering abgestufte Bewertungsskala und zum Teil ohne einen möglichen Mittelwert. Auf der anderen Seite soll das Ergebnis abgestuft sein, damit die Dienstleister spezifiziert bewertet werden können.
- Um komplizierte Berechnungen oder Berechnungsformeln zu umgehen und die Transparenz zu fördern, könnte aufgrund der Vorstellung einiger Interviewpartner 100 Punkte oder 100 Prozent vergeben werden. Das heißt, wenn eine der vier Kategorien bei der Wissenskategorisierung zum Beispiel 25% Wertigkeit hat, dann können insgesamt 25 Prozentpunkte als Maximalwert vergeben werden. Damit ist eine detailliertere Abstufung möglich.
- Diese Bewertung nach den Prozentpunkten würde zur Vergleichbarkeit zwischen den Dienstleistern und den Wissensgebieten beitragen und sobald definierte Prozentwerte über- oder unterschritten werden, wird Handlungsbedarf notwendig.

5.2 Referenzmodell-Phase 1: Strategie und Planung

Nach MONCZKA et al. ist für die Phase *Strategie und Planung* der Aufsichtsrat, Chief Executive Officer (CEO) und Chief Financial Officer (CFO) verantwortlich. Diesen Verantwortlichen müssen die Ergebnisse der ersten drei Funktionen vorgestellt werden um die weiteren Maßnahmen zu definieren. In diesem Unterkapitel werden diese drei Funktionen beschrieben:

[796] Vgl. IP_2, IP_5, IP_8.

- Funktion 1: Strategische Planung für Wissensschutz durchführen
- Funktion 2: Wissensschutz im Rahmen der Projektkategorisierung ermitteln
- Funktion 3: Wissensgebiete auf Wissensschutzbedarf prüfen

Nach CHAN & LEE gibt es für die Bewertung des Wissens einen Top-down und einen Bottom-up Ansatz.[797] Bei dem entwickelten Modellansatz wird in der strategischen Planung (Funktion 1) im Top-Down Ansatz die IT-Projekt-Wissensschutzstrategie ermittelt. Nach der Identifikation der Fach- und Technologiewissensgebiete innerhalb der Projektkategorisierung (Funktion 2) bewerten die ermittelten Akteure im Bottom-up Ansatz die Wissensgebiete (Funktion 3) nach den identifizierten Bewertungskategorien.

5.2.1 Funktion 1: Strategische Planung für Wissensschutz durchführen

Die Aufarbeitung der Informationen für die Funktion 1, eruieren die Strategiemanager, die vom CEO gesteuert werden. Im Abschnitt 4.2.2 wurde die relevante Literatur zu der strategischen Abhängigkeit der Wissensschutzziele erörtert. Die Ziele, die sich IT-Beratungen für ihre IT- und (Out-)Sourcing-Strategie definieren sind demnach dependent von Unternehmensgröße / -art, Branche, Marktaktivitäten, Rechtssystem, Wissensart, organisationaler Kultur und individuellem Hintergrund. Diese Funktion basiert auf diesen Erkenntnissen.

Zum Themengebiet des Outsourcings gibt es umfangreiche Forschungsliteratur. Grundgedanken in der (Out-)Sourcingforschung sind, dass die Ziele transparent und nachvollziehbar sind und dass eine IT-Strategie vorliegt. Des Weiteren haben sich mehrere Autoren für Regeln, Verfahren und Richtlinien zum Wissensaustausch ausgesprochen.[798]

Funktion Strategische Planung für Wissensschutz durchführen (Abbildung 36)

Die Funktion ermittelt die Rahmenbedingungen, die in einer IT-Beratung vorliegen und die Auswirkung auf die Gestaltung der IT-Projekt-Wissensschutzstrategie haben. Neben der vorhandenen IT-Strategie gehören dazu die definierten Wissensschutzziele. Der Begriff der IT-Projekt-Wissensschutzstrategie ist auf einen Hinweis von einem Interviewpartner zurückzuführen.[799]

[797] Vgl. Chan & Lee 2011, S. 98 ff.
[798] Vgl. Ahmad et al. 2014, S. 30.
[799] Vgl. IP_7.

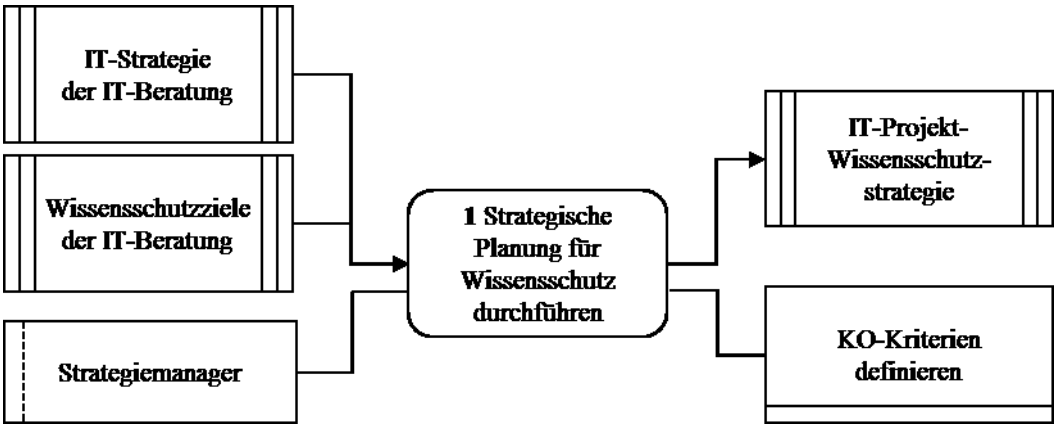

Abbildung 36: Funktion Strategische Planung für Wissensschutz durchführen[800]

In der Definitionsphase von IT-Projekten haben sich Umfeldanalysen etabliert.[801] Damit werden die Einflussfaktoren auf die IT-Projekte und die IT-Beratung transparent und sichtbar. Diese Umfeldinformationen geben Hinweise zum notwendigen Wissensschutz und sind Voraussetzung für die Erarbeitung der Wissensschutzziele, zum Beispiel nach Kundensegmenten. Diese Analysen überschneiden sich mit der Funktion Projektkategorisierung, die im nächsten Abschnitt erläutert wird. Diese Umfeldanalysen sind in der Funktion 1 im Allgemeinen und in der Funktion 2 im spezifischen IT-Projekt präsent. Die Projektumfeldfaktoren klassifizieren sich nach ELLMANN et al. in interne und externe Faktoren (Tabelle 28):[802]

Tabelle 28: Tabellarische Darstellung des Projektumfeldes[803]

	Intern	Extern
Sachlich	Betriebsvereinbarung Projektmanagement-Handbuch Richtlinien Umsatzentwicklung	Gesetze Normen und Standards RFC (Request for Comments) Marktentwicklung
Sozial	Betriebsrat Beauftragte (z. B. QM, Sicherheit) Vorstand, Abteilungsleiter Mitarbeiter (außerhalb des Projektes)	Auftraggeber (AG) Mitarbeiter der AG-Organisation Lieferanten Kunden

Die Erarbeitung der Umfeldanalyse ist Voraussetzung für die anschließende Stakeholderanalyse bei der die sozialen Faktoren betrachtet werden.[804] Die Stakeholderanalyse fokussiert die Stakeholder im Projekt und im internen und externen Umfeld.[805] Zudem sind für die weiteren Stakeholder wie Auftraggeber und Mitbewerber Steckbriefe zu erstellen. Um diese Informationen zu erhalten, muss der Strategiemanager als Hauptakteur den IT-Sourcing Manager und den Kundenmanager hinzuziehen. Diese Analysen sind notwendig, damit eine IT-Projekt-Wis-

[800] Eigene Darstellung.
[801] Vgl. Ellmann et al. 2009, S. 88.
[802] Vgl. Tabelle 28.
[803] Ellmann et al. 2009, S. 88.
[804] Vgl. Ellmann et al. 2009, S. 89.
[805] Vgl. Ellmann et al. S. 89.

sensschutzstrategie für die Dienstleister, Auftraggeber und damit für die verschiedenen Kundensegmente vorliegen. Mit der definierten IT-Projekt-Wissensschutzstrategie wird die Basis für die folgende Projekt- und Wissenskategorisierung gelegt.

In der IT-Projekt-Wissensschutzstrategie muss zudem dokumentiert werden, dass bestimmtes Wissen absolut nicht diffundieren darf, also zum Beispiel nach Schweregraden unterscheiden.[806] Um die Alleinstellungsmerkmale einer IT-Beratung zu verlieren reicht oft schon ein Wissensbaustein für einen Dienstleister aus, der die Initialzündung für die Lösung eines komplizierten Problems liefert.[807] Die Alleinstellungsmerkmale und damit die Wettbewerbsfähigkeit sind auf den erarbeiteten Wissensvorsprung der untersuchten IT-Beratung zurückzuführen. Diese liegen darin, dass sie weiß, wie die Geschäftsprozesse ihrer Auftraggeber funktionieren, welche Themen und Probleme zu lösen sind und wie diese Themen weiterentwickelt werden können.[808] Das einzelne Technologiewissen hat kein Alleinstellungsmerkmal, jedoch wie eine IT-Beratung gewisse Technologien miteinander kombiniert.[809]

Für das Modell bedeutet das, dass Managementvorgaben zum Dienstleistereinsatz und schützenswertem Wissen aus strategischer Perspektive in einer konkreten IT-Projekt-Wissensschutzstrategie[810] definiert werden, damit die Austauschbarkeit[811] einer IT-Beratung durch einen externen Dienstleister nicht unterstützt wird. Besonders strategisch geprüft werden müssen systemrelevante IT-Projekte, die auf die regionale Wirtschaft Auswirkungen haben, damit mögliche Nachteile für den Auftraggeber und eine IT-Beratung in Bezug auf den Wissensschutz ausgeschlossen werden.[812]

5.2.2 Funktion 2: Wissensschutz im Rahmen der Projektkategorisierung ermitteln

Identifizierte Akteure für diese Funktion sind der Projektmanager mit seinem Management. FEENY & WILLCOCKS untersuchten im Rahmen vom IT-Outsourcing die Kernfähigkeiten für Informationssysteme. Als Ergebnis zählen sie die Projektmanagement-Kompetenz zu den organisatorischen Kernkompetenzen, die nicht an einen Dienstleister im Rahmen eines Projektes outgesourct werden dürfen.[813] Demnach ist die Projektkategorisierung durch einen internen Projektmanager durchzuführen. Der Projektmanager ist für den Erfolg des IT-Projektes zuständig und verantwortet die Ressourcenentscheidungen sowie die Risiken. Die Interviewpartner bestätigten diese Sichtweise, dass Ressourcenentscheidungen nur durch interne Projektmanager

[806] Vgl. IP_3.
[807] Vgl. IP_3.
[808] Vgl. IP_4.
[809] Vgl. IP_4.
[810] Vgl. IP_7.
[811] Vgl. IP_5.
[812] Vgl. IP_2.
[813] Vgl. Feeny & Willcocks 1998, S. 15 f.

erfolgen dürfen.[814] Für diese Funktion wird im Wesentlichen die Praxiserfahrung des Verfassers genutzt, da die Forschungsliteratur zum Wissensschutz und dem Projektgeschäft sowie speziell in der Prinzipal-Agenten-Beziehung kaum bis keine Hinweise gibt.

Funktion Wissensschutz für IT-Projekt ermitteln (Abbildung 37)

Die Voraussetzung für die Bestimmung der Projektkategorisierung sind die IT-Projekt-Wissensschutzstrategie, der bewertete Projektsteckbrief und die Technologie- und Fachwissenskombinationen in dem zu prüfenden IT-Projekt. Ein IP merkte an, dass die Projektkategorisierung aus der Projektperspektive oder der Kundenperspektive durchgeführt werden kann und dass die eingenommene Perspektive dokumentiert werden muss.[815]

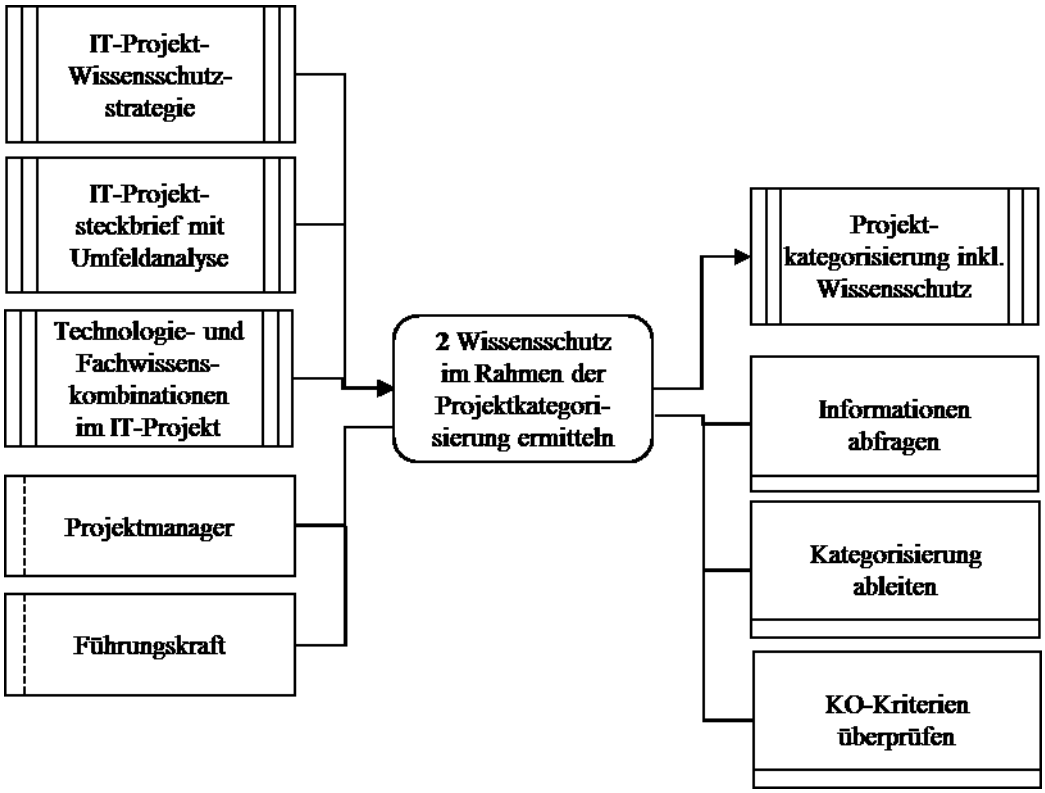

Abbildung 37: Funktion Wissensschutz für IT-Projekt ermitteln (Kategorisierung)[816]

Bei der Projektkategorisierung müssen die bestehenden und die neuen IT-Projekten betrachtet werden:

- Bestehende IT-Projekte: werden im Ist-Zustand kategorisiert. Mögliche Entscheidungen oder Entscheidungsempfehlungen können erst getroffen werden, wenn die weiteren Analysen für die Risikobewertung vorliegen.
- Neue IT-Projekte: werden kategorisiert und der Bedarf an externen Dienstleistern dokumentiert. Eine Entscheidung zum Dienstleistereinsatz kann erst nach den weiteren Analysen von Wissenskategorisierung, Dienstleisterkategorisierung und Risikobewertung erfolgen.

Für neu bewertete Projekte muss der Bedarf an externem Dienstleistereinsatz formuliert werden, damit mögliche Dienstleister in der Dienstleisterkategorisierung vorausgewählt werden

[814] Vgl. IP_9.
[815] Vgl. IP_7.
[816] Eigene Darstellung.

können. In bestehenden Projekten sind bereits Dienstleister im Einsatz, deren Wissensrisiko in der Risikobewertung nach erfolgter Bewertung ersichtlich ist.

IT-Projektsteckbrief

Im Abschnitt 2.2.1 wurden die fünf Projektmanagementphasen beschrieben. Nach dieser Übersicht wird transparent, dass in den ersten beiden Phasen, der Initialisierungsphase und der Definitionsphase ein Projektsteckbrief erarbeitet wird. In der untersuchten IT-Beratung werden bereits solche Projektsteckbriefe ausgefüllt, um eine Projektkategorisierung für das Management vorzunehmen. Dieser Projektsteckbrief enthält jedoch nicht die für den Wissensschutz relevanten Faktoren, beziehungsweise werden diese nicht für den Wissensschutz ausgewertet. Ein Projektsteckbrief ist in der Regel ein standardisiertes Dokument in einer Projektmanagementorganisation und kann als Zusammenfassung der Projektdefinition angesehen werden.[817] Für den Inhalt des Projektsteckbriefes existiert keine Norm und auch das Layout ist nicht standardisiert.[818] Mögliche Projektsteckbrief-Inhalte für IT-Projekte aus der praktischen Erfahrung sind:[819]

- Projektname, -nummer, -typ, -dauer, -kosten, -fokus, -vorgehen, -führende Abteilung
- Projektansprechpartner: Projektmanager, Account- / Kundenmanager, Auftraggeber
- Angebotsaufwand nach Schätzung und Istaufwand
- Auftraggeber: Beziehung, Funktion, Business Impact, Projektkritikalität, Beschlüsse
- Projekt: Erreichbarkeit vom Projektziel, Formulierung der fachlichen Anforderungen
- Kritikalität und Risiken: Zusagen zu Time / Scope / Budget, unternehmenskritische Anwendung, Ausschreibung, Projektverantwortung
- Vorgehen und Technologie: Kompetenz beim Projekt / Dienstleister / Auftraggeber, Schnittstellen zu anderen Projekten / Anwendungen, Anzahl der betroffenen Projekte
- Personalplanung: Eigenfertigungsquote, Einsatz von Keyplayern und besonderer Expertise, notwendiger Einsatz von externen Dienstleistern, Anzahl der Projektmitarbeiter, Reifegrad vom Projektteam

Weitere Beispiele für projekt- und organisationsbezogene Projektsteckbriefergänzungen sind „Ausgangslage, Projektanlass, kritische Erfolgsfaktoren, gegebene Voraussetzungen, Randbedingungen, Mitwirkung des Kunden“.[820]

Um das Projekt für den Wissensschutz zu kategorisieren, muss dieser Projektsteckbrief um die folgenden relevanten Kategorien ergänzt werden (Tabelle 29). Die mit Stern (*) und kursiv markierten Bewertungskategorien ergänzen das theoretisch entwickelte Modell und haben nach Auffassung der Interviewpartner eine Wissensschutzrelevanz. Hinweise wurden notiert, in den Folgeinterviews diskutiert und von den Interviewpartnern in den Folgeinterviews für valide bestimmt. In der Spalte Referenz sind die Interviewpartner (IP) oder die Quellen benannt, die die neuen Kategorien eingeführt und präzisiert haben.

[817] Vgl. Duncan & Dörrenberg 2009, S. 595, Motzel 2006, S. 152.
[818] Duncan & Dörrenberg 2009, S. 595.
[819] Vgl. Inhalte vom Projektkategorisierungsblatt der untersuchten IT-Beratung.
[820] Duncan & Dörrenberg 2009, S. 595.

Tabelle 29: Relevante Wissensschutz Informationen im IT-Projektsteckbrief[821]

Kategorie	Inhalt der Bewertung	Referenz (IP)
Projekttyp	Neuentwicklungsprojekt Wartungsprojekt Weiterentwicklungsprojekt **prototypische Entwicklung (F&E)*	4
**Marktattraktivität (Marktwachstum)*	**zukunftsweisend / Standardgeschäft / Auslaufmodell, unternehmensspezifisches / branchenspezifisches Wissen*	3, 10
**Innovationsgrad*	**hat Einfluss auf den Wissensschutzbedarf, dazu werden die Alleinstellungsmerkmale vom IT-Projekt gekennzeichnet*	3, 8, 11
**Strategische Relevanz*	**strategische Einordnung vom Projekt auf der Grundlage der IT-Projekt-Wissensschutzstrategie*	Vorinterview[822]
**Unterstützt Wettbewerbsfähigkeit*	**bewertet das IT-Projekt, damit die IT-Beratung / der Auftraggeber ihre Wettbewerbsfähigkeit halten und langfristig sichern. Dient zur Prävention ungewollter Wissensdiffusion.*	IV-Leitfaden
Fachwissensgebiete	Benennung des Geschäftsprozesswissens in der Auftraggeberbranche	
Technologiewissensgebiete	Benennung des verwendeten Technologiewissens der IT-Beratung	
Externe Dienstleister	ausfüllbar in bestehenden IT-Projekten, für neue Projekte erst nach der Rücksprache mit dem Ressourcenmanagement und IT-Sourcing Management ausfüllbar (Wissenskategorisierung, Dienstleisterkategorisierung).	
Projektsituation	Beschreibung besonderer Gegebenheiten zum Beispiel Umfeldanalyse für Risikobewertung, **interne Ressourcenverfügbarkeit bewerten*	4
**Wissensschutzkategorie oder -grad*	**Notwendigkeit an Wissensschutz nach definierten Kriterien und KO-Kriterien für den externen Dienstleistereinsatz definieren*	4, 5, 8, 9, 11

Kategorien: Projekttyp, Marktattraktivität (Marktwachstum), Innovationsgrad

Der Projekttyp gruppiert das IT-Projekt für den Wissensschutz nach Komplexität und Neuartigkeit ein,[823] da Neuentwicklungsprojekte wegen ihrem möglichen Innovationsgrad tendenziell genauer zu betrachten sind als bestehende Projekte. Jedoch müssen ebenso die bestehenden IT-Projekte, die sich in der Entwicklung, Wartung und Weiterentwicklung befinden, auf den Wissensschutz hin geprüft werden. Der Projekttyp **prototypische Entwicklung* kommt zum

[821] Eigene Darstellung.
[822] Aus einem Vorinterview mit zwei IT-Sourcing Experten.
[823] Vgl. Koch et al. 1991, S. 36 f.

Einsatz bevor eine umfangreiche Neuentwicklung durchgeführt wird.[824] Ein anderer Interviewpartner bezeichnet diesen Projekttyp als F&E.[825]

Die **Marktattraktivität (Marktwachstum)* kategorisiert das Projekt, ob es zukunftsweisend ist, zum Standardgeschäft gehört oder ein Auslaufmodell ist. In einem neuen attraktiven Markt ist Wissensschutz bedeutsamer als in einem bestehenden Markt.[826] Zu der **Marktattraktivität* gehört die Eingruppierung, ob das Wissen vom IT-Projekt als **unternehmensspezifisch* oder **branchenspezifisch* gesehen wird. Ein anderer Interviewpartner beschränkte die Bewertung des Fachwissens auf **spezifisch* oder **allgemeingültig*.[827] Das branchenspezifische Wissen hat einen allgemeingültigeren Charakter und kann auch anderen Auftraggebern hilfreich sein. Das unternehmensspezifische Wissen ist lediglich auf diesen einen Auftraggeber anwendbar und wäre damit nicht im Fokus des Wissensschutzes.

In den Interviews gab es zum einen Hinweise, dass die **Alleinstellungsmerkmale* vom Projekt zu charakterisieren sind.[828] Zum anderen besteht Bedarf an der Kategorisierung der Vertraulichkeit und damit vom Schutzbedarf.[829] Diese Eingruppierungen werden in dem Modell bei der Kategorie **Innovationsgrad* zusammengefasst.[830] Bei einem Projekt mit einem hohen *Innovationsgrad* muss dem Wissensschutz besondere Aufmerksamkeit zugeordnet werden.

Kategorien: Fachwissen und Technologiewissen

Nach OLANDER et al. ist das wertvollste und schützenswerteste Vermögen einer IT-Beratung das Humankapital (Fachwissen) und das technische Wissen (Technologiewissen).[831] Diese Aussage fundamentiert sich in dem Modell als das Technologiewissen und das Fachwissen von IT-Beratungen. Jeder ISE können identifizierte Technologiewissensgebiete und Fachwissensgebiete zugeordnet werden. Diese Kernbegriffe werden für das Modell folgend definiert:

- **Technologiewissen:** befähigt die IT-Beratung die Informationssysteme auf einer technologischen Basis zu implementieren.
- **Fachwissen:** ist das aufgebaute Humankapital in Form des Arbeits- und Geschäftsprozesswissens in der Auftraggeber-Branche.

Das Fachwissen wird vom Auftraggeber in Form von Geschäftsprozesswissen zugeliefert und mit dem Technologiewissen in einer Anwendung umgesetzt.[832] Damit die Vergleichbarkeit vom Fachwissen über alle IT-Projekte in der IT-Beratung gewährleistet wird, besitzt das Fachwissen einen Branchenbezug.

---

[824] Vgl. IP_4.
[825] Vgl. IP_11.
[826] Vgl. IP_3.
[827] Vgl. IP_10.
[828] Vgl. IP_11.
[829] Vgl. IP_8.
[830] Vgl. IP_3.
[831] Vgl. Olander et al. 2011, S. 606.
[832] Vgl. IP_10.

Projektsituation

Der verantwortliche Projektmanager ist angehalten die Projektsituation zu dokumentieren. Das bedeutet, dass das Auftraggeberumfeld oder besondere Gegebenheiten im Projekt erfasst sind. So kann in einem bestehenden Projekt der Projekterfolg zum Beispiel vom externen Dienstleister abhängig sein. Eine personelle Änderung würde zum Projektzeitverzug führen und diese wiederum zu Vertragsstrafen. Da die Auswirkungen komplex sein können, sollte die vorliegende Projektsituation im Rahmen der Risikobewertung (Abschnitt 5.3.2) herangezogen werden. Der verantwortliche Projektmanager und sein Management erhalten damit Hinweise auf zu prüfende Risikofaktoren.

In die Projektsituation ist die Ressourcenverfügbarkeit der eigenen Wissensträger aufzunehmen.[833] Wenn das Wissen in einer IT-Beratung zwar verfügbar ist, aber alle Ressourcen die das *Know-How* besitzen in IT-Projekten gebunden sind, dann erhält das Management die Begründung, dass für dieses Wissensgebiet eigene Mitarbeiter aufgebaut oder externe Dienstleister eingebunden werden müssen.[834] In diesem Szenario ist der Wissensschutzbedarf zu begutachten.

Wissensschutzkategorie / -grad und KO-Kriterien

Die IT-Projekte müssen vorselektiert werden um zu definieren, wie viel Wissensschutz nach der IT-Projekt-Wissensschutzstrategie notwendig ist.[835] Die IP bezeichneten diesen als **Wissensschutzgrad*[836] oder **Wissensschutzkategorie*[837] vom IT-Projekt. Zudem sind **KO-Kriterien* für IT-Projekte zu definieren, in die Dienstleister nicht disponiert werden dürfen.[838] Besonders in hochstrategischen IT-Projekten ist kein externer Dienstleister zu involvieren.[839] Diese Wissensschutzkategorisierung selektiert die IT-Projekte, damit werden bei einem hohen *Wissensschutzgrad* oder *-kategorie* weitere Detailbetrachtungen zum Wissensschutz optional.

Für die Vorselektierung können zum Beispiel die Kategorien **Innovationsgrad, *Marktattraktivität, *strategische Relevanz* und **Wettbewerbsfähigkeit* genutzt werden. Nach der erfolgreichen Projektkategorisierung müssen die Ergebnisse (aus dieser Funktion) ebenso den verantwortlichen Aufsichtsrat, CEO und CFO bekannt sein. Besonders entscheidend ist eine Beteiligung bei Projekten, die die qualifizierten Wissensschutzkriterien erfüllen. Diese **KO-Kriterien* oder Grenzwerte, die ein Projekt zu einem schützenswerten Objekt werden lassen, muss jede IT-Beratung selbst definieren.

---

[833] Vgl. IP_4.
[834] Vgl. IP_4.
[835] Vgl. IP_11.
[836] Vgl. IP_11.
[837] Vgl. IP_8.
[838] Vgl. IP_9, IP_11.
[839] Vgl. IP_5.

Verhältnis zwischen Fach- und Technologiewissen in der untersuchten IT-Beratung

In den Experteninterviews wurde die Gewichtung des Fach- und Technologiewissens für den Wissensschutz in der IT-Beratung diskutiert. Die Ergebnisse sind in der folgenden Übersicht zusammengefasst.

Tabelle 30: IV-Ergebnis Verhältnis Fachwissen Technologiewissen[840]

IP	Verhältnis Fachwissen Technologiewissen, Begründung der IP
1	60:40, weil: • Fachwissen ist für unser Ziel als Enabler wichtiger • Technologiewissen werden wir vom Markt holen, wenn wir keine Zukunft für das Technologiewissen sehen
2	50:50, weil: • abhängig von den Unternehmenszielen (Innovationsgeber, Integrator, Trusted Advisor)
3	70:30, weil: • Fachwissen befähigt uns den Kunden zu verstehen • Technologiewissen können tausende IT-Beratungen besitzen
4	70:30, weil: • Fachwissen hat viel mit Erfahrung und Kundenwissen zu tun • Technologiewissen können wir eher zukaufen
5	80:20 oder 75:25, weil: • Fachwissen unterscheidet uns von anderen IT-Beratungen • Technologiewissen unterscheidet uns nicht
6	60:40 oder 70:30, weil: • Fachwissen ist Alleinstellungsmerkmal und Differenzierungsmerkmal gegenüber Mitbewerbern • Technologiewissen ist breiter gestreut
7	40:60, weil: • Geschäftsprozesswissen befähigt zum Verständnis
8	66:33, weil: • Fachwissen beinhaltet die persönliche Beziehung zum Kunden • Technologiewissen ist tägliches Werkzeug und lässt sich leichter akquirieren
9	60:40 oder 70:30, weil • Fachwissen kann *USP* haben • Technologiewissen ist *commodity*
10	60:40, weil: • Fachwissen ist für unsere zukünftige Strategie als *Integrator* wichtiger
11	60:40, weil: • Fachwissen, Geschäftswissen, Prozesskenntnisse, das muss man sich über lange Jahre erarbeiten • Technologiewissen ist austauschbarer

Das Fachwissen wird von nahezu allen Experten als wertvoller und damit als schützenswerter gesehen, da die Alleinstellungsmerkmale der untersuchten IT-Beratung darauf aufgebaut wer-

[840] Eigene Darstellung.

den. Ein IP hat das Verhältnis 50:50 bewertet und dieses in Abhängigkeit zu den Unternehmenszielen gesetzt.[841] Abweichend beurteilte ein IP das Fachwissen zum Technologiewissen mit dem Verhältnis 40:60, jedoch korrigiert seine verbale Begründung das Verhältnis zugunsten des Fachwissens.[842] Bei einem Technologiehersteller oder einem produzierenden Unternehmen, zum Beispiel einem Maschinenbauer, würde das Technologiewissen bedeutsamer und somit schützenswerter sein, merkte ein Interviewpartner an.[843] Die Interviewpartner interpretierten das Fachwissen im Zusammenhang mit Erfahrungswissen, Geschäfts(prozess)wissen, Prozesskenntnissen und Kundenwissen. Hingegen wird das Technologiewissen in Verbindung mit Werkzeug, *commodity* und Austauschbarkeit definiert. Das Technologiewissen ist im Vergleich zum Fachwissen in der IT-Branche leichter zu streuen. Das Fachwissen bedingt Geschäftswissen und Prozesskenntnisse, die über mehrere Jahre erarbeitet werden müssen.[844] Das ältere durch jahrelange Erfahrung gewonnene Technologiewissen und Fachwissen in IT-Projekten ist wertvoll und schützenswert, weil es gering verfügbar und oft nicht ersetzbar ist. Hingegen hat ein verbreitetes Technologiewissen eher eine geringere Bedeutung.

Technologie- und Fachwissenskombinationen im IT-Projekt

Im zweiten Schritt der Projektkategorisierung sind die Kombinationen vom Fachwissen und Technologiewissen in der Projektkategorisierungsmatrix einzutragen, um die Wissenskombinationen des IT-Projektes darzustellen. Diese Matrixsichtweise ist die Grundlage für das Modell. Die Matrix kann wie folgt dargestellt werden:

Tabelle 31: Projektkategorisierung nach Technologie-/Fachwissen im IT-Projekt[845]

Technologiewissen / Fachwissen	Technologiewissen 1	Technologiewissen 2	Technologiewissen n
Fachwissen 1	--	*300 PT*	*250 PT*
Fachwissen 2	*200 PT*	--	--
Fachwissen n	--	*100 PT*	*500 PT*

In den Experteninterviews wurde die Relevanz der geschätzten Personentage (PT) pro Kombination für die Projektrealisierung neben der Kennzeichnung der Fach- und Technologiewissenskombination protokolliert.[846] Damit wird die Komplexität der ISE deutlich und der Bedarf an internen oder externen Mitarbeitern wird transparent.

[841] Vgl. IP_2.
[842] Vgl. IP_7.
[843] Vgl. IP_3.
[844] Vgl. IP_11.
[845] Eigene Darstellung.
[846] Vgl. IP_11.

5.2.3 Funktion 3: Wissensgebiete auf Wissensschutz-Bedarf prüfen (Kategorisierung)

Identifizierte Akteure für diese Funktion sind das Management mit Strategie- und Kundenmanagern. Damit eine IT-Beratung identifiziert, welches Wissen geschützt werden muss, haben sich mehrere Forscher für das Identifizieren und Analysieren vom wertvollen Wissen ausgesprochen.[847] Dieser Abschnitt baut auf den Erkenntnissen zur Spezifizierung der Unternehmensgrenze beim *Wissen-Teilen und -Zurückhalten* im Abschnitt 4.2.3 auf. BOUNCKEN erwähnt in diesem Zusammenhang eine Identifikationsmatrix um diese Unternehmensgrenze zu definieren, jedoch wird nicht ausgeführt wie diese strukturiert werden soll.[848] Die Wissenskategorisierung des Fach- und Technologiewissens ist Voraussetzung für die Risiko-Identifikationsmatrix im Abschnitt 5.3.2.

Funktion Wissensgebiete auf Wissensschutzbedarf prüfen (Abbildung 38)

Um die Wissenskategorisierung zu ermitteln sind die IT-Projekt-Wissensschutzstrategie und die Fach- und Technologiewissensbewertung die Voraussetzungen. Die IT-Projekt-Wissensschutzstrategie wurde bereits in der Funktion Strategischen Planung entwickelt.

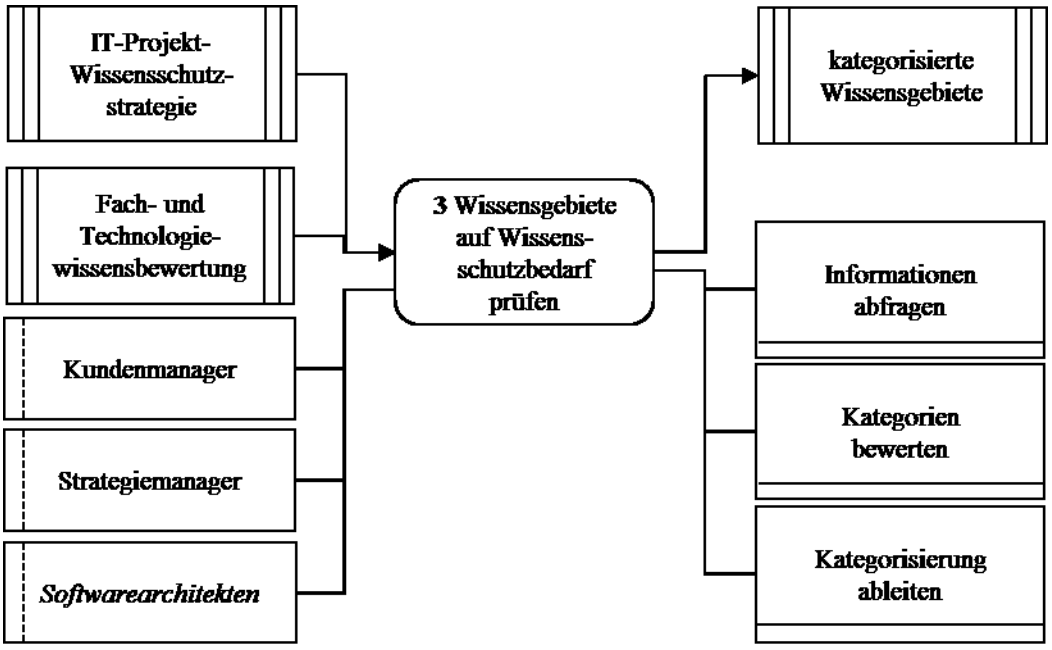

Abbildung 38: Funktion Wissensgebiete auf Wissensschutzbedarf prüfen[849]

Die IT-Beratungen bauen über Jahre hinweg spezialisiertes Fachwissen in den Auftraggeber-Projekten auf und spezialisieren sich in der Regel auf Technologiewissensgebiete. Zu diesen Wissensgebieten müssen die Informationen abgefragt und die Kategorisierung abgeleitet werden.

---

[847] Vgl. Ahmad et al. 2014, S. 30, Norman 2001, Hamel & Prahalad 1994, Hoecht & Trott 2005, Bloodgood & Salisbury 2001, Aljafari & Sarnikar 2009, Liebeskind 1996, O'Donoghue & Croasdell 2009, Olander & Hurmelinna-Laukunnen 2010, Teece 2009.
[848] Vgl. Bouncken 2003, S. 21.
[849] Eigene Darstellung.

Fach- und Technologiewissensbewertung – vier Bewertungskategorien

Die Fach- und Technologiewissensbewertungen basieren auf den Erkenntnissen von HAMEL & PRAHALAD[850] und HOECHT & TROTT[851]. Sie empfehlen die Wissensgebiete nach den drei Kategorien *Kundennutzen*, *Mitbewerberabgrenzung* und *Übertragbarkeit* zu bewerten.[852]

Eine identische Sichtweise haben BLOODGOOD & SALISBURY. Um nachhaltige Wettbewerbsvorteile zu sichern, muss die Wissensressource vier Eigenschaften erfüllen, diese sind:[853]

1. in der Situation wertvoll und nützlich (zum Beispiel branchenspezifisches Fachwissen),[854]
2. selten im Vergleich zu ihren Mitbewerbern,
3. unnachahmlich, das heißt für die Mitbewerber schwer nachzuahmen und[855]
4. nicht substituierbar.

Diese vier Eigenschaften reflektieren sich ebenso in den oben genannten drei Kategorien, deshalb werden diese drei Eigenschaften im Modell wiederverwendet. Des Weiteren spricht sich NORMAN[856] für eine strategische Wissensbewertung aus.

- Schützenswert ist das strategische Wissen, das im Zusammenhang mit Geschäftsentscheidungen wie zukünftige Produkte und Kostenstrukturen steht.[857]

Auf die Bewertung der strategischen Wissensrelevanz wurde ebenso in den Vorinterviews hingewiesen und deshalb wird die *Strategie*-Kategorie in das Modell aufgenommen. Basierend auf diesen Erkenntnissen sind die Fach- und Technologiewissensgebiete einer IT-Beratung nach den folgenden vier Kategorien zu bewerten:[858]

- **Strategie** bewertet die strategische Bedeutung (Relevanz) des Fachwissens / Technologiewissens und deren *zukünftige* Auswirkungen auf die Unternehmensstrategie. Das strategisch relevante Wissen steht im Zusammenhang mit Geschäftsentscheidungen.[859]
- **Kundennutzen** bewertet den überproportionalen *relativen* Wertbeitrag des Fachwissens / Technologiewissens *zum Unternehmenserfolg*. Das sind zum Beispiel die Unternehmensfähigkeiten, die einen wesentlichen Kundennutzen zu liefern.[860] *In die Bewertung vom Kundennutzen ist ebenso der Endanwendernutzen miteinzubeziehen.*
- **Mitbewerberabgrenzung** bewertet die Wettbewerbsfähigkeit des Fachwissens / Technologiewissens. Um als sehr wertvolles organisationales Fachwissen / Technologiewissen bewertet zu werden, muss das Wissensgebiet nicht unbedingt einmalig sein.[861]
- **Übertragbarkeit** bewertet die Anwendbarkeit des Fachwissens / Technologiewissens auf neue Informationssysteme, Kunden und Märkte. Voraussetzung für die Übertragbarkeit sind Mitarbeiter, die *mit ihrem Know-how und Erfahrungen* befähigt sind, das angeeignete Fachwissen / Technologiewissen anzuwenden.[862]

---

[850] Hamel & Prahalad 1994.
[851] Hoecht & Trott 2005.
[852] Vgl. Hoecht & Trott 2005, S. 403, Hamel & Prahalad 1994.
[853] Vgl. Bloodgood & Salisbury 2001, S. 57.
[854] Vgl. Bloodgood & Salisbury 2001, S. 57, Barney 1991, Cohen et al. 1996.
[855] Vgl. Bloodgood & Salisbury 2001, S. 57, Barney 1986, Barney 1991, Clemons & Row 1991.
[856] Norman 2001.
[857] Vgl. Norman 2001, S. 54.
[858] Die kursiv markierten Definitionsbestandteile ergänzen das theoretisch entwickelte Modell und wurden von den Interviewpartnern validiert.
[859] Vgl. Norman 2001, S. 54.
[860] Vgl. Hoecht & Trott 2005, S. 403, Hamel & Prahalad 1994, S. 224.
[861] Vgl. Hoecht & Trott 2005, S. 403, Hamel & Prahalad 1994, S. 226.
[862] Vgl. Hoecht & Trott 2005, S. 403, Hamel & Prahalad 1994, S. 227.

Mehrere Interviewpartner hatten angeregt die Zukunftssicht vom jeweiligen Wissensgebiet zu ermitteln und diese zu bewerten.[863] Die Strategiedefinition wurde deshalb um das Wort **zukünftig* erweitert. Die *Strategie* bewertet, ob dieses Wissensgebiet zukunftsweisend ist.[864] Bei der Bewertung der *Strategie* muss geprüft werden, wie spezifisch das Wissensgebiet für eine IT-Beratung ist, um die strategische Relevanz zu definieren.[865] Die inquirierten Experten aus dem Bereich Strategiemanagement examinierten die Kategorie *Strategie* unabhängig voneinander, ob diese in der Kategorie Kundennutzen integriert oder in mehrere Unterkategorien unterteilt werden könnte.[866] Aufgrund der Hinweise zur Zukunftssicht der anderen Experten wurde dieser Hinweis nicht in das Modell aufgenommen.

Ein Interviewpartner regte an, den Wertbeitrag des *Kundennutzens* genauer zu definieren, ob es sich um einen Wertbeitrag oder einen höheren Umsatz beim Kunden handelt.[867] Die Definition wurde deshalb um die Worte **relative* Wertbeitrag und *Unternehmenserfolg* erweitert. Ein weiterer Interviewpartner ergänzte den *Kundennutzen* mit dem Begriff Endanwendernutzen.[868] Mit dem Endanwendernutzen ist die Wirksamkeit auf den Endkunden und die Bedeutung für den Endkunden zu bewerten, weil die Endkunden die Anforderungen für die ISE definieren.[869] Auf einen möglichen Nebeneffekt verwies ein Interviewpartner. Wenn *Kundennutzen* und Endanwendernutzen zusammen bewertet werden, dann könnte diese Kategorie höher bewertet werden.[870] Zu der *Mitbewerberabgrenzung* gab es einen Hinweis der Experten. Nach ihnen ist bei der Bewertung der Mitbewerberabgrenzung die Zugriffsmöglichkeit von Wettbewerbern auf das zu bewertende Wissensgebiet einzubeziehen. Für die Definition der *Übertragbarkeit* sollte herausgestellt werden, dass das *Know-how* und das *Erfahrungswissen* der Mitarbeiter dafür notwendig ist.[871] Die zu bewertenden vier theoretisch hergeleiteten Kategorien der Wissenskategorisierung werden von den befragten Experten bestätigt. Nach den Expertenrückmeldungen sind keine weiteren Bewertungskategorien aufzunehmen.

Fach- und Technologiewissensbewertung: Akteursgruppen

Jeder Experte wurde bei dieser Funktion zu den Akteursgruppen befragt, die die Wissenskategorisierung vorzunehmen haben. Die Interviewergebnisse sind in der folgenden Tabelle 32 zusammengefasst.

[863] Vgl. IP_2, IP_7.
[864] Vgl. IP_7.
[865] Vgl. IP_10.
[866] Vgl. IP_5, IP_9.
[867] Vgl. IP_3.
[868] Vgl. IP_1.
[869] Vgl. IP_10.
[870] Vgl. IP_10.
[871] Vgl. IP_1.

Tabelle 32: Ergebnisse vom Experteninterview: Akteursgruppen für die Wissenskategorisierung[872]

IP	Kategorie: Strategie	Kategorie: Kundennutzen	Kategorie: Übertragbarkeit	Kategorie: Mitbewerberabgrenzung
Akteurs-empfehlung	*Strategiemanagement mit Softwarearchitekten*	*Kundenmanagement*	*Softwarearchitekten*	*Softwarearchitekten mit Kundenmanagement und Strategiemanagement*
1	Siehe Modell: Management, Strategiemanagement, Kundenmanagement			
2	Siehe Modell: Management, Strategiemanagement, Kundenmanagement			
3	Strategiemanagement	Kundenmanagement	Architekten	Kundenmanagement
4	Strategiemanagement	Kundenmanagement	Management, Presales Berater	Kundenmanagement, Strategiemanagement
5	Kundenmanagement Hauptverantwortlich, jeder wird seinen Beitrag leisten			
6	Strategiemanagement	Kundenmanagement	Management Projektbereiche, Architekten	Kundenmanagement Strategiemanagement
7	Strategiemanagement, CIO Bereich			
8	Strategiemanagement	Kundenmanagement	Strategiemanagement, Architekten	Strategiemanagement, Architekten
9	Enthaltung	Enthaltung	Enthaltung	Enthaltung
10	Architekten	Kundenmanagement	Architekten	Architekten
11	Strategiemanagement, CIO Bereich	Kundenmanagement	Architekten	Strategiemanagement, CIO Bereich

Im Tabellenkopf ist die Akteursempfehlung der IP für das validierte Referenzmodell kursiv eingetragen. Ursprünglich war vorgesehen, dass das Management der Hauptakteur für alle Bewertungskategorien ist, denn MAJCHRZAK & JARVENPAA heben hervor, dass in vielen Organisationen, wo einzelne Mitarbeiter kollaborieren und in Situation mit opportunistischen Risiken beteiligt sind, das Management Regeln vorgibt, was geteilt werden darf und was nicht.[873] Bei den Rückmeldungen zeigte sich ein detailliertes Bild. Ein Interviewpartner hat sich bei der Fragestellung enthalten, andere hatten eine dezidierte Vorstellung zu den Akteursgruppen. Als Ergebnis ist festzuhalten, dass die **(fachlichen und technischen) Softwarearchitekten* als Akteursgruppe in die Wissenskategorisierung für die *Übertragbarkeit* und *Mitbewerberabgrenzung* aufzunehmen sind. Für die Bewertung der *Übertragbarkeit* ist ein hohes Fach- und Technologiewissen notwendig, damit die Bewertung valide ist.[874] Deshalb haben die Softwarearchitekten die Verantwortung für diese Kategoriebewertung.

Die Bestimmung der Unternehmensgrenze muss nach den Analysen eine gemeinsame Entscheidung einer IT-Beratung sein und nicht von einer Mitarbeitergruppe oder einem übergreifenden Experten (Gatekeeper) allein realisiert werden. Mehrere Projektakteure bringen ihre

[872] Eigene Darstellung.
[873] Vgl. Majchrzak & Jarvenpaa 2010, S. 78.
[874] Vgl. IP_4.

Sichtweise für eine möglichst objektive Bewertung ein, da die Entscheidung zum *Wissen-Teilen* eine weitreichende ist. Eine IT-Beratung unterstützt den externen Dienstleister beim allgemeinen Wissensfortschritt, wenn sie den Wert des Wissens selbst nicht kennt und das Wissen leichtfertig geteilt wird.[875] Aus der Risikomanagementperspektive werden in der Wissenskategorisierung die Werte / Assets als schützenswertes Wissen identifiziert und quantifiziert.[876] Damit wird das Schadenspotential bestimmt. Dieses ist Voraussetzung für die Risikobewertung und Auswahlentscheidung im Abschnitt 5.3.2.

Fach- und Technologiewissensbewertung: Validierung und Erweiterung

In der Tabelle 33 sind die Kategorien für die Wissenskategorisierung illustriert. Herauszustellen ist, dass die Bewertung projektunabhängig und in regelmäßigen Zyklen erfolgen muss. Diese regelmäßigen Bewertungszyklen bestätigten die Interviewpartner, da sich die Marktsituation ändern kann.[877] In den Experteninterviews wurde ebenso bestätigt, dass die zukünftigen Wissensgebiete zu kategorisieren sind. Damit können Rahmenbedingungen zum Wissensaufbau frühzeitig geschaffen werden, bevor ein IT-Projekt in Auftrag gegeben wird.[878] Es ist von Bedeutung, dass für die zukünftigen Wissensgebiete eine Strategie vorliegt.[879] Bei den Technologiewissensgebieten ist die Aufnahme der zukünftigen Wissensgebiete entscheidender, da sich das Technologiewissen im Vergleich zum Fachwissen häufiger ändert.[880] Das ist auf die rasant wachsende Digitalisierung mit den radikalen Innovationen in der IT-Branche zurückzuführen. Durch neues Technologiewissen können die Geschäftsprozesse, die auf dem Fachwissen basieren, noch effizienter und effektiver unterstützt werden. Ein weiterer Interviewhinweis war, dass gleiche Technologiewissensgebiete in verschiedenen Varianten existieren und übergreifend bewertet werden können. Das ist zum Beispiel bei der Cloudtechnologie der Fall.[881]

In den Interviews wurde bestätigt, dass die Anzahl der IT-Projekte zum Wissensgebiet eine Aussage für den Wissensschutz hat. Diese Information ist im Zusammenhang mit dem **Auftragsvolumen* und den **Personentagen* zu betrachten, um eine valide Aussage zu erhalten.[882]

Im Unterkapitel 5.1 wurde begründet, warum im Referenzmodell auf eine Bewertungsskala verzichtet wird. An dieser Stelle soll darauf hingewiesen werden, dass im theoretischen Modell eine Kategoriegewichtung zwischen den vier Bewertungskategorien vorgesehen war. Diese Gewichtung kann nach einer Interviewrückmeldung entfallen, weil in der Bewertung bereits eine Gewichtung integriert ist.[883] Diese praktische Sicht wurde in der exemplarischen Bewertung eines realen IT-Projekts und im Gruppeninterview bestätigt.

---

[875] Vgl. IP_11.
[876] Vgl. Abschnitt 2.2.3.
[877] Vgl. IP_2, IP_6.
[878] Vgl. IP_6.
[879] Vgl. IP_10.
[880] Vgl. IP_8.
[881] Vgl. IP_6.
[882] Vgl. IP_4, IP_11.
[883] Vgl. IP_11.

Tabelle 33: Wissenskategorisierung vom Technologie-/Fachwissen in der IT-Beratung[884]

Bewertungskategorie	Fachwissen 1 / Technologiewissen 1	Fachwissen 2 / Technologiewissen 2	(Zukünftiges) Fachwissen n / Technologiewissen n
Strategie	• Bewertungsskala muss von jeder IT-Beratung festlegt werden • **Begründungfeld zu jeder Bewertung*		
Kundennutzen			
Mitbewerberabgrenzung			
Übertragbarkeit			
Wissenskategorisierung	• z. B. ABC- und Farbgruppierung		
IT-Projekte mit dem Wissensgebiet	• Namen und Anzahl der IT-Projekte		
**Gesamtauftragsvolumen in PT*	**15. 000 PT mit Jahresangabe*	**30.000 PT mit Jahresangabe*	
**Interne Expertise im Wissensgebiet*	• **Bewertungsskala festlegen und Begründungsfeld*		
**Kernkompetenz*	• **Auswahlfeld Ja / Nein*		

Bei den vorbereitenden Einzelinterviews zum *Projekt α* für das Gruppeninterview lieferten die Projektmitarbeiter jeweils Begründungen, warum sie die entsprechende Bewertung gegeben haben. Damit die Nachvollziehbarkeit der Bewertung gewährleistet ist, wird ein Begründungsfeld zu jeder Kategoriebewertung aufgenommen. Bei dem Gruppeninterview wurde das Begründungsfeld validiert.

Um die Wissensgebiete nach wertvollem und schützenswertem Wissen zu ordnen, wurde in den Experteninterviews eine ABC-Gruppierung verwendet. Die A-Gruppierung dokumentiert das wertvolle und schützenswerte Wissen. In den Interviews wurden auf weitere mögliche Gruppierungen hingewiesen. Aus der Perspektive der Vertraulichkeit könnte das Fachwissen nach den Geheimhaltungsstufen gruppiert werden,[885] jedoch ist diese Gruppierung dem Informationsschutz zuzuordnen. Für die Technologiewissensgebiete ist zu entscheiden, wie weit diese aus strategischer Sicht zu den Kernkompetenzen gehören. Eine mögliche Gruppierung der Technologiewissensgebiete wäre in Schlüsseltechnologie, unternehmensspezifische Technologie und allgemeingültige Technologie.

Aus den Interviews wurden drei gekennzeichnete Bewertungskategorien in das Modell aufgenommen. Diese sind das **Gesamtauftragsvolumen* vom Wissensgebiet, die **interne Expertise im Wissensgebiet* und die **Kernkompetenzeinordnung*. Damit der Eigenfertigungsgrad der Wissensgebiete bestimmt werden kann, ist das **Gesamtauftragsvolumen* des Wissensgebietes

[884] Eigene Darstellung.
[885] Vgl. IP_8.

in Jahresscheiben zu dokumentieren.[886] Dieses kann dann in das Verhältnis zum *Auftragsvolumen vom externen Dienstleister* gesetzt werden. Zum anderen können über die Entwicklung von Jahresscheibe zu Jahresscheibe Tendenzen ermittelt werden.

Zum zweiten muss die **interne Expertise im Fach- und Technologiewissen* gekennzeichnet werden, damit ist auch nachvollziehbar und begründbar, wann das Fach- und Technologwissen an einen externen Dienstleister ausgelagert wird.[887] Ein Interviewpartner hat die *interne Expertise* als Wissensverfügbarkeit bezeichnet, damit dokumentiert wird, wie gut eine IT-Beratung in dem Wissensgebiet ist.[888]

Zum dritten ist zu dokumentieren, ob dieses Wissensgebiet zu den **Kernkompetenzen* gehört.[889] Zu der Bewertung der *Kernkompetenz* wird auf die gesammelte Erfahrung im Gruppeninterview verwiesen. Bei den vorbereitenden Einzelinterviews für das Gruppeninterview haben die befragten Experten zum Teil Wissensgebiete zu einer *Kernkompetenz* zugeordnet, obwohl das Bewertungsergebnis ein weniger schützenswertes Wissensgebiet war. Auf Nachfrage bestätigten die Interviewpartner diese korrekte Bewertung. Das bedeutet, dass schützenswerte und wertvolle Wissensgebiete zu den *Kernkompetenzen* gehören kann.

5.3 Referenzmodell-Phase 2: Dienstleisterauswahl

Der COO und CPO verantworten diese Phase der Dienstleisterauswahl. Sie sind über die Entscheidung zu informieren. Die Phase der Dienstleisterauswahl wird im originären Phasenmodell als Partnerauswahl und Vertragsmanagement[890] bezeichnet. Die Zusammenarbeit mit dem externen Dienstleister beruht auf einer Prinzipal-Agenten-Beziehung und wird deshalb anstatt Partnerauswahl als Dienstleisterauswahl deklariert, da Partner im Vergleich zu einer Prinzipal-Agenten-Beziehung bidirektional kommunizieren.[891] Das Vertragsmanagement entfällt, da dieses als Voraussetzung für das Wissensschutz-Modell definiert ist und außerhalb vom Fokus der Arbeit liegt. Das Vertragsmanagement ist den formalen[892] Wissensschutzmechanismen zugeordnet. Dennoch ist darauf hinzuweisen, dass die formalen Mechanismen ausgeschöpft werden müssen, da sonst bei einer Wissensschutzverletzung keine rechtlichen Schritte eingeleitet werden können. Die Interviewpartner bestätigten in diesem Zusammenhang, dass in den Verträgen nachvollziehbar dokumentiert sein muss, welche Konsequenzen, zum Beispiel Vertragsstrafen, auf eine Zuwiderhandlung folgen.

Nachdem im ersten Abschnitt die Dienstleisterkategorisierung (Funktion 4) beschrieben wird, fokussiert der zweite Unterabschnitt die Risikobewertung und die anschließende Dienstleisterauswahl mit Bezug auf das IT-Projekt. Die Grundlagen zur Risikoermittlung und die Einfluss-

[886] Vgl. IP_5.
[887] Vgl. IP_5, IP_6.
[888] Vgl. IP_6.
[889] Vgl. IP_4, IP_6.
[890] Vgl. Nassimbeni et al. 2012, S. 410 ff.
[891] Vgl. Unterkapitel 2.3
[892] Vgl. Siehe Abschnitt 4.2.2.

größen sind im Abschnitt 2.2.3 beschrieben. Im Modell werden der Gefahr, der Eintrittswahrscheinlichkeit und dem Schadenspotenzial die folgenden Kategorien zugeordnet, um die Risikobewertung zu ermitteln.

- Gefahr (Dienstleister-Gefahrenpotential):
  - absorptive Dienstleisterkapazität (Lernbereitschaft und Innovationsfähigkeit, Dienstleistergröße, Dienstleisteraktivitäten, Dienstleisterart, Dienstleisterbranche (Marktumfang))
  - aufgebautes und vorhandenes Fachwissen und Technologiewissen vom Dienstleister
- Eintrittswahrscheinlichkeit: Vertrauen (Erfahrungen mit dem Dienstleister)
- Schadenspotential: Bewertung des zu schützenden wertvollen Wissens (Werte / Assets und dessen Quantifizierung) - siehe Wissenskategorisierung

5.3.1 Funktion 4: Dienstleister kategorisieren

Akteure für diese Funktion sind das IT-Sourcing Management mit dem Ressourcenmanagement. Die Dienstleisterkategorisierung basiert auf den Erkenntnissen vom Abschnitt 4.2.4 und unterteilt sich in drei Unterfunktionen (Steckbriefe, Gefahrenpotential, Fach- und Technologiewissen).

Funktion Dienstleister kategorisieren (Abbildung 39)

Die erste Unterfunktion befasst sich mit dem Generieren von Dienstleistersteckbriefen. Die zweite Unterfunktion ordnet den Dienstleister in ein *Gefahrenpotential* ein. Der Gedanke der *Gefahrenpotential-Bestimmung* ist auf LI et al. zurückzuführen. Wie oben bereits erwähnt, empfehlen sie den Dienstleistungspartner nach dem Allianzziel in drei Bereiche einzuteilen, diese sind: Freunde, Bekannte und Unbekannte.[893] Ihre Untersuchungen beziehen sich auf die Partnerauswahl in Forschungs- und Entwicklungsallianzen. In den Limitationen ihrer Untersuchungen wird explizit weiterer Forschungsbedarf avisiert, dass bei konkreten Projektentscheidungen vom Management die Zusammenarbeit mit Dienstleistern eine weitere Herausforderung bedeutet.[894] Dieses Modell adressiert diese Projektentscheidungen für den Einsatz von externen Dienstleistern. Die dritte Unterfunktion bewertet das Fach- und Technologiewissen des Dienstleisters.

[893] Vgl. Li et al. 2008, S. 315.
[894] Vgl. Li et al. 2008, S. 329.

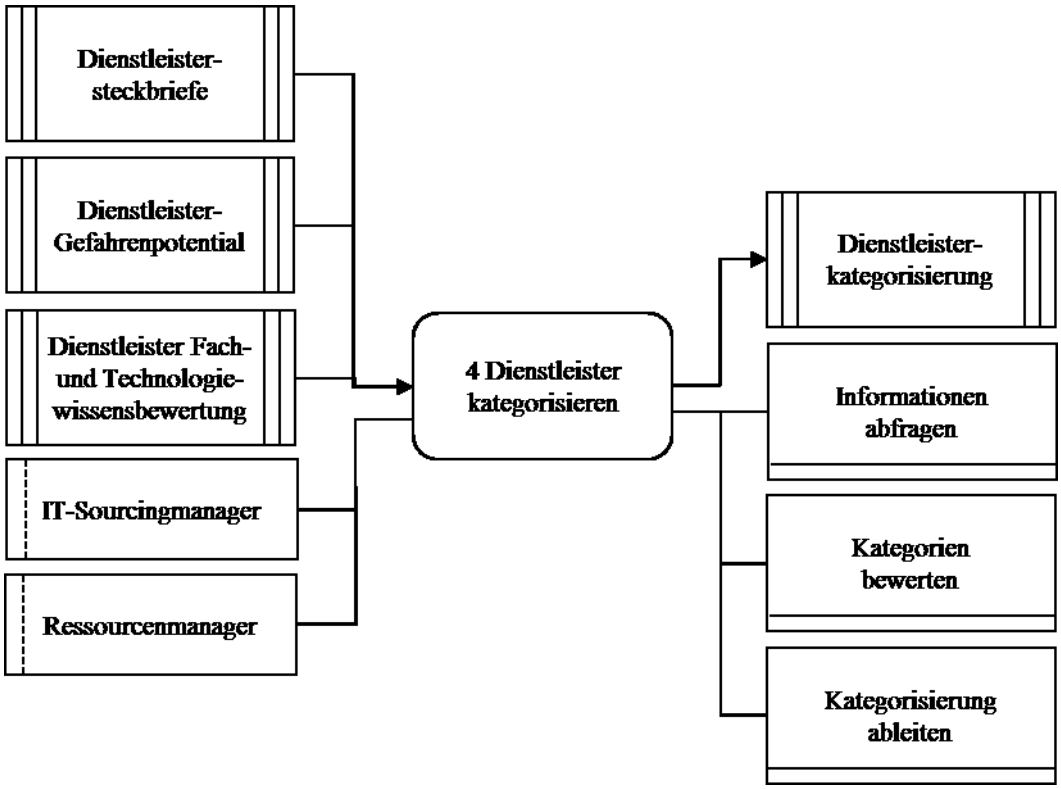

Abbildung 39: Funktion Dienstleister kategorisieren[895]

Unterfunktion Dienstleistersteckbriefe

Mehrere Autoren haben sich für ein *Background-Screening* des Dienstleisters ausgesprochen.[896] Das *Background-Screening* ist ein Beispiel für einen strategischen Mechanismus[897] zur Entwicklung von Strategien, Verfahren und Richtlinien. Die unter anderem von AHMAD et al. identifiziert und zusammengefassten strategischen Managementinitiativen zum Wissensschutz von wertvollem Wissen sind im Abschnitt 4.2.1 dargestellt. In der betrieblichen Praxis werden Dienstleistersteckbriefe eingesetzt, die ein praktisches Pendant zum *Background-Screening* sind. Diese müssen die folgenden Informationen integrieren:

- Unternehmensname, Hauptsitz, Niederlassungen, Gründungsjahr
- Anzahl der Mitarbeiter (Deutschland, EU, weltweit)
- Umsatz in Euro, Wachstum p.a. in Prozent in den letzten Jahren, wirtschaftliche Lage
- Unternehmensleitlinien, Referenzprojekte, Referenzkunden
- Dienstleistungs- / Technologieportfolio
- Spezielle Expertisen, sonstige Informationen, Awards, Zertifizierungen
- Historie der Projekteinsätze in der IT-Beratung, Dauer der Zusammenarbeit
- Einsatz in aktuellen IT-Projekten der IT-Beratung und Projektgröße
- Erfahrungen, Vertrauen
- Kooperationen mit Mitbewerbern und Auftragsverhältnisse mit Auftraggebern
- Besondere Vorfälle
- Abhängigkeiten zum Dienstleister

[895] Eigene Darstellung.
[896] Vgl. Ahmad et al. 2014, S. 30.
[897] Vgl. Ahmad et al. 2014, S. 30, Aljafari & Sarnikar 2009, Bloodgood & Salisbury 2001, Ford & Helayne 2004, Gold et al. 2001, Liebeskind 1996.

Diese Steckbriefe sind Voraussetzung für die Risikobewertung, damit die Chancen und Risiken sichtbar werden. Gleichzeitig dokumentieren sie Hinweise auf die Wettbewerbs- und die Marktüberlappung mit dem externen Dienstleister.[898] Ein IP merkte an, dass die externen Dienstleister zu kennzeichnen sind, die ein besonderes Interesse zur Mitarbeit in bestimmten IT-Projekten und Wissensgebieten zeigen.[899]

Aus der Dienstleisterhistorie heraus ist zu prüfen, ob die Dienstleistergröße und der -umsatz durch den jahrelangen Projekteinsatz in einer IT-Beratung zugenommen haben. Mögliche Szenarien sind, dass der Dienstleister durch die gesteigerte Projektunterstützung größer geworden ist oder durch das diffundierte Wissen andere Auftraggeberprojekte realisieren konnte.[900] Ebenso ist das Vertragsverhältnis zu prüfen, ob der Dienstleister die Leistungen selbst erbringt oder an andere externe Subunternehmen weitergeben kann.[901]

Unterfunktion Dienstleister-Gefahrenpotential

Mit der Eruierung des *Gefahrenpotentials* wird der Dienstleister kategorisiert und konstatiert, welche negative Auswirkung für die Wettbewerbsfähigkeit einer IT-Beratung entstehen können, wenn wertvolles Wissen mit ihm geteilt wird. Um das *Gefahrenpotential* zu identifizieren, werden die Literaturerkenntnisse angewendet. Der Wissensschutz wird in der Forschungsliteratur im Zusammenhang mit der *absorptiven Kapazität*[902] und dem Vertrauen[903] diskutiert. Das Vertrauen basiert auf den gewonnenen Erfahrungen mit dem Dienstleister aus früheren Beziehungen. Beim Gruppeninterview zur Themenfokussierung bestätigten die Teilnehmer die Relevanz der *absorptiven Kapazität* und verglichen diese mit dem *Staubsaugermodus* der externen Dienstleister. Die Interviewteilnehmer berichteten in diesem Zusammenhang aus ihrer betrieblichen Praxis. Sie können wahrnehmen, wenn der externe Dienstleister seine absorbierende Fähigkeit einsetzt und hohes Interesse an dem Projektwissen zeigt.

Umso ähnlicher die Qualifikationen, Ressourcen und Fähigkeiten, desto größer ist nach NORMAN die *absorptive Kapazität*.[904] Diese Aussage begründen die Kategorien Dienstleistergröße, Dienstleisteraktivitäten, Dienstleisterart und Dienstleisterbranche. Diese Informationen geben Hinweise auf die Wettbewerbs- und Marktüberlappung. Umso größer die Branchenüberlappung zwischen einer IT-Beratung und dem externen Dienstleister, desto höher ist das Gefahrenpotential.[905] Dazu gehört ebenso die Überlappung der potenziellen Auftraggeber in den Branchen zu prüfen.[906] Zum Beispiel in der Mobilitäts-, Finanzdienstleistungs-, Versicherungs-, Chemie-, Pharma- und Automobilbranche.[907]

---

[898] Vgl. Norman 2001, S. 58.
[899] Vgl. IP_10.
[900] Vgl. IP_11.
[901] Vgl. IP_11.
[902] Vgl. Abschnitt 4.3.3.
[903] Vgl. Abschnitt 4.3.1.
[904] Vgl. Norman 2002, S. 183, 2004, S. 612.
[905] Vgl. IP_6, IP_7.
[906] Vgl. IP_6.
[907] Vgl. IP_6.

Während diese Überschneidungen die Zusammenarbeit beim *Wissen-Teilen* erleichtern können, ist das Risiko vom Wissensverlust größer.[908] COHEN & LEVINTHAL, die Begründer der *absorptiven Kapazität,* etablieren den Begriff mit der Lernfähigkeit und Innovationsfähigkeit. Auf der Basis dieser Literaturerkenntnisse ergeben sich die folgenden Relationen um das *Gefahrenpotential* vom externen Dienstleister zu kategorisieren. Diese theoretisch hergeleiteten Relationen wurden in den Experteninterviews verifiziert und validiert.

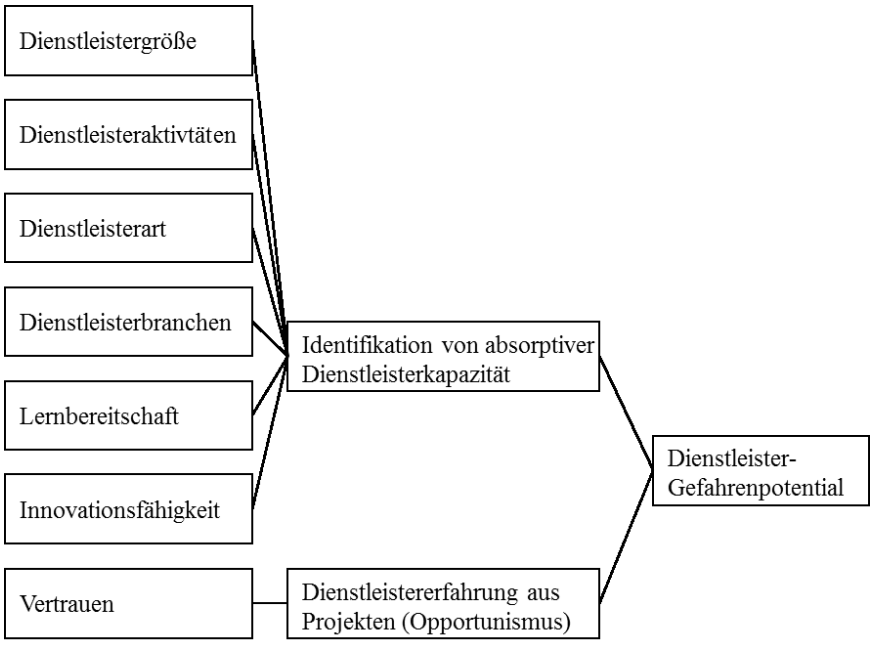

Abbildung 40: Dienstleisterkategorisierung nach Gefahrenpotential[909]

Die Begrifflichkeiten aus dem Relationsdiagramm werden in der Tabelle 34 beschrieben und die relevanten Studien aufgeführt.

[908] Vgl. Norman 2002, S. 181, S. 183, Norman 2004, S. 612.
[909] Eigene Darstellung.

Tabelle 34: Bestimmung der absorptiven Kapazität für die Dienstleisterkategorisierung[910]

Kategorie	Inhalt der Bewertung	Autoren / Studien
Dienstleister-größe	Erfasst die Anzahl der Mitarbeiter im Inland und Ausland.	Norman 2002, Mowery et al. 1996
Dienstleister-aktivitäten (Anzahl der Länder)	Erfasst die Anzahl der Länder in denen der Dienstleister aktiv ist, damit kann die Anzahl der Märkte identifiziert werden.	Norman 2002, Gold et al. 2001
Dienstleisterart	Erfasst die Zuordnung des Dienstleisters im Dienstleistungsbereich. **Bei Mischformen ist die überwiegende einzutragen.*[911] *Zum Beispiel Einteilung in Global Player, Mittelständler und Fachkraftvermittler.*[912]	Jiang 2002, Norman 2002, Mowery et al. 1996
Dienstleister-branche (Markt-umfang)	Dokumentiert die Branchen-Aktivitäten des Dienstleisters.	Norman 2002, Gold et al. 2001
Lernbereitschaft / Lernfähigkeit	Ergibt sich aus der Fähigkeit neues Wissen aufzunehmen und dieses für das eigene Unternehmen zu nutzen. **Das beinhaltet die Transferleistung auf andere Märkte und Kunden.*[913]	Cohen & Levinthal 1990, Mowery et al. 1996
Innovations-fähigkeit	Ergibt sich aus dem komplexen Zusammenspiel der Unternehmen und seiner hervorgebrachten Innovationen.	Cohen & Levinthal 1990, Mowery et al. 1996
Absorptive Dienstleister-kapazität	Kumuliert sich aus allen zuvor definierten Bewertungskategorien des Dienstleisters.	Cohen & Levinthal 1990, Mowery et al. 1996, Norman 2002; Norman 2004
Dienstleister-erfahrung aus Projekten (Vertrauen)[914]	Ergibt sich aus dem aufgebauten Vertrauen, der Einschätzung vom Opportunismus, der **Lieferqualität des Dienstleisters*[915], den bestehenden und erfolgreich abgeschlossenen Projekten mit dem Dienstleister.	Mowery et al. 1996, Jiang 2002, Hoecht & Trott 2005, Li et al. 2008, Kale et al. 2000, Kogut & Zander 1992, Mowery et al. 1998, Szulanski 1996, von Hippel 1994, Zahra & George 2002
Dienstleister-Gefahren-potential	Ergibt sich aus der kumulierten Bewertung der absorptiven Dienstleisterkapazität und der Dienstleistererfahrung aus Projekten.	Li et al. 2008

Die Positionsbestimmung zur Lernfähigkeit und Innovationsfähigkeit vom externen Dienstleister ist durch das langjährige Erfahrungswissen aus dem IT-Sourcing Management möglich, da diese aus den IT-Projekten Rückmeldung zu Dienstleistern erhalten.[916] Die inquirierten Experten aus dem IT-Sourcingbereich verwiesen auf die über mehrere Jahre hinweg erhobenen 360°

[910] Eigene Darstellung.
[911] Vgl. IP_3.
[912] Vgl. IP_6.
[913] Vgl. IP_6.
[914] Vgl. Tabelle 18.
[915] Vgl. IP_4.
[916] Vgl. IP_2, IP_6.

Feedbacks aus den Projekten zu den Dienstleistern, die für die Einschätzung herangezogen werden können.[917]

Das organisationsübergreifende Vertrauen[918] kann sich bei einem vorteilhaften Wissensaustausch erhöhen und somit zu einem verminderten wahrgenommenen Risiko führen.[919] Die Beteiligten zeigen Vertrauen, wenn sie sich dem Risiko vom opportunistischen Verhalten aussetzen und sie keinen Grund zu glauben haben, dass die Gegenseite ihr entgegengebrachtes Vertrauen ausnutzen wird.[920] Die Bestimmung vom *Dienstleister-Gefahrenpotential* soll eine IT-Beratung sensibilisieren zu erkennen, dass dieser Dienstleister die Fähigkeiten mitbringt, das wertvolle Wissen nutzbringend für sich einzusetzen.

Unterfunktion Dienstleister Fach- und Technologiewissen

Der dritte Teil der Dienstleisterkategorisierung konzentriert sich auf die Identifizierung der Wissensüberlappung zwischen den kooperierenden Unternehmen. Um den Wissensschutz sicherzustellen, ist laut der Forschungsliteratur die Wissensüberlappung mit dem kooperierenden Unternehmen zu identifizieren.[921]

Tabelle 35: Bestimmung der Wissensüberlappung für die Dienstleisterkategorisierung[922]

Inhalt	Autoren / Studien
Wissensüberlappung	*Bouncken 2003, Bogers 2011, Jiang 2002, Kale et al. 2000, Oxley 1999, Norman 2004*

Um diese Wissensüberlappung festzustellen, müssen die Technologie- und Fachwissensgebiete vom externen Dienstleister nach seiner **internen Expertise* in der IT-Beratung und seiner externen Marktstellung bewertet werden. Die **interne Expertise zu Wissensgebieten des externen Dienstleisters* basiert auf der Projekthistorie. Um die externe Markstellung zu bestimmen, können zum Beispiel unabhängige Marktforschungsunternehmen (Benchmarking) angefragt werden. Der Dienstleistersteckbrief kann Spezialisierungen des Dienstleisters offenlegen und zur Bewertung herangezogen werden. Die Bewertungskategorien des Dienstleisters zur Feststellung der Wissensüberlappung sind:

- **Interne Expertise:** Auf der Grundlage der Informationen des IT-Sourcing Managements, aus den bestehenden kategorisierten Projekten und den bereits eingenommenen Projektrollen des Dienstleisters kann die interne Bewertung in Bezug auf die Fach- und Technologiewissensgebiete erfolgen.
- **Externe Marktstellung:** Auf der Grundlage der externen Marktinformationen über den Dienstleister kann die externe Bewertung in Bezug auf die Fach- und Technologiewissensgebiete erfolgen.

[917] Vgl. IP_2.
[918] Vgl. Abschnitt 4.3.1.
[919] Vgl. Trkman & Desouza 2012, S. 11 f.
[920] Vgl. Hoecht & Trott 2005, S. 408 f.
[921] Vgl. Lei et al. 1997, S. 205.
[922] Eigene Darstellung.

Tabelle 36: Kategorisierung des Technologie-/Fachwissens vom Dienstleister[923]

Bewertungskategorien	Fachwissen 1 / Technologiewissen 1	Fachwissen 2 / Technologiewissen 2	Fachwissen n / Technologiewissen n
**Interne Expertise*	• Bewertungsskala IT-Beratung individuell		
Externe Marktstellung			
Dienstleisterkategorisierung	• z. B. abc- und Farbgruppierung		
**Auftragsvolumen in Personentage (Kalenderjahr) und in Relation zum Gesamtauftragsvolumen der IT-Beratung*	**1.000 PT mit Jahresangabe, 6,7 % vom Gesamtauftrags-Volumen*	Wissensgebiet nicht praktiziert	**3.000 PT mit Jahresangabe, 10 % vom Gesamtauftrags-Volumen*

Die Bewertung der Wissensgebiete erfolgt nicht auf der Expertise des einzelnen Beraters, sondern der externe Dienstleister wird gesamtheitlich evaluiert. Ein Interviewpartner deklarierte die Bewertung der **internen Expertise* und externen Marktstellung im Wissensgebiet als Qualitätsmerkmale des Dienstleisters.[924] Um das Qualitätsmerkmal zu präzisieren, sind die nicht praktizierten Wissensgebiete des Dienstleisters zu kennzeichnen.

Des Weiteren gab es ab dem ersten Interview Hinweise das **Auftragsvolumen des externen Dienstleisters in Personentagen* in jedem Wissensgebiet aufzunehmen.[925] Dieses **Auftragsvolumen* muss in Relation zum Gesamtvolumen vom Wissensgebiet in der IT-Beratung gesetzt werden, damit die Wertschöpfungstiefe in dem Wissensgebiet deutlich wird.[926] Diese Wertschöpfungstiefe in Personentagen ist jahresscheibenweise für jedes Wissensgebiet zu erfassen.[927] Ebenso zu kennzeichnen sind die Wissensgebiete, die ein Dienstleister nicht leistet oder umsetzen kann.

Einfluss der Projektrolle des externen Beraters

In den Interviews wurde über die eingenommene Projektrolle des externen Beraters diskutiert. Die eingenommene Projektrolle vom externen Dienstleister im IT-Projekt hat Einfluss auf die Wissenskritikalität.[928] Mehrere Interviewpartner verwiesen darauf, dass umso zentraler oder höherwertiger die Projektrolle angesiedelt ist, desto eher kommt diese mit wertvollem und schützenswertem Wissen einer IT-Beratung in Kontakt.[929] Besonders Projektrollen mit direktem Kundenkontakt[930], fachlichem und fachlich-technischem Bezug[931] sind hinsichtlich des Wissensschutzes zu examinieren.

---

[923] Eigene Darstellung.
[924] Vgl. IP_9.
[925] Vgl. IP_1.
[926] Vgl. IP_5.
[927] Vgl. IP_8.
[928] Vgl. IP_1.
[929] Vgl. IP_2, IP_3, IP_5.
[930] Vgl. IP_4, IP_11.
[931] Vgl. IP_10.

5.3.2 Funktion 5: Risikobewertung durchführen und Dienstleister auswählen

Identifizierte Akteure für diese Funktion sind das Ressourcenmanagement mit dem Projektmanager. Die Risikobewertung konkludiert alle erfassten Daten und Informationen zum Projekt, den Wissensgebieten und den potentiellen Dienstleistern. Sie stellt sie in einer Managementansicht für jedes IT-Projekt dar. Die folgenden Autoren begründen diese Funktion.

Tabelle 37: Risikobewertung zum Wissensschutz in einer IT-Beratung[932]

Inhalt	Autoren / Studien
(Risk) Evaluation	Pai & Basu 2007, Lacity & Willcocks 1998, Khalfan 2004, Jennex & Olfmann 2005, Norman 2002, Farrell 2010, Norman, 2001, Arac & Ozkarahan 2007
Bewertung Wissensrisiko	Trkman & Desouza 2012, Päällysaho & Kuusisto, 2011, Pai & Basu 2007, Olander et al. 2011

Funktion Risikobewertung durchführen und Dienstleister auswählen (Abbildung 41)

IT-Beratungen, die ihr *Wissen-Teilen* wollen und gewillt sind zu lernen, müssen strategisch entscheiden, inwieweit sie mit Dienstleistern zusammenarbeiten können.[933] DESOUZA stellte in seinen Untersuchungen fest, dass beim strategischen Sourcing Risiken vernachlässigt werden.[934] Zum Beispiel, wenn ein IT-Projekt eine Bedarfsanalyse durchführt, ist es erheblich die Risiken und Probleme zu hinterfragen, die in Bezug auf Wissen entstehen können, wenn in einem Projekt ein externer Dienstleister beteiligt wird.[935] In der Initialisierungsphase von Projekten sind nach DESOUZA die Chancen hoch, mögliche Probleme beim Wissensschutz zu identifizieren.[936] Aus Projektmanagementsicht ist eine erste Risikobewertung und damit auch die Bewertung der Wissensrisiken in der Initialisierungs- und Definitionsphase durchzuführen. In die Risikobewertung zum Wissensschutz fließen alle Informationen der vorherigen Funktionen 1, 2, 3 und 4 ein. In dieser Projektinitialisierungs- und Projektdefinitionsphase können mögliche Probleme beim Wissensschutz identifiziert werden. GHODESWAR & VAIDYANATHAN konstatieren, dass bevor eine Vereinbarung mit einem Dienstleister getroffen wird, müssen geprüfte Risikominimierungspläne, geprüfte Hochsicherheitsniveaus, ausgereifte Projektmanagementkompetenzen und bewährte Business Continuity Pläne vorliegen.[937]

[932] Eigene Darstellung.
[933] Vgl. Drechsler & Natter 2012, S. 439.
[934] Anmerkung des Autors: Das Paper von Desouza 2008 hat nicht den Wissensschutz im Fokus, sondern Sicherheitsrisiken beim strategischen Sourcing.
[935] Vgl. Desouza 2008, S. 291.
[936] Vgl. Desouza 2008, S. 292.
[937] Vgl. Ghodeswar & Vaidyanathan 2008, S. 26.

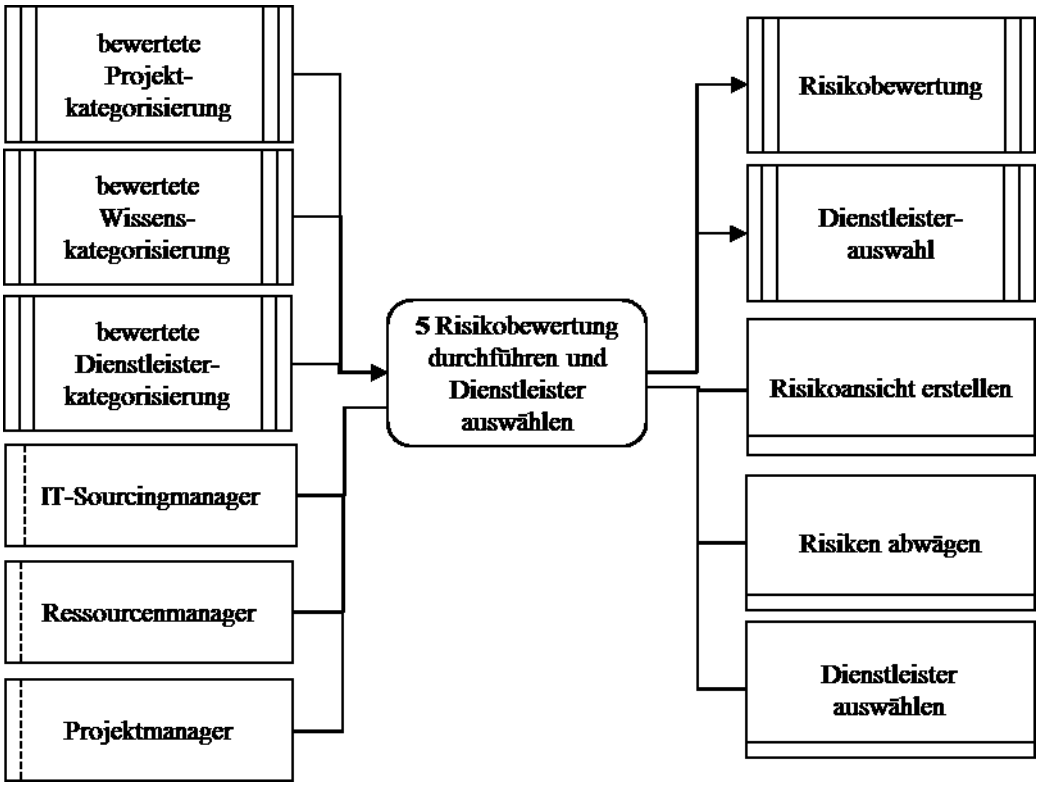

Abbildung 41: Funktion Risikobewertung durchführen und Dienstleister auswählen[938]

Details zur Risikobewertung durchführen

In der schematischen Abbildung 42 müssen die Bewertungsergebnisse aus den Funktionen 2, 3 und 4 eingetragen werden. Das sind die Fach- und Technologiewissensgebiete vom IT-Projekt aus der Funktion 2 und deren Bewertungen in den Funktionen 3 und 4. Zudem sind bei den bestehenden Projekten die Dienstleister und ihre *Dienstleister-Gefahrenpotentiale* einzutragen. Die Farbgebung in den Quadranten der **Risikomatrix* visualisiert den Bedarf an Wissensschutz. Umso dunkler (rot) die Farbgebung, desto mehr Wissensschutz wird bei der Wissenskombination gefordert.

[938] Eigene Darstellung.

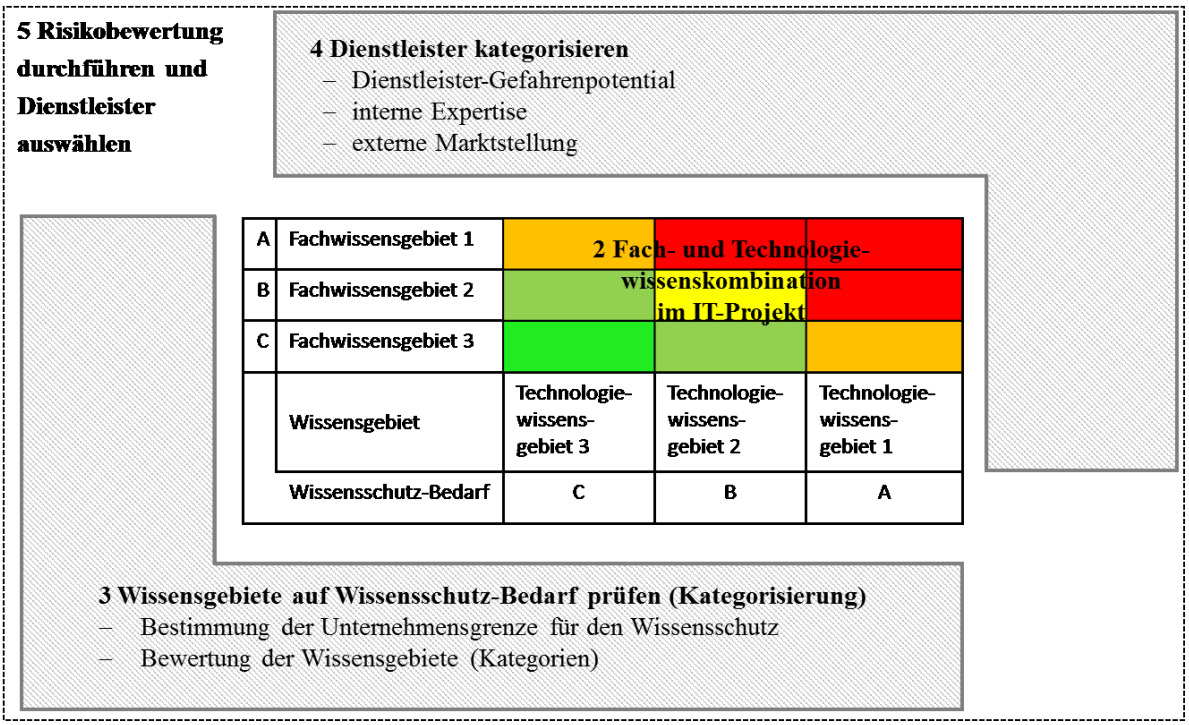

Abbildung 42: Risikobewertung für das Technologie-/Fachwissen im IT-Projekt[939]

Eine Hauptänderung ist die geforderte **Visualisierung der Risikobewertung*, die in den ersten sieben Interviews als eine zu verbessernde Steuerungsübersicht für das Management zurückgemeldet wurde. Denn die Manager müssen auf einen Blick sehen, dass in einem Projekt Handlungsbedarf besteht, zum Beispiel mit einer Ampelanzeige.[940] Die bestehenden Wissensrisiken müssen den Projektakteuren in der Risikobewertung durch eine Visualisierung bewusst werden. Die Interviewpartner forderten, dass mit der Risikobewertung in den bestehenden IT-Projekten transparent und sichtbar werden muss, welches wertvolle Wissen mit den externen Dienstleistern im Status Quo geteilt wird.[941] Nach diesen Forderungen wurde die Risikobewertung aufgearbeitet. Nach der Aufarbeitung gaben die Interviewpartner die Rückmeldung, dass in der Risikobewertung visualisiert und transparent wird:

- welche Wissensgebiete und welche -kombinationen den Unternehmenswert der IT-Beratung ausmachen.[942]
- welche Wissensgebiete in den bestehenden IT-Projekt von welchen Dienstleistern geleistet werden und damit welche Abhängigkeiten existieren.[943]
    - welche Wissensflüsse zu den eingesetzten Dienstleistern in den IT-Projekten nach Fach- und Technologiewissensgebieten bestehen.
    - welche Defaktoabhängigkeiten zu Dienstleistern bestehen, wenn nur diese das Spezialwissen besitzen, mit dem mehrere Auftraggeber-Projekte realisiert werden.[944]
- welches Gefahrenpotential der Dienstleister in Bezug auf das wertvolle und schützenswerte Wissen hat.[945]

---

[939] Eigene Darstellung.
[940] Vgl. IP_3, IP_10.
[941] Vgl. IP_2.
[942] Vgl. IP_10.
[943] Vgl. IP_11.
[944] Vgl. IP_11.
[945] Vgl. IP_11.

- welche Spezialisierung der jeweilige Dienstleister in der IT-Beratung hat und ob diese Spezialisierung gewollt ist.[946]

Zeigt der Status Quo auf, dass der Unternehmenswert einer IT-Beratung und damit das wertvolle und schützenswerte Wissen beim Dienstleister liegen, dann verfügt die IT-Beratung über keinen eigenen Wert.[947] Um dieser Situation entgegenzuwirken wäre eine mögliche *Regel*, dass in wertvollen Wissensgebieten keine externen Dienstleister beteiligt werden.[948] Mehrere Interviewpartner äußerten den Bedarf zur **Kennzeichnung des Handlungsbedarfes* und der **Handlungsempfehlungen*. Angeregt wurden die **Vorgabe von Regeln* und die **Festlegung von Steuerungsgrößen* in der Risikobewertung.[949] Diese *Regeln* und *Steuerungsgrößen* sind von der IT-Beratung festzulegen. Mögliche sind:

- dass das Dienstleister-Gefahrenpotential und dessen Bewertung in den Fach- und Technologiewissensgebieten (Funktion 4) im akzeptierbaren Verhältnis zu der Wissenskategorisierung (Funktion 3) stehen. In Abhängigkeit vom festgestellten Verhältnis und vom ermittelten Wissensschutz für das IT-Projekt (Funktion 2) muss geringer bis hohen Handlungsbedarf für den Wissensschutz vorgegeben werden.
- dass die Eigenfertigungsquote vom zu bewertenden IT-Projekt in Relation zum Wissensschutzbedarf vom IT-Projekt stehen.[950]
- dass vorhandene Mitarbeiter für die wertvollen und schützenswerten Wissensgebiete ausgebildet oder neue Mitarbeiter für diese eingestellt werden.[951]
- dass für wertvolle und schützenswerte Wissensgebiete keine Sourcinganfragen an Dienstleister gestellt werden (Funktion 2).[952]

Details zu Dienstleister auswählen

Für den Auswahlprozess müssen das Ressourcen- und das IT-Sourcing Management die Entscheidung für den Projektmanager vorbereiten, da diese beiden Akteursgruppen eine ganzheitlichere Sicht zum Dienstleister, seinen Projekteinsätzen und der IT-Beratung haben.[953] Für jeden möglichen Dienstleister kann nach der Risikobewertung in neuen IT-Projekten eine Empfehlung ausgesprochen werden. In bestehenden Projekten kann damit eine Risikobewertung der eingesetzten externen Dienstleister erfolgen. In neuen IT-Projekten kann der Projektmanager auf der Grundlage der Risikobewertung und den Informationen aus der Projektkategorisierung (Funktion 2) eine Auswahlentscheidung für oder gegen den Dienstleistereinsatz treffen.

Der Projektmanager muss gegebenenfalls mit dem Ressourcenmanagement nach der Projektsituation abwägen, welchen Stellenwert der Wissensschutz hat. Gleichzeitig ist die vorliegende Projektsituation mit den vorgegebenen Kundenanforderungen (Zeit und Qualität) zu prüfen. Eine Entscheidung zur Akzeptanz eines Restrisikos muss in einer Risikotabelle aufgeführt und

[946] Vgl. IP_4.
[947] Vgl. IP_10.
[948] Vgl. IP_2.
[949] Vgl. IP_6, IP_9, IP_10.
[950] Vgl. IP_5.
[951] Vgl. IP_2.
[952] Vgl. IP_2.
[953] Vgl. IP_11.

begründet werden. Insbesondere wurde in der Pilotierung darauf hingewiesen, dass eine Risikobetrachtung eine Momentaufnahme zu einem bestimmten Zeitpunkt ist, die immer auf dem aktuellen Stand gehalten werden muss.

5.4 Evaluation

Dieses Unterkapitel unterteilt sich in die Modellevaluation im Rahmen der Pilotierung (Abschnitt 5.4.1) und beschreibt anschließend die ausgewählten Evaluationsperspektiven. Wie im Abschnitt 3.1.3 dargestellt, wird das Referenzmodell nach der deployment, epistemologischen und einem Teil der ökonomischen Perspektive in den folgenden Abschnitten evaluiert. Eine weitere vierte Perspektive ist die technische, welche im Rahmen der Arbeit nicht berücksichtigt wurde. In den Abschnitten (5.4.2, 5.4.3, 5.4.4) werden die Kriterien der Aspekte kurz beschrieben und anschließend erfolgt anhand dieser Kriterien die Evaluation in Bezug auf das Modell.

5.4.1 Modellevaluation im Rahmen der Pilotierung

Im Abschnitt 3.3.4 wurde im Rahmen des Forschungsvorgehens die Pilotierung beschrieben. In diesem Abschnitt liegt der Fokus auf der Evaluation des Wissensschutz-Referenzmodells anhand der dokumentierten Interviews. Die Interviews fokussierten die entwickelten Modellfunktionen 2, 3, 4, 5 und damit nicht die strategische Planung (Funktion 1). Diese Funktion 1 ist unternehmensspezifisch und kundenspezifisch zu eruieren.

Funktion 2: Wissensschutz im Rahmen der Projektkategorisierung ermitteln und IT-Projekt-Auswahlprozess

Der erweiterte Projektsteckbrief für die vom Management benannten zu prüfenden IT-Projekte ist im Abschnitt 3.3.4 in der Tabelle 15 bereits dokumentiert und ebenso die Auswahl des *Projektes α*. Bestandteil der Funktion 2 ist auch die Erfassung der Fachwissens- und Technologiewissenskombinationen des *Projektes α*. Diese sind in der Tabelle 38 dargestellt.

Tabelle 38: Erweiterte Projektsteckbrief Projekt α – Fachwissens- und Technologiewissenskombination

Technologiewissen / **Fachwissen**	**Technologiewissen 1**	**Technologiewissen 2**	**Technologiewissen 3**	**Technologiewissen 4**	**Leistungserbringung**
Fachwissen XY1 in der Mobilitätsbranche	100 PT	100 PT	100 PT	100 PT	intern
	50 PT, Implementierungsverantwortliche, Architekt	50 PT, Implementierungsverantwortliche		100 PT, Implementierungsverantwortliche, Architekt	Dienstleister 1
	300 PT Architekt	300 PT Entwickler			Dienstleister 2
	150 PT Architekt				Dienstleister 3
			100 PT Entwickler		Dienstleister 4

Funktion 3: Überprüfung der Wissensgebiete auf Wissensschutz-Bedarf

Zur Vorbereitung des halb-standardisierten Gruppeninterviews konnten in Einzelinterviews mit fünf benannten Schlüsselpersonen die Wissensgebiete (1x Fachwissen, 4x Technologiewissen) des Projektes α begleitend kategorisiert werden. Diese 45-minütigen Einzelinterviews dienten zur Vorbereitung des Gruppeninterviews. Die aufgearbeiteten Bewertungen wurden in die Präsentation vom Gruppeninterview integriert und waren Grundlage der Diskussion.

Für die Interviews wurde eine fünfer Likert-Skala eingesetzt, da sich in der IT-Beratung fünfer und siebener Skalen bei anderen Bewertungen etabliert haben. Die Interviewpartner avisierten in Gesprächen eine geringer abgestufte Bewertungsskala, weshalb die siebener Likert-Skala keine Anwendung fand. Bei der fünfer Likert-Skala ist die fünf der höchste (sehr wichtig / sehr hoch) und die eins der niedrigste Wert (weniger wichtig / gering) der bei den Bewertungskategorien vergeben werden konnte.

Die Kategorisierung der Wissensgebiete des Projektes α sind in der Tabelle 39 und Tabelle 40 dokumentiert. In der Zeile „Sichtweise (Rolle)“ ist die Rolle dokumentiert, die die Bewertung vorgenommen hat. Um eine Visualisierung für das wertvolle und schützenswerte Wissen zu erreichen, wurde eine ABC-Gruppierung mit Farbgebung angewendet:

- A - sehr wertvolles Wissensgebiet und damit sehr schützenswertes Wissen (rot)
- B - wertvolles Wissensgebiet (gelb)
- C - weniger wertvolles Wissensgebiet (grün)

Tabelle 39: Projekt α - Wissenskategorisierung des Fachwissens

	Fachwissen in der IT-Beratung				
Sichtweise (Rolle)	Projekt-manager	Fachliche Berater	Fachliche Architekt	Kunden-manager	Technische Architekt
Kernkompetenz ja / nein	j.	j.	j.	j.	j.
Eigene Expertise	4	4	4	4-4,5	4
Bewertungskategorie	**Fachwissen XY1 in der Mobilitätsbranche**				
Strategie	5	4	4,5	5	3,5
Kundennutzen	5	4,5	4	5	5
Mitbewerberabgren-zung	4	5	3	5	4
Übertragbarkeit	4	3,5	4	3,5	3,5
Wissens-kategorisierung	**A**				

Das Fachwissensgebiet gehört nach der Auffassung der Interviewpartner zu den sehr wertvollen Wissensgebieten. Übereinstimmend wurde das Fachwissensgebiet zur Kernkompetenz der IT-Beratung zugeordnet.

Tabelle 40: Projekt α - Wissenskategorisierung des Technologiewissens

	Technologiewissen in der IT-Beratung											
Sichtweise (Rolle)	P.-Ma	K.-Ma	T.-Ar	P.-Ma	K.-Ma	T.-Ar	P.-Ma	K.-Ma	T.-Ar	P.-Ma	K.-Ma	T.-Ar
Kernkompetenz ja / nein	n.	n.	n.	j.	j.	n.	j.	j.	j.	n.	j.	n.
Eigene Expertise	2	3	4,5	4	4	4	5	3,5	4	1	4	5
Bewertungskategorie	**Technologie-wissen 1**			**Technologie-wissen 2**			**Technologie-wissen 3**			**Technologie-wissen 4**		
Strategie	4	4	3	5	5	1	4	5	5	1	4	1
Kundennutzen	4	5	4,5	5	5	4	4	5	5	5	5	3
Mitbewerberabgrenzung	3	4	4	4	2	2	5	2	4	4	4	2
Übertragbarkeit	5	5	2,5	4	5	4	3	5	4	4	5	4
Wissens-kategorisierung	**A**			**B**			**A**			**B**		

Die Technologiewissen 1 und 3 gehören durch die A-Gruppierung zu den sehr wertvollen Wissensgebieten. Die Technologiewissensgebiete 2 und 4 gehören zu den wertvollen Wissensgebieten und sind gelb markiert.

Werden die Wissenskategorisierung und die Farbgebung von allen möglichen Wissenskombinationen im Projekt α in einer Matrix in Beziehung zueinander gesetzt, ergibt sich die folgende Übersicht, welche in die Risikobewertung (Abbildung 43) übernommen wird.

Tabelle 41: Kombination vom Fachwissen und Technologiewissen im Projekt α

Wissenskategorisierung		**A**	**B**	**A**	**B**
	Technologiewissen / Fachwissen	**Technologie-wissen 1**	**Technologie-wissen 2**	**Technologie-wissen 3**	**Technologie-wissen 4**
A	**Fachwissen XY1 in der Mobilitätsbranche**				

Funktion 4: Dienstleister kategorisieren

Die Ermittlung des Dienstleister-Gefahrenpotentials (Unterkapitel 4.4) für die Dienstleister 1 bis 4 wurden im Rahmen vertiefender Experteninterviews erstellt. Die farblichen Einstufungsergebnisse sind in der Tabelle 42 und Abbildung 43 dargestellt. Die Detailbewertungen können wegen Compliance-Gründen und Rückverfolgbarkeit auch nicht anonymisiert hier dargestellt werden. Das Gleiche gilt für die Dienstleistersteckbriefe der vier Dienstleister, welche für die Interviews genutzt wurden.

Tabelle 42: Projekt α - Dienstleisterkategorisierung nach Gefahrenpotential

Bewertungs-kategorien / Dienstleister	**Dienstleister-Größe**	**Dienstleister-Aktivitäten**	**Dienstleister-Art**	**Dienstleister-Branchen**	**Lernbereitschaft / Lernfähigkeit**	**Innovations-fähigkeit**	**Absorptive DL-Kapazität**	**Erfahrung aus Projekten**	**Dienstleister-Gefahren-potential**
Dienstleister 1									
Dienstleister 2									
Dienstleister 3									
Dienstleister 4									

Für alle kursiv markierten Zahlen wurden Annahmen zugrunde gelegt, weil sich die tatsächlichen Gesamtvolumen erst ergeben, wenn alle Projekte einer IT-Beratung mit dem bewerteten Fach- / Technologiewissen dokumentiert sind.

Für die Bewertung (Tabelle 43, Tabelle 44) der internen Expertise und externen Markstellung wurden zugängliche Informationen, wie interne Dokumente und offizielle Webseiten genutzt sowie das Dienstleistermanagement befragt. Die Anzahl der Personentage (PT) sowie die eingenommenen Rollen der Dienstleister für die Wissensgebiete im Projekt α werden aus der Tabelle 38 übernommen.

Tabelle 43: Projekt α - Dienstleisterkategorisierung zum Fachwissen

		Fachwissen der IT-Beratung
Gesamtvolumen für das Wissensgebiet in der IT-Beratung		*4.000* PT
Auftragsvolumen Dienstleister 1		200 PT Implementierungsverantwortliche und Architekt
Auftragsvolumen Dienstleister 2		600 PT Architekt
Auftragsvolumen Dienstleister 3		150 PT Architekt
Auftragsvolumen Dienstleister 4		100 PT Entwickler
Bewertungskategorie		**Fachwissen XY1 in der Mobilitätsbranche**
Interne Expertise	Dienstleister 1	4
	Dienstleister 2	5
	Dienstleister 3	3
	Dienstleister 4	3
Externe Marktstellung	Dienstleister 1	?
	Dienstleister 2	4
	Dienstleister 3	3
	Dienstleister 4	3
Dienstleister-kategorisierung	Dienstleister 1	B
	Dienstleister 2	**A**
	Dienstleister 3	B
	Dienstleister 4	B
Auftragsvolumen in Personentage (2016) und in Relation zum Gesamtauftragsvolumen der IT-Beratung	Dienstleister 1	200 PT / *4.000 PT = 5%*
	Dienstleister 2	600 PT / *4.000 PT = 15%*
	Dienstleister 3	150 PT / *4.000 PT = 3,75 %*
	Dienstleister 4	600 PT / *4.000 PT = 2,5 %*

Bei den beiden Tabellen (Tabelle 43, Tabelle 44) wird im Folgenden auf die A-Gruppierung eingegangen. Diese A-Dienstleisterkategorisierung zeigt ein mögliches Wissensrisiko bei einem Dienstleistereinsatz auf. Die B-Gruppierung für die Dienstleister 1, 3 und 4 sollten in Bezug auf den Wissensschutz beobachtet werden. Der Dienstleister 2 besitzt nach der Bewertung der internen Expertise und der externen Marktstellung eine A-Gruppierung im Bezug auf das Fachwissensgebiet XY1. Die interne Expertise hat die höchste Bewertung, da der Dienstleister 2 bereits länger die Projektrolle einnimmt und Erfahrungswissen gesammelt hat. Auch die externe Marktstellung des Dienstleisters 2 ist ausgeprägt und hat eine hohe Bewertung erhalten. Unter der Annahme, dass 4.000 PT für dieses Fachwissensgebiet in einem Jahr in der IT-Beratung für IT-Projekte aufgewendet werden, deckt der Dienstleister 2 15 Prozent des Gesamtaufwandes ab. Die Interviewpartner forderten, dass diese Relation zum Gesamtauftragsvolumen

dokumentiert wird, damit bewusst entschieden werden kann, ob diese Spezialisierung des Dienstleisters gewollt ist.

Der Dienstleister 2 hat in den Technologiewissen 1 und 2 ebenso eine A-Gruppierung erhalten (Tabelle 44). Auch diese A-Dienstleisterkategorisierung zeigt ein mögliches Wissensrisiko auf, weil das Technologiewissen 1 von den Projektakteuren als ein sehr wertvolles Wissensgebiet und damit sehr schützenswertes Wissen (A-Gruppierung) bewertet wurde. Unter der Annahme, dass 4.000 PT für dieses Technologiewissen in einem Jahr in der IT-Beratung für IT-Projekte aufgewendet werden, leistet der Dienstleister 2 für das Technologiewissen 1 7,5 Prozent des Gesamtaufwandes.

Tabelle 44: Projekt α - Dienstleisterkategorisierung zum Technologiewissen

		Technologiewissen der IT-Beratung			
Gesamtvolumen für das Wissensgebiet in der IT-Beratung		*4.000* PT	*10.000* PT	*6.000* PT	*2.000* PT
Auftragsvolumen Dienstleister 1		50 PT, Implementierungsverantwortliche, Architekt	50 PT, Implementierungsverantwortliche		100 PT, Implementierungsverantwortliche, Architekt
Auftragsvolumen Dienstleister 2		300 PT Architekt	300 PT Entwickler		
Auftragsvolumen Dienstleister 3		150 PT Architekt			
Auftragsvolumen Dienstleister 4				100 PT Entwickler	
Bewertungskategorie		**Technologiewissen 1**	**Technologiewissen 2**	**Technologiewissen 3**	**Technologiewissen 4**
Interne Expertise	Dienstleister 1	4	4	-	3
	Dienstleister 2	5	5	3	-
	Dienstleister 3	3	-	-	-
	Dienstleister 4	-	-	3	-
Externe Marktstellung	Dienstleister 1	?	?	-	2
	Dienstleister 2	4	5	?	-
	Dienstleister 3	?	?	-	-
	Dienstleister 4	-	-	3	-
Dienstleisterkategorisierung	Dienstleister 1	B	B	-	B
	Dienstleister 2	A	A	B	-
	Dienstleister 3	B	?	-	-
	Dienstleister 4	-	-	B	-
Auftragsvolumen in Personentage (2016) und in Relation zum Gesamtauftragsvolumen der IT-Beratung	Dienstleister 1	50 PT / *4.000 PT = 1,25%*	50 PT / *10.000 PT = 0,5%*	-	100 PT / *2.000 PT = 5%*
	Dienstleister 2	300 PT / *4.000 PT = 7,5%*	300 PT / *10.000 PT = 3%*	-	-
	Dienstleister 3	150 PT / *4.000 PT = 3,75%*	-	-	-
	Dienstleister 4	-	-	100 PT / *6.000 PT = 1,67%*	-

In der anschließenden Risikobewertung (Funktion 5) werden alle Informationen in einer Übersicht visualisiert dargestellt, damit Transparenz für eine nachvollziehbare Entscheidung vorliegt.

Funktion 5: Risikobewertung durchführen und Dienstleister auswählen

Bei dem vorliegenden Projekt α waren die Dienstleister bekannt und die vorgenommene Risikobewertung sollte im Rahmen des Gruppeninterviews überprüft werden, ob Handlungsbedarfe im Bezug auf den Wissensschutz bestehen. Bei dem Gruppeninterview wurde die Abbildung 43 als das zentrale Ergebnis für das Projekt α vorgestellt und anschließend dazu diskutiert. Die erarbeiteten Bewertungen aus den vorangegangenen Funktionen sind in die Abbildung eingearbeitet. In der Übersicht sind für das Verständnis vom Modell drei weitere Fachwissensgebiete (XY2, XY3, XY4) aufgenommen, damit das Gesamtbild und die Methodik verdeutlicht wird. Das Projekt α (Pα) ist in den relevanten Wissenskombinationen vom Pilotprojekt gekennzeichnet. Durch die Matrixdarstellung wird deutlich, dass sich zwei Wissenskombinationen vom Projekt α im roten Quadranten befinden. Die anderen beiden Wissenskombinationen sind orange markiert. Diese Darstellungsweise mit den verschiedenen Quadranten ist bereits in der Abbildung 42 zu sehen. Im oberen rechten Bereich der Matrix befinden sich immer die schützenswerten Wissenskombinationen (Fachwissen / Technologiewissen).

In dem Gruppeninterview wurde zu dem identifizierten Wissensrisiko, das vom Dienstleister 2 (orange eingefärbt) ausgeht, diskutiert. Dabei wurde die Empfehlung ausgesprochen, dass das Fachwissen XY1 in Kombination mit dem Technologiewissen 1 von einem internen Mitarbeiter wegen des bestehenden Wissensrisikos bearbeitet werden sollte.

Bei dem Projekt-Einsatz der Dienstleister 1, 3 und 4 geht nach dem Informationsstand keine dringende Handlungsempfehlung aus Sicht des Wissensschutzes aus. Der Projektmanager räumte jedoch ein, dass bei den Technologiewissensgebieten 1 und 3 interne Mitarbeiter aufgebaut werden sollten.

				Auftragsvolumen in PT: Interne Expertise: Externe Marktstellung:	- - -	- - ?	150 3 ?	- - -	DL3
				Auftragsvolumen in PT: Interne Expertise: Externe Marktstellung:	100 3 2	50 4 ?	50 4 ?	- - -	DL1
				Auftragsvolumen in PT: Interne Expertise: Externe Marktstellung:	- - -	- - -	- - -	100 3 3	DL4
				Auftragsvolumen in PT: Interne Expertise: Externe Marktstellung:	- - -	300 5 5	300 5 4	- 3 ?	DL2
6k ↓	Ja	4	A	Fachwissen XY2 in der Logistikbranche					? ? ?
2k ↑	Ja	4	A	**Fachwissen XY1 in der Mobilitätsbranche**	Pα	Pα	Pα	Pα	600 5 4
8k ↓	Nein	3	B	Fachwissen XY4 in der Personalbranche					? ? ?
10k ↓	Nein	2	C	Fachwissen XY3 in der IT-Branche					? ? ?
				Fachwissens-gebiet / Technologie-wissensge-biet	**Technologie-wissen 4**	**Technologie-wissen 2**	**Technologie-wissen 1**	**Technologie-wissen 3**	
				Wissenskategorisierung	B	B	A	A	
				Eigene Expertise	3	4	3	4	
				Kernkompetenz	Nein	Ja	Nein	Ja	
				Gesamt-Volumen in PT (Tendenz)	2k ↓	10k ↑	4k →	6k ↑	

? ? ?	? ? ?	? ? ?	? ? ?
100 3 3	200 4 ?	150 3 3
? ? ?	? ? ?	? ? ?	? ? ?
? ? ?	? ? ?	? ? ?	? ? ?

Abbildung 43: Risikobewertung für das Technologie-/Fachwissen im IT-Projekt α

5.4.2 Deployment Perspektive

Aus der fokussierten deployment Perspektive definiert FRANK die drei Aspekte Verständlichkeit, Einsatztauglichkeit und Einstellung. Zu jedem dieser Aspekte werden Kriterien aufgeführt, die in der Tabelle 45 dokumentiert sind und deren Erfüllung mit Bezug auf die Arbeit nachfolgend zusammengefasst werden.

Tabelle 45: Evaluation aus der deployment Perspektive[954]

Aspekte	Verständlichkeit	Einsatztauglichkeit	Einstellung
Kriterien	• Strukturen für die Dokumentation • Umfassende Dokumentation • Szenarien und Beispiel • Modellierungssprache • Terminologie • Intuitive Zugriff auf grafische Darstellung • Ansichten für verschiedene Interessensgruppen	• Unterstützung der Modellnutzer zum relevanten Zweck • Unterstützt zukünftige Technologien / Methoden	• „Not invented here“ - Syndrom • Reputation der Modellentwickler • Widerstand gegen organisatorische Veränderungen • Kulturelle Barrieren

Deployment Perspektive: Verständlichkeit

Nach diesem Aspekt ist eine *umfassende* und *strukturierte Dokumentation* mit *Beispielszenarien* zu evaluieren. Zudem müssen die Beschreibungen auf einer *Modellierungssprache* und auf einer definierten *Terminologie* aufbauen. Des Weiteren sind eine *grafische* nachvollziehbare *Darstellungsweise* für verschiedene *Interessensgruppen* zu wählen.

Um die Dokumentation zu strukturieren wird eine semiformale *Darstellungsweise* mit den *Modellierungselementen* von ARIS in Form einer eEPK (Abbildung 34) / EPK (Abbildung 35) genutzt, die innerhalb der Funktionen (Unterkapitel 5.2 und 5.3) im Detail erläutert werden. Um die *Verständlichkeit* der EPK und der FZD zu gewährleisten, wurden diese einem Prozessmodellierer mit langjähriger Erfahrung vorgelegt und einem Review unterzogen. Durch dieses Review ist sichergestellt, dass die Gestaltungsbeschreibung aller relevanten Prozesse und Strukturen verständlich sind und es somit als Vorlage für ein organisatorisches Konzept verwendet werden kann. Wie im Abschnitt 3.2.1 dokumentiert, wird mit dieser *Darstellungsweise* auch die Einführungszeit reduziert. Das beschriebene Referenzmodell, die Ergebnispräsentation, der Interviewleitfaden mit der Interviewunterlage und den zwei *Beispielprojekten* dokumentieren das Modell für die Wissenschaft und IT-Beratungen umfassend.

Damit die Experten ein Verständnis zu einem kritischen Wissensschutz-*Szenario* erhalten, wurden die Interviewpartner bei der Themenvorstellung gebeten sich vorzustellen, dass sie ein IT-Projekt mit den folgenden Eigenschaften verantworten:

- sehr innovativ und strategisch wichtig für den Auftraggeber und für die Kundenbeziehung
- die Wettbewerbsfähigkeit des Auftraggebers ist vom IT-Projekt abhängig

[954] Vgl. Frank 2006, S. 131.

- die Wettbewerbsfähigkeit der IT-Beratung ist vom IT-Projekt abhängig

In diesem IT-Projekt wird mit mehreren externen Mitarbeitern eines Dienstleisters zusammengearbeitet und der externe Dienstleister wie folgt charakterisiert:

- der Dienstleister ist größer als die IT-Beratung
- der Dienstleister agiert international und hat Büros in fünfzig Ländern
- seine Auftraggeber kommen aus verschiedenen Branchen (marktübergreifend)
- er ist innovativ, lernbereit und lernfähig

Die aufgezeigte Problemsituation des obligatorischen Wissensschutzes im IT-Projekt war den Interviewpartnern spätestens nach dem *Beispielszenario* bewusst. Dieses bewusst machen, dass in dieser Situation ein Wissensrisiko vorliegt und das der Dienstleister das Potential hat die Wettbewerbsfähigkeit zu gefährden, war eine entscheidende Erkenntnis für die Notwendigkeit des Wissensschutzes bei der ISE. Die beschriebenen kritischen Ereignisse der Experten verifizieren und ergänzen die skizzierte Problemsituation.

Um ein gemeinsames Verständnis für die verwendete Modell-*Terminologie* und seine Kategorien zu dokumentieren, wurden diese definiert, damit sie nach den Vorgaben einheitlich bewertet werden können. Diese Definitionen wurden den Experten vorgelegt und in der Interviewstudie präzisiert, wie in den Modell-Abschnitten (Unterkapitel 5.2 und 5.3) dokumentiert.

Für die *grafische Darstellung* werden die verschiedenen Sichten (Funktionen 1 bis 4) der Projektakteure (*Interessensgruppen*) in der Risikobewertung zusammengeführt (Abbildung 42). Diese Visualisierung wurde ab dem achten Interview vorgestellt, damit das Management eine Steuerungsübersicht für Handlungsbedarfe erhält. Diese *grafische Darstellungsweise* der Risikobewertung wurde von den Interviewpartnern (IP_8 bis IP_11) und im anschließenden Gruppeninterview bestätigt. Im Abschnitt 5.3.2 sind die Rückmeldungen zum erzielten Mehrwert dieser Ansicht dokumentiert. Mit diesen Ausführungen ist der Aspekt der *Verständlichkeit* evaluiert.

Deployment Perspektive: Einsatztauglichkeit

Nach diesem Aspekt sind die Modellnutzer zu einem *relevanten Zweck* zu unterstützen, das eine *Anforderungsanalyse* notwendig macht (Tabelle 45). Des Weiteren muss der Einsatz von *zukünftigen Technologien* oder *Methoden* sichergestellt werden.

Wie bereits ausgeführt, gehört der Wissensschutz zu den kritischen Erfolgsfaktoren für ein WM und ist damit ein *relevantes Themengebiet*. Zudem sind Unternehmen nach der ISO Norm 9001 seit 2015 verpflichtet WM und damit auch den Wissensschutz einzuführen. Die *Relevanz* des entwickelten Wissensschutz-Referenzmodells dokumentieren auch die identifizierten Forschungslücken in Theorie und Praxis (Unterkapitel 1.2). Die Vorinterviews zur Themenfokussierung sind Bestandteil der *Anforderungsanalyse* für das entwickelte Referenzmodell, sie grenzen das Thema ein und zeigen den praktischen Bedarf auf. Das Thema ist auch deshalb relevant, weil durch die Anwendung des Referenzmodells die Wissensrisiken für eine IT-Beratung und seine Auftraggeber reduziert werden und das sichert und baut die Wettbewerbsvorteile aus, damit sie langfristig bestehen. In diesem Zusammenhang wurde mit potentiellen Auftraggebern

für IT-Projekte zum Wissensschutz-Referenzmodell bei einer Themen-Session innerhalb eines Workshops diskutiert.[955] Einige Teilnehmer postulierten, dass sie die IT-Projekte an einen Dienstleister abgeben und dieser sich um alles kümmert, weil sie selbst nicht die IT-Expertise besitzen. Diese Rückmeldung zeigt, dass auch die Auftraggeber wenig zum Wissensschutz sensibilisiert sind und wie sie mit ihrem über mehrere Jahre erarbeiteten Fachwissen umgehen. Damit wird die Relevanz des Themas für eine IT-Beratung und der Schutz der wertvollen Wissensgebiete (Wettbewerbsvorteile) nochmals hervorgehoben.

Die *Einsatztauglichkeit* bestätigten die Interviewpartner der IT-Beratung damit, dass die Dokumentation zum entwickelten Referenzmodell eine geschlossene Systematik ist, das von der Idee bis zum Ziel nachvollziehbar ist.[956] Mit Bezug auf diese geschlossene Systematik wird wegen der aufbauenden Abhängigkeit der Modell-Funktionen empfohlen, dass Modell in die bestehenden Projektprozesse einzubinden. Dennoch können in Abhängigkeit von der vorliegenden Projektorganisation auch einzelne Modell-Funktionen schrittweise eingeführt werden. Mit der Umsetzung des Modells lassen sich Aussagen zum Wissensschutz ableiten und auch ihre Identität bestimmen, auf denen der Wert einer IT-Beratung beruht. Nach den Anmerkungen der Interviewpartner werden Abhängigkeiten oder Defaktoabhängigkeiten zu Dienstleistern in Bezug auf Wissen sichtbar und können als ableitende Maßnahme adressiert werden.

Das entwickelte Referenzmodell ist *technologieunabhängig* und ist für *zukünftige Technologien* offen. Es kann als Grundlage für die Entwicklung von Software, die die Projektprozesse in einer IT-Beratung unterstützen, verwendet werden. Bei bereits bestehender Software zu den IT-Projektprozessen können die im Modell identifizierten Wissensschutz-Kategorien in die bestehende Anwendung integriert werden. Mit diesen Ausführungen ist der Aspekt der *Einsatztauglichkeit* evaluiert.

Deployment Perspektive: Einstellung

Nach diesem Aspekt sind die *Einstellungen der Modellnutzer* und die *Reputation des Modellentwicklers* zu evaluieren (Tabelle 45). Zudem sind zu der geplanten *organisatorischen Änderung* der Widerstand und die *kulturellen Barrieren* zu bewerten.

Die Interviewpartner haben beim vermittelnden Interviewbestandteil Verständnisfragen gestellt und beim ermittelnden Interviewbestandteil auch intensiv diskutiert. Die potentiellen Modellnutzer zeigten eine entsprechende offene *Einstellung* gegenüber der Spezifizierung der Kategorien und weiteren Modellkategorien (Tabelle 27). Die Anpassungen und Erweiterungen des Modells sind in der Tabelle 25 und den Funktionsbeschreibungen (Unterkapitel 5.2 und 5.3) gekennzeichnet. So werden zum Beispiel die Projektkategorisierung und die vier Bewertungskategorien (*Strategie, Kundennutzen, Mitbewerberabgrenzung, Übertragbarkeit*) aus der Literatur zur Bestimmung der Unternehmensgrenze im Forschungsprozess präzisiert und bestätigt.

---

[955] Themen-Session beim WIMA-Camp am 19.06.2018.
[956] Vgl. IP_8.

Eine Besonderheit dieser Arbeit ist, dass der Modellentwickler dauerhaft in das Forschungsobjekt eingebunden war und deshalb im Vergleich zu anderen Aktionsforschungsarbeiten nicht nur zeitweise praktische Einblicke hatte. Damit konnte zum einen die langjährige Projekterfahrung des Autors in die Untersuchung aufgenommen werden. Zum anderen wurde durch die Unternehmenszugehörigkeit (*Reputation*) eine Vertrauenssituation mit den internen Experten bei den Interviews geschaffen, um die sensitiven Erfahrungen zum Wissensschutz zu erhalten. Ein externer Forscher hat nicht die interne Projektexpertise und hätte damit nicht auf der Erfahrungsebene die Experten befragen und mit ihnen diskutieren können. Jedoch könnte durch die dauerhafte Einbindung in das Forschungsobjekt auch die Gefahr eines Bias beim Modellentwickler vorliegen. Aufgrund der langen Unternehmenszugehörigkeit könnte eine Voreingenommenheit zum Modell bestehen, der jedoch mit dem zyklischen Prozess und der Samplingstrategie entgegengewirkt wurde. Mit der Auswahl der Interviewpartner nach einer Samplingstrategie wurde ebenso dem sozial erwünschten Antwortverhalten entgegengewirkt.[957] Auf die jeweilige Fachkenntnis der Experten und auch auf deren angeeigneten Erfahrungen in anderen Unternehmen wurde in jedem Interview eingegangen.

Der zu evaluierende Widerstand zur *organisatorischen Änderung* wird eher gering bewertet. Das ist darauf zurückzuführen, dass durch das Bewusst machen der existierenden Wissensrisiken die Projektakteure auf den Wissensschutz sensibilisiert werden. Zudem sehen die Projektakteure die Notwendigkeit ihre erarbeiteten Wettbewerbsvorteile zu sichern und damit auch die Sicherung des eigenen Arbeitsplatzes. Des Weiteren können die im Modell identifizierten Kategorien in die bestehenden Projektmanagement-Prozesse mit geringem Aufwand aufgenommen werden. Damit ist für die Realisierung des Wissensschutz-Referenzmodells keine eigenständige Anwendung zu entwickeln. IT-Beratungen die einen Projektbereich zur ISE etablieren wollen, können das Wissensschutz-Referenzmodell mit den Phasen und Funktionen als Vorlage verwenden. Mit diesen Ausführungen ist der Aspekt der Einstellung evaluiert.

Die Evaluation der *kulturellen Barrieren* ist ein interessantes weiteres Kriterium. Dieses war außerhalb des Fokus und sollte bei weiterer Forschung betrachtet werden.

5.4.3 Epistemologische Perspektive

Die epistemologische Perspektive unterteilt sich in die vier Aspekte Evaluation von Theorien, generische Prinzipien, kritische Distanz und wissenschaftlicher Fortschritt. Die Kriterien zu diesen Aspekten sind in der Tabelle 46 dokumentiert.

[957] Vgl. Möhring & Schlütz 2010, S. 61 ff.

Tabelle 46: Evaluation aus der epistemologischen Perspektive[958]

Aspekte	Evaluation von Theorien	Generische Prinzipien	Kritische Distanz	Wissenschaftlicher Fortschritt
Kriterien	• Genaue Beschreibung der Kerntheorie in Bezug auf die jeweiligen Realweltkonzepte • Genaue Beschreibung der zugrundeliegenden Annahmen	• Verallgemeinerung • Originalität • Entscheidung	• Subjektivität der zugrundeliegenden Entscheidungen • Bias durch bekannte Modellierungssprache • Ein hoher Verbreitungsgrad kann mit hoher Qualität verwechselt werden	• Diskussion der langfristigen Forschungsziele • Ausführliche Modelldokumentation im Hinblick auf generische Prinzipien und langfristige Forschungsziele • Vergleich mit Alternativen

Epistemologische Perspektive: Evaluation von Theorien

Nach diesem Aspekt ist die *Kerntheorie* in Bezug auf die jeweiligen Realweltkonzepte und die zugrundeliegenden *Annahmen* genau zu beschreiben. Die Forschungsarbeit liefert in Bezug auf IT-Sourcing in einer Prinzipal-Agenten-Beziehung und der Betrachtung des Wissensschutzes beim Dienstleistereinsatz eine der ersten Erkenntnisse. Die Prinzipal-Agent-Theorie mit ihren *Annahmen* bildet die *Haupttheorie* für diese Arbeit (Abschnitt 2.3.1). Die weiteren theoretischen Ansatzpunkte (Transaktionskostentheorie, *relationalen Perspektive*, *Resource-based view* und *Knowledge-based view*) wurden im Abschnitt 2.3.2 beschrieben.

Die Bewertung und der wissenschaftliche Beitrag (neue Artefakte) begründet sich in der Erweiterung der Lösungsansätze *Signalisieren*, *Screening* und *Monitoring* der Prinzipal-Agent-Theorie. Diese werden um die Wissensschutzerkenntnisse der Literatur und der Praxis ergänzt. Die neuen Artefakte sind in die Referenzmodell-Phasen mit ihren Funktionen integriert.

Epistemologische Perspektive: Generische Prinzipien

Nach diesem Aspekt sind die Kriterien *Verallgemeinerung*, *Originalität* und *Entscheidung* zu erfüllen. Die Rückmeldung der Interviewpartner zur *Verallgemeinerung* ergab, dass der Modell-Grundgedanke für die IT-Projekte auch für die Technologieberatungs-, Strategieberatungs- und Produktentwicklungsprojekte, bei denen Dienstleister ausgewählt werden sollen, angewendet werden kann. Dieses Feedback zeigt die mögliche *Verallgemeinerung* des entwickelten Modells auf, das für eine geplante Anwendung noch geprüft werden sollte.

Einige Interviewpartner waren zu Beginn des Interviews unsicher wie sie diese skizzierte Problemstellung lösen könnten und äußerten in diesem Zusammenhang ihr ausdrückliches Interesse am Lösungsweg. Die *Originalität* des Referenzmodells und damit die ideenreiche Herangehensweise bestätigt sich auch in der Schlussbemerkung der Interviewpartner. Demnach wird es als eine geschlossene Systematik verifiziert, das von der Idee bis zum Ziel nachvollziehbar ist und das damit Aussagen zum Wissensschutz abgeleitet werden können.[959]

[958] Vgl. Frank 2006, S. 135.
[959] Vgl. IP_8.

Die *Entscheidungen* für oder gegen den Wissensschutz, die bei der Anwendung des Modells getroffen werden, müssen nicht dem bewerteten Wissensrisiko entsprechen. Demnach ist auch bei einem bestehenden Risiko situationsabhängig zu bewerten, ob eine Dienstleisterbeziehung bei einem schützenswerten und wertvollen Wissensgebiet eingegangen wird, z. B. bei Zeitkritikalität mit drohender Vertragsstrafe. Bei einer *Entscheidung* für oder gegen den Wissensschutz muss den verantwortlichen Projektakteuren das Wissensrisiko bekannt und bewusst sein.

Epistemologische Perspektive: Kritische Distanz

Nach diesem Aspekt sind die *Subjektivität* der zugrundliegenden Entscheidungen und der Bias durch bekannte *Modellierungssprachen* zu bewerten. Zudem kann bei einer Evaluation ein hoher *Verbreitungsgrad* mit hoher Qualität verwechselt werden.

Der *Subjektivität* konnte mit den Experteninterviews entgegengewirkt werden, da die Experten nach der aufgeführten Samplingstrategie (maximalen Kontrastierung) ausgewählt wurden. Wie bereits aufgeführt, wurde das Modell von Interview zu Interview präzisiert und bestätigt. Alle Prozesse der untersuchten IT-Beratung sind in einer Prozess-Bibliothek mit weiterführenden Dokumenten beschrieben, die alle Projektmitarbeiter als Vorgabe nutzen müssen. Die bestehende Prozess-Bibliothek basiert auf der semiformalen Darstellungsweise mit den Modellierungselementen von ARIS. Auch einem möglichen Bias durch die bekannte *Modellierungssprache* konnte mit einem Review eines Prozessmodellierers mit langjähriger Erfahrung entgegengewirkt werden. Somit wurden die Prozessformulierungen des Modells geprüft, damit sie in die bestehende Prozess-Bibliothek aufgenommen werden kann.

Die identifizierten wissenschaftlichen Veröffentlichungen zum Wissensschutz basieren wie weiter oben geschrieben zumeist auf einzelnen theoretischen Erkenntnissen, die das Modell zusammenfasst. Damit ist der *Verbreitungsgrad* der identifizierten Kategorien zum Wissensschutz in der Praxis nicht dokumentiert und deshalb könnte erst später eine Qualität bewertet werden. Jedoch könnte wegen der erwähnten Geheimhaltung zur Sicherung der Wettbewerbsvorteile vom Unternehmen, der Verbreitungsgrad des entwickelten Referenzmodells schwer zu verifizieren sein.

Epistemologische Perspektive: wissenschaftlicher Fortschritt

Nach diesem Aspekt sind die Kriterien einer *ausführlichen Modellbeschreibung* im Hinblick auf die generischen Prinzipien und eine Diskussion der *langfristigen Forschungsziele* zu erfüllen. Zudem sind *Alternativen* zu vergleichen. Die Beschreibung im Unterkapitel 5.1, 5.2 und 5.3 mit den Hinweisen der Interviewpartner dokumentieren das Modell umfassend. Das Unterkapitel 6.3 diskutiert und gibt Anregung zur *weiterführenden Forschung*.

Eine *Alternative* zum Referenzmodell ist der erwähnte Einsatz eines übergreifenden Experten (Gatekeeper), um den Wissensschutz im IT-Projekt mit externen Dienstleistern sicherzustellen. In der Literatur wird auf diesen Ansatz verwiesen, aber es wird nicht ausgeführt, was genau dieser Experte für Aufgaben hat. Zudem sollte die Entscheidung zum Wissensschutz eine gemeinschaftliche und keine eines Individuums sein. Jedoch könnte der Einsatz eines übergreifenden Experten in anderen Situationen und abhängig von der Organisationsform als sinnvoll

bewertet werden. Ein weiterführender Vergleich mit dieser Alternative war nicht möglich, da kein (Referenz-)Modell oder weitere Details zu dem erwähnten Ansatz in der Literatur vorliegen.

5.4.4 Ökonomische Perspektive

Bei der Evaluation aus der ökonomischen Perspektive mit ihrem Fokus auf Kosten entstehen Schwierigkeiten, da im Rahmen der Arbeit das Wissen einer IT-Beratung und deren erfolgreiche Wissensschutz diffizil monetär bewertet werden konnte. Die Kosten und damit der Aufwand für die Implementierung des Wissensschutzes in einer IT-Beratung ist von mehreren Faktoren abhängig. Diese sind zum Beispiel:

- die vorliegenden implementierten Projekt-Prozesse, Mitarbeiteranzahl, Mitarbeiterqualifikationen, Strategie, Fach- und Technologiewissensgebiete einer IT-Beratung,
- der Typ, die Attraktivität und der Umfang der IT-Projekte,
- die Branchen, die Anzahl und die Strategie der Auftraggeber bzw. Kunden,
- die Größe, die Aktivitäten, die Art, die Branche und die Anzahl der Dienstleister.

Nach der Rückmeldung der Interviewpartner ist eine Kategorisierung der Wissensgebiete (Funktion 3) zeitnah möglich, vorausgesetzt die entsprechenden Experten werden involviert.

Beim Fokus auf die Vermögenswerte der ökonomischen Perspektive sind die Aspekte der Verbreitung, des Einsatzes und die Technologieänderung mit seinen Kriterien zu bewerten. Auch hier entstehen Schwierigkeiten bei der Bewertung. Bei den Aspekten Verbreitung und Einsatz ist, wie bereits aufgeführt, jedes Unternehmen im Sinne des Wissensschutzes bestrebt Wissen zu erhalten. Jedoch möchte es wegen des Erhalts der Wettbewerbsvorteile kein oder kaum Wissen aus wertvollen und schützenswerten Wissensgebieten weitergeben. So sensibilisierten die Gremien- und Verbandsvertreter bei den BITKOM Arbeitskreisen zum Wirtschaftsschutz die Unternehmensvertreter und präsentierten ihre Erfahrungen zum Thema. Die anwesenden Unternehmensvertreter rezipierten und diskutierten das geteilte Wissen, weil sie vermutlich wie der Autor der Arbeit von der Unternehmenskommunikation angewiesen wurden, kein Wissen vom Unternehmen ohne Freigabe nach außen zu geben. Das zeigt, dass die verantwortlichen Manager, zumindest bei Gremienbeteiligungen der Mitarbeiter außerhalb des Unternehmens in Bezug auf *Wissen-Teilen*, sensibilisiert sind. Jedoch zeigen die Interviews, dass der Wissensschutz in den IT-, Produktentwicklungs- und Strategieberatungsprojekten, bei denen Dienstleister beteiligt werden, wenig Beachtung findet. Wegen der Geheimhaltung kann dieser Aspekt für das Modell im Rahmen dieser Arbeit nicht evaluiert werden. Zudem würde die Information ein Wissensschutzmodell einzuführen kaum ein Unternehmen öffentlich machen, noch würde die Einführung eines solchen Modells auf Nachfrage wahrscheinlich nicht bestätigt werden. Denn die langfristige Existenz des Unternehmens und damit die Wettbewerbsfähigkeit muss gesichert sein.

Bei der Evaluation legt die Arbeit einen Fokus auf Leistungen und ihren Aspekten der Koordination und dem Wissensmanagement, weil Wissensschutz ein Bestandteil vom Wissensmanagement ist (Abschnitt 2.1.2 und 2.1.3), wie bereits geschrieben. Zu jedem dieser Aspekte

werden von FRANK Kriterien aufgeführt, die in der Tabelle 47 dokumentiert sind und deren Erfüllung in Bezug auf die vorliegende Arbeit nachfolgend zusammengefasst sind.

Tabelle 47: Evaluation aus der ökonomischen Perspektive - Leistungen[960]

Aspekte	Koordination	Wissensmanagement
Kriterien	• Überwindet Kommunikationsbarrieren im Unternehmen • Fördert Kommunikation mit externen Partnern • Verbessert Koordination von Geschäftsprozessen • Fördert interorganisationale Koordination	• Fördert Internationale Verbreitung von relevantem Wissen • Unterstützt Entwicklung von relevanten Mitarbeiterfähigkeiten • Fördert organisatorischen Wissensaustausch • Integriert relevantes externes Wissen • Bringt neue Mitarbeiter, Geschäftspartner auf neuesten Stand • Fördert einheitliche, unternehmensweite Terminologie

Ökonomische Perspektive: Koordination

Nach diesem Aspekt muss evaluiert werden, ob mit dem Referenzmodell *Kommunikationsbarrieren* im Unternehmen überwunden werden und ob die *Kommunikation* mit externen Partnern gefördert wird. Zudem zu bewerten ist, ob die *interorganisationale Koordination* und die *Koordination der Geschäftsprozesse* durch den Modelleinsatz verbessert und gefördert werden.

In der Tabelle 25 sind die Phasen, Funktionen und die verantwortlichen Projektakteure identifiziert und diese können nach dem definierten Prozess (Abbildung 34 und Abbildung 35) ihre Funktionen umsetzen. Damit ist die Verantwortlichkeit transparent und die Projektakteure müssen sich zu den definierten Kategorien austauschen, womit die *Kommunikationsbarrieren* überwunden werden.

Zu den Geschäftspartnern gehören die Auftraggeber (Kunden) der IT-Projekte und die externen Dienstleister. Damit eine IT-Projekt-Wissensschutzstrategie (Funktion 1) entwickelt werden kann, ist eine Strategie für den Kunden und Dienstleistersteckbriefe zu erstellen. Die kommunikative Abfrage von relevanten Informationen um die Dienstleister zu kategorisieren und auch die *Kommunikation* mit dem Kunden, ist somit notwendig. Das fördert die *interorganisationale Koordination*. Mit der eEPK (Abbildung 34) ist ein *Geschäftsprozess* skizziert, der die *Koordination* bei der Initialisierungs- und Definitionsphase von IT-Projekten mit Bezug auf den Wissensschutz verbessert.

Ökonomische Perspektive: Wissensmanagement

Nach diesem Aspekt ist zu evaluieren, ob das Modell *relevantes externes Wissen* integriert und ob durch das Modell die *internationale Verbreitung* von relevantem Wissen und der organisatorische *Wissensaustausch*, aufbauend auf einer definierten *Terminologie*, gefördert wird. Zu-

[960] Vgl. Frank 2006, S. 129.

dem ist zu bewerten, ob durch das Modell die Mitarbeiter und Geschäftspartner auf einen aktuellen *Wissensstand* gehalten werden und ob die Entwicklung relevanter *Mitarbeiterfähigkeiten* durch den Modelleinsatz unterstützt werden.

Bei der Modellentwicklung wurde sichergestellt, dass relevantes externes Wissen aus *Literature Reviews*, Experteninterviews und Gruppeninterviews aufgenommen wurden. Bei der Beschreibung der Funktionen (1 bis 5) sind alle aufgenommenen externen Erkenntnisse zur Nachvollziehbarkeit dokumentiert. Jede aufgenommene Kategorie wurde definiert und auch die Definitionen einem Review in den Interviews unterzogen. Damit ist eine erste einheitliche und unternehmensweite *Terminologie* dokumentiert, auf denen IT-Beratungen aufbauen können. Mit dem Modell wird das wertvolle und schützenwerte Wissen bei den IT-Projektakteuren identifiziert und kann somit in einer IT-Beratung gehalten werden. Identifizierte Wissensgebiete, die nicht für die Wettbewerbsvorteile der IT-Beratung relevant sind, können mit einem Dienstleister geteilt werden. Das fördert auch den organisatorischen *Wissensaustausch*, in dem nur das Wissen geteilt wird, was nach der gemeinschaftlichen Entscheidung der Projektakteure geteilt werden darf.

Die Interviewpartner merkten an, dass mit dem Modell die Wissensgebiete identifiziert werden, in denen die internen Mitarbeiter entwickelt werden müssen, damit das wertvolle und schützenswerte Wissen in der IT-Beratung bleibt. Die Entwicklung von relevanten *Mitarbeiterfähigkeiten* war nicht im Fokus, jedoch kann nach der Rückmeldung der Interviewpartner dieser Mehrwert des Modells dokumentiert werden. So könnte auch gezielt ein führender Dienstleister zu einem Wissensgebiet involviert werden, der die *Mitarbeiterfähigkeiten* einer IT-Beratung entwickelt, damit interne Innovationen ohne Dienstleistereinsatz vorangetrieben werden können. Aufbauend auf dem dokumentierten Prozess (Abbildung 34 und Abbildung 35) und der Funktionsbeschreibung können neue interne Mitarbeiter auf den neuesten *Wissensstand* gebracht werden. Neue Geschäftspartner wie Auftraggeber können auf der Grundlage der Modellprozesse, auf den aktuellsten *Wissensstand* gebracht werden, wenn dieses Vorgehen von der IT-Beratung gewollt ist. Geschäftspartner wie externe Dienstleister sind wegen der Sicherung von Wettbewerbsvorteilen nicht über den Wissensschutz und die Prozesse zu informieren.

Damit schließt das Kapitel zum Wissensschutz-Referenzmodell ab. Aus diesen Forschungsergebnissen lassen sich praktische Implikationen ableiten, die im nächsten Kapitel diskutiert werden.

6 Synthese und Ausblick

Das Kapitel 4 mit dem Forschungsstand und das entwickelte Wissensschutz-Referenzmodell im Kapitel 5 dokumentieren die Ergebnisse, die im Weiteren zusammengefasst und diskutiert werden. Dazu gehören die Beantwortung der Forschungsfragen im Unterkapitel 6.1 bevor die theoretischen und praktischen Implikationen und mögliche Limitationen im Unterkapitel 6.2 beschrieben werden. Ein Ausblick auf zukünftige Forschungsthemen komplettiert die Arbeit (Unterkapitel 6.3).

6.1 Beantwortung der Forschungsfragen

Ausgehend vom erkannten Defizit, dem Fehlen konkreter Gestaltungsempfehlungen für ein Risikoinformationssystem für den Wissensschutz in IT-Projekten mit externen Dienstleistern, leistet das Forschungsdesiderat einen Beitrag um die hergeleiteten Forschungslücken im Kapitel 1 zu untersuchen. Für das Forschungsprojekt wurden auf dieser Basis die Forschungsfragen formuliert, damit die erarbeitete Gestaltungsempfehlung in Form eines Wissensschutz-Referenzmodells in IT-Beratungen verwendet werden kann. Die Leitfrage hierbei lautet:

Wie muss ein Risikoinformationssystem einer IT-Beratung zur Unterstützung des Wissensschutzes bei der ISE mit externen IT-Dienstleistern gestaltet sein?

Um das Risikoinformationssystem in einer IT-Beratung zu erarbeiten sind im Kapitel 5 die Phasen mit den zugeordneten Funktionen beschrieben. Das aus der Literatur abgeleitete Modell mit den praktischen Erfahrungen des Autors wurde in den Experteninterviews erfolgreich weiterentwickelt, korrigiert und validiert. Einen Ergebnisüberblick geben die Tabelle 25 und die Prozessübersicht (Abbildung 34 und Abbildung 35). Die Prozessübersicht visualisiert die Abhängigkeiten der einzelnen Funktionen. Die Erweiterungen und Korrekturen sind in der Tabelle 25, Abbildung 34 und Abbildung 35 kursiv dargestellt. In der Tabelle sind zu den zwei betrachteten Phasen mit den insgesamt fünf Funktionen die Projektakteure einer IT-Beratung zugeordnet.

Eine zusammenfassende schematische Darstellung zum Risikoinformationssystem auf deren Grundlage die *Dienstleisterauswahlentscheidungen* getroffen werden kann, ist in Abbildung 42 illustriert. Durch die Anwendung des Modells können die bestehenden Wissensflüsse zu externen Dienstleistern und die Projektbeteiligungen visualisiert werden. Die Interviewpartner bestätigen den Mehrwert dieser Darstellungsweise der Risikobewertung für ihre tägliche Arbeit, die sich im Interviewprozess durch die verschiedenen Sichtweisen und Hinweise weiterentwickelt hat.

Die recherchierten Erkenntnisse aus dem *Literature Review* und die Interviewstudien dienen der Beantwortung einzelner Forschungsfragen.

Forschungsfrage 1: *Wie identifiziert eine IT-Beratung die **Unternehmensgrenze** beim Wissen-Teilen und -Zurückhalten, um den Wissensschutz in der ISE mit externen Dienstleistern sicherzustellen?*

Speziell der Abschnitt 4.2.3 beschreibt den aktuellen Stand der Forschungsliteratur, um diese Frage zu diskutieren. Die Erkenntnisse fließen in die Funktion 3 (Abschnitt 5.2.3) vom Modell ein. Um diese Frage mit Hilfe des Modells zu beantworten, erfolgte die Kombination von Top-down (Funktion 1) und Bottom-up (Funktion 2 und 3) Ansatz. Die vier Bewertungskategorien (*Strategie, Kundennutzen, Mitbewerberabgrenzung, Übertragbarkeit*) aus der Literatur zur Bestimmung der Unternehmensgrenze werden im Forschungsprozess bestätigt. In dem erarbeiteten Referenzmodell sind die Akteure identifiziert, die für die Bestimmung der Unternehmensgrenze zu involvieren sind. Dieses Ergebnis differenziert sich von anderen Modellen, in denen übergreifende Experten (Gatekeeper)[961] für diese Funktion zuständig sind. Die Entscheidung zum *Wissen-Teilen und -Zurückhalten* im vorliegenden Modell basiert auf einer gemeinsamen Leistung der Projektakteure. Den Akteuren sind konkrete Funktionen zugeordnet, damit der Wissensschutz funktioniert. Der Einsatz eines übergreifenden Experten könnte in anderen Situationen und abhängig von der Organisationsform als sinnvoll bewertet werden. Einige Interviewpartner forderten, dass bei der Projektkategorisierung *KO-Kriterien* für den Wissensschutz und damit für die Involvierung von externen Dienstleistern zu definieren sind. Mit der Aufnahme der geforderten *KO-Kriterien* (Funktion 2) für das Beteiligen von Dienstleistern wird nach der Forderung von LIEBESKIND der Aufwand nur für die IT-Projekte durchgeführt, wo sich der Schutzaufwand amortisiert.[962] Diese mögliche Prozessalternative ist in Abbildung 34 und Abbildung 35 dargestellt.

Forschungsfrage 2: *Mit welchen **externen Dienstleistern** kann eine IT-Beratung in der ISE **zusammenarbeiten,** ohne ihre **Wettbewerbsfähigkeit** oder die ihrer Auftraggeber zu riskieren?*

Insbesondere der Abschnitt 4.2.4 und das Unterkapitel 4.3 beschreiben den aktuellen Stand der Forschungsliteratur, um diese Frage zu beantworten. Diese Erkenntnisse fließen in die Funktion 4 und 5 ein und werden im Unterkapitel 5.3 um die Interview-Anmerkungen ergänzt. Die Lösungsansätze *Signalisieren*, *Screening* und *Monitoring* der Prinzipal-Agent-Theorie werden um die Wissensschutzerkenntnisse der Literatur und der Praxis erweitert. Da diese Forschungsfrage eng mit dem wissenschaftlichen Beitrag verbunden ist, sind weitere Detailerläuterung im anschließenden Unterkapitel aufgeführt.

Forschungsfrage 3: *Welche **Funktionen** werden den **Akteuren** in einer IT-Beratung beim Wissensschutz **zugeordnet**, damit wertvolles Wissen geschützt werden kann?*

In der Tabelle 25 sind die identifizierten Akteure aufgeführt. Eine Spezifizierung der Akteure wurde in den Interviews eruiert. Eine Akteursempfehlung für die Bewertungskategorien der Wissensgebiete sind in der Tabelle 32 dokumentiert. Diese Empfehlung basiert auf einer intensiven Diskussion mit den befragten Experten und konnte im Vergleich zum initialen Modell präzisiert werden. Besonders die fachlichen und technischen Softwarearchitekten waren zuerst

[961] Vgl. Ahmad et al. 2014, S. 31, Hoecht & Trott 2005, S. 407, Norman 2001, S. 52.
[962] Vgl. Liebeskind 1996, S. 102.

nicht im Fokus, wurden jedoch von den Interviewpartnern mehrfach aufgeführt. Die Empfehlung sieht vor, dass bei den Kategorien *Übertragbarkeit* und *Mitbewerberabgrenzung* die Softwarearchitekten maßgebend sind. Bei der Bewertung der *Strategie*-Kategorie sind die Architekten vom Strategiemanagement einzubeziehen.

Zusammenfassend ist festzuhalten: Die Adressaten des Modells sind IT-Beratungen mit ihren IT-Projektakteuren die ISE für Kunden mit externen Dienstleistern realisieren. IT-Beratungen erhalten mit dem Wissensschutz-Referenzmodell Handlungsempfehlungen um den Wissensschutz in den zwei Phasen Strategie und Planung sowie der Dienstleisterauswahl durchzuführen. Das Modell unterstützt IT-Beratungen und ihre Kunden, die in den IT-Projekten erarbeiteten Wettbewerbsvorteile zu sichern. Zudem kann eine IT-Beratung mit der Bewertung der Wissensgebiete ihre Identität bestimmen, auf denen ihr Wert beruht und diesen Wert im Unternehmen manifestieren. Mit diesen Informationen können bestehende Wissensrisiken identifiziert und zukünftige minimiert werden, die in IT-Projekten mit externen Dienstleistern bestehen. Wie auch die Interviewpartner anmerkten, können mit der Anwendung des Referenzmodells zudem Abhängigkeiten oder Defaktoabhängigkeiten zu Dienstleistern in Bezug auf Wissen identifiziert, reduziert und ausgeschlossen werden. Diese Erkenntnis war nicht der Fokus des Modells, jedoch kann dieser praktische Mehrwert als Ergebnis der Diskussion hervorgehoben werden, der in weiteren Forschungsarbeiten fokussiert werden sollte.

6.2 Reflexion: Erkenntnisse und Limitationen

Aufbauend auf dem DS-Paradigma und der Aktionsforschung wurde das erarbeitete Referenzmodell über mehrere Jahre mit einer IT-Beratung entwickelt. Die gewonnenen Implikationen und mögliche Limitationen der Forschungsarbeit werden nach den gestellten Anforderungen von HEVNER et al. diskutiert.[963] Wegen der Limitationen des Wissensschutz-Referenzmodells und den angewendeten Forschungsmethoden gelten die Erkenntnisse nicht uneingeschränkt. Im Speziellen ist anzumerken, dass der Fokus auf einer IT-Beratung und damit auf einer dezidierten Branche liegt.

Die sieben gestellten Anforderungen von HEVNER et al. können im Wesentlichen in einen praktischen und theoretischen Schwerpunkt eingeteilt werden. Diese werden in den folgenden zwei Abschnitten dokumentiert. Die siebente Anforderung adressiert sowohl die praktischen als auch die theoretischen Erkenntnisse und wird deshalb bereits hier beschrieben.

Aufbereitung und Kommunikation der Forschungsergebnisse

Der Anforderung zur Kommunikation der Forschungsergebnisse wird mit der Dokumentation der Arbeit, Aufbereitung von Ergebnispräsentationen, Fachkonzepten und Musterdokumenten erfüllt. Weiterhin sind Ergebnispräsentationen bei Arbeitskreisen von Verbänden (zum Beispiel BITKOM) geplant. Neben der Wissenschaftsgemeinschaft sind die identifizierte Hauptziel-

[963] Vgl. Unterkapitel 3.1.

gruppe IT-Beratungen, die mit externen Dienstleistern zusammenarbeiten. Der konkrete Personenkreis für eine Realisierung des Referenzmodells sind Führungskräfte, Manager und Projektmanager, die die Projektleistungen in einer IT-Beratung verantworten.[964] Für diese wurden die Ergebnisse in Form einer semiformalen Darstellungsweise mit den Modellierungselementen von ARIS und den entsprechend sprachlich-textuellen Beschreibungen aufbereitet. Dadurch wird gleichermaßen eine verständliche Darstellung des Referenzmodells für die Wissenschaft und verantwortlichen Projektakteure sichergestellt.

6.2.1 Wissenschaftlicher Beitrag

Die drei Anforderungen nach HEVNER et al. mit einem theoretischen Fokus werden folgend beschrieben.

Wissenschaftlicher Beitrag durch neue Artefakte

In Bezug auf IT-Sourcing in einer Prinzipal-Agenten-Beziehung und der Betrachtung des Wissensschutzes liefert diese Forschungsarbeit eine der ersten Erkenntnisse. Die bisherigen Untersuchungen fokussieren sich auf den Wissensschutz zwischen gleichberechtigten Partnern und zudem auf einzelne Aspekte. Der wissenschaftliche Beitrag liegt in der Konstruktion neuer Artefakte und der Erkenntnisse für die Prinzipal-Agent-Theorie. Die neuen Artefakte sind die Funktionen für das etablierte Phasenmodell von MONCZKA et al. und NASSIMBENI et al. Diese Funktionen bilden das Fundament für die wissenschaftliche Diskussion und Weiterentwicklung. Von theoretischer Relevanz ist ebenso, dass diese Arbeit Limitationen anderer Arbeiten adressiert. Der Forschungsbedarf für die Auswahl von Projekt-Dienstleistern wird von Li et al. als eine weitere Herausforderung angesehen, die mit dieser Arbeit untersucht wurde.[965]

Die bisherigen Lösungsansätze für die Probleme in einer Prinzipal-Agenten-Beziehung konzentrieren sich auf Vertrauen, Unternehmenskultur, Reputation, Verträge, Anreize, Informationssysteme und bürokratische Kontrolle. Die Interviewpartner bestätigen das Vertrauen und Reputation in den Agentenauswahlprozess einbezogen werden müssen. Auch die genannte Voraussetzung vom Modell, dass die Verträge für die rechtliche Absicherung den Wissensschutz enthalten müssen, werden von Interviewpartnern quittiert. Ebenso bestätigt wird, dass in Bezug auf den Schutz des impliziten Wissens vertragliche Regelungen wegen der diffizilen Nachweisbarkeit bei einer vertraglichen Verletzung wenig helfen.

Mit dem Modell werden die bestehenden Lösungsansätze *Signalisieren, Screening* und *Monitoring* in einer Prinzipal-Agenten-Beziehung erweitert, insbesondere für die entstehenden Wissensrisiken. Für die Auswahl potentieller Dienstleister sind die relevanten Wissensschutz-Informationen abzufragen und in den Auswahlprozess aufzunehmen. Der Selektionsprozess bezieht zudem die Erfahrungen aus abgeschlossenen und bestehenden IT-Projekten (*Monitoring*) mit dem jeweiligen Dienstleister ein.[966] Mit Hilfe der Dienstleisterkategorisierung (Funktion 4)

---

[964] Vgl. Unterkapitel 1.2.
[965] Vgl. Li et al. 2008, S. 329.
[966] Vgl. Abschnitt 5.3.1.

wird das *Dienstleister-Gefahrenpotential* in Bezug auf Wissensrisiken mit der Bewertung der *absorptiven Dienstleisterkapazität* und den bisherigen Dienstleistererfahrungen (Vertrauen) bestimmt. Zum anderen basiert die Einschätzung des Dienstleisters in den Fach- und Technologiewissensgebieten auf der internen Expertise und der externen Marktstellung. Für neue IT-Projekte werden die Ergebnisse der Dienstleisterkategorisierung in einer Risikobewertung (Funktion 5) mit der Projektkategorisierung und Wissenskategorisierung in Bezug auf Wissensschutz visualisiert dargestellt. Auf dieser Grundlage können Dienstleisterauswahl-Entscheidungen vorgenommen werden.

So können die Wissensrisiken für den Prinzipal und seine Auftraggeber reduziert werden, da eine visuelle Dokumentation mit der Risikobewertung (Funktion 5) vorliegt. Die beschriebenen Funktionen 4 und 5 der Dienstleisterauswahl stellen das Vorgehen dar. Der wissenschaftliche Beitrag liegt damit zum einen in der Erweiterung der Prinzipal-Agent-Theorie beim Dienstleister-Auswahlprozess (*Signalisieren* und *Screening*).

Zum anderen können durch den Modelleinsatz die bestehenden IT-Projekte mit den eingesetzten externen Dienstleistern gemonitort werden. Der Lösungsansatz *Monitoring* wird um eine Risikobewertung für die bestehenden IT-Projekte erweitert.[967] Zudem können neue IT-Projekte mit Fokus auf Wissensschutz überwacht werden. Wenn sich Rahmenbedingungen wie die strategische Planung, Wissensschutz-Bedarfe oder Dienstleisterkategorisierungen ändern, dann werden diese in der Risikobewertung und damit beim *Monitoring* transparent. Damit können Handlungsbedarfe im Hinblick auf Wissensschutz und Agenteneinsatz für die Projektakteure sichtbar werden. Für die Prinzipal-Agent-Theorie wird ein innovatives Artefakt geschaffen, mit dem IT-Beratungen wissenschaftlich fundiert ihre Dienstleister auswählen können.

Anwendung von Methoden bei der Konstruktion und Bewertung des Artefaktes

Das theoretische Fundament des entwickelten, validierten und evaluierten Wissensschutz-Referenzmodells basiert auf dem Design-Science-Research Ansatz und der Aktionsforschung. Die Stringenz der Forschungsarbeit ist durch die Anwendung des bestehenden Vorgehensmodells zur Referenzmodell-Konstruktion von SCHLAGHECK erfüllt. Zudem wurden ergänzende Forschungsmethoden eingesetzt, um auch die differenzierten Kriterien von Wissenschaft und Praxis in der Aktionsforschung zu erfüllen.[968] Innerhalb vom konstruktionsorientierten Forschungsansatz bestand das methodische Vorgehen im Prototyping, in der Prototypevaluation mit Experteninterviews und der Pilotierung. Insbesondere der entwickelte Prototyp liefert einen bedeutsamen Beitrag zur theoretischen Erkenntnis. Dieser basiert auf den wissenschaftlichen Erkenntnissen zum Wissensschutz und seiner angrenzenden Forschungsdisziplinen, die im Kapitel 4 dokumentiert sind. Des Weiteren nutzt das Forschungsvorhaben die Methoden des *Lite-*

[967] Vgl. Abschnitt 5.3.2.
[968] Vgl. Mingers 2001, S. 243, Chiasson et al. 2008, S. 37, Österle et al. 2010, S. 4 f.

rature Reviews, die qualitativen Experteninterviews und die Inhaltsanalyse (Zusammenfassung). Die Details zum angewendeten Methodenpluralismus sind im Unterkapitel 3.1 beschrieben.

In der Evaluationsphase (Pilotierung) wurde das Artefakte auf ein IT-Projekt angewendet und mit den Projektakteuren aus praktischer Perspektive diskutiert. Mit Hilfe der qualitativen Experteninterviews (Prototypevaluation) konnte zudem eine theoretische Bewertung aus der Sichtweise der betrieblichen Praxis vorgenommen werden.

Das sozial erwünschte Antwortverhalten könnte ebenfalls die Validität der Ergebnisse vermindert haben.[969] Dieser Limitation konnte durch eine Samplingstrategie und damit der Auswahl der Praxisvertreter entgegengewirkt werden. Zu jeder Modell-Funktion und deren Akteursgruppe wurden zudem mehrere Experten befragt und auf die Spezialisierung der Interviewexperten eingegangen. Des Weiteren konnte gesichert werden, dass die befragten Experten bereits in anderen Unternehmen Berufserfahrung gesammelt hatten. Von den elf ausgewählten Interviewpartnern erfüllten zehn dieses Kriterium. Die Erfahrungswerte der Experten aus ihren Einflussbereichen fließen dadurch in das Modell ein und fördern damit die Übertragbarkeit des Modells.

Für die Bewertung des Artefakts aus der Kosten- und Leistungsrechnungsperspektive entstehen Schwierigkeiten, da das Wissen einer IT-Beratung und deren erfolgreiche Wissensschutz diffizil monetär bewertet werden kann. Einen Ansatz für eine monetäre Bewertung könnte die Wissensbilanz liefern, die den Fokus auf die Unternehmensprozesse legt.[970] Die zeitlichen Aufwände und damit die Aufwandskosten der Umsetzung des Wissensschutzes in einer IT-Beratung könnten durch die Projektakteure erfasst und ermittelt werden.

Entwicklung der Ergebnisse durch iterativen Suchprozess

Wegen des hohen Abstraktionsgrades der Design-Science Methodik und damit auch vom Referenzmodellierungsprozess wird diese Methoden nach OSTROWSKI & HELFERT noch zu selten angewendet.[971] Die von ihnen modellierten und detaillierten Aktivitäten (Verfahren, Werkzeuge, Techniken) für die Prozesse *Literature Review* und Kollaboration mit Praktikern finden in dieser Arbeit Anwendung, um die neuen Artefakte für das Wissensschutz-Referenzmodell zu entwickeln. Den Anforderungen zur Konstruktion von Referenzmodellen entsprechend, kombiniert die vorliegende Arbeit im Suchprozess:

- die gewonnen theoretischen Erkenntnisse,
- die Erfahrungen, das Wissen sowie die Beurteilung involvierter Praxisvertreter und
- die praktische Erfahrung des Verfassers.

Die Qualität der Arbeit basiert auf diesen Einflussbereichen, die das Modell sukzessiv präzisiert haben. Der zyklische Prozess, der in der Aufnahme von Hinweisen, neuen Kategorien und der anschließenden Diskussion von Interview zu Interview bestand, hat sich als Vorgehen für das

[969] Vgl. Möhring & Schlütz 2010, S. 61 ff.
[970] Vgl. Mertins et al. 2005, S. 14.
[971] Vgl. Ostrowski & Helfert 2012, S. 1, Peffers et al. 2007.

entwickelte Referenzmodell bewährt. Dieses konkrete methodische Vorgehen hat zu dem evaluierten Wissensschutz-Referenzmodell geführt, das im Kapitel 5 dargestellt ist. Die Forschungsmethoden und das Forschungsvorgehen im Kapitel 3 dokumentieren das konkrete Vorgehen. Damit wird ein möglicher Gang der Arbeit dokumentiert um dem hohen Abstraktionsgrad der Design-Science zu reduzieren.

Im Vergleich zu anderen Aktionsforschungsarbeiten, bei denen der Forscher in das Forschungsobjekt zeitweise eingebunden ist, konnten die Erkenntnisse des Autors durch seine dauerhafte langjährige Projekterfahrung in die Untersuchungen aufgenommen werden. Durch die Aktionsforschung und damit die Aufnahme der praktischen Erfahrung des Autors in die Modellentwicklung bestehen Limitationen. CHECKLAND & HOLWELL kritisieren diese Vorgehensweise: „What Weltanschauung would make this research seem 'plausible'?"[972] Die Forschungsarbeit grenzt sich von dieser Auffassung durch die vorangestellte Determinierung des Forschungsgegenstandes und -vorgehens ab.[973] Dennoch ist die Reproduzierbarkeit des Modells bei identischen Prämissen und Anwendung der Forschungsmethoden eine Limitation der Arbeit.

6.2.2 Praktische Erkenntnisse

Die weiteren drei Anforderungen nach HEVNER et al. mit einem praktischen Fokus werden folgend beschrieben.

Anwendbare Artefakte in Form von Konstrukten, Modellen, Methoden oder Instanzen

Die vorliegende Arbeit stellt ein Referenzmodell zum strategischen Wissensschutz in IT-Projekten mit externen Dienstleistern vor. Dem etablierten Phasenmodell werden zu den fünf identifizierten Funktionen die Akteure einer IT-Beratung zugeordnet. Die praktische Anwendung an einem existenten IT-Projekt validierte das entwickelte Referenzmodell und lieferte weitere Ergebnisartefakte, die die Basis für einen folgenden Modelleinsatz ist. Die für den Interviewleitfaden entwickelten zwei praxisnahen IT-Projekt-Beispiele in Form von Prototypen zeigten sich ebenso als ein fundiertes Instrument um den Interviewpartnern das Modell im Rahmen der Prototypevaluation zu erläutern. Zudem konkretisierte und bestätigte die Pilotierung die Forschungsergebnisse.

Das Referenzmodell konnte noch nicht in die bestehenden Prozesse vom Untersuchungsobjekt integriert werden, um den Wissensschutz im Projektgeschäft zu etablieren. Seitens der untersuchten IT-Beratung besteht Interesse das Modell in die Praxis zu inkludieren, sobald das Referenzmodell veröffentlicht ist.

---

[972] Vgl. Checkland & Holwell 1998, S. 18.
[973] Vgl. Fleisch 2001, S. 292.

Entwicklung von Lösungen für bedeutende und relevante Probleme

Die informellen Gespräche, die Praxiserfahrung des Autors und die Vorinterviews zur Themenfokussierung mit Experten vom Digitalverband, der Außenhandelskammer, (IT-) Beratungsunternehmen sowie IT-Sicherheitsexperten zeigten den praktischen Bedarf dieser Forschungsarbeit auf. Ursprünglich wurde die Beziehung zu ausländischen Dienstleistern fokussiert, weil das Auslagern von IT-Projektleistungen an internationale Dienstleister im großen Umfang zugenommen hat. Bei den informellen Gesprächen zeigte sich jedoch, dass die inländischen Dienstleister in Bezug auf den Wissensschutz noch kritischer gesehen werden. Aus diesem Grund adressiert das Modell den nationalen und internationalen Dienstleistereinsatz in einer IT-Beratung. Diese identifizierte Herausforderung wurde in einem Gruppeninterview mit verantwortlichen Managern aus den Bereichen IT-Sourcing, Technologie und Projektgeschäft validiert und verifiziert. Die Problemdefinition und damit die praktische Relevanz dieser Arbeit beruht auf den Aussagen der befragten Experten, die sich nicht zwangsläufig im gleichen Umfang in anderen IT-Beratungen reflektieren müssen.

Die Relevanz des Wissensschutzes in einer Prinzipal-Agenten-Beziehung wird bisher nur von DESOUZA & AWAZU[974] erwähnt. Das zu diesem relevanten Problem kaum Untersuchungen vorliegen, bestätigen die Forschungslücke und den Forschungsbedarf. Der Wissensaustausch mit Dienstleistern dient jedoch auch der Erhaltung und Entwicklung wertvollen Wissens, das in den IT-Projekten für mehrere Kunden angewendet werden kann. Jede IT-Beratung muss sich dieser ambivalenten Situation selbst stellen und entsprechend der Wissensbasis Regelungen erarbeiten.

Das Modell betrachtet nicht, dass die externen Berater vom Dienstleister kündigen und das aufgebaute Fach- und Technologiewissen zu anderen Dienstleistern oder Kunden mitnehmen können. Die gleiche Möglichkeit besteht ebenso bei internen Projektakteuren, die kündigen und das aufgebaute Fach- und Technologiewissen in ein anderes Unternehmen transferieren können. An dieser Stelle ist auf die Erkenntnisse von OLANDER et al. zu verweisen. Das Verlieren eines Keyplayers an ein konkurrierendes Unternehmen wäre das *worst-case* Szenario.[975] Aus diesem Grund ist auch die Mitarbeiterbindung eine entscheidende Maßnahme zum Wissensschutz, die nicht im Fokus dieser Arbeit stand.

Durch die nicht eindeutige Abgrenzung des Wissensschutzes zu den äquivalenten Bezeichnungen in der Literatur ergeben sich weitere Limitationen der Arbeit.[976] Außerhalb des Fokus waren:

- die formalen Wissensschutzmechanismen (Vertragsklärung, Angebotsbetrachtung, Copyrights, Patente, Handelsgeheimnisse, Markenzeichen und andere),
- der Schutz vom expliziten Wissen (siehe Informationsschutz),
- die Wissenssicherheit,
- die Intellectual Property Rights Protection,

[974] Desouza & Awazu 2004.
[975] Olander et al. 2011, S. 608.
[976] Vgl. Tabelle 4.

- die Cybersicherheit, die Sicherheit von IT-Systemen und
- (strategische) Allianzen oder Partnerschaften.

Weitere Wissensschutzmechanismen wie die Sensibilisierung der Projektakteure, Schulungen der Mitarbeiter und die Verankerung in der Unternehmenskultur standen nicht im Fokus der Forschungsarbeit und bilden weitere Limitationen.

Nutzen, Qualität und Wirksamkeit des Artefaktes

Diese Anforderungen bestätigen die Interviewpartner mit der Aussage, dass sie das Wissensschutz-Referenzmodell als eine geschlossene Systematik verifizieren, das von der Idee bis zum Ziel nachvollziehbar ist und das damit Aussagen zum Wissensschutz abgeleitet werden können.[977] Mit der Auswahl eines bestehenden IT-Projektes und der Erprobung des Wissensschutz-Referenzmodells in diesem IT-Projekt konnte die Qualität demonstriert werden. Zu der Erprobung gehört ebenso die Durchführung von einem Gruppeninterview mit Projektakteuren.

Einige Interviewpartner merkten auf qualitativer Ebene an, dass im Modell nicht das individuelle Wissen von einem externen Berater in einem IT-Projekt bewertet wird, sondern die Bewertung der Wissensgebiete erfolgt für den externen Dienstleister gesamtheitlich. Der Hintergrund für die ganzheitliche Bewertung basiert auf der gegebenen Wissensüberlappung mit dem externen Dienstleister, die zu dokumentieren ist. Bei der Bewertung vom externen Berater würde es eine Diskrepanz zwischen vorgesehener und gelebter Rolle innerhalb des IT-Projektes geben. Die Bewertung wäre abhängig von den Vorkenntnissen und der Projekthistorie des einzelnen Beraters. So sind zum Beispiel fachliche Architekten mit technischen Hintergrundwissen denkbar oder umgekehrt.

Der Nutzen und die Wirksamkeit des Wissensschutz-Referenzmodells kann erst mit der Integration in die täglichen IT-Projekt-Prozesse und durch eine weitere empirische Validierung noch signifikanter bewertet und demonstriert werden. Dazu müsste das Referenzmodell in mehreren IT-Beratungen eingesetzt werden, was im limitierten Zeitraum des Forschungsvorhabens nicht realisiert werden konnte. Die Bewertung der Allgemeingültigkeit und des Empfehlungscharakters vom konstruierten Referenzmodell kann nicht objektiv nachgewiesen werden, da diese auf der subjektiven Wahrnehmung zum Anwendungszeitpunkt basiert.[978] Das vorliegende Referenzmodell wurde in Experteninterviews und in einem Gruppeninterview zur praktischen Anwendung qualitativ positiv evaluiert. Diese praktische Anwendung des Referenzmodells im Forschungsprozess wirkt der subjektiven Wahrnehmung entgegen. Die am Forschungsprojekt beteiligte IT-Beratung hat das Ziel mit dem Abschluss der Forschungsarbeit die Erkenntnisse dieser Studie in die täglichen IT-Projekt-Prozesse zu integrieren. Dieser Schritt bedeutet weitere evidente Erkenntnisse für die praktische Anwendung, wenn die IT-Beratung weiter in den Forschungsprozess integriert wird.

Bei der Bewertung von IT-Projekten, den Fach- und Technologiewissensgebieten kann es zur Fehlinterpretation einzelner Kategorien kommen, was zu zu viel oder zu wenig Wissensschutz

[977] Vgl. IP_8.
[978] Vgl. vom Brocke 2003, S. 31 f.

führen könnte. Die gemeinsame Bewertung durch mehrere Projektakteure wirkt jedoch einer fehlerhaften Deutung entgegen. Diesem Problem kann zusätzlich durch eine begleitende Einführung und Moderation entgegengewirkt werden.

Beim IT-Projekt-Auswahlprozess wurde dokumentiert, dass ein Projektmanager gegenüber dem Wissensschutz in den IT-Projekten gering zugänglich war. Nach seiner Rückmeldung werden die meisten Punkte beim Dienstleisterauswahlprozess im Hinblick auf den Wissensschutz bereits von ihm im Sinne der IT-Beratung beachtet. Nach der Rücksprache mit anderen Interviewpartnern wurde zurückgemeldet, dass durch die systematische Anwendung des Modells mit mehreren Projektakteuren ein Rahmen zur objektiveren Bewertung geschaffen wird. Denn jeder Projektmanager kann seine individuellen Einschätzungen zu einem Projekt, Wissensgebiet, Dienstleister und Risiko haben. Jedoch ist es unrealistisch, dass einem Experten alle Informationen für eine nachvollziehbare Entscheidung vorliegen. Bei diesem Szenario besteht die Gefahr, dass der Projektmanager dann nicht im Sinne der IT-Beratung handelt und das wertvolles und schützenswertes Wissen die Unternehmensgrenze verlässt oder nicht nachhaltig geschützt wird. Im Gruppeninterview wurde von den Teilnehmern auch darauf hingewiesen, dass eine vorgenommene Bewertung nachvollziehbar begründet werden muss.

6.3 Anregung zur weiterführenden Forschung

Die Führungsebene sowie die Manager im Unternehmen sind nach der ISO Norm 9001 seit 2015 verpflichtet das WM und damit den Wissensschutz einzuführen.[979] Dazu gehört auch das Wissensrisikomanagement um die Wettbewerbsposition vom Unternehmen abzusichern, denn der Stellenwert von Wissensarbeit wird in Zukunft weiter zunehmen.[980] Wissen ist die einzige Ressource, die sich durch Gebrauch vermehrt, die Einzigartigkeit eines Unternehmens begründen kann und weitere Innovationen hervorbringt.[981] In Zukunft ist deshalb auch zu prüfen, ob Unternehmen im Rahmen dieser Norm den Wissensschutz neben dem Daten- und Informationsschutz einhalten. Aus den Limitationen und den Ergebnissen der Arbeit ergeben sich Ausgangspositionen für zukünftige Forschungsthemen im Umfeld von (IT-) Projekten und Prinzipal-Agenten-Beziehungen. In den folgenden Forschungsbereichen sind weitere Untersuchungen denkbar.

Anwendung der Modell-Funktionen

Die entwickelten Referenzmodell-Funktionen wurden auf ein ausgewähltes IT-Projekt angewendet und diskutiert, dennoch ist eine permanente Integration in der betrieblichen Praxis für weitere Evaluation zu empfehlen. In solchen Langzeitstudien könnten Entwicklungen und Tendenzen identifiziert werden. Zu empfehlen wäre, das Modell für ein Jahr anzuwenden, die Erkenntnisse zu dokumentieren und dann einen neuen Zyklus zu starten. Damit würde eine der wesentlichen Limitationen des Forschungsdesiderates bearbeitet werden. Daraus könnten sich

[979] Vgl. DIN EN ISO Norm 9001:2015.
[980] Vgl. Davenport 2011.
[981] Vgl. Fried & Baitsch 2000, S. 33.

weitere quantitative Forschungsbedarfe ergeben. Denkbar wären zum Beispiel die Ergebnisse zum Wissensschutz mit Conjoint-Analysen oder Netzwerkanalysen zu überprüfen. Weiterhin ist zu prüfen, ob bei Prinzipal-Agenten-Beziehungen und dem interorganisationalen Wissensschutz ein Unterschied zwischen kleinen, mittleren und großen IT-Beratungen existiert.

Einführung von einzelnen Modell-Funktionen

Zu empfehlen ist, dass die Referenzmodell-Phasen mit ihren Funktionen in die bestehenden Projektprozesse ganzheitlich eingebunden werden, da sie abhängig zueinander sind. In Abhängigkeit von der vorliegenden Projektorganisation und Ressourcen im Praxisunternehmen wäre auch eine auf Kernbestandteile reduzierte oder eine schrittweise Einführung denkbar. Daraus können sich weitere Forschungsbereiche im Umfeld vom Changemanagement ergeben.

Anwendung des Modells in weiteren Branchen

Damit die Ergebnisse zu den erarbeiteten Forschungsfragen weiter generalisiert werden können, bietet es sich an diese in weiteren Branchen mit Dienstleistungsbezug zu prüfen. Die Praxisvertreter verwiesen darauf, dass Fach- und Technologiewissen auch in anderen Unternehmen eine bedeutende Rolle einnimmt. Diese Erkenntnisse ermöglichen dann komparative Analysen in Bezug auf den Wissensschutz bei Prinzipal-Agenten-Beziehungen. Erste informelle Gespräche zu dem Wissensschutz-Referenzmodell mit Akteuren der Automobilindustrie-Entwicklung und des Personalrekrutings bestätigen auch in diesem Umfeld einen potentiellen Nachholbedarf bei der Zusammenarbeit mit Dienstleistern.

Anwendung auf andere Projektarten

Nach den Hinweisen von Li et al. auf Forschungsbedarf im Projektgeschäft und der Dienstleisterkategorisierung,[982] liefert die Arbeit einen Beitrag bei der Auswahl von Dienstleistern, um den Wissensschutz zu etablieren. Innerhalb der Interviews zeigte sich der Bedarf, dass Modell auf andere Projektarten als die ISE anzuwenden. Exemplarisch genannt wurden Produktentwicklungsprojekte, Strategieberatungsprojekte für Kunden und die einer IT-Beratung. Die Nicht-Auftraggeber-Projekte, die eine IT-Beratung selbst betreffen, könnten demnach ebenso in Bezug auf Wissensschutz geprüft werden. In diesem Zusammenhang weisen die befragten Experten und die bisherige Forschung daraufhin, dass Unternehmen ihre Dienstleister aufgrund ihrer Ressourcen und Fähigkeiten auswählen,[983] jedoch nicht nach den strategischen Zielen zum Wissensschutz.

[982] Vgl. Li et al. 2008, S. 329.
[983] Vgl. Li et al. 2008, S. 327 f.

Schutz des impliziten Wissens in Prinzipal-Agenten-Beziehungen

Die Arbeit stellt Techniken vor, um das implizite Wissen in einer Prinzipal-Agenten- Beziehung zu schützen. Wünschenswert ist, wenn sich zukünftige Forschung und Veröffentlichungen in diesem Umfeld auf Modellbestandteile konzentrieren sowie Best-Practice-Erkenntnisse dokumentieren. So ist zum Beispiel der erwähnte Einfluss der eingenommenen Projektrolle des externen Beraters und die Auswirkung auf den Wissensschutz im IT-Projekt noch weiter zu untersuchen. Wie bereits BOLISANI et al. im Umfeld von KIBS feststellten, sind die Auswirkungen von informellen Wissensschutzmechanismen auf operative Prozesse und ihre Beziehungen zu WM-Praktiken noch wenig erforscht.[984] An dieser Stelle ist auf die in der Motivation aufgeführte Forschungsagenda hinzuweisen. Drei der fünf aufgezeigten Forschungsagenda-Themen von MANHART & THALMANN[985] sind mit der Arbeit adressiert.[986] Diese sind:

- "Opening the black box around the protection of tacit knowledge
- Analysing the phenomena in-depth
- Designing supportive IT".

Die dokumentierten Ergebnisse liefern Impulse für diese Forschungsagenda, jedoch besteht weiterhin großes Forschungspotential, wie detailliert in diesem Kapitel erörtert.

Die Forschungsarbeitet und damit das Referenzmodell bietet für diese potentiellen Themenbereiche eine Basis für weitere wissenschaftliche Forschung. Die Praxis erhält ein mögliches Vorgehensmodell und eine Diskussionsgrundlage, um die erarbeiteten Wettbewerbsvorteile innerhalb einer IT-Beratung zu halten und damit auch die Existenz der Kunden, die die Projekte finanzieren, zu sichern.

[984] Vgl. Bolisani et al. 2013, S. 209.
[985] Vgl. Manhart & Thalmann 2015, S. 204 f.
[986] Vgl. Unterkapitel 1.1.

7 Literaturverzeichnis

Ahmad, A.; Bosua, R. und Scheepers, R. (2014): Protecting organizational competitive advantage: A knowledge leakage perspective. In: Computers & Security, 42, S. 27-39.

Aksin, O. Z. und Masini, A. (2008): Effective strategies for internal outsourcing and offshoring of business services: an empirical investigation. In: Journal of Operations Management, 26(2), S. 239-256.

Alavi, M. und Leidner, D. E. (2001): Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues. In: MIS Quarterly, 25(1), S. 107-136.

Aljafari, R. und Sarnikar, S. (2009): A Framework for Assessing Knowledge Sharing Risks in Interorganizational Networks. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS), 572.

Alvisi, A. (2012): KIBS Roles in KIBS Industries. In: Di Maria, E.; Grandinetti, R.; Di Bernardo, B. (Hrsg.): Exploring Knowledge Intensive Business Services. Knowledge Management Strategies. Hampshire, New York: Palgrave Macmillan, S. 100-119.

Amara, N.; Landry, R. und Traoré, N. (2008): Managing the protection of innovations in knowledge-intensive business services. In: Research Policy, 37(9), S. 1530-1547.

Amara, N.; Landry, R. und Doloreux, D. (2009): Patterns of innovation in knowledge-intensive business services. In: The Service Industries Journal, 29(4), S. 407-430.

Arrow, K. J. (1974): The limits of organization. New York: Norton.

Arrow, K. J. (1991): The Economics of Agency. In: Pratt, J. und Zeckhauser, R. J. (Hrsg.): Principals and Agents: The Structure of Business. Boston, Mass.: Harvard Business School Press, S. 37 – 51

Arundel, A. und Kabla, I. (1998): What percentage of innovations are patented? Empirical estimates for European firms. In: Research Policy, 27(2), S. 127-141.

Arundel, A. (2001): The relative effectiveness of patents and secrecy for appropriation. In: Research Policy, 30, S. 611-624.

Backes-Gellner, U., Lazear, E. und Wolff, B. (2001): Personalökonomik: Fortgeschrittene Anwendungen für das Management. Stuttgart: Schäfer-Poeschel.

Baker, M. J. (2000): Writing a Literature Review. In: Marketing Review, 1(2), S. 219-247.

Ballod, M. (2009): K^3: Koordination, Kooperation, Kommunikation. Wie Wissensmanagement gelingen kann! Plenumsvortrag auf dem 5. Stuttgarter Wissensmanagement-Tagen in Stuttgart am 10.11.2009.

Balzert, H. (1999): Lehrbuch Grundlagen der Informatik. Heidelberg: Spektrum Akademischer Verlag.

Barney, J. B. und Hansen, M. (1994): Trustworthiness as a source of competitive advantage. In: Strategic Management Journal, 15, S. 175-190.

Barney, J. B. (1986): Organizational culture: can it be a source of sustained competitive advantage? In: Academy of Management Review, 11(3), S. 656-665.

Barney, J. B. (1991): Firm resources and sustained competitive advantage? In: Journal of Management, 17(1), S. 99-120.

Barney, J. B. (1995): Looking inside for competitive advantage. In: Academy of Management Executive, 9(4), S. 49-61.

Barrier, M. (2004): Protecting trade secrets: HR professionals are key lines of defense when it comes to protecting information that provides your business with a competitive advantage. In: HR Magazine,

49(5). Online verfügbar unter https://www.shrm.org/hr-today/news/hr-magazine/pages/0504barrier.aspx, zuletzt geprüft am 22.03.2018.

Baskerville, R. und Wood-Harper, T. (1998): Diversity in information systems action research methods. In: European Journal of Information Systems, 7(2), S. 90-107.

Baskerville, R.; Pries-Heje, J. und Venable, J. (2009): Soft design science methodology. In: Proceedings of design science research in information systems and technology, Malvern.

Baughn, C. C.; Denekamp, J. G.; Stevens, J. H. und Osborn, R. N. (1997): Protecting Intellectual Capital in International Alliances. In: Journal of World Business, 32 (2), S. 103-117.

Baum, J. A. C.; Calabrese, T. und Silverman, B. S. (2000): Don't go it alone: alliance network composition and startups' performance in Canadian biotechnology. In: Strategic Management Journal, 21, S. 267-294.

BDI (2012): BDI Positionspapier, Wirtschaftsschutz in der deutschen Industrie stärken! Online verfügbar unter https://bdi.eu/media/presse/publikationen/marketing/Positionspapier_online_2_.pdf, zuletzt geprüft am 18.01.2018.

BDI (2015): Themenfelder "Wirtschaftsschutz" im BDI, internes Dokument BITKOM, Arbeitskreis Wirtschaftsschutz.

Becerra, M.; Lunnan, R. und Huemer, L. (2008): Trustworthiness, Risk, and the Transfer of Tacit and Explicit Knowledge Between Alliance Partners. In: Journal of Management Studies, 45(4), S. 691-713.

Becker, J. und Schütte, R. (2004): Handelsinformationssystem: Domänenorientierte Einführung in die Wirtschaftsinformatik. 2. Aufl. Landsberg/Lech: Moderne Industrie Verlag.

Becker, J.; Algermissen, L.; Delfmann, P. und Knackstedt, R. (2002): Referenzmodellierung. Das Wirtschaftsstudium (WISU), 31(11), S. 1392-1395.

Becker, J.; Holten, R.; Knackstedt, R. und Niehaves, B. (2003): Forschungsmethodische Positionierung in der Wirtschaftsinformatik - epistemologische, ontologische und linguistische Leitfragen. In: Becker, J.; Grob, H.-L.; Klein, S.; Kuchen, H.; Müller-Funk, U. und Vossen, G. (Hrsg.): Arbeitsberichte des Instituts für Wirtschaftsinformatik, 93, Münster: Institut für Wirtschaftsinformatik, WWU Münster.

Becker, J.; Delfmann, P. und Knackstedt, R. (2004): Konstruktion von Referenzmodellierungssprachen. Ein Ordnungsrahmen zur Spezifikation von Adaptionsmechanismen für Informationsmodelle. In: Wirtschaftsinformatik, 46(4), S. 251-264.

Becker, J.; Niehaves, B.; Olbrich, S. und Pfeiffer, D. (2009): Forschungsmethodik einer Integrationsdisziplin: Eine Fortführung und Ergänzung zu Lutz Heinrichs "Beitrag zur Geschichte der Wirtschaftsinformatik" aus gestaltungsorientierter Perspektive. In: Becker, J.; Krcmar, H. und Niehaves, B. (Hrsg.): Wissenschaftstheorie und gestaltungsorientierte Wirtschaftsinformatik. Heidelberg: Physica Verlag, S. 1-22.

Beckman, C.; Haunschild, P. und Phillips, D. (2004): Friends or strangers? Firm-specific uncertainty, market uncertainty, and network partner selection. In: Organization Science, 15, S. 259-275.

Belsis, P.; Kokolakis, S. und Kiountouzis, E. (2005): Information systems security from a knowledge management perspective. In: Information Management & Computer Security, 13(3), S. 189-202.

Bettencourt, L. A.; Ostrom, A. L.; Brown, S. W. und Roundtree, R. I. (2002): Client co-production in knowledge-intensive business services. In: California Management Review, 44(4), S. 100-128.

BfV (2015): Wirtschaftsschutz, Wirtschaftsspionage + Aktuelle Entwicklungen. Bundesamt für Verfassungsschutz, BITKOM Arbeitskreis Wirtschaftsschutz, Juli 2015.

Bhalla, A.; Sodhi, M. S. und Son, B. (2008): Is more IT offshoring better?: An exploratory study of western companies offshoring to South East Asia. In: Journal of Operations Management, 26(2), S. 322-35.

BITKOM (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter, Studienbericht. Online verfügbar unter https://www.bitkom.org/Bitkom/Publikationen/Spionage-Sabotage-und-Datendiebstahl-Wirtschaftsschutz-im-digitalen-Zeitalter.html, zuletzt geprüft am 18.01.2018.

Bleeke, J. und Ernst, D. (1993): Collaborating to Compete: Using Strategic Alliances and Acquisitions in the Global Market Place. New York: Wiley.

Bloodgood, J. M. und Salisbury, D. (2001): Understanding the influence of organizational change strategies on information technology and knowledge management strategies. In: Decision Support Systems, 31(1), S. 55-69.

Bogers, M. (2011): The open innovation paradox: knowledge sharing and protection in R&D collaborations. In: European Journal of Innovation Management, 14(1), S. 93-117.

Bogner, A. und Menz, W. (2002): Das theoriegenerierende Experteninterview. Erkenntnisinteresse, Wissensformen, Interaktion. In: Bogner, A., Littig, B. und Menz, W. (Hrsg.): Das Experteninterview. Theorie, Methode, Anwendung. Opladen: Leske + Budrich, S. 33-70.

Böhmann, T. (2004): Modularisierung von IT-Dienstleistungen - Eine Methode für das Service Engineering. Wiesbaden: Deutscher Universitätsverlag.

Bolisani, E.; Paiola, M. und Scarso, E. (2013): Knowledge protection in knowledge-intensive business services. In: Journal of Intellectual Capital, 14(2), S. 192-4211.

Bönte, W. (2008): Inter-firm trust in buyer–supplier relations: are knowledge spillovers and geographical proximity relevant? In: Journal of Economic Behavior & Organization, 67, S. 855-870.

Bortz, J. und Döring, N. (2006): Forschungsmethoden und Evaluation für Humanund Sozialwissenschaftler. 4. Aufl. Heidelberg: Springer Verlag.

Boschma, R. (2005): Proximity and innovation: a critical assessment. In: Regional Studies, 39, S. 61-74.

Bouncken, R. B. (2003): Konstruktion von organisationalem Wissen in Virtuellen Unternehmungen. In: Die Unternehmung, 57(1), S. 21-44.

Bounfour, A. (1999): Is outsourcing of intangibles a real source of competitive advantage? In: International Journal of Applied Quality Management, 2(2), S. 127-51.

Brocke, H. F. (2011): Kundenorientierte Gestaltung und Vereinbarung standardisierter IT-Dienstleistungen. Dissertation. Universität St. Gallen.

Brown, D. und Wilson, S. (2005): The Black Book of Outsourcing – How to Manage the Changes, Challenges, and Opportunities. New Jersey: Wiley, S. 19-43.

Brugger, R. (2005): IT-Projekte strukturiert realisieren: Situationen analysieren, Lösungen konzipieren - Vorgehen systematisieren, Sachverhalte visualisieren - UML und EPKs nutzen. 2. Aufl. Wiesbaden: Vieweg und Sohn Verlag.

Brüsemeister, T. (2000): Qualitative Forschung - ein Überblick. 1. Aufl. Wiesbaden: Westdeutscher Verlag.

BSI (2016a): IT-Grundschutz-Kataloge, 15. Ergänzungslieferung. Online verfügbar unter https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf, zuletzt geprüft am 18.01.2018.

BSI (2016b): Überblick IT-Grundschutz – Entscheidungshilfe für Manager. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Ueberblick-IT-Grundschutz.pdf?__blob=publicationFile&v=3, zuletzt geprüft am 18.01.2018.

Bullinger, H.-J. und Fähnrich, K.-P. (1997): Betriebliche Informationssysteme: Grundlagen und Werkzeuge der methodischen Softwareentwicklung. Berlin: Springer Verlag.

Büren, A.; Kolbe, L. und Brenner, W. (2003): Content Management zur Realisierung von Customer Knowledge Performance - Konzeption und Umsetzung bei einem Finanzdienstleister. In: Uhr, W.; Esswein, W. und Schoop, E. (Hrsg.): Wirtschaftsinformatik 2003/Band II: Medien, Märkte, Mobilität. Heidelberg: Physica Verlag, S. 519-539.

Carayannopoulos, S. und Auster, E. R. (2010): External knowledge sourcing in biotechnology through acquisition versus alliance. A kbv approach. In: Research Policy, 39(2), S. 254-267.

Carlsson, S. A. (2004): Strategic Knowledge Managing within the Context of Networks. In: Holsapple C. W. (Hrsg.): Handbook on Knowledge Management 1. International Handbooks on Information Systems. 1. Aufl. Berlin, Heidelberg: Springer Verlag, S. 623-650.

CEN / ISSS (2004): Europäischer Leitfaden zur erfolgreichen Praxis im Wissensmanagement, Knowledge Management Workshop. Online verfügbar unter http://www.iwp.jku.at/born/mpwfst/04/German-text-KM-CWAguide.pdf, zuletzt geprüft am 22.03.2018.

Chai, K.-H.; Yap, C.-M. und Wang, X. (2011): Network closure's impact on firms' competitive advantage: The mediating roles of knowledge processes. In: Journal of Engineering and Technology Management, 28(1-2), S. 2-22.

Chan, P. C. W. und Lee, W. B. (2011): Knowledge Audit with Intellectual Capital in the Quality Management Process: An Empirical Study in an Electronics Company. In: The Electronic Journal of Knowledge Management, 9(2), S. 98-116.

Checkland, P. und Holwell S. (1998): Action Research: Its Nature and Validity. In: Systemic Practice and Action Research, 11(1), S. 9-21.

Chiasson, M.; Germonprez, M. und Mathiassen, L. (2008): Pluralist Action Research - a Review of the Information Systems Literature. In: Information Systems Journal, 19(1), S. 31-54.

Clemons, E. K. und Row, M. C. (1991): Sustaining IT advantage: the role of structural differences. In: MIS Quarterly, 15(3), S. 275-292.

Coase, R. H. (1937): The Nature of the Firm. In: Economica, 4(16), S. 386-405.

Cohen, W. M. und Levinthal, D. A. (1990): Absorptive capacity: A new perspective on learning and innovation. In: Administrative Science Quarterly, Special Issue, 35(1), S. 128-152.

Cohen, M. D.; Burkhardt, R.; Dosi, G.; Egidi, M.; Marengo, L.; Warglein, M. und Winter, S. (1996): Routines and other recurring action patterns of organizations: contemporary research issues. In: Industrial and Corporate Change, Oxford University Press, 5(3), S. 653-698.

Cohen, W. M.; Nelson, R.R. und Walsh, J.P. (2000): Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not). Working Paper Nr. 7552, National Bureau of Economic Research, Cambridge, Mass.

Conner, K. R. (1991): A Historical Comparison of the Resource-Based Theory and Five Schools of Thought within Industrial Organization Economics: Do We Have a New Theory of the Firm. In: Journal of Management, 17(1), S. 121-154.

Corsten, H. und Gössinger, R. (2007): Dienstleistungsmanagement. 5. Aufl. München: Oldenbourg Verlag.

Crozier, M. und Friedberg, E. (1979): Macht und Organisation: Zwänge kollektiven Handelns. Königstein: Athenäum Verlag.

Currall, S. C. und Judge, T. A. (1995): Measuring trust between organizational boundary role persons. In: Organizational Behavior and Human Decision Processes, 64(2), S. 151-170.

Currie, W. L.; Michell, V. und Abanishe, O. (2008): Knowledge process outsourcing in financial services: the vendor perspective. In: European Management Journal, 26(2), S. 94-104.

Damm, D.; Kirsch, P.; Schlienger, T.; Teufel, S.; Weidner, H. und Zurfluh, U. (1999): Rapid secure development. Ein Verfahren zur Definiton eines Internet-Sicherheitskonzeptes. Projektbericht SINUS - Sichere Nutzung von Online-Diensten. Online verfügbar unter https://files.ifi.uzh.ch/hkunz/techreports/TR-99/ifi-99.01.pdf, zuletzt geprüft am 18.01.2018.

Davenport, T. H. und Prusak, L. (1999): Wenn Ihr Unternehmen wüsste, was es alles weiß…, Das Praxishandbuch zum Wissensmanagement. 2. Aufl. Landsberg/Lech: Verlag Moderne Industrie.

Davenport, S. (2005): Exploring the role of proximity in sme knowledge-acquisition. In: Research Policy, 34, S. 683-701.

Davenport, T. H. (2011): Rethinking knowledge work: A strategic approach. In: McKinsey Quarterly, February 2011. Online verfügbar unter http://www.mckinsey.com/insights/organization/rethinking_knowledge_work_a_strategic_approach, zuletzt geprüft am 25.02.2018.

Davis, L. (2004): Intellectual property rights, strategy and policy. In: Economics of Innovation and New Technology, 13(5), S. 399-415.

Dawes, S. S.; Cresswell, A. M. und Pardo, T. A. (2009): From "Need to Know" to "Need to Share": Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks. In: Public Administration Review, 69(3), S. 392-402.

de Faria, P. und Sofka, W. (2010): Knowledge Protection Strategies of Multinational Firms - A Cross-Country Comparison. In: Research Policy, 39(7), S. 956-68.

Delfmann, P. (2006): Adaptive Referenzmodellierung. Methodische Konzepte zur Konstruktion und Anwendung wiederverwendungsorientierter Informationsmodelle. Dissertation. Westfälische Wilhelms-Universität Münster. Berlin: Logos Verlag.

Desouza, K. und Awazu, Y. (2004): "Need to Know" - Organizational Knowledge and Management Perspective. In: Information Knowledge Systems Management, 4(1), S. 1-14.

Desouza, K. und Awazu, Y. (2005): Engaged Knowledge Management - Engagement with New Realities. Hampshire, New York: Palgrave Macmillan.

Desouza, K. C. und Vanapalli, G. K. (2005): Securing knowledge in organizations: lessons from the defense and intelligence sectors. In: International Journal of Information Management, 25, S. 85-98.

Desouza, K. C. (2006): Knowledge Security: An Interesting Research Space. In: Journal of Information Science and Technology, 3(1), S. 1-7.

Desouza, K. C. (2008): The neglected dimension in strategic sourcing: security. In: Strategic Outsourcing: An International Journal, 1(3), S. 288-292.

Devargas, M. (1993): Network security. Oxford: NCC Blackwell, S. 43-59.

Dibbern, J. und Heinzl, A. (2009): Outsourcing der Informationsverarbeitung im Mittelstand: Test eines multitheoretischen Kausalmodells. In: Wirtschaftsinformatik, 51(1), S. 118-129.

Diekmann, A. (1995): Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. 1. Aufl. Reinbek: Rowohlt Verlag.

DIN Deutsches Institut für Normung e.V. (2009): DIN 69901 1-5: Projektmanagement – Projektmanagementsysteme: Normengruppe zum Projektmanagement. Berlin: Beuth Verlag.

DIN Deutsches Institut für Normung e.V. (2009): DIN 69901-5. Projektmanagement. Projektmanagementsysteme. Teil 5: Begriffe. Berlin: Beuth Verlag.

Disterer, G.; Fels, F. und Hausotter, A. (Hrsg.) (2003): Taschenbuch der Wirtschaftsinformatik. 2. Aufl. München, Wien: Carl Hanser Verlag.

Drechsler, W. und Natter, M. (2012): Understanding a firm's openness decisions in innovation. In: Journal of Business Research, 65, S. 438-445.

Dresbach, S. (1999): Epistemologische Überlegungen zu Modellen in der Wirtschaftsinformatik. In: Becker, J.; König, W.; Schütte, R.; Wendt, O. und Zelewski, S. (Hrsg.): Wirtschaftsinformatik und Wissenschaftstheorie: Bestandsaufnahme und Perspektiven. Wiesbaden: Gabler Verlag, S. 71-94.

Dumke, R. (2003): Software-Engineering: Eine Einführung für Informatiker und Ingenieure - Systeme, Erfahrungen, Methoden, Tools. 4. Aufl. Braunschweig: Vieweg Verlag.

Duncan, W. und Dörrenberg, F. E. (2009): Leistungsumfang und Lieferobjekt (Scope & deliverables). In: Gessler, M. (Hrsg.): Kompetenzbasiertes Projektmanagement (PM3), Handbuch für die Projektarbeit, Qualifizierung und Zertifizierung auf Basis der IPMA Competence Baseline Version 3.0 (E-Book). 1. Aufl. Nürnberg: GPM Deutsche Gesellschaft für Projektmanagement e.V., S. 581-610.

Dyer, J. H. und Chu, W. (2003): The role of trustworthiness in reducing transaction costs and improving performance: Empirical evidence from the United States, Japan, and Korea. In: Organization Science, 14(1), S. 57-68.

Dyer, J. und Singh, H. (1998): The relational view: cooperative strategy and sources of interorganizational competitive advantage. In: Academy of Management Review, 23(4), S. 660-679.

Easterby-Smith, M.; Lyles, M. A. und Tsang, E. W. K. (2008): Inter-organizational knowledge transfer: current themes and future prospects. In: Journal of Management Studies, 45(4), S. 677-690.

Eckert, C. (2004): IT-Sicherheit: Konzepte, Verfahren, Protokolle. 3. Aufl. München: Oldenbourg Verlag.

EITO (2007): European Information Technology Observatory 2007. Frankfurt: European Information Technology Observatory - European Economic Interest Grouping.

Elango, B. (2008): Using outsourcing for strategic competitiveness in small and medium-sized firms. In: Competitiveness Review: An International Business Journal, 18(4), S. 322-332.

Elche-Hotelano, D. (2011): Sources of knowledge, investments and appropriability as determinants of innovation: An empirical study in service firms. In: Innovation: Management, Policy & Practice, 13(2), S. 220-235.

Ellmann, S.; Behrend, F. D.; Hübner, R. und Weitlaner, E. (2009): Interessengruppen/Interessierte Parteien (Interested parties). In: Gessler, M. (Hrsg.): Kompetenzbasiertes Projektmanagement (PM3),

Handbuch für die Projektarbeit, Qualifizierung und Zertifizierung auf Basis der IPMA Competence Baseline Version 3.0 (E-Book). 1. Aufl. Nürnberg: GPM Deutsche Gesellschaft für Projektmanagement e.V., S. 81-136.

Ellram, L. M.; Tate, W. L. und Billington, C. (2008): Offshore outsourcing of professional services: a transaction cost economics perspective. In: Journal of Operations Management, 26(2), S. 148-63.

Embleton, P. R. und Wright, P. C. (1998): A practical guide to successful outsourcing. In: Empowerment in Organizations, 6(3), S. 94-106.

Encaoua, D.; Guellec, D. und Martinez, C. (2006): Patent Systems for Encouraging Innovation: Lessons from Economic Analysis. In: Research Policy, 35(9), S. 1423-1440.

Ensign, P. C. und Hébert, L. (2010): How reputation affects knowledge sharing among colleagues. In: MIT Sloan Management Review, 51(2), S. 79-81.

Farrell, D. (2004): Beyond offshoring: access your company's global potential. In: Harvard Business Review, 82(12), S. 82-90.

Farrell, M. (2010): Developing a Framework for Measuring Outsourcing Performance. In: LRN Conference, University of Leeds, Institute for Transport Studies and CILT (UK).

Feeny, D. F. und Willcocks, L. P. (1998): Core IS Capabilities for Exploiting Information Technology. In: Sloan Management Review, 39(3), S. 9-21.

Fettke, P. und Loos, P. (2004): Referenzmodellierungsforschung. In: Wirtschaftsinformatik, 46(5), S. 331-340.

Fettke, P. und Loos, P. (2004): Referenzmodellierungsforschung - Langfassung eines Aufsatzes. In: Information Systems & Management Working Papers, 16.

Fettke, P. (2006): Referenzmodellevaluation - Konzeption der strukturalistischen Referenzmodellierung und Entfaltung ontologischer Gütekriterien. Dissertation. Johannes Gutenberg-Universität Mainz.

Fink, D. und Knoblach, B. (2003): Die großen Management Consultants. Ihre Geschichte, ihr Konzepte, ihre Strategien. 1. Aufl. München: Vahlen Verlag.

Fink, A.; Schneidebreit, G. und Voß, S. (2005): Grundlagen der Wirtschaftsinformatik. 2. Aufl. Heidelberg: Physica Verlag.

Fleisch, E. (2001): Das Netzwerkunternehmen. Strategien und Prozesse zur Steigerung der Wettbewerbsfähigkeit in der "Networked Economy". 1. Aufl. Berlin: Springer Verlag.

Flick, U. (2004): Konstruktivismus. In: Flick, U.; von Kardorff, E. und Steinke, I. (Hrsg.): Qualitative Forschung. Ein Handbuch. 3. Aufl. Reinbek: Rowohlt Verlag, S. 150-164.

Flick, U. (2005): Standards, Kriterien, Strategien - Zur Diskussion über Qualität qualitativer Sozialforschung. In: Zeitschrift für qualitative Bildungs-, Beratungs- und Sozialforschung, 6(2), S. 191-210.

Flick, U., von Kardorff, E. und Steinke, I. (2003): Was ist qualitative Forschung? Einleitung und Überblick. In: Flick, U., von Kardorff, E. und Steinke, I. (Hrsg.): Qualitative Forschung. Ein Handbuch. 2. Aufl. Reinbek: Rowohlt Verlag, S. 13-29.

Ford, R. und Helayne, R. (2004): Googling for gold: web crawlers, hacking and defense explained. In: Network Security, 1, S. 10-13.

Frank, U. (2006): Towards a Pluralistic Conception of Research Methods in Information Systems Research. ICB-Research Reports 7, Institut für Informatik und Wirtschaftsinformatik (ICB), Universität Duisburg-Essen.

Frank, U. (2006): Evaluation of Reference Models. In: Fettke, P. und Loos, P. (Hrsg.): Reference Modeling for Business Systems Analysis. Idea Group: Hershey, S. 118-140.

Frank, U.; Klein, S.; Krcmar, H. und Teubner, A. (1998): Aktionsforschung in der WI - Einsatzpotentiale und -probleme. In: Schütte, R.; Siedentopf, J. und Zelewski, S. (Hrsg.): Wirtschaftsinformatik und Wissensschaftstheorie: Grundpositionen und Theoriekerne. Arbeitsbericht Nr. 4, Institut für Produktion und Industrielles informationsmanagement, Universität Essen, S. 71-90.

Fried, A. und Baitsch, C. (2000): Mutmaßungen zu einem überraschenden Erfolg - Zum Verhältnis von Wissensmanagement und Organisationalem Lernen. In: Götz, K. (Hrsg.): Wissensmanagement - zwischen Wissen und Nichtwissen. Schriftenreihe: Managementkonzepte. 2. Aufl. München, Mehring: Hampp Verlag, S. 33-45.

Fried, A. (2001): Konstruktivismus. In: Weik, E.; Lang, R. (Hrsg.): Moderne Organisationstheorien. Eine sozialwissenschaftliche Einführung. 1. Aufl. Wiesbaden: Gabler Verlag, S. 29-60.

Fritsch, M; Wein, T. und Ewers, H.-J. (2005): Marktversagen und Wirtschaftspolitik. Mikroökonomische Grundlagen staatlichen Handelns. 6. Aufl. München: Vahlen Verlag.

Gabriel, R.; Knittel, F.; Taday, H. und Reif-Mosel, A.-K. (2002): Computergestützte Informations- und Kommunikationssysteme in der Unternehmung: Technologien, Anwendungen, Gestaltungskonzepte. 2. Aufl. Berlin et al.: Springer Verlag.

Gadatsch, A. (2008): Grundkurs Geschäftsprozess-Management - Methoden und Werkzeuge für die IT-Praxis: Einführung für Studenten und Praktiker. 5. Aufl. Wiesbaden: Vieweg Verlag.

Gallié, E.-P. und Legros, D. (2012): French firms' strategies for protecting their intellectual property. In: Research Policy, 41, S. 780-794.

Gelwick, R. (1977): The way of discovery: An introduction to the thought of Michael Polanyi. New York: Oxford University Press.

Gerber, M. und von Solms, R. (2005): Management of risk in the information age. In: Computers & Security, 24(1), S. 16-30.

Ghodeswar, B. und Vaidyanathan, J. (2008): Business process outsourcing: an approach to gain access to world-class capabilities. In: Business Process Management Journal, 14(1), S. 23-38.

Gläser, J. und Laudel, G. (2004): Experteninterviews und qualitative Inhaltsanalyse. 1. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

Glaser, B. und Strauss, A. (1967): The discovery of grounded theory: Strategies for qualitative research. Chicago: Aldine.

Göbel, E. (2002): Neue Institutionenökonomik. Konzeption und betriebswirtschaftliche Anwendungen. Stuttgart: Lucius & Lucius Verlag, S. 129-154.

Goeken, M. (2003): Die Wirtschaftsinformatik als anwendungsorientierte Wissenschaft. Symptome, Diagnose und Therapievorschläge. In: Fachberichte des Instituts für Wirtschaftsinformatik der Philipps-Universität Marburg, Nr. 01/03.

Gold, A. H.; Malhotra, A. und Segars, A. H. (2001): Knowledge management: an organizational capabilities perspective. In: Journal of Management Information Systems, 18(1), S. 185-214.

Goldman, J. E. (1998): Applied Data Communications: A Business-Oriented Approach. New York: Wiley.

Gonzalez, R.; Gasco, J. und Llopis, J. (2006): Information systems offshore outsourcing: a descriptive analysis. In: Industrial Management & Data Systems, 106(9), S. 1233-1248.

Grant, R. M. (1991): The Resource-based Theory of Competitive Advantage. Implications for Strategy Formulation. In: California Management Review, 33(3), S. 114-135.

Grant, R. M. (1996): Toward a Knowledge-Based Theory of the Firm. In: Strategic Management Journal, Special Issue, 17, S. 109-122.

Grant, R. M. (1997): The Knowledge-based View of the Firm: Implications for Management Practice. In: Long Range Planning, 30(3), S. 450-454.

Gronau, G. und Bahrs, J. (2010): Systematische Risikoanalyse zur Verhinderung ungewollten Know-How Abflusses. In: Bentele, M.; Gronau, N.; Schütt, P. und Weber, M. (Hrsg.): Mit Wissensmanagement Innovationen vorantreiben! - Kongressband zur KnowTech, 12. Kongress zum IT-gestützten Wissensmanagement in Unternehmen und Organisationen Bad Homburg, 15.-16. September 2010. BITKOM.

Großmann, S. (2010): Die Verifizierung von Nachhaltigkeitsberichten zur Reduzierung von Informationsasymmetrien. Dissertation. Katholische Universität Eichstätt Ingolstadt.

Grund, M. A. (1998): Interaktionsbeziehungen im Dienstleistungsmarketing. Zusammenhänge zwischen Zufriedenheit und Bindung von Kunden und Mitarbeitern, Band 4 der Basler Schriften zum Marketing, Wiesbaden.

Gulati, R. (1995): Does familiarity breed trust? The implications of repeated ties for contractual choices in alliances. In: Academy of Management Journal, 38(1), S. 85-112.

Gummesson, E. (2000): Qualitative methods in management research. 2. Aufl. Thousand Oaks: Sage Publications.

Gutzwiller, T. (1994): Das CC RIM-Referenzmodell für den Entwurf von betrieblichen, transaktionsorientierten Informationssystemen. 1. Aufl. Heidelberg: Physica Verlag.

Hackney, R. A.; Desouza, K. C. und Irani, Z. (2008): Constructing and sustaining competitive inter-organizational knowledge networks: an analysis of managerial web-based facilitation. In: Information Systems Management, 25, S. 356-363.

Hall, B. H. (2005): Exploring the patent explosion. In: Journal of Technology Transfer, 30(1-2), S. 35-48.

Hambrick, D. C. (1983): High profit strategies inmature capital goods industries: a contingency approach. In: Academy of Management Journal, 26(4), S. 687-707.

Hamel, G. und Prahalad, C. K. (1994): Competing for the future. In: Harvard Business Review, 72(4), S. 122-128.

Hamel, G. (1991): Competition for competence and inter-partner learning within international strategic alliances. In: Strategic Management Journal, 12, S. 83-104.

Hanel, P. (2001): Current intellectual protection practices by manufacturing firms in Canada. Université de Sherbrooke, Département d'économie, Working Paper 09-01.

Hannah, D. R. (2005): Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. In: Organization Science, 16(1), S. 71-84.

Harabi, N. (1995): Appropriability of Technological Innovations - an Empirical Analysis. In: Research Policy, 24, S. 981-992.

Hausler, J. H.; Hohn, H.-W. und Lutz, S. (1994): Contingencies of Innovative Networks: A Case Study of Successful R&D Collaboration. In: Research Policy, 23(1), S. 47-66.

Heiman, B. A. und Nickerson, J. A. (2002): Towards reconciling transaction cost economics and the knowledge-based view of the firm: The context of interfirm collaborations. In: International Journal of the Economics of Business, 9(1), S. 97-116.

Heiman, B. A. und Nickerson, J. A. (2004): Empirical evidence regarding the tension between knowledge sharing and knowledge expropriation in collaborations. In: Managerial and Decision Economics, Special Issue, 25(6-7), S. 401-420.

Heinrich, L. J. und Lehner, F. (2005): Informationsmanagement: Planung, Überwachung und Steuerung der Informationsinfrastruktur. 8. Aufl. München: Oldenbourg Verlag.

Heinrich, L. J.; Riedl, R. und Stelzer, D. (2014): Informationsmanagement: Grundlagen, Aufgaben, Methoden. 11. Aufl. München: Oldenbourg Verlag.

Helfferich, C. (2005): Die Qualität qualitativer Daten. Manual für die Durchführung qualitativer Interviews. 2. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

Hertzfeld, H. R.; Link, A. N. und Vonortas, N. S. (2006): Intellectual Property Protection Mechanisms in Research Partnerships. In: Research Policy, 35(6), S. 825-838.

Herzwurm, G. und Stelzer, D. (2008): Wirtschaftsinformatik versus Information Systems - Eine Gegenüberstellung. In: Stuttgarter Schriften zur Unternehmenssoftware der Universität Stuttgart, Arbeitsbericht Nr. 2.

Herzwurm, G. (2000): Kundenorientierte Softwareproduktentwicklung. Teubner Reihe Wirtschaftsinformatik. 1. Aufl. Wiesbaden: Springer Verlag.

Hevner, A. und Chatterjee, S. (2010): Design Research in Information Systems, Theory and Practice. 1. Aufl. New York et al.: Springer Verlag.

Hevner, A.R.; March, S.T.; Park, J. und Ram, S. (2004): Design science in information systems research. In: MIS Quarterly, 28(1), S. 75-105.

Hilke, W. (1989): Grundprobleme und Entwicklungstendenzen des Dienstleistungs-Marketing. In: Hilke W. (Hrsg.): Dienstleistungs-Marketing. Schriften zur Unternehmensführung. Wiesbaden: Gabler Verlag, S. 5-44.

Hoecht, A. und Trott, P. (2005): Outsourcing, information leakage and the risk of losing technology-based competencies. In: European Business Review, 18(5), S. 395-412.

Holthaus, M. (2000): Management der Informationssicherheit in Unternehmen. Dissertation. Universität Zürich.

Howells, J.; Blind, K.; Elder, J. und Evangelista, R. (2003): Knowledge regimes, appropriability and intellectual property protection: a conceptual framework for services. In Lind, K.; Elder, J.; Schmoch, U.; Anderson, B.; Howells, J.; Miles, I.; Roberts, J.; Green, L.; Evangilista, R.; Hipp, C. und Herstatt, C. (Hrsg.): Patents in the Service Industries, Fraunhofer Institute Systems and Innovation Research.

Hradilak, K. P. (2007): Führen von IT-Service-Unternehmen: Zukunft erfolgreich gestalten. Wiesbaden: Vieweg Verlag.

Humphrey, J. und Schmitz, H. (1996): Trust in economic development. Institute of Development Studies (IDS), Paper 355, University of Sussex, Brighton.

Humphreys, P. K.; Li, W. L. und Chan, L. Y. (2004): The impact of supplier development on buyer-supplier performance. In: Omega, 32, S. 131-143.

Hurmelinna-Laukkanen, P. (2011): Enabling collaborative innovation - knowledge protection for knowledge sharing. In: European Journal of Innovation Management, 14(3), S. 303-321

Iivari, J. und Venable, J. (2009): Action research and design science research - seemingly similar but decisively dissimilar. In: Proceedings of the 17th European Conference on Information Systems.

Ilvonen, I. (2013): Knowledge security-a conceptual analysis. Dissertation. Tampere University of Technology.

Inkpen, A. C. und Li, K.-Q. (1999): Joint venture formation: planning and knowledgegathering for success. In: Organizational Dynamics, 27(4), S. 33-47.

Jagersma, P. K. und Gorp, D. M. V. (2007): Redefining the paradigm of global competition: offshoring of service firms. In: Business Strategy Series, 8(1), S. 35-42.

Jennex, M. und Olfman, L. (2005): Assessing knowledge management success. In: International Journal of Knowledge Management, 1(2), S. 33-49.

Jennex, M. und Zyngier, S. (2007): Security as a contributor to knowledge management success. In: Information Systems Frontiers, 9(5), S. 493-504.

Jensen, M. C. und Meckling, W. H. (1976): Theory of the firm: Managerial behavior, agency costs and ownership structure. In: Journal of Financial Economics, 3(4), S. 305-360.

Jiang, R. J. (2002): Knowledge Protection in Strategic Alliances. In: Administrative Sciences Association of Canada (ASAC), Winnipeg.

Jordan, J. und Lowe, J. (2004): Protecting strategic knowledge: insights from collaborative agreements in the aerospace sector. In: Technology Analysis & Strategic Management, 16(2), S. 241-259.

Kaas, K. P. (1995): Einführung: Marketing und Neue Institutionenökonomik. In: Kaas, K. P. (Hrsg.): Kontrakte, Geschäftsbeziehungen, Netzwerke - Marketing und Neue Institutionenökonomik. Zfbf: Sonderheft Nr. 35. Düsseldorf et al.: Verlagsgruppe Handelsblatt, S. 1-18.

Kaas, K. P. (1995b): Marketing zwischen Markt und Hierarchie. In: Kaas, K. P. (Hrsg.): Kontrakte, Geschäftsbeziehungen, Netzwerke - Marketing und Neue Institutionenökonomik. Zfbf: Sonderheft Nr. 35 Düsseldorf et al.: Verlagsgruppe Handelsblatt, S. 19-42.

Kale, P.; Singh, H. und Perlmutter, H. (2000): Learning and protection of proprietary assets in strategic alliances: building relational capital. In: Strategic Management Journal, 21(3), S. 217-237.

Kamoche, K. und Newenham-Kahindi, A. (2012): Knowledge appropriation and HRM: the MNC experience in Tanzania. In: The International Journal of Human Resource Management, 23(14), S. 2854-2873.

Kampffmeyer, U. (2014): Was ist ECM, Enterprise Content Management. Online verfügbar unter http://www.softselect.de/_uploads/pdf/ECM-Enterprise-Content-Management.pdf, zuletzt geprüft am 22.03.2018.

Karabulut, Y.; Kerschbaum, F.; Massacci, F.; Robinson, P. und Yautsiukhin, A. (2007): Security and trust in IT business outsourcing: a manifesto. In: Electronic Notes in Theoretical Computer Science, 179(6), S. 47-58.

Ke, W. und Wei, K. K. (2007): Factors affecting trading partners' knowledge sharing: using the lens of transaction cost economics and socio-political theories. In: Electronic Commerce Research and Applications, 6(3), S. 297-308.

Khalfan, A. Mo. (2004): Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. In: International Journal of Information Management, 24(1), S. 29-42.

Khanna, T. (1998): The scope of alliances. In: Organization Science, 9(3), S. 340-355.

Khanna, T.; Gulati, R. und Nohria, N. (1998): The dynamics of learning alliances: competition, cooperation, and relative scope. In: Strategic Management Journal, 19(3), S. 193-210.

Knackstedt, R. (2006): Fachkonzeptionelle Referenzmodellierung einer Managementunterstützung mit quantitativen und qualitativen Daten: Methodische Konzepte zur Konstruktion und Anwendung. Berlin: Logos Verlag.

Knothe, T.; Herbst, K. und Husen, C. (2004): IT-Services: Neue Wege zur professionellen Dienstleistungsentwicklung. In: Mertins, K. und Spath, D. (Hrsg.): Neue Wege zur professionellen Dienstleistungsentwicklung. Stuttgart: Fraunhofer IRB Verlag.

Koberg, C.; Detienne, D. und Heppard, K. (2003): An empirical test of environmental, organizational, and process factors affecting incremental and radical innovation. In: Journal of High Technology Management Research, 14(1), S. 21-45.

Koch, M; Reiterer, H. und Tjoa, A. M. (1991): Software-Ergonomie: Gestaltung von Edv-Systemen - Kriterien, Methoden und Werkzeuge. Wien: Springer Verlag.

Kogut, B. und Zander, U. (1992): Knowledge of the firm, combinative capabilities, and the replication of technology. In: Organization Science, Special Issue, 3(3), S. 383-397.

König, W.; Heinzl, A.; Rumpf, M.-J. und Poblotzki, A. (1996): Zur Entwicklung der Forschungsmethoden und Theoriekerne der Wirtschaftsinformatik - Eine kombinierte Delphi- und AHP-Untersuchung. In: Heilmann, H.; Heinrich, L. J. und Roithmayr, F. (Hrsg.): Information Engineering - Wirtschaftsinformatik im Schnittpunkt von Wirtschafts-, Sozial- und Ingenieurwissenschaften. München: Oldenbourg Verlag, S. 35-65.

Koza, M. P. und Lewin, A. Y. (1998): The co-evolution of strategic alliances. In: Organization Science, 9(3), S. 255-264.

Kräkel, M. (2002): Withholding of Knowledge in Organizations. In: Schmalenbach Business Review, 54, S. 221-242.

Krcmar, H. (2015): Informationsmanagement. 6. Aufl. Wiesbaden: Springer Verlag.

Kremer, R. und Rohde A. (2009): Projektorganisation (Project organisation). In: Gessler, M. (Hrsg.): Kompetenzbasiertes Projektmanagement (PM3), Handbuch für die Projektarbeit, Qualifizierung und Zertifizierung auf Basis der IPMA Competence Baseline Version 3.0 (E-Book). 1. Aufl. Nürnberg: GPM Deutsche Gesellschaft für Projektmanagement e.V., S. 293-350.

Kremer, R. (2005): Formen der Projektorganisation. Projektrollen und Aufgabenbereiche. In: Litke, H.-D. (Hrsg.) Projektmanagement Handbuch für die Praxis. München: Carl Hanser Verlag, S. 75-126.

Kutschker, M. und Schmid, S. (2011): Internationales Management. 7. Aufl. München: Oldenbourg Verlag.

Kuusisto, A. (2008): Customer roles in business services production: implications for involving customers in service innovation. Research Report Nr. 195, Lappeenranta University of Technology.

Lamnek, S. und Krell, C. (2016): Qualitative Sozialforschung. 6. Aufl. Weinheim: Beltz.

Lau, F. (1997): A Review on the Use of Action Research in Information Systems Studies. In: Lee, A. S.; Liebenau, J. und DeGross, J. (Hrsg.): Information Systems and Qualitative Research. London: Chapman & Hall, S. 31-68.

Laursen, K. und Salter, A. (2005): My precious - the role of appropriability strategies in shaping innovative performance. Copenhagen Business School, Department of Industrial Economics and Strategy / Aalborg University, Department of Business Studies. DRUID Working Papers (05-02).

Lawson, B.; Samson, D. und Roden, S. (2012): Appropriating the value from innovation: inimitability and the effectiveness of isolating mechanisms. In: R&D Management, 42(5), S. 420-434.

Lee, S.-C.; Chang, S.-N.; Liu, C.-Y. und Yang, J. (2007): The Effect of Knowledge Protection, Knowledge Ambiguity, and Relational Capital on Alliance Performance. In: Knowledge and Process Management, 14(1), S. 58-69.

Lehmann, F. R. (2008): Integrierte Prozessmodellierung mit ARIS. 1. Aufl. Heidelberg: Dpunkt Verlag.

Lehner, F.; Hildebrand, K.; Maier, R. (1995): Wirtschaftsinformatik. Theoretische Grundlagen. München et al.: Carl Hanser Verlag.

Lehrer, M.; Ordanini, A.; DeFillippi, R. und Miozzo, M. (2012): Challenging the orthodoxy of value co-creation theory: A contingent view of co-production in designintensive business services. In: European Management Journal, 30(6), S. 499-509.

Lei, D.; Slocum Jr., J. W. und Pitts, R. A. (1997): Building cooperative advantage: managing strategic alliances to promote organizational learning. In: Journal of World Business, 32(3), S. 203-223.

Leiponen, A. und Byma, J. (2009): If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies. In: Research Policy, 38(9), S. 1478-1488.

Leist, S. (2002): Bankenarchitektur des Informationszeitalters - Zielsetzung und Gestaltungsebenen. In: Leist, S. und Winter, R. (Hrsg.): Retail-Banking im Informationszeitalter: integrierte Gestaltung der Geschäfts-, Prozess- und Applikationsebene. Business engineering. Berlin: Springer Verlag, S. 3-28.

Lemarie, S.; Mangematin, V. und Torre, A. (2001): Is the creation and development of biotech smes localised? Conclusions drawn from the french case. In: Small Business Economics, 17(1-2), S. 61-76.

Leonard-Barton, D. (1992): Core Capabilities and Core Rigidities: A Paradox in Managing New Product Development. In: Strategic Management Journal, Special Issue, 13, S. 111-125.

Levinthal, D. A. und March, J. G. (1993): The Myopia of Learning. In: Strategic Management Journal, Special Issue, 14, S. 95-112.

Levitin, A. V. und Redman, T. C. (1998): Data as a ressource. Properties, implications and prescriptions. In: Sloan Management Review, 40(1), S. 89-102.

Lewin, K. (1946): Action Research and Minority Problems. In: Journal of Social Issues, 2(4), S. 34-46.

Li, D.; Eden, L.; Hitt, M. A. und Ireland, R. D. (2008): Friends, acquaintances, or strangers? Partner selection in R&D Alliances. In: Academy of Management Journal, 51(2), S. 315-334.

Lieberman, M. B. und Montgomery, D. B. (1988): First-mover advantages. In: Strategic Management Journal, Special Issue, 9, S. 41-85.

Liebeskind, J. P. (1996): Knowledge, strategy, and the theory of the firm. In: Strategic Management Journal, Special Issue, 17, S. 93-107.

Liebeskind, J. P. (1997): Keeping Organizational Secrets: Protective Institutional Mechanisms and Their Costs. In: Industrial & Corporate Change, 6(3), S. 623-663.

Lindemann, U.; Meiwald, Th.; Petermann, M. und Schenkl, S. (2012): Know-how-Schutz im Wettbewerb, Gegen Produktpiraterie und unerwünschten Wissenstransfer. 1. Aufl. Heidelberg et al.: Springer Verlag.

Link, A. und Ruhm, C. (2011): Public knowledge, private knowledge: the intellectual capital of entrepreneurs. In: Small Business Economics, Springer Verlag, 36(1), S. 1-14.

Lippold, D. (2016): Grundlagen der Unternehmensberatung: Strukturen - Konzepte - Methoden. 1. Aufl. Wiesbaden: Springer Gabler Verlag.

Loh, L. und Venkatraman, N. (1992): Diffusion of information technology outsourcing: Influence sources and kodak effect. In: Information Systems Research, 3(4), S. 334-358.

Loos, P. und Fettke, P. (2007): Zum Beitrag empirischer Forschung in der Informationsmodellierung. In: Loos, P. und Krcmar H. (Hrsg.): Architekturen und Prozesse: Strukturen und Dynamik in Forschung und Unternehmen. Berlin: Springer Verlag, S. 33-50.

Luoma, T.; Paasi, J. und Valkokari, K. (2010): Intellectual property in inter-organisational relationships - findings from an interview study. In: International Journal of Innovation Management, 14(3), S. 399-414.

Maier, R. (2007): Knowledge Management Systems. Information and Communication Technologies for Knowledge Management. 3. Aufl. Berlin et al.: Springer Verlag.

Maier, R.; Hädrich, T. und Peinl, R. (2005): Enterprise knowledge infrastructures. Berlin et al.: Springer Verlag.

Majchrzak, A. und Jarvenpaa, S. (2010): Safe Contexts for Interorganizational Collaborations Among Homeland Security Professionals. In: Journal of Management Information Systems, 27(2), S. 55-86.

Manhart, M. und Thalmann, S. (2013): An Integrated Risk Management Framework: Measuring the Success of Organizational Knowledge Protection. In: Proceedings of the 19th Americas Conference on Information Systems (AMCIS), Chicago.

Manhart, M. und Thalmann, S. (2015): Protecting organizational knowledge: a structured literature review. In: Journal of Knowledge Management, 19(2), S. 190-211.

Manhart, M.; Thalmann, S. und Maier, R. (2015): The ends of knowledge sharing in networks using information technology to start knowledge protection. In: Proceedings of the 23rd European Conference on Information Systems (ECIS), Münster.

Manning, S.; Massini, S. und Lewin, A. Y. (2008): A dynamic perspective on next-generation offshoring: the global sourcing of science and engineering talent. In: Academy of Management Perspectives, 22(3), S. 35-54.

March, J. G. (1991): Exploration and Exploitation in Organizational Learning. In: Organization Science, 2(1), S. 71-87.

Mayer, K. J. (2006): Spillovers and governance: an analysis of knowledge and reputational spillovers in information technology. In: Academy of Management Journal, 49(1), S. 69-84.

Mayer, R. C.; Davis, J. H. und Schoorman, F. D. (1995): An integrative model of organizational trust. In: The Academy of Management Review, 20(3), S. 709-734.

Mayring, P. (2015): Qualitative Inhaltsanalyse: Grundlagen und Techniken. 12. Aufl. Weinheim: Beltz.

Mayring, P. (2016): Einführung in die Qualitative Sozialforschung. 6. Aufl. Weinheim: Beltz.

McCutchen, W. W.; Swamidass, P. M. und Teng, B.-S. (2004): R&D risk-taking in strategic alliances: New explanations for R&D alliances in the biopharmaceutical industry. In: Management International Review, 44(1), S. 53-67.

McEvily, B.; Perrone, V. und Zaheer, A. (2003): Trust as an organizing principle. In: Organization Science, 14(1), S. 91-103.

Meffert, H. und Bruhn, M. (2009): Dienstleistungsmarketing. Grundlagen - Konzepte - Methoden. 6. Aufl. Wiesbaden: Gabler Verlag.

Mentzer, J. T.; Min, S. und Zacharia, Z. G. (2000): The nature of interfirm partnering in supply chain management. In: Journal of Retailing, 76(4), S. 549-568.

Mertens, P.; Back, A.; Becker, J.; König, W.; Krallmann, H.; Rieger, B.; Scheer, A.-W.; Seibt, D.; Stahlknecht, P.; Strunz, H.; Thome, R. und Wedekind, H. (1997): Lexikon der Wirtschaftsinformatik. 3. Aufl. Berlin, Heidelberg: Springer Verlag.

Mertins, K., Alwert, K. und Heisig, P. (2005): Wissensbilanzen: Intellektuelles Kapital erfolgreich nutzen und entwickeln. Berlin, Heidelberg: Springer Verlag.

Mertins, K.; Orth, R. und Finke, I. (2009): Grundlagen für Wissensmanagement. In: Mertins, K. und Seidel, H. (Hrsg.): Wissensmanagement im Mittelstand. Grundlagen - Lösungen - Praxisbeispiele. Berlin: Springer Verlag.

Metters, R. (2008): A typology of offshoring and outsourcing in electronically transmitted services. In: Journal of Operations Management, 26(2), S. 198-211.

Meuser, M. und Nagel, U. (1991): Experteninterviews - vielfach erprobt, wenig bedacht: Ein Beitrag zur qualitativen Methodendiskussion. In: Garz, D. und Kraimer, K. (Hrsg.): Qualitativ-empirische Sozialforschung: Konzepte, Methoden, Analysen. Opladen: Westdeutscher Verlag, S. 441-471.

Miles, I.; Kastrinos, N.; Bilderbeek, R.; den Hertog, P.; Flanagan, K.; Huntink, W. und Bouman, M. (1995): Knowledge-intensive business services: users, carriers and sources of innovation. In: European Innovation Monitoring System (EIMS) Reports, DG13. Online verfügbar unter https://www.e-scholar.manchester.ac.uk/api/datastream?publicationPid=uk-ac-man-scw:75252&datastreamId=FULL-TEXT.PDF, zuletzt geprüft am 22.03.2018.

Miles, I.; Andersen, B.; Boden, M. und Howells, J. (2000): Service production and intellectual property. In: International Journal of Technology Management, 20(1-2), S. 95-115.

Milgrom, P. R. und Roberts, J. (1992): Economics, Organization and Management. Englewood Cliffs: Prentice-Hall.

Mingers, J. (2001): Combining IS Research Methods - Towards a Pluralist Methodology. In: Information Systems Research, 12(3), S. 240-259.

Möhring, W. und Schlütz, D. (2010): Die Befragung in der Medien- und Kommunikationswissenschaft: Eine praxisorientierte Einführung. 2. Aufl. Wiesbaden: VS Verlag für Sozialwissenschaften.

Monczka, R. M.; Carter, J. R.; Markham, W. J., Blascovich, J. und Slaight, T. (2005): Outsourcing Strategically for Sustainable Competitive Advantage. Binghamton: CAPS Research.

Monteiro, F.; Mol, M. J. und Birkinshaw, J. (2011): External Knowledge Access Versus Internal Knowledge Protection: A Necessary Trade-Off? In: Academy of Management, Annual Meeting Proceedings, S. 1-6.

Motzel, E. (2006): Projektmanagement Lexikon. Begriffe der Projektwirtschaft von ABC-Analyse bis Zwei-Faktoren-Theorie. Weinheim: Wiley.

Mowery, D. C.; Oxley, J. E. und Silverman, B. S. (1996): Strategic alliance and interfirm knowledge transfer. In: Strategic Management Journal, Special Issue, 17(2), S. 77-91.

Mowery, D. C.; Oxley, J. E. und Silverman, B. S. (1998): Technological overlap and interfirm cooperation: Implications for the resource-based view of the firm. In: Research Policy, 27(5), S. 507-523.

Muller, E. und Doloreux, D. (2007): The key dimensions of knowledge-intensive business services (KIBS) analysis: a decade of evolution. Hg. v. Fraunhofer Institute for Systems and Innovation Research ISI. Arbeitspapiere Unternehmen und Region (U1/2007). Online verfügbar unter http://www.isi.fraunhofer.de/isi-wAssets/docs/p/de/arbpap_unternehmen_region/ap_u1_2007.pdf, zuletzt geprüft am 18.01.2018.

Nassimbeni, G.; Sartor, M. und Dus, D. (2012): Security risks in service offshoring and outsourcing. In: Industrial Management & Data Systems, 112(3), S. 405-440.

Nelson, R. R. und Winter, S. G. (1982): An Evolutionary Theory of Economic Change. Cambridge, Mass.: The Belknap Press of Harvard University Press.

Neuhäusler, P. (2012): The use of patents and informal appropriation mechanisms - Differences between sectors and among companies. In: Technovation, 32(12), S. 681-693.

Neville, K.; Powell, P. und Panteli, N. (2003): Knowledge and security. In: Proceedings of the 9th Americas Conference on Information Systems (AMCIS), Tampa.

Nonaka, I. und Takeuchi, H. (1995): The knowledge-creating company. How Japanese Companies create the dynamics of innovation. New York: Oxford University Press.

Nonaka, I. und Takeuchi, H. (1997): Die Organisation des Wissens: Wie japanische Unternehmen eine brachliegende Ressource nutzbar machen. Frankfurt am Main: Campus Verlag.

Nonaka, I. (1994): A Dynamic Theory of Organizational Knowledge Creation. In: Organization Science, 5(1), S. 14-37.

Norman, P. M. (2001): Are your Secrets Safe? Knowledge Protection in Strategic Alliances. In: Business Horizons, 44(6), S. 51-60.

Norman, P. M. (2002): Protecting knowledge in strategic alliances Resource and relational characteristics. In: The Journal of High Technology Management Research, 13(2), S. 177-202.

Norman, P. M. (2004): Knowledge acquisition, knowledge loss, and satisfaction in high technology alliances. In: Journal of Business Research, 57(6), S. 610-619.

North, K. und Güldenberg, S. (2008): Produktive Wissensarbeit(er). Antworten auf die Management-Herausforderung des 21. Jahrhunderts. 1. Aufl. Wiesbaden: Gabler Verlag.

North, K. und Reinhardt, K. (2005): Kompetenzmanagement in der Praxis. 1. Aufl. Wiesbaden: Gabler Verlag, S. 20-32, S. 113-116.

OECD (2008): Glossary of Statistical Terms. Online verfügbar unter http://www.oecd-ilibrary.org/docserver/download/3008121e.pdf?expires=1521713287&id=id&accname=guest&checksum=8474E8082868F2313162C745D1C51692, zuletzt geprüft am 22.03.2018.

Olander, H. und Hurmelinna-Laukkanen, P. (2010): The effects of HRM-related mechanisms on communication in R&D collaboration. In: International Journal of Innovation Management, 14(3), S. 415-433.

Olander, H.; Hurmelinna-Laukkanen, P. und Mähönen, J. (2009): What's small size got to do with it? Protection of intellectual assets in SMEs. In: International Journal of Innovation Management, 13(3), S. 349-370.

Olander, H.; Hurmelinna-Laukkanen, P.; Blomqvist, K. und Ritala, P. (2010): The Dynamics of Relational and Contractual Governance Mechanisms in Knowledge Sharing of Collaborative R&D Projects. In: Knowledge and Process Management, 17(4), S. 188-204.

Olander, H.; Hurmelinna-Laukkanen, P. und Heilmann, P. (2011): Do SMEs benefit from HRM-Related knowledge protection in innovation management. In: International Journal of Innovation Management, 15(3), S. 593-616.

Olander, H.; Vanhala, M. und Hurmelinna-Laukkanen, P. (2014): Reasons for choosing mechanisms to protect knowledge and innovations. In: Management Decision, 52(2), S. 207-229.

Olsen, K. B. (2006): Productivity impacts of offshoring and outsourcing: a review. OECD Directorate for Science, Technology and Industry. STI Working Paper, Paris. Online verfügbar unter http://www.oecd.org/science/sci-tech/36231337.pdf, zuletzt geprüft am 22.03.2018.

Olson, M. (1971): The logic of collective action: Public Goods and the Theory of Groups. In: Cambridge, Mass.: Harvard University Press.

Österle, H.; Becker, J.; Frank, U.; Hess, T.; Karagiannis, D.; Krcmar, H.; Loos, P.; Mertens, P.; Oberweis, A. und Sinz, E. J. (2010): Memorandum zur gestaltungsorientierten Wirtschaftsinformatik. In: Österle, H.; Winter, R. und Brenner, W. (Hrsg.): Gestaltungsorientierte Wirtschaftsinformatik: Ein Plädoyer für Rigor und Relevanz. München: infowerk ag, S. 1-6.

Ostrowski, L. und Helfert, M. (2012): Reference Model in Design Science Research to Gather and Model Information. In: Proceedings of the 18th Americas Conference on Information Systems (AMCIS), Seattle.

Oxley, J. E. (1999): Institutional environment and the mechanisms of governance: the impact of intellectual property protection on the structure of inter-firm alliances. In: Journal of Economic Behavior & Organization, 38, S. 283-309.

Oxley, J. E. und Sampson, R. C. (2004): The scope and governance of international R&D alliances. In: Strategic Management Journal, 25(8-9), S. 723-749.

Päällysaho, S. und Kuusisto, J. (2008a): Intellectual Property Protection in Service Sector. International Chamber of Commerce, Paris. Online verfügbar unter https://www.researchgate.net/publication/265221605_Intellectual_property_protection_in_service_sector, zuletzt abgerufen am 22.03.2018.

Päällysaho, S. und Kuusisto, J. (2008b): Intellectual property protection as a key driver of service innovation: an analysis of innovative KIBS businesses in Finland and UK. In: International Journal of Services Technology and Management, 9(3-4), S. 268-284.

Päällysaho, S. und Kuusisto, J. (2011): Informal ways to protect intellectual property (IP) in KIBS businesses. In: Innovation: Management, Policy & Practice, 13(1), S. 62-76.

Pai, A. P. und Basu, S. (2007): Offshore technology outsourcing: overview of management and legal issues. In: Business Process Management Journal, 13(1), S. 21-46.

Palvia, P.; Mao, E.; Salam, A. F. und Soliman, K. S. (2003): Management Information Systems Research: What's There in a Methodology? In: Communications of the Association for Information Systems, 11(16), S. 289-309.

Parkhe, A. (1993): Strategic alliance structuring: A game theoretic and transaction cost examination of interfirm cooperation. In: The Academy of Management Journal, 36(4), S. 794-829.

Pawlowsky, P. (2019): Wissensmanagement. Berlin, Boston: De Gruyter Oldenbourg Verlag.

Peffers, K.; Tuunanen, T.; Rothenberger, M. und Chatterjee, S. (2007): A Design Science Research Methodology for Information Systems Research. In: Journal of Management Information Systems, 24(3), S. 45-78.

Penrose, E. T. (1959): The Theory of the Growth of the Firm. New York: Wiley.

Peritsch, M. (2000): Wissensbasiertes Innovationsmanagement: Analyse - Gestaltung - Implementierung. Dissertation. Universität Graz. Wiesbaden: Deutscher Universitätsverlag.

Perri, A. und Andersson, U. (2014): Knowledge Outflows from Foreign Subsidiaries and the Tension Between Knowledge Creation and Knowledge Protection: Evidence from the Semiconductor Industry. In: International Business Review, 23(1), S. 63-75.

Pfetzing, K. und Rohde, A. (2006): Ganzheitliches Projektmanagement. 2. Aufl. Zürich: Versus Verlag.

Polanyi, M. (1958): Personal Knowledge. Chicago: The University of Chicago Press.

Polanyi, M. (1966): The Tacit Dimension. London: Routledge & Kegan Paul.

Polanyi, M. (1985): Implizites Wissen. 1. Aufl. Frankfurt am Main: Suhrkamp Taschenbuch Verlag.

Porter, M. E. (1996): What is strategy? In: Harvard Business Review, 74(6), S. 61-78.

Probst, G.; Raub, St. und Romhardt, K. (1999): Wissen Managen: Wie Unternehmen ihre wertvollste Ressource optimal nutzen. 3. Aufl. Frankfurt am Main: Gabler Verlag.

Probst, G.; Raub, S. und Romhardt, K. (2006): Wissen managen, Wie Unternehmen ihre wertvollste Ressource optimal nutzen, 5. Aufl. Wiesbaden: Gabler Verlag, S. 15-30.

Quinn, J. B. (1992): Intelligent Enterprise. A Knowledge and Service Based Paradigm for Industry. New York: Free Press.

Quinn, J. B. (1999): Strategic outsourcing: leveraging knowledge capabilities. In: Sloan Management Review, 40(4), S. 9-21.

Quintas, P.; Lefrere, P. und Jones, G. (1997): Knowledge management: a strategic agenda. In: Long Range Planning, 30(3), S. 385-391.

Rapoport, R. N. (1970): Three Dilemmas in Action Research. In: Human Relations, 23(6), S. 499-513.

Rebernik, M. und Bradac, B. (2006): Cooperation and opportunistic behaviour in transformational outsourcing. In: Kybernetes, 35(7-8), S. 1005-1013.

Richter, R. und Furobotn, E. (1996): Neue Institutionenökonomik: Eine Einführung und kritische Würdigung, Tübingen: Mohr (Siebeck).

Roehl, T. W. und Truitt, J. F. (1987): Stormy Open Marriages Are Better: Evidence from U.S., Japanese and French Cooperative Ventures in Commercial Aircraft. In: The Columbia journal of world business, 22(2), S. 87-95.

Rosemann, M. und Schütte, R. (1999): Multiperspektivistische Referenzmodellierung. In: Becker, J.; Rosemann, M. und Schütte, R. (Hrsg.): Referenzmodellierung: State-of-the-art und Entwicklungsperspektiven. Heidelberg: Physica Verlag, S. 22-44.

Rosenbaum, H. (2000): The information environment of electronic commerce. Information imperatives for the firm. In: Journal of Information Science, 26(3), S. 161-171.

Rudolph, S. (2009): Servicebasierte Planung und Steuerung der IT-Infrastruktur im Mittelstand: Ein Modellansatz zur Struktur der IT-Leistungserbringung. Informationsmanagement und Computer Aided Team. 1. Aufl. Wiesbaden: Gabler Verlag.

Sabel, C. F. (1993): Studied trust: Building new forms of cooperation in a volatile economy. In: Human Relations, 46(9), S. 1133-1170.

Sako, M. (1992): Prices, Quality and Trust: Inter-firm Relations in Britain and Japan. Cambridge: Cambridge University Press.

Sampson, R. (2007): R&D alliances and firm performance: The impact of technological diversity and alliance organization on innovation. In: The Academy of Management Journal, 50(2), S. 364-386.

Scheppele, K. L. (1988): Legal Secrets. Equality and Efficiency in the Common Law. Chicago und London: The University of Chicago Press.

Schlagheck, B. (2000): Objektorientierte Referenzmodelle für das Prozess- und Projektcontrolling: Grundlagen - Konstruktion - Anwendungsmöglichkeiten. Wiesbaden: Gabler Verlag.

Schneider, G.; Geiger, I. K. und Scheuring, J. (2008): Prozess- und Qualitätsmanagement: Grundlagen der Prozessgestaltung und Qualitätsverbesserung mit zahlreichen Beispielen, Repetitionsfragen und Antworten. Zürich: Compendio Bildungsmedien.

Schneier, B. (2001): Secrets & Lies. IT-Sicherheit in einer vernetzten Welt. 1. Aufl. Heidelberg: dpunkt-Verlag.

Schreiner, M; Hess, T. und Benlian, A. (2015): Gestaltungsorientierter Kern oder Tendenz zur Empirie? Zur neueren methodischen Entwicklung der Wirtschaftsinformatik. Arbeitsbericht 1/2015, Ludwig Maximiliansuniversität München. Online verfügbar unter http://www.ise.tu-darmstadt.de/media/ise/publikationen_3/AB_WI_Methoden_1_15.pdf, zuletzt geprüft am 18.01.2018.

Schultze, U. und Leidner, D. E. (2002): Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions. In: MIS Quarterly, 26(3), S. 213-242.

Schütte, R. (1998): Grundsätze ordnungsmäßiger Referenzmodellierung: Konstruktion konfigurations- und anpassungsorientierter Modelle. Wiesbaden: Gabler Verlag.

Schütte, R. (2007): Der Non Statement View in der Wirtschaftsinformatik. Einsatz- und Erfolgsbarrieren. In: Lehner, F. und Zelewski, S. (Hrsg.): Wissenschaftstheoretische Fundierung und wissenschaftliche Orientierung der Wirtschaftsinformatik. Berlin: GITO-Verlag, S. 61-70.

Schwabe, G. (2008): Designorientierung in der Wirtschaftsinformatik - ein Beitrag zu einer Streitschrift. In: Jung, R. und Myrach, T. (Hrsg.): Quo vadis Wirtschaftsinformatik? Festschrift für Prof. Gerhard F. Knolmayer zum 60. Geburtstag. Wiesbaden: Gabler Verlag, S. 147-162.

Scott, W. R. (1986): Grundlagen der Organisationstheorie. Frankfurt am Main: Campus-Verlag.

Sen, F. und Shiel, M. (2006): From business process outsourcing (BPO) to knowledge process outsourcing (KPO): some issues. In: Human Systems Management, 25(2), S. 145-155.

Siebert, H. (2004): Sozialkonstruktivismus, Gesellschaft als Konstruktion. In: Journal of Social Science Education, 3(2), S. 95-103.

Simatupang, T. und Sridharan, R. (2002): The collaborative supply chain. In: Journal of Logistics Management, 13(1), S. 15-30.

Simon, H. A. (1991): Bounded Rationality and Organizational Learning. In: Organization Science, 2(1), S. 125-134.

Simon, H. A. (1996): The Sciences of Artificial. 3. Aufl. Cambridge Mass.: MIT Press.

Smedlund, A. (2006): The roles of intermediaries in a regional knowledge system. In: Journal of Intellectual Capital, 7(2), S. 204-220.

Sofka, W. und Shehu, E. (2009): Host Country Contigencies on Knowledge Protection Strategies of Multinational Firms - Bring a Knife to a Gunfight? Zentrum für Europäische Wirtschaftsforschung, Discussion Paper, 09-002. Online verfügbar unter http://ftp.zew.de/pub/zew-docs/dp/dp09002.pdf, zuletzt geprüft am 22.03.2018.

Song, D. (2008): Konzept zum Entwurf einer Methode zum Wissens- und Datenschutz in der Produktentstehung im Automobilbau. Dissertation. TU Darmstadt.

Speck, M. und Schnetgöke, N. (2005): Sollmodellierung und Prozessoptimierung. In: Becker, J.; Kugeler, M. und Rosemann, M. (Hrsg.): Prozessmanagement: Ein Leitfaden zur prozessorientierten Organisationsgestaltung. 5. Aufl. Berlin: Springer Verlag, S. 185-220.

Spender, J.-C. (1994): Organizational Knowledge, Collective Practice and Penrose Rents. In: International Business Review, 3(4), S. 353-367.

Spender, J.-C. (1996): Organizational Knowledge, Learning and Memory: Three Concepts in Search of a Theory. In: Journal of Organizational Change Management, 9(1), S. 63-78.

Stachowiak, H. (1973): Allgemeine Modelltheorie. Wien und New York: Springer Verlag.

Stahlknecht, P. und Hasenkamp, U. (2005): Einführung in die Wirtschaftsinformatik. 11. Aufl. Berlin: Springer Verlag.

Steininger, K.; Riedl, R.; Roithmayr, F. und Mertens, P. (2009): Moden und Trends in Wirtschaftsinformatik und Information Systems - Eine vergleichende Literaturanalyse. In: Wirtschaftsinformatik, 51(6), S. 478-495.

Stelzer, D. (2014): Definition Wissen. Online verfügbar unter http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/daten-wissen/Wissensmanagement/Wissen/index.html/, zuletzt geprüft am 18.01.2018.

Strambach, S. (2008): Knowledge-intensive business services (KIBS) as rivers of multilevel knowledge dynamics. In: International Journal of Services Technology and Management, 10(2-4), S. 152-174.

Subramanyam, R. und Susarla, A. (2007): Contracting, incentives and inter-organizational routines in information technology outsourcing. In: Academy of Management, Best Paper Proceedings, 1, S. 1-7.

Szulanski, G. (1996): Exploring internal stickiness: Impediments to the transfer of best practice within the firm. In: Strategic Management Journal, Special Issue, 17(S2), S. 27-43.

Taylor, C. T. und Silberston, Z. A. (1973): The Economic Impact of the Patent System: A study of the British experience. Cambridge: Cambridge University Press.

Teece, D. J. (1998): Capturing Value from Knowledge Assets: The New Economy, Markets for Know-How, and Intagible Assets. In: California Management Review, 40(3), S. 55-79.

Teubner, R. A. (1999): Organisations- und Informationssystemgestaltung. Theoretische Grundlagen und integrierte Methoden. In: Becker, J.; Grob, H. L. und Klein, S. (Hrsg.): Informationsmanagement und Controlling. Wiesbaden: Gabler Verlag und Deutsche Universitäts-Verlag.

Teubner, A. (2008): IT-Service Management: Ein neues Paradigma für das Informationsmanagement. In: Becker, J.; Grob H. L.; Klein, S.; Kuchen, H.; Müller-Funk U. und Vossen, G. (Hrsg.): Arbeitsberichte des Instituts für Wirtschaftsinformatik. Münster: Institut für Wirtschaftsinformatik, Westfälische Wilhelms-Universität Münster.

Thalmann, S. und Manhart, M. (2013): Enforcing Organizational Knowledge Protection: An Investigation of Currently Applied Measures. In: Paper presented at the 7th (pre-ICIS) Workshop on Infor-

mation Security and Privacy (WISP), Milan, Italy. Online verfügbar unter: https://www.researchgate.net/profile/Stefan_Thalmann/publication/271212108_Enforcing_Organizational_Knowledge_Protection_An_Investigation_of_Currently_Applied_Measures/links/54c262740cf256ed5a8cdd7b/Enforcing-Organizational-Knowledge-Protection-An-Investigation-of-Currently-Applied-Measures.pdf, zuletzt geprüft am 22.03.2018.

Thalmann, S.; Bachlechner, D.; Demetz, L. und Maier, R. (2012): Challenges in Cross-Organizational Security Management. In: 45th Hawaii International Conference on System Sciences (HICSS).

Tongo, C. I. (2013): A Performance Model for Knowledge-Based Firms: Lessons for Managers. In: International Journal of Management, 30(2), S. 704-716.

Traoré, N. (2005): Innovation commercialization by Canadian biotech firms: pathways from ideas to market. In: Paper Presented at the DRUID 10th Anniversary Conference 2005 on "Dynamics of Industry and Innovation: Organizations, Networks and Systems", Copenhagen.

Trkman, P. und Desouza, K. C. (2012): Knowledge Risks in Organizational Networks: An Exploratory Framework. In: The Journal of Strategic Information Systems, 21(1), S. 1-17.

Tsoukas, H. (1996): The Firm as a Distributed Knowledge System: A Constructionist Approach. In: Strategic Management Journal, Special Issue, 17, S. 11-25.

Ulrich, H. (1984): Management. Schriftenreihe Unternehmung und Unternehmungsführung. Band 13. Bern: Haupt Verlag.

Ulrich, H. (2001): Das St. Galler Management-Modell. Hans Ulrich Gesammelte Schriften. Band 2. Bern: Haupt Verlag.

van Wijk, R.; Jansen, J. J. P. und Lyles, M. A. (2008): Inter- and Intra-Organizational Knowledge Transfer: A Meta-Analytic Review and Assessment of its Antecedents and Consequences. In: Journal of Management Studies, 45(4), S. 830-853.

Väyrynen, K.; Hekkala, R. und Liias, T. (2013): Knowledge Protection Challenges of Social Media Encountered by Organizations. In: Journal of Organizational Computing and Electronic Commerce, 23(1), S. 34-55.

vom Brooke, J. und Fettke, P. (2018): Referenzmodellierung - Enzyklopaedie der Wirtschaftsinformatik. Online verfügbar unter https://www.researchgate.net/publication/322289374_Referenzmodellierung_-_Enzyklopaedie_der_Wirtschaftsinformatik, zuletzt abgerufen am 22.03.2018.

vom Brocke, J. (2003): Referenzmodellierung, Gestaltung und Verteilung von Konstruktionsprozessen. Dissertation. Westfälische Wilhelms-Universität Münster.

von Hippel, E. (1994): "Sticky information" and the Locus of Problem Solving: Implications for Innovation. In: Management Science, 40(4), S. 429-439.

Wagner, R.; Roeschlein, R. und Waschek, G. (2009): Projekt, Projektmanagement, Projektarten und PM-Prozesse. In: Gessler, M. (Hrsg.): Kompetenzbasiertes Projektmanagement (PM3), Handbuch für die Projektarbeit, Qualifizierung und Zertifizierung auf Basis der IPMA Competence Baseline Version 3.0 (E-Book). 1. Aufl. Nürnberg: GPM Deutsche Gesellschaft für Projektmanagement e.V., S. 29-52.

Walls, J.; Widmeyer, G. und El Sawy, O. (1992): Building an Information System Design Theory for Vigilant EIS. In: Information Systems Research, 3(1), S. 36-59.

Walter, S.; Müller, D. und Walter, A. (2010): Dysfunktionen in F&E-Koopetitionen: Präventivmaßnahmen und Kooperationserfolg. In: Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung (ZfbF), 62(2), S. 134-159.

Wamsteker, S. (2012): IT-Technologieberatung. In: Hies, M. (Hrsg.): Perspektive Unternehmensberatung. Das Expertenbuch zum Einstieg (S. 22-24). München.

Webster, J. und Watson, R. T. (2002): Analyzing the Past to Prepare for the Future: Writing a Literature Review. In: MIS Quarterly, 26(2), S. 13-23.

Weiber, R. (2002): Handbuch Electronic Commerce: Informationstechnologien - Electronic Commerce - Geschäftsprozesse. 2. Aufl. Wiesbaden: Gabler Verlag.

Weiershäuser, S. (1996): Mitarbeiterverhalten im Beratungsprozeß. Eine ökonoische Betrachtung. Wiesbaden: Gabler Verlag und Deutscher Universitäts-Verlag.

Wernerfelt, B. (1984): A resource-based view of the firm. In: Strategic Management Journal, 5(2), S. 171-180.

Whyte, W. F.; Greenwood, D. J. und Lazes P. (1991): Participatory Action Research - Through Practice to Science in Social Research. In: Whyte, W. F. (Hrsg.): Participatory Action Research. Newbury Park, Kalifornien: Sage Publications, S. 19-55.

Wilde, T. und Hess T. (2007): Forschungsmethoden der Wirtschaftsinformatik - Eine empirische Untersuchung. In: Wirtschaftsinformatik, 49(4), S. 280-287.

Williamson, O. E. (1975): Markets and Hierarchies: Analysis and antitrust implication: A study of the economics of internal organization. New York: The Free Press.

Williamson, O. E. (1985): The Economic Institution of Capitalism: Firms, Markets, Relational Contracting. New York: The Free Press.

Williamson, O. E. (1990): Chester Barnard and the Incipient Science of Organization. In: Oliver, E. W. (Hrsg.): Organization Theory: From Chester Barnard to the Present and Beyond. New York: Oxford University Press, S. 172-206.

Williamson, O. E. (1991): Comparative Economic Organization: The Analysis of Discrete Structural Alternatives. In: Administrative Science Quarterly, 36(2), S. 269-96.

WKWI (1994): Wissenschaftliche Kommission Wirtschaftsinformatik, Profil der Wirtschaftsinformatik. In: Wirtschaftsinformatik, 36(1), S. 80-81.

Wolff, B. (1995): Organisation durch Verträge. Koordination und Motivation in Unternehmen. München: Gabler Verlag.

Wrona, T. (2005): Die Fallstudienanalyse als wissenschaftliche Forschungsmethode. ESCP-EAP Working Paper (10). Berlin.

Wrona, T. (2006): Fortschritts- und Gütekriterien im Rahmen qualitativer Sozialforschung. In: Zelewski, S. und Akca, N. (Hrsg.): Fortschritt in den Wirtschaftswissenschaften. Wissenschaftstheoretische Grundlagen und exemplarische Anwendungen. Wiesbaden: Deutscher Universitäts-Verlag, S. 189-216.

Yang, C. H. und Kuo, N. F. (2008): Trade-related influences, foreign intellectual property rights and outbound international patenting. In: Research Policy, 37(3), S. 446-459.

Yapp, P. (2003): Information security. In: Jolly, A. (Hrsg.): Managing business risk. London: Kogan Page, S. 173-177.

Yeung, J. H. Y.; Selen, W.; Zhang, M. und Huo, B. (2009): The effects of trust and coercive power on supplier integration. In: International Journal of Production Economics, 120(1), S. 66-78.

Zahn, E., Foschiani, S. und Tilebein, M. (2000): Nachhaltige Wettbewerbsvorteile durch Wissensmanagement. In: Krallmann, H. (Hrsg.): Wettbewerbsvorteile durch Wissensmanagement - Methodik und Anwendungen des Knowledge Management. Stuttgart: Schäfer-Poeschel Verlag, S. 239-270.

Zahra, S. A. und George, G. (2002): Absorptive capacity: A review, reconceptualization, and extension. In: Academy of Management Review, 27(2), S. 185-203.

Zarnekow, R. (2007): Produktionsmanagement von IT-Dienstleistungen. Grundlagen, Aufgaben und Prozesse. Berlin: Springer Verlag.

Zhao, M. (2006): Conducting R&D in Countries with Weak Intellectual Property Rights Protection. In: Management Science, 52(8), S. 1185-1199.

Zucker, L. (1986): Production of trust: institutional sources of economic structure, 1840-1920. In: Research in Organizational Behaviour, 8, S. 53-111.

8 Anhang

8.1 Experten-Interviewleitfaden

Einleitung

Guten Tag, Herr/Frau ….

Bevor wir mit dem Interview beginnen, möchte ich mich kurz bei Ihnen vorstellen. Mein Name ist André Karg. Am [Name des Lehrstuhls] bearbeite ich das Thema „Strategischer Wissensschutz bei nationalen und internationalen IT-Projekten mit externen Dienstleistern“. Die intendierte Promotion entwickelt ein Wissensschutz-Referenzmodell für den Schutz des wertvollen organisationalen Wissens einer IT-Beratung bei IT-Projekten mit externen nationalen und internationalen Dienstleistern (Outsourcing).
Das Interview ist für ca. 90 Minuten geplant und in der folgenden Weise untergliedert. Zuerst werde ich das Thema vorstellen und Ihnen allgemeine Fragen stellen und anschließend das literaturbasierte Wissensschutz-Modell entwickeln. Im zweiten Teil geht es um die praktische Anwendung des entwickelten Referenzmodells. Hier soll besprochen werden, ob die identifizierten Akteure in den Funktionen befähigt werden, das Wissensschutz-Referenzmodell anzuwenden. Dazu gehört ebenso die Diskussion zu den aus der Wissenschaft transkribierten Kategorien.

Wenn Sie einverstanden sind, würde ich gerne das Interview mit einem Aufnahmegerät protokollieren, um den genauen Gesprächsverlauf nachvollziehen zu können, damit ich später nicht nur auf mein Gedächtnis angewiesen bin. Das aufgenommene Protokoll wird nach den geltenden Datenschutzgesetzen behandelt. Damit werden keine personenbezogenen Daten weitergegeben oder veröffentlicht. Außerdem werden alle Angaben, aus denen Rückschlüsse auf Ihre Person gezogen werden können, bei der Transkription des Interviews anonymisiert. [Einverständniserklärung zur Unterschrift übergeben]
Ich möchte Sie bitten aus Ihrer persönlichen Sicht und aus Ihrer beruflichen Erfahrung die Interviewfragen zu beantworten.

Themenvorstellung sowie -abgrenzung (offene Eingangsfragen)

Stellen Sie sich vor, dass eine IT-Beratung mit 23 Dienstleistern in IT-Projekten zusammenarbeitet. Diese Dienstleister sind zum Beispiel in vier unterschiedliche Aufgabencluster eingeordnet, um die Dienstleisterauswahl für die IT-Projekte nach Spezialgebieten vorzuselektieren. Jedes der IT-Projekte der IT-Beratung lässt sich mindestens einem Cluster zuordnen.

Sie stehen vor der Herausforderung, dass Sie Ihr sehr wertvolles organisationales Wissen schützen müssen, um Ihre Wettbewerbsfähigkeit zu bewahren.

Für diese Arbeit wurden die folgenden Forschungsfragen aufgestellt:

Leitfrage: *Wie muss ein Risikoinformationssystem einer IT-Beratung zur Unterstützung des Wissensschutzes bei der ISE mit externen IT-Dienstleistern gestaltet sein?*

a. *Wie identifiziert eine IT-Beratung die **Unternehmensgrenze** beim Wissen-Teilen und -Zurückhalten, um den Wissensschutz in der ISE mit externen Dienstleistern sicherzustellen?*

b. *Mit welchen **externen Dienstleistern** kann eine IT-Beratung in der ISE **zusammenarbeiten,** ohne ihre **Wettbewerbsfähigkeit** oder die ihrer Auftraggeber zu riskieren?*

c. *Welche **Funktionen** werden den **Akteuren** in einer IT-Beratung beim Wissensschutz **zugeordnet**?*

Beispielszenario neues Projekt:

Stellen Sie sich vor, dass Sie ein IT-Projekt mit den folgenden Eigenschaften verantworten:

- sehr **innovativ** und **strategisch** wichtig für den Auftraggeber und für Ihre Kundenbeziehung
- die Wettbewerbsfähigkeit von **Ihrem Auftraggeber** ist von dem IT-Projekt abhängig
- die Wettbewerbsfähigkeit **Ihrer IT-Beratung** ist von dem IT-Projekt abhängig

In diesem IT-Projekt arbeiten Sie mit mehreren externen Mitarbeitern eines Dienstleisters zusammen. Der externe Dienstleister besitzt folgende Eigenschaften:

- die Organisationsgröße ist **größer** als die eigene IT-Beratung
- der Dienstleister agiert **international** und hat Büros in 50 Ländern
- seine Auftraggeber kommen aus **verschiedenen Branchen** (marktübergreifend)
- er ist **innovativ**, **lernbereit** und **lernfähig**

Eingangsfrage

Für das gemeinsame Verständnis zum Wissensschutz wurde aus der Literatur eine Definition formuliert:

Wissensschutz schützt wertvolles organisationales Wissen einer Organisation um Wissensvorsprung zu sichern und setzt Schutzmethoden (formale / informale Mechanismen) nach dem bewerteten Präventionsgrad vom abgehenden Wissenstransfers zu anderen Organisationen ein. Um die Wettbewerbsfähigkeit zu erhalten, werden organisationale Wissensflüsse zur Prävention von ungewollter Wissensdiffusion geprüft. Zu definieren ist, welches Wissen die „Grenze" der Organisation verlassen darf und welches Wissen in der Organisation verbleiben soll.

1. Was verstehen Sie unter Wissensschutz in IT-Projekten mit externen Dienstleistern? (basierend auf dieser Definition)

Begriffsabgrenzung

Die Daten- und Informationssicherheit ist sehr strukturiert und unterliegt strengen Kontrollen und Überprüfungen in den Organisationen. Organisationen nehmen umfangreiche Aktivitäten auf sich, um ihre Daten zu schützen und investieren Kapital und Ressourcen zur Implementierung des organisationalen Rahmens, zum Beispiel Zertifizierung nach Control Objectives for Information and Related Technology (COBIT)[987] oder Information Technology Infrastructure Library (ITIL)[988].

2. Definitionen / Begriffsabgrenzung: Wie würden Sie die folgenden Begriffe voneinander abgrenzen?
    a. Wissensschutz und Datenschutz
    b. Wissensschutz und Informationsschutz

Persönliche Berufspraxis

3. Gibt es kritische Ereignisse mit externen Dienstleistern aus ihrer Berufspraxis in Bezug auf den Wissensschutz?
    a. Wenn ja, wie haben sie sich in dieser konkreten Situation verhalten?
    b. Konnte die Situation erfolgreich gelöst werden?

[987] Control Objectives for Information and Related Technology ist ein international anerkanntes Framework zur Information Technology (IT)-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives.
[988] IT Infrastructure Library ist eine Sammlung von Best Practices in einer Reihe von Publikationen zur Umsetzung eines IT-Service-Managements und gilt inzwischen als internationaler De-facto-Standard im Bereich IT-Geschäftsprozesse.

Modellvorstellung - Grundlagen

Bei der Modellvorstellung wird jeweils zuerst das Template gezeigt und anschließend ein ausgefülltes durchgängiges Beispiel, damit der Praxisbezug verdeutlicht wird.

Funktionen	Akteure
Strategische Planung	Management mit Strategiemanagement
Projektkategorisierung	Projektmanager mit Management
Wissenskategorisierung	Management mit Strategie-, Kundenmanagement
Dienstleisterkategorisierung	IT-Sourcing Management mit Ressourcenmanagement
Risikobewertung	Projektmanager mit Management

Tabelle 48: Funktionen und Akteure beim Wissensschutz

Eine zentrale Rolle für das Modell sind das Technologiewissen und das Fachwissen der IT-Beratung. Nach der Forschungsliteratur ist das wertvollste Vermögen der IT-Beratung das Technologiewissen und das Fachwissen. Diese Kernbegriffe werden folgend definiert:

> **Technologiewissen** befähigt die Organisation die Informationssysteme auf einer technologischen Basis zu implementieren.
>
> **Fachwissen** ist das aufgebaute Humankapital in Form von dem Geschäftsprozesswissen in der Auftraggeber-Branche.

Funktion 1: Strategische Planung

Akteur: Management mit Strategiemanagement

- Die IT-Strategie ist definiert.
- Die Outsourcing-/Offshoring-Strategie ist definiert.
- Die Umfeldanalyse zur IT-Beratung (Auftraggeber, Dienstleister, Mitbewerber) liegt vor:
    - Auftraggebersteckbrief (Branche)
        - IT-Strategie für das Kundensegment
    - Dienstleistersteckbrief für jeden externen Dienstleister (Projekteinsätze (Historie), Dienstleistererfahrung, Vertrauen, mit welchen Mitbewerbern agiert der Dienstleister, Bereitschaft für Partnerschaftsmodelle (Technologieausbildung), wirtschaftliche Lage, Referenzkunden, …)
        - Dienstleisterstrategie

Funktion 2: Projektkategorisierung

Akteur: Projektmanager mit Management

- Für die Ist-Projekte müssen IT-Projektsteckbriefe (inkl. Projektkategorisierung) erstellt werden. In dem Projektsteckbrief muss die Zuordnung von dem Fachwissen, dem Technologiewissen, den externen eingesetzten Dienstleister(n) und die Projektsituation zum Projekt erfasst werden.

Projektsteckbrief für Ist-Projekte

Projektart
- Neuentwicklungs- / Wartungs- / Weiterentwicklungsprojekt
Fachwissen
- Geschäftsprozesswissen in der Branche
Technologiewissen
- Technologiewissen der IT-Beratung
externe Dienstleister
- eingesetzte externe Dienstleister
Projektsituation
- Umfeldanalyse für Risikobewertung

Abbildung 44: Projektsteckbrief für Ist-Projekte

- Folgend abgebildet ist die Projektkategorisierung, um die Fachwissens- und die Technologiewissenskombinationen zu bestimmen:

Projektkategorisierung nach Technologie-/Fachwissen im Projekt

Technologiewissen / Fachwissen	Technologie-wissen 1	Technologie-wissen 2	Technologie-wissen n
Fachwissen 1			
Fachwissen 2			
Fachwissen n			

Abbildung 45: Projektkategorisierung nach Technologie- / Fachwissen im IT-Projekt

- Für jedes **neue** Projekt muss ebenso ein Projektsteckbrief mit den genannten Kategorien ausgefüllt werden. Jedoch wird das Feld „externe Dienstleister“ erst nach der Rücksprache mit dem Ressourcenmanagement und IT-Sourcing Management befüllt (Wissenskategorisierung, Dienstleisterkategorisierung).

Beispiel 1

Projektsteckbrief: Projekt **Vertriebssystem**

Projektart
- Weiterentwicklungsprojekt
Fachwissen
- Endkundenticketvertrieb in Mobilitätsbranche - Geschäftskundenvertrieb in Mobilitätsbranche
Technologiewissen
- Big Data - Mobile Applikationen
externe Dienstleister
- Meyer (national)
Projektsituation
- Geschäftsbeziehung mit Zeitkritikalität - Hohe Anforderungen an Qualität

Abbildung 46: Projektsteckbrief für Beispiel 1

Beispiel 2

Projektsteckbrief: Projekt **Logistiksystem**

Projektart
- Neuentwicklungsprojekt
Fachwissen
- Geschäftskundenvertrieb in Mobilitätsbranche - Abrechnung in Logistikbranche - Lagerprozesse in Logistikbranche
Technologiewissen
- Mobile Applikationen - Cloud Technologie - Software as a Service (SaaS)
externe Dienstleister
- Schmidt (international)
Projektsituation
- Drohende Vertragsstrafen bei nicht Verfügbarkeit - Projekterfolg vom externen Dienstleisterbeitrag abhängig

Abbildung 47: Projektsteckbrief für Beispiel 2

Projekt **Vertriebssystem** Projektkategorisierung nach Technologie-/Fachwissen

Technologiewissen / Fachwissen	Big Data	Mobile Applikation
Endkundenticketvertrieb in Mobilitätsbranche	x	x
Geschäftskundenvertrieb in Mobilitätsbranche	-	x

Abbildung 48: Projektkategorisierung für Beispiel 1

Projekt **Logistiksystem** Projektkategorisierung nach Technologie-/Fachwissen

Technologiewissen / Fachwissen	Mobile Applikation	Cloud Technologie	Software as a Service
Geschäftskundenvertrieb in Mobilitätsbranche	x	-	-
Abrechnung in Logistikbranche	-	x	x
Lagerprozesse in Logistikbranche	x	x	-

Abbildung 49: Projektkategorisierung für Beispiel 2

Funktion 3: Wissenskategorisierung

Akteur: Management mit Strategie-, Kundenmanagement

Um das wertvolle organisationale Wissen zu identifizieren und damit die Grenze zu bestimmen, welches Wissen geteilt werden kann und welches Wissen zurückgehalten werden sollte, wurden aus der Wissenschaftsliteratur zum Wissensschutz die folgenden Bewertungskategorien transkribiert.

- **Strategie** bewertet die strategische Bedeutung (Relevanz) des Fachwissens / des Technologiewissens und deren Auswirkungen auf die Unternehmensstrategie.
- **Kundennutzen** bewertet den überproportionalen Wert zum Kundenbeitrag des Fachwissens / des Technologiewissens. Das sind z.B. die Organisationsfähigkeiten, die einen wesentlichen Kundennutzen liefern. In die Bewertung vom Kundennutzen ist ebenso der Endanwendernutzen miteinzubeziehen.
- **Mitbewerberabgrenzung** bewertet die Wettbewerbsfähigkeit des Fachwissens / des Technologiewissens. Um als sehr wertvolles organisationales Fachwissen / Technologiewissen bewertet zu werden, muss das Wissensgebiet nicht unbedingt einmalig sein.
- **Übertragbarkeit** bewertet die Anwendbarkeit des Fachwissens / des Technologiewissens auf neue Informationssysteme, Kunden und Märkte. Voraussetzung für die Übertragbarkeit sind Mitarbeiter die befähigt sind, dass angeeignete Fachwissen / Technologiewissen anzuwenden.

Kategorisierungsmatrix des Fachwissens / Technologiewissens

			Fachwissen / Technologiewissen der IT-Beratung		
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Fachwissen 1 / Technologie-wissen 1	Fachwissen 2 / Technologie-wissen 2	Fachwissen n / Technologie-wissen n
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,xx	Strategie			
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,xx	Kundennutzen			
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,xx	Mitbewerberabgrenzung			
sehr hoch = 5 hoch = 3 gering = 1	0,xx	Übertragbarkeit			
A sehr wertvoll 4 bis 5 B wertvoll 2,01 bis 3,99 C weniger wertvoll 1 bis 2	-	Wissenskategorisierung			

Abbildung 50: Kategorisierungsmatrix des Fachwissens / Technologiewissens Template

Bewertung des Technologiewissens aus Beispiel 1 und 2

Beispiel Kategorisierungsmatrix des Technologiewissens

			Technologiewissen der IT-Beratung			
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Big Data	Mobile Applikation	Cloud Technologie	Software as a Service
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,25	Strategie	5	4	5	4
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,4	Kundennutzen	3	5	4	3
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,15	Mitbewerberabgrenzung	3	4	4	3
sehr hoch = 5 hoch = 3 gering = 1	0,2	Übertragbarkeit	4	3	3	4
A sehr wertvoll 4 bis 5 B wertvoll 2,01 bis 3,99 C weniger wertvoll 1 bis 2	1,00	Wissenskategorisierung	3,7	4,2	4,05	3,45
			B	A	A	B

Abbildung 51: Kategorisierungsmatrix des Technologiewissens für Beispiel 1 und 2

Weitere Technologiewissensgebiete können sein, Java, Internet of Things, Predictive Analytics, Predictive Maintnance, SaaS und XaaS.

Bewertung des Fachwissens aus Beispiel 1 und 2

Beispiel Kategorisierungsmatrix des Fachwissens

			Fachwissen der IT-Beratung			
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Endkunden-ticketvertrieb in Mobilitäts-branche	Geschäftskunden-vertrieb in Mobilitäts-branche	Abrechnung in Logistikbranche	Lagerprozesse in Logistikbranche
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,25	Strategie	4	4	4	3
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,4	Kundennutzen	5	4	4	5
sehr wichtig = 5 wichtig = 3 weniger wichtig = 1	0,15	Mitbewerberabgrenzung	3	3	3	3
sehr hoch = 5 hoch = 3 gering = 1	0,2	Übertragbarkeit	3	3	4	4
A sehr wertvoll 4 bis 5 B wertvoll 2,01 bis 3,99 C weniger wertvoll 1 bis 2	1,00	Wissenskategorisierung	4,05	3,65	3,85	4
			A	B	B	A

Abbildung 52: Kategorisierungsmatrix des Fachwissens für Beispiel 1 und 2

Weitere mögliche Fachwissensgebiete können sein, Finanzsysteme in der Logistikbranche, Sicherheitsmanagement in der Mobilitätsbranche, Fuhrparkmanagement in der Automobilbranche, Ausschreibungsmanagement in der Logistikbranche, Regelwerksmanagement in der Mobilitätsbranche und Vertragsmanagement im Baumanagement.

Die kombinierte Bewertung vom Fach- und Technologiewissen mit Projektbezug aus:

Beispiel 1:

Projekt **Vertriebssystem** Projektkategorisierung nach Technologie-/Fachwissen

Technologiewissen / Fachwissen	Big Data	Mobile Applikation
Endkundenticketvertrieb in Mobilitätsbranche	x	x
Geschäftskundenvertrieb in Mobilitätsbranche	-	x

Abbildung 53: Projektkategorisierung für Beispiel 1

Beispiel 2:

Projekt **Logistiksystem** Projektkategorisierung nach Technologie-/Fachwissen

Technologiewissen / Fachwissen	Mobile Applikation	Cloud Technologie	Software as a Service
Geschäftskundenvertrieb in Mobilitätsbranche	x	-	-
Abrechnung in Logistikbranche	-	x	x
Lagerprozesse in Logistikbranche	x	x	-

Abbildung 54: Projektkategorisierung für Beispiel 2

Beispiel Wissenskategorisierungsmatrix der IT-Beratung mit Projektbezug

Bewertungsskala		Bewertungskategorie	Bewertung			
		Wissenskategorisierung	3,7	4,2	4,05	3,45
	A sehr wertvoll 4 bis 5 B wertvoll 2,01 bis 3,99 C weniger wertvoll 1 bis 2	Technologiewissen / Fachwissen	Big Data	Mobile Applikation	Cloud Technologie	Software as a Service
Bewertung	4,05	Endkundenticketvertrieb in Mobilitätsbranche	AB - 1 Vertriebssystem	AA - 1 Vertriebssystem	-	-
	3,65	Geschäftskundenvertrieb in der Mobilitätsbranche	-	BA - 2 Vertriebssystem, Logistiksystem	-	-
	3,85	Abrechnung in Logistikbranche	-	-	BA - 1 Logistiksystem	BB - 1 Logistiksystem
	4	Lagerprozesse in Logistikbranche	-	AA - 1 Logistiksystem	AA - 1 Logistiksystem	-

Abbildung 55: Bsp. Wissenskategorisierung der IT-Beratung mit Projektbezug

Legende:

AA - #	Kombination aus sehr wertvollen organisationalem Wissen
AB/BA - #	Kombination aus sehr wertvollen und wertvollem organisationalem Wissen
AC/CA - #	Kombination aus sehr wertvollen und weniger wertvollen organisationalem Wissen
BB - #	Kombination aus wertvollen organisationalem Wissen
BC/CB - #	Kombination aus wertvollen und weniger wertvollen organisationalem Wissen
CC - #	Kombination aus weniger wertvollen organisationalem Wissen
#	Anzahl der IT Projekte mit dieser Fachwissens- und Technologiewissenskombination
	Tabellenausschnitt zur Übertragung von Projektkategorisierung zu Wissenskategorisierung ist farblich gekennzeichnet.

Funktion 4: Dienstleisterkategorisierung

Akteur: IT-Sourcing Management mit Ressourcenmanagement

Die Dienstleisterkategorisierung ist in zwei Bestandteile unterteilt. Zuerst werden alle Dienstleister der IT-Beratung nach Dienstleister-Gefahrenpotential bewertet. Im zweiten Schritt werden die Kenntnisse und die Fähigkeiten vom externen Dienstleister mit Bezug zum Fachwissen und Technologiewissen der IT-Beratung bewertet.

Die folgenden Bewertungskategorien vom externen Dienstleister dienen dazu den Dienstleister einem Gefahrenpotential zuzuordnen. Diese Einordnung soll bei sehr wertvollen betroffenem Wissen eine Handlungspriorisierung verdeutlichen.

Bewertungskategorien vom Dienstleister-Gefahrenpotential:

Dienstleistergröße erfasst die Anzahl der Mitarbeiter im Inland und Ausland.

Dienstleisteraktivität erfasst die Anzahl der Länder in denen der Dienstleister aktiv ist, damit kann die Anzahl der Märkte identifiziert werden.

Dienstleisterart erfasst die Zuordnung des Dienstleisters in dem Dienstleistungsbereich.

Dienstleisterbranche (Marktumfang) dokumentiert die Branchen-Aktivitäten vom Dienstleister.

Lernbereitschaft / Lernfähigkeit ergibt sich aus der Fähigkeit neues Wissen aufzunehmen und dieses für die eigene Organisation zu nutzen.

Innovationsfähigkeit ergibt sich aus dem komplexen Zusammenspiel der Organisation und seiner hervorgebrachten Innovationen.

Absorptive Dienstleisterkapazität kumuliert sich aus allen zuvor definierten Bewertungskategorien vom Dienstleister.

Dienstleistererfahrung aus Projekten ergibt sich aus dem aufgebauten Vertrauen, der Lieferqualität des Dienstleisters und den erfolgreich abgeschlossenen Projekten mit dem Dienstleister.

Dienstleister-Gefahrenpotential ergibt sich aus der kumulierten Bewertung von der absorptiven Dienstleisterkapazität und der Dienstleistererfahrung aus Projekten.

Beispiel Dienstleisterkategorisierung nach Gefahrenpotential

Dienstleister-bewertungskategorien	Dienstleistergröße	Dienstleister-aktivitäten	Dienstleisterart	Dienstleister-branche Marktumfang	Lernbereit-schaft / Lernfähig-keit	Innovations-fähigkeit	absorptive Dienstleister-kapzität	Dienstleister-erfahrung aus Projekten	Dienstleister-Gefahren-potential
Bewertungsskala	Anzahl der Mitarbeiter im Inland / Anzahl der Mitarbeiter im Ausland	Anzahl in aktiven Ländern	I = Management Beratung II = IT-Beratung III = Freelancer	I = ab 5 Branchen II = 3-4 Branchen III = 1-2 Branchen	I = hoch II = mittel III = gering	I = hoch II = mittel III = gering	I = hoch II = mittel III = gering	I = hoch II = mittel III = gering	I = hoch II = mittel III = gering
Meyer (national)	500 / 0	1	II	II	II	II	II	II	**II**
Schmidt (international)	10000 / 190000	50	I	I	I	I	I	I	**I**
Partner xy (national)	200 / 0	1	III	III	III	III	III	II	**III**

Abbildung 56: Dienstleisterkategorisierung nach Gefahrenpotential für Beispiel 1 und 2

Nach der Bestimmung der Dienstleister-Gefahrenpotential erfolgt die Bewertung der Kenntnisse und der Fähigkeiten des Dienstleisters nach dem identifizierten Fachwissen und Technologiewissen der IT-Beratung.

Bewertungskategorien vom Dienstleister (Wissenskategorisierung):

Interne Expertise: Auf der Grundlage der Informationen des IT-Sourcing Managements, aus den bestehenden kategorisierten Projekten und den bereits eingenommenen Projektrollen des Dienstleisters kann die interne Bewertung in Bezug auf die Fach- und Technologiewissensgebiete erfolgen.

Externe Marktstellung: Auf der Grundlage der externen Marktinformationen über den Dienstleister kann die externe Bewertung in Bezug auf das Fach- und Technologiewissensgebiet erfolgen.

Template

Kategorisierungsmatrix nach Dienstleister Fachwissen/Technologiewissen

			Fachwissen/Technologiewissen der IT-Beratung		
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Fachwissen 1 / Technologie-wissen 1	Fachwissen 1 / Technologie-wissen 1	Fachwissen n / Technologie-wissen n
führende Expertise = 5 durchschnittliche Expertise = 3 geringe Expertise = 1 keine Expertise = -	0,xx	interne Expertise			
Marktführer = 5 Marktdurchschnitt = 3 Marktbeteiligte = 1 nicht Aktiv = - nicht bekannt = ?	0,xx	externe Marktstellung			
a sehr hoch 4 bis 5 b hoch 2,01 bis 3,99 c gering 1 bis 2	1,00	Dienstleisterkategorisierung			

Abbildung 57: Kategorisierungsmatrix nach Dienstleister Fachwissen/Technologiewissen Template

Bewertung vom Dienstleister Meyer (national) Fach- und Technologiewissen

Dienstleister Meyer (national) Kategorisierungsmatrix nach Fachwissen

			Fachwissen der IT-Beratung			
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Endkunden-ticketvertrieb in Mobilitäts-branche	Geschäftskunden-vertrieb in Mobilitäts-branche	Abrechnung in Logistikbranche	Lagerprozesse in Logistikbranche
führende Expertise = 5 durchschnittliche Expertise = 3 geringe Expertise = 1 keine Expertise = -	0,5	interne Expertise	4	5	3	-
Marktführer = 5 Marktdurchschnitt = 3 Marktbeteiligte = 1 nicht Aktiv = - nicht bekannt = ?	0,5	externe Marktstellung	3	3	1	-
a sehr hoch 4 bis 5 b hoch 2,01 bis 3,99 c gering 1 bis 2	1,00	Dienstleisterkategorisierung	3,5	4	2	-
			b	b	c	-

Abbildung 58: Kategorisierungsmatrix Fachwissen für Dienstleister Meyer

Dienstleister Meyer (national) Kategorisierungsmatrix nach Technologiewissen

			Technologiewissen der IT-Beratung			
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Big Data	Mobile Applikation	Cloud Technologie	Software as a Service
führende Expertise = 5 durchschnittliche Expertise = 3 geringe Expertise = 1 keine Expertise = -	0,5	interne Expertise	4	4	-	-
Marktführer = 5 Marktdurchschnitt = 3 Marktbeteiligte = 1 nicht Aktiv = - nicht bekannt = ?	0,5	externe Marktstellung	4	2	-	-
a sehr hoch 4 bis 5 b hoch 2,01 bis 3,99 c gering 1 bis 2	1,00	Dienstleisterkategorisierung	4	3	-	-
			a	b	-	-

Abbildung 59: Kategorisierungsmatrix Technologiewissen für Dienstleister Meyer

Bewertung vom Dienstleister Schmidt (international) Fach- und Technologiewissen

Dienstleister Schmidt (international) Kategorisierungsmatrix nach Fachwissen

			Fachwissen der IT-Beratung			
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Endkunden-ticketvertrieb in Mobilitäts-branche	Geschäftskunden-vertrieb in Mobilitäts-branche	Abrechnung in Logistikbranche	Lagerprozesse in Logistikbranche
führende Expertise = 5 durchschnittliche Expertise = 3 geringe Expertise = 1 keine Expertise = -	0,5	interne Expertise	-	5	5	4
Marktführer = 5 Marktdurchschnitt = 3 Marktbeteiligte = 1 nicht Aktiv = - nicht bekannt = ?	0,5	externe Marktstellung	-	4	3	3
a sehr hoch 4 bis 5 b hoch 2,01 bis 3,99 c gering 1 bis 2	1,00	Dienstleisterkategorisierung	-	4,5	4	3,5
			-	a	a	b

Abbildung 60: Kategorisierungsmatrix Fachwissen für Dienstleister Schmidt

Dienstleister Schmidt (international) Kategorisierungsmatrix nach Technologiewissen

			Technologiewissen der IT-Beratung			
Bewertungsskala	Kategorie-gewichtung	Bewertungskategorie	Big Data	Mobile Applikation	Cloud Technologie	Software as a Service
führende Expertise = 5 durchschnittliche Expertise = 3 geringe Expertise = 1 keine Expertise = -	0,5	interne Expertise	-	3	3	3
Marktführer = 5 Marktdurchschnitt = 3 Marktbeteiligte = 1 nicht Aktiv = - nicht bekannt = ?	0,5	externe Marktstellung	4	1	5	4
a sehr hoch 4 bis 5 b hoch 2,01 bis 3,99 c gering 1 bis 2	1,00	Dienstleisterkategorisierung	4	2	4	3,5
			a	c	a	b

Abbildung 61: Kategorisierungsmatrix Technologiewissen für Dienstleister Schmidt

Die Dienstleisterkategorisierung dient zur Feststellung der Kenntnisse und der Fähigkeiten vom externen Dienstleister. In dieser Matrix wird ersichtlich, wie die Wissenskategorisierung mit der Projektkategorisierung und der Dienstleisterkategorisierung kombiniert wird.

Dienstleisterkategorisierung für Template

Dienstleisterkategorisierung zur Feststellung der Technologie-/Fachwissenüberlappung

A sehr wertvoll 4 bis 5 B wertvoll 2,01 bis 3,99 C weniger wertvoll 1 bis 2	Dienstleisterkategorisierung	*,**	*,**	*,**
	Technologiewissen / Fachwissen	Technologiewissen 1	Technologiewissen 2	Technologiewissen 3
*,**	Fachwissen 1	aa, Projektname (Rollen)	ab	ac
*,**	Fachwissen 2	ba, Projektname (Rollen)	bb, Projektname (Rollen)	bc
*,**	Fachwissen 4	ca, Projektname (Rollen)	cb	cc, Projektname (Rollen)

Abbildung 62: Dienstleisterkategorisierung Template

Legende:

aa	Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination sehr hoch
ab/ba	Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination sehr hoch und hoch
ac/ca	Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination sehr hoch und gering
bb	Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination hoch
bc/cb	Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination hoch und gering
cc	Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination gering

Dienstleisterkategorisierung für Beispiel 1

Dienstleister: Meyer (national) Dienstleisterkategorisierung zur Feststellung der Technologie-/Fachwissenüberlappung (im Ist-Zustand und später Soll-Zustandsabbildung)

a Marktleader 4 <= 5 b Marktdurchschnitt 2 < 4 c Marktbeteiligte 1 <= 2	Dienstleisterkategorisierung	4,5	3,5	-	?
	Technologiewissen / Fachwissen	Big Data	Mobile Applikation	Cloud Technologie	Software as a Service
3	Endkundenticketvertrieb in Mobilitätsbranche	ba Vertriebssystem (Projektleitung)	bb Vertriebssystem (Projektleitung, SW-Architekt)	b-	b-
3	Geschäftskundenvertrieb in der Mobilitätsbranche	ba	bb Vertriebssystem (Projektleitung, SW-Architekt)	b-	b-
1,5	Abrechnung in Logistikbranche	ca	cb	c-	c-
-	Lagerprozesse in Logistikbranche	-a	-b	--	--

Abbildung 63: Dienstleisterkategorisierung Beispiel 1

Dienstleisterkategorisierung für Beispiel 2

Dienstleister Schmidt (international) Dienstleisterkategorisierung zur Feststellung der Technologie-/Fachwissenüberlappung (im Ist-Zustand und später Soll-Zustandsabbildung)

a Marktleader 4 <= 5 b Marktdurchschnitt 2 < 4 c Marktbeteiligte 1 <= 2	Dienstleisterkategorisierung Technologiewissen / Fachwissen	4,5 Big Data	1,5 Mobile Applikation	4,5 Cloud Technologie	3,5 Software as a Service
-	Endkundenticketvertrieb in Mobilitätsbranche	-a	-c	-a	-b
4,5	Geschäftskundenvertrieb in der Mobilitätsbranche	aa	ac Logisitiksystem (Beratung, Test)	aa	ab
4,5	Abrechnung in Logistikbranche	aa	ac	aa Logisitiksystem (Entwicklung)	ab Logisitiksystem (Test)
3	Lagerprozesse in Logistikbranche	ba	bc Logisitiksystem (Beratung, Test)	ba Logisitiksystem (Entwicklung)	bb

Abbildung 64: Dienstleisterkategorisierung Beispiel 2

Für **neue Projekte** kann das IT-Sourcing Management Ressourcen zu der Fachwissens- und Technologiewissenskombination empfehlen.

Funktion 5: Risikobewertung

Akteur: Projektmanager mit Management

Beispiel 1

Projektsteckbrief: Projekt **Vertriebssystem**

Projektart
- Weiterentwicklungsprojekt
Fachwissen
- Endkundenticketvertrieb in Mobilitätsbranche - Geschäftskundenvertrieb in Mobilitätsbranche
Technologiewissen
- Big Data - Mobile Applikationen
externe Dienstleister
- Meyer (national)
Projektsituation
- Geschäftsbeziehung mit Zeitkritikalität - Hohe Anforderungen an Qualität

Abbildung 65: Projektsteckbrief für Beispiel 1

Die Beispiel Ergebnisse der Projekt-, der Wissens- und der Dienstleisterkategorisierung sind in der folgenden Tabelle zusammenfassend für die Risikobewertung dargestellt.

Projekt **Vertriebssystem** Projektkategorisierung nach Technologie-/Fachwissen für Dienstleister Meyer (national)

Technologiewissen / Fachwissen	Big Data	Mobile Applikation
Endkundenticketvertrieb in Mobilitätsbranche	AB - 1 - ba - II Projektleitung	AA - 1 - bb - II Projektleitung, SW-Architekt
Geschäftskundenvertrieb in Mobilitätsbranche	-	BA - 2 - bb - II Projektleitung, SW-Architekt

Abbildung 66: Risikobewertung Vertriebssystem

Beispiel 2

Projektsteckbrief: Projekt **Logistiksystem**

Projektart
- Neuentwicklungsprojekt
Fachwissen
- Geschäftskundenvertrieb in Mobilitätsbranche - Abrechnung in Logistikbranche - Lagerprozesse in Logistikbranche
Technologiewissen
- Mobile Applikationen - Cloud Technologie - Software as a Service (SaaS)
externe Dienstleister
- Schmidt (international)
Projektsituation
- Drohende Vertragsstrafen bei nicht Verfügbarkeit - Projekterfolg vom externen Dienstleisterbeitrag abhängig

Abbildung 67: Projektsteckbrief für Beispiel 2

Die Beispiel Ergebnisse der Projekt-, der Wissens- und der Dienstleisterkategorisierung sind in der folgenden Tabelle zusammenfassend für die Risikobewertung dargestellt.

Projekt **Logistiksystem** Projektkategorisierung nach Technologie-/Fachwissen für Dienstleister Schmidt (international)

Technologiewissen / Fachwissen	Mobile Applikation	Cloud Technologie	Software as a Service
Geschäftskundenvertrieb in Mobilitätsbranche	BA - 2 - ac - I Beratung, Test	-	-
Abrechnung in Logistikbranche	-	BA - 1 - aa - I Entwicklung	BB - 1 - ab - I Test
Lagerprozesse in Logistikbranche	AA - 1 - bc - I Beratung, Test	AA - 1 - ba - I Entwicklung	-

Abbildung 68: Risikobewertung Logistiksystem

Bei einem neuen Projekt kann für jeden Dienstleister eine eigene Analyse zur Risikobewertung herangezogen werden. Der Projektmanager mit dem Management muss auf der Grundlage der vorliegenden Informationen die Ressourcenentscheidung treffen. In die Risikobewertung sollte die Projektsituation einbezogen werden.

Beispiel AA–1-bb-II:

AA Bewertung aus der Wissenskategorisierung

1 Anzahl der Projekte mit der Fachwissens- und Technologiewissenskombination

bb Bewertung der Kenntnisse und Fähigkeiten des Dienstleisters in der Fach- und Technologiewissenskombination

II Dienstleisterbewertung nach Gefahrenpotential

In den rot gekennzeichneten Matrix-Bereichen wird „viel“ Wissensschutz gebraucht. Für die bestehenden Projekte sollte eine Risikobewertung der eingesetzten externen Dienstleister vom Projektmanager mit dem Management durchgeführt werden. Für neue IT-Projekte kann für jeden Dienstleister eine Empfehlung vom IT-Sourcing Management auf der Grundlage des Wissensschutz-Referenzmodells ausgesprochen werden.

Interviewfragen zu den Fragenclustern Projekt-, Wissens-, Dienstleisterkategorisierung und Risikobewertung

Projektkategorisierung

1. Akteure:
    a. Welche Kompetenzen ordnen Sie bei der Projektkategorisierung dem Projektmanager und seinem Management zu und welche nicht?
2. Projektbewertung:
    a. Welche weiteren Projektinformationen sollten nach Ihrer praktischen Erfahrung in die Projektkategorisierung aufgenommen werden?

Wissenskategorisierung

1. Akteure:
    a. Welche Kompetenzen ordnen Sie bei der Wissenskategorisierung dem Management mit dem Strategie- und dem Kundenmanagement zu und welche nicht?
    b. Wie bewerten Sie die Durchführbarkeit der Wissenskategorisierung vom Management mit dem Strategie- und dem Kundenmanagement?
2. Bewertungskategorien:
    a. Welche weiteren Bewertungskategorien sollten nach Ihrer praktischen Erfahrung in die Wissenskategorisierung aufgenommen werden? (siehe Bewertungskategorien: Strategie, Kundennutzen, Mitbewerberabgrenzung, Übertragbarkeit)
    b. Wie schätzen Sie die Bewertungsskala ein, bildet die vorhandene Skala den Bewertungsbereich ab?
    c. Wie sollte die Gewichtung der Bewertungskategorien für das Fachwissen und das Technologiewissen sein: gleich oder verschieden?
    d. Wie würden Sie die Bewertungskategorien für Ihre IT-Beratung gewichten?
3. Kombinierte Bewertung mit Projektbezug:
    a. Welche generelle Gewichtung sollte das Fachwissen im Vergleich zum Technologiewissen erhalten?
    b. Wie würden Sie die Kombination von sehr wertvollem Fachwissen und Technologiewissen mit der Zuordnung zu mehreren Projekten (BA) und externer Dienstleisterbeteiligung gewichten?
    c. Sollte das Fachwissen und das Technologiewissen in die Wissenskategorisierung aufgenommen und bewertet werden, welches erst in der Zukunft für die IT-Beratung wichtig werden könnte? (mit Begründung)

Dienstleisterkategorisierung

1. Akteure:
    a. Welche Kompetenzen ordnen Sie bei der Dienstleisterkategorisierung dem IT-Sourcing Management zu und welche nicht?
    b. Wie bewerten Sie die Durchführbarkeit der Dienstleisterkategorisierung vom IT-Sourcing Management?
2. Dienstleisterkategorisierung nach Gefahrenpotential:

a. Welche Informationen brauchen und brauchen wir nicht über unsere externen Dienstleister, damit wir in die Lage versetzt werden können das wertvolle Wissen zu schützen?

b. Empfinden Sie die Bewertungsskala nach Gefahrenpotential I-III als ausreichend?

3. Bewertungskategorien für die Feststellung der Fachwissens- und Technologiewissensüberlappung:

a. Welche weiteren Dienstleisterbewertungskategorien sollten nach ihrer praktischen Erfahrung in die Dienstleisterkategorisierung aufgenommen werden?

b. Welche Informationen brauchen und brauchen wir nicht über Dienstleister, damit wir in die Lage versetzt werden können das wertvolle Wissen zu schützen?

c. Welchen Einfluss hat nach Ihrer Erfahrung die Projektrolle auf den Wissensschutz? Gibt es im IT-Projekt Rollen, die kritischer in Bezug auf den Wissensabfluss zum externen Dienstleister sind?

Risikobewertung

1. Akteure

a. Werden nach Ihrem Verständnis die Akteure befähigt eine Risikobewertung durchzuführen? (mit Begründung)

b. Welche weiteren Informationen sollten nach Ihrer praktischen Erfahrung in die Risikobewertung aufgenommen werden, damit der Projektmanager nachhaltig für die Wettbewerbsfähigkeit der IT-Beratung handeln kann?

Sonstige Fragen

- Wie bewerten Sie die Anwendbarkeit des Wissensschutzmodells?
- Welchen Einfluss hat die Fluktuationsquote des externen Dienstleisters auf den Wissensschutz? (in der Risikobestimmung?)
- Das Thema Wirtschafsschutz findet in der deutschen Industrie zunehmend an Bedeutung. Wo sehen sie die Abgrenzung des Wissensschutzes oder Informationsschutzes zum Wirtschaftsschutz?
- Welches dieser Handlungen des externen Dienstleisters würden sie der Wirtschaftsspionage zuordnen? / Würden sie sagen, dass diese Aktivitäten zum Wissensschutz der Wirtschaftsspionage vom externen Dienstleister entgegenwirken?
- Welche zusätzlichen Kategorien würden sie in das Modell bzgl. internationaler Dienstleister aufnehmen?
- Wie lange sind sie schon im IT-Geschäft tätig? In welchen anderen IT-Beratungen haben sie gearbeitet? In welcher Fachrichtung haben sie studiert?