

Schlussbericht vom 30.11.2022

zu IGF-Vorhaben Nr. 21191 N

Thema

Legitimise IT – Gestaltung eines Ansatzes zur Nutzung von Schatten-IT für produzierende kleine und mittelständische Unternehmen (KMU)

Berichtszeitraum

01.06.2020 bis 31.05.2022

Forschungsvereinigung

Forschungsinstitut für Rationalisierung FIR e. V. an der RWTH Aachen

Forschungseinrichtung(en)

Forschungseinrichtung 1: Forschungsinstitut für Rationalisierung FIR e. V. an der RWTH Aachen

Forschungseinrichtung 2: IPRI – International Performance Research Institute gGmbH

Gefördert durch:

Das IGF-Vorhaben 21191 N der Forschungsvereinigung Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen wurde über die AiF im Rahmen des Programms zur Förderung der Industriellen Gemeinschaftsforschung und -entwicklung (IGF) vom Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages gefördert.

Autorschaft



Max-Ferdinand Stroh
Bereichsleiter Informationsmanagement
FIR e. V. an der RWTH Aachen



Mischa Seiter
Univ.-Prof. Dr.
IPRI International Performance Research Institute



Rafael Götzen
M. Sc.
FIR e. V. an der RWTH Aachen



Kajan Kandiah
M. Sc.
FIR e. V. an der RWTH Aachen



Laura Vetter
M. A.
IPRI International Performance Research Institute

Inhaltsverzeichnis

Abbildungsverzeichnis	8
Tabellenverzeichnis	10
Zusammenfassung	12
1. Wissenschaftlich-technische und wirtschaftliche Problemstellung	13
2. Gegenüberstellung der Ergebnisse mit den Zielsetzungen laut Einreichung	16
3. Detaildarstellung der erzielten Ergebnisse	17
3.1 Arbeitspaket 1: Identifikation von Schatten-IT	17
3.1.1 <i>Definition von Schatten-IT und Entstehungsfelder</i>	17
3.1.2 <i>Identifikationsansätze von Schatten-IT</i>	19
3.1.3 <i>Fallstudien</i>	22
3.1.4 <i>Vorgehen zur Identifikation von Schatten-IT</i>	23
3.2 Arbeitspaket 2: Risiken und Nutzenaspekte identifizieren und quantifizieren	25
3.2.1 <i>Klassifikation der Risiken und Nutzenaspekte</i>	25
3.2.2 <i>Aktuelle Relevanz der Thematik</i>	25
3.2.3 <i>Literaturanalyse und Fallstudien</i>	26
3.2.4 <i>Identifikation, Analyse und Bewertung von IT-Risiken</i>	34
3.2.5 <i>Methoden</i>	36
3.2.6 <i>Fallstudien</i>	40
3.2.7 <i>Bewertungsmetrik für Schatten-IT und Validierung</i>	41
3.3 Arbeitspaket 3: Entwicklung und Bestimmung von Lösungsansätzen für die Nutzung von Schatten-IT	46
3.3.1 <i>Anforderungen an Lösungsansätze für die Nutzung von Schatten-IT</i>	46
3.3.2 <i>Plattformbasierter Lösungsansatz</i>	47
3.3.3 <i>Allgemeine Lösungsansätze für die Nutzung von Schatten-IT</i>	49
3.3.4 <i>Fallstudien</i>	52
3.3.5 <i>Assessment der Ansätze zur Legitimierung von Schatten-IT</i>	52
3.4 Arbeitspaket 4: Konzeption und Validierung eines ganzheitlichen Vorgehens für Schatten-IT bei KMU	54
3.4.1 <i>Auswahl und Konzeption eines ganzheitlichen Vorgehensmodells</i>	54
3.4.1 <i>Nutzeroberfläche des Webdemonstrators</i>	54
3.4.2 <i>Funktionsweise des Webdemonstrators</i>	60
3.4.3 <i>Validierung des Webdemonstrator mit dem projektbegleitenden Ausschuss</i> 62	
3.5 Arbeitspaket 5: Entwicklung eines Reifegradmodells für den Umgang mit Schatten-IT64	

3.5.1	<i>Grundlagen für ein Reifegradmodell zum Umgang mit Schatten-IT</i>	64
3.5.2	<i>Anforderungen an das Reifegradmodell zum Umgang mit Schatten-IT</i>	65
3.5.3	<i>Entwicklung des Reifegradmodells zum Umgang mit Schatten-IT</i>	65
3.6	Arbeitspaket 6: Dokumentation, Transfer und Projektmanagement	79
4.	Notwendigkeit und Angemessenheit der geleisteten Arbeit sowie Verwendung der Zuwendung	80
5.	Innovativer Beitrag und Nutzen für KMU	81
5.1	Wissenschaftlich-technischer und wirtschaftlicher Nutzen der erzielten Ergebnisse für KMU	81
5.2	Industrielle Anwendungsmöglichkeiten der erzielten Ergebnisse	82
6.	Veröffentlichungen und Transfermaßnahmen	83
6.1	Projektbegleitender Ausschuss im Projekt.....	83
6.2	Plan zum Ergebnistransfer	84
6.3	Einschätzung zur Realisierbarkeit des vorgeschlagenen und aktualisierten Transferkonzepts	87
7.	Forschungsstellen	89
7.1	Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen	89
7.2	International Performance Research Institute (IPRI) gGmbH.....	89
Anhang	91
Literaturverzeichnis	114

Abbildungsverzeichnis

Abbildung 1 Vorgehen in Arbeitspaket 1 (eigene Darstellung)	17
Abbildung 2: Identifikationsmöglichkeiten für Schatten-IT (eigene Darstellung)	19
Abbildung 3: Bewertung der Fallstudien (subjektiv) (eigene Darstellung)	23
Abbildung 4: Vorgehen in Arbeitspaket 2 (eigene Darstellung)	25
Abbildung 5: Prozess der Literaturrecherche und -evaluation (eigene Darstellung)	27
Abbildung 6: Suchstrings für die verschiedenen Datenbanken (eigene Darstellung)	27
Abbildung 7: Suchergebnisse in den verschiedenen Datenbanken (eigene Darstellung)	28
Abbildung 8: Klassen der Nutzenaspekte von Schatten-IT nach Wirkungsbereich (eigene Darstellung)	29
Abbildung 9: Klassen der Risiken von Schatten-IT nach Wirkungsbereich (eigene Darstellung)	30
Abbildung 10: Einflussfaktoren für das Zustandekommen von Risiken (eigene Darstellung)	35
Abbildung 11: Beispiel eines Risikomodells (eigene Darstellung)	35
Abbildung 12: Beispiel eines Angriffsbaums (eigene Darstellung)	37
Abbildung 13: Beispiel eines Fehlerbaums einer Schatten-IT mit Wahrscheinlichkeiten (eigene Darstellung)	38
Abbildung 14: FMEA (eigene Darstellung)	39
Abbildung 15: Risikomatrix (eigene Darstellung)	39
Abbildung 16: Eignung der Methoden zur Bewertung der Risiken von Schatten-IT (eigene Darstellung)	41
Abbildung 17: Beispielhafte Risikomatrix (eigene Darstellung)	43
Abbildung 18: Beispielhaftes, aggregiertes Risikoportfolio (eigene Darstellung)	45
Abbildung 19: Vorgehen in Arbeitspaket 3 (eigene Darstellung)	46
Abbildung 20: Konsolidierte Anforderungen an Low-Code-/No-Code Plattformlösungen	47
Abbildung 21: Vorlage eines Funktionssteckbrief für Low-Code-/No-Code Plattformen	48
Abbildung 22: Übersicht von verschiedenen Arten von IoT-Plattformen	49
Abbildung 23: Übersicht von Lösungsansätzen (eigene Darstellung)	49
Abbildung 24: Vorgehen in Arbeitspaket 4 (eigene Darstellung)	54
Abbildung 25: Individuelle Gewichtung der Aspekte der IT-Strategie (eigene Darstellung)	56
Abbildung 26: Ansätze zur Identifikation von Schatten-IT (eigene Darstellung)	57
Abbildung 27: Eingabemaske zur Erfassung von Schatten-IT (eigene Darstellung)	58
Abbildung 28: Visualisierung und Auswertung der erfassten Schattenlösungen (eigene Darstellung)	59
Abbildung 29: Bewertung und Darstellung der Eignung von Lösungsansätzen (eigene Darstellung)	60

Abbildung 30: Vorgehen in Arbeitspaket 5 (eigene Darstellung)	64
Abbildung 31: Vorgehensweise zur Entwicklung des Reifegradmodells in Anlehnung an NEFF ET AL. (2014)	66
Abbildung 32: Übersicht über das Reifegradmodell zum Umgang mit Schatten-IT (eigene Darstellung)	68
Abbildung 33: Ausschnitt aus dem Self-Assessment (eigene Darstellung)	78
Abbildung 34: Ergebnisse des Self-Assessments aus Interview (eigene Darstellung)	79

Tabellenverzeichnis

Tabelle 1: Gegenüberstellung von Zielsetzung und erarbeiteten Ergebnissen	16
Tabelle 2: Übersicht der Fallstudien	32
Tabelle 3: Relevanz der Nutzenaspekte in den befragten Unternehmen (eigene Darstellung)	33
Tabelle 4: Relevanz der Risiken in den befragten Unternehmen (eigene Darstellung)	34
Tabelle 5: Risikotabelle (eigene Darstellung)	39
Tabelle 6: CIA-Tabelle (eigene Darstellung).....	40
Tabelle 7: Nutzwert- und Risikoanalyse (eigene Darstellung)	43
Tabelle 8: Weitere Bewertungskriterien (eigene Darstellung).....	44
Tabelle 9: Matching der IT-Aspekte mit den Nutzenmerkmalen (eigene Darstellung).....	60
Tabelle 10: Matching der IT-Aspekte mit den Risikomerkmale (eigene Darstellung)	61
Tabelle 11: Wertzuordnung in Abhängigkeit von der Nutzeranzahl (eigene Darstellung).....	62
Tabelle 12: Bewertungslogik zur Auswahl der Lösungsansätze (eigene Darstellung)	62
Tabelle 13: Bezeichnung und Kurzbeschreibung der Reifegradstufen	67
Tabelle 14: Ausprägungen Gestaltungsobjekt IT-Strategie	69
Tabelle 15: Ausprägungen Gestaltungsobjekt Unterstützung durch das Management.....	69
Tabelle 16: Ausprägungen Gestaltungsobjekt Potenzialbewusstsein	70
Tabelle 17: Ausprägungen Gestaltungsobjekt IT-Feedbackkultur und Kommunikation	70
Tabelle 18: Ausprägungen Gestaltungsobjekt Transparenz	71
Tabelle 19: Ausprägungen Gestaltungsobjekt Prozesse zur Identifikation von Schatten-IT.....	71
Tabelle 20: Ausprägungen Gestaltungsobjekt Prozesse zum Umgang mit Schatten-IT	72
Tabelle 21: Ausprägungen Gestaltungsobjekt Risiko- und Nutzenbewertung.....	72
Tabelle 22: Ausprägungen Gestaltungsobjekt Definition von Verantwortlichkeiten.....	73
Tabelle 23: Ausprägungen Gestaltungsobjekt Ressourcenbereitstellung	73
Tabelle 24: Ausprägungen Gestaltungsobjekt Schulungen zum Thema Schatten-IT	74
Tabelle 25: Ausprägungen Gestaltungsobjekt Awareness	74
Tabelle 26: Ausprägungen Gestaltungsobjekt Silodenken und Zusammenarbeit	75
Tabelle 27: Ausprägungen Gestaltungsobjekt Monitoring-Tools.....	75
Tabelle 28: Bezeichnung und Beschreibung der Reifegradstufen	76
Tabelle 29: Personaleinsatz der Forschungseinrichtungen	80
Tabelle 30: Mitglieder des Projektbegleitenden Ausschusses	83
Tabelle 31: Sitzungen des PA und inhaltliche Schwerpunkte der jeweiligen Sitzung.....	83
Tabelle 32: Transfermaßnahmen während der Projektlaufzeit	84
Tabelle 33: Transfermaßnahmen nach Projektende.....	86

Tabelle 34: FIR e. V. an der RWTH Aachen.....	89
Tabelle 35: IPRI gemeinnützige GmbH.....	90

Zusammenfassung

Im Forschungsprojekt „Legitimise IT“ wurde ein einheitlicher Ansatz zur Nutzung von Schatten-IT für produzierende kleine und mittlere Unternehmen (KMU) entwickelt. Dadurch sollen KMU zur kontrollierten Legitimierung nutzenstiftender Schatten-IT unter Berücksichtigung vorhandener Risiken befähigt werden.

Schatten-IT ist in den meisten Unternehmen vorhanden. Durch den unkontrollierten Einsatz von Schatten-IT im Unternehmen entstehen zahlreiche Risiken, welche zu Ineffizienzen und Fehleranfälligkeiten bei den Betriebsabläufen führen können. Dabei wird die Entstehung von Schatten-IT nicht zuletzt durch die Schnelllebigkeit und Vielfalt der technologischen Entwicklungen weiter beschleunigt. Der Ansatz, durch eine strikte Vorgabe der Unternehmensführung lediglich auf genehmigte und zentral verwaltete IT-Anwendungen zurückzugreifen, um Schatten-IT zu unterbinden, hat sich in der unternehmerischen Praxis nicht bewährt. Bisherige Ansätze adressieren nicht die Gründe für die Notwendigkeit von Schatten-IT und bieten keinen organisatorischen und insbesondere technologischen Rahmen, um deren Vorteile unternehmerisch zu nutzen.

Daher wurde im Projekt ein Ansatz entwickelt, der einerseits die aufgezeigten Risiken minimiert und andererseits Mitarbeitenden die notwendigen Freiheiten für eigene, kreative Lösungen bietet. Damit Unternehmen ihre großen Herausforderungen bei der Abschätzung der Risiken- und Nutzenaspekte wie auch beim strikten Verzicht auf die eingesetzten Schatten-IT-Anwendungen bewältigen können, wird eine entsprechende Methodik gefordert.

Zunächst wurden Ansätze zur Identifikation von Schatten-IT in der Praxis identifiziert und systematisiert. Dazu wurde ein entwickelter Fragebogen genutzt, um Schatten-IT in direkten Gesprächen mit den Fachabteilungen zu erfassen. Die Risiken- und Nutzenaspekte von Schatten-IT wurden daraufhin anhand einer systematischen Literaturanalyse identifiziert und klassifiziert. Auf Basis der Klassifizierung wurde eine qualitative Bewertungsmethodik zur Risiken- und Nutzwertanalyse von Schatten-IT erarbeitet und mit Unternehmensvertretern in der direkten Anwendung validiert. Darauf aufbauend wurden bestehende und neue Lösungsansätze zum Umgang mit Schatten-IT strukturiert erfasst, beschrieben und mit Unternehmen des projektbegleitenden Ausschusses validiert. Neben klassischen Ansätzen wie Dokumentation und Verantwortungsübertragung wurden auch plattformbasierte und legitimierende Ansätze entwickelt. Die Ergebnisse wurden anschließend in Form eines dreistufigen Vorgehens zum Umgang mit Schatten-IT integriert und in Form eines frei zugänglichen, webbasierten Tools (<https://legitimise-it-tool.fir.de/>) umgesetzt, welches sich speziell an Entscheidende der zentralen IT richtet. Konkret unterstützt das Webtool Anwendende bei der Identifikation von Schatten-IT und stellt ein Self-Assessment zur Risiko- und Nutzwertanalyse identifizierter Anwendungen bereit. Auf Basis der Analyse werden passende Lösungsansätze bereitgestellt.

Es zeigte sich zudem, dass Unternehmen eher eine objektive Einstufung der Ausgangssituation wünschen als die Ausarbeitung einer technologischen Plattformlösung für die Verwaltung von Schatten-IT. Im letzten Schritt wurde daher ein praxisnahes Reifegradmodell für den Umgang mit Schatten-IT entwickelt und mit Unternehmen des projektbegleitenden Ausschusses validiert. Das Reifegradmodell integriert die identifizierten Handlungsfelder sowie alle bis dato erarbeiteten Forschungsergebnisse und ermöglicht Unternehmen, ihre Entwicklungsstufe im Umgang mit Schatten-IT mehrdimensional zu erfassen und dadurch Entwicklungspfade abzuleiten.

1. Wissenschaftlich-technische und wirtschaftliche Problemstellung

Im durchgeführten Forschungsprojekt wurden gemeinsam mit dem projektbegleitenden Ausschuss (pbA) neue Methoden zur Identifikation, Beurteilung und Legitimierung von Schatten-IT in KMU erarbeitet. Die dabei adressierte Problemstellung ist vielschichtig und wird im Folgenden an Beispielen näher erläutert.

KMU des produzierenden Gewerbes nutzen zumeist ein ERP-System zur bedarfsgerechten Planung und Steuerung von Ressourcen. Bei dessen Nutzung können Probleme für KMU entstehen. Ein Beispiel ist die Situation, dass ein ERP-System nicht alle notwendigen Informationen für weiterführende Analysen bereitstellt. Insbesondere sind jedoch die wenig intuitiven Nutzerschnittstellen in der Anwendung ein Problem für KMU. Dieses Problem erhöht die Wahrscheinlichkeit für die Entstehung von Schatten-IT, weil der Nutzerkreis das System umgeht, um praktikable oder einfachere Lösungen zu nutzen (s. BEHRENS 2009; GORLA ET AL. 2010; TAJUL URUS ET AL. 2011). Unter Schatten-IT wird in diesem Schlussbericht jegliche Software (sowohl intern wie extern betrieben) verstanden, die autonom von Fachbereichen in Unternehmen, neben der offiziellen IT-Infrastruktur, eingesetzt oder entwickelt wird, ohne die unternehmenseigene IT-Abteilung zu informieren (s. KOPPER U. WESTNER 2016). Dabei distanziert sich die hier aufgeführte Definition klar von der negativ vorbelasteten Ansichtswiese von Schatten-IT.

Hierzu ein Beispiel aus der Praxis: Der Vertriebsinnendienst möchte im Rahmen der individuellen Angebotserstellung die Installationskosten einer komplexen Maschine kalkulieren. Dazu wird eine detaillierte Kalkulation auf Basis des Materials und der Personalkapazitäten im Kontext möglicher individueller Gegebenheiten durchgeführt. Dies können mögliche Besonderheiten am Ort der Installation sein, bspw. die Beschaffenheit der Wände, wodurch zusätzliches Material und zusätzliche Zeit zur Installation der Maschine aufgewendet werden müssen. Derartige Informationen fließen auf Basis von Erfahrungswerten der Mitarbeitenden in die Kalkulation ein. Dazu existiert in ERP-Systemen kein Standardprozess, sodass Vertriebsmitarbeitende ihre eigenständig konzipierten Lösungen zur Kalkulation verwenden. Excelbasierte Anwendungen (oft in Verbindung mit Visual-Basic-for-Applications(VBA)-Makros) sind häufig auftretende Beispiele für derartige Lösungen, welche nicht zentral von der IT-Abteilung erfasst werden können und zumeist nur unzureichend dokumentiert sind.

Durch den unkontrollierten Einsatz von Schatten-IT im Unternehmen entstehen zahlreiche Risiken (s. Rentrop u. Zimmermann 2015). Im Beispiel führt die Entnahme der Daten aus dem ERP-System sowie die Verarbeitung in eigenständigen Schatten-IT-Anwendungen zu einer nicht nachvollziehbaren Kalkulation der Kosten. Des Weiteren ist die Kalkulation vom Erfahrungsschatz des jeweiligen Vertriebsmitarbeitenden abhängig. Dies kann zu einer falschen Kalkulation und damit zu erhöhten Kosten für das produzierende KMU führen. Grundsätzlich stellt sich die Frage, ob nicht Ansätze entwickelt werden müssen, die die Entstehung von Schatten-IT als „Symptom“ von vornherein vermeiden. Durch eine entsprechende Ausrichtung der IT-Abteilung und der Antizipation weiterer Gründe, die die Entstehung von Schatten-IT begünstigen, würde sich die Notwendigkeit des hier aufgezeigten Forschungsvorhabens gar nicht erst stellen. Dieser Ansatz ist jedoch aus zwei Gründen nicht realistisch: Zum einen wird es nie möglich sein, die Entstehung von Schatten-IT gänzlich zu unterbinden. Dies liegt nicht zuletzt in der Schnellebigkeit und Vielfalt der technologischen und gesellschaftlichen Entwicklungen begründet (s. Stoop 2016). Zum anderen knüpft das hier aufgezeigte Forschungsvorhaben bewusst an die heute bestehende Schatten-IT in vielen produzierenden KMU an. Sie stehen vor der Herausforderung, ihren aktuellen Status quo

anhand anwendbarer Methoden zu optimieren, bevor sie sich der Fragestellung widmen können, wie sich Schatten-IT vor ihrer Entstehung vermeiden lässt.

Schatten-IT ist in den meisten Unternehmen vorhanden (s. Bröhl 2017). Sie entsteht in unterschiedlichem Umfang, je nach vorhandenem IT-Budget, vorhandener bzw. nicht vorhandener Expertise und technischen Einschränkungen in den Fachbereichen. Aufgrund kleiner IT-Abteilungen, Ressourcenengpässen und fehlender Expertise sind vor allem KMU davon betroffen (s. Fliehe u. Alici 2014). Für Unternehmen stellen die Abschätzung der aufgezeigten Risiken und Nutzenaspekte sowie der strikte Verzicht auf die eingesetzten Schatten-IT-Anwendungen große Herausforderungen dar. Demnach soll nutzenstiftende Schatten-IT, unter Berücksichtigung vorhandener Risiken, in den Unternehmen kontrolliert zugelassen und genutzt werden (s. Walterbusch et al. 2014).

Die zentrale Forschungsfrage dieses Forschungsprojekts lautete:

Wie können KMU durch ein Vorgehen zur Legitimierung bestehende Schatten-IT nutzen?

Aus ihr ließen sich die folgenden Teilfragen ableiten:

1. Wie kann Schatten-IT in einem Unternehmen identifiziert werden?

Es existiert kein einheitliches Verständnis und somit keine offizielle Definition für Schatten-IT. Demnach existierte auch kein standardmäßiger Prozess zu deren Erfassung. Unternehmen stehen dabei zunächst vor der Herausforderung, vorhandene Schatten-IT zu identifizieren.

2. Wie können Nutzenaspekte und Risiken von Schatten-IT identifiziert und bewertet werden?

Für Unternehmen, insbesondere produzierende KMU, besteht, wie aufgezeigt, eine Schwierigkeit darin, das Ausmaß von Schatten-IT hinsichtlich der Nutzenaspekte und Risiken im Unternehmen abzuschätzen (s. Hoff 2015; Moore et al. 2007). Um die Vielzahl der Schatten-IT-Anwendungen voneinander abgrenzen zu können, galt es, diese zu priorisieren.

3. Welche Lösungsansätze kommen unter Berücksichtigung der Mensch-, Technik-, Organisation-(MTO)-Perspektiven in Frage?

Aufgrund der genannten Herausforderungen für KMU (s. Fliehe u. Alici 2014) müssen diese beim Umgang mit Schatten-IT und deren Nutzung unterstützt werden. Es galt, insbesondere Fragen der technischen Umsetzung, der Systemintegration und der organisatorischen Regelungen zu beantworten. Fokussiert wurde hier die Entwicklung neuer Ansätze (z. B. ein zentraler Intermediär in Form einer Software-Plattform).

4. Wie kann aus den einzelnen Lösungsansätzen ein Vorgehen abgeleitet werden, mit dem KMU ihr eigenes Vorhaben zur Nutzung der Schatten-IT gestalten?

Durch die Nutzung eines einzelnen Ansatzes können die Ziele der KMU nicht erfüllt werden. Durch die unternehmensspezifische Kombination einzelner Ansätze zu einem ganzheitlichen Legitimierungsvorgehen ist ein praktisch einsetzbarer Umsetzungsleitfaden entstanden.







5. Wie können die Auswirkungen dieses Vorgehens zur kontrollierten Nutzung gemessen werden?

Für die Erfolgsbewertung wurde die Auswirkung des Legitimierungsvorgehens zur Nutzung von Schatten-IT gemessen.

2. Gegenüberstellung der Ergebnisse mit den Zielsetzungen laut Einreichung

Die Institute FIR und IPRI bearbeiteten gemäß dem angedachten Forschungsvorgehen die aus den Forschungsfragen abgeleiteten Arbeitspakete. Dabei wurde der Großteil der antizipierten Ergebnisse vollends erreicht oder vom pbA befürwortete Alternativergebnisse erarbeitet, welche sich als unmittelbar nutzenstiftend erwiesen. Dazu zählt vor allem die Auskopplung der Teilergebnisse in einem passenden Web-Tool, welches unmittelbar in die operative Arbeit bei KMU eingebunden werden kann. Eine Gegenüberstellung der Ergebnisse ist Tabelle 1 zu entnehmen. Die Ausdetaillierung der einzelnen Arbeitspakete kann Kapitel 3 entnommen werden.

Tabelle 1: Gegenüberstellung von Zielsetzung und erarbeiteten Ergebnissen

Arbeitspaket (AP)	Geplante Ergebnisse	Erzielte Ergebnisse	Geplante Ergebnisse erreicht?
AP 1: Identifikation von Schatten-IT	Ein KMU-gerechtes Vorgehen zur aufwandsarmen Identifikation von Schatten-IT	Erhebung von vier Ansätzen zur Identifikation von Schatten-IT in KMU. Überführung in ein anwendungsfreundliches Vorgehen.	
AP 2: Risiken und Nutzenaspekte identifizieren und quantifizieren	Leitfaden zur Aufdeckung sowie Bewertung der Risiken und Nutzenaspekte von identifizierten Schatten-IT-Anwendungen anhand der ERP-Prozesslandschaft von Unternehmen	Identifikation der Chancen und Risiken von Schatten-IT. Entwicklung einer Checkliste und Nutzwertanalyse zur Bewertung identifizierter Schatten-IT-Anwendungen.	
AP 3: Entwicklung und Bestimmung von Lösungsansätzen für die Nutzung von Schatten-IT	Auswahl-Assessment entwickelter sowie beschriebener Ansätze zur Legitimierung von Schatten-IT	Identifikation von sechs Ansätzen zur Handhabung von Schatten-IT. Entwicklung einer Bewertungslogik als Auswahl-Assessment.	
AP 4: Konzeption und Validierung eines ganzheitlichen Vorgehens für Schatten-IT bei KMU	Vorgehen und erweiterter Leitfaden zur Legitimierung von Schatten-IT	Überführung der Ergebnisse in einen aufwandsarmen Web-Demonstrator, welcher als Leitfaden für die u. a. Legitimierung von Schatten-IT dient.	
AP 5: Messung der finanziellen Auswirkungen des Ansatzes zur Nutzung von Schatten-IT	Monetäre Quantifizierung der Legitimierung von Schatten-IT	Änderung: Entwicklung eines Reifegradmodells auf Wunsch des projektbegleitenden Ausschusses.	
AP 6: Dokumentation, Transfer und Projektmanagement	Erfolgreich verlaufendes Projekt mit öffentlicher Wirkung, Ergebnistransfer	Erfolgreich durchgeführtes Projekt mit angemessenen Aktivitäten der Dissemination zur Gewährleistung der Praxistauglichkeit und des Ergebnistransfers.	

3. Detaildarstellung der erzielten Ergebnisse

3.1 Arbeitspaket 1: Identifikation von Schatten-IT

Ziel des ersten Arbeitspakets (s. Abbildung 1) war die Entwicklung eines KMU-gerechten Vorgehens zur aufwandsarmen Identifikation von Schatten-IT. Dazu wurde zunächst eine übergreifende Definition und mögliche Entstehungspfade für Schatten-IT erarbeitet und aufbereitet. Diese bilden die Grundlage für die organisatorische wie auch architekturelle Verortung von Schatten-IT. Auf Basis einer Literaturrecherche wurden existierende Ansätze und die formellen Lösungen zur Erfassung der Ist-Situation zur Identifikation von Schatten-IT aufbereitet. Mittels Fallstudien wurden weitere Kriterien für die Identifikation von Schatten-IT in KMU erhoben. Hierbei wurden die Unternehmen hinsichtlich des Verständnisses der Thematik und der ersten Auffälligkeiten befragt sowie nach den aktuellen Umgangsmethoden bei selbstentwickelten und unentdeckten Lösungen der Mitarbeitenden. Daraus wurde ein standardisierter Interviewleitfaden für die Befragung von Fachbereichen und somit zur strukturierten Identifikation von Schatten-IT entwickelt und im Zuge der Experteninterviews validiert. Allgemein wurde auf eine ausführliche Erhebung von Architekturen und Prozessen verzichtet, da im pbA keine ausreichende Prozessreife vorhanden war und eine grundlegende Methodik zur Unterstützung bei der Identifikation als zielführender angesehen wurde.

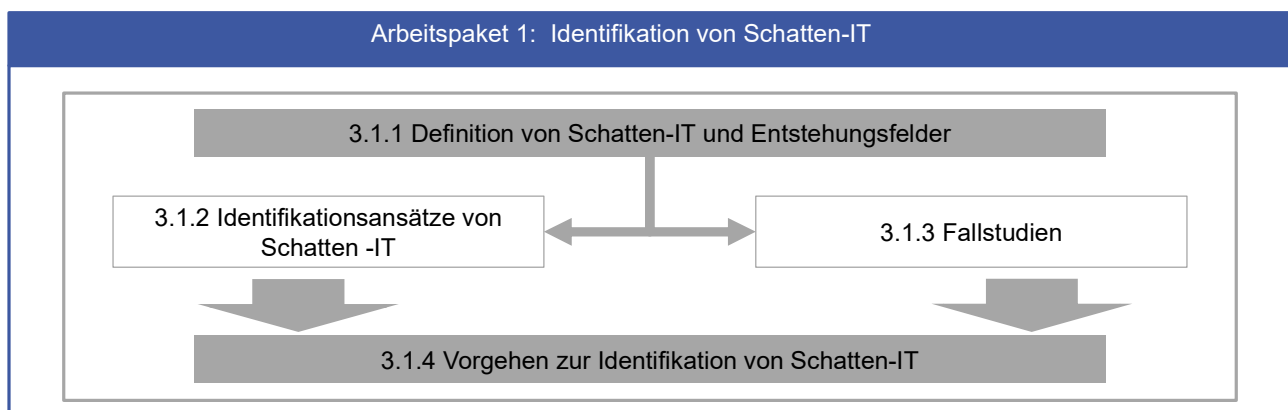


Abbildung 1: Vorgehen in Arbeitspaket 1 (eigene Darstellung)

3.1.1 Definition von Schatten-IT und Entstehungsfelder

Für die genaue Definition des Begriffs der Schatten-IT ist auf die Frage einzugehen, wann eine IT-Lösung im Schatten liegt. Die alleinige Unterscheidung nach Kenntnis oder Nichtkenntnis der IT-Abteilung über die Existenz und Nutzung einer bestimmten Schatten-IT ist nicht ausreichend. Demzufolge definieren Rentrop u. Zimmermann im Jahr 2015 Schatten-IT als sämtliche geschäftsprozessunterstützende Systeme, die weder technisch noch strategisch in das IT-Servicemanagement des Unternehmens eingebunden sind (s. RENTROP U. ZIMMERMANN 2015). Es sind drei Ausprägungen von Schatten-IT zu unterscheiden (s. Brenner et al. 2011):

- Von der IT-Abteilung registrierte Lösungen, die aber nicht gesteuert werden (Monitoring ohne Steuerung),
- von der IT-Abteilung unerkannte Lösungen, die allerdings technisch auffindbar wären, wobei die Lokalisierung kostenintensiv und rechtlich problematisch wäre (ohne Monitoring),
- Lösungen, die technisch nicht auffindbar sind, da ein technischer Zugriff fehlt (z. B. bei Cloudanwendungen).

Für die Identifikation von Schatten-IT ist es notwendig, ein gemeinsames Verständnis zu etablieren, aus welchen Gründen Schatten-IT entsteht, aber auch, welche neuen Entwicklungen durch die Digitalisierung die Entstehung fördern. Dies ermöglicht es, Entstehungsfelder zu identifizieren.

Klassische Entstehungsgründe

Schatten-IT entsteht von Natur aus oft dann, wenn das zentrale System nicht die Anforderungen der Fachabteilungen erfüllt. Für den Fall, dass Schatten-IT aufgedeckt wird, lässt sich aus den Funktionen, die die Schattenlösung erfüllt, ein Anforderungskatalog ableiten. Schatten-IT ist somit ein Indikator für nicht erfüllte oder nicht ausreichend beachtete Anforderungen der Fachabteilungen (s. Huber et al. 2017). Schatten-IT ist in den meisten Unternehmen vorhanden (s. Bröhl 2017). Sie entsteht in unterschiedlichem Umfang, je nach vorhandenem IT-Budget, vorhandener bzw. nicht vorhandener Expertise und technischen Einschränkungen in den Fachbereichen. Aufgrund kleiner IT-Abteilungen, Ressourcenengpässen und fehlender Expertise sind vor allem kleine und mittlere Unternehmen (KMU) davon betroffen (s. Fliehe u. Alici 2014). Für Unternehmen stellen die Abschätzung der aufgezeigten Risiken und Nutzenaspekte sowie der strikte Verzicht auf die eingesetzten Schatten-IT- Anwendungen große Herausforderungen dar. Demnach soll nutzenstiftende Schatten-IT, unter Berücksichtigung vorhandener Risiken, in den Unternehmen kontrolliert zugelassen und genutzt werden (s. Walterbusch et al. 2014). Daher ist es aus Sicht des IT-Managements und der IT-Steuerung notwendig, ein geeignetes Vorgehen zu beschreiben.

Neue Entwicklungen

Schatten-IT kann in unterschiedlichen Erscheinungsformen auftauchen und wird besonders in neuen Trends in der Digitalisierung deutlich. Hierfür unterscheidet das Institut für Wirtschaft der Universität St. Gallen drei Trends (s. Brenner et al. 2011):

- Cloud-Computing,
- Mobile-Computing,
- Digital Natives.

Cloud-Computing bezeichnet Dienste, mit denen infrastruktur-, entwicklungs- und geschäftsprozessorientierte Leistungen über das Internet bezogen werden können. Gründe für die Nutzung von Cloud-Computing-Diensten sind in den meisten Fällen die Anwenderfreundlichkeit und die Bereitstellungszeit. Hinzu kommt, dass die Mehrheit der Dienste kostenlos im Internet zur Verfügung steht und somit von den Mitarbeitenden zweifellos ausgeführt wird. Cloud-Computing-Dienste können nach Auswertung der Sicherheit im Unternehmen integriert werden oder als Indikatoren für die Ausarbeitung der IT-Abteilung verwendet werden, um den Anforderungen der Mitarbeitenden gerecht zu werden.

Mobile-Computing bezeichnet das Bedürfnis und den Einsatz von immer leistungsfähigeren Endgeräten, welche mit dem Internet verbunden sind. Dabei geht die Erwartung der Mitarbeitenden damit einher, dass der mobile Zugriff auf firmeninterne IT-Dienste, wie z. B. ERP-Systeme, E-Mails, Adressbuch oder Intranet-Zugriff, zu jeder Zeit mit ihrer eigenen Infrastruktur möglich ist. Während Mobile-Computing die Produktivität und Verfügbarkeit der Mitarbeitenden steigert, kann auf der anderen Seite die Datensicherheit durch die IT-Abteilung nicht vollständig gewährleistet werden.

Als Digital Natives werden Mitarbeitende bezeichnet, die dieselben Ansprüche gegenüber IT-Lösungen im Unternehmen haben, wie sie es ihren privaten IT-Umgebung gewohnt sind. Mithilfe

dieser Ansprüche der Mitarbeitenden, welche IT-Affinität und Kenntnis der Geschäftsprozesse aufweisen, kommt es vermehrt zu Schatten-IT (s. Brown u. Czerniewicz 2010).

Ein Beispiel für Cloud-Computing und für die Entstehung von Schatten-IT ist die Nutzung von Softwareprogrammen für die geschäftliche Kommunikation und den Datenaustausch, welche von Anbietern aus dem Internet bereitgestellt werden. Weiterhin gelten für die meisten Unternehmen Anwendungen, wie eigenentwickelte Spreadsheet- und Datenbankanwendungen auf Basis von Microsoft Excel oder Access als Schatten-IT, da diese sehr selten mit der IT-Abteilung kommuniziert werden und somit unbekannt bleiben.

3.1.2 Identifikationsansätze von Schatten-IT

Im Rahmen des Arbeitspakets wurden mithilfe einer intensiven Literaturrecherche und Workshops unterschiedliche Möglichkeiten zur Identifikation von Schatten-IT erarbeitet, die sowohl die IT als auch die Fachbereiche einbezieht. In Abbildung 2 werden die empfohlenen Lösungen zur Ermittlung von Schatten-IT aufgezeigt und im Folgenden kurz erläutert.

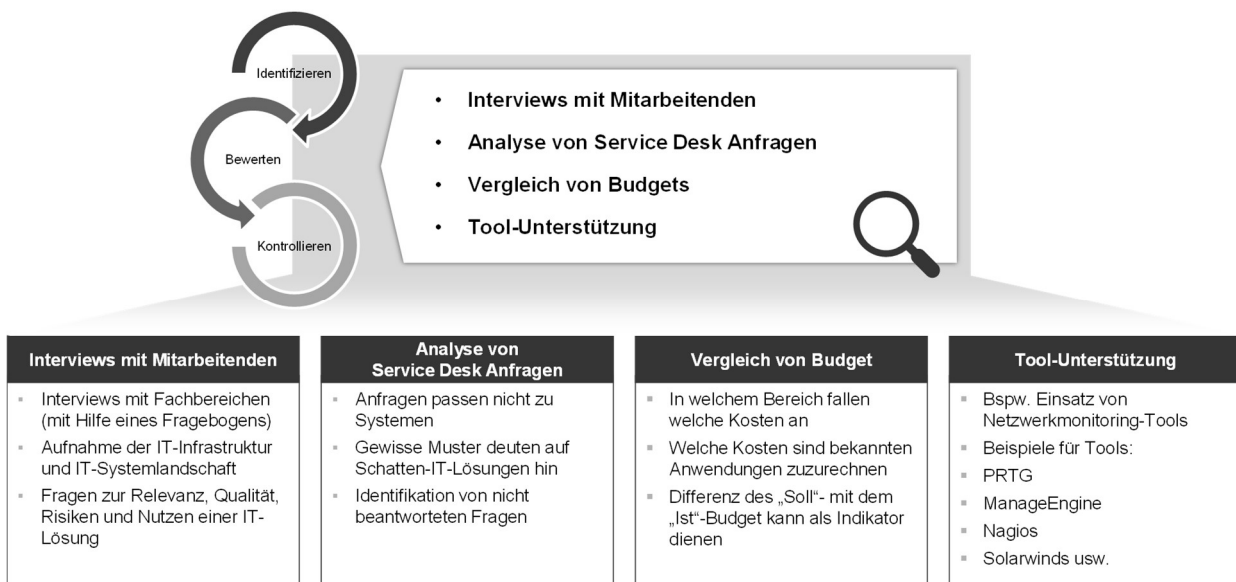


Abbildung 2: Identifikationsmöglichkeiten für Schatten-IT (eigene Darstellung)

Interviews mit Mitarbeitenden

Der Ermittlung des Ist-Zustands soll Transparenz über die Arbeitsprozesse, deren Dokumentation und die damit verbundenen technischen Lösungen schaffen. Um Unregelmäßigkeiten in den Prozessschritten zu identifizieren, können abteilungsinterne Interviews, verknüpft mit aufklärenden und interaktiven Workshops, mit den Fachbereichen durchgeführt werden. Es gibt zum einen eine standardisierte und zum anderen eine offene Interviewmöglichkeit.

Offene Befragungen finden als Leitfaden- und Experteninterviews statt. Bei dieser Befragungsform wird zunächst vor dem Interview eine strukturierte Fragenliste erstellt, welche im Interview Schritt für Schritt befolgt wird. Jedoch können während des Interviewverlaufs auch weitere Fragen ergänzt werden. Leitfaden- und Experteninterviews unterscheiden sich hauptsächlich im Status der befragten Partner. Bei Leitfrageninterviews stehen die persönliche Perspektive des Interviewpartners und seine Erfahrungen im Vordergrund. Experteninterviews unterscheiden sich von ihnen dadurch, dass ein neutraler und breiter Blick auf das Phänomen durch einen Spezialisten

dargestellt wird. In beiden Befragungsformen wird versucht, das Benutzerverhalten zu identifizieren und dann aufzuzeigen (s. Baur u. Blasius 2014).

Für die Identifikation des Phänomens Schatten-IT wurde die standardisierte Befragungsform bevorzugt, da somit eine Basis für ein allgemeines Vorgehen geschaffen werden konnte. Die standardisierte Befragungsform ermöglicht eine qualitative und quantitative Forschung mithilfe eines Fragebogens mit wesentlichen Punkten zur Ermittlung von Schatten-IT (s. Baur u. Blasius 2014). Die Reihenfolge der Fragen ist für den Detailgrad und für die Schatten-IT-Vorkommnisse ein zentraler Aspekt. Daher wurde für das Forschungsprojekt ein Leitfaden für ein standardisiertes Interview mit den Fachbereichen erstellt (s. Anhang 1). Dieser wurde in vier Abschnitte geteilt mit zwei thematisch aufeinander aufbauenden Blöcken. Nach einer Vorstellung der Interviewenden und Befragten hinsichtlich des Fachbereichs und der Position im Unternehmen werden im ersten Themenblock Kernfragen zur Identifikation und Beschreibung von Schatten-IT entlang der Prozessschritte im Fachbereich gestellt. Anschließend wurden Fragen zur Relevanz, Qualität, Risiken und Nutzung der Schatten-IT-Lösung formuliert. Nach Abschluss des Interviews werden die gesammelten Daten analysiert und ausgewertet. Die dabei gewonnene Transparenz zwischen den Abteilungen schafft Diskussionsfreiraum für die legalisierte und effiziente Nutzung der identifizierten Schatten-IT. Es wird eine Entscheidung getroffen bezüglich der weiteren Nutzung oder der Abschaffung der Lösung. Hierbei kann außerdem beurteilt werden, ob die von den Mitarbeitenden genutzten Methoden bzw. Ansätze mit der IT-Abteilung weiter ausgebaut werden können und die Prozesse standardisiert und somit in die zentrale IT aufgenommen werden können. Falls die genutzte Anwendung nicht profitabel für das Unternehmen ist oder eine bereits bekannte Anwendung von der IT bereitgestellt werden kann, können Aufklärungsgespräche und eine Umstellung durchgeführt werden. In den meisten Fällen können die genutzten Anwendungen der technikaffinen Mitarbeitenden als Motivation zur Verbesserung der Dienstleitungen der IT-Abteilungen dienen.

Bei der Analyse des Ist-Zustands musste der Fokus auf organisatorische Schwachstellen gelegt werden; eine Betrachtung der informationstechnischen Differenzen ist ergänzend anzuraten. Mithilfe einer ganzheitlichen Medienbruch- oder Schnittstellenanalyse werden Ineffizienzen an den Schnittstellen entlang des Wertstroms festgestellt. Medienbrüche können beispielsweise mittels Fragebogen mit definierten Bewertungskriterien identifiziert werden. (s. AKTIV-kommunal 2019).

Analyse der Service-Desk-Anfragen

Eine Analyse der Service-Desk-Anfragen ist ein weiteres Vorgehen, um Schatten-IT zu identifizieren, da Mitarbeitende sich oftmals aufgrund von unbeantworteten Anfragen, fehlenden Lösungsansätzen oder mangelnder Akzeptanz für neue bzw. innovative Lösungen selbst aushelfen. Ebenso werden formalisierte und veraltete Entscheidungs- und Bewilligungswege von den Mitarbeitenden für zu langsam oder nicht nachvollziehbar empfunden, sodass eigene Lösungen entwickelt werden (s. Zimmermann u. Rentrop 2012). Die Service-Desk-Analyse ermöglicht eine direkte und schnelle Suche von Schatten-IT innerhalb der IT-Architektur des Unternehmens. Allerdings ist diese Methodik nicht die einzige Vorgehensweise zur Identifikation und es ist außerdem schwierig, damit alle Schatten-IT-Vorkommnisse ausfindig zu machen (s. Zimmermann 2018).

Vergleich von Budgets

Ein weiteres Beispiel für die Entstehung von Schatten-IT umfasst neben der Software auch die Hardware, denn auch End- und Peripheriegeräte, wie bspw. Smartphones, Personal Computer,

Server, Router oder Drucker, können als Schatten-IT auftreten (s. Zimmermann 2018). Die Mitarbeitenden beschaffen sich auf eigenem Wege die benötigte Hardware, statt die Kataloge der IT-Abteilung zu nutzen. Aus dieser Problematik resultiert die Notwendigkeit für eine technische Analyse des Unternehmensbudgets. Um herauszufinden, ob im Unternehmen hardwareseitig Schatten-IT auftritt, kann ein Vergleich vom Budget durchgeführt werden. Falls sich eine Differenz beim Vergleich ergibt, ist dies ein Indikator für Schatten-IT.

Tool-Unterstützung

Implementierte Schatten-IT kann mithilfe von technischen Maßnahmen, wie z. B. Netzwerk-Monitoring identifiziert und/oder reduziert werden. Dazu ist der Einsatz von Ressourcen für Anwendungen, welche das gesamte Netzwerk auf Fehler oder Probleme scannen können, notwendig. Mithilfe der Auswertung von Logs und Reports der Firewall-Systeme kann eine Analyse der genutzten Applikationen erstellt werden. Bei diesem Ansatz ist eine gezielte Überwachung obligatorisch. Bei der Auswertung können bestimmte identifizierte Anwendungen von der IT-Abteilung als zu großes Risiko der Datensicherheit eingestuft werden, wodurch viele Applikationen an der Firewall gesperrt werden. Jedoch besteht die Möglichkeit, die gewünschte Anwendung der Mitarbeitenden in eine bestehende Applikation einzubauen.

Um Mitarbeitenden in ihrer Freiheit nicht enorm einzuschränken, können unterschiedliche Monitoring-Methoden angewendet werden:

- Monitoring mit Steuerung,
- Monitoring ohne Steuerung.

Monitoring mit Steuerung ist eine Form des Monitorings, bei der alle Lösungen von der IT-Abteilung verwaltet werden. Da der Einflussgrad der IT-Abteilung sehr hoch ist, ist die Wahrscheinlichkeit für die Entstehung von Schatten-IT sehr gering. Dahingegen bietet das Monitoring ohne Steuerung den Mitarbeitenden der Fachabteilungen mehr Freiraum. Denn bei dieser Lösung ist die Nutzung von Schatten-IT der IT-Abteilung bekannt. Doch auf Basis eines Vertrauensverhältnisses und einer umfassenden Transparenz findet keine bewusste Kontrolle seitens der IT-Abteilung statt (s. Brenner et al. 2011).

Eine Kombination der Service-Desk-Analyse und der technischen Analyse kann einen positiven Einfluss auf den Arbeits- und Zeitaufwand bei der Identifikation von Schatten-IT haben (s. Zimmermann 2018). Da keine expliziten Schatten-IT-Beispiele vorlagen, konnte der konkrete Anwendungsfall nicht durch Fallstudien validiert werden. Die Literaturrecherche ergab jedoch eine Liste an Vorteilen der identifizierten Möglichkeiten.

Fazit

Die vorgestellten Ansätze zur Identifikation können sowohl in KMU als auch größeren Unternehmen angewendet werden. In KMU existieren im Gegensatz zu großen Unternehmen oft nur ungenügende IT-Serviceprozesse bei gleichzeitig fehlender IT-Expertise. Servicemanager sind aufgrund der Größe von KMU teils nicht vorhanden (s. Adeyeri et al. 2019). Lizenzmanagementsysteme und Netzwerkanalysertools sind zum Teil frei verfügbar, doch auch hier ist nicht davon auszugehen, dass diese in der Mehrheit der KMU zum Einsatz kommen (s. Bollhöfer u. Jäger 2018). Die Annahme, dass in diesen Unternehmen ein organisierter Service-Desk existiert, ist zumindest für einen Teil der KMU nicht haltbar. Da in KMU informelle Informationskanäle mit geringem Formalisierungsgrad vorherrschen, ist der Informationsaustausch von mündlicher Weitergabe geprägt (s. Haake 2002). Somit stellt das gezielte Suchen nach Schatten-IT mithilfe strukturierter Interviews, erweitert um ein

ständiges Verarbeiten mündlich weitergegebener Informationen, die beste Lösung zur Identifikation von existierenden Schatten-Lösungen in KMU dar. Wichtig ist zudem, dass das Management von Schatten-IT eine kontinuierliche Aufgabe ist und in regelmäßigen Abständen wiederholt werden muss. Die Ergebnisse dieser Methoden zur Identifikation von Schatten-IT wurden in einem Katalog zusammengefasst, der die einzelnen Schatten-Lösungen auflistet.

3.1.3 Fallstudien

Im Rahmen des Arbeitspakets wurden drei Fallstudien mit unterschiedlichen Unternehmen in Form von Experteninterviews durchgeführt. Mithilfe der Analyse dieser Fallstudien wurde die Grundlage für die Gestaltung eines Ansatzes zur Nutzung von Schatten-IT für KMU gelegt. Aufbauend auf der Analyse bestehender Ansätze zur Identifikation von Schatten-IT-Anwendungen können mögliche Einsatzgebiete und technische Umsetzungen evaluiert werden.

Um eine standardisierte Auswertung anhand aller Fallstudien und eine spätere Auswertung von Mustern und Gemeinsamkeiten zu gewährleisten, wurden alle Fallstudien anhand derselben Kriterien evaluiert. Hierfür wurden folgende Dimensionen betrachtet:

- Status quo
- Aktuell genutzte Ansätze
- Anforderungen an zu entwickelnde Ansätze

Mit den gewählten Kriterien sollte das Ziel zur Entwicklung eines Ansatzes zur Identifikation und Dokumentation von IT-Anwendungen, welche der offiziellen IT-Infrastruktur des Unternehmens unbekannt sind, erreicht werden.

Zuerst wurden die Interviewpartner hinsichtlich der Identifikation und der Beschreibung von Schatten-IT entlang der Prozessschritte im Fachbereich befragt. Alle bestätigten die Existenz von Schatten-IT Anwendungen in unterschiedlichen Bereichen des Unternehmens (s. Abbildung 3). Es konnte evaluiert werden, dass die identifizierten Anwendungen nicht untersagt wurden. Stattdessen bewerteten die Unternehmen die Anwendungen hinsichtlich der Kriterien:

- Qualität
- Relevanz

Das Aufkommen ist unter anderem auf unerfüllte Anforderungen der Mitarbeitenden zurückzuführen. Es stellte sich heraus, dass die Anwendungen auf unterschiedlichen technischen Grundlagen basieren, aufgrund von nicht zur Verfügung gestellten oder veralteten Lösungen seitens der zentralen IT-Abteilung. Daneben beschafften sich einige Mitarbeitende externe Softwarelösungen, welche lokal installiert und direkt genutzt wurden. Weiterhin ergaben die Experteninterviews Einblicke in die komplexen Lösungen der Fachbereiche, bei denen extra Prozesse für Hardware und Software eingeführt wurden.

Aktuell gibt es bei den befragten Unternehmen kein genau definiertes Vorgehen zur Identifikation und Kontrolle von Schatten-IT. Viele der Schatten-IT-Systeme konnten erst aufgrund von auftretenden Fehlern oder Problemen durch die IT-Abteilung festgestellt werden. Jedoch beschreiben die Fachabteilungen erste Ansätze, wie das Sensibilisieren der Geschäftsführung und der Mitarbeitenden für Schatten-IT-Themen. Außerdem werden durch die IT-Abteilung Kanäle angeboten, in denen Mitarbeitende ihr Anliegen (infrastruktur- und applikationsseitig) einsteuern können.

In einigen Fällen wurde die Qualität der somit identifizierten Schatten-IT Lösung der Mitarbeitenden in der technischen Umsetzung der Systeme als profitabel angesehen, sodass diese zugelassen wurden. Jedoch ist in vielen anderen Fällen wegen der ungeplanten Vorgehensweise das Risiko für die Vertraulichkeit unternehmensinterner Informationen, Compliance und die Integrität von Entscheidungen zu hoch. Falls ein solches Sicherheitsrisiko festgestellt wird, finden Aufklärungsgespräche statt. Weiterhin ist die Dokumentation eine der größten zu bewältigenden Herausforderungen. Wegen der fehlenden bzw. mangelnden Dokumentation und fehlender Revisionsicherheit besteht generell eine erhebliche Abhängigkeit von den Entwicklern der Systeme. Daher wird die Qualität der Lösung von der IT-Abteilung des Öfteren als technisch nicht anwendbar eingestuft, sodass die Relevanz nicht vollumfänglich eingeschätzt werden kann.

Die Interviewpartner erwarteten ein Vorgehen, mit dem die Identifikation von Schatten-IT-Anwendungen bereits in den frühen Stadien stattfindet, bevor ein Sicherheitsrisiko entsteht. Außerdem sollen die Kreativität und die Motivation der Mitarbeitenden nicht begrenzt oder untersagt werden, vielmehr soll ein Mittelweg gefunden werden. Die aus den Fallstudien gewonnenen Erkenntnisse dienen im nächsten Schritt für die Analyse und Bewertung der Chancen und Risiken.

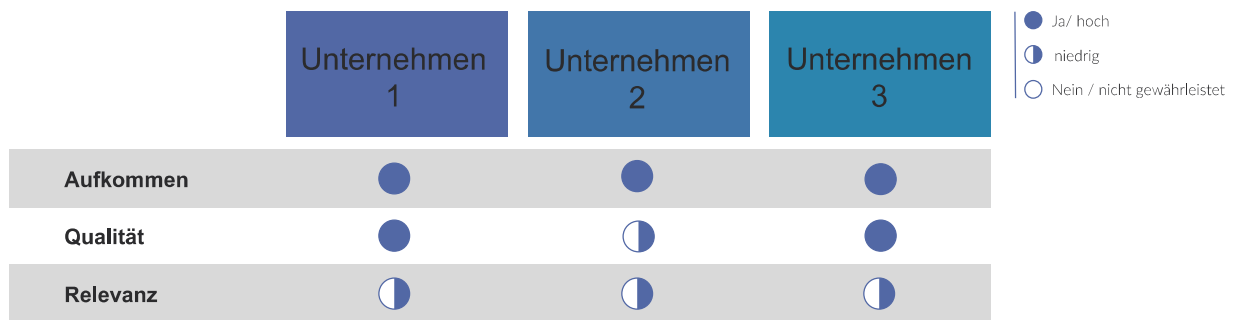


Abbildung 3: Bewertung der Fallstudien (subjektiv) (eigene Darstellung)

3.1.4 Vorgehen zur Identifikation von Schatten-IT

Für die aufwandsarme Identifikation von Schatten-IT wurde im Arbeitspaket ein standardisierter Leitfaden zur Befragung von Fachbereichen (s. Anhang 1) als auch eine Dokumentationshilfe (s. Anhang 2) entwickelt. Wie die Literaturrecherche und Expertengespräche aufzeigen, entstehen die meisten Schatten-IT-Anwendungen hauptsächlich aufgrund von Anforderungen, welche die IT-Abteilung nicht erfüllt oder veralteten und zu lang dauernden Entscheidungs- und Bewilligungswegen für formelle Lösungen in Abstimmungsprozessen mit der IT-Abteilung. Die Fachbereiche entwickeln sich ihre eigenen IT-Lösungen, wodurch sie flexibler und produktiver sind. Doch aufgrund der mangelnden Transparenz und Professionalität stellen die meisten Schatten-IT-Anwendungen ein Risiko für das Unternehmen dar. Mit dem beschriebenen Vorgehen können Unternehmen Schatten-IT-Vorkommnisse ermitteln.

Im Allgemeinen sind die Methoden zur Identifikation nicht kostenaufwendig, können jedoch zeitaufwendig sein. Daher empfiehlt es sich nach dem Feedback des pbAs, an Leitfäden festzuhalten und diese zu befolgen. Für eine systematische Erfassung von Schatten-IT sollte weiterhin zunächst ein Sicherheitslevel für Schatten-IT, welche durch die IT-Abteilung, die Führungskräfte und den Mitarbeitenden erarbeitet wird, erstellt werden. Außerdem ist das Festlegen eines IT-Beschaffungsprozesses für die Transparenz gegenüber der IT-Abteilung essenziell. Hinzu kommt die Aufklärung der Mitarbeitenden über die Risiken von Schatten-IT, damit die unregelmäßige Entstehung verhindert wird. Nachdem die Schatten-IT-Anwendungen im Unternehmen identifiziert

wurden, sollte eine Bewertung nach der in den weiteren Arbeitspaketen entwickelten Bewertungsmethodik stattfinden.

Die Identifikationsansätze bilden die Grundlage für die weiteren Arbeitspakete und beschreiben den Betrachtungsbereich bei KMU.

.

3.2 Arbeitspaket 2: Risiken und Nutzenaspekte identifizieren und quantifizieren

Das zweite Arbeitspaket diente dem Ziel, ein praxisnahes Vorgehen zur Aufdeckung sowie Bewertung der Risiken und Nutzenaspekte von identifizierter Schatten-IT zu entwickeln. Mit besonderem Fokus auf KMU sollte damit eine aufwandsarme, aber systematische Bewertung von Schatten-IT ermöglicht werden. Die Bearbeitung des Arbeitspakets erfolgte im Wesentlichen in sieben Arbeitsschritten, wie in Abbildung 4 grafisch dargestellt. In Kapitel 3.2.1. wurden relevante Risiken und Nutzenaspekte von Schatten-IT klassifiziert und zunächst auch die aktuelle Relevanz der Thematik betrachtet (s. Kapitel 3.2.2). Die Risiken und Nutzenaspekte von Schatten-IT wurden dabei systematisch mithilfe der Literatur identifiziert und mit den Mitgliedern des pbAs validiert (s. Kapitel 3.2.3). In Kapitel 3.2.4 wurden verschiedene Methoden zur Identifikation, Analyse und Bewertung von IT-Risiken ermittelt und im Rahmen von Fallstudien auf ihre Eignung zur Bewertung von Schatten-IT hin überprüft (s. Kapitel 3.2.6). Auf Basis der Ergebnisse wurde in Kapitel 3.2.7 eine Bewertungsmetrik für Schatten-IT entwickelt, die eine Nutzwert- und Risikoanalyse sowie weitere Bewertungskriterien umfasst. Die Bewertungsmetrik wurde anschließend mittels Fallstudien erprobt (s. Kapitel 3.2.7).

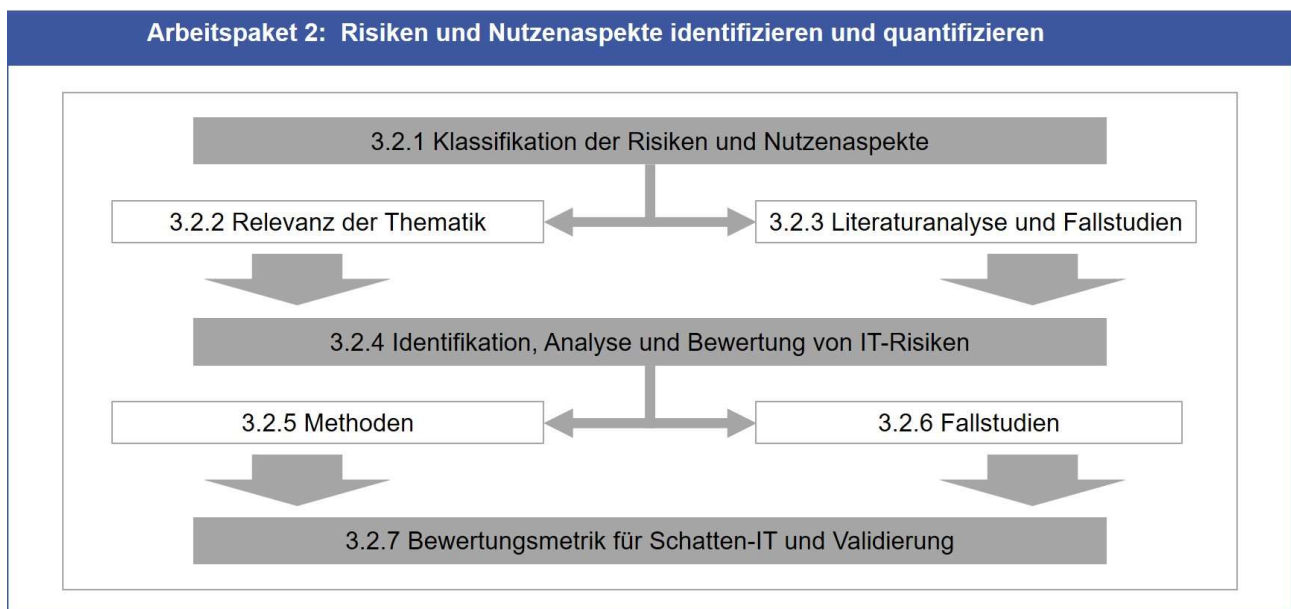


Abbildung 4: Vorgehen in Arbeitspaket 2 (eigene Darstellung)

3.2.1 Klassifikation der Risiken und Nutzenaspekte

Als Vorarbeit erfolgte zunächst die Recherche zur aktuellen Relevanz der Thematik (s. Kapitel 3.2.2). Im nächsten Schritt wurde eine systematische Literaturanalyse zur Identifikation sowie Klassifikation der Risiken und Nutzenaspekte von Schatten-IT durchgeführt und im Rahmen von Experteninterviews mit Praxispartnern des pbAs validiert (s. Kapitel 3.2.3).

3.2.2 Aktuelle Relevanz der Thematik

Im deutschsprachigen Raum war bereits jedes zweite KMU aus dem verarbeitenden Gewerbe ein Opfer von Wirtschaftsspionage oder Konkurrenzausspähung (s. Bollhöfer u. Jäger 2018). Während Firewalls, Anti-Spam-Filter oder Virens Scanner weit verbreitet sind, fehlen Datensicherungskonzepte und effektive Präventionsstrategien vor allem in kleinen Unternehmen. Das Mitbringen und Nutzen privater Geräte für Unternehmenszwecke ist selten reguliert und Penetrationstests werden nur in den wenigsten Fällen durchgeführt. Des Weiteren werden unternehmensinterne Abläufe

unzureichend überwacht. So bleibt das Kopieren großer Datenmengen unbeobachtet, Datenabflüsse werden nicht überprüft und Anomalien in der IT-Infrastruktur werden nicht entdeckt (s. Bollhöfer u. Jäger 2018). Sowohl das Fehlen von Strategien im Umgang mit Unternehmensdaten als auch das versäumte Monitoring bieten Lücken für die Entstehung von Schatten-IT. Die aktuell zunehmende, pandemiebedingte Verlagerung des Arbeitsplatzes in das Homeoffice verstärkt diese Problematik und erschwert das Auffinden nicht-autorisierter IT Anwendungen (s. McAfee 2020). Die Verwendung solcher Schatten-IT-Anwendungen birgt durch die fehlende Integration in die zentrale IT wiederum spezifische Risiken bezüglich der Datensicherheit, Compliance und Prozessrobustheit (s. Haag u. Eckhardt 2017).

Die Risiken durch den Gebrauch von Schatten-IT werden von Unternehmen häufig unterschätzt (s. Rentrop u. Zimmermann 2015). Dennoch ist das strikte Verbot oder Verhindern von Schatten-IT entgegen der Ergebnisse früherer Forschung nicht mehr zielführend (s. Brenner et al. 2011). Um wettbewerbsfähig zu bleiben, gilt es gerade für KMU, Innovationspotenziale auszuschöpfen und Chancen, die durch Schatten-IT entstehen, entsprechend zu nutzen (s. Horváth 2017). Der Nutzen von Schatten-IT manifestiert sich beispielsweise in mitarbeitendengetriebenen Innovationen oder einer gesteigerten Produktivität (s. Walterbusch et al. 2014; Zimmermann 2018). Eine differenzierte Herangehensweise für den Umgang mit Schatten-IT ist deshalb erforderlich. Die Identifikation sowie Bewertung wesentlicher Risiken und Nutzenaspekte von Schatten-IT ist die Grundlage für solch einen kontrollierten Umgang. Aufgrund mangelnder Ressourcen fehlt es gerade KMU an einem Vorgehen zur aufwandsarmen Identifikation sowie Bewertung der Risiken und Nutzenaspekte von Schatten-IT (s. Kardel 2011). In der Forschungs- und Praxisliteratur werden zudem nur Teilaspekte von Schatten-IT wie Entstehungsgründe oder Governance-Themen betrachtet. Konkrete Risiken und Nutzenaspekte, die sich aus dem Gebrauch von Schatten-IT ergeben, sind bisher nicht in übersichtlicher Weise erarbeitet. Die Risiken und Nutzenaspekte von Schatten-IT wurden deshalb im Rahmen einer systematischen Literaturanalyse identifiziert sowie klassifiziert und anschließend mit Experten aus der Unternehmenspraxis validiert.

3.2.3 Literaturanalyse und Fallstudien

Im folgenden Abschnitt wird zunächst der Prozess der Literaturanalyse erläutert. Anschließend werden ein Literaturüberblick skizziert sowie die Ergebnisse der Literaturanalyse in Form einer Klassifikation der Risiken und Nutzenaspekte von Schatten-IT dargestellt. Die Begriffe Chancen und Nutzenaspekte von Schatten-IT werden im weiteren Verlauf synonym verwendet.

Prozess der Literaturanalyse

Die Literaturanalyse setzte sich aus der Recherche in Datenbanken und wissenschaftlichen Zeitschriften sowie durch eine Schlagwortsuche und Vorwärts-Rückwärts-Analyse zusammen. Auf Basis des Titels, Abstracts oder des Volltexts wurden die gefundenen Veröffentlichungen anschließend inhaltlich evaluiert. Weitere Qualitätskriterien wie Aktualität (Jahr der Veröffentlichung), thematischer Zusammenhang (Forschungsfeld) oder Ort (Veröffentlichungsort) wurden zur Evaluation und Reduktion der Datenbasis herangezogen (s. Abbildung 5).



Abbildung 5: Prozess der Literaturrecherche und -evaluation (eigene Darstellung)

Neben den Online-Bibliotheken Scopus, IEEE Explore und Springer Link wurde die Suchmaschine Google Scholar genutzt. Die Wahl der Suchbegriffe ist aufgrund der synonymen Verwendung verschiedener deutsch- und englischsprachiger Begriffe für Schatten-IT wie *versteckte IT*, *graue IT*, *rogue IT*, *IT artefact*, *unofficial project* nicht eindeutig. Im Rahmen dieser Literaturrecherche wurden die Begriffe *Schatten-IT* und *shadow-IT* als zielführend eingestuft. Die Suchstrings wurden zudem mit dem UND-Konnektor um die Begriffe *Chance* und *Risiko* beziehungsweise *Nutzen* und *Risiko* respektive um die Stichworte *benefits*, *opportunities* und *risks* erweitert (s. Abbildung 6).

Scopus	(TITLE-ABS-KEY („shadow it“ AND risk AND benefits) OR TITLE-ABS-KEY („shadow it“ AND risk AND opportunities))
IEEE Explore	(((„Abstract“:shadow IT) AND „Abstract“:risk) AND „Abstract“:benefits) OR (((„Abstract“:shadow IT) AND „Abstract“:risk) AND „Abstract“:opportunities)
Springer Link	(Nutzen AND Risiko AND „Schatten IT“) OR (Chancen AND Risiko AND „Schatten IT“) OR (risks AND benefits AND „shadow it“) OR (risks AND opportunities AND „shadow it“)
Google Scholar	<ol style="list-style-type: none"> allintitle: Nutzen OR Risiko OR Chancen „Schatten IT“ allintitle: risks OR benefits OR opportunities „shadow IT“

Abbildung 6: Suchstrings für die verschiedenen Datenbanken (eigene Darstellung)

Über eine stufenweise Evaluation und Reduktion, bspw. durch die Einschränkung auf die Disziplinen *Computer Science* und *Business and Management*, wurde die Datenbasis schließlich auf 20 relevante Quellen reduziert. Durch die Dopplung mehrerer Veröffentlichungen in zwei oder mehr Datenbanken ist die folgende Grafik als zeitliche Abfolge von links nach rechts zu verstehen (s. Abbildung 7).

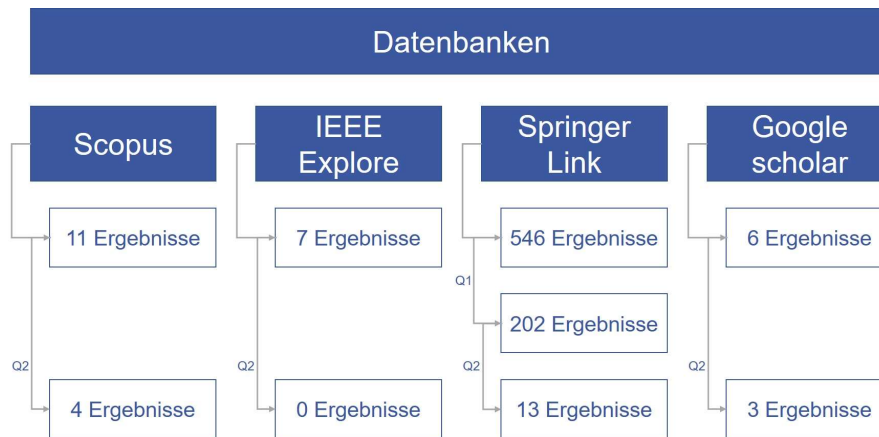


Abbildung 7: Suchergebnisse in den verschiedenen Datenbanken (eigene Darstellung)

Mittels einer Vorwärts-Rückwärts-Analyse wurden bisher nicht integrierte Quellen identifiziert. Darüber hinaus wurden die Publikationen der aus der Datenbankanalyse oft hervorgehenden Autoren Christopher Rentrop und Stephan Zimmermann detaillierter betrachtet. Auf diese Weise ergaben sich weitere neun Quellen, sodass insgesamt 29 Quellen auf Risiken und Nutzenaspekte der Nutzung von Schatten-IT hin analysiert wurden.

Literaturüberblick und Zwischenfazit

Die Forschung im Themenkomplex Schatten-IT wird generell aus vielen verschiedenen Richtungen getrieben. Häufig werden Faktoren und Motivatoren für die Entstehung von Schatten-IT betrachtet (s. Chua et al. 2014; Kopper u. Westner 2016; Rentrop u. Zimmermann 2015) oder Governance-Aspekte beleuchtet (s. Hoff 2015; Reinheimer u. Robra-Bissantz 2014; Walterbusch et al. 2014; Zimmermann 2018).

In der Literatur lassen sich zudem viele verschiedene Aspekte der Risiken und Nutzenaspekte von Schatten-IT finden. Eine Klassifikation dieser lag bis zum Zeitpunkt der Literaturanalyse nicht vor. Die Chancen und Risiken wurden deshalb in wenige, übersichtliche und distinkte Kategorien klassifiziert. Eine Klassifikation baut im Gegensatz zur Typisierung auf einem konstituierenden Merkmal auf und wird durch detaillierende Merkmalsausprägungen spezifiziert. Als Teil der analytischen Forschungsmethoden hat sie das primäre Ziel der „systematische[n] Ordnung einer Menge von Untersuchungsobjekten“ (Welter 2006). Die aus der Literatur identifizierten Chancen und Risiken stellen dabei die Untersuchungsobjekte dar. Es wurden demnach zwei Klassifikationen angestrebt – eine der Chancen und eine der Risiken. Die Klassifikation erfolgte nach dem konstituierenden Merkmal *Wirkungsbereich* – also anhand des unternehmensspezifischen Bereichs, in dem sich das Risiko oder der jeweilige Nutzen der Schatten-IT manifestiert. Die detaillierenden Merkmalsausprägungen bilden die zugeordneten Chancen und Risiken innerhalb der Klassen.

Klassifikation der Nutzenaspekte von Schatten-IT

Im Zuge der Literaturanalyse wurden 13 Chancen bzw. Nutzenaspekte von Schatten-IT identifiziert. Nach ihrem Wirkungsbereich wurden die Chancen in die Klassen *abteilungsinternen Prozesse*, *IT-Landschaft*, *personale Arbeitsumgebung* und *individuelle Kompetenzen* gruppiert (s. Abbildung 8).

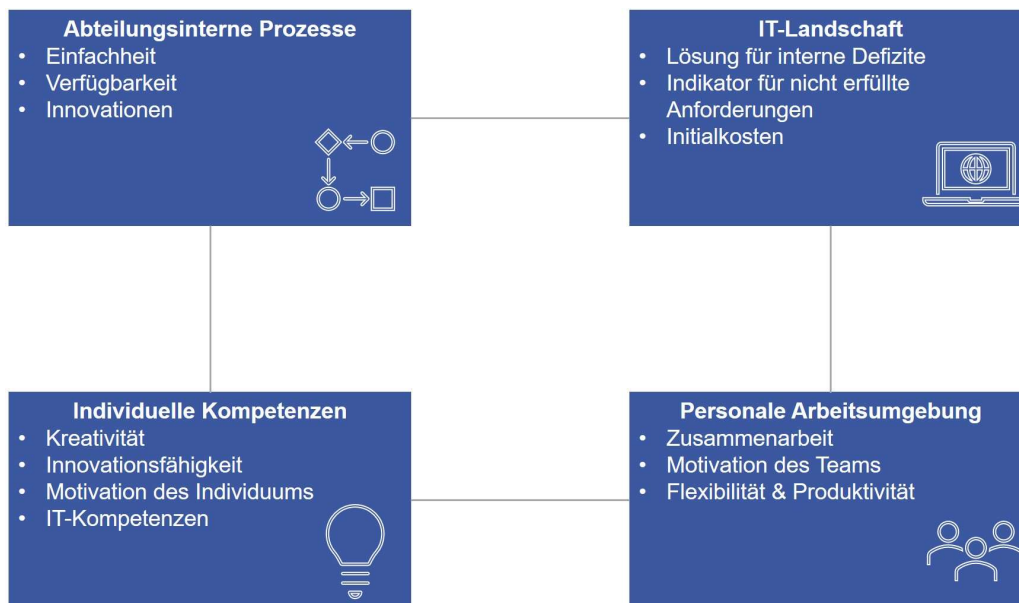


Abbildung 8: Klassen der Nutzenaspekte von Schatten-IT nach Wirkungsbereich (eigene Darstellung)

Der Wirkungsbereich **Abteilungsinterne Prozesse** umfasst diejenigen Chancen, die einen unmittelbaren Einfluss auf die Prozesse in den Fachabteilungen haben. Dazu zählt die *Einfachheit* von Schatten-IT, denn mit dieser werden in den Fachabteilungen häufig Prozesse umgangen. Die Schatten-IT Lösung stellt dann eine einfachere Abkürzung in einem Arbeitsprozess dar (s. Rains 2015). Zudem ist Schatten-IT häufig *schneller verfügbar*, da sie in Eigenregie und ohne unternehmensweite Prüfung sowie Genehmigung eingeführt wird, wodurch ein zeitlicher Vorteil entsteht. Die Time-to-Market der offiziellen IT-Abteilung ist aufgrund von hoher Auslastung und Qualitätsrichtlinien meist deutlich länger (s. Brenner et al. 2011). Schatten-IT kann darüber hinaus eine *Innovation* darstellen, indem ein alter, zentral genehmigter Prozess durch eine neuartige und fortschrittliche Lösung ersetzt wird (s. Behrens 2009; Kopper u. Westner 2016; Zimmermann 2018)).

Im Wirkungsbereich **IT-Landschaft** sind Chancen gebündelt, die über die Grenzen der nutzenden Fachabteilung hinweg die gesamte IT-Landschaft des Unternehmens beeinflussen. So kann Schatten-IT eine *Lösung für interne Defizite* des zentralen IT-Systems darstellen und als *Indikator für nicht erfüllte Anforderungen* der Fachabteilungen dienen (s. Huber et al. 2017; Urbach u. Ahlemann 2016; Rains 2015). Weiterhin sind bei Schatten-IT-Anwendungen die *Initialkosten* durch die dezentrale Einführung und den fehlenden Genehmigungsprozess deutlich geringer (s. Huber et al. 2017).

Im Kontext der **personalen Arbeitsumgebung** sind jene Chancen gemeint, die das soziale Miteinander in den Fachabteilungen betreffen. Konkret kann Schatten-IT die *Zusammenarbeit* in der Fachabteilung verbessern. Das gemeinsame Erarbeiten einer Lösung für ein akut auftretendes Problem fokussiert die einzelnen Mitarbeitenden auf ein gemeinsames Ziel. Die Mitarbeitenden ziehen an einem Strang, der Austausch untereinander wird verbessert und die *Motivation* des Teams gesteigert (s. Hoff 2015). Stellt die Schatten-IT eine effiziente Lösung für ein intern auftretendes Problem oder Defizit dar, wird außerdem die *Produktivität* der Fachabteilung erhöht. Die Lösung behebt ein existierendes Problem oder verbessert einen Prozessschritt. Durch die Schatten-IT als schnelle und einfache Alternative wird die Fachabteilung zudem *flexibler* (s. Kopper u. Westner 2016; Urbach u. Ahlemann 2016).

Der Wirkungsbereich der **individuellen Kompetenz** klassifiziert die Chancen, welche unmittelbar den einzelnen Mitarbeitenden betreffen. Dazu zählt, dass bei der Entstehung von Schatten-IT als

aktiver Problemlöseprozess der einzelne Mitarbeitende in seiner *Kreativität* gefordert wird (s. Behrens 2009; Myers et al. 2017). Im gleichen Zug wird die *Innovationsfähigkeit* der Mitarbeitenden trainiert, da eine innovative Lösung für ein auftretendes Problem entwickelt wird (s. Dehning 2016). Die erfolgreiche und eigenständige Problemlösung steigert wiederum die *Motivation* des Einzelnen. Da Schatten-IT per se eine Anwendung im Rahmen der IT darstellt, fördert die Auseinandersetzung mit solchen Themen schlussendlich auch die *IT-Kompetenz* der Mitarbeitenden (s. Reinheimer u. Robra-Bissantz 2014).

Klassifikation der Risiken von Schatten-IT

Basierend auf der Literaturanalyse wurden neben den aufgeführten Chancen ebenfalls elf Risiken identifiziert. Nach ihrem Wirkungsbereich wurden die Risiken in die Klassen *Unternehmensinfrastruktur*, *IT-Landschaft* und *individuelle Arbeitseinstellung* systematisiert (s. Abbildung 9).

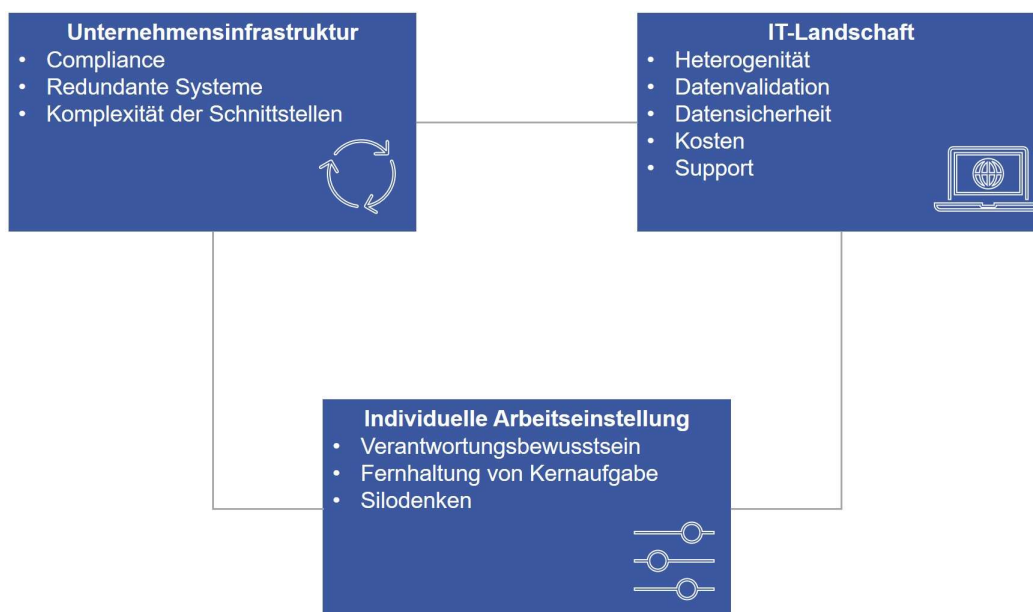


Abbildung 9: Klassen der Risiken von Schatten-IT nach Wirkungsbereich (eigene Darstellung)

In der Klasse **Unternehmensinfrastruktur** werden alle Risiken von Schatten-IT gruppiert, die die gesamte Wertschöpfungskette nach Porter beeinflussen (s. Porter 1998). Ein Risiko betrifft die unternehmensweite *Compliance*, welche das Befolgen gesetzlicher wie auch unternehmensinterner Vorschriften und Richtlinien umfasst. Die Einhaltung dieser Regeln, ob gesetzlich, intern oder aus Zertifizierungen stammend, kann beim Gebrauch von Schatten-IT nicht mehr gewährleistet werden. Die Natur solcher Systeme als im Schatten liegend impliziert die fehlende Möglichkeit zur Kontrolle und Überwachung. Die Folgen der Nicht-Einhaltung von Compliance-Richtlinien für das Unternehmen sind vielfältig. So sind beispielsweise rechtliche Folgen bei Verstößen gegen Datenschutzgesetze denkbar. Da Schatten-IT häufig eine Ersatzlösung darstellt, werden teils *redundante Systeme* geschaffen. Die Ausführung einer Aufgabe oder eines Prozessschrittes ist auf zwei Wegen möglich – die Systeme sind redundant. Schon die Begrifflichkeit der Redundanz impliziert die Überflüssigkeit eines dieser Systeme (s. Brenner et al. 2011; Silic u. Back 2014). Bei der Einführung von Schatten-IT entstehen zudem neue Schnittstellen, die nicht zentral betreut werden, was wiederum die *Komplexität der Schnittstellen* erhöht. Die Schnittstelle von bzw. hin zur jeweiligen Schatten-IT Lösung ist nicht an den Rest des Prozesses angepasst. Die Prozesse innerhalb des Unternehmens sind in Folge nicht mehr robust, da ein reibungsloser Ablauf und Durchlauf von Informationen oder Daten über mehrere Schnittstellen hinweg nicht mehr

gewährleistet werden kann. Ein mögliches Folgeszenario ist die Unterbrechung gesamter und kritischer Geschäftsprozesse (s. Hoff 2015; Huber et al. 2017).

Im Wirkungsbereich der **IT-Landschaft** sind analog zu den Chancen jene Risiken klassifiziert, die speziell die IT-Landschaft des Unternehmens betreffen. Die Integration von Schatten-IT Lösungen, die nicht von zentraler Stelle eingebunden werden, erhöht beispielsweise die *Heterogenität* der IT-Systemlandschaft. Eine heterogene IT-Landschaft führt grundsätzlich zu Ineffizienzen und verpassten Synergieeffekten. Außerdem kann die *Datenkonsistenz* und *-validität* durch die fehlende Kontrolle im Rahmen von Schatten-IT Anwendungen nicht mehr gewährleistet werden. Die Herkunft und Entstehung der Daten ist häufig schwer nachzuvollziehen, sodass im schlimmsten Fall auf Basis veralteter Daten falsche Schlussfolgerungen abgeleitet und Entscheidungen getroffen werden (s. Rentrop u. Zimmermann 2015). Durch den Einsatz von Schatten-IT entstehen zudem Gefahren bezüglich der *Datensicherheit*. Diese beinhaltet im Gegensatz zum Datenschutz nicht nur personenbezogene Daten, sondern alle unternehmensbezogenen und schützenswerten Daten. Ziel der Datensicherheit ist das Schützen aller Daten vor dem unbefugten Zugriff Dritter. Die Anforderungen an die Datensicherheit werden in die drei Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit unterteilt (s. Kapitel 3.2.7). Schatten-IT durchläuft in der Regel keine Sicherheits- oder Qualitätsprüfung und beinhaltet kaum Authentifizierungsmaßnahmen, was das Risiko eines Datenzugriffs durch Unbefugte maßgeblich erhöht. Der wirtschaftliche Schaden durch unbefugtes Abgreifen, Verändern oder Entfernen von sensiblen Daten ist a priori nur schwer zu beziffern (s. Fürstenau et al. 2017; Huber et al. 2017; Myers et al. 2017). Als finanzielles Risiko sind darüber hinaus die zum Teil versteckten *laufenden Kosten* von Schatten-IT zu nennen. Die anfallenden Kosten werden nicht in der IT-Budgetierung erfasst und sind demnach nicht plan- oder kontrollierbar. Zusätzlich kann der nachträgliche Integrationsaufwand offengelegter Schatten-Lösungen hohe Kosten verursachen (s. Myers et al. 2017). Im Zusammenhang mit Schatten-IT ist überdies kein durchgängiger *Support* gegeben. Es fehlt die Dokumentation des Systems. Im Worst Case kann dies zu Schwierigkeiten, Hindernissen oder Ausfällen im Geschäftsablauf führen. Das „Hit-by-a-Bus-Szenario“ stellt eine Situation dar, in der Entwickler und Entwicklerinnen und der Nutzerkreis der Schatten-IT plötzlich nicht mehr verfügbar sind und somit die Funktionalität des Systems verloren geht. Die Schattenlösung fällt ersatzlos aus, da das Domänenwissen über die Funktionsweise und die Nutzung undokumentiert in den Händen einer einzigen Person existiert (s. Behrens 2009).

Zuletzt kann auch die **individuelle Arbeitseinstellung** negativ von Schatten-IT beeinflusst werden. Hier ist das häufig fehlende *Verantwortungsbewusstsein* bei der leichtfertigen Entwicklung einer Schatten-IT-Anwendung problematisch. Die Tragweite der Entscheidung zur Schatten-IT wird von den einzelnen Mitarbeitenden meist unterschätzt und die möglichen Folgen werden nicht durchdacht (s. Walterbusch et al. 2014). Die Entwicklung von Schatten-IT ist außerdem nicht Teil des Aufgabenbereichs des betroffenen Mitarbeitenden, sodass dieser von seinen *Kernaufgaben ferngehalten* wird. Dies hat möglicherweise eine Minderung der Arbeitsleistung zur Folge (s. Dehning 2016). Im Zusammenhang mit Schatten-IT sind Beteiligte zudem oft von *Silodenken* geprägt, also von einer gedanklichen Fokussierung der Einzelnen auf die eigene Abteilung als abgeschlossener Bereich. In einer Fachabteilung wird, ohne Schnittstellen zu anderen Fachabteilungen zu bedenken oder unternehmensweite Sichtweisen einzunehmen, eine Schatten-IT-Lösung entwickelt. Schatten-IT fördert solch ein Silodenken, da ihr Fokus natürlicherweise auf den Fachabteilungen liegt. Dies führt weiterhin zu Frontenbildung innerhalb des Unternehmens. Während die Fachabteilungen in solchen Lösungen die Steigerung der eigenen (unternehmensdienlichen) Produktivität sehen, fokussiert die zentrale IT oder das Management die einhergehenden Risiken. Schatten-IT als Förderer von Silodenken schadet also letztendlich dem Betriebsklima (s. Fürstenau et al. 2017).

Fallstudien

Im Rahmen von fünf Fallstudien in Form von halbstandardisierten Experteninterviews mit unterschiedlichen Unternehmen des pbAs, wurden die identifizierten Risiken und Nutzenaspekte von Schatten-IT validiert und auf ihre Praxisrelevanz hin überprüft.

Tabelle 2: Übersicht der Fallstudien

#	Branche	Interviewpartner	Datum
1	Mechatronik- und Kunststofftechnik	Stellvertretender IT-Leiter	23.03.2021
2	Nahrungsmittelproduktion	IT-Spezialist	24.04.2021
3	IT-Dienstleistung	Geschäftsführer	26.03.2021
4	Antriebstechnik	IT-Leiter	13.04.2021
5	Textilmaschinen	Head of Group IT and Organization	20.04.2021

Die Interviews basierten auf einem Leitfaden mit vorformulierten, aber dennoch offenen Fragen (s. Anhang 3). Es wurde jedoch auch auf die jeweiligen Impulse der Interviewpartner eingegangen, um keine relevanten Informationen auszuschließen. Der Interviewleitfaden umfasste neben einem einführenden Abschnitt zu Hintergrundinformationen über den Interviewpartner und das Unternehmen die drei Themenblöcke *Bisherige Erfahrungen mit Risiken und Nutzen von Schatten-IT*, *Nutzen von Schatten-IT* und *Risiken von Schatten-IT*. Dabei wurde speziell auf die generelle Risiko- und Nutzenwahrnehmung sowie Erfahrungen der Interviewpartner mit besonders kritischer oder nützlicher Schatten-IT eingegangen. Der vierte Themenblock umfasste die Validierung der *Ansätze zur Identifikation, Analyse und Bewertung der Risiken sowie Nutzenaspekte von Schatten-IT*, worauf im späteren Verlauf eingegangen wird (s. Kapitel 3.2.6).

Ergebnisse der Fallstudien: Risiko und Nutzen von Schatten-IT in der Unternehmenspraxis

Generell wurden das Thema Schatten-IT sowie deren Risiken und Nutzenpotenzial über alle Experteninterviews hinweg als brisant und relevant eingestuft. Das Nutzenpotenzial von Schatten-IT wurde geringer als die dadurch entstehenden Risiken eingeschätzt (s. Tabelle 3 und Tabelle 4). Dennoch bewertet ein Großteil der Experten Schatten-IT durchaus als nutzenstiftend für ihr jeweiliges Unternehmen. Der Nutzen konzentriert sich in den Unternehmen der Praxispartner jedoch zum Großteil auf die abteilungsinternen Prozesse sowie die IT-Landschaft. Häufig wurden die Einfachheit und schnelle Verfügbarkeit von Schatten-IT-Lösungen herausgestellt. Als Beispiel aus der Praxis nannte ein Experte die Entwicklung eines Programms im Fachbereich, das das umständliche händische Ableiten eines Reports aus dem ERP-System automatisierte. Darüber hinaus löse Schatten-IT in vielen Fällen ein internes Defizit und stelle eine Lösung für einen ganz bestimmten Anwendungsfall des Nutzerkreises dar: „Was man natürlich im Kopf haben muss, ist, dass das nicht von ungefähr kommt. Die, die [Schatten-IT] nutzen, die haben einen Business-Need. Und vielleicht ist die IT auch manchmal zu langsam oder zu schwerfällig.“ (I3). Auch die häufig geringen initialen Kosten bewerten zwei der Interviewpartner als zentralen Nutzenaspekt. Dennoch wird die Kostenseite, wie auch bereits in der Literaturanalyse aufgezeigt, als ambivalent eingestuft: „Initiale Kosten sind bei Schatten-IT sehr gering oder nicht vorhanden. Kosten treten meist erst auf, wenn es darum geht, die Schatten-IT abzulösen. [...] vor allem bei der Integration von Excel-Schatten-IT kann es zu hohen Kosten kommen.“ (I3).

Tabelle 3: Relevanz der Nutzenaspekte in den befragten Unternehmen (eigene Darstellung)

Nutzenaspekte	Unternehmen				
	#1	#2	#3	#4	#5
<i>Abteilungsinterne Prozesse</i>					
Einfachheit	•	•	•		
Verfügbarkeit	•	•	•		•
Innovation					•
<i>IT-Landschaft</i>					
Lösung für interne Defizite	•		•		
Indikator für nicht erfüllte Anforderungen				•	
Initialkosten	•		•		
<i>Personale Arbeitsumgebung</i>					
Zusammenarbeit					
Motivation des Teams					
Produktivität und Flexibilität					
<i>Individuelle Kompetenzen</i>					
Kreativität					•
Innovationsfähigkeit					
Motivation des Individuums					
IT-Kompetenzen					•

• = Nennung im Experteninterview

Für einen Experten ist der Nutzen von Schatten-IT im Vergleich zu den entstehenden Risiken für das Unternehmen marginal: „Es gibt keinen Nutzen. Das Risiko ist viel höher als der Nutzen. Ein Nutzen kann da sein, wenn die Abteilung nicht genau weiß, was sie tatsächlich braucht und daher erst mal selbst etwas bastelt und dann die IT eingeschaltet wird.“ (I4). Von allen Experten genannt und priorisiert wurden Ausfallrisiken, die durch den fehlenden Support bei Schatten-IT entstehen. In diesem Zusammenhang berichteten die Praxispartner von ihren Erfahrungen mit besonders prozesskritischen Schatten-IT Anwendungen: „In unserem Unternehmen gab es ein ERP-System, das nicht wirklich auf das Unternehmen zugeschnitten war. Ein Mitarbeiter aus dem Fachbereich hat parallel dazu eine ganze Reihe an Anwendungen entwickelt, die zum Teil auf das ERP-System zugegriffen und ganz elementare Unternehmensprozesse gesteuert haben. Der Mitarbeiter war jedoch der Einzige, der wusste, wie die Applikationen funktionieren. Das ist [...] ein ganz großes Risiko.“ (I1). Ein weiteres Beispiel einer Schatten-IT zeigt, wie auf Basis veralteter und nicht hinreichend valider Daten Ineffizienzen in den Planungsprozessen entstehen können: „Die gesamte Fertigungsplanung wurde in Excel mit Makros aufgebaut – ohne die IT. Das ging dann durch mehrere Hände und irgendwann war nicht mehr klar, woher die Daten kommen und wie das zu pflegen ist. Die Fertigungsplanung war nach einer Zeit einfach falsch.“ (I4). Auch Compliance-Risiken sowie die Bedrohung der Datensicherheit des Unternehmens wurden von den Experten als äußerst relevant eingestuft. Ein Praxispartner beschrieb: „Es gibt [Schatten-IT]-Anwendungen, da steht das Admin-Passwort unverschlüsselt im Code.“ (I5). So entsteht ein massives Risiko für einen unbefugten Zugriff Dritter durch Sicherheitslücken.

Tabelle 4: Relevanz der Risiken in den befragten Unternehmen (eigene Darstellung)

Risiken	Unternehmen				
	#1	#2	#3	#4	#5
<i>Unternehmensinfrastruktur</i>					
Compliance		•	•	•	
Redundante Systeme		•			
Komplexität der Schnittstellen	•			•	
<i>IT-Landschaft</i>					
Heterogenität					
Datenvalidität	•			•	
Datensicherheit	•	•	•	•	•
Kosten	•	•	•	•	
Support	•	•	•	•	•
<i>Individuelle Arbeitseinstellung</i>					
Verantwortungsbewusstsein		•			
Fernhaltung von Kernaufgaben					
Silodenken		•	•	•	

• = Nennung im Experteninterview

Die Experteninterviews lieferten Einblicke in die Nutzen- und Risikowahrnehmung von Schatten-IT in der Unternehmenspraxis. Außerdem konnten durch die Priorisierung der Risiken und Nutzenaspekte durch die Praxispartner wertvolle Erkenntnisse in Bezug auf die entwickelte Bewertungsmetrik für Schatten-IT gewonnen werden (s. Kapitel 3.2.7).

3.2.4 Identifikation, Analyse und Bewertung von IT-Risiken

Im folgenden Abschnitt werden aus der praxisorientierten Fachliteratur ermittelte Methoden des Risikomanagements zur Identifikation, Analyse und Bewertung von IT-Risiken dargestellt. Zunächst werden grundsätzliche Begriffe des IT-Risikomanagements definiert.

Grundsätzliche Begrifflichkeiten

Im weiteren Sinne wird *Risiko* in der Literatur als „[...] Auswirkung von Ungewissheit auf Ziele [...]“ definiert (Königs 2017). Dabei bezieht sich der Begriff Risiko also sowohl auf mögliche positive als auch auf negative Auswirkungen. Im Unternehmenskontext wird jedoch meist das *engere Risiko* betrachtet, welches sich auf die Abweichung des tatsächlichen Zustands von den Unternehmenszielen bezieht. Hiernach ist das Risiko „[...] eine nach Wahrscheinlichkeit und Konsequenz bewertete Bedrohung hinsichtlich der Abweichung von erwarteten Systemzielen [...]“ (Königs 2017). Da diese Definition aber weiterhin auch positive Abweichungen beinhaltet, werden die unerwünschten Abweichungen nochmals als *Downside-Risiken* abgegrenzt. Betrachtet man das Risiko allgemein in einem Risikomodell, so zeigen sich mehrere Einflussfaktoren: Asset, Schutz, Bedrohungen, Schwachstellen und Schaden (s. Abbildung 10).

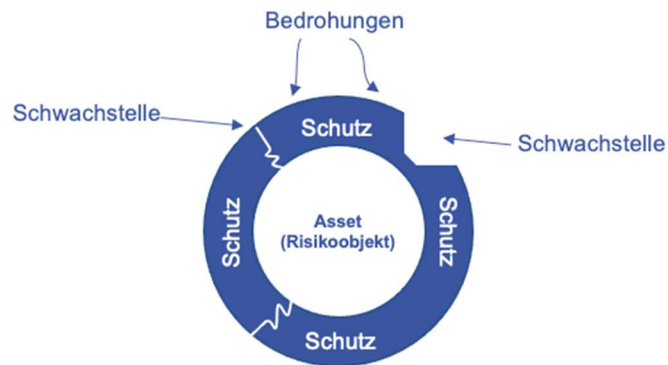


Abbildung 10: Einflussfaktoren für das Zustandekommen von Risiken (eigene Darstellung)

Das *Asset* bezeichnet hierbei das Risikoobjekt, also das zu schützende System-Ziel. Als *Schutz* werden hier die Vorkehrungen oder Sicherheitsmaßnahmen bezeichnet, um dieses Asset vor Risiken zu schützen, welche dann eintreten, wenn bestimmte *Bedrohungen* bestehen. Von einer *Schwachstelle* ist dann die Rede, wenn es für eine Bedrohung keine entsprechende Maßnahme gibt.



Abbildung 11: Beispiel eines Risikomodells (eigene Darstellung)

Im obigen Beispiel (s. Abbildung 11) wäre also ein kranker Mitarbeitender keine aktive Bedrohung für die Einhaltung einer Projekt-Deadline, da durch Maßnahmen wie Aushilfen und einen zeitlichen Puffer für genügend Schutz gesorgt ist. Existiert solch ein Schutz nicht und es tritt ein Schaden auf, wird dieser Schaden auch als *Business-Impact* bezeichnet (s. Knoll 2017).

Ein spezifisches *IT-Risiko* meint die „[...] Gefahr der Realisierung von Verlusten, die infolge der Verletzung eines oder mehrerer der Schutzziele aufgrund eines durchgeführten Angriffs unter Ausnutzung von Schwachstellen eintreten.“ (Prokein 2008). Grundlage für die Existenz eines Risikos sind folglich, wie aus den bereits genannten Definitionen hervorgeht, Ziele. Im Fall von IT-Risiken sind dies die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (s. Prokein 2008). Vertraulichkeit zielt darauf ab, dass Daten nur von Personen eingesehen, bearbeitet und verwaltet werden dürfen, die dazu befugt sind. Ziel der Integrität ist es, die Korrektheit von Daten und die korrekte Funktionsweise von den dazugehörigen Systemen zu garantieren. Das Schutzziel Verfügbarkeit hat den Anspruch, zu jeder Zeit die Funktion eines Systems zu garantieren.

3.2.5 Methoden

Identifikation von IT-Risiken

Die Identifikation von IT-Risiken stellt den ersten Schritt im Prozess des Risikomanagements dar. Ziel ist es, relevante Assets (Prozesse, IT-Systeme, Personen, Daten) sowie Risiken zu definieren, indem existierende Bedrohungen und Verwundbarkeiten (Schwachstellen) ermittelt und kategorisiert werden. Die hierfür verwendeten Methoden lassen sich in die drei Kategorien *Kollektionsmethoden*, *Kreativitätsmethoden* und *analytische Suchmethoden* einteilen.

Eine mögliche **Kollektionsmethode** ist die *Checkliste*: Dabei handelt es sich um eine Sammlung standardmäßig bekannter Schwachstellen und Angriffe, welche beispielsweise vom Bundesamt für Sicherheit in der Informationstechnik bereitgestellt werden. Da diese Checklisten eine Vielzahl an sehr konkreten Risiken beinhalten, welche jedoch kaum aggregiert sind, dienen sie als erster Ansatzpunkt für die Risikoidentifikation. Im Rahmen von Befragungstechniken sind sowohl *strukturierte Experteninterviews* als auch das *Self-Assessment* möglich. Erstere zielen darauf ab, das Wissen von internen und externen Experten zu nutzen. Die Befragung von internen Experten ist besonders nützlich, da so auch Schwachstellen identifiziert werden können, welche bislang zwar nicht zu einem Angriff geführt haben, aber dennoch risikobehaftet sind (Prokein, 2008). Self-Assessments können einerseits in Form von Online-Fragebögen, welche die jeweiligen Mitarbeitenden ausfüllen, oder durch moderierte Workshops durchgeführt werden. Beides dient dazu, sowohl das Bewusstsein der Mitarbeitenden für IT-Risiken und Bedrohungen zu stärken als auch speziell für das Unternehmen relevante Risiken zu identifizieren. Vorteil des Self-Assessments ist, dass Einschätzungen der eigenen Mitarbeitenden im Firmenumfeld meist zuverlässiger als jene von externen Experten sind (Königs, 2017). Als Basis für die *Analyse unternehmensinterner und -externer Daten* können Daten aus dem Finanz- und Rechnungswesen, aus IT-Audits sowie Log-Dateien und Computer-Protokolle genutzt werden. Abrechnungen und Bilanzen geben beispielsweise Aufschluss darüber, ob es Zahlungen für Schäden oder ähnliche Auffälligkeiten gab. Des Weiteren kann anhand von IT-Audits überprüft werden, ob die Geschäftstätigkeiten im Einklang mit Sicherheitsrichtlinien sind. Zuletzt können durch Log-Dateien IT-unterstützte Prozessabläufe überprüft werden.

Zu den **Kreativitätsmethoden** zählen das *Brainstorming* und *Brainwriting*, die beide das Ziel verfolgen, mögliche, bisher unbekannte Risiko-Szenarien zu entwickeln. Beim Brainstorming können sich Mitarbeitende frei und kreativ zu möglichen Risiken und Schwachstellen äußern. Beim Brainwriting werden die einzelnen Ideen an die anderen Teilnehmer weitergegeben, welche die Gedanken dann weiter ausführen. Bei der *Delphi-Methode* wird eine Gruppe von Experten bezüglich mehrerer risikobezogenen Faktoren befragt. Nach jeder Befragung wird der Median der Umfrage ermittelt und der Gruppe wiederum mitgeteilt. Die Experten haben dann die Möglichkeit, ihre Entscheidung erneut zu überdenken und gegebenenfalls anzupassen. Ziel des Prozesses ist es, mit der Zeit einen Konsens in der Gruppe zu finden und die einzelnen Entscheidungen dem Median näher zu bringen. Folgende beispielhafte Fragestellungen sind im Zusammenhang mit IT-Risiken sinnvoll: Welche Risiken sind möglich (Qualität)? In welchem Ausmaß treten diese auf (Quantität)? Wann treten die Risiken auf (Zeit)? Mit welcher Wahrscheinlichkeit treten diese auf (Wahrscheinlichkeit)?

Die Kategorie der **analytischen Suchmethoden** beinhaltet die Modellierung von *Bedrohungs- bzw. Angriffsbäumen*. Diese stellen konzeptionelle Diagramme dar, welche Bedrohungen auf IT-Systeme und mögliche Angriffe zur Realisierung dieser Bedrohungen nachzeichnen (s. Abbildung 12). Dabei wird von einem verletzten Schutzziel wie bspw. der Integrität ausgegangen. Für dieses Schutz- bzw.

Angriffsziel werden daraufhin verschiedene Angriffswege entwickelt. Werden hierbei Schwachstellen identifiziert, werden diese ebenfalls im Angriffsbaum aufgeführt. Für eine weiterführende Risikoanalyse kann das Modell um die Wahrscheinlichkeiten der einzelnen Angriffspfade sowie der daraus resultierenden Schäden ergänzt werden. Weitere ausgewählte Methoden der Risikoanalyse und Bewertung werden im Folgenden aufgeführt.

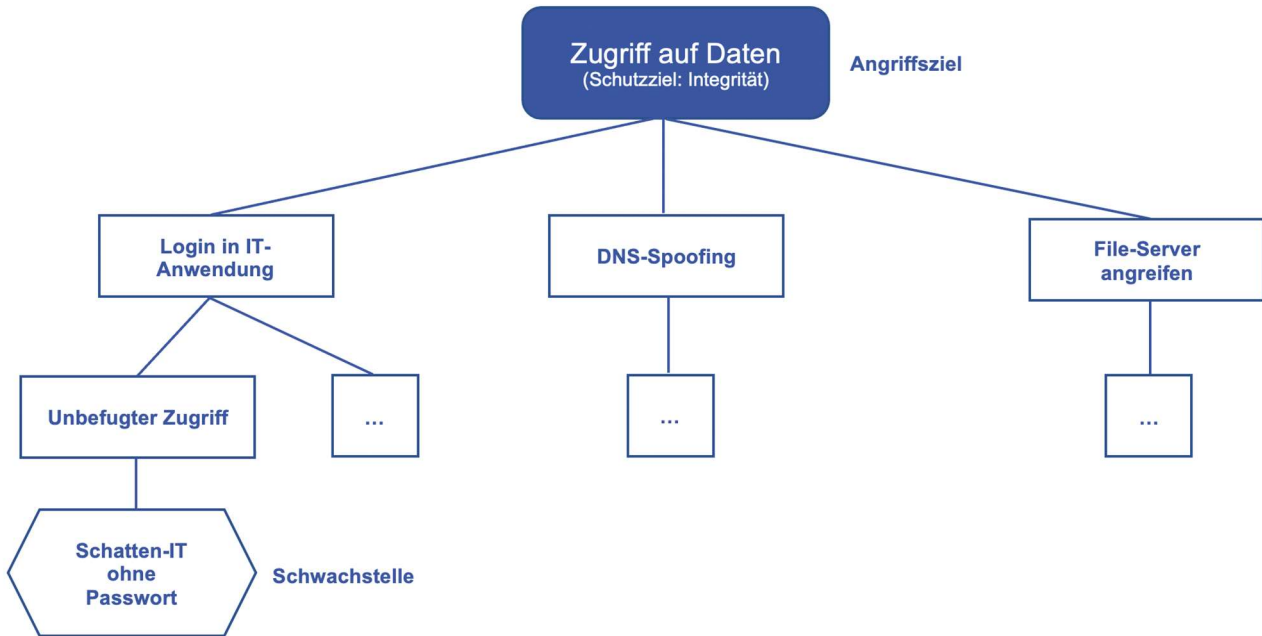


Abbildung 12: Beispiel eines Angriffsbaums (eigene Darstellung)

Analyse und Bewertung von IT-Risiken

Für ein zielführendes Risikomanagement müssen die identifizierten Risiken im nächsten Schritt *analysiert* und *bewertet* werden. Dies ist notwendig, um Risiken einschätzen sowie priorisieren zu können und bildet somit die Grundlage für Entscheidungen im Umgang mit den IT-Risiken (s. Königs 2017). Ziel der *Analyse* ist es, die Eintrittswahrscheinlichkeiten der Risiken sowie deren potenzielle Schadensauswirkung zu ermitteln. Die anschließende *Bewertung* priorisiert die Risiken nach ihrer Kritikalität (s. Königs 2017). Grundsätzlich wird dabei in *quantitative* und *qualitative* Methoden unterschieden. Erstere zielen darauf ab, numerische Werte mit realer Bedeutung zu ermitteln (s. Königs 2017). So wird die Kritikalität eines Risikos bewertet, indem das Schadensausmaß in Form von entstehenden Kosten in Euro oder Zeitverlust in Stunden beziffert wird. Ein wesentlicher Vorteil quantitativer Methoden stellt die Vergleichbarkeit der IT-Risiken mit Risiken aus anderen Unternehmensbereichen dar, in denen quantitative Risikobewertungen vorherrschend sind (s. Prokein 2008). So kann ein bestimmtes Risiko im Gesamtunternehmenskontext bewertet werden. Qualitative Methoden weisen Risiken eine geschätzte Bewertung zu, definieren also die Eintrittswahrscheinlichkeit und das Schadensausmaß näherungsweise. Grund für die Wahl einer qualitativen Risikobewertung ist, dass der Eintritt eines Schadensfalls von etlichen Bedingungen abhängt, die sich mit bedingten Wahrscheinlichkeiten nur unzureichend berechnen lassen. Die Eintrittswahrscheinlichkeit sowie das Schadensausmaß der Risiken lassen sich in der Regel besser qualitativ abschätzen. Zudem ermöglichen qualitative Methoden schnellere Entscheidungen über notwendige Maßnahmen der Risikobehandlung (s. Witt 2016).

Die *Fehlerbaumanalyse* eignet sich sowohl zur quantitativen als auch qualitativen Risikoanalyse. Ausgehend von einem Fehlerereignis wird hier deduktiv nach den ursächlichen Ereignissen gesucht, welche für das Fehlerereignis verantwortlich sind. Neben der Möglichkeit, diese Analyse sowohl top-

down als auch bottom-up durchzuführen, kann der Fehlerbaum auch durch logische Verknüpfungen wie AND-Gates als auch OR-Gates ergänzt werden. Den verschiedenen Ereignissen können numerische Werte wie beispielsweise Eintrittswahrscheinlichkeiten (s. Abbildung 13) zugewiesen und die Analyse so quantifiziert werden.

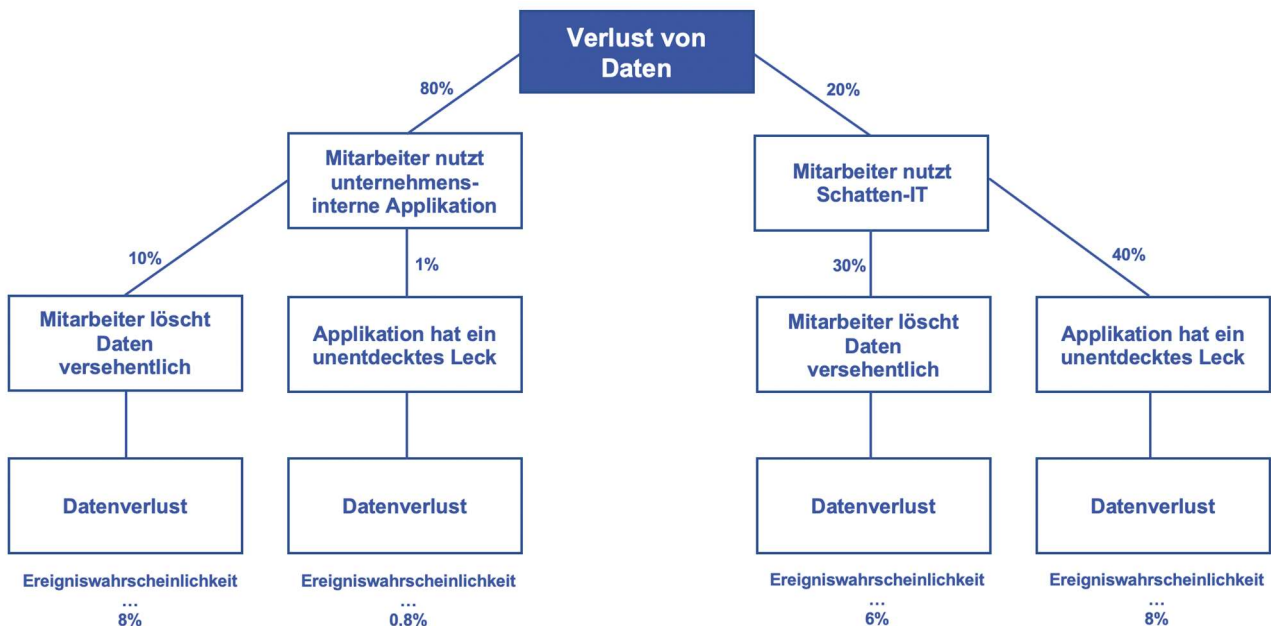


Abbildung 13: Beispiel eines Fehlerbaums einer Schatten-IT mit Wahrscheinlichkeiten (eigene Darstellung)

Eine weitere Methode zur Risikoquantifizierung stellt die *Szenarioanalyse* dar. Den Kern bildet die Ermittlung und Analyse von potenziellen Verlustereignissen durch Expertenwissen, die noch nicht unbedingt eingetreten sind, jedoch für die Zukunft als möglich und relevant für das Unternehmen eingeschätzt werden. Folglich kommen Szenarioanalysen dann zum Einsatz, wenn wenige oder überhaupt keine historischen Verlustereignisse bekannt sind. Unter dem Vorbehalt der Subjektivität der Expertenschätzungen können durch Szenarioanalysen potenzielle Verlustereignisse ermittelt werden. Zur mathematischen und statistischen Ermittlung der (un-)erwarteten Verluste müssen Experten, oftmals im Rahmen von Expertenbefragungen oder Self-Assessments, Angaben zur Verlusthöhe und -häufigkeit machen. Eine Monte-Carlo-Simulation ermöglicht dann die Abschätzung der erwarteten und unerwarteten Verluste aus dem analysierten Szenario. Charakteristisch für eine Szenarioanalyse ist, dass nicht nur ein Szenario, sondern mehrere Szenarien erstellt werden. Die erstellten Szenarien werden durch eine Zuweisung von Eintrittswahrscheinlichkeiten gewichtet und bewertet. Szenarioanalysen sind von der Qualität der subjektiven Einschätzungen abhängig. Werden nur wenige Angaben zu den Zielvariablen gemacht, ist eine exakte Quantifizierung der IT-Risiken kaum möglich.

Die *Failure Mode and Effect Analysis* (FMEA) ermittelt die Priorität eines bestimmten Risikos anhand von drei Variablen: Bedeutung des Risikos (Beurteilung anhand einer Skala von 1-10), Auftretswahrscheinlichkeit (Wahrscheinlichkeit in Prozent) und Entdeckungswahrscheinlichkeit (1 - Wahrscheinlichkeit in Prozent) (s. Abbildung 14). Je schwerer also der Fehler zu entdecken ist, desto höher das Risiko. Allerdings ist die Entdeckungswahrscheinlichkeit a priori oft nur schwer zu bestimmen und bedarf deshalb ausreichend historischer Vergleichswerte. Die Risikoprioritätszahl erlaubt zudem die Priorisierung der Risiken nach Kritikalität.

$$\text{Risikoprioritätszahl} = \text{Bedeutung} \cdot \text{Eintrittswahrscheinlichkeit} \cdot \text{Entdeckungswahrscheinlichkeit}$$

Abbildung 14: FMEA (eigene Darstellung)

Im gleichen Zug der Risikobewertung baut die sogenannte *Risikotabelle* auf der FMEA auf. Hier werden die identifizierten Risiken anhand von ihrer Risikoprioritätszahl geordnet. Unterteilt werden die Risiken dann in „akzeptierbar“ und „erfordert Maßnahmen“ (s. Tabelle 5). Neben einer gut strukturierten Auflistung aller Risiken bietet diese Methode auch eine Grundlage für die Entwicklung von Maßnahmen.

Tabelle 5: Risikotabelle (eigene Darstellung)

Risiko-Rang	Risiko-Kategorie	Auswirkung	Eintrittswahrscheinlichkeit	Risikofaktor	
1.	1	A ₁	W ₁	A ₁ *W ₁	Erfordert Maßnahmen
2.	1	A ₂	W ₂	A ₂ *W ₂	
...	
n	n	A _n	W _n	A _n *W _n	
5.	4		akzeptierbar

Die *Portfolioanalyse* zielt ebenfalls darauf ab, die Risikolandschaft anhand von Schadenseintrittswahrscheinlichkeit und Schadensausmaß in niedrige, mittlere, schwere und gravierende Risiken einzuteilen. Sie schafft somit eine übersichtliche und visuelle Darstellung der IT-Risiken in Form einer Risikomatrix (s. Abbildung 15).

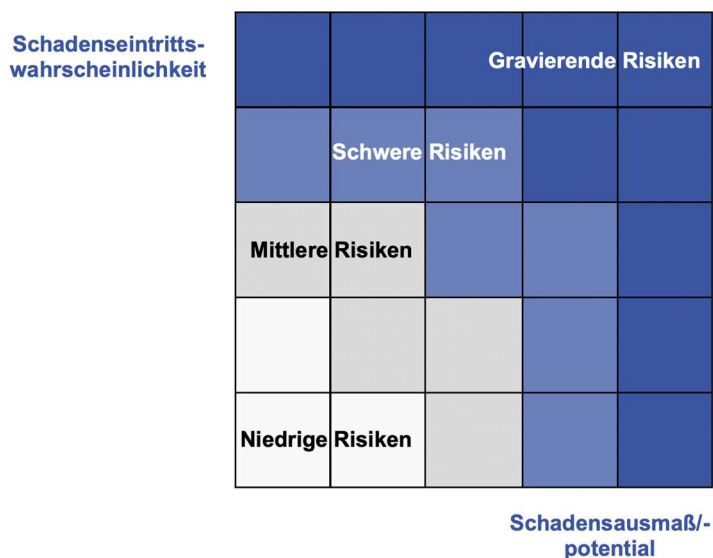


Abbildung 15: Risikomatrix (eigene Darstellung)

Die sogenannte *CIA-Analyse* (s. Tabelle 6) konzentriert sich auf die drei Schutzziele der Informationssicherheit: Vertraulichkeit (*Confidentiality*), Integrität (*Integrity*) und Verfügbarkeit (*Availability*) (s. Königs 2017). Im ersten Schritt der CIA-Analyse werden mögliche Bedrohungen wie bspw. ein unbefugter Zugriff Dritter gesammelt und tabellarisch aufgelistet. Zusätzlich wird jeder Bedrohung eine mögliche Schwachstelle (s. Kapitel 3.2.4) zugeordnet. Im darauffolgenden Schritt folgt die eigentliche Bewertung. Hier wird zuerst die Eintrittswahrscheinlichkeit der jeweiligen Bedrohung auf einer Skala von 1 bis 5 definiert. Der mögliche Schaden wird anhand der Auswirkungen auf die drei Schutzziele auf einer Skala von 1 bis 5 bewertet (s. Witt 2016).

Tabelle 6: CIA-Tabelle (eigene Darstellung)

Bedrohung	Schwachstelle	Eintrittswahrscheinlichkeit	Schaden		
			C	I	A
Datenverlust	Unentdeckte Schatten-IT	4	5	1	1
Unbefugter Zugriff	Schatten-IT ohne Passwortschutz	2	5	2	3
Viren	Schatten-IT ohne Penetrationstest	3	4	4	3

Die identifizierten Ansätze zur Identifikation, Analyse und Bewertung wurden mittels Fallstudien mit Unternehmen im Kontext von Schatten-IT als konkreter Anwendungsfall diskutiert und validiert.

3.2.6 Fallstudien

Im Rahmen der fünf halbstandardisierten Experteninterviews mit Unternehmen des pbAs zu den Risiken und Nutzenaspekten von Schatten-IT (s. Kapitel 3.2.3) wurden die eben aufgezeigten Ansätze zur Identifikation, Analyse und Bewertung der IT-Risiken auf ihre Praxistauglichkeit hin überprüft. Dabei wurde zunächst abgefragt, ob im Unternehmen generell standardisierte Ansätze zur Identifikation, Analyse und Bewertung von IT-Risiken existieren. Zudem schätzten die Praxispartner die Eignung der verschiedenen Ansätze zur Risikobeurteilung von Schatten-IT ein. Außerdem wurden mit den Experten mögliche Herangehensweisen zur Nutzenbewertung von Schatten-IT diskutiert und evaluiert. Die Erkenntnisse aus den Fallstudien bildeten die Grundlage für die Konzeption der Bewertungsmetrik für Schatten-IT (s. Kapitel 3.2.7).

Ergebnisse der Fallstudien: Ansätze zur Risiko- und Nutzenbewertung von Schatten-IT in der Unternehmenspraxis

Ein Großteil der Unternehmen verfügt nicht über einen Standardprozess zur Identifikation, Analyse und Bewertung von IT-Risiken. Selbst die größeren Unternehmen aus den Fallstudien nutzen wenig bis keine formalen Risikoanalyse-Methoden. Vieles sei „einfach auch Kopfwissen und gesunder Menschenverstand.“ (I1). Gibt es einen IT-Sicherheitsbeauftragten wird dieser bspw. bei der Anschaffung eines neuen Systems eng in den Entscheidungsprozess miteinbezogen. Im engen Austausch mit den Fachbereichen werden die systemseitigen Risiken dann anhand von Checklisten oder nach eigenem Ermessen sowie Erfahrungsschatz beurteilt (I2). Vereinzelt führen die Unternehmen Schwachstellenanalysen in Form von Penetrationstests sowohl intern als auch mit externen Dienstleistern durch (I2; I4).

Ein systematisches Vorgehen zur Bewertung von Schatten-IT existiert in keinem der befragten Unternehmen, da es meist schon an der Aufstellung bestehender Schatten-IT mangelt. Dies unterstreicht die Relevanz einer Methodik zur Aufdeckung sowie Bewertung von Schatten-IT. Eine strukturierte Bewertungsmethodik für Schatten-IT wurde von allen Experten als sinnvoll und deren Notwendigkeit als hoch eingestuft. Trotzdem sei es „wichtig [...] eine Balance zu finden, dass nicht zu methodisch und wissenschaftlich vorgegangen wird. Ansätze zur Bewertung sollten daher praktikabel und lean sein.“ (I1). Quantitative Ansätze wurden als wenig geeignet, wohingegen qualitative Methoden – sowohl Risiken- als auch nutzenseitig – als praxistauglich für die Analyse von Schatten-IT bewertet wurden (s. Abbildung 16): „Eine qualitative Risikobewertung macht sowohl präventiv als auch wenn bereits Schatten-IT-Anwendungen auftauchen Sinn. Nur sollte sie nicht zu kleinteilig und daher noch praktikabel sein.“ (I3). Speziell für KMU solle auf eine intuitive und einfache Methodik geachtet werden, da diese häufig gar nicht die Kapazitäten für einen mehrstufigen und quantitativen Bewertungsprozess mitbrächten. Eine Kombination aus einer „sinnvollen Fragetechnik und einer Bewertung wäre das Richtige. So kann ermittelt werden, ob das System wichtig ist und ob die Technik passt.“ (I4). Die hier angesprochene Relevanz bzw. Kritikalität der Schatten-IT für unternehmensinterne Prozesse sowie deren technische Qualität sehen alle Interviewpartner als

wichtige Kriterien für eine zielführende Bewertung. Außerdem wurde von den Experten der (potenzielle) Nutzerkreis einer Schatten-IT als weiteres Bewertungskriterien angeführt. Je weniger Anwendende, desto geringer sei auch das Risiko et vice versa (I5). Als zentrale Anforderung an eine Bewertungsmetrik wurde zudem die Anwendbarkeit sowohl seitens der IT als auch der Fachbereiche genannt. Die Bewertungskriterien sollten demnach für beide Zielgruppen verständlich sein (I3; I5). Eine monetäre Nutzenquantifizierung von Schatten-IT anhand einer verbesserten Prozessdurchlaufzeit, wie im Forschungsantrag beschrieben, schätzen alle Interviewpartner als wenig sinnvoll ein. Die Aufwands- und Nutzenrelation sei nicht zielführend und die Anwendung im Unternehmen nicht praktikabel (I1 – I5). Bei der Entwicklung einer Bewertungsmetrik für Schatten-IT wurde der Fokus deshalb auf ein praktikables, qualitatives Vorgehen mit angemessenem Aufwand- und Nutzenverhältnis für die anwendenden Unternehmen gelegt.

	Unternehmen				
	#1	#2	#3	#4	#5
Methoden					
<i>Identifikation</i>					
Kollektionsmethoden (z.B. Checkliste, Self-Assessment)	●	◐	●	●	●
Kreativitätsmethoden (z.B. Brainstorming, Brainwriting)	◐	○	◐	◐	◐
Analytische Suchmethoden (z.B. Angriffsbaum)	○	●	○	◐	○
<i>Analyse und Bewertung</i>					
Fehlerbaumanalyse	○	◐	○	◐	○
Szenarioanalyse	◐	○	○	○	◐
Failure Mode and Effect Analysis (FMEA)	○	○	◐	◐	○
Risikotabelle	◐	●	●	◐	○
Risikoportfolio	●	◐	●	◐	●
CIA-Analyse	○	◐	○	○	◐

● Ja/ geeignet
 ◐ Teilweise geeignet
 ○ Nein / nicht geeignet

Abbildung 16: Eignung der Methoden zur Bewertung der Risiken von Schatten-IT (eigene Darstellung)

Zusammenfassend wurden im Rahmen der Fallstudien die folgenden Anforderungen an eine Bewertungsmetrik für Schatten-IT identifiziert:

- Qualitative Methode
- Praktikables und intuitives Vorgehen
- Verständlichkeit und Einsetzbarkeit im/mit Fachbereich

Im Folgenden wird die abgeleitete Bewertungsmetrik für identifizierte Schatten-IT dargestellt.

3.2.7 Bewertungsmetrik für Schatten-IT und Validierung

Auf Basis der Klassifikation der Risiken und Nutzenaspekte von Schatten-IT sowie den vorangegangenen Fallstudien wurde eine zweistufige Bewertungsmetrik für identifizierte Schatten-IT-Anwendungen entwickelt sowie mit zwei Fallstudienpartnern (Unternehmen 1 und 5 gemäß Tabelle 2) erprobt und validiert. Die Metrik dient als Self-Assessment und wird im Idealfall von der

IT gemeinsam mit den Fachbereichen genutzt. Im ersten Schritt wird für jede identifizierte Schatten-IT-Anwendung eine Nutzwert- und Risikoanalyse in Form einer Checkliste mit 17 anwendungsbezogenen Fragen und simpler Ja/Nein-Antwortkategorie durchgeführt. Eine Gewichtung der einzelnen Fragen erlaubt den Unternehmen eine Anpassung der Metrik nach ihren Bedürfnissen und Schwerpunkten. Auf Basis des Fragenkatalogs werden die Schatten-IT-Anwendungen nach ihrem Risiko und Nutzen in einer Risikomatrix klassifiziert und visualisiert. Der erste Schritt erlaubt somit eine einfache und schnelle Bewertung der Schatten-IT und schafft Transparenz in Bezug auf das Risiko- und Nutzenverhältnis. Im zweiten Schritt erfolgt eine verfeinerte Bewertung anhand der Kriterien Relevanz und Kritikalität sowie Qualität, Nutzungsumfang und Redundanz der Anwendung. Die anschließende Visualisierung im Risikoportfolio aggregiert die Ergebnisse in anschaulicher Weise und gibt eine erste Einordnung der Schatten-IT nach möglichen Lösungsansätzen (s. Kapitel 3.3).

Schritt 1: Nutzwert- und Risikoanalyse

In die Metrik wurden die Risiken und Nutzenkriterien mitaufgenommen, welche die Fallstudienpartner in Kapitel 3.2.3 als relevant eingestuft hatten. Im Rahmen der Nutzwertanalyse beantwortet der Anwendende zunächst anwendungsbezogene Fragen aus den Wirkungsbereichen *Abteilungsinterne Prozesse*, *IT-Landschaft* und *Personale Arbeitsumgebung* (s. Kapitel 3.2.3) und gewichtet diese gemäß seinen/ihren Präferenzen. Durch die Gewichtung kann die Metrik bspw. an individuelle Schwerpunkte der IT-Strategie des Unternehmens angepasst werden. Jede mit „ja“ beantwortete Frage wird dabei numerisch mit einem Wert von 1 versehen, welcher, je nach Gewichtung, mit einem Faktor von 0,8 (bei einer Gewichtung von 1) bis 1, 2 (bei einer Gewichtung von 5) multipliziert wird. Hierbei kann ein Maximalwert von 9,6 erreicht werden. Die Risikoanalyse beinhaltet Fragen aus den Wirkungsbereichen *Unternehmensinfrastruktur* und *IT-Landschaft* (s. Kapitel 3.2.3). Sie basiert auf derselben Metrik wie die Nutzwertanalyse und unterscheidet sich durch eine zusätzliche Frage, wodurch ein Maximalwert von 10,8 erreicht werden kann.

Tabelle 7: Nutzwert- und Risikoanalyse (eigene Darstellung)

Nutzen Anwendungsbezogene Fragen		Antwort (ja / nein)	Gewichtung (1-5)
1	Vereinfacht oder verkürzt die Anwendung einzelne Arbeitsprozesse in der Fachabteilung?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
2	Macht die Anwendung einzelne Arbeitsprozesse in der Fachabteilung effizienter?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
3	Stellt die Anwendung eine innovative Lösung dar?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
4	Löst die Anwendung ein internes Defizit der IT?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
5	Erfüllt die Anwendung bestimmte Anforderungen des Fachbereichs, die eine genehmigte Lösung nicht erfüllt?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
6	Arbeitet die Fachabteilung durch die Anwendung besser zusammen?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
7	Wird die Fachabteilung durch die Anwendung produktiver?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
8	Wird die Fachabteilung durch die Anwendung flexibler?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
Risiken Anwendungsbezogene Fragen			
9	Verarbeitet die Anwendung personenbezogene Daten?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
10	Verarbeitet die Anwendung sensible, unternehmensbezogene und schützenswerte Daten?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
11	Ist die Herkunft der verarbeiteten Daten in der Anwendung nicht hinreichend nachvollziehbar?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
12	Können unbefugte Dritte auf die Anwendung zugreifen? (bspw. durch fehlende Authentifizierungsmaßnahmen oder mangelnden Passwortschutz)	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
13	Ist spezifisches Wissen notwendig, um die Anwendung zu betreiben?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
14	Ist die Ausführung der Anwendung von einer oder wenigen Personen abhängig?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
15	Wird durch die Anwendung die Anzahl der Medienbrüche erhöht?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
16	Besteht ein verhältnismäßig hoher Integrationsaufwand für die Anwendung?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...
17	Sind die laufenden Kosten der Anwendung hoch oder nicht hinreichend kalkulierbar?	<input type="checkbox"/> ja <input type="checkbox"/> nein	...

Jeder Anwendung wird auf Basis der Analyse ein Nutzen- und Risikoverhältnis zugeordnet und in ein Koordinatensystem in Form einer Risikomatrix eingeordnet (s. Abbildung 17). Diese erlaubt in anschaulicher Weise eine erste Einordnung der identifizierten Schatten-IT nach ihrem Nutzen und Risiko.

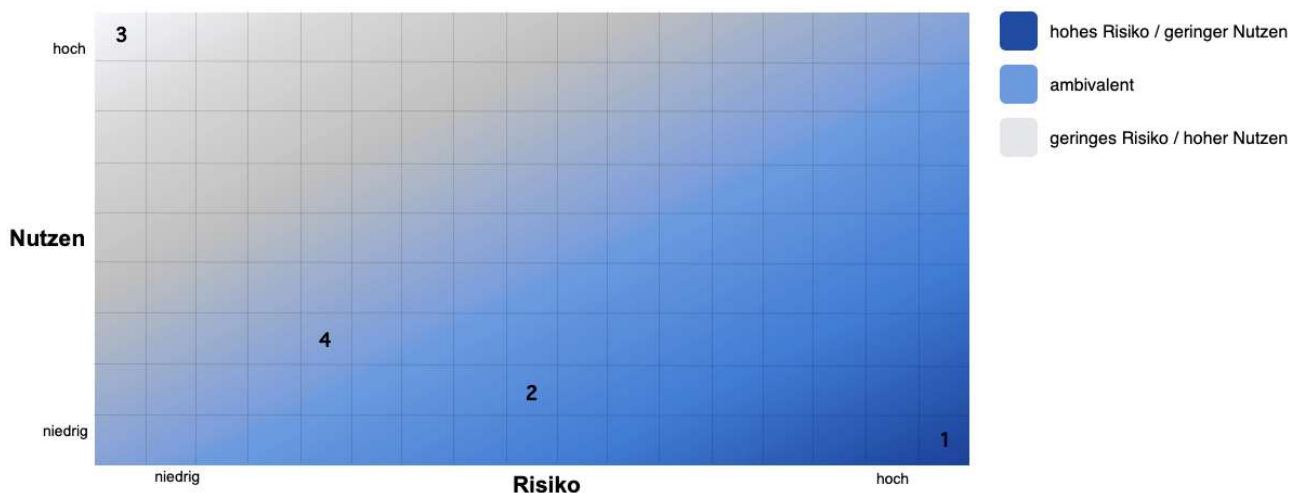


Abbildung 17: Beispielhafte Risikomatrix (eigene Darstellung)

Schritt 2: Weitere Bewertungskriterien

Die Beantwortung weiterer anwendungsbezogener Fragen dient dazu, die identifizierte Schatten-IT-Anwendung möglichst vollumfänglich zu bewerten und passende Lösungsansätze für den richtigen Umgang mit der jeweiligen Anwendung abzuleiten (s. Tabelle 8). Die Metrik ist identisch zur Nutzwert- und Risikoanalyse und umfasst die Kriterien *Relevanz und Kritikalität*, *Qualität*, *Nutzungsumfang* und *Redundanz*, welche im Rahmen der Fallstudien mit den Unternehmen des pbAs identifiziert wurden. Relevanz und Kritikalität umfassen Fragen zur Abhängigkeit strategischer bzw. operativer Entscheidungen sowie fachbereichsspezifischer, -übergreifender und geschäftsmodellkritischer Prozesse der Schatten-IT-Anwendung. Zudem fließt hier der Nutzungsumfang der Anwendung mit ein und bildet die Anzahl der Nutzerschaft im Unternehmen ab. Bei einer geringen Nutzerzahl (1-5 Nutzer) wird einer Anwendung eine eher geringe Relevanz zugeordnet und der in Schritt 1 ermittelte kumulierte Nutzwert mit dem Faktor 0,8 multipliziert. Der ermittelte Wert für die Relevanz und Kritikalität bei einer Anwendung mit einer großen Nutzerzahl (mehr als 20 Nutzer und Nutzerinnen), würde als relevanter eingestuft und mit dem Faktor 1,2 multipliziert werden. In der Kategorie **Relevanz und Kritikalität** kann somit ein Maximalwert von 5,76 erreicht werden und in der Kategorie **Qualität** ein Wert von 6. Hierunter sind Fragen zur technischen und funktionalen Qualität der Schatten-IT Anwendung sowie deren Bedienbarkeit gefasst und die Frage, inwieweit bereits ein Support der IT-Abteilung zur Qualitätssicherung besteht. Schlussendlich kann im Rahmen der Redundanz angegeben werden, ob bereits eine offizielle Lösung der zentralen IT im Unternehmen mit gleicher Funktionalität wie die der identifizierten Schatten-IT existiert.

Tabelle 8: Weitere Bewertungskriterien (eigene Darstellung)

Relevanz Anwendungsbezogene Fragen	und	Kritikalität	Antwort (ja / nein)	Gewichtung (1-5)
1	Werden mit Hilfe der Anwendung strategische oder operative Entscheidungen getroffen? (bspw. über Investitionen, Lieferzusagen)		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
2	Sind fachbereichsspezifische Prozesse von der Anwendung abhängig?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
3	Sind fachbereichsübergreifende Prozesse von der Anwendung abhängig?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
4	Sind geschäftsmodellkritische Prozesse von der Anwendung abhängig?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
Nutzungsumfang Anwendungsbezogene Frage				
5	Wie viele Beschäftigte nutzen die Anwendung?		näherungsweise	
Qualität Anwendungsbezogene Fragen				
6	Ist die technische Umsetzung der Anwendung professionell?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
7	Ist die Anwendung einfach zu bedienen?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
8	Ist die Funktionsweise der Schatten-IT zuverlässig?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
9	Kann die Anwendung an unterschiedliche Bedürfnisse angepasst werden?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
10	Besteht ein Support der Anwendung durch die IT-Abteilung zur Qualitätssicherung?		<input type="checkbox"/> ja <input type="checkbox"/> nein	...
Redundanz Anwendungsbezogene Fragen				
11	Gibt es eine offizielle Lösung der zentralen IT, die redundant zur Anwendung ist?		<input type="checkbox"/> ja <input type="checkbox"/> nein	

Die bewerteten Schatten-IT-Anwendungen werden im nächsten Schritt anhand der aggregierten Werte in einem Risikoportfolio kategorisiert. Die Koordinaten setzen sich aus der Relevanz und Kritikalität (y-Achse) sowie Qualität (x-Achse) zusammen. Die Legende visualisiert zudem die Redundanz sowie das Risiko- und Nutzenverhältnis aus Schritt 1 (s. Abbildung 18).

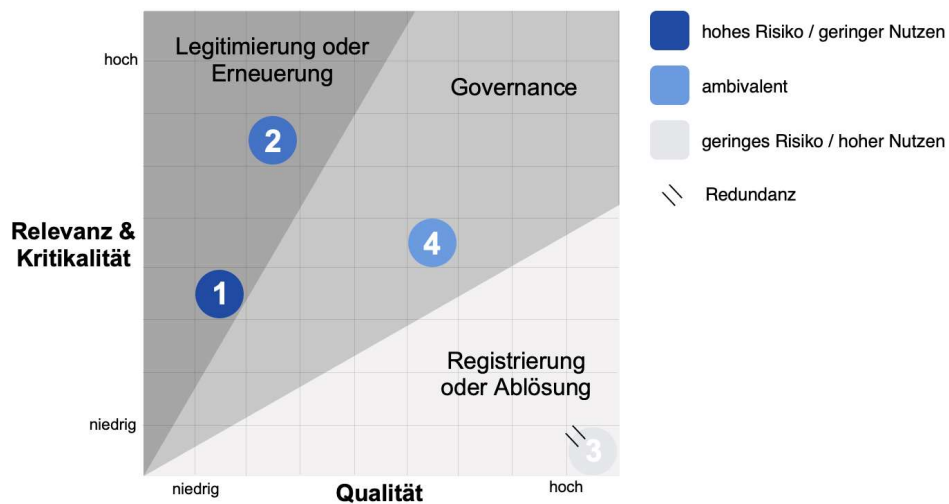


Abbildung 18: Beispielhaftes, aggregiertes Risikoportfolio (eigene Darstellung)

Das aggregierte Risikoportfolio schafft in übersichtlicher Weise Transparenz in Bezug auf die identifizierten und bewerteten Schatten-IT-Anwendungen und kategorisiert diese in Lösungsansätze ein. Wenn die Schatten-IT redundant zu einer offiziellen Lösung der zentralen IT mit gleicher Funktionalität ist, wird jene folgerichtig durch die offizielle Anwendung abgelöst. Beim Lösungsansatz *Registrierung* besteht keine redundante Lösung, die Schatten-IT hat eine angemessene Qualität sowie einen hohen Nutzen und eine eher geringe Kritikalität bzw. Relevanz. Sie wird registriert, also in den Servicekatalog aufgenommen, überwacht und es wird ein Support seitens der zentralen IT bereitgestellt. Sonst sind keine weiteren Maßnahmen erforderlich. Hat die Schatten-IT-Anwendung eine hohe Relevanz und Kritikalität sowie eine angemessene Qualität, muss eine *Governance* erfolgen. Hierunter werden auch ambivalente Anwendungen verortet, die sowohl ein hohes Risiko als auch ein hohes Nutzenpotenzial aufweisen. Bei einer *Governance* wird die Verantwortung bspw. für die anwendungsbezogene Nutzung, Wartung und den Support zwischen der zentralen IT und den Fachbereichen verteilt und klare Rollen definiert, um mögliche Risiken zu minimieren. In die Lösungsansätze *Legitimierung oder Erneuerung* werden ambivalente Schatten-IT-Anwendungen gefasst, die eine hohe Relevanz und Kritikalität mitbringen, jedoch gleichzeitig sehr risikobehaftet sind oder nicht den Qualitätsanforderungen der zentralen IT entsprechen. Hier muss entweder eine Erneuerung der Anwendung, oder die völlige Integration in die IT-Architektur erfolgen, wobei die Verantwortlichkeit in vollem Umfang an die IT-Abteilung übertragen wird. Die Lösungsansätze für Schatten-IT werden in Arbeitspaket 3 ausgeführt, wobei auch auf *Plattformen* als Intermediäre eingegangen wird.

3.3 Arbeitspaket 3: Entwicklung und Bestimmung von Lösungsansätzen für die Nutzung von Schatten-IT

Ziel von Arbeitspaket 3 war es, bestehende Lösungsansätze zur Nutzung von Schatten-IT zu strukturieren und zu beschreiben sowie neue Ansätze zu entwickeln. Dies diente der Erarbeitung eines Auswahl-Assessments der erarbeiteten Lösungsansätze aufbauend auf der Risiko- und Nutzenbewertung aus den Vorarbeiten und als Kernelement des ganzheitlichen Vorgehens.

Für die Bearbeitung der Kernfragen ergab sich das Vorgehen in Abbildung 19. Dazu wurden zunächst gemeinsam im pbA grundlegende Anforderungen an Lösungsansätze zum Umgang mit Schatten-IT erhoben wie auch besondere Anforderungen für einen plattformbasierten Lösungsansatz. Dazu gehörte neben einer Anforderungsdokumentation auch eine Marktstudie zu Low-Code-/No-Code-Plattformen als möglicher Lösungsansatz. Ursprünglich sollte der Fokus in diesem Arbeitspaket insbesondere auf die plattformbasierten Ansätze gelegt werden, jedoch stellte sich im Laufe der Bearbeitung heraus, dass in der Praxis die alleinige Anwendung von Plattformlösungen keine hohe Akzeptanz hat. Daher wurden weitere Lösungsansätze mithilfe von Literaturrecherche und Studien ausgearbeitet und beschrieben. In Fallstudien wurden die Tauglichkeit der Ansätze wie auch die Akzeptanz festgestellt, um darauf basierend ein Assessment vorzunehmen.

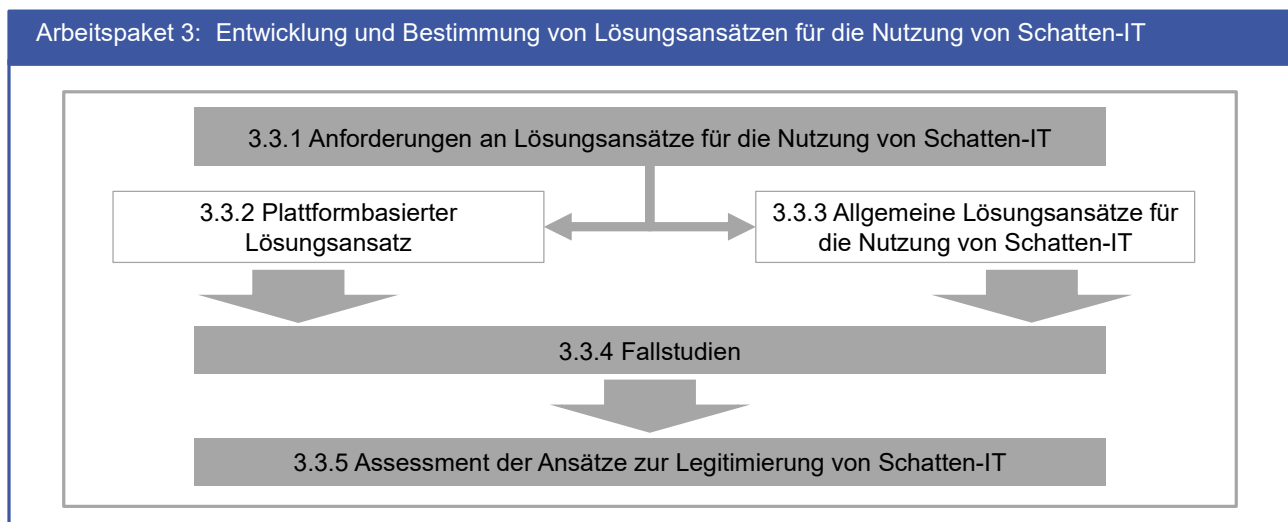


Abbildung 19: Vorgehen in Arbeitspaket 3 (eigene Darstellung)

3.3.1 Anforderungen an Lösungsansätze für die Nutzung von Schatten-IT

Für die Bestimmung passender Lösungsansätze wurde in dem Arbeitspaket gemeinsam mit dem pbA eine Anforderungsaufnahme und -dokumentation durchgeführt. Dabei wurden die Anforderungen hinsichtlich der Perspektive einer zentralen IT wie auch der Fachbereiche aufgenommen. Da zu Beginn des Projekts noch der Fokus auf eine plattformbasierte Lösung gelegt wurde, wurden in diesem Workshop Anforderungen für Low-Code/No-Code-Plattformen als intermediär aus den zwei Rollenperspektiven in Form von User-Stories erhoben und konsolidiert (s. Abbildung 20).



Abbildung 20: Konsolidierte Anforderungen an Low-Code-/No-Code-Plattformlösungen

Für die IT war es vor allem wichtig, eine sichere Möglichkeit bereitzustellen, beispielsweise zentral verwaltete Kleinanwendungen oder Anwendungsbausteine zu erstellen, um Schatten-IT zu reduzieren und die Eigeninitiative der Mitarbeitenden zu fördern wie auch ein Controlling-Tool zu haben. Dabei sollen aber wichtige Rahmenbedingungen hinsichtlich der Sicherheit, Berechtigungen und der Deployment-Strategie eingehalten werden. Auf Seiten der Fachbereiche soll es eine verpflichtende Regelkonformität der Anwendungen geben. Für eine geeignete Daten- und Prozessintegration sind sowohl die Usability für die Anwendung relevant als auch notwendige Integrationshilfen.

3.3.2 Plattformbasierter Lösungsansatz

Die Erarbeitung und Konzeption des plattformbasierten Lösungsansatzes wurden aufbauend auf der Anforderungsaufnahme durch eine Marktstudie und der Erarbeitung eines Funktionsradars durchgeführt. Dafür wurden gängige Low-Code-/No-Code-Plattformlösungen untersucht und anschließend in einem Steckbrief gem. Abbildung 21 überführt. Die Steckbriefe sind in Anhang 5 dokumentiert worden. Das daraus resultierende Funktionsradar in Anhang 4 fasst die Ergebnisse der Marktstudie zusammen. Die Vorlage wurde ergänzt, um die Kernanforderungen, die aus IT-Sicht und Fachbereichssicht existieren zu konsolidieren und kann somit als eine Entscheidungsvorlage für die Auswahl von Plattformlösungen genutzt werden.

Bezeichnung:	Funktionen:	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/"Selbstbestimmtheit" <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung:		
Voraussetzungen / Kosten:		

Abbildung 21: Vorlage eines Funktionssteckbriefs für Low-Code-/No-Code-Plattformen

Mit einem Plattform-Ansatz bietet sich die Möglichkeit, die Zuständigkeiten der IT und des Unternehmens zu trennen. Zum einen kann die IT-Organisation eine sichere und kontrollierte Infrastruktur für Schatten-IT oder lokale Proofs of Concept bereitstellen, um ein gewisses Maß an Standardisierung, Kontrolle, Sicherheit und Kosten-/Skalierungsvorteile zu gewährleisten. Zum anderen bieten Plattformen die Bereitstellung einer Self-Service-Datenintegration, bei dem die IT-Fachabteilung die technische Integration mit dem bestehenden System verwaltet. Anwendende können somit aus mehreren Systemen zu Berichtszwecken konsolidieren oder potenziell neue Anwendungen über eine einfache Drag-and-Drop-Schnittstelle integrieren. Wichtig dabei ist ein eingeschränkter Zugriff auf einen zentralen Datenspeicher, sodass die flexible Erstellung von Berichtslösungen in den Geschäftsbereichen unter Nutzung des fachspezifischen Prozesswissens ermöglicht wird. Durch den direkten (nur lesenden) Datenzugriff und die Möglichkeit, Abfragen zu erstellen, wird sichergestellt, dass die Fachanwender und Fachanwenderinnen aktuelle und konsistente Informationen erhalten. Zudem können Tabellenkalkulationslösungen separat und flexibel für temporäre Anforderungen bearbeitet werden. Falls für eine Anwendung ein langfristiger Bedarf besteht, kann diese zentral verwaltet und iterativ weiterentwickelt werden, um somit Konsistenz zu erhalten.

Im Zuge der Erarbeitung wurde im pbA jedoch deutlich, dass eine reine Auswahl von Low-Code-/No-Code-Plattformen als alleiniger Lösungsansatz für die Nutzung von Schatten-IT nicht ausreicht. Neben der hohen Varianz und Funktionsumfängen, wie aus dem Funktionsradar (s. Anhang 4) ersichtlich, sind KMU in der aktuellen Stufe mit der Einführung von Internet-of-Things(IoT)-Plattformen beschäftigt, was als Einstiegspunkt in mögliche Low-Code-/No-Code-Lösungen dient. Entsprechend wurde auch eine Einordnung von Legitimierungsansätzen im Bereich der IoT-Plattformen als sinnvoll erachtet. Dafür wurde eine entsprechende Literaturrecherche durchgeführt und gängige Plattformlösungen betrachtet. Abbildung 22 beschreibt die Unterteilung der Klassen und Arten von IoT-Plattformen und den besonderen Fokusbereich, in dem Lösungsansätze zur Nutzung von Schatten-IT verortet werden können.

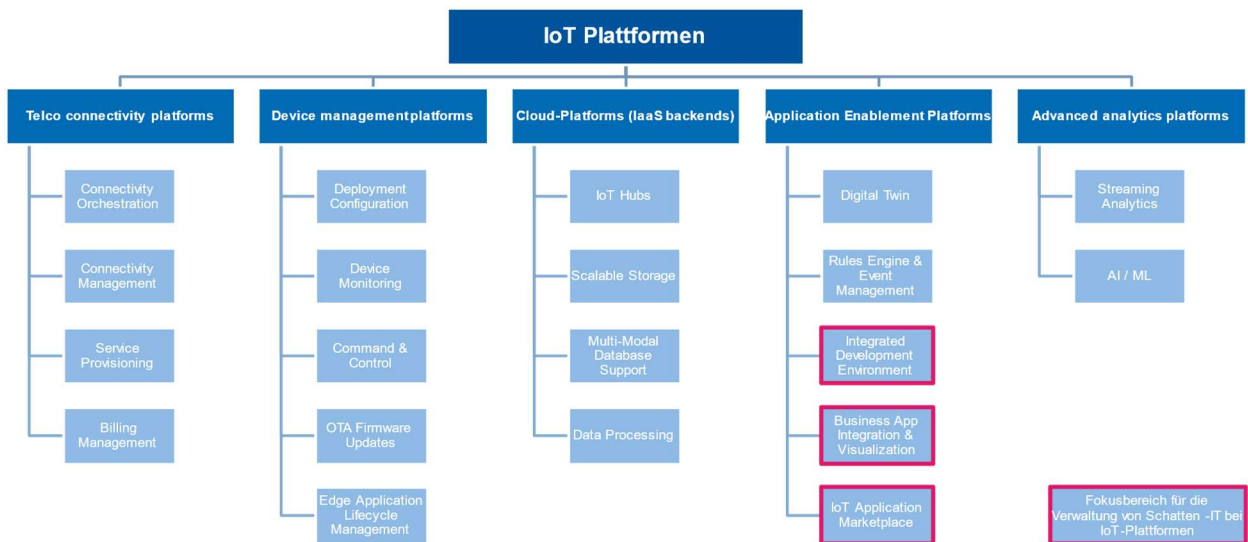


Abbildung 22: Übersicht von verschiedenen Arten von IoT-Plattformen

3.3.3 Allgemeine Lösungsansätze für die Nutzung von Schatten-IT

Neben den plattformbasierten Lösungsansätzen wurden in diesem Arbeitspaket weitere Lösungsansätze für die Nutzung von Schatten-IT durch Literaturrecherchen und halbstrukturierte Experteninterviews erarbeitet. Dabei wurden fünf weitere Lösungsansätze (s. Abbildung 23) betrachtet, welche im Folgenden beschrieben werden. Diese Ansätze sollen den Unternehmen eine größere Auswahl an Lösungspfaden geben und damit eine Unterstützung bieten, basierend auf der Identifikation und Risikoanalyse der Schatten-IT einen passenden Lösungsansatz zu wählen. Dieser sollte sowohl mit der Technologie- als auch mit der Prozessreife im Unternehmen übereinstimmen. Im pbA wurde festgestellt, dass einige Unternehmen noch nicht die grundlegenden Voraussetzungen geschaffen haben, um die direkte Einführung von Plattformlösungen umzusetzen.

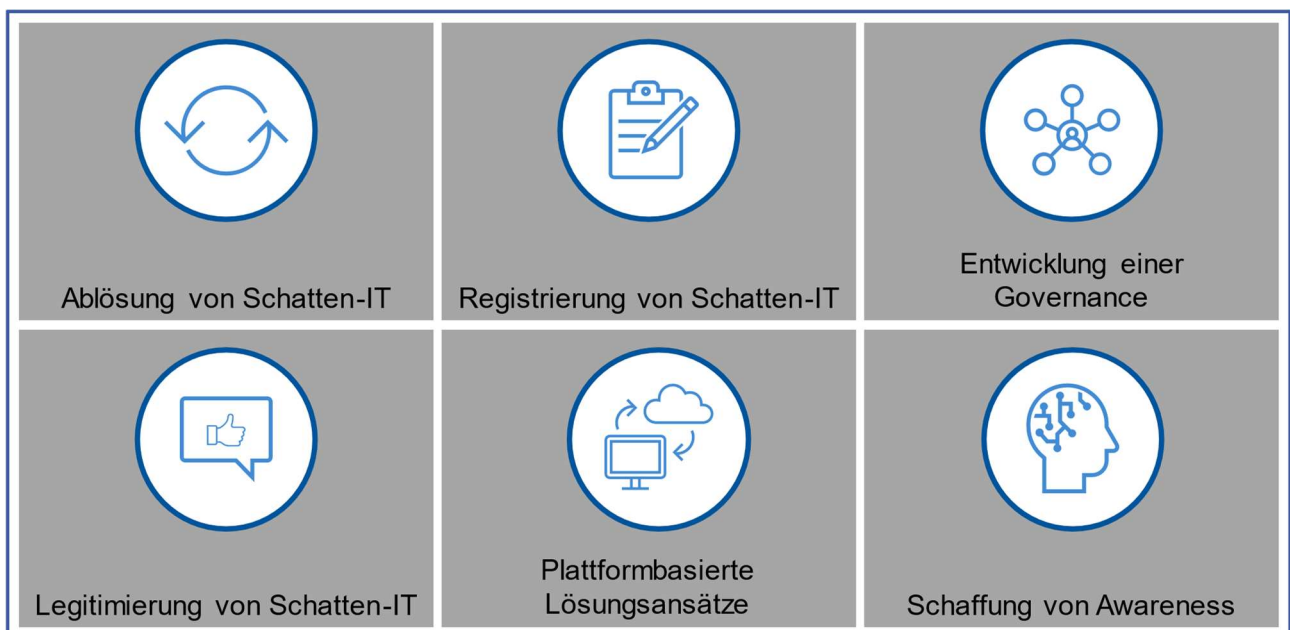


Abbildung 23: Übersicht von Lösungsansätzen (eigene Darstellung)

Ablösung von Schatten-IT

Die Ablösung bezieht sich auf eine Situation, in der ein Schatten-IT-System nach der Identifizierung durch ein anderes System ersetzt wird. In dieser Situation wechseln die Nutzer und Nutzerinnen von einem System zu einem anderen. Das erste System ist dabei ein Schatten-IT-System und das zweite möglicherweise ein neues System, das von den offiziellen IT-Einheiten betrieben wird. Die Ablösung erfolgt hierbei in drei Schritten:

- *Klare Anforderungen*
Der Ist-Zustand wird erfasst. Dazu zählen fachliche, technische und organisatorische Herausforderungen. Ebenso werden Rahmenbedingungen und Ziele festgelegt und somit verbindliche Anforderungen formuliert.
- *Belastbare Lösungsansätze*
Für den künftigen Umgang wird ein klares Zielsystem ausgewählt, welches intern entwickelt oder bei Bedarf extern beschafft werden muss. Dazu gehört eine Umsetzungsplanung, welche explizit die Planung der Altdatenübernahme beinhaltet wie auch den notwendigen Schulungsplan der Mitarbeitenden für die Systemnutzung und die Planung des Go-live.
- *Verlässliche Umsetzung*
Neben dem Go-live mit der Altdatenübernahme, eine Stabilisierungsphase und einem Projektabschluss gehört zur verlässlichen Umsetzung zusätzlich zu der Umsetzung des neuen Zielsystems ein geeigneter Change-Prozess zur Akzeptanzförderung bei den Mitarbeitenden.

Registrierung von Schatten-IT

Der Lösungsansatz „Registrierung“ empfiehlt sich bei einer identifizierten Schatten-IT-Anwendung mit relativ geringer Relevanz, d. h. mit geringer Nutzungsintensität und angemessener Qualität. Im Falle einer hohen Qualität bezüglich des Designs, der Technik, des Engineering-Prozesses und der Service- sowie Informationsqualität und gleichzeitig hohem Nutzen wird die Lösung als Fachbereichs-IT in das Servicemanagement aufgenommen. Wichtig ist dabei ein fortlaufendes bzw. regelmäßiges Monitoring der Anwendung. Um dies zu gewährleisten, müssen Verantwortungen eindeutig definiert werden, indem die Zuständigkeit für die Wartung der Anwendungen festgelegt werden. Durch eine Festlegung des Phase-out einer Anwendung bei der Registrierung wird sichergestellt, dass die Anwendung nicht weiterentwickelt wird.

Entwicklung einer Governance

Für den Umgang mit Schatten-IT bestehen verschiedene Verfahrensweisen, welche unterschiedliche Implikationen bei Aufwänden innerhalb der Organisation zwischen IT und Business mit sich bringen. Eine Formalisierung der Umgangsformen innerhalb einer geeigneten Governance, die sich aus der Organisationsstrategie für Schatten-IT ergibt, muss vorhanden sein, um klare Richtlinien auf allen Ebenen zu haben.

Eine mögliche Umgangsform ist die Übertragung der Verantwortung für eine identifizierte Schatten-IT an die zentrale IT. Basierend auf der Bewertung des Systems ist die Überführung von Schatten-IT in das offizielle IT-Systemportfolio eine mögliche Lösung. Dies kann einerseits nur einer strategischen Übertragung dienen, andererseits jedoch auch dem Zweck, die Anwendung zur Sicherstellung der Gesamtintegrität des Systemportfolios neu und von Grund auf zu entwickeln. Eine vollständige Übertragung aller identifizierten Schatten-IT setzt jedoch voraus, dass die zusätzlich benötigten Ressourcen in der IT-Abteilung vorhanden sind.

Eine weitere Möglichkeit ist die Eigentumslegitimierung. Dies bedeutet, dass bestimmte Schatten-IT-Instanzen nach der Identifizierung nicht an die IT-Abteilung übertragen werden und die

Verantwortung für die Wartung beim aktuellen Business-User verbleibt. Dies ist ein Weg, um den Ressourcenbedarf der IT-Abteilung zu reduzieren, der durch die Eigentumsübertragung entsteht. Eine gewisse Kontrolle kann beibehalten werden, indem ein Pool von freien Ressourcen zur Unterstützung der Schatten-IT-Initiativen eingerichtet wird. In Anerkennung der Legitimität oder sogar Notwendigkeit von Schatten-IT in betrieblichen Kontexten könnte eine parallele Unternehmensarchitektur eingerichtet werden, die sich auf diese Art von Systemen konzentriert, welche entsprechend organisiert und reglementiert werden sollte.

Legitimierung von Schatten-IT

Falls eine Schatten-IT mit hohem Nutzen aber mit einem beachtlichen Risiko für die IT-Sicherheit identifiziert wird und diese den Anforderungen des IT-Fachbereichs nicht vollständig entspricht, empfiehlt sich eine Legitimierung. Sofern keine konkurrenzfähige Alternative durch die IT-Abteilung angeboten werden kann, ist die Ablösung durch die formelle IT oder die Integration in eine neue IT-Architektur angemessen. Wenn die entdeckte Anwendung in den offiziellen Servicekatalog aufgenommen wird, ist zu beachten, dass die User in den Prozess der Aufnahme eingebunden werden müssen. Essenziell bei diesem Lösungsansatz ist die enge Einbindung der Nutzerschaft in den Prozess, um das Verantwortungsgefühl zum Ausdruck zu bringen. Wird Schatten-IT ohne IT-Verständnis und ohne geeignete Alternativen verhindert, besteht die Gefahr, dass Anwendende weiterhin Schatten-IT generieren. Wenn die IT-Abteilungen die Bedürfnisse der Anwendenden nicht verstehen und Schatten-IT-Lösungen eher verhindern, besteht die Gefahr, weiterhin Schatten-IT zu schaffen.

Plattformbasierter Lösungsansatz

Die Ausarbeitung des plattformbasierten Lösungsansatzes bestehend aus Low-Code-/No-Code Lösungen und die Verortung im Funktionsumfang bestehender IoT-Lösungen ist Kapitel 3.3.2 zu entnehmen.

Schaffung von Awareness

Das Bewusstsein für die formale Politik ist eine Voraussetzung für ihre Einhaltung. Im Falle der Sicherheit beeinflusst das Bewusstsein der Nutzer und Nutzerinnen für die Richtlinien direkt das wahrgenommene Sicherheitsrisiko. Die Steigerung des Bewusstseins für Richtlinien ist daher der Schlüssel zur Einhaltung von IT-Standards.

Generell können zwei Möglichkeiten unterschieden werden. Zum einen sollte Schatten-IT als wesentlicher Bestandteil in interne IT-Sicherheitsunterweisungen integriert werden. Zum anderen bietet eine IT-Sicherheits-Kampagne im Unternehmen einen gängigen Weg, um Awareness zu schaffen. Um das Sicherheitsbewusstsein der Mitarbeitenden zu fördern und zu stärken, sollte auf die folgenden Aspekte eingegangen werden (TreeSolution Consulting GmbH 2021):

- „Nutzen Sie bei Kampagnen eine einfache und verständliche Sprache mit so wenig Fachausdrücken wie möglich.“
- „Vermeiden Sie eine angstmachende Kommunikation („Das ist falsch“, „Das darf man nicht“, „Das ist verboten“ etc.) und verwenden Sie stattdessen humoristische Elemente. So können die Risiken beispielsweise mit einem Cartoon vermittelt werden.“
- „Zeigen Sie Risiken und Erfolge anhand interner Beispiele. Das hilft den Mitarbeitenden, sich besser mit dem Unternehmen und dem gewünschten Verhalten zu identifizieren und es umzusetzen.“

- „Das Verhalten eines Menschen ist je nach Kultur unterschiedlich. Dies kann regional sein (z. B. bei internationalen Firmen) aber auch je nach Abteilung (Finanz- vs. Verkaufsabteilung). Ist die Schulung nur spezifisch für eine Abteilung oder eine Region, sollte die Kampagne basierend auf deren kulturellem Verhalten aufgebaut werden. Bei einer firmenübergreifenden Kampagne versuchen Sie am besten, möglichst alle in der Kommunikation abzudecken. Das heißt, dass Sie z. B. die individuelle Ebene („ich“) wie auch die gemeinschaftliche Ebene („wir“) ansprechen.“
- „Oft wird Sicherheit als Verhinderer angesehen. Daher ist es wichtig, Maßnahmen zu definieren, welche anwendbar sind. Zeigen Sie, wie auf einfache Art und Weise das gewünschte Verhalten umgesetzt werden kann. Zeigen Sie ebenfalls die Vorteile des sicheren Verhaltens auf.“

3.3.4 Fallstudien

Ein systematisches Vorgehen zur Nutzung der identifizierten Schatten-IT existierte in keinem der befragten Unternehmen. Daher besteht eine Relevanz von Methodiken zur Nutzung von Schatten-IT. Um die selbstentwickelten IT-Lösungen nicht zu eliminieren, wurde mithilfe von Fallstudien Gestaltungsansätze hergeleitet, wodurch die Anforderungen der Unternehmen bestmöglich abgedeckt werden.

Im Rahmen von halbstrukturierten Experteninterviews wurden Anforderungen erhoben und Bewertungen der Lösungsansätze bezüglich der Praxistauglichkeit im Unternehmen durchgeführt und evaluiert. Die Interviews stellten sich zusammen aus einem Portfolio an Fragen bezüglich des Nutzens, Risikos sowie Relevanz und Qualität für die Bewertung der identifizierten Schatten-IT anhand einer Nutzwert-Risikoanalyse-Matrix. Die Ergebnisse der Matrix bilden die Grundlage für ein Assessment der Lösungsansätze. Eine zusätzliche Überlegung war es, die Bewertung von Verbesserungsansätzen zur Praktikabilität und Anwendbarkeit der ermittelten Ansätze hinsichtlich der vorangegangenen Nutzwert- und Risikoanalyse durchzuführen. In den Interviews wurden die Partner zunächst bezüglich der Nutzwertanalyse befragt und es wurde ermittelt, anhand welcher Kriterien der Nutzen eingeschätzt wird. Dasselbe wurde für die Risikoanalyse durchgeführt. Nach einer Matrixauswertung, worin eine eindeutige Einstufung der Ergebnisse abgeleitet werden konnte, wurden Lösungsansätze erarbeitet, welche sich eher peripher in das Unternehmen einbinden ließen. Hierbei wurden folgende Ansätze befolgt:

- Klassische Ansätze
- Organisatorische Ansätze
- Plattformbasierte Ansätze
- Ansätze zur Migration

3.3.5 Assessment der Ansätze zur Legitimierung von Schatten-IT

Für das Auswahl-Assessment wurden in den Fallstudien die erarbeiteten Lösungsansätze analysiert. Im Laufe der Interviews für die Fallstudien stellte sich heraus, dass eine reine Betrachtung und Bewertung der Lösungsansätze nicht zielführend waren, da hier keine Bewertung auf Grundlage der vorangegangenen Nutzwertanalyse getroffen werden kann, sondern in der Praxis eine subjektive Entscheidung seitens der IT-Abteilung unternommen wird. Es wurde angemerkt, dass den KMU nach einer Risiko-Nutzen-Bewertung ihrer Schatten-IT eine Art individuelle Lösung für ihr Problem empfohlen werden sollte. Zudem nutzten einige der befragten Unternehmen bereits plattformbasierte Ansätze, welche den Mitarbeitern und Mitarbeiterinnen zur Verfügung gestellt wurden, aber nicht immer den richtigen Lösungsansatz boten. Jedoch war dem Anwenderkreis die eigene Erstellung von Anwendungen nicht möglich, sodass dadurch die

Entstehung von Schatten-IT vermieden werden konnte. Dafür müssen Freigabeerlaubnisse erstellt werden sowie Richtlinien festgelegt werden.

Somit ergab sich für die weitere Bearbeitung, dass neben den plattformbasierten Lösungen weitere Lösungsansätze erarbeitet wurden, um die Wahl der passenderen Lösung zu ermöglichen. Diese Lösungsansätze wurden entsprechend weiter aufbereitet und ins ganzheitliche Vorgehen und im Demonstrator integriert.

3.4 Arbeitspaket 4: Konzeption und Validierung eines ganzheitlichen Vorgehens für Schatten-IT bei KMU

Arbeitspaket 4 verfolgte das Ziel der Konzeption eines einfachen ganzheitlichen methodischen Vorgehens und einer Entscheidungshilfe, mit der produzierende KMU über den Umgang mit identifizierter Schatten-IT entscheiden und diese ggf. legitimieren können (s. Abbildung 24). In dem Arbeitspaket wurde auf Basis der Risiko- und Potenzialanalyse aus AP 2 sowie der Ansätze zur Legitimierung aus AP 3 ein ganzheitliches Vorgehen entwickelt. Dabei wurde das Vorgehen so ausgestaltet, dass die verschiedenen Legitimierungsansätze aus AP 3 unternehmensspezifisch und optimal kombiniert werden können. Darüber hinaus wurde das Vorgehen kontinuierlich und gemeinsam mit den Unternehmen des pbAs entwickelt und validiert.

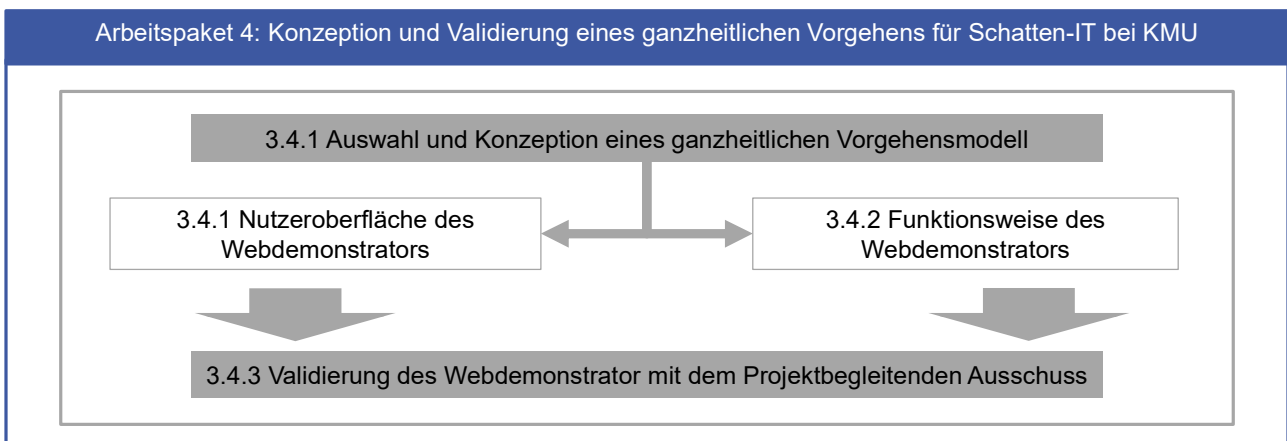


Abbildung 24: Vorgehen in Arbeitspaket 4 (eigene Darstellung)

3.4.1 Auswahl und Konzeption eines ganzheitlichen Vorgehensmodells

Um Unternehmen eine Entscheidungshilfe sowie ein ganzheitliches Vorgehen an die Hand zu geben, wurde gemeinsam mit dem pbA entschieden, die Ergebnisse des Forschungsprojekts in ein zentrales IT-Tool zu überführen. Dieses IT-Tool beinhaltet als Webdemonstrator nicht nur Ansätze zur Entscheidung darüber, ob Schatten-IT-Lösungen legitimiert oder abgeschafft werden soll, sondern zudem auch die entwickelten Ansätze zur Identifikation. Somit sind Unternehmen in der Lage, die Erkenntnisse des Forschungsprojekts Ende-zu-Ende ganzheitlich nutzen zu können und das Tool direkt operativ zu verwenden.

Um die passende Gestaltung des Vorgehensmodells in einem IT-Tool abzubilden, wurde in einem gemeinsamen Design-Thinking-Workshop ein Prototyp des Demonstrators erstellt. Dieses Mock-up (s. Anhang 6) diente dazu, die erste Anwendbarkeit und Praxistauglichkeit zu analysieren und im pbA zu prüfen. Basierend auf dem Feedback wurde aus einem anfangs zehnstufigen Verfahren ein fünfstufiges Verfahren für das IT-Tool erarbeitet, welches in den folgenden Kapiteln dargestellt wird.

3.4.1 Nutzeroberfläche des Webdemonstrators

Im Folgenden wird der Aufbau des IT-Tools beschrieben. Dieses ist kostenfrei unter dem folgenden Link nutzbar: <https://legitimise-it-tool.fir.de/>.

Registrierung und Login

Für die Nutzung des Tools können Unternehmen mithilfe einer E-Mail-Adresse einen Account erstellen und sich anmelden. Die Anmeldung dient in keiner Weise der Datensammlung und

bezweckt ausschließlich das Speichern von Projekten und Projektdaten. Die Betreiber des Tools nehmen den Schutz der persönlichen Daten sehr ernst. Daher werden personenbezogene Daten vertraulich und entsprechend den gesetzlichen Datenschutzvorschriften sowie der dargestellten Datenschutzerklärung behandelt. Wenn ein Account erstellt wird, werden sowohl die verwendete E-Mail als auch die im Rahmen der Tool-Nutzung erfassten Daten gespeichert.

Aufbau des IT-Tools

Das Tool dient zur Unterstützung von Unternehmen im Umgang mit Schatten-IT-Anwendungen. Konkret unterstützt es Anwendende bei der Identifikation von Schatten-IT und stellt ein Self-Assessment zur Risiko- und Nutzwertanalyse identifizierter Anwendungen bereit. Auf Basis der Analyse werden Lösungsvorschläge bereitgestellt. Dabei werden die einzelnen Schritte des Tools chronologisch durchlaufen. Im ersten Schritt können einzelne Aspekte nach deren Relevanz für die unternehmensindividuelle IT-Strategie gewichtet werden. Der darauffolgende Schritt liefert eine Hilfestellung und gibt vier verschiedene Methoden zur Identifikation von Schatten-IT an die Hand. Im weiteren Verlauf können bereits identifizierte Schatten-IT-Anwendungen sowie zentral verwaltete IT-Anwendungen im Tool erfasst, charakterisiert sowie bewertet werden. Die erfassten Anwendungen werden daraufhin transparent visualisiert und passende Lösungsansätze auf Basis der Charakterisierung vorgeschlagen. An spezifischen Stellen im Tool finden sich Download-Links für weiterführende Informationen (z. B. Report-Logik, Interviewleitfaden).

Das Tool stellt in keiner Weise einen Ersatz für professionelle Beratungsleistungen dar. Ferner hat es keinen Anspruch auf Vollständigkeit. Die einzelnen Berechnungsschritte sind unter Hinzunahme von wissenschaftlichen Erkenntnissen sowie Erfahrungen von Unternehmen entstanden. Die Anwendung des Tools soll nur als Anregung für die eigene Planung verstanden werden und muss vom Anwender oder von der Anwenderin angepasst und überprüft werden.

Schritt 1: Gewichtung

Um Unternehmen bestmögliche Handlungsempfehlungen im Umgang mit Schatten-IT-Anwendungen bereitzustellen, werden in einem ersten Schritt zunächst die Schwerpunkte der unternehmensindividuellen IT-Strategie erfasst. Der Anwenderkreis des Tools erhält verschiedene Aspekte einer IT-Strategie als Objekt, die Sie per Drag-and-Drop entsprechend der Gewichtung (gering bis hoch) ordnen können (s. Abbildung 25). Dies dient als notwendige Berechnungsbasis, um die Chancen und Risiken individuell bewerten zu können.

Bitte ordnen Sie die jeweiligen Aspekte gemäß ihrer Relevanz für Ihre IT-Strategie:

Hohe Gewichtung	Prozessstandardisierung und -optimierung heben
	Datenschutz sicherstellen
	Systemintegration vorantreiben
	Schutz von Betriebsgeheimnissen sicherstellen
	Datenqualität und -validität sicherstellen
	Datenverfügbarkeit sicherstellen
	Effizienzen anheben
	Wirtschaftlichkeit heben
	Zentrale IT ist ganzheitlicher Lösungsanbieter
	Zentrale IT ist Enabler für Zusammenarbeit, Produktivität und Flexibilität
	Innovationsfähigkeit unterstützen
Geringe Gewichtung	

Abbildung 25: Individuelle Gewichtung der Aspekte der IT-Strategie (eigene Darstellung)

Schritt 2: Identifikation

Nachdem die Gewichtung erfolgt ist, wird die anwendende Person zum nächsten Schritt weitergeleitet. Dieser zielt darauf ab, existierende Schatten-IT im Unternehmen zu identifizieren. Im Rahmen des Projekts wurden vier zentrale Ansätze zur Identifikation erhoben: Interviews mit Mitarbeitenden, die Analyse von Service-Desk-Anfragen, Vergleich von Budgets und die Nutzung von unterstützenden Tools. Der anwendenden Person wird innerhalb des Tools eine umfangreiche Erklärung sowie die Möglichkeit von Downloads geboten. Die dargestellten Ansätze dienen hierbei als Unterstützungsleistung für die Identifikation (s. Abbildung 26).

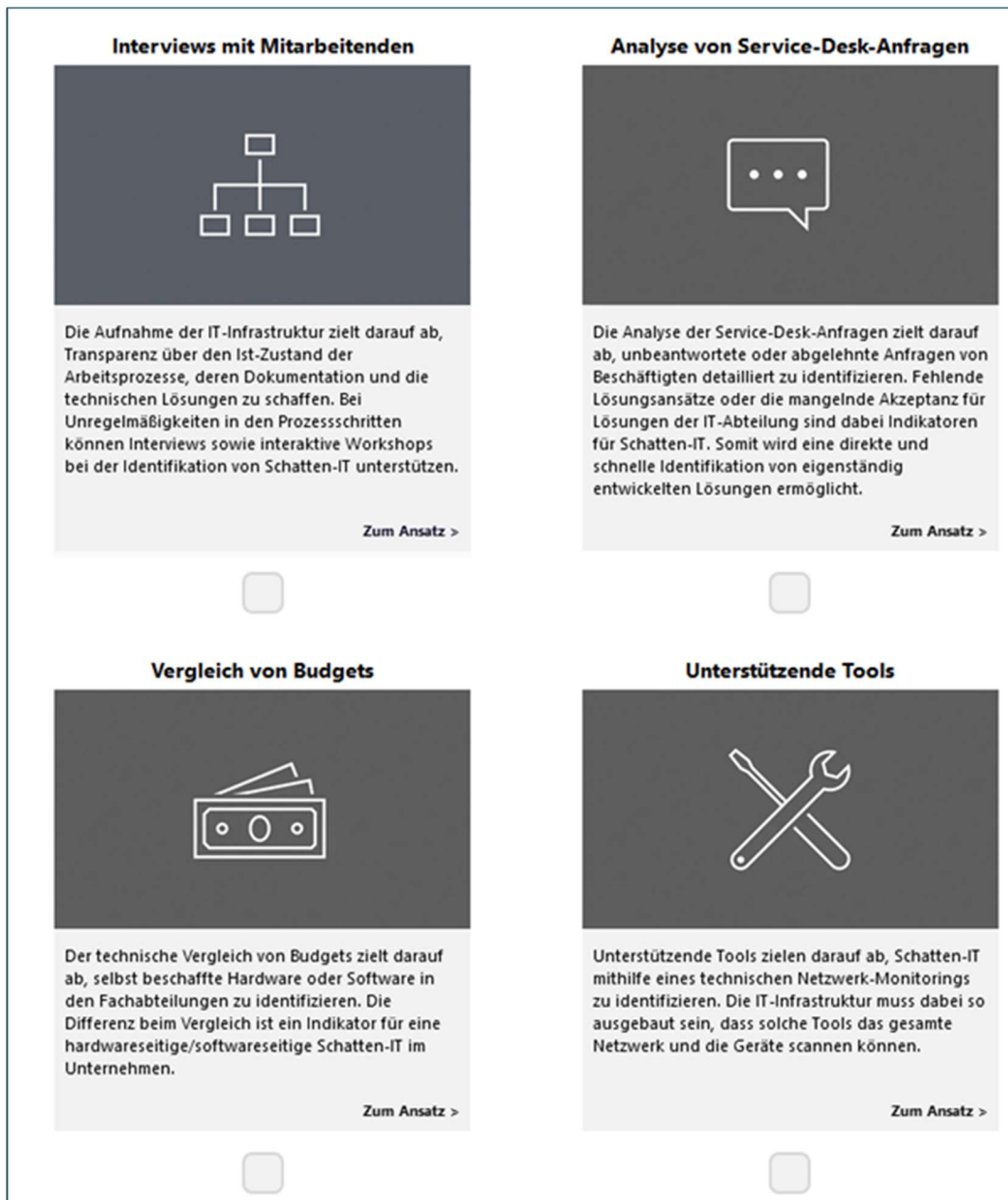


Abbildung 26: Ansätze zur Identifikation von Schatten-IT (eigene Darstellung)

Schritt 3: Erfassung

Nachdem existierende Schattenlösungen identifiziert worden sind, gilt es, diese im Tool zu erfassen und umfangreich zu charakterisieren sowie zu bewerten. Hierzu hat der Anwendende die Möglichkeit, in einer Eingabemaske die einzelnen Applikationen einzutragen (s. Abbildung 27). Um Unternehmen ein ganzheitliches Tool bereitzustellen, können zudem die zentralen Systeme der IT-Infrastruktur erfasst werden, falls dies vom Anwendenden gewünscht wird. Die Eingabemaske zur Aufnahme von Schattenlösungen umfasst neben dem Namen, einer Beschreibung und der Nennung des Nutzerkreises auch eine Kategorisierung. Es ist möglich, die Schattenlösung als technische, betriebswirtschaftliche, übergreifende Lösung usw. zu klassifizieren und eine Typisierung (z. B. CAD, CAM, ERP, HR, CRM) vorzunehmen. Im nächsten Schritt erfolgt die Bewertung. Dem Anwendenden werden verschiedene Optionen für Nutzen und Risiken aufgezeigt, die per Mausklick ausgewählt werden müssen. Die Identifikation, welcher Aspekt als Nutzen oder Risiko eingestuft wird, erfolgt hierbei auf individueller Basis durch Gespräche mit den Fachbereichen bzw. den

Entwicklern der Schattenlösung. Darüber hinaus können weitere Merkmale wie Prozesskritikalität, Informationsqualität oder die technische Qualität der Lösung angegeben werden. Für eine vollständige und detaillierte Auswertung ist es notwendig, alle Felder der Eingabemaske auszufüllen.

The form contains the following sections and data:

- Name:** Beispiel 1
- Beschreibung:** Excel-Dokument
- Nutzerkreis:** 8
- Kategorie:** Betriebswirtschaftliche Anwendungen
- Typ:** ReWe / FiBu: Finanzbuchhaltung & Rechnungswesen
- Nutzen:**
 - Buttons: Innovative Lösung, Lösung für IT-Defizit, Lösung für funktionales Defizit, Effizienz, Produktivität, Vereinfachung von Prozessen, Flexibilität, Zusammenarbeit.
 - Text: zusätzliche Makros ermöglichen Funktionen, die in anderen Programmen nicht verfügbar sind.
- Risiken:**
 - Buttons: Datenvollständigkeit, Zugriff, Verarbeitung personenbezogener Daten, Medienbrüche, Integrationsaufwand, Verarbeitung sensibler Daten, Kosten, Personale Abhängigkeit.
 - Text: die Applikation ist nicht mit den internen ReWe-/FiBu-Systemen verknüpft. Daher ist eine automatisierte Datenübertragung nicht gegeben, wodurch eine erhöhte Fehleranfälligkeit besteht.
- weitere Merkmale:**
 - Prozesskritikalität: 1 (empty), 2 (empty), 3 (empty), 4 (filled), 5 (empty)
 - Informationsqualität: 1 (filled), 2 (empty), 3 (empty), 4 (empty), 5 (empty)
 - Support: 1 (filled), 2 (empty), 3 (empty), 4 (empty), 5 (empty)
 - Technische Qualität: 1 (empty), 2 (empty), 3 (filled), 4 (empty), 5 (empty)
 - Benutzerfreundlichkeit: 1 (empty), 2 (empty), 3 (empty), 4 (empty), 5 (filled)
 - Redundanz: Nein (empty), Ja (filled)

Abbildung 27: Eingabemaske zur Erfassung von Schatten-IT (eigene Darstellung)

Schritt 4: Auswertung

Nachdem der Anwendende alle identifizierten Schattenlösungen im vorherigen Schritt in der Eingabemaske erfasst hat, erfolgt im weiteren Vorgehen die Visualisierung und Auswertung. Im Rahmen einer Risiko-Nutzen-Matrix wird eine übersichtliche Darstellung geliefert. Diese soll einen ersten Eindruck über die Auswirkungen der einzelnen Applikationen liefern. Aus Gründen der Übersichtlichkeit wird zusätzlich eine zusammenfassende Tabelle mit den relevanten Kopfdaten aufgezeigt (s. Abbildung 28). Die Visualisierung der eingegebenen Informationen bietet zeitgleich die Möglichkeit, Managemententscheidungen visuell unterstützt in einer verständlichen Darstellung vorzubereiten.



Abbildung 28: Visualisierung und Auswertung der erfassten Schattenlösungen (eigene Darstellung)

Schritt 5: Lösungsansätze

Im letzten Schritt werden die zuvor erfassten und visualisierten Schattenlösungen bewertet und Lösungsvorschläge gegeben (s. Abbildung 29). Diese orientieren sich an den erarbeiteten Forschungsergebnissen und können Ablösung, Abschaltung, Registrierung, Governance und Legitimierung beinhalten. Da mitunter mehrere Ansätze in kombinierter Form (z. B. Legitimierung bei zeitgleicher Schaffung einer Governance) infrage kommen, kann eine Mehrfachauswahl möglich sein. Dies geschieht in Abhängigkeit der zuvor bewerteten Risiken und Nutzen. Die detaillierte Logik zur Auswahl der Lösungsansätze ist im folgenden Kapitel dargestellt. An dieser Stelle muss erwähnt werden, dass die Lösungsansätze einer wissenschaftlichen Herleitung entstammen und lediglich eine Entscheidungsunterstützung darstellen. Der individuelle Umgang mit Schatten-IT muss im Unternehmen geprüft und die Anwendbarkeit der Lösungsansätze validiert werden. Der Anwendende hat die Möglichkeit, weiterführende Informationen zu den einzelnen Lösungsansätzen per Mausklick einzuholen.

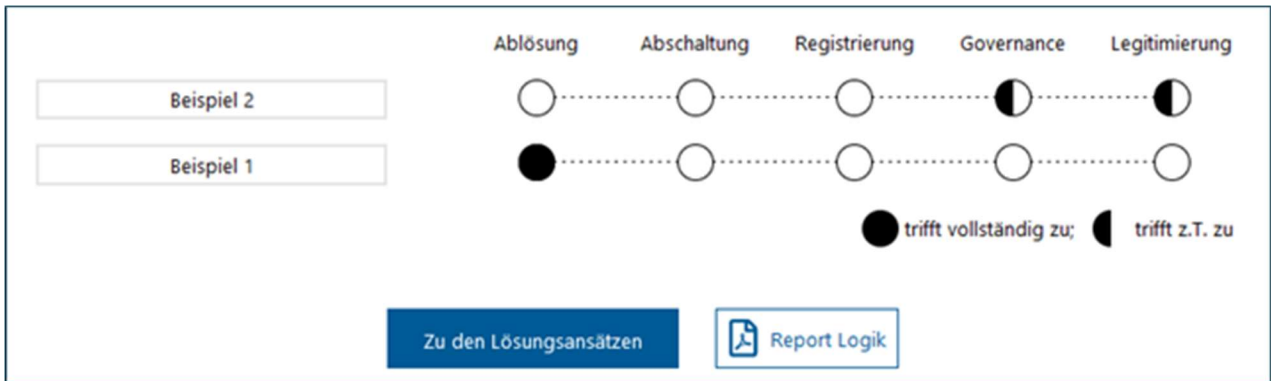


Abbildung 29: Bewertung und Darstellung der Eignung von Lösungsansätzen (eigene Darstellung)

3.4.2 Funktionsweise des Webdemonstrators

Die erfassten Anwendungen werden auf Basis einer Logik, die im Hintergrund des Tools läuft, zunächst anhand des Nutzen- und Risikoverhältnisses im Portfolio visualisiert und anschließend den Lösungsansätzen zugeordnet. Im Folgenden wird beschrieben, wie sich der Nutz- und Risikowert einer Anwendung zusammensetzt.

Nutzwert

Die in der Eingabemaske der jeweiligen Anwendung ausgewählten Nutzenaspekte ergeben kumuliert einen Nutzwert. Dieser setzt sich folgendermaßen zusammen: Jeder Nutzenaspekt hat einen Wert von 1. Das im Schritt „Gewichtung“ vorgenommene Ranking der Aspekte der individuellen IT-Strategie beeinflusst den Wert des Nutzenaspekts zusätzlich je nach Priorisierung. Der an erster Stelle gesetzte Aspekt fließt mit einem Faktor von 1,5 ein, der an zweiter Stelle gesetzte Aspekt mit einem Faktor von 1,4 und so weiter (minimaler Faktor von 1,0). Dieser Faktor wird mit dem Wert des Nutzenaspekts multipliziert. Die Nutzenaspekte sind gemäß Tabelle 9 den Aspekten der IT-Strategie wie folgt zugeordnet:

Tabelle 9: Matching der IT-Aspekte mit den Nutzen-Merkmalen (eigene Darstellung)

Aspekt der IT-Strategie	Nutzen
Prozessstandardisierung und -optimierung	Vereinfachung von Prozessen
Effizienz heben	Effizienz
Zentrale IT ist ganzheitlicher Lösungsanbieter	Lösung für IT-Defizit und Lösung für funktionales Defizit
Zentrale IT ist Enabler für Zusammenarbeit, Produktivität und Flexibilität	Zusammenarbeit, Produktivität und Flexibilität
Innovationsfähigkeit unterstützen	Innovative Lösungen

Der kumulierte Nutzwert addiert sich aus den gewichteten Werten der ausgewählten Nutzenaspekte. Der maximale Nutzwert einer Anwendung liegt somit bei 10,9.

Risikowert

Analog zum Nutzwert errechnet sich der kumulierte Risikowert aus den Risiken, die für die jeweilige Anwendung in der Erfassungsmaske ausgewählt wurden. Auch hier hat jedes in der Erfassung ausgewählte Risiko an sich einen Wert von 1. Das Ranking der Aspekte im Schritt „Gewichtung“ beeinflusst den Wert der Risiken mit einem maximalen Faktor von 1,5 bis zu einem minimalen Faktor von 0,9. Die Nutzenaspekte sind den Aspekten der IT-Strategie gemäß Tabelle 10 wie folgt zugeordnet:

Tabelle 10: Matching der IT-Aspekte mit den Risiko-Merkmalen (eigene Darstellung)

Aspekt der IT-Strategie	Risiko
Prozessstandardisierung und -optimierung	Medienbrüche
Systemintegration vorantreiben	Integrationsaufwand
Datenschutz sicherstellen	Verarbeitung personenbezogener Daten
Schutz vor Betriebsgeheimnissen sicherstellen	Verarbeitung sensibler Daten und Zugriff
Datenqualität und -validität sicherstellen	Datenvalidität
Datenverfügbarkeit sicherstellen	Personale Abhängigkeit
Wirtschaftlichkeit heben	Kosten

Der kumulierte Risikowert addiert sich aus den gewichteten Werten der ausgewählten Risiken. Der maximale Risikowert einer Anwendung liegt somit bei 9,9.

Das Nutzen- und Risikoverhältnis wird für jede Anwendung im Portfolio visualisiert. Die Koordinaten zeigen dabei den jeweiligen Nutzwert (y-Achse) und Risikowert (x-Achse) an. Im Folgenden wird die Zuordnung zu den Lösungsansätzen beschrieben.

Zuordnung zu den Lösungsansätzen

Für die Zuordnung zu den Lösungsansätzen fließen neben dem Nutz- und Risikowert noch die Merkmale Qualität, Relevanz und Redundanz mit ein. Die Dimensionen Technische Qualität, Informationsqualität, Benutzerfreundlichkeit und Support aus der Erfassungsmaske ergeben im Mittelwert das Merkmal Qualität (maximaler Wert von 5). Die Dimensionen **Prozesskritikalität** und **Nutzerkreis** aus der Erfassungsmaske ergeben im Mittelwert das Merkmal **Relevanz** (maximaler Wert von 5). Die Werte für den Nutzerkreis ergeben sich gemäß Tabelle 11 hierbei wie folgt:

Tabelle 11: Wertzuordnung in Abhängigkeit von der Nutzeranzahl (eigene Darstellung)

Nutzeranzahl	Wert
0	0
0 bis 4	1
5 bis 8	2
9 bis 12	3
13 bis 16	4
17 und höher	5

Die Zuordnung der Anwendungen zu den Lösungsansätzen erfolgt anhand nach Tabelle 12 folgender Grenzwerte der jeweiligen Merkmale:

Tabelle 12: Bewertungslogik zur Auswahl der Lösungsansätze (eigene Darstellung)

Lösungsansatz	Variable	Cases
Ablösung	Redundanz	Redundanz <i>true</i>
Abschaltung	Nutzwert	Nutzwert <5 und Risikowert >5
	Risikowert	
	Qualität	Qualität <2 und Relevanz <2
	Relevanz	
Registrierung	Nutzwert	Nutzwert >6 und Risikowert <4
	Risikowert	
	Qualität	Qualität >3 und Relevanz <4
	Relevanz	
Governance	Nutzwert	Nutzwert >4 und Risikowert >3
	Risikowert	
	Qualität	Qualität >3 und Relevanz >2
	Relevanz	
Legitimierung	Nutzwert	Nutzwert >7 und Risikowert >6
	Risikowert	
	Qualität	Qualität <4 und Relevanz >3
	Relevanz	

Ist einer der Cases erfüllt, wird die Anwendung mit „50 %“ beim jeweiligen Lösungsansatz eingefärbt, sind beide Cases erfüllt, mit „100 %“.

3.4.3 Validierung des Webdemonstrator mit dem projektbegleitenden Ausschuss

Das IT-Tool wurde in verschiedenen Entwicklungsstadien in Interviews mit dem pbA vorgestellt und validiert. Die Interviewpartner konnten aufgrund der kurzzyklischen Einbindung wertvolles Feedback liefern, um das Tool anwendungsfreundlicher zu gestalten. Im Rahmen des vierten und letzten

Treffens des pbAs wurden das gesamte Tool sowie die darin integrierte Logik vorgestellt. Die Unternehmen aus der Praxis bestätigten den hohen Nutzen und das Innovationspotenzial dieser Applikation.

3.5 Arbeitspaket 5: Entwicklung eines Reifegradmodells für den Umgang mit Schatten-IT

Das fünfte Arbeitspaket diente dem Ziel, ein praxisnahes Reifegradmodell für den Umgang mit Schatten-IT zu entwickeln. Im Forschungsantrag wurde ursprünglich die monetäre Quantifizierung der Legitimierung von Schatten-IT forciert. Dies wurde jedoch von den Unternehmen des pbAs als nicht zielführend, praxistauglich und umsetzbar bewertet. Hauptgrund war die fehlende Reife der Prozesse in den Unternehmen. In enger Abstimmung mit den Praxispartnern wurde deshalb der Fokus des Arbeitspakets auf die Entwicklung eines Reifegradmodells zum Umgang mit Schatten-IT gelegt. Der Mehrwert eines solchen Reifegradmodells für die Praxis wurde vom pbA als hoch eingeschätzt. Die Bearbeitung des Arbeitspakets erfolgte im Wesentlichen in drei Arbeitsschritten, wie Abbildung 30 grafisch darstellt. In Kapitel 3.5.1 wurden die Grundlagen für die Entwicklung des Reifegradmodells erarbeitet. Kapitel 3.5.2 fokussiert die inhaltlichen und formalen Anforderungen an das Reifegradmodell. Kapitel 3.5.3 umfasst die schrittweise Entwicklung und Validierung des Reifegradmodells zum Umgang mit Schatten-IT.

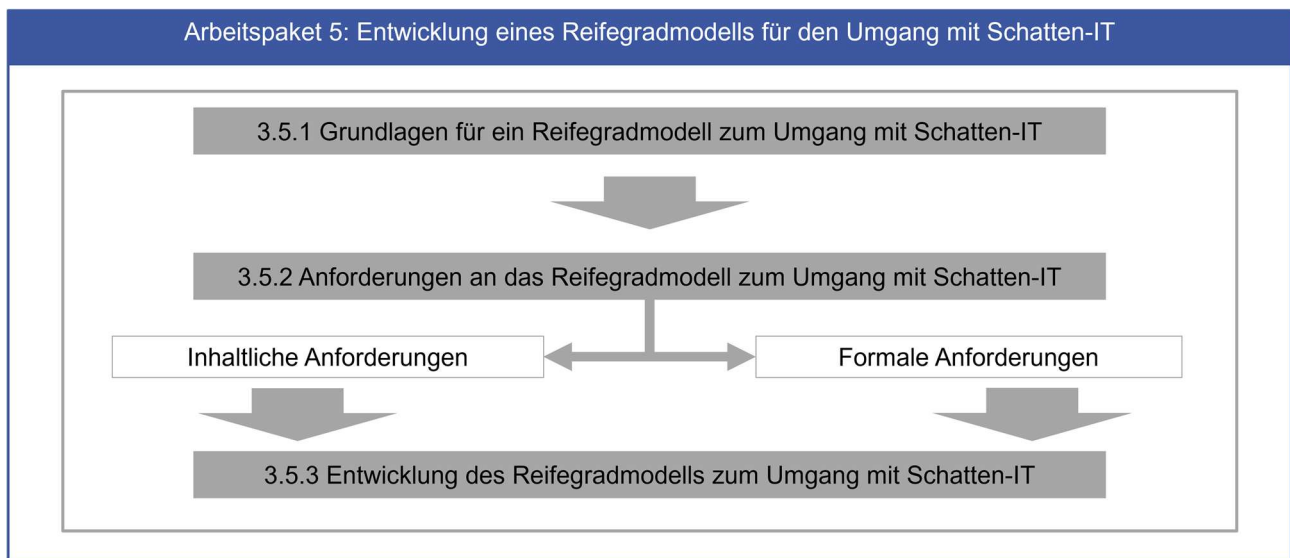


Abbildung 30: Vorgehen in Arbeitspaket 5 (eigene Darstellung)

3.5.1 Grundlagen für ein Reifegradmodell zum Umgang mit Schatten-IT

Die bisherigen Ergebnisse des Forschungsprojekts haben gezeigt, dass sich Unternehmen beim Umgang mit Schatten-IT nicht nur mit technischen, sondern ebenso mit organisatorischen und menschlichen Aspekten konfrontiert sehen. Zudem wurde aus den zahlreichen Fallstudien und Experteninterviews mit Praxispartnern ersichtlich, dass Unternehmen unterschiedliche Reifegrade im Umgang mit Schatten-IT aufweisen. Manche sind diesbezüglich weit fortgeschritten und haben beispielsweise bereits standardisierte Prozesse zur Identifikation von Schatten-IT implementiert, andere (und häufig KMU) haben wiederum erst kürzlich begonnen, den Themenkomplex Schatten-IT in ihrer IT-Strategie zu adressieren. Damit Unternehmen ihre Entwicklungsstufe im Umgang mit Schatten-IT mithilfe eines praxistauglichen Werkzeugs analysieren können, wurde in Absprache und enger Zusammenarbeit mit dem pbA ein Reifegradmodell entwickelt. Ein solches Reifegradmodell ermöglicht eine strukturierte Vorgehensweise bei der Analyse der Entwicklungsstufe (s. Willeke u. Kassermann 2016). Dabei wird die Realwelt durch eine vereinfachte Darstellung eines stufenweisen Entwicklungspfades skizziert (s. Schütte 1998). Der Begriff **Reife** beschreibt in diesem Zusammenhang den evolutionären Entwicklungsprozess von einem Anfangszustand zu einem erwünschten Endzustand einer bestimmten Zielerreichung oder einer bestimmten Fähigkeit (s.

Mettler u. Rohner 2009). Die erreichte Stufe im Reifegradmodell wird als Reifegrad bezeichnet. Durch die Bestimmung einer Reifegradstufe kann der derzeitige Ist-Zustand eines Unternehmens hinsichtlich des Umgangs mit Schatten-IT identifiziert werden. Davon ausgehend kann ein Unternehmen sein Verbesserungspotenzial erkennen, wodurch Handlungsmaßnahmen zur Erreichung einer höheren Reifegradstufe abgeleitet werden können (s. Schütte 1998).

3.5.2 Anforderungen an das Reifegradmodell zum Umgang mit Schatten-IT

Die spezifischen Anforderungen an das Schatten-IT-Reifegradmodell werden von Becker et al. (2009) abgeleitet. Die Anforderungen werden dabei in inhaltliche und formale Anforderungen gegliedert.

Inhaltliche Anforderungen

Das Schatten-IT-Reifegradmodell soll sinnvolle Entwicklungsstufen sowie Merkmalsausprägungen beinhalten, welche den Ist-Zustand eines Unternehmens hinsichtlich des Umgangs mit Schatten-IT widerspiegeln (s. Becker et al. 2008). In anderen Worten ist das Reifegradmodell mindestens als ein deskriptives Modell zu gestalten. Ein Reifegradmodell mit deskriptivem Charakter beschreibt, wie anhand festgelegter Kriterien der Ist-Zustand bzw. die aktuellen Fähigkeiten beurteilt werden können. Ein Reifegradmodell dieser Art stellt ein Diagnoseinstrument dar. Hingegen stellt ein Reifegradmodell mit präskriptivem Charakter darüber hinaus Verbesserungsmaßnahmen zur Verfügung. Zuletzt können Reifegradmodelle auch für Zwecke des Benchmarkings – intern oder extern – verwendet werden. Hierfür wird jedoch eine ausreichende Menge an historischen Daten benötigt, um bspw. den eigenen Reifegrad mit anderen Organisationen vergleichen zu können (s. Pöppelbuß u. Röglinger 2011). Darüber hinaus wird von dem zu entwickelnden Reifegradmodell verlangt, dass dessen Gültigkeit nicht von einer bestimmten Branche oder Unternehmensgröße abhängt. Weiterhin soll das Reifegradmodell möglichst vollumfänglich alle Aspekte abdecken, die den Umgang mit Schatten-IT im Unternehmen kennzeichnen. Das bedeutet, dass das Reifegradmodell möglichst genau den Ist-Zustand abbilden soll. Darüber hinaus wird gefordert, dass das Reifegradmodell auf inhaltlich relevante Aspekte anderer Konzepte oder Modelle Bezug nimmt. Ebenfalls soll die Praxisnähe des Reifegradmodells gewährleistet sein (s. Becker et al. 2008).

Formale Anforderungen

Bezüglich der Struktur eines Reifegradmodells wird eine Orientierung an bewährten Modellen empfohlen, um sowohl dessen Verständlichkeit als auch Anwendbarkeit zu gewährleisten (s. Becker et al. 2008). Bis zu fünf Reifegradstufen gelten zudem als sinnvolle Anzahl (s. Bruin et al. 2005). Auch sollte ein Reifegradmodell aussagekräftige Beschreibungen für jede Reifegradstufe beinhalten. Weitere Anforderungen sind die Definition der Reifegradstufen als Zusammenfassung der wesentlichen Kriterien, eine Beschreibung der Elemente innerhalb der Reifegradstufe und das Vorhandensein einer bestimmten Anzahl an Dimensionen sowie einer bestimmten Anzahl von Elementen für jede Dimension (s. Becker et al. 2008).

3.5.3 Entwicklung des Reifegradmodells zum Umgang mit Schatten-IT

Die Entwicklung des Reifegradmodells zum Umgang mit Schatten-IT folgt dem Vorgehensmodell nach Neff et al. (2014) und umfasst vier Vorgehensschritte (s. Abbildung 31). Diese umfassen die Problemdefinition, den Vergleich bestehender Reifegradmodelle, die literaturgestützte Entwicklung des Reifegradmodells und die Durchführung und Validierung des Reifegradmodells.

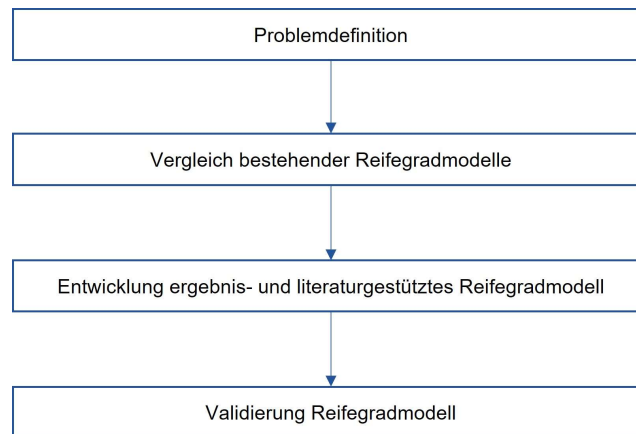


Abbildung 31: Vorgehensweise zur Entwicklung des Reifegradmodells (eigene Darstellung i. A. a. Neff et al. 2014, S. 3)

Problemdefinition

Wie in Kapitel 3.2.3 beschrieben, wird für Unternehmen ein praxistaugliches Werkzeug zur Analyse ihrer Entwicklungsstufe im Umgang mit Schatten-IT benötigt. Dies erfordert jedoch einen ganzheitlichen Ansatz, der nicht nur technische bzw. IT-seitige Aspekte von Schatten-IT, sondern insbesondere auch organisatorische und personelle Faktoren adressiert.

Bestehende Reifegradmodelle

Die durchgeführte Literaturrecherche hatte zum Ziel, bestehende Reifegradmodelle zu identifizieren, die sich explizit auf den Umgang mit Schatten-IT beziehen und dabei sowohl organisatorische, menschliche als auch technische Aspekte berücksichtigen. Hierbei konnte kein Reifegradmodell identifiziert werden, welches die genannten Kriterien erfüllt. Es konnten nur Reifegradmodelle identifiziert werden, die sich auf das generelle IT-Management beziehen. Anhang 7 umfasst die Steckbriefe der identifizierten Reifegradmodelle. Ein beispielhaftes, existierendes Modell aus dem Bereich IT-Management ist das Capability-Maturity-Model (CMM). Dieses bezieht sich auf die Optimierung von Entwicklungsprozessen innerhalb eines Unternehmens und berücksichtigt daher lediglich das Management von Central-Managed-IT (s. Paulk et al. 1993). Ein weiteres Modell ist das Software-Process-Improvement-and-Capability-Determination-Framework (SPICE). Sein Fokus liegt auf der Bewertung von Entwicklungsprozessen anhand internationaler Standards. Ähnlich wie beim CMM liegt jedoch auch hier der Fokus auf offiziellen Anwendungen und umfasst lediglich technische Aspekte (s. Renault et al. 2015). Das Business-IT-Maturity-Model (s. Pearlson u. Saunders 2007) bewertet, inwieweit die Anforderungen der Fachabteilung ("Business-Demand") durch die IT-Abteilung abgedeckt werden ("IT-Supply"). Eine niedrige Reife eines Unternehmens in diesem Modell könnte daher das Auftreten von Schatten-IT befördern, dies wird aber nicht explizit aufgeschlüsselt. Keines der identifizierten Reifegradmodelle eignet sich demnach, um den Ist-Zustand eines Unternehmens in Bezug auf den Umgang mit Schatten-IT abzubilden. Umso notwendiger wird die Entwicklung eines ebensolchen Reifegradmodells im Rahmen dieses Forschungsprojekts eingeschätzt.

Festlegung der Entwicklungsstrategie

Das Reifegradmodell wird aus den bisherigen Ergebnissen des Forschungsprojekts sowie ergänzender Literatur ausgestaltet. Die iterative Entwicklung des Reifegradmodells erfolgt durch zwei Iterationen mittels eines Top-down-Ansatzes. Zunächst werden die Art und der Aufbau des Reifegradmodells vorgestellt. Im Anschluss wird der Inhalt des Reifegradmodells anhand der bisherigen Projektergebnisse und ergänzender Literatur ausgearbeitet.

Art und Aufbau des Reifegradmodells

Das Reifegradmodell zum Umgang mit Schatten-IT wird als ein stufenförmiges Reifegradmodell ausgestaltet. Zudem wird das zu entwickelnde Reifegradmodell als ein *Maturity*-Reifegradmodell konzipiert. *Maturity*-Reifegradmodelle bilden den aktuellen Entwicklungszustand bzw. die Reife eines Unternehmens in Bezug auf eine Fähigkeit, Technologie oder Konzepte ab. Das im Rahmen des Forschungsprojekts entwickelte *Maturity*-Reifegradmodell bildet den Ist-Zustand eines Unternehmens in Bezug auf den Umgang mit Schatten-IT ab, also wie diese spezifische Herausforderung im Unternehmen auf organisatorischer, menschlicher und technischer Ebene adressiert wird.

Der Stufenlogik von Willeke und Kasselmann (2016) folgend, erstrecken sich die Reifegradstufen von 0 bis 3. Die Bezeichnung der Reifegradstufen wurde aus den bisherigen Ergebnissen des Forschungsprojekts abgeleitet und mit dem pbA sowie zwei Fallstudienpartnern validiert. Reifegrad 0 beschreibt Unternehmen, in denen Schatten-IT als Problem gänzlich ignoriert wird. In Reifegrad 1 sind Unternehmen verortet, in denen ein Problembewusstsein für Schatten-IT vorhanden ist, jedoch bisher keine Standards für den Umgang existieren. Reifegrad 2 umfasst Unternehmen, in denen Standards für den Umgang mit Schatten-IT vorhanden und unternehmensweit implementiert sind. Der letzte Reifegrad 3 beschreibt Unternehmen, die ihre Standards für den Umgang mit Schatten-IT kontinuierlich prüfen und optimieren (s. Tabelle 13).

Tabelle 13: Bezeichnung und Kurzbeschreibung der Reifegradstufen

RG	Bezeichnung	Kurzbeschreibung
0	Ignorance	Schatten-IT wird im Unternehmen als Problem ignoriert.
1	Awareness	Ein Problembewusstsein für Schatten-IT ist im Unternehmen vorhanden, es gibt jedoch keine Standards für den Umgang.
2	Management	Standards für den Umgang mit Schatten-IT sind im Unternehmen vorhanden und unternehmensweit implementiert.
3	Optimization	Die Standards für den Umgang mit Schatten-IT im Unternehmen werden kontinuierlich geprüft und verbessert. Die Herangehensweise ist proaktiv.

RG = Reifegrad

Struktur des Reifegradmodells

Das Reifegradmodell soll aus Gestaltungsebenen, Gestaltungsdimensionen, Gestaltungsobjekten und Reifegraden bestehen sowie stufenabhängige Anforderungen umfassen. *Gestaltungsebenen* fassen dabei die themenrelevanten Anforderungen zusammen. Die Gestaltungsebenen für das vorliegende Reifegradmodell sind: Organisation, Mensch und Technologie. Dabei kann eine Gestaltungsebene mehrere *Gestaltungsdimensionen* umfassen. Gestaltungsdimensionen dienen dazu, die Gestaltungsebene weiter zu konkretisieren. Hierzu kann eine Gestaltungsdimension ein oder mehrere *Gestaltungsobjekte* beinhalten. Diese dienen der Reifegradbeurteilung und nehmen entlang der Reifegrade eine unterschiedliche Ausprägung an. Für die Festlegung der *stufenabhängigen Anforderungen* werden jedem Gestaltungsobjekt – sofern keine Übertragung aus anderen Reifegradmodellen möglich ist oder sich Ausprägungen aus der Literatur ableiten lassen – ordinalskalierte Merkmalsausprägungen zugeordnet. Handelt es sich hierbei um qualitative Merkmale, dann können auch sprachliche Ausprägungen verwendet werden.

Validierung des Reifegradmodells mit der Praxis

Die erste Version des Reifegradmodells zum Umgang mit Schatten-IT wurde auf Basis der bisherigen Ergebnisse des Forschungsprojekts sowie ergänzender Literatur entwickelt und daraufhin im Rahmen von zwei Treffen mit dem pbA (09.12.2021 und 31.05.2022) sowie Experteninterviews mit Praxispartnern (18.05.2022 und 10.05.2022) validiert. Die Experteninterviews wurden auf Basis eines halbstandardisierten Leitfadens durchgeführt (s. Anhang 8). Einerseits hatte die Validierung zum Ziel, die Verständlichkeit des Reifegradmodells abzufragen sowie Verbesserungspotenzial zu identifizieren und die Gewichtung innerhalb des Reifegradmodells zu bestimmen. Im Rahmen der Validierung wurden folgende Verbesserungsvorschläge und Anforderungen in das finale Reifegradmodell integriert:

- Die Ausprägungen sollten kurz und kompakt dargestellt werden.
- Das Reifegradmodell sollte möglichst allgemein gefasst werden, um eine erste Einschätzung des Unternehmens im Hinblick auf den Umgang mit Schatten-IT zu ermöglichen.
- Es soll ein Schwerpunkt auf die Gestaltungsebenen Organisation und Mensch gelegt werden, da diese beim unternehmensweiten Umgang mit Schatten-IT besonders relevant sind.
- Ein Self-Assessment zur Ermittlung des Gesamtreifegrads wird als sinnvoll eingeschätzt.

Um Dopplungen zu vermeiden, wird im nachfolgenden Abschnitt das angepasste und bereits validierte Reifegradmodell beschrieben.

Validiertes ergebnis- und literaturgestütztes Reifegradmodell

Im folgenden Abschnitt wird die inhaltliche Ausarbeitung des Reifegradmodells zum Umgang mit Schatten-IT vorgenommen. Das Reifegradmodell umfasst die drei Gestaltungsebenen *Organisation*, *Mensch* und *Technologie*, die sich wiederum in sechs Gestaltungsdimensionen kategorisieren lassen. Die Gestaltungsdimensionen umfassen: *Strategie und Führung*, *Unternehmenskultur*, *Organisation und Prozesse*, *Schulung und Awareness*, *Kollaboration* und *unterstützende Technologien*. Ferner werden die Gestaltungsdimensionen in 19 Gestaltungsobjekte unterteilt. Abbildung 32 gibt einen Überblick über die Gestaltungsebenen, Gestaltungsdimensionen und Gestaltungsobjekte. Die Ausarbeitung der Ausprägungen der jeweiligen Reifegradstufen stützt sich primär auf die erarbeiteten Ergebnisse des Forschungsprojekts, die Validierung mit der Praxis sowie auf ergänzende Literatur.



Abbildung 32: Übersicht über das Reifegradmodell zum Umgang mit Schatten-IT (eigene Darstellung)

Gestaltungsebene Organisation

Die Gestaltungsebene *Organisation* stellt Themen wie bspw. IT-Strategie und Führung, Unternehmens- und Feedbackkultur, Prozesse zur Identifikation von Schatten-IT oder Ressourcenverfügbarkeit zur Durchführung in den Mittelpunkt. Hierfür werden die entsprechenden Gestaltungsdimensionen weiter in Gestaltungsobjekte untergliedert. Im Folgenden werden die Gestaltungsdimensionen und -objekte sowie die Ausprägungen in den einzelnen Reifegraden beschrieben.

Strategie und Führung

Die Gestaltungsdimension *Strategie und Führung* beurteilt mit ihren zwei Gestaltungsobjekten, inwieweit der Umgang mit Schatten-IT im Unternehmen strategisch adressiert und entsprechende Initiativen auf Management-Ebene unterstützt werden. Mit dem Gestaltungsobjekt *IT-Strategie* kann beurteilt werden, inwieweit Richtlinien für den Umgang mit Schatten-IT in der IT-Strategie des Unternehmens verankert sind. In der Ausprägung 0 sind keinerlei Richtlinien vorhanden, während in der Ausprägung 1 teilweise Richtlinien für den Umgang mit Schatten-IT verankert sind. In der Ausprägung 2 sind Unternehmen verortet, die bereits umfassende Richtlinien zum Umgang mit Schatten-IT in ihrer IT-Strategie verankert haben. Gemäß der Reifegradbeschreibung umfasst die Ausprägung 3 Unternehmen, die diese Richtlinien nicht nur umfassend verankert haben, sondern diese regelmäßig überprüfen (s. Tabelle 14).

Tabelle 14: Ausprägungen Gestaltungsobjekt IT-Strategie

RG	Ausprägung
0	Die IT-Strategie beinhaltet keine Richtlinien für den Umgang mit Schatten-IT.
1	Die IT-Strategie beinhaltet nur wenige Richtlinien für den Umgang mit Schatten-IT.
2	Die IT-Strategie beinhaltet umfassende Richtlinien für den Umgang mit Schatten-IT.
3	Die IT-Strategie beinhaltet umfassende Richtlinien für den Umgang mit Schatten-IT, die regelmäßig überprüft werden.

Mit dem Gestaltungsobjekt *Unterstützung durch das Management* wird abgebildet, inwieweit die Führungsebene im Unternehmen Initiativen zum Umgang mit Schatten-IT befürwortet. In der Ausprägung 0 werden Initiativen zum Umgang mit Schatten-IT nicht auf Managementebene unterstützt, während in der Ausprägung 1 diese in geringem Maße unterstützt werden. In der Ausprägung 2 sind Unternehmen verortet, in denen Initiativen zum Umgang mit Schatten-IT auf Managementebene unterstützt werden. Die Ausprägung 3 umfasst Unternehmen, in denen die Managementebene Initiativen zum Umgang mit Schatten-IT proaktiv unterstützt (s. Tabelle 15).

Tabelle 15: Ausprägungen Gestaltungsobjekt Unterstützung durch das Management

RG	Ausprägung
0	Initiativen zum Umgang mit Schatten-IT werden nicht auf Managementebene unterstützt.
1	Initiativen zum Umgang mit Schatten-IT werden nur in geringem Maße auf Managementebene unterstützt.
2	Initiativen zum Umgang mit Schatten-IT werden auf Managementebene unterstützt.
3	Initiativen zum Umgang mit Schatten-IT werden aktiv auf Managementebene unterstützt.

Unternehmenskultur

Anhand von drei Gestaltungsobjekten bildet die Gestaltungsdimension *Unternehmenskultur* ab, inwieweit das Thema Schatten-IT und der Umgang mit damit in der Kultur des Unternehmens verankert ist. Das erste Gestaltungsobjekt *Potenzialbewusstsein* bezieht sich auf die grundsätzliche Betrachtungsweise von Schatten-IT im Unternehmen. Im Vordergrund steht hier die Frage, ob sich das jeweilige Unternehmen über die möglichen Risiken, aber auch insbesondere die Nutzenpotenziale von Schatten-IT bewusst ist. Das Objekt ist vor dem Hintergrund, dass insbesondere KMU das Nutzenpotenzial von Schatten-IT ausschöpfen sollten, besonders relevant. In der ersten Ausprägung ist gemäß dem Reifegrad 0 weder ein Risiko- noch ein Potenzialbewusstsein für Schatten-IT vorhanden, da das Thema vom Unternehmen ignoriert wird. In Ausprägung 1 wird Schatten-IT weitestgehend als Risiko betrachtet, wohingegen in Ausprägung 2 sowohl ein Risiko- als auch ein Potenzialbewusstsein für Schatten-IT vorhanden ist. In Ausprägung 3 wird das Nutzenpotenzial von identifizierten Schatten-IT Anwendungen darüber hinaus aktiv geprüft (s. Tabelle 16).

Tabelle 16: Ausprägungen Gestaltungsobjekt Potenzialbewusstsein

RG	Ausprägung
0	Im Unternehmen ist weder ein Risiko- noch ein Potenzialbewusstsein für Schatten-IT vorhanden.
1	Schatten-IT wird im Unternehmen weitestgehend als Risiko betrachtet.
2	Im Unternehmen ist sowohl ein Risiko- als auch ein Potenzialbewusstsein für Schatten-IT vorhanden.
3	Im Unternehmen ist sowohl ein Risiko- als auch ein Potenzialbewusstsein für Schatten-IT vorhanden. Das Nutzenpotenzial identifizierter Schatten-IT wird aktiv geprüft.

Das zweite Gestaltungsobjekt IT-Feedbackkultur und Kommunikation fokussiert die Kommunikation seitens der zentralen IT an die Fachbereiche in Bezug auf Schatten-IT. In der ersten Ausprägung ignoriert die IT-Abteilung gemäß dem Reifegrad 0 das Thema Schatten-IT und kommuniziert diesbezüglich nicht mit den Fachabteilungen. In der Ausprägung 1 setzt die IT-Abteilung im Umgang mit Schatten-IT weitestgehend auf Verbote und kommuniziert diese linear, also einseitig, an die Fachabteilungen. Ausprägung 2 adressiert Unternehmen, in denen die IT-Abteilung im Umgang mit Schatten-IT tendenziell auf Richtlinien statt Verbote setzt. Gleichzeitig legt sie Wert auf eine zirkuläre, also gegenseitige und kontinuierliche Kommunikation mit den Fachabteilungen. Ausprägung 3 bildet eine offene und proaktive IT-Feedback-Kultur und -Kommunikation ab, in der die IT-Abteilungen im Umgang mit Schatten-IT auf Richtlinien setzt, aktiv mit den Fachabteilungen kommuniziert und regelmäßig Feedback einholt (s. Tabelle 17).

Tabelle 17: Ausprägungen Gestaltungsobjekt IT-Feedbackkultur und Kommunikation

RG	Ausprägung
0	Die IT-Abteilung ignoriert das Thema Schatten-IT und kommuniziert diesbzgl. nicht mit den Fachabteilungen.
1	Die IT-Abteilung setzt im Umgang mit Schatten-IT weitestgehend auf Verbote und kommuniziert diese linear an die Fachabteilungen.
2	Die IT-Abteilung setzt im Umgang mit Schatten-IT auf Richtlinien. Gleichzeitig legt sie Wert auf eine zirkuläre Kommunikation mit den Fachabteilungen.
3	Die IT-Abteilung setzt im Umgang mit Schatten-IT auf Richtlinien. Dabei kommuniziert sie aktiv mit den Fachabteilungen und holt regelmäßig Feedback ein.

Das dritte Gestaltungsobjekt *Transparenz* bildet ab, inwieweit der Entscheidungsprozess zum Umgang mit Schatten-IT den Fachabteilungen seitens der zentralen IT transparent gemacht wird. Solch ein Prozess beinhaltet bspw. die Entscheidung darüber, ob eine identifizierte Schatten-IT gänzlich abgeschaltet, registriert oder erneuert werden soll. In der ersten Ausprägung ignoriert die IT-Abteilung gemäß dem Reifegrad 0 das Thema Schatten-IT und es werden dementsprechend auch keine Entscheidungen über den Umgang mit dieser getroffen. In Ausprägung 1 werden Entscheidungen über den Umgang mit Schatten-IT von der IT-Abteilung getroffen und der Entscheidungsprozess ist nur wenig transparent. In Ausprägung 2 ist der Entscheidungsprozess hingegen transparent. Ausprägung 3 trifft zu, wenn Entscheidungen über den Umgang mit Schatten-IT von der IT-Abteilung in enger Abstimmung mit den Fachabteilungen getroffen werden und der Entscheidungsprozess dabei für alle betroffenen Parteien transparent ist (s. Tabelle 18).

Tabelle 18: Ausprägungen Gestaltungsobjekt Transparenz

RG	Ausprägung
0	Es werden keine Entscheidungen von der IT-Abteilung über den Umgang mit Schatten-IT getroffen.
1	Entscheidungen über den Umgang mit Schatten-IT werden von der IT-Abteilung getroffen. Der Entscheidungsprozess ist nur wenig transparent.
2	Entscheidungen über den Umgang mit Schatten-IT werden von der IT-Abteilung getroffen. Der Entscheidungsprozess ist transparent.
3	Entscheidungen über den Umgang mit Schatten-IT werden von der IT-Abteilung in enger Abstimmung mit den Fachabteilungen getroffen. Der Entscheidungsprozess ist für alle betroffenen Parteien transparent.

Organisation und Prozesse

Die Gestaltungsdimension *Organisation und Prozesse* bewertet anhand von fünf Gestaltungsobjekten, inwieweit der Umgang mit Schatten-IT in die Organisation und Prozesse des Unternehmens integriert ist und diese dokumentiert sowie standardisiert sind. Das Gestaltungsobjekt *Prozesse zur Identifikation von Schatten-IT* bewertet, ob und in welchem Ausmaß Prozesse, die gezielt Schatten-IT im Unternehmen identifizieren, vorhanden sowie dokumentiert sind. Ausprägung 0 charakterisiert Unternehmen, in denen keinerlei Prozesse zur Identifikation von Schatten-IT vorhanden sind. In Ausprägung 1 sind Unternehmen verortet, in denen Prozesse zur Identifikation von Schatten-IT vorhanden jedoch nicht dokumentiert sind. In Ausprägung 2 sind diese Prozesse in bereits in dokumentierter Form vorhanden und werden regelmäßig händisch durchgeführt. Ausprägung 3 erweitert dies um die automatisierte Durchführung sowie Überprüfung und Optimierung der Prozesse zur Identifikation von Schatten-IT (s. Tabelle 19).

Tabelle 19: Ausprägungen Gestaltungsobjekt Prozesse zur Identifikation von Schatten-IT

RG	Ausprägung
0	Prozesse zur Identifikation von Schatten-IT sind nicht vorhanden.
1	Prozesse zur Identifikation von Schatten-IT sind vorhanden, jedoch nicht dokumentiert.
2	Prozesse zur Identifikation von Schatten-IT sind in dokumentierter Form vorhanden und werden regelmäßig händisch durchgeführt.
3	Prozesse zur Identifikation von Schatten-IT sind in dokumentierter Form vorhanden und werden regelmäßig automatisiert durchgeführt, überprüft sowie ggf. optimiert.

Das zweite Gestaltungsobjekt *Prozesse zum Umgang mit Schatten-IT* legt einen Schwerpunkt auf die Prozesse zum Umgang mit identifizierten Schatten-IT-Anwendungen, ist also lösungsorientiert. In Ausprägung 0 sind gemäß dem Reifegrad 0 Unternehmen verortet, in denen keinerlei Prozesse zum Umgang mit Schatten-IT vorhanden sind. Ausprägung 1 umfasst Unternehmen, in denen solche Prozesse vorhanden, jedoch nicht dokumentiert sind. In Ausprägung 2 sind Prozesse zum Umgang mit identifizierter Schatten-IT bereits in dokumentierter Form vorhanden. Ausprägung 3 erweitert dies um die regelmäßige Überprüfung und Optimierung der Prozesse (s. Tabelle 20).

Tabelle 20: Ausprägungen Gestaltungsobjekt Prozesse zum Umgang mit Schatten-IT

RG	Ausprägung
0	Prozesse zum Umgang mit Schatten-IT sind nicht vorhanden.
1	Prozesse zum Umgang mit Schatten-IT sind vorhanden, jedoch nicht dokumentiert.
2	Prozesse zum Umgang mit Schatten-IT sind in dokumentierter Form vorhanden.
3	Prozesse zum Umgang mit Schatten-IT sind in dokumentierter Form vorhanden und werden regelmäßig überprüft sowie ggf. optimiert.

Die *Risiko- und Nutzenbewertung* stellt das dritte Gestaltungsobjekt dar und bildet ab, inwieweit identifizierte Schatten-IT im Unternehmen nach ihrem Risiko und Nutzenpotenzial bewertet wird. In der ersten Ausprägung wird gemäß dem Reifegrad 0 identifizierte Schatten-IT ignoriert und dementsprechend auch nicht auf ihr Risiko und Nutzenpotenzial hin analysiert. Ausprägung 1 charakterisiert Unternehmen, in denen identifizierte Schatten-IT nur vereinzelt und nicht systematisch nach ihrem Risiko und Nutzenpotenzial bewertet wird. In Ausprägung 2 erfolgt die Risiko- und Nutzenbewertung systematisch anhand festgelegter Kriterien. In Ausprägung 3 werden die Kriterien darüber hinaus regelmäßig überprüft und ggf. erweitert (s. Tabelle 21).

Tabelle 21: Ausprägungen Gestaltungsobjekt Risiko- und Nutzenbewertung

RG	Ausprägung
0	Identifizierte Schatten-IT wird ignoriert und nicht nach ihrem Risiko und Nutzenpotenzial bewertet.
1	Identifizierte Schatten-IT wird nur vereinzelt und nicht systematisch nach ihrem Risiko und Nutzenpotenzial bewertet.
2	Identifizierte Schatten-IT wird systematisch anhand festgelegter Kriterien nach ihrem Risiko und Nutzenpotenzial bewertet.
3	Identifizierte Schatten-IT wird systematisch anhand festgelegter Kriterien nach ihrem Risiko und Nutzenpotenzial bewertet. Die Kriterien werden regelmäßig überprüft und ggf. erweitert.

Das vierte Gestaltungsobjekt *Definition von Verantwortlichkeiten* bewertet, inwieweit die Verantwortlichkeiten im Sinne von Zuständigkeiten und Rollen der Mitarbeitenden im Umgang mit Schatten-IT definiert sowie dokumentiert sind (bspw. Vorhandensein von Ansprechpartnern und Meldestellen). In Ausprägung 0 sind Unternehmen verortet, in denen Verantwortlichkeiten für den Umgang mit Schatten-IT weder definiert noch dokumentiert sind. Ausprägung 1 umfasst Unternehmen, in denen die Verantwortlichkeiten definiert, jedoch nicht dokumentiert sind. In Ausprägung 2 sind Verantwortlichkeiten zum Umgang mit Schatten-IT bereits in dokumentierter Form vorhanden. Ausprägung 3 erweitert dies um die regelmäßige Überprüfung der Verantwortlichkeiten (s. Tabelle 22).

Tabelle 22: Ausprägungen Gestaltungsobjekt Definition von Verantwortlichkeiten

RG	Ausprägung
0	Verantwortlichkeiten für den Umgang mit Schatten-IT sind nicht definiert und dokumentiert.
1	Verantwortlichkeiten für den Umgang mit Schatten-IT sind definiert, aber nicht dokumentiert.
2	Verantwortlichkeiten für den Umgang mit Schatten-IT sind definiert und dokumentiert.
3	Verantwortlichkeiten für den Umgang mit Schatten-IT sind definiert sowie dokumentiert und werden regelmäßig überprüft.

Zuletzt bildet das Gestaltungsobjekt *Ressourcenbereitstellung* ab, inwieweit sowohl finanzielle als auch personelle Ressourcen für den Umgang mit Schatten-IT bereitgestellt werden. In der Ausprägung 0 werden gemäß dem Reifegrad keinerlei Ressourcen für den Umgang mit Schatten-IT bereitgestellt. Ausprägung 1 charakterisiert Unternehmen, in denen nur wenige Ressourcen für den Umgang mit Schatten-IT bereitgestellt werden, wohingegen in Ausprägung 2 ausreichend Ressourcen vorhanden sind. In Ausprägung 3 werden umfassende Ressourcen für den Umgang mit Schatten-IT zur Verfügung gestellt (s. Tabelle 23).

Tabelle 23: Ausprägungen Gestaltungsobjekt Ressourcenbereitstellung

RG	Ausprägung
0	Es werden keine Ressourcen für den Umgang mit Schatten-IT bereitgestellt.
1	Es werden nur wenige Ressourcen für den Umgang mit Schatten-IT bereitgestellt.
2	Es werden ausreichend Ressourcen für den Umgang mit Schatten-IT bereitgestellt.
3	Es werden umfassende Ressourcen für den Umgang mit Schatten-IT bereitgestellt.

Gestaltungsebene Mensch

Die Gestaltungsebene *Mensch* stellt die Themen Schulungen und Awareness sowie Kollaboration in den Mittelpunkt. Hierfür werden die entsprechenden Gestaltungsdimensionen weiter in Gestaltungsobjekte untergliedert. Im Folgenden werden die Gestaltungsdimensionen und -objekte sowie die Ausprägungen in den einzelnen Reifegraden beschrieben.

Schulung und Awareness

Die erste Gestaltungsdimension *Schulung und Awareness* bildet ab, inwieweit bei den Mitarbeitenden und Führungskräften ein Bewusstsein für die Risiken von Schatten-IT vorhanden ist und jene vom Unternehmen zum Thema geschult werden. Das erste Gestaltungsobjekt *Schulungen zum Thema Schatten-IT* adressiert die Weiterbildung der Mitarbeitenden zu Schatten-IT und die Integration solcher Weiterbildungen in das Schulungsangebot des Unternehmens. In Ausprägung 0 ist das Thema Schatten-IT nicht in das Schulungsangebot des Unternehmens integriert, in Ausprägung 1 nur in geringem Maße. Ausprägung zwei umfasst Unternehmen, in denen das Thema Schatten-IT weitestgehend in das Schulungsangebot integriert ist. Ausprägung 3 charakterisiert Unternehmen mit einer umfassenden Integration der Schatten-IT in das Schulungsangebot, wobei die Schulungsinhalte regelmäßig überprüft und ggf. weiterentwickelt werden (s. Tabelle 24).

Tabelle 24: Ausprägungen Gestaltungsobjekt Schulungen zum Thema Schatten-IT

RG	Ausprägung
0	Das Thema Schatten-IT ist nicht in das Schulungsangebot des Unternehmens integriert.
1	Das Thema Schatten-IT ist nur in geringem Maße in das Schulungsangebot des Unternehmens integriert.
2	Das Thema Schatten-IT ist weitestgehend in das Schulungsangebot des Unternehmens integriert.
3	Das Thema Schatten-IT ist umfassend in das Schulungsangebot des Unternehmens integriert. Die Schulungsinhalte werden dabei regelmäßig überprüft und ggf. weiterentwickelt.

Das zweite Gestaltungsobjekt *Awareness* bildet ab, inwieweit die Mitarbeitenden und Führungskräfte für die Risiken von Schatten-IT sensibilisiert sind. In der Ausprägung 0 sind entsprechend dem Reifegrad Unternehmen charakterisiert, in denen Mitarbeitende und Führungskräfte überhaupt nicht für die Risiken von Schatten-IT sensibilisiert sind. In Ausprägung 1 sind diese nur in geringem Maße sensibilisiert, in Ausprägung 2 weitestgehend. Ausprägung 3 bildet Unternehmen ab, in denen die Mitarbeitenden und Führungskräfte umfassend für die Risiken von Schatten-IT sensibilisiert sind und entsprechende Sensibilisierungskampagnen in regelmäßigen Abständen durchgeführt werden (s. Tabelle 25).

Tabelle 25: Ausprägungen Gestaltungsobjekt Awareness

RG	Ausprägung
0	Die Mitarbeitenden und Führungskräfte des Unternehmens sind nicht für die Risiken von Schatten-IT sensibilisiert.
1	Die Mitarbeitenden und Führungskräfte des Unternehmens sind nur in geringem Maße für die Risiken von Schatten-IT sensibilisiert.
2	Die Mitarbeitenden und Führungskräfte des Unternehmens sind weitestgehend für die Risiken von Schatten-IT sensibilisiert.
3	Die Mitarbeitenden und Führungskräfte des Unternehmens sind umfassend für die Risiken von Schatten-IT sensibilisiert. Entsprechende Kampagnen werden regelmäßig durchgeführt.

Kollaboration

Unter die Gestaltungsdimension *Kollaboration* fällt das Gestaltungsobjekt *Silodenken und Zusammenarbeit*, das gezielt abbildet, inwiefern die zentrale IT und die Fachabteilung im Umgang mit Schatten-IT zusammenarbeiten und dabei die Bedürfnisse der betroffenen Fachabteilung integriert werden. In Ausprägung 0 ignoriert die IT-Abteilung gemäß dem Reifegrad 0 das Thema Schatten-IT und arbeitet dementsprechend auch nicht mit den Fachabteilungen zusammen. In Ausprägung 1 werden Entscheidungen über den Umgang mit Schatten-IT von der IT-Abteilung getroffen und der Entscheidungsprozess ist nur wenig transparent. In Ausprägung 2 ist der Entscheidungsprozess hingegen transparent. Ausprägung 3 trifft zu, wenn Entscheidungen über den Umgang mit Schatten-IT von der IT-Abteilung in enger Abstimmung mit den Fachabteilungen getroffen werden und der Entscheidungsprozess dabei für alle betroffenen Parteien transparent ist (s. Tabelle 26).

Tabelle 26: Ausprägungen Gestaltungsobjekt Silodenken und Zusammenarbeit

RG	Ausprägung
0	Die IT-Abteilung ignoriert das Thema Schatten-IT und arbeitet diesbzgl. nicht mit den Fachabteilungen zusammen.
1	Die IT-Abteilung arbeitet im Umgang mit Schatten-IT in den meisten Fällen unter Ausschluss der betroffenen Fachabteilungen.
2	Die IT-Abteilung arbeitet im Umgang mit Schatten-IT mit der betroffenen Fachabteilungen zusammen.
3	Die IT-Abteilung arbeitet im Umgang mit Schatten-IT vollumfänglich mit der betroffenen Fachabteilungen zusammen und strebt eine Lösung an, die deren Bedürfnisse integriert.

Gestaltungsebene Technologie

In der Gestaltungsebene *Technologie* werden die technologischen Anforderungen für den Umgang mit Schatten-IT adressiert, wobei im Rahmen der Gestaltungsdimension *Unterstützende Technologien* die Verwendung von *Monitoring-Tools* zur Identifikation von Schatten-IT als zentral identifiziert werden konnte. Es wird demnach abgebildet, inwieweit technische Tools zur automatisierten Identifikation von Schatten-IT eingesetzt werden. In der Ausprägung 0 werden im Unternehmen keinerlei Monitoring-Tools für die Identifikation von Schatten-IT eingesetzt. Ausprägung 1 charakterisiert Unternehmen, welche für die Identifikation von Schatten-IT vereinzelt Monitoring-Tools einsetzen (bspw. in einzelnen Fachabteilungen). In Ausprägung 2 sind Unternehmen verortet, welche für die Identifikation von Schatten-IT in größerem Umfang Monitoring-Tools einsetzen (bspw. in mehreren Geschäftsbereichen), wohingegen diese in Ausprägung 3 flächendeckend, also unternehmensweit, eingesetzt werden (s. Tabelle 27).

Tabelle 27: Ausprägungen Gestaltungsobjekt Monitoring-Tools

RG	Ausprägung
0	Für die Identifikation von Schatten-IT werden keine Monitoring-Tools eingesetzt.
1	Für die Identifikation von Schatten-IT werden vereinzelt Monitoring-Tools eingesetzt.
2	Für die Identifikation von Schatten-IT werden in größerem Umfang Monitoring-Tools eingesetzt.
3	Für die Identifikation von Schatten-IT werden flächendeckend Monitoring-Tools eingesetzt.

Beschreibung der Reifegradstufen

Die nachfolgende Tabelle 28 baut auf der Kurzbeschreibung der Reifegradstufen auf und ergänzt diese durch die entsprechend ausführlichen Beschreibungen der Reifegradstufen, welche die jeweiligen Ausprägungen der Gestaltungsobjekte in aggregierter Form darstellen.

Tabelle 28: Bezeichnung und Beschreibung der Reifegradstufen

RG	Bezeichnung	Beschreibung
0	Ignorance	<p>Ihr Unternehmen ignoriert Schatten-IT als Problem. Ihr Management unterstützt Initiativen zum Umgang mit Schatten-IT nicht und es werden dementsprechend auch keine Ressourcen oder Schulungsangebote zur Verfügung gestellt. Es sind weder Richtlinien im Rahmen der IT-Strategie für den Umgang mit Schatten-IT noch ein generelles Risiko- und Potenzialbewusstsein in Ihrem Unternehmen vorhanden. Prozesse zur Identifikation und zum Umgang mit Schatten-IT sind nicht existent, zufällig identifizierte Schatten-IT wird ignoriert und Verantwortlichkeiten sind nicht definiert. Ihre IT-Abteilung ignoriert das Thema Schatten-IT generell und kommuniziert bzw. arbeitet diesbzgl. auch nicht mit den Fachabteilungen zusammen.</p>
1	Awareness	<p>Ein Problembewusstsein für Schatten-IT ist in Ihrem Unternehmen vorhanden, es gibt jedoch keine Standards für den Umgang damit. Ihr Management unterstützt Initiativen zum Umgang mit Schatten-IT nur geringfügig, Dementsprechend werden nur wenige Ressourcen und Schulungsangebote zur Verfügung gestellt. Schatten-IT wird in Ihrem Unternehmen weitestgehend als Risiko betrachtet, wobei Ihre Beschäftigten aber nur in geringem Maße für die Risiken sensibilisiert sind. Ihre IT-Abteilung setzt deshalb auch weitestgehend auf Verbote. Entscheidungen über den Umgang mit Schatten-IT werden ohne Einbezug der Fachabteilungen getroffen. Der Entscheidungsprozess ist dabei nur wenig transparent. Prozesse zur Identifikation und zum Umgang mit Schatten-IT sowie generelle Verantwortlichkeiten sind prinzipiell vorhanden, aber nicht dokumentiert. Es werden vereinzelt Monitoring-Tools zur Identifikation eingesetzt und identifizierte Schatten-IT wird in einzelnen Fällen, aber nicht systematisch nach ihrem Risiko und Nutzenpotenzial bewertet.</p>
2	Management	<p>Standards für den Umgang mit Schatten-IT sind in Ihrem Unternehmen vorhanden und unternehmensweit implementiert. Ihr Management unterstützt Initiativen zum Umgang mit Schatten-IT. Ressourcen und Schulungsangebote werden dementsprechend ausreichend zur Verfügung gestellt. In Ihrem Unternehmen ist sowohl ein Risiko- als auch ein Potenzialbewusstsein für Schatten-IT vorhanden, wobei Ihre Beschäftigten auch weitestgehend für die Risiken sensibilisiert sind. Ihre IT-Abteilung setzt im Umgang mit Schatten-IT auf Richtlinien und legt Wert auf einen transparenten Entscheidungsprozess sowie eine Zusammenarbeit mit den Fachabteilungen. Prozesse zur Identifikation und zum Umgang mit Schatten-IT sowie generelle Verantwortlichkeiten sind definiert und dokumentiert. Es werden in größerem Umfang Monitoring-Tools zur Identifikation eingesetzt und identifizierte Schatten-IT wird systematisch anhand festgelegter Kriterien nach ihrem Risiko und Nutzenpotenzial bewertet.</p>
3	Optimization	<p>Die Standards für den Umgang mit Schatten-IT in Ihrem Unternehmen werden regelmäßig überprüft und verbessert. Der Umgang mit Schatten-IT ist proaktiv. Ihr Management unterstützt Initiativen zum Umgang mit Schatten-IT aktiv, es werden dementsprechend umfassende Ressourcen und Schulungsangebote zur Verfügung gestellt. In Ihrem Unternehmen ist sowohl ein Risiko- als auch ein Potenzialbewusstsein für Schatten-IT vorhanden, wobei Ihre Beschäftigten durch regelmäßige Kampagnen auch umfassend für die Risiken sensibilisiert sind. Ihre IT-Abteilung setzt im Umgang mit Schatten-IT auf Richtlinien sowie eine aktive Kommunikation. Darüber hinaus legt sie Wert auf einen transparenten Entscheidungsprozess in enger Abstimmung mit den Fachabteilungen, wobei deren Bedürfnisse, wenn möglich, integriert werden. Prozesse zur Identifikation und zum Umgang mit Schatten-IT sowie generelle Verantwortlichkeiten sind definiert und dokumentiert. Diese werden zudem regelmäßig überprüft und optimiert. Es werden flächendeckend Monitoring-Tools zur Identifikation eingesetzt und identifizierte Schatten-IT wird aktiv sowie systematisch anhand festgelegter Kriterien nach ihrem Risiko und Nutzenpotenzial bewertet. Die Kriterien werden dabei regelmäßig überprüft und ggf. erweitert.</p>

Berechnung und Erhebung des Gesamtreifegrads

Zur Berechnung des Reifegrads wird der Vorgehensweise von Große-Schwiep et al. (2020) gefolgt. Dabei wird einer Gestaltungsdimension der minimale Reifegrad der einzelnen Gestaltungsobjekte zugeteilt. Umfasst zum Beispiel eine Gestaltungsdimension drei Gestaltungsobjekte, zwei Gestaltungsobjekte erzielen den Reifegrad 3 und der letzte Gestaltungsobjekt den Reifegrad 2, dann erhält die Dimension den Reifegrad 2. Durch die Bewertung auf Basis des Reifegrades des kleinsten Gestaltungsobjekts wird eine pessimistische Haltung eingenommen bzw. Reifegradbewertung ermöglicht. Dies ist nach Große-Schwiep et al. (2020) notwendig, um die Anforderungen der anderen Gestaltungsobjekte zu berücksichtigen und Lücken zu vermeiden. Darauf aufbauend wird der Median zur Reifegradbestimmung der Gestaltungsebene aus den Gestaltungsdimensionen bestimmt.

Die Gespräche mit den Interviewpartnern haben ergeben, dass eine Gewichtung der Gestaltungsobjekte sinnvoll erscheint. Zum Beispiel wurden die IT-Strategie und Unterstützung des Managements als weitaus wichtiger eingeschätzt als die Definition von Verantwortlichkeiten. Im Rahmen der Experteninterviews wurde deshalb eine Gewichtung der Gestaltungsobjekte vorgenommen (Anhang 9).

Aufgrund der Gewichtung der Gestaltungsobjekte wurde das Berechnungsschema daraufhin angepasst. Die Berechnung der Gestaltungsdimensionen erfolgt dabei in Anlehnung an Schumacher et al. (2016). Die restliche Berechnung bleibt unverändert, d. h. die Gestaltungsebenen werden aus dem Median der jeweiligen Gestaltungsdimensionen berechnet und auch der Gesamtreifegrad ergibt sich aus dem Median der Gestaltungsebenen. Durch die Bestimmung des Gesamtreifegrads kann der aktuelle Ist-Zustand des Unternehmens im Umgang mit Schatten-IT abgebildet werden und somit eine qualitative Einordnung erfolgen. Nachfolgend wird die entsprechende Berechnungsformel dargestellt.

$$M_D = \frac{\sum_{i=1}^n M_{DIi} \times g_{DIi}}{\sum_{i=1}^n g_{DIi}}$$

Erläuterungen:

<p><i>M</i> = Reife <i>D</i> = Dimension <i>I</i> = Gestaltungsobjekt <i>g</i> = Gewichtungsfaktor <i>n</i> = Anzahl der Gestaltungsobjekte einer Dimension</p>

Für die Beurteilung des Reifegrads bzw. zur Bestimmung des Ist-Zustands wird zu einer bestimmten Zeit ein Self-Assessment durchgeführt. Das Assessment erfolgt mithilfe einer zuvor definierten Datenerfassungs- und Untersuchungsmethode. Eine Datenerhebung kann zum Beispiel anhand einer Selbsteinschätzung mithilfe eines Fragebogens erfolgen, z. B. kann der Fragebogen auf einer Likert-Skala basieren.

Für das vorliegende Forschungsprojekt wurde für eine Bewertung des Reifegrads durch die Gestaltungsobjekte das Self-Assessment in Form eines standardisierten Fragebogens bzw. Fragekatalogs, bestehend aus einer geschlossenen Frage pro Gestaltungsobjekt, entwickelt. Dabei erfordert jede Frage eine Antwort basierend auf einer Likert-Skala. Die Antwortmöglichkeiten sollen

die Ausprägungen des Gestaltungsobjekts widerspiegeln und erstrecken sich entsprechend auf der Likert-Skala von 0 bis 3. Abbildung 33 zeigt einen Ausschnitt des Self-Assessments.

Gestaltungsobjekt	Frage	0	1	2	3
IT-Strategie	Die IT-Strategie beinhaltet umfassende Richtlinien für den Umgang mit Schatten-IT, die regelmäßig überprüft werden.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
Unterstützung durch das Management	Initiativen zum Umgang mit Schatten-IT werden aktiv auf Managementebene unterstützt.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
Potenzialbewusstsein	Im Unternehmen ist sowohl ein Risiko- als auch ein Potenzialbewusstsein für Schatten-IT vorhanden.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
	Das Nutzenpotenzial identifizierter Schatten-IT wird aktiv geprüft.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
IT-Feedback Kultur und Kommunikation	Die IT-Abteilung setzt im Umgang mit Schatten-IT auf Richtlinien.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
	Die IT-Abteilung kommuniziert aktiv mit den Fachabteilungen und holt regelmäßig Feedback ein.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
Transparenz	Entscheidungen über den Umgang mit Schatten-IT werden von der IT-Abteilung in enger Abstimmung mit den Fachabteilungen getroffen.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
	Der Entscheidungsprozess ist allen betroffenen Parteien transparent.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu
Prozesse zur Identifikation von Schatten-IT	Prozesse zur Identifikation von Schatten-IT sind in dokumentierter Form vorhanden und werden regelmäßig automatisiert durchgeführt, überprüft sowie ggf. optimiert.	Trifft überhaupt nicht zu	Trifft eher nicht zu	Trifft eher zu	Trifft völlig zu

Abbildung 33: Ausschnitt aus dem Self-Assessment (eigene Darstellung)

Ergebnisse einer Anwendung des Reifegradmodells zum Umgang mit Schatten-IT

Mit einem Praxispartner (10. – 11.05.2022) wurde das Self-Assessment durchgeführt und das Reifegradmodell demnach testweise angewendet. Während des Interviews wurden dem Interviewpartner die 14 Fragen bzw. Aussagen der jeweiligen Gestaltungsobjekte gestellt und eine entsprechende Antwort vom Interviewpartner abgegeben. Dabei führte die Durchführung des Self-Assessments zu einem Gesamtreifegrad von 2, was folgende Bewertung zur Folge hat: **Standards für den Umgang mit Schatten-IT sind in Ihrem Unternehmen vorhanden und unternehmensweit implementiert.**

Neben der Berechnung und Darstellung des Gesamtreifegrads werden die Ergebnisse aus Sicht der Ebenen und Dimensionen durch Spinnennetzdiagramme veranschaulicht. Durch die grafische Darstellung der erreichten Reifegrade, insbesondere aus Sicht der Dimensionen, wird das Verbesserungspotenzial eines Unternehmens erkennbar.

So zeigt beispielsweise das Ergebnis des Interviewpartners, dass grundsätzlich Verbesserungspotenzial hinsichtlich der Dimensionen *Strategie und Führung* sowie *Kollaboration* bestehen. In beiden Dimensionen wurde der Reifegrad 1 erreicht, wohingegen die Dimensionen Unternehmenskultur, Organisation und Prozesse, Schulung und Awareness sowie unterstützende Technologien einen Reifegrad von 2 aufweisen.

Die nachstehende Abbildung 34 zeigt die Ergebnisse des Self-Assessments auf Ebene der Gestaltungsdimensionen.

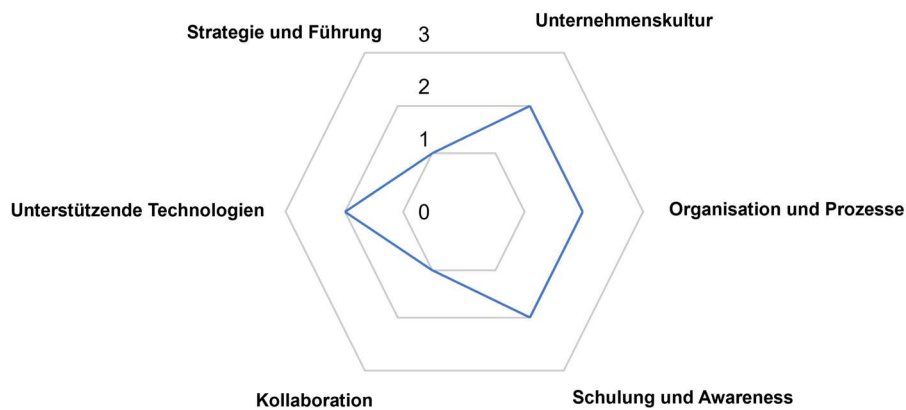


Abbildung 34: Ergebnisse des Self-Assessments aus Interview (eigene Darstellung)

3.6 Arbeitspaket 6: Dokumentation, Transfer und Projektmanagement

Innerhalb dieses Arbeitspakets wurden alle übergreifenden und nachfolgenden Maßnahmen zu Dokumentation und Dissemination sowie das erfolgreiche Projektmanagement zur Durchführung des Projekts zusammengefasst. Ein erfolgreicher Transfer der Forschungsergebnisse und die Förderung der Quervernetzung der beteiligten und interessierten KMU wurden durch verschiedene Maßnahmen gewährleistet. Zu den Maßnahmen zählen:

- Regelmäßige Treffen mit den Unternehmen des pbAs
- Veröffentlichung der Ergebnisse innerhalb eines öffentlichen und „Ready-to-use“-Webtools für die Zielgruppe
- Veröffentlichung der Ergebnisse bei wissenschaftlichen Konferenzen und in Fachzeitschriften
- Präsentation auf Fachtagungen
- Übertrag der Erkenntnisse in die Lehre und Seminare

Eine detaillierte Aufstellung der durchgeführten Maßnahmen ist Tabelle 32 und Tabelle 33 zu entnehmen.

Ebenso wurde die erfolgreiche Durchführung des Projekts durch ein entsprechendes Projektmanagement bewerkstelligt. Neben der Schaffung von digitalen Kollaborationsmöglichkeiten wurden regelmäßige Abstimmungen zwischen den Projektpartnern und dem pbA umgesetzt.

4. Notwendigkeit und Angemessenheit der geleisteten Arbeit sowie Verwendung der Zuwendung

Forschungsstelle 1: FIR e. V. an der RWTH Aachen

Für die wissenschaftliche und technische Bearbeitung des Projekts wurden insgesamt 22,67 Personenmonate für Angestellte mit abgeschlossener wissenschaftlicher Ausbildung eingesetzt.

Forschungsstelle 2: IPRI

Für den Berichtszeitraum wurden insgesamt 26,96 Personenmonate für Angestellte mit abgeschlossener wissenschaftlicher Ausbildung eingesetzt.

Tabelle 29: Personaleinsatz der Forschungseinrichtungen

Jahr	FIR	IPRI	Gesamt
2020	8,39 PM	5,20 PM	13,59 PM
2021	12,80 PM	12,83 PM	25,63 PM
2022	1,48 PM	8,93 PM	10,41 PM
Gesamt	22,67 PM	26,96 PM	49,63 PM

Die durchgeführten Arbeiten und das eingesetzte Personal entsprechen dem beantragten Arbeitsplan und waren insofern für den Projekterfolg notwendig und angemessen. Darüber hinaus wurde der erfolgreiche Projektabschluss durch bereits im Projektantrag aufgeführte Methoden herbeigeführt.

Es wurde eine umfassende Recherche zu Möglichkeiten für die Identifikation von Schatten-IT durchgeführt und ein Methodenportfolio (z. B. Interviewleitfaden) entwickelt. Dieses dient als Grundlage für die Identifikation von Schatten-IT im gesamten Unternehmen. Darüber hinaus wurde eine Literaturrecherche durchgeführt, um Chancen und Risiken von Schatten-IT zu erheben. Die gesammelten Forschungsergebnisse dienen als Grundlage, um eine Bewertung identifizierter Schattenlösungen vorzunehmen und darauf aufbauend Lösungsansätze (z. B. Registrierung, Ablösung) zu bestimmen.

Im Rahmen der vier virtuellen Sitzungen des pbAs wurden die erreichten Zwischenergebnisse präsentiert und zur Diskussion gestellt. Expertengespräche und individuelle Fallstudien mit Unternehmen des pbAs dienen dazu, wichtige Informationen über praktische Rahmenbedingungen und unternehmensspezifische Anforderungen zu erheben.

Die Ergebnisse wurden aufbereitet und gemeinsam mit Handlungsempfehlungen in einem IT-Tool verfügbar gemacht. Dieses wurde ebenfalls mit den Unternehmen des pbAs iterativ validiert und kontinuierlich optimiert, um eine langfristige Nutzung in der Praxis sicherzustellen. Das entwickelte Tool vereint alle relevanten Forschungsergebnisse, Methoden und Ansätze in einer zentralen Applikation, welche nutzerfreundlich in jedem Unternehmen, auch über die Größe von KMU hinaus, Anwendung finden kann.

5. Innovativer Beitrag und Nutzen für KMU

Im Forschungsprojekt ‚Legitimise IT‘ wurden die durch die Komplexität und Heterogenität heutiger IT-Systeme und Applikationen entstehenden Herausforderungen von Schatten-IT bei KMU und vor allem dem produzierenden Gewerbe adressiert.

Dafür wurde eine übergreifende Definition von Schatten-IT erarbeitet und somit eine zielgruppenspezifische Grundlage zur Kommunikation des Forschungsbereichs geschaffen. KMU sind somit in der Lage, auf eine Referenzbeschreibung von Schatten-IT zurückzugreifen und mittels der erarbeiteten Methodik aufwandsarm Schatten-IT im eigenen Unternehmen zu identifizieren. Der entwickelte Leitfaden ermöglicht die Bewertung von Nutzen und Risiken der identifizierten Schatten-IT speziell in ERP-System-dominierten System- und Prozesslandschaften. Für die weitere Legitimierung ausgewählter Schatten-IT wurden entsprechend verschiedene Lösungsansätze herausgearbeitet und passende Leitfäden bereitgestellt. Besonders herauszustellen ist, dass die geplante Plattformlösung im befragten Nutzerkreis als wenig nutzenstiftend eingeschätzt wurde und vielmehr eine weitere Sammlung verschiedener Lösungsansätze gewünscht wird, welche im Projektverlauf erarbeitet und nutzerfreundlich zur Verfügung gestellt werden. Ein Reifegradmodell zur Einschätzung des Umgangs mit Schatten-IT wurde auf Wunsch des pbAs erarbeitet und bietet damit die Möglichkeit, die Entwicklungsstufe von Schatten-IT ganzheitlich einordnen zu können.

Die Forschungsergebnisse aus ‚Legitimise IT‘ bieten damit einen innovativen Beitrag zur Identifikation, Bewertung und anwenderfreundlichen Legitimierung von Schatten-IT für kleine und mittlere Unternehmen sowie die produzierende Industrie.

5.1 Wissenschaftlich-technischer und wirtschaftlicher Nutzen der erzielten Ergebnisse für KMU

Im Forschungsprojekt ‚Legitimise IT‘ wurden mit den Ergebnissen mittelbare wie auch unmittelbare Nutzenpotenziale geschaffen. Unmittelbarer Nutzen wurde durch die Umsetzung der Forschungsergebnisse in ein anwenderfreundliches Web-Tool generiert, welches von interessierten Unternehmen und Verantwortlichen genutzt werden kann. Dazu zählen:

- Methodisch unterstützte Aufnahme und Dokumentation der Systeme und Identifikation von Schatten-IT in den erfassten IT-Anwendungen für verschiedene Verfahren
- Kategorisierung und Bewertung von Schatten-IT zu Ableitung von Handlungsmaßnahmen mithilfe der erarbeiteten Dimensionen und Priorisierung
- Matrix mit Übersicht über das Nutzen- und Risikoverhältnis der erfassten IT-Anwendungen
- Automatisierte Darstellung der Eignung einzelner Lösungsansätze für die identifizierten Schatten-IT Ansätze

Der mittelbare Nutzen ergibt sich für die Nutzerschaft durch die Umsetzung der Forschungsergebnisse:

- Die systematische Erfassung von Schatten-IT in die IT-Anwendungslandschaft schafft langfristig eine bessere Prozesstransparenz und erleichtert die Prozessüberwachung. Eine entsprechende Legitimierung von Schatten-IT in nutzenstiftenden Bereichen fördert die Akzeptanz bei Mitarbeitenden und steigert die Partizipation in der proaktiven Kommunikation von neuen Prozessverbesserungen auf Basis neuer IT-Anwendungen als fachbereichsübergreifende Nutzung neuer Tools.

- Die Transparenz und Legitimierung führt mittel- und langfristig zu geringeren Kosten und Ressourcenverschwendungen durch beispielsweise doppelte Datenhaltungen und Parallelprozesse. Die freigewordenen Ressourcen können somit auf die Verbesserung von Produkten und zur Erarbeitung neuer Innovationen genutzt werden. Ebenso kann sichergestellt werden, dass sowohl Fachbereichssilos aufgebrochen werden als auch Prozesswissen, welches zunächst wegen Schatten-IT nur implizit bei einzelnen Mitarbeitenden gehalten wurde, nun aber transparent verfügbar ist. Dies kann entscheidende Wettbewerbsvorteile generieren, indem nicht nur die Prozesse effektiver werden, sondern auch Kompetenzen nachhaltig im Unternehmen verankert bleiben.
- Ebenso erfolgskritisch für Unternehmen wird die Steigerung der IT/OT-Sicherheit, welche durch erfasste Schatten-IT ein wichtiges Hilfsmittel zur Risikobegrenzung darstellt. Durch eine transparente Kommunikation der Legitimierung oder Nicht-Legitimierung einzelner Schatten-IT-Anwendungen wird die kritische Awareness bzgl. der sicherheitsrelevanten Risiken erzeugt. Die Ergebnisse werden Unternehmen entscheidend unterstützen, um mögliche Verstöße bzgl. der Datenschutz-Grundverordnung (DSGVO) zu verhindern.

5.2 Industrielle Anwendungsmöglichkeiten der erzielten Ergebnisse

Die industrielle Anwendbarkeit der Forschungsergebnisse nach Projektende ist im potenziellen Nutzerkreis als hoch zu bewerten. Dieser besteht vorrangig aus kleinen und mittleren produzierenden Unternehmen. Darüber hinaus können die Ergebnisse von Unternehmen anderer Branchen genutzt werden, die sich mit dem kontrollierten Einsatz von Schatten-IT in ihrer Organisation auseinandersetzen möchten und dabei über alle Phasen der Umsetzung methodisch unterstützt werden möchten.

Die Abbildung der Forschungsergebnisse entlang eines ganzheitlichen Prozesses ermöglicht die einfache Anwendung in der unternehmerischen Praxis. Es unterstützt Verantwortliche aus IT-Abteilungen und bildet einen aufwandsarmen Werkzeugkasten für ohnehin beanspruchte IT-Organisationen ab. Die Ergebnisse wurden entlang der Arbeitsphasen der Gewichtung, Identifikation, Erfassung, Auswertung und Lösung strukturiert und stellen somit die Arbeit aus der Ableitung der Unternehmensstrategie als auch aus der Prozesserfassung in Fachbereichen auf strukturierte Art und Weise dar. Es kann somit einen idealen Begleiter in Unternehmensworkshops darstellen und Ergebnisse schnell optisch aufbereiten und für das unternehmensinterne Berichtswesen bereitstellen.

Das Forschungsprojekt fügt sich thematisch nahtlos in die Forschungsschwerpunkte am FIR und am IPRI ein. Die erzielten Ergebnisse können damit interessierten Unternehmen in unterschiedlichen zielgruppenorientierten Formen zugänglich gemacht und weiterentwickelt werden.

Ebenso relevant ist das umgesetzte Transferkonzept, welches Unternehmen nicht nur sensibilisiert für die Thematik, sondern auch eine einfache Nutzung der Ergebnisse durch Veröffentlichungen ermöglicht.

6. Veröffentlichungen und Transfermaßnahmen

6.1 Projektbegleitender Ausschuss im Projekt

Durch die aktive Einbindung des pbAs wurde einerseits die Praxisrelevanz und andererseits die Verbreitung der Ergebnisse sichergestellt. Während der Projektlaufzeit wurden die Ergebnisse auf den Sitzungen des pbAs präsentiert und durch Fachvorträge sowie Veröffentlichungen weiteren Firmen zugänglich gemacht. Die Mitglieder des pbAs sind die in Tabelle 30 aufgeführten Unternehmen.

Tabelle 30: Mitglieder des projektbegleitenden Ausschusses

Unternehmen	KMU	Ansprechpartner
BOS GmbH & Co. KG		Dr. Jörg Hoffmann
Heinen Automation GmbH & Co. KG	X	Kurt Heinen
ID Ingenieure & Dienstleistungen GmbH	X	Patrick Prinz
Kiepe Electric GmbH		Jürgen Kroppen
Kögel Schornsteine GmbH & Co. KG	X	Sebastian Zuleger
KTR Systems GmbH & Co. KG		Olaf Korbanek
NETRONIC Software GmbH	X	Markus Hammers
Novartis Pharma Stein AG		Franck Palacios Mora
Phlowsec	X	Florian Franke
Trützscher AG		Martin Drude

Der pbA trat vier Mal zu gemeinsamen Sitzungen zusammen, in denen die bisherigen Ergebnisse diskutiert und das weitere Vorgehen abgestimmt wurde. Für jede dieser Sitzungen wurden inhaltliche Schwerpunkte festgelegt (s. Tabelle 31).

Tabelle 31: Sitzungen des PAs und inhaltliche Schwerpunkte der jeweiligen Sitzung

Datum	Ort	Schwerpunkt
01.07.2020	Remote	Kick-off, Erwartung, Diskussion und Expertengespräch mit Fokus auf AP 1 und AP 2
28.04.2021	Remote	Vorstellung der bisherigen Projektergebnisse und Anforderungsaufnahme für AP 3
09.12.2021	Remote	Vorstellung der bisherigen Projektergebnisse mit Fokus auf AP 4
31.05.2022	Remote	Abschlussveranstaltung und Präsentation der Gesamtprojektergebnisse und Live-Demo des neuen Webtools

Zwischen den Sitzungen des pbAs fanden Arbeitstreffen bei den Unternehmen vor Ort sowie in weiteren interessierten Unternehmen und in den Forschungsstellen statt, zudem wurden Telefoninterviews durchgeführt. In diesen wurden einzelne Fragestellungen vertiefend diskutiert und unter Einsatz von verschiedenen Moderationstechniken bearbeitet.

6.2 Plan zum Ergebnistransfer

Erste Schritte zum Ergebnistransfer sind während der Projektlaufzeit durchgeführt worden. Weitere Maßnahmen zur Verwertung und Verbreitung der Projektergebnisse sind im Anschluss an das Projekt vorgesehen. Über den Austausch zwischen den Forschungsstellen und den Unternehmen des pbAs sowie weiteren interessierten Unternehmen hat bereits ein erster Wissenstransfer stattgefunden. Dieser ist die Basis für die praktische Umsetzbarkeit der Ergebnisse. Die während des Berichtszeitraums durchgeführten Maßnahmen zum Ergebnistransfer in die Wirtschaft sind in Tabelle 32 zu entnehmen. Die nach dem Berichtszeitraum geplanten Maßnahmen für den Ergebnistransfer sind in Tabelle 33 aufgeführt.

Besonders hervorzuheben ist das entwickelte Schatten-IT-Webtool, das unter folgendem Link frei zugänglich ist: <https://legitimise-it-tool.fir.de/>. Konkret unterstützt das Webtool Anwendende bei der Identifikation von Schatten-IT und stellt ein Self-Assessment zur Risiko- und Nutzwertanalyse identifizierter Anwendungen bereit. Auf Basis der Analyse werden Lösungsansätze bereitgestellt. Das Webtool richtet sich an Entscheidende aus der zentralen IT und transferiert die Projektergebnisse unmittelbar zur Anwendung in die Unternehmenspraxis.

Tabelle 32: Transfermaßnahmen während der Projektlaufzeit

Maßnahmen	Ziel	Ort/Rahmen	Datum/Zeitraum/Link
Best-Practices-Vlog (Video-Blog)	Darstellung einzelner Umsetzungsbeispiele dafür, wie in Unternehmen Schatten-IT genutzt wird. Diese werden in einem Vlog veröffentlicht.	Zur Präsentation von Praxisbeispielen und Umsetzungsbeispielen aus dem Projekt.	Konsolidierung der Ergebnisse in einem webbasierten Tool, das online frei verfügbar ist: https://legitimise-it-tool.fir.de/
Presse-/ Öffentlichkeitsarbeit	Bekanntmachung des Projekts und der Ergebnisse	<ul style="list-style-type: none"> ▪ 3 Pressemitteilungen über den IDW – Informationsdienst Wissenschaft ▪ IPRI- und FIR-Homepage ▪ IPRI-Journal (Sommer 2020, Sommer 2021) ▪ IPRI-Jahresbericht ▪ FIR-Jahrbuch 	<ul style="list-style-type: none"> ▪ Pressemitteilung (23.06.2020): https://idw-online.de/de/news749861 ▪ Pressemitteilung (04.03.2022): https://idw-online.de/de/news789517 ▪ Pressemitteilung (05.07.2022): https://idw-online.de/de/news797836 ▪ IPRI-Homepage: https://ipri-institute.com/forschungsprojekte/legitimise-it/ ▪ FIR-Homepage: https://www.fir.rwth-aachen.de/forschung/forschungsprojekte/detail/legitimise-it-21191-n/ ▪ IPRI Journal 2020: https://ipri-institute.com/wp-content/uploads/2020/08/IPRI_Journal_Sommer_2020.pdf ▪ IPRI Journal 2021: https://ipri-institute.com/wp-content/uploads/2021/08/IPRI-Journal_Sommer_2021.pdf ▪ IPRI-Jahresbericht 2020 und 2021: https://ipri-institute.com/wp-content/uploads/2022/07/IPRI-Jahresbericht-2021.pdf ▪ FIR-Jahrbuch 2020 und 2021: https://www.fir.rwth-aachen.de/sites/default/dateie

			n/flipping-books/fir-jahrbuch-2020/26/ https://www.fir.rwth-aachen.de/sites/default/dateien/flipping-books/fir-jahrbuch-2021/index.html
Vorstellung der Projektergebnisse auf Konferenzen und in Fachzeitschriften	Bekanntmachung des Projekts und der Ergebnisse	<ul style="list-style-type: none"> ▪ mindestens ein wissenschaftlicher Vortrag, z. B. EuroCACS/CSX Conference oder Hannover Messe ▪ Veröffentlichung in Fachzeitschriften, z. B. IT & Production, Controller-Magazin 	<ul style="list-style-type: none"> ▪ Vortrag auf Legacy IT Konferenz (27.09.2021): „Legacy IT im Schatten - Legitimieren statt abschalten? Erkenntnisse aus Forschung und Praxis“ ▪ Veröffentlichung in IT & Production (07.02.2022): „Inoffizielle Systeme legitimiert: Risiken und Chancen in der Schatten-IT“ https://www.it-production.com/produktionsmanagement/inoffizielle-systeme-legitimiert/ ▪ Veröffentlichung in IT-Mittelstand (eingereicht am 12.08.2022): „Schatten-IT: Fluch oder Segen für KMU“
Vorstellung des Projekts in diversen Arbeitskreisen und Fachtagungen	Bekanntmachung des Projekts und der Ergebnisse	<ul style="list-style-type: none"> ▪ Schmalenbach Arbeitskreis „Integrationsmanagement für neue Produkte“ Sitzungen ▪ Arbeitskreis 4.0 des IPRI ▪ <i>Roundtable Information Manager</i> des FIR 	<ul style="list-style-type: none"> ▪ Digital Demo Day (09.09.2021) ▪ <i>Roundtable Information Manager</i> FIR (11/2021)
Veröffentlichung der Projektergebnisse mit Fokus auf die Praxis	Bekanntmachung der Ergebnisse in der Praxis, Aufzeigen von Anwendungsfällen	<ul style="list-style-type: none"> ▪ VDMA-Nachrichten ▪ Wissenschaft trifft Praxis ▪ Unternehmen der Zukunft 	<ul style="list-style-type: none"> ▪ FIR-Fachzeitschrift UdZforschung (11/2020): https://www.fir.rwth-aachen.de/sites/default/dateien/flipping-books/udzforschung_2-2020/4/index.html ▪ Verbreitung des webbasierten Tools in diversen praxisorientierten Medien: IT-Welt: https://itwelt.at/news/legitimise-it-webtool-gegen-schatten-it/ Com-Magazin: https://m.com-magazin.de/artikel/webtool-schatten-it-2780493.html It-Daily: https://www.it-daily.net/shortnews/neues-webtool-fuer-schatten-it
Treffen des Projektbegleitenden Ausschusses	<ul style="list-style-type: none"> ▪ Validierung der Ergebnisse mit den Praxispartnern ▪ Übertragbarkeit der Ergebnisse auf praxisrelevante Problemstellungen 	<ul style="list-style-type: none"> ▪ IPRI/FIR ▪ Mitglieder des projektbegleitenden Ausschusses 	<ul style="list-style-type: none"> ▪ Treffen des Projektbegleitenden Ausschusses: 01.07.2020 (online) 28.04.2021 (online) 09.12.2021 (online) 31.05.2022 (online)

Präsenz im Internet	Bekanntmachen der Ergebnisse und Termine	<ul style="list-style-type: none"> ▪ Projekt-Webseite ▪ IPRI- und FIR-Webseite ▪ Forschungsblog: Neues aus der Forschung: https://neues-aus-der-forschung.de/ 	<ul style="list-style-type: none"> ▪ LinkedIn Beiträge über IPRI Account: 16.03.2021: https://www.linkedin.com/feed/update/urn:li:activity:6795272161193013248 04.05.2021: https://www.linkedin.com/feed/update/urn:li:activity:6795272161193013248 07.10.2021: https://www.linkedin.com/feed/update/urn:li:activity:6851825402126700546 05.11.2021: https://www.linkedin.com/feed/update/urn:li:activity:6862305983767695361 07.12.2021: https://www.linkedin.com/feed/update/urn:li:activity:6873932182113665024 01.03.2022: https://www.linkedin.com/feed/update/urn:li:activity:6904371599567634432 21.06.2022: https://www.linkedin.com/feed/update/urn:li:activity:6944918987981918210 • Beitrag in „Neues aus der Forschung“ (28.10.2021): https://neues-aus-der-forschung.de/2021/10/28/schatten-it-in-kleinen-und-mittleren-unternehmen-risiken-kontrollieren-und-chancen-nutzen/
Weitergabe der Inhalte an künftige Fach- und Führungskräfte	Bekanntmachung der Ergebnisse in der Praxis, Aufzeigen von Anwendungsfällen	<ul style="list-style-type: none"> ▪ RWTH Aachen 	<ul style="list-style-type: none"> • Schatten-IT-Workshop April 2022 https://idw-online.de/de/news789517

Tabelle 33: Transfermaßnahmen nach Projektende

Maßnahmen	Ziel	Ort/Rahmen	Datum/Zeitraum
Seminar in der IPRI-Seminarreihe/ FIR-Zertifikatskurse	<ul style="list-style-type: none"> ▪ Sensibilisierung und Schulung von Mitarbeitenden aus KMU 	<ul style="list-style-type: none"> ▪ IPRI Stuttgart ▪ FIR Aachen 	<p>Online-Sensibilisierungsworkshops für Mitte 2023 geplant</p> <p>https://www.linkedin.com/feed/update/urn:li:activity:6996753355033210880</p>
Veröffentlichung in Fachzeitschriften	<ul style="list-style-type: none"> ▪ Bekanntmachung der Projektergebnisse 	<ul style="list-style-type: none"> ▪ Veröffentlichungen in Fachzeitschriften z. B. IT & Production, HMD – Praxis der Wirtschaftsinformatik 	<p>Veröffentlichung in IT-Mittelstand (eingereicht am 12.08.2022): „Schatten-IT: Fluch oder Segen für KMU“</p>
Webinar/ Webcast	<ul style="list-style-type: none"> ▪ Diskussion von Zwischenergebnissen mit KMU ▪ Vorstellung und Demonstration des 	<ul style="list-style-type: none"> ▪ Internet 	<p>Schatten-IT Workshop April 2022</p>

	abgeschlossenen Web-Tool		https://idw-online.de/de/news789517 Vorstellung im CIO-Arbeitskreis am 30.11.2022
Angebot von Beratungsprojekten	<ul style="list-style-type: none"> Unterstützung von KMU bei individuellen Problemstellungen 	<ul style="list-style-type: none"> Vor Ort bei den KMU 	Die beiden Institute prüfen die Potenziale für gemeinsame Beratungsprojekte in 2023.
Integration in die Lehre	<ul style="list-style-type: none"> Weitergabe der Inhalte an künftige Fach- und Führungskräfte 	<ul style="list-style-type: none"> RWTH Aachen 	Integration der Inhalte in Zertifikatskurs „Digital Transformation Expert“ – Modul: „Cloud-Transformation – das digital Vernetzte Unternehmen“ 2022
Integration in FIR-Lehrbücher (insb. Informationsmanagement)	<ul style="list-style-type: none"> Vorstellung des Legitimierungsansatzes in thematisch passendem Buch für Führungskräfte 	<ul style="list-style-type: none"> 2. Auflage des Buches voraussichtlich 2021 	Ausstehend

6.3 Einschätzung zur Realisierbarkeit des vorgeschlagenen und aktualisierten Transferkonzepts

Die äußeren Rahmenbedingungen, die aufgrund der Covid-19-Pandemie zum Projektstart eingetreten sind, hatten auf die Durchführung des Forschungsprojekts positive und negative Effekte. Durch die Verlagerung der Projekttreffen in eine digitale Form konnte der pbA mit erheblichem geringerem Aufwand und Kosten an den Treffen teilnehmen. Dadurch konnte die Anzahl der Teilnehmenden an den Treffen erhöht werden. Allerdings waren dadurch keine physischen Treffen möglich und der persönliche Austausch von Best Practices wurde erschwert. Aus unserer Sicht ist das Durchführen von Projekttreffen in digitaler Form eine gute Alternative für deutschlandweite und diverse Themen, die sonst einen hohen Aufwand der Teilnahme erfordern.

Das vorgeschlagene Transferkonzept und die Finanzierbarkeit nach Abschluss des Projekts wird als realistisch eingeschätzt. Eine optimale Umsetzung der Ergebnisse wird in Zusammenarbeit der durchführenden Forschungseinrichtungen realisiert. Die zeitnahe Umsetzung wird durch folgende Maßnahmen unterstützt:

- Zur Unterstützung der industriellen Umsetzung bei KMU werden die Projektergebnisse in Form eines frei zugänglichen Webtools angeboten und durch ein Video erklärt. Das Webtool wird auf Veranstaltungen der Forschungseinrichtungen präsentiert, deren thematische Abgrenzung in den Umfang des Forschungsprojekts fällt. Die Nutzung und erfolgreiche Verbreitung innerhalb der Branche wird sich in Zukunft zeigen und kann nur in begrenztem Rahmen beeinflusst werden.
- Für die Anwendung des Webtools sind von/in? den Unternehmen keine besonderen technischen Voraussetzungen notwendig. Aufgrund der browserbasierten Umsetzung des Webtools kann dieses ohne zusätzlichen Softwarebedarf eingesetzt werden. Die integrierten Informationstexte zur Bedienung sowie das Dokument zur Logik, welches im Webtool als Download zur Verfügung steht, erhöht die Anwendbarkeit sowie Akzeptanz auf Anwenderseite und wurde durch den pbA besonders positiv bewertet.

- Die Ergebnisse des Forschungsprojekts sind für alle Unternehmen über die Projekthomepage zugänglich.
- Die Integration der Projektergebnisse in die aktuellen Lehrinhalte sind ohne große Aufwände möglich und werden ab dem Sommersemester 2023 analysiert und forciert.
- Im Transferkonzept werden Maßnahmen ergriffen, um Ergebnisse während und nach der Projektlaufzeit zu verbreiten und dem potenziellen Nutzerkreis zur Verfügung zu stellen. Durch die Transfermaßnahmen wird eine Vielzahl an Unternehmen erreicht.

7. Forschungsstellen

7.1 Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen

Der Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen ist seit 60 Jahren eine der führenden deutschen Forschungseinrichtungen in den Bereichen Betriebsorganisation und Unternehmensentwicklung. In den Themenbereichen Produktionsmanagement, Dienstleistungsmanagement, Business Transformation und Informationsmanagement werden am FIR in Kooperation mit Partnern aus Wissenschaft und Wirtschaft die Unternehmen der Zukunft gestaltet.

Das FIR ist maßgeblich im Bereich der industrienahen Forschung tätig und entwickelt einzigartige Ansätze, Methoden und Werkzeuge, die in Zusammenarbeit mit den jeweiligen Partnerunternehmen erprobt und umgesetzt werden. Mit dem Bereich Dienstleistungsmanagement und seinen Fachgruppen Service-Engineering, Lean Services und Community-Management konzentriert sich das FIR auf unternehmensbezogene und technologiebasierte Dienstleistungen. Dabei gilt es, Lösungsansätze für die derzeitigen und zukünftigen Herausforderungen bzw. Probleme eines der bedeutendsten Industriesektoren zu entwickeln. Die Themen reichen von der systematischen Entwicklung von Produkt-Service-Systemen mit stark technologischer Prägung im Kontext der Industrie 4.0 bis hin zur Professionalisierung der Dienstleistungserbringung. Ferner stellen die effiziente Integration von Mensch, Technik und Organisation sowie die Gestaltung von cyberphysischen Systemen und Systemen für die Dienstleistungsproduktion Betrachtungsfelder dar.

Die Kompetenzen und Vorarbeiten des FIR im Bereich Business Transformation sind v. a. die Steigerung der Innovations- und Veränderungsfähigkeit von Unternehmen. Die Expertise in puncto Initiierung, Gestaltung und Steuerung von Transformationsprozessen und dazugehörigen Methoden stützt sich auf mehr als 50 Drittmittel-Projekte und über 60 Industrieberatungsmandate pro Jahr. Die Transferleistung von der Wissenschaft in die Praxis in Unternehmen konnte das FIR in der Vergangenheit in zahlreichen Forschungsprojekten realisieren.

Tabelle 34: FIR e. V. an der RWTH Aachen

Forschungsstelle 1	Forschungsinstitut für Rationalisierung (FIR) e. V. an der RWTH Aachen
Anschrift	Campus-Boulevard 55, 52074 Aachen
Leiter der Forschungsstelle	Prof. Dr.-Ing. Dipl.-Wirt.-Ing. Günther Schuh
Projektleitung	Max-Ferdinand Stroh
Kontakt	Tel.: +49 241 47705-510, www.fir.rwth-aachen.de

7.2 International Performance Research Institute (IPRI) gGmbH

Die IPRI – International Performance Research Institute gemeinnützige GmbH wurde mit der Zielsetzung gegründet, Forschung auf dem Gebiet des Performance Managements von Organisationen, Unternehmen und Unternehmensnetzwerken zu betreiben.

Unter der Leitung von Prof. Dr. Mischa Seiter untersucht das IPRI in Zusammenarbeit mit anderen Forschungseinrichtungen und kleinen und mittleren Unternehmen die Wirkungszusammenhänge und Potenziale in den Bereichen Controlling, Finanzen, Logistik und Produktion.

Forschungsschwerpunkt ist die Erarbeitung neuer Methoden im Bereich des Controllings und der Transfer dieser Ergebnisse in die Praxis. Die Forschungsstelle arbeitet eng mit der Bundesvereinigung Logistik e. V., dem VDMA und Unterverbänden (Forschungsvereinigung Antriebstechnik e. V., Forschungsvereinigung Werkzeugmaschinen und Fertigungstechnik e. V.) sowie der IHK zusammen. Zudem wird der Kontakt zu Experten aus der Praxis über regelmäßige Veranstaltungen und Workshops hergestellt.

Tabelle 35: IPRI gemeinnützige GmbH

Forschungsstelle 2	IPRI International Performance Research Institute gGmbH
Anschrift	Reuchlinstraße 27, 70176 Stuttgart
Leiter der Forschungsstelle	Prof. Dr. Mischa Seiter
Projektleitung	Laura Vetter, M.A.
Kontakt	Tel.: +49 711/ 6203268-8029, www.ipri-institute.com

Anhang

Anhang 1 Leitfaden für standardisierte Interviews mit den Fachbereichen zur Identifikation von Schatten-IT

Einführung	Themenblock 1	Themenblock 2
<p>Themenblock 1 – Kernfragen zur Identifikation und Beschreibung</p> <p><i>Abfrage der Interviewpartner zur Identifikation und Beschreibung von Schatten-IT entlang der Prozessschritte im Fachbereich</i></p> <p>1. Welche IT-Lösungen nutzt Ihre Abteilung für die Prozessschritte 1, 2, 3... neben der im Prozessmodell der IT-Infrastruktur aufgeführten?</p> <p><i>Falls Schatten-IT identifiziert werden konnte, geht das Interview für jede IT-Lösung wie folgt weiter:</i></p> <p>2. Beschreibung der IT-Lösung hinsichtlich:</p> <ul style="list-style-type: none">a. Was ist die Art, Funktion und Zweck dieser Lösung?b. Wer ist für die Pflege und Wartung verantwortlich?c. Welche Komponenten und Technologien beinhaltet die Lösung (Software, Infrastruktur...)?d. Welche Datenschnittstellen sind vorhanden?e. Ist die Lösung eigenentwickelt oder von Drittanbietern bezogen?		

Einführung	Themenblock 1	Themenblock 2
<p>Themenblock 2 – Fragen zur Relevanz, Qualität, Risiken und Nutzen der IT-Lösung</p> <p><i>Abfrage der Interviewpartner zur Relevanz der IT-Lösung für bspw. die Entscheidungsfindung oder spezifische Geschäftsprozesse sowie deren Qualität, Risiken und Nutzen</i></p> <ol style="list-style-type: none"> 1. Wie viele Nutzer verwenden die Lösung? 2. Wie viele Geschäftsprozesse werden durch die Lösung unterstützt? 3. Beschreibung der IT-Lösung hinsichtlich ihrer Relevanz: <ol style="list-style-type: none"> a. Hat die Lösung einen Einfluss auf die Unternehmensziele? b. Sind die Informationen und Ergebnisse der Lösung relevant für die strategische oder operative Entscheidungsfindung? c. Wie geschäftskritisch sind die Prozesse, die durch die Lösung unterstützt werden? d. Wie kritisch ist die Lösung für die Durchführung der Prozesse? 4. Beschreibung der IT-Lösung hinsichtlich ihrer Qualität: <ol style="list-style-type: none"> a. Wie schätzen Sie die Systemqualität ein? (Qualität der technischen Umsetzung, Zuverlässigkeit, Modifizierbarkeit) b. Wie schätzen Sie die Informationsqualität ein? c. Bitte beschreiben Sie die Prozessabwicklung mit der Lösung. Gibt es viele Dinge, die manuell erledigt werden müssen? Gibt es Medienbrüche? d. Welche Wartungsprozesse gibt es in der Abteilung für die Lösung? Gibt es eine Dokumentation, Versionierung und Zugriffskontrolle? Wie wird die Lösung entwickelt/getestet? 5. Beschreibung der IT-Lösung hinsichtlich ihrer Risiken: <ol style="list-style-type: none"> a. Wie kritisch ist die Lösung unter dem Gesichtspunkt Compliance? b. Wie kritisch ist die Lösung unter dem Gesichtspunkt der IT-Sicherheit? c. Wie hoch sind die initialen und laufenden Kosten der Lösung? 6. Beschreibung der IT-Lösung hinsichtlich ihres Nutzens: <ol style="list-style-type: none"> a. Inwieweit löst die Lösung ein Defizit unseres zentralen IT-Systems? b. Wie schätzen Sie den Innovationsgrad der Lösung ein? c. Inwieweit vereinfacht die Lösung Arbeitsprozesse in der Abteilung? d. Inwieweit verbessert die Lösung die Flexibilität und Produktivität der Abteilung? 		

Anhang 2 Vorlage zur Dokumentation identifizierter Schatten-IT

Nr.	Beschreibung/ Kennung der Schatten-IT	Kategorisierung					Weitere In- formationen (z. B. Fach- bereich, Nutzerkreis)
		Hardware (mobiler Ein- satz, z. B. Smartphones)	Server (im Eigenbe- trieb und Drittanbieter, inkl. PaaS, IaaS)	Software as a Service (von Dritt- anbietern, z. B. Share- Point, Google Mail)	Software (installierte Fremd-Soft- ware, z. B. Skype, oder selbstentwi- ckelt, z. B. BI-Lösung)	Skripte (für intern un- terstützte Soft- ware, z. B. Excel-Macros, Batch-Files)	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							

Anhang 3 Interviewleitfaden zu Risiken und Nutzen von Schatten-IT und mögliche Bewertungsmethoden

Grundlegendes	Themenblock 1	Themenblock 2	Themenblock 3	Themenblock 4
Qualitative Befragung der Experten				
<p>Themenblock 1 – Einführung</p> <p>Kurze Vorstellung des Experten hinsichtlich</p> <ul style="list-style-type: none"> • Position im Unternehmen: • Jahre der Zugehörigkeit zum Unternehmen: <p>Kurze Vorstellung des Unternehmens hinsichtlich</p> <ul style="list-style-type: none"> • Name und Gründungsjahr: • Familienunternehmen: Ja/Nein • Branche: • Tätigkeit/Geschäftsmodell: • Produkte/Dienstleistungen: • Standort: • Mitarbeitendenzahl: • Umsatz: 				

Grundlegendes	Themenblock 1	Themenblock 2	Themenblock 3	Themenblock 4
<p>Themenblock 1 – Bisherige Erfahrungen mit Risiken und Nutzen von Schatten-IT</p> <p><i>Abfrage der Interviewpartner zu genereller Risiko- und Nutzenwahrnehmung sowie Erfahrungen mit besonders kritischen oder nützlichen Schatten-IT-Anwendungen</i></p> <ol style="list-style-type: none"> 1. Wie aktuell/brisant ist Ihrer Meinung nach das Thema Schatten-IT für Unternehmen? 2. Wie schätzen Sie generell das Nutzenpotenzial von Schatten-IT für Unternehmen ein? 3. Wie schätzen Sie generell das Risiko von Schatten-IT für Unternehmen ein? 4. Haben Sie bislang im beruflichen Umfeld bereits Erfahrungen mit besonders riskanten/nützlichen Schatten-IT-Anwendungen gemacht? <ol style="list-style-type: none"> 5.1 Wenn ja, um was für Schatten-IT-Anwendungen hat es sich gehandelt? 5.2 Was waren die Folgen für das Unternehmen? 5.3 Wie sah die Lösung im Unternehmen aus? 				

Grundlegendes	Themenblock 1	Themenblock 2	Themenblock 3	Themenblock 4
---------------	---------------	---------------	---------------	---------------

Themenblock 2 – Nutzen von Schatten-IT

Abfrage der konkreten Nutzenaspekte von Schatten-IT

- 1. Worin sehen Sie konkrete Vorteile/Chancen von Schatten-IT im Unternehmen?**
- 2. Wie hoch schätzen Sie das Potenzial von Schatten-IT zur Verbesserung abteilungsinterner Prozesse ein?**
 - 2.1 Inwieweit kann Schatten-IT Arbeitsprozesse vereinfachen und effizienter machen?
 - 2.2. Inwieweit kann Schatten-IT schneller verfügbar sein als genehmigte IT-Anwendungen?
 - 2.3. Inwieweit kann Schatten-IT eine innovative Lösung darstellen?
- 3. Wie hoch schätzen Sie das Potenzial von Schatten-IT zur Verbesserung der IT-Landschaft im Unternehmen ein?**
 - 3.1 Inwieweit kann Schatten-IT spezifische Anforderungen erfüllen, die genehmigte IT-Anwendungen nicht erfüllen?
 - 3.2 Inwieweit kann Schatten-IT ein Defizit des zentralen, genehmigten IT-Systems lösen?
 - 3.3 Inwieweit kann Schatten-IT kostengünstiger als genehmigte IT-Anwendungen sein?
- 4. Wie hoch schätzen Sie das Potenzial von Schatten-IT zur Verbesserung der personalen Arbeitsumgebung ein?**
 - 4.1 Inwieweit kann Schatten-IT die Zusammenarbeit im Team verbessern?
 - 4.2 Inwieweit kann Schatten-IT zur Motivation und Arbeitszufriedenheit des Teams beitragen?
 - 4.3 Inwieweit kann Schatten-IT die Flexibilität der Fachabteilung erhöhen?
 - 4.4 Inwieweit kann Schatten-IT die Produktivität der Fachabteilung erhöhen?
- 5. Wie hoch schätzen Sie das Potenzial von Schatten-IT zur Verbesserung der individuellen Kompetenzen der Mitarbeitenden ein?**
 - 5.1 Inwieweit kann Schatten-IT die Kreativität der Mitarbeitenden fördern?
 - 5.2 Inwieweit kann Schatten-IT die Innovationfähigkeit der Mitarbeitenden stärken?
 - 5.3 Inwieweit kann Schatten-IT die IT-Kompetenzen der Mitarbeitenden verbessern?
 - 5.4 Inwieweit kann Schatten-IT die Motivation der Mitarbeitenden erhöhen?
- 6. Gibt es Ihrer Meinung nach weitere Chancen/Vorteile von Schatten-IT für Unternehmen?**

Grundlegendes	Themenblock 1	Themenblock 2	Themenblock 3	Themenblock 4
---------------	---------------	---------------	------------------	------------------

Themenblock 3 – Risiken von Schatten-IT

Abfrage der konkreten Risiken von Schatten-IT

- 1. Worin sehen Sie konkrete Risiken/Nachteile von Schatten-IT im Unternehmen?**
- 2. Wie hoch schätzen Sie das Risiko von Schatten-IT für die Unternehmensinfrastruktur ein?**
 - 2.1. Inwieweit kann Schatten-IT die Compliance im Unternehmen gefährden? (Bspw. durch Verstöße gegen das DSGVO)
 - 2.2. Inwieweit kann Schatten-IT die Komplexität der Schnittstellen erhöhen? (Bspw. durch unterbrochene Prozesse)
 - 2.3. Inwieweit kann Schatten-IT ein redundantes System darstellen? (Die Schatten-IT besteht neben einem bestehenden System mit gleicher Aufgabe.)
- 3. Wie hoch schätzen Sie das Risiko von Schatten-IT für die IT-Landschaft im Unternehmen ein?**
 - 3.1 Inwieweit kann Schatten-IT die Datensicherheit gefährden? (Bspw. durch Sicherheitslücken und die Gefahr von Cyberangriffen)
 - 3.2 Inwieweit kann Schatten-IT die Datenvalidität und -konsistenz gefährden?
 - 3.3 Inwieweit kann Schatten-IT zu einer Heterogenität und Fragmentierung der IT-Landschaft beitragen? Inwieweit ist die IT in Folge weniger kontrollierbar?
 - 3.3 Inwieweit können Risiken durch einen fehlenden Support der Schatten-IT entstehen?
 - 3.4 Inwieweit kann Schatten-IT zu hohen laufenden Kosten und einem hohen Integrationsaufwand führen?
- 4. Wie hoch schätzen Sie das Risiko von Schatten-IT für die individuelle Arbeitseinstellung ein?**
 - 4.1 Inwieweit kann Schatten-IT das Silo-Denken der Fachabteilungen verstärken?
 - 4.2 Inwieweit kann Schatten-IT die Mitarbeitenden von ihren Kernaufgaben fernhalten?
 - 4.3 Inwieweit kann Schatten-IT zu leichtfertigen Handlungen der Mitarbeitenden führen?
- 5. Gibt es Ihrer Meinung nach weitere Risiken/Nachteile von Schatten-IT für Unternehmen?**

Grundlegendes	Themenblock 1	Themenblock 2	Themenblock 3	Themenblock 4
<p>Themenblock 4 – Ansätze zur Identifikation und Bewertung von Risiken sowie Nutzen von Schatten-IT</p> <p><i>Abfrage der Interviewpartner zu im Unternehmen genutzten Ansätzen zur Identifikation, Analyse und Bewertung von Risiken sowie Nutzenaspekten von (Schatten-)IT-Anwendungen</i></p> <ol style="list-style-type: none"> 1. Existieren in Ihrem Unternehmen generell Ansätze/Methoden zur Identifikation von Risiken von IT-Anwendungen? <ul style="list-style-type: none"> • Methoden zur Identifikation relevanter Assets (Prozesse, IT-Systeme, Personen, Daten) • Methoden zur Identifikation von Bedrohungen und Verwundbarkeiten (bspw. Schwachstellenanalyse) • Weitere Methoden: Brainstorming, Interviews, Szenariotechnik, Checklisten 2. Existieren in Ihrem Unternehmen generell Ansätze/Methoden zur Analyse sowie Bewertung von Risiken von IT-Anwendungen (quantitativ und qualitativ)? <ul style="list-style-type: none"> • Methoden zur Analyse: Bspw. Fehlerbaumanalyse, Angriffsbaumanalyse, Fehlermöglichkeits- und Einflussanalyse (FMEA) • Methoden zur Bewertung: Bspw. Risikomatrix, Portfolioanalyse, Business-Impact-Analyse, CIA-Analyse, Value-at-Risk 3. Existieren in Ihrem Unternehmen Ansätze/Methoden zur Bewertung von Risiken bzw. Nutzenaspekten speziell für Schatten-IT-Anwendungen? 4. Wie schätzen Sie die Praktikabilität quantitativer und qualitativer Bewertungsmethoden speziell für Schatten-IT-Anwendungen für die Unternehmenspraxis ein? 				

Anhang 4 Ergebnisse zur Marktrecherche zu Low-Code-/No-Code-Plattformen

● = vorhanden ○ = nicht vorhanden											
Funktionen	appian	Bubble	Caspio	eLegere	LANSa	mendix	Ninox	OutSystems	PEGA	quixy	Studio Creatio
Agile Methodiken	○	○	○	●	○	○	○	○	○	○	○
Aktivitäts-Dashboard	○	○	○	●	○	○	○	●	○	●	●
Alarmfunktion / Benachrichtigungen	●	○	●	●	○	○	○	●	○	○	●
Anforderungsmanagement	○	○	○	○	○	●	○	●	○	●	●
Anpassbare Berichte, Felder, Formulare, Vorlagen	○	○	●	●	○	○	○	○	○	●	○
Anpassbare Felder, Formulare	○	○	○	○	○	○	○	○	○	○	●
Anpassbare Felder, Formulare, Vorlagen	○	○	○	○	○	○	●	●	○	○	○
Anpassbare Vorlagen	●	○	○	○	○	○	○	○	○	○	○
Anwendungsmanagement	○	○	○	○	○	○	○	○	○	○	●
API	●	○	●	●	●	●	●	●	○	●	●
Audit-Trail	○	○	●	○	○	○	○	●	○	●	●
Aufgabenmanagement	●	○	●	●	○	○	●	○	○	●	●
Authentifizierung	○	○	○	●	○	○	○	○	○	○	○
Automatisierung von Geschäftsprozessen	○	○	○	○	●	○	○	○	○	●	●
Benutzerdefinierte Entwicklung	●	○	●	●	○	●	●	●	○	○	●
Berichterstattung / Analyse	●	○	●	●	○	○	●	●	●	●	●
CRM	○	○	○	○	○	○	○	○	○	●	●
Datenbank-Unterstützung	○	○	●	●	●	○	●	●	○	●	○
Datenimport/-export	○	○	●	●	●	○	●	●	○	●	●
Datenvisualisierung	○	○	●	●	○	○	●	○	○	●	●
Drag-and-Drop	●	●	●	●	●	●	●	●	○	●	●
Drittanbieter-Integration	○	○	●	●	○	○	●	●	○	●	●
Echtzeit-Aktualisierung	○	○	○	●	○	○	●	○	○	○	○
Echtzeit-Benachrichtigungen	○	○	○	●	○	○	○	○	○	○	○
Echtzeit-Berichterstattung	○	○	●	●	○	○	○	○	○	○	●
Echtzeit-Daten	●	○	●	●	○	●	○	○	○	○	●
Einsatz-Management	○	●	●	●	●	●	○	○	○	○	●
Entwicklung von Web-Apps/mobilen Apps	○	●	●	●	●	●	○	●	○	●	●
Formularverwaltung	●	○	○	○	○	○	○	○	○	○	○
Geschäftsprozess-Steuerung	○	○	○	○	○	○	○	○	●	○	○
Integrationsmanagement	○	●	●	○	●	●	○	●	○	●	●
Integrierte Entwicklungsumgebung	○	○	○	●	○	○	○	○	○	○	○
Iterationsverwaltung	○	○	●	○	●	●	●	●	○	●	●
Kalenderverwaltung	●	○	○	○	○	○	○	○	○	○	○
KI-unterstützte Entwicklung	○	○	○	○	●	●	○	●	○	○	●
Kollaborative Entwicklung	○	○	●	○	●	●	○	○	○	●	●
Konfigurierbarer Workflow	○	○	○	●	○	○	○	●	○	○	●

Kontrolle des Genehmigungsprozesses	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Kundenspezifisches Branding	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Lifecycle-Management	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Mobiler Zugriff	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
No-Code	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
No-Code-Entwicklung	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Offline-Zugriff	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Projektmanagement	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Prozessmodellierung & Design	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Überwachung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Versionskontrolle	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Visuelle Modellierung	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vorgefertigte Module	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vorgefertigte Vorlagen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web-Formulare	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Werkzeuge zur Zusammenarbeit	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Workflow-Management	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Zugriffskontrollen/Berechtigungen	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Anhang 5 Funktionssteckbriefe für Low-Code-/No-Code-Plattformen



Bezeichnung: quixy Hyderabad, Indien https://quixy.com	Funktionen: API Aktivitäts-Dashboard Anforderungsmanagement Anpassbare Berichte, Felder, Formulare, Vorlagen Audit Trail Aufgabenmanagement Automatisierung von Geschäftsprozessen Berichterstattung und Statistik CRM Daten-Import / -Export Datenbank-Unterstützung Datenvisualisierung Drag-and-Drop Drittanbieter-Integration Entwicklung von Web-Apps/mobilen Apps Integrationsmanagement Iterationsverwaltung Kollaborative Entwicklung Kontrolle des Genehmigungsprozesses Kundenspezifisches Branding Lifecycle-Management Mobiler Zugriff Projektmanagement Versionskontrolle Zugriffskontrollen/Berechtigungen	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsamer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Cloudbasierte, nutzerfreundliche digitale Transformationsplattform, die es Geschäftsanwendern ohne Programmierkenntnissen ermöglicht, beliebig viele Anwendungen für Unternehmen zu erstellen.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Android (mobil) iPhone (mobil)	Startpreis 10.00 \$/Monat Kostenlose Version Nein Gratis Testen Ja	

©FIR e.V. an der RWTH Aachen und IPRI gGmbH



Bezeichnung: Bubble (keine Muttergesellschaft) New York, USA https://bubble.io	Funktionen: Drag-and-Drop Einsatz-Management Entwicklung von Web-Apps/mobilen Apps No-Code-Entwicklung Integrationsmanagement Visuelle Modellierung Vorgefertigte Module Werkzeuge zur Zusammenarbeit Workflow-Management	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsamer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Cloudbasierte Lösung, mit der Unternehmen ohne Programmierkenntnisse mobile und Webanwendungen erstellen und entwerfen können.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert)	Startpreis 29.00 \$/Monat Kostenlose Version Ja Gratis Testen Nein	

©FIR e.V. an der RWTH Aachen und IPRI gGmbH





Bezeichnung: OutSystems (keine Muttergesellschaft) Boston, USA https://www.outsystems.com	Funktionen: API Aktivitäts-Dashboard Alarmfunktion / Benachrichtigungen Anforderungsmanagement Anpassbare Felder, Formulare, Vorlagen Audit Trail Benutzerdefinierte Entwicklung Berichterstattung und Statistik Daten-Import / -Export Datenbank-Unterstützung Drag-and-Drop Drittanbieter-Integration Integrationsmanagement Entwicklung von Web-Apps/mobilen Apps Iterationsverwaltung KI-unterstützte Entwicklung Konfigurierbarer Workflow Kontrolle des Genehmigungsprozesses Kundenspezifisches Branding Lifecycle-Management Versionskontrolle Visuelle Modellierung Zugriffskontrollen/Berechtigungen Überwachung	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Wir dienen IT-Teams in mittelgroßen bis großen Unternehmen, in jeder Branche, die Technologie schnell entwickeln, implementieren, verwalten und die mobilen und Web-Apps schnell gemäß ihrer geschäftlichen Anforderungen ändern müssen.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Mac (Desktop) Windows (Desktop) Linux (Desktop) Android (mobil) iPhone (mobil)	Startpreis auf Anfrage Kostenlose Version Ja Gratis Testen Ja	

©FIR e.V. an der RWTH Aachen und IPRI gGmbH



Bezeichnung: Ninox (keine Muttergesellschaft) Berlin, Deutschland https://ninox.com/de	Funktionen: API Anpassbare Felder, Formulare, Vorlagen Aufgabenmanagement Benutzerdefinierte Entwicklung Berichterstattung und Statistik Daten-Import / -Export Datenbank-Unterstützung Datenvisualisierung Drag-and-Drop Drittanbieter-Integration Echtzeit-Aktualisierung Iterationsverwaltung No-Code Werkzeuge für die Zusammenarbeit Zugriffskontrollen/Berechtigungen	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Ninox ermöglicht es Anwendungen aus verschiedenen Abteilungen, z. B. CRM, ERP, HR, Buchhaltung, Vertrieb und PM, zu integrieren und anzupassen, um Abläufe effizienter zu gestalten. Zusätzlich fördert Ninox Teamzusammenarbeitsfunktionen und die Integration der am häufigsten verwendeten Dienste wie Google (Sheets, Drive, Calendar, Forms) und vieles mehr.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Mac (Desktop) Windows (Desktop) Android (mobil) iPhone (mobil)	Startpreis 10,00 €/Monat Kostenlose Version Ja Gratis Testen Ja	

©FIR e.V. an der RWTH Aachen und IPRI gGmbH





Bezeichnung: PEGA (keine Muttergesellschaft) Cambridge, USA https://www.pega.com	Funktionen: Berichterstattung / Analyse Geschäftsprozess-Steuerung Prozessmodellierung & Design Werkzeuge zur Zusammenarbeit	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Plattform mit Fokus auf die schnelle, kollaborative Entwicklung von Anwendungen mit integriertem Projektmanagement.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Startpreis Android (mobil) 90,00 \$/Monat iPhone (mobil) Kostenlose Version Ja Gratis Testen Ja		

©FIR e.V. an der RWTH Aachen und IPRI gGmbH



Bezeichnung: mendix (Siemens) Boston, USA https://www.mendix.com	Funktionen: API Anforderungsmanagement Benutzerdefinierte Entwicklung Drag-and-Drop Echtzeit-Daten Einsatz-Management Entwicklung von Web-Apps/mobilen Apps Integrationsmanagement Iterationsverwaltung KI-unterstützte Entwicklung Kollaborative Entwicklung Lifecycle-Management Mobiler Zugriff Visuelle Modellierung Workflow-Management Zugriffskontrollen/Berechtigungen Überwachung	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Das Erstellen von Anwendungen auf Mendix ist durch die Verwendung visueller Modelle einfach, schnell und intuitiv. Dies ermöglicht es einem breiten Personalrats, vom Entwickler bis zum Business Analyst, robuste Anwendungen ohne Code zu erstellen. Mit der modellgetriebenen Entwicklung können Unternehmensleiter und IT eine gemeinsame Sprache verwenden, in der sie rasch innovativ sein können.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Startpreis Windows (Desktop) 10,00 €/Monat Linux (Desktop) Kostenlose Version Ja Gratis Testen Ja		

©FIR e.V. an der RWTH Aachen und IPRI gGmbH





Bezeichnung: LANSa (Idera Inc.) Austin, USA https://lansa.com	Funktionen: API Automatisierung von Geschäftsprozessen Daten-import/-Export Datenbank-Unterstützung Drag-and-Drop Einsatz-Management Entwicklung von Web-Apps/mobilen Apps Integrationsmanagement Iterationsverwaltung KI-unterstützte Entwicklung Kollaborative Entwicklung Versionskontrolle Visuelle Modellierung Zugriffskontrolle/Berechtigungen	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit												
Beschreibung: Low-Code-Tool zur schnellen Anwendungsentwicklung für Mobil-, Web- und Cloud-Entwickler. LANSa bietet eine einsprachige IDE, um Client-seitig, serverseitig und alles dazwischen zu generieren.														
Voraussetzungen / Kosten: <table style="width: 100%; border: none;"> <tr> <td style="border: none;">Cloud, SaaS (webbasiert)</td> <td style="border: none;">Startpreis auf Anfrage</td> </tr> <tr> <td style="border: none;">Mac (Desktop)</td> <td style="border: none;">Kostenlose Version</td> </tr> <tr> <td style="border: none;">Windows (Desktop)</td> <td style="border: none;">Nein</td> </tr> <tr> <td style="border: none;">Linux (Desktop)</td> <td style="border: none;">Gratis Testen</td> </tr> <tr> <td style="border: none;">Android (mobil)</td> <td style="border: none;">Ja</td> </tr> <tr> <td style="border: none;">iPhone (mobil)</td> <td style="border: none;"></td> </tr> </table>			Cloud, SaaS (webbasiert)	Startpreis auf Anfrage	Mac (Desktop)	Kostenlose Version	Windows (Desktop)	Nein	Linux (Desktop)	Gratis Testen	Android (mobil)	Ja	iPhone (mobil)	
Cloud, SaaS (webbasiert)	Startpreis auf Anfrage													
Mac (Desktop)	Kostenlose Version													
Windows (Desktop)	Nein													
Linux (Desktop)	Gratis Testen													
Android (mobil)	Ja													
iPhone (mobil)														

©FIR e.V. an der RWTH Aachen und IPRI gGmbH



Bezeichnung: appian McLean, USA https://appian.com	Funktionen: API Alarmfunktion/Benachrichtigungen Anpassbare Vorlagen Aufgabenmanagement Benutzerdefinierte Entwicklung Berichterstattung und Statistik Drag-and-Drop Echtzeit-Daten Formularverwaltung Kalenderverwaltung Mobiler Zugriff Offline-Zugriff Werkzeuge zur Zusammenarbeit	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit												
Beschreibung: Software-Entwicklungsplattform, die intelligente Automatisierung und Low-Code-Entwicklung für Unternehmen kombiniert, um schnell leistungsstarke Geschäftsanwendungen bereitzustellen.														
Voraussetzungen / Kosten: <table style="width: 100%; border: none;"> <tr> <td style="border: none;">Cloud, SaaS (webbasiert)</td> <td style="border: none;">Startpreis</td> </tr> <tr> <td style="border: none;">Mac (Desktop)</td> <td style="border: none;">75,00 \$/Monat</td> </tr> <tr> <td style="border: none;">Windows (Desktop)</td> <td style="border: none;">Kostenlose Version</td> </tr> <tr> <td style="border: none;">Linux (Desktop)</td> <td style="border: none;">Nein</td> </tr> <tr> <td style="border: none;">Android (mobil)</td> <td style="border: none;">Gratis Testen</td> </tr> <tr> <td style="border: none;">iPhone (mobil)</td> <td style="border: none;">Ja</td> </tr> </table>			Cloud, SaaS (webbasiert)	Startpreis	Mac (Desktop)	75,00 \$/Monat	Windows (Desktop)	Kostenlose Version	Linux (Desktop)	Nein	Android (mobil)	Gratis Testen	iPhone (mobil)	Ja
Cloud, SaaS (webbasiert)	Startpreis													
Mac (Desktop)	75,00 \$/Monat													
Windows (Desktop)	Kostenlose Version													
Linux (Desktop)	Nein													
Android (mobil)	Gratis Testen													
iPhone (mobil)	Ja													

©FIR e.V. an der RWTH Aachen und IPRI gGmbH





Bezeichnung: eLegere Pavia, Italien https://www.elegere.com	Funktionen: API Agile Methodiken Aktivitäts-Dashboard Alarmfunktion / Benachrichtigungen Anpassbare Berichte, Felder, Formulare, Vorlagen Aufgabenmanagement Authentifizierung Benutzerdefinierte Entwicklung Berichterstattung und Statistik Daten-Import / -Export Datenbank-Unterstützung Datensvisualisierung Drag-and-Drop Drittanbieter-Integration Echtzeit-Aktualisierungen Echtzeit-Benachrichtigungen Echtzeit-Berichterstattung Echtzeit-Daten Einsatz-Management Entwicklung von Web-Apps/mobilen Apps Integrierte Entwicklungsumgebung Konfigurierbarer Workflow Kontrolle des Genehmigungsprozesses Kundenspezifisches Branding Mobiler Zugriff No-Code Versionskontrolle Vorgefertigte Vorlagen Web-Formulare Werkzeuge zur Zusammenarbeit Workflow-Management Zugriffskontrollen/Berechtigungen	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: eLegere ist eine All-In-One Plattform die es ermöglicht Geschäftsprozesse und operative Daten zentral in einer digitalen Anwendung zu vereinen.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Startpreis Mac (Desktop) auf Anfrage Windows (Desktop) Kostenlose Version Linux (Desktop) Nein Android (mobil) Gratis Testen iPhone (mobil) Ja		

©FIR e.V. an der RWTH Aachen und IPRI gGmbH



Bezeichnung: Studio Creatio Boston, USA https://www.creatio.com/studio	Funktionen: API Aktivitäts-Dashboard Alarmfunktion / Benachrichtigungen Anforderungsmanagement Anpassbare Felder, Formulare Anwendungsmanagement Audit Trail Aufgabenmanagement Automatisierung von Geschäftsprozessen Benutzerdefinierte Entwicklung Berichterstattung und Statistik CRM Daten-Import / -Export Datensvisualisierung Drag-and-Drop Drittanbieter-Integration Echtzeit-Berichterstattung Echtzeit-Daten Einsatz-Management Entwicklung von Web-Apps/mobilen Apps Integrationsmanagement Iterationsverwaltung KI-unterstützte Entwicklung Kollaborative Entwicklung Konfigurierbarer Workflow Kontrolle des Genehmigungsprozesses Kundenspezifisches Branding Lifecycle-Management Mobiler Zugriff Projektmanagement Versionskontrolle Workflow-Management Zugriffskontrollen/Berechtigungen	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/Selbstbestimmtheit* <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Intelligente Low-Code- und Business-Process-Management-Plattform mit sofort einsatzbereiten Lösungen und Vorlagen, die mittleren und großen Unternehmen die einfache Erstellung von Anwendungen für verschiedene Geschäftsaufgaben ermöglicht – von kundenorientierten Anwendungen bis hin zu Integrationen in Lösungen von Drittanbietern.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert) Startpreis Mac (Desktop) 25,00 \$/Monat Windows (Desktop) Kostenlose Version Linux (Desktop) Nein Android (mobil) Gratis Testen iPhone (mobil) Ja		

©FIR e.V. an der RWTH Aachen und IPRI gGmbH





Bezeichnung: Caspio Sunnyvale, USA https://www.caspio.com	Funktionen: API Alarmfunktion / Benachrichtigungen Anpassbare Berichte, Felder, Formulare, Vorlagen Audit Trail Aufgabenmanagement Benutzerdefinierte Entwicklung Berichterstattung und Statistik Daten-Import / -Export Datenbank-Unterstützung Datenvisualisierung Drag-and-Drop Drittanbieter-Integration Echtzeit-Berichterstattung Echtzeit-Daten Einsatz-Management Entwicklung von Web-Apps/mobilen Apps Integrationsmanagement Iterationsverwaltung Kollaborative Entwicklung Kontrolle des Genehmigungsprozesses Kundenspezifisches Branding Mobiler Zugriff Projektmanagement Versionskontrolle Workflow-Management Zugriffskontrollen/Berechtigungen	Erfüllte Anforderungen Zentrale IT: <input type="checkbox"/> Sicherheit <input type="checkbox"/> Berechtigungskonzept <input type="checkbox"/> Kontrolliertes Deployment <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Wiederverwendbare Elemente <input type="checkbox"/> Zugriff auf Daten und Apps <input type="checkbox"/> Dokumentation/Nachvollziehbarkeit <input type="checkbox"/> Einfache Bedienbarkeit <input type="checkbox"/> Aufwandsarmer Support <input type="checkbox"/> Integration Code Revision, CI/CD <input type="checkbox"/> Export von Daten <input type="checkbox"/> Anonymisierung Zentrale IT: <input type="checkbox"/> Visual Development <input type="checkbox"/> Einfache Bedienbarkeit per Drag & Drop <input type="checkbox"/> Lösungsorientiert <input type="checkbox"/> Klare Vorgaben <input type="checkbox"/> Unbürokratisch <input type="checkbox"/> Selbsthilfe über Tutorials <input type="checkbox"/> Freiräume/"Selbstbestimmtheit" <input type="checkbox"/> Interoperabilität <input type="checkbox"/> Export von Daten <input type="checkbox"/> Mehrsprachigkeit
Beschreibung: Low-Code-Plattform zur Erstellung von Online-Datenbankanwendungen ohne Programmierung. Die All-in-one-Plattform bietet alles um Geschäftsabläufe und Workflows digital umzuwandeln. Die Plattform beinhaltet eine integrierte Cloud-Datenbank, einen visuellen Anwendungs-Builder, Sicherheit auf Unternehmensebene, Einhaltung gesetzlicher Vorschriften und eine skalierbare globale Infrastruktur.		
Voraussetzungen / Kosten: Cloud, SaaS (webbasiert)	Startpreis 100,00 \$/Monat Kostenlose Version Ja Gratis Testen Ja	

©FIR e.V. an der RWTH Aachen und IPRI gGmbH



Anhang 6 Mock-up des Webdemonstrators

Legitimise IT | Startseite | Dashboard | Tool | Projekt | **Institute**

Willkommen auf der Projekt-Homepage von Legitimise IT!

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

Registrierung

E-Mail Adresse

 Passwort

 Log-In

fir RWTH Aachen | IPRI INTERNATIONAL PERFORMANCE RESEARCH INSTITUTE

Gefördert durch:

 Das IGF-Vorhaben 05339/19 N der Forschungsvereinigung FIR e. V. an der RWTH Aachen wird über die AIF im Rahmen des Programms zur Förderung der industriellen Gemeinschaftsforschung (IGF) vom Bundesministerium für Wirtschaft und Energie (BMWi) aufgrund eines Beschlusses des Deutschen Bundestages gefördert.

AF
 Forschungsnetzwerk Mittelstand

Möchten Sie zum IT-Tool?

Suchen Sie weitere Informationen über das Projekt?

Legitimise IT | Startseite | Dashboard | Tool | Projekt | **Institute**

Gewichtung

Identifikation

Legitimise IT | Startseite | Dashboard | Tool | Projekt | **Institute**

Gewichtung

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua.

Bitte geben Sie an, wie wesentlich der jeweilige Aspekt für Ihre IT-Strategie ist:

Prozessstandardisierung und -optimierung heben unwichtig ————— wichtig	Systemintegration vorantreiben unwichtig ————— wichtig
Datenschutz sicherstellen unwichtig ————— wichtig	Schutz von Betriebsgeheimnissen sicherstellen unwichtig ————— wichtig
Datenqualität und -validität sicherstellen unwichtig ————— wichtig	Datenverfügbarkeit sicherstellen unwichtig ————— wichtig
Effizienzen heben unwichtig ————— wichtig	Wirtschaftlichkeit heben unwichtig ————— wichtig
Zentrale IT ist ganzheitlicher Lösungsanbieter unwichtig ————— wichtig	Zentrale IT ist Enabler für Zusammenarbeit, Produktivität und Flexibilität unwichtig ————— wichtig
Innovationsfähigkeit unterstützen unwichtig ————— wichtig	

Identifikation von Schatten IT

Analyse der IT-Infrastruktur

zum Ansatz

Analyse von Service-Desk-Anfragen

zum Ansatz

Vergleich von Budgets

zum Ansatz

Unterstützende Tools

zum Ansatz

Zurück | Weiter | Zurück | Weiter

Legitimise IT Startseite Dashboard Tool Projekt Institute

Erfassung

Erfassung der Schatten IT


Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

Welche Anwendung suchen Sie?

Name, Typ, etc.

Lorem
 Ipsum
 Dolor
 Sit
 Amet


Business Managed IT



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

+


Central Managed IT



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

+

Schnittstellen



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

+

Name
Excel-Sheet, Batch-File, etc.

Beschreibung

Kategorie
Kategorie

Nutzen
Bitte wählen Sie die Nutzenaspekte aus, welche auf die Lösung zutreffen:

Innovative Lösung
 Lösung für IT-Defizit
 Lösung für funktionales Defizit

Effizienz
 Produktivität
 Vereinfachung von Prozessen

Flexibilität
 Zusammenarbeit
 Lorem ipsum dolor

Risiken
Bitte wählen Sie die Risiken aus, welche auf die Lösung zutreffen:

Datenakzidität
 Zugriff
 Verarbeitung personenbezogener Daten

Medienbrüche
 Integrationsaufwand
 Verarbeitung sensibler Daten

Kosten
 Personelle Abhängigkeit

weitere Merkmale

Prozessakzidität: 1 - 10
 Technische Qualität: Lorem ipsum dolor

Informationsqualität: 1 - 10
 Benutzerfreundlichkeit: 1 - 10

Support: 1 - 10
 Redundanz:

Nutzerkreis:

[Hinzufügen](#)

[Zurück](#)
[Weiter](#)

Legitimise IT Startseite Dashboard Tool Projekt Institute

Erfassung

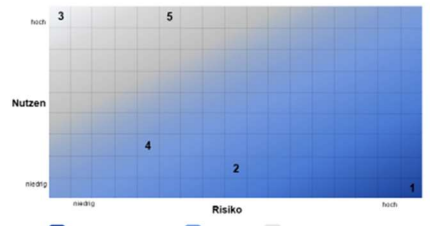
Auswertung der Business Managed IT

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

hoch

3

5



nutzen

hoch

1

2

4

3

hoch

nutzen

hoch

hoch

hohes Risiko / geringer Nutzen
 ambivalent
 geringes Risiko / hoher Nutzen

Anzeige

Filter

Lorem
 Ipsum
 Dolor
 Sit
 Amet

[Zurück](#)
[Weiter](#)

Legitimise IT Startseite Dashboard Tool Projekt Institute

Erfassung

Report

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

Government



Platform



Regulation



Legitimierung



BM1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BM2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BM3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
BM4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Ablösen



Die Lösungsmatrix **Ablösen** zielt darauf ab die Nutzung einer identifizierten Schatten-IT besonders bei Redundanzen anzuweisen und durch ein anderes System, meist eines der offiziellen IT-Infrastruktur, zu ersetzen.

[Literatur](#)

Awareness



Der Ansatz **Awareness** und Training dient der generischen Prävention. Er zielt darauf ab, das Bewusstsein der Mitarbeiter für IT-Risikofälle und die Konsequenzen einer Nicht-Erfüllung dieser zu stärken, um so die Erhaltung von Schatten-IT zu verhindern.

[Literatur](#)

Governance



Der Lösungsansatz **Governance** zielt darauf ab die Verantwortungen über eine identifizierte Schatten-IT entweder klar zu definieren oder zu übertragen. Die Übertragung von Verantwortungen, beispielsweise an die Zentrale IT, kann auch dazu dienen die Anwendung weiterzuentwickeln.

[Literatur](#)

Legitimierung



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

[Literatur](#)

Plattformen



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

[Literatur](#)

Registrierung



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet citta kasd gubergren, no sea takimata.

[Literatur](#)

[Zurück](#)
[Weiter](#)

Anhang 7: Steckbriefe der bestehenden Reifegradmodelle

Titel	Autor(en)	Jahr	Herkunft	Anwendungsbereich	Reifegradstufen	Dimensionen	Entwicklungsstrategien
Capability Maturity Model (CMM)	Mark C. Paulik et. al (1993)	1993	Wissenschaft	Beurteilung der Qualität des Softwareprozesses (Softwareentwicklung, Wartung, Konfiguration etc.)	Bestehend aus fünf Reifegradstufen. Diese lauten wie folgt: <i>Initial</i> (beginnend) <i>repeatable</i> (wiederholbar) <i>defined</i> (definiert) <i>managed</i> (gesteuert) <i>optimizing</i> (optimierend)	IT-Systeme Daten Software	Keine Angaben
Capability Maturity Level Integration	Chrissis (2003)	2003	Wissenschaft	Reifegradmodell für die Entwicklung von Produkten und Dienstleistungen	Bestehend aus fünf Reifegradstufen, welche je nach Anwendungsbereich ausgestaltet werden können. Diese lauten wie folgt: <ul style="list-style-type: none"> • Initial • Managed • Defined • Quantitatively Managed • Managed • Optimizing 	Projektmanagement, Prozessmanagement, Support	Weiterentwicklung des Maturity-Model- und Quality-Management-Maturity-Grids
Organizational Project Management Maturity Level (OPM3)	Fahrenkrog et al. (2003)	2003	Wissenschaft	Strategische Ebene des Projektmanagements	<ul style="list-style-type: none"> • Standardize • Measure • Control • Continuously Improve 	Projektmanagement, Prozesssteuerung	keine Angaben
Software Process Improvement and Capability Determination (SPICE)	Dorling (1993)	1993	Wissenschaft	Spezialisiertes Capability-Maturity-Modell für die Softwareentwicklung	Die Befähigungs- oder Reifegrad-Dimension besteht aus den sechs Stufen, in denen jeweils neue Prozessattribute eingeordnet sind: <ul style="list-style-type: none"> • Unvollständig 	Software-Prozess-Management, Projektmanagement	keine Angaben

					<ul style="list-style-type: none"> • durchgeführt: Prozessdurchführung • gesteuert: Leistungssteuerung, Ergebnissteuerung • etabliert: Prozessdefinition, Prozessumsetzung • vorhersagbar: Prozessmessung, Prozesssteuerung • optimierend: Prozessinnovation, Prozessoptimierung 		
IBM-IT Maturity Model	IBM (2007)	2007	Praxis	Reifegradmodell zur Effektivität der IT-Landschaft	<ul style="list-style-type: none"> • Initial: Es gibt keine Standards und innerhalb der Organisation herrscht Uneinheitlichkeit. • managed: Ein Prozess ist vorhanden und Aktivitäten werden verwaltet, aber der Prozess ist eine Orchestrierung ohne Erkenntnisse. • defined: Ein Prozess ist unternehmensweit als Standard definiert und wird auf einzelne Projekte zugeschnitten. • Quantitatively Managed: Der Prozess wird gemessen und jede Abweichung vom Standard wird behandelt. • optimiert: Der Prozess wird kontinuierlich verbessert. 	Sicherheit Organisation Data Science Governance Architektur	Keine Angaben
Business-IT Maturity Model	Pearlson u. Saunders (2007)	2007	Wissenschaft	Beschreibt Verhältnis zwischen Demand von IT-Anwendungen und Supply durch die IT	Das Modell umfasst drei Stufen, die aus zwei verschiedenen Perspektiven betrachtet werden: Geschäftsnachfrage und IT-	IT-Architektur Projektmanagement, Prozessmanagement	keine Angaben

					<p>Angebot. Das Modell stellt eine S-förmige Lernkurve dar, die den mit zunehmenden Reifegraden verbundenen Lernprozess widerspiegeln.</p> <p>Die drei Stufen lauten:</p> <ul style="list-style-type: none"> • Business-IT-Reife • Business-Effizienz • Business-Transformation 		
IT Capability Maturity Framework	Curley (2004)	2004	Praxis	Reifegradmodell für IT-Performance	<p>Beim IT-CMF geht es um die schrittweise Verbesserung des IT-Reifegrads in den vier Makrofähigkeiten auf der Grundlage einer fünfstufigen Reifekurve:</p> <ul style="list-style-type: none"> • <i>Initial</i> • <i>Basic</i> • <i>Intermediate</i> • <i>Advanced</i> • <i>Optimising</i> <p>Makroebenen</p> <ul style="list-style-type: none"> • Managing IT like a Business • Managing the IT Budget • Managing the IT Capability • Managing IT for Business 	IT-Management, IT-Budget	keine Angaben
IT-Governance, Risiko und Compliance-Management (IT-GRC)	Johannsen u. Kant (2020)	2020	Wissenschaft	Reifegradmodell für IT-Governance, Risiko- und Compliance-Management	<p>Fünf Reifegrade in den Kategorien:</p> <ul style="list-style-type: none"> • Mobile Sicherheit • Cyber-Sicherheit • ISMS • Security-Awareness • IT-Governance • IT-Compliance 	IT-Management IT-Governance IT-Risiko	

<p>P3M3 - Portfolio, Programme & Project Management Maturity Model</p>	<p>Axelos (2015)</p>	<p>2015</p>	<p>Praxis</p>	<p>Reifegradmodell zur Effektivität im Projektmanagement</p>	<p>P3M3-Bewertungen können sowohl auf Portfolio-, Programm- und/oder Projektmanagement-Aktivitäten angewendet werden, die in einer Organisation durchgeführt werden.</p> <p>P3M3 besteht aus drei Modellen, die einzeln oder als Gruppe bewertet werden können:</p> <ul style="list-style-type: none"> • Project-Management <ul style="list-style-type: none"> • Programme-Management • Portfolio-Management <p>Für jedes der Modelle überprüft P3M3 den Reifegrad und die Leistung anhand von sieben Perspektiven: Organisational Governance</p> <ul style="list-style-type: none"> • Benefits and/or Requirements Management • Financial Controls • Risk-Management • Stakeholder-Management • Resource-Management • Management-Controls 	<p>Informations- und Wissensmanagement, Infrastruktur und Instrument, Planung, Organisation, Techniken, Prozess, Integration von Modellen</p>	<p>CMM</p>
--	----------------------	-------------	---------------	--	--	---	------------

Anhang 8: Halbstandardisierter Interviewleitfaden

Teil 1: Einführung	
	<ul style="list-style-type: none">• Vorstellung des Interviewers
	<ul style="list-style-type: none">• (ggf.) Vorstellung des Interviewpartners
	<ul style="list-style-type: none">• Genehmigung einholen zwecks Tonaufzeichnung des Interviews
Teil 2: Vorstellung des RPA-Reifegradmodells	
	<ul style="list-style-type: none">• Aufzeigen des RPA-Reifegradmodells (Excel-Tool)
	<ul style="list-style-type: none">• Aufzeigen des dazugehörigen Fragebogens
Teil 3: Evaluation	
Vollständigkeit und Verständlichkeit des Reifegradmodells	<ul style="list-style-type: none">• Geben die Gestaltungsebenen, Gestaltungsdimensionen, insbesondere die Gestaltungsobjekte ein adäquates Bild der Realität ab?• Wurde etwas vergessen?• Wo sehen Sie im Reifegradmodell Verbesserungsbedarf? Konkrete Vorschläge• Ist das Reifegradmodell in seiner jetzigen Form zu komplex?
Praxistransfer	<ul style="list-style-type: none">• Sind Sie der Meinung, dass das Reifegradmodell auch in der Praxis einsetzbar ist?

Anhang 9: Aggregierte Gewichtung der Gestaltungsobjekte aus den beiden Experteninterviews

Gestaltungsobjekt	Relevanz				
	1 = sehr gering	2 = gering	3 =mittel	4 = hoch	5 = sehr hoch
IT-Strategie	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Unterstützung durch das Management	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Potenzialbewusstsein	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT-Feedback Kultur und Kommunikation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Transparenz	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Prozesse zur Identifikation von Schatten-IT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Prozesse für den Umgang mit Schatten-IT	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Risiko- und Nutzenbewertung	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Definition von Verantwortlichkeiten	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Ressourcenbereitstellung	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Schulungen zum Thema Schatten-IT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Awareness	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Silodenken und Zusammenarbeit	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Monitoring-Tools	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Literaturverzeichnis

- ADEYERI, M. K.; AYODEJI, S. P.; AKINNULI, B. O.; FARAYIBI, P. K.; OJO, O. O.; ADELEKE, K.: Development of SMEs Coping Model for Operations Advancement in Manufacturing Technology. In: *Advanced Applications in Manufacturing Engineering*. Hrsg.: M. Ram; J. P. Davim. Elsevier, Amsterdam [u. a.] 2019, S. 169–190. <https://doi.org/10.1016/B978-0-08-102414-0.00006-9>
- AKTIV-KOMMUNAL (HRSG.): Medienbrüche und Schnittstellen im Prozess analysieren. 2019. <https://aktiv-kommunal.de/index.php/toolbox-zur-digitalisierung-interner-arbeit-und-leistungsprozesse/ist-prozesse-analysieren/medienbrueche-und-schnittstellen-im-prozess-analysieren/> (Link zuletzt geprüft: 28.03.2023)
- BAUR, N.; BLASIUS, J.: Methoden der empirischen Sozialforschung. In: *Handbuch Methoden der empirischen Sozialforschung*. Hrsg.: N. Baur; J. Blasius. Springer Gabler, Wiesbaden 2014, S. 41–62. https://doi.org/10.1007/978-3-531-18939-0_1
- BECKER, J.; KNACKSTEDT, R.; PÖPPELBUß, J.: Entwicklung von Reifegradmodellen für das IT-Management: Vorgehensmodell und praktische Anwendung. In: *Wirtschaftsinformatik* 51(2009)3, S. 249–260.
- BECKER, J.; KNACKSTEDT, R.; PÖPPELBUß, J.; SCHWARZE, L.: Das IT Performance Measurement Maturity Model – Ein Reifegradmodell für die Business-Intelligence-Unterstützung des IT-Managements. In: *DW2008*. Hrsg.: B. Dinter; R. Winter; P. Chamoni; N. Gronau; K. Turowski. Gesellschaft für Informatik e. V., Bonn 2008, S. 53–74. https://dl.gi.de/bitstream/handle/20.500.12116/24078/P138_3.pdf?sequence=1&isAllowed=y (Link zuletzt geprüft: 28.03.2023)
- BEHRENS, S.: Shadow systems: The Good, The Bad and The Ugly. In: *Communications of the ACM* 52(2009)2, S. 124–129. <https://doi.org/10.1145/1461928.1461960>.
- BOLLHÖFER, E; JÄGER, A.: Wirtschaftsspionage und Konkurrenzausspähung – Vorfälle und Prävention bei KMU im Zeitalter der Digitalisierung. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Reihe A: Arbeitsberichte, Bd. A 8 09/2018. Hrsg.: H.-J. Albrecht; U. Sieber. Freiburg im Breisgau 2018. https://pure.mpg.de/rest/items/item_3002884_8/component/file_3016263/content (Link zuletzt geprüft: 28.03.2023)
- BRENNER, W.; GYÖRY, A.; PIROUZ, M.; UEBERNICKEL, F.: Bewusster Einsatz von Schatten-IT: Zwischen Sicherheit & Innovationsförderung. Universität St. Gallen, 20.10.2011. <https://www.alexandria.unisg.ch/214464/1/ATT2R549.pdf> (Link zuletzt geprüft: 28.03.2023)
- BRÖHL, B.: Unterschätztes Sicherheitsrisiko Schatten-IT. *manage IT online*, 21.02.2017. <https://ap-verlag.de/unterschaetztes-sicherheitsrisiko-schatten-it/31302/> (Link zuletzt geprüft: 28.03.2023)
- BROWN, C.; CZERNIEWICZ, L.: Debunking the ‘digital native’: beyond digital apartheid, towards digital democracy. In: *Journal of Computer Assisted Learning* 26(2010)5, S. 357–369. <https://doi.org/10.1111/j.1365-2729.2010.00369.x>
- BRUIN, T. DE; FREEZE, R.; KULKARNI, U.; ROSEMANN, M.: Understanding the Main Phases of Developing a Maturity Assessment Model. In: [Proceedings] 16 th Australasian Conference on Information Systems Maturity Assessment Model 29 Nov – 2 Dec 2005, Sydney 2005. Association for Information Systems, 11 S. <https://www.researchgate.net/profile/Michael->

Rosemann/publication/27482282_Understanding_the_Main_Phases_of_Developing_a_Maturity_Assessment_Model/links/00b7d51f71c388cc54000000/Understanding-the-Main-Phases-of-Developing-a-Maturity-Assessment-Model.pdf (Link zuletzt geprüft: 28.03.2023)

- CHUA, C. E.; STOREY, V. C.; CHEN, L.: [Conference Paper] Central IT or Shadow IT? Factors Shaping Users' Decision to Go Rogue with IT. In: Proceedings of the 35th International Conference on Information Systems, Auckland 2014.
<https://core.ac.uk/download/pdf/301363359.pdf> (Link zuletzt geprüft: 28.03.2023)
- DEHNING, O.: Die Cloud wirft ihre Schatten auf die IT-Infrastruktur. In: *Wirtschaftsinformatik & Management* (2016)8, S. 26–31.
- FLIEHE, M.; ALICI, E.: IT-Sicherheitsaspekte in KMU. In: *Controlling* 26(2014)6, S. 314–319.
https://doi.org/10.15358/0935-0381_2014_6_314
- FÜRSTENAU, D.; ROTHE, H.; SANDNER, M.: Shadow Systems, Risk, and Shifting Power Relations in Organizations. In: *Communications of the Association for Information Systems* 41(2017), S. 43–61. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=4007&context=cais> (Link zuletzt geprüft: 28.03.2023)
- GORLA, N.; SOMERS, T. M.; WONG, B.: Organizational impact of system quality, information quality, and service quality. In: *The Journal of Strategic Information Systems* 19(2010)3, S. 207–228.
- HAAG, S.; ECKHARDT, A.: Shadow IT. *Business & Information Systems Engineering* 59(2017)6, S. 469–473. <https://doi.org/10.1007/s12599-017-0497-x>
- HAAKE, K.: Beratung in Klein- und Mittelunternehmen (KMU). In: *Strategische Unternehmensberatung: Konzeptionen – Prozesse – Methoden*. Hrsg.: I. Bamberger. 3. Auflage. Springer Gabler, Wiesbaden 2002, S. 215–240.
- HOFF, D.: How to securely embrace shadow IT in the enterprise.
<https://www.itproportal.com/2015/12/14/how-to-securely-embrace-shadow-it-in-the-enterprise/> (Link zuletzt geprüft: 20.12.2022)
- HORVÁTH, P.: Geschäftsmodellinnovationen durch Digitalisierung – Neue Herausforderungen an den Controller. In: *Technologie, Strategie und Organisation*. Hrsg.: W. Burr; M. Stephan. Springer Gabler, Wiesbaden 2017, S. 113–125. https://doi.org/10.1007/978-3-658-16042-5_6.
- HUBER, M.; ZIMMERMANN, S.; RENTROP, C.; FELDEN, C.: The Influence of Shadow IT Systems on Enterprise Architecture Management Concerns. In: [Conference Proceedings] *Information Systems. 14th European, Mediterranean, and Middle Eastern Conference, EMCIS 2017, Coimbra, Portugal, September 7–8, 2017*. Hrsg.: M. Themistocleous; V. Morabito. Springer, Cham [u. a.] 2017, S. 461–477.
- KARDEL, D.: IT-Sicherheitsmanagement in KMU. In: *HMD – Praxis der Wirtschaftsinformatik* 48(2011)5, S. 44–51. <https://doi.org/10.1007/BF03340623>
- KNOLL, M.: IT-Risikomanagement im Zeitalter der Digitalisierung. In: *HMD – Praxis der Wirtschaftsinformatik* 54(2017)1, S. 4–20. <https://doi.org/10.1365/s40702-017-0287-4>
- KÖNIGS, H.-P.: IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken. 5. Auflage. Springer Vieweg, Wiesbaden [u. a.] 2017. <https://doi.org/10.1007/978-3-658-12004-7>

- KOPPER, A.; WESTNER, M.: [Conference Paper] Deriving a Framework for Causes, Consequences, and Governance of Shadow IT from Literature. In: Multikonferenz Wirtschaftsinformatik (MKWI) 2016: Technische Universität Ilmenau, 09. – 11. März 2016. Hrsg.; V. Nissen; D. Stelzer; S. Straßburger; D. Fischer. Universitätsverlag Ilmenau, Ilmenau 2016, 12 S.
- MC AFFEE (HRSG.): Sicherheitslücken im Home-Office. McAfee-Kommentar: Umgang mit Schatten-IT. LANline, 03.07.2020. <https://www.lanline.de/it-security/mcafee-kommentar-umgang-mit-schatten-it.251951.html> (Link zuletzt geprüft: 31.03.2023)
- METTLER, T.; ROHNER, P.: [Conference Paper] Situational maturity models as instrumental artifacts for organizational design. In: DESRIST '09. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. Hrsg.: V. Vaishanvi; S. Purao. ACM Press, 2009, 9 S. <https://doi.org/10.1145/1555619.1555649>
- MOORE, RITA; JACKSON, M. J.; WILKES, R.: End-User Computing Strategy: An Examination of Its Impact on End-User Satisfaction. In: Academy of Strategic Management Journal 6(2007), S. 69–89.
- MYERS, N.; STARLIPER, M. W.; SUMMERS, S. L.; WOOD, D. A.: The Impact of Shadow IT Systems on Perceived Information Credibility and Managerial Decision Making. In: Accounting Horizons 31(2017)3, S. 105–123. <https://doi.org/10.2308/acch-51737>
- NEFF, A. A.; HAMEL, F.; HERZ, T. P.; UEBERNICKEL, F.: Developing a Maturity Model for Service Systems in Manufacturing Enterprises. In: Information & Management 51(2014)7, 17 S.
- PAULK, M. C.; CURTIS, B.; CHRISSIS, M. B.; WEBER, C. V.: Capability maturity model, Version 1.1. In: IEEE Software 10(1993)4, S. 18–27. <https://doi.org/10.1109/52.219617>
- PEARLSON, K.; SAUNDERS, C.: Managing and using information systems. John Wiley & Sons, Hoboken (NJ) [u. a.] 2007.
- PÖPPELBUß, J.; RÖGLINGER, M.: [Conference Paper] What makes a useful maturity model? A framework of general design principles for maturity models and its demonstration in business process management. In: [Proceedings] European Conference of Information Systems (ECIS) Helsinki 2011, 12 S. https://www.researchgate.net/profile/Jens-Poeppelbuss/publication/221409904_What_makes_a_useful_maturity_model_A_framework_of_general_design_principles_for_maturity_models_and_its_demonstration_in_business_process_management/links/53eb5f030cf2593ba708799b/What-makes-a-useful-maturity-model-A-framework-of-general-design-principles-for-maturity-models-and-its-demonstration-in-business-process-management.pdf (Link zuletzt geprüft: 28.03.2023)
- PORTER, M. E.: The Competitive Advantage: Creating and Sustaining Superior Performance. Free Press, New York 1998.
- PROKEIN, O.: IT-Risikomanagement: Identifikation, Quantifizierung und wirtschaftliche Steuerung. Gabler, Wiesbaden 2008. – Zugl.: Freiburg (Breisgau), Univ., Diss., 2007. <https://doi.org/10.1007/978-3-8349-9688-6>
- RAINS, J.: Shadow IT: The Impact on Technical Support and the Opportunities for IT. HDI Research Brief, März 2015. <https://www.thinkhdi.com/~media/HDICorp/Files/research-corner/promotion/rb-shadow-it-mar15.pdf> (Link zuletzt geprüft: 28.03.2023)
- REINHEIMER, S.; ROBRA-BISSANTZ, S.: Business-IT-Alignment – Kernaufgabe der Wirtschaftsinformatik. In: HMD – Praxis der Wirtschaftsinformatik 51(2014)5, S. 526–548. <https://doi.org/10.1365/s40702-014-0078-0>

- RENTROP, C.; ZIMMERMANN, S.: Schatten-IT. In: Informatik-Spektrum 38(2015)6, S. 564–567.
- RENAULT, A.; CORTINA, S.; BARAFORT, B.: Towards a Maturity Model for ISO/IEC 20000-1 for ITIL Based on The TIPA Process Capability Assessment Model. In: [Proceedings] Software Process Improvement and Capability Determination. 15th International Conference, SPICE 2015, Gothenburg, Sweden, June 16. – 17., 2015. Hrsg.: T. Rout; R. V. O'Connor; A. Dorling. Springer, Berlin [u. a.] 2015, S. 188 – 200.
- SCHÜTTE, R.: Grundsätze ordnungsmäßiger Referenzmodellierung. Konstruktion konfigurations- und anpassungsorientierter Modelle. Neue betriebswirtschaftliche Forschung; Bd. 233. Gabler, Wiesbaden 1998. – Zugl.: Münster (Westfalen), Univ., Diss., 1997. <https://doi.org/10.1007/978-3-663-10233-5>
- SILIC, M.; BACK, A.: Shadow IT – A view from behind the curtain. In: Computers & Security 45(2014)9, S. 274–283.
- STOOP, W.: Statt Schatten-IT bekämpfen, Unified Communications leben. manage IT online, 15.03.2016. <https://ap-verlag.de/statt-schatten-it-bekaempfen-unified-communications-leben/19690/> (Link zuletzt geprüft: 28.03.2023)
- TAJUL URUS, S.; MOLLA, A.; TEOH, S. Y.: Post ERP Feral System and use of 'Feral Systemas Coping Mechanism. World Academy of Science, Engineering and Technology. International Journal of Economics and Management Engineering 5(2011)12, S. 1858–1865.
- TREESOLUTION CONSULTING GMBH (HRSG.): 10 Tipps, zur Umsetzung einer Security Awareness Kampagne. TreeSolution Consulting online, 21.06.2021. <https://www.treesolution.com/news/umsetzung-security-awareness-kampagne-10-tipps> (Link zuletzt geprüft: 28.03.2023)
- URBACH, N.; AHLEMANN, F.: IT-Management im Zeitalter der Digitalisierung: Auf dem Weg zur IT-Organisation der Zukunft. Springer, Berlin [u. a.] 2016. <https://doi.org/10.1007/978-3-662-52832-7>
- WALTERBUSCH, M.; FIETZ, A.; TEUTEBERG, F.: Schatten-IT: Implikationen und Handlungsempfehlungen für Mobile Security. In: HMD – Praxis der Wirtschaftsinformatik 51(2014)1, S. 24–33.
- WELTER, M.: Die Forschungsmethode der Typisierung. In: WiSt – Wirtschaftswissenschaftliches Studium 35(2006)2, S. 113–116. <https://doi.org/10.15358/0340-1650-2006-2-113>
- WILLEKE, S.; KASSELMANN, S.: Einführung interaktiver Assistenzsysteme über Reifegradmodelle. In: Zwf – Zeitschrift für wirtschaftlichen Fabrikbetrieb 111(2016)1, S. 691–695. <https://doi.org/10.3139/104.111625>
- WITT, B. C.: Grundlagen des Datenschutzes und der IT-Sicherheit (Teil 2c): Vorlesung im Sommersemester 2016 an der Universität Ulm. Universität Ulm, Ulm 2016. https://www.uni-ulm.de/fileadmin/website_uni_ulm/iui/datenschutz/VL2016-2c.pdf (Link zuletzt geprüft: 28.03.2023)
- ZIMMERMANN, S.: Der Umgang mit Schatten-IT in Unternehmen: Eine Methode zum Management intransparenter Informationstechnologie. Schriften zur Business Analytics und zum Informationsmanagement. Springer Gabler, Wiesbaden 2018. – Zugl.: Freiberg, Techn. Univ., Diss., 2016.
- ZIMMERMANN, S.; RENTROP, C.: SchattenIT. In: HMD – Praxis der Wirtschaftsinformatik 49(2012)6, S. 60– 68.

