Bundesministerium
für Bildung
und Forschung

ProBITS

19.12.2024

Multikriterielles Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von IT-Sicherheitsmaßnahmen (MEBITS)

Kurzbericht zum Teilvorhaben im Verbundprojekt

“Prozessorientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen (ProBITS)”

Martin-Luther-Universität Halle-Wittenberg

Lehrstuhl für Wirtschaftsinformatik,

insb. Betriebliches Informationsmanagement

Autorinnen und Autoren:

Dr. Stephan Kühnel

Laura Bauer

Leonard Nake

Prof. Dr. Stefan Sackmann

1. Aufgabenstellung und Anknüpfung an den Stand der Wissenschaft und Technik

Das Teilvorhaben „Multikriterielles Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von IT-Sicherheitsmaßnahmen“ (MEBITS) zielte als Teil des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojekts „Prozessorientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen“ (ProBITS) darauf ab, die vier zentralen ProBITS-Bausteine (1. Erweiterte Prozessmodellierungssprache, 2. Multikriterielles Entscheidungsmodell, 3. Vorgehensmodell und 4. IT-Werkzeug) gemeinsam mit den Verbundpartnern zu entwickeln. Durch die Realisierung der Bausteine wurde im Gesamtprojekt ein innovativer, skalierbarer und werkzeuggestützter Ansatz bereitgestellt, der eine mehrdimensionale, geschäftsprozessorientierte Bewertung von IT-Sicherheitsmaßnahmen (ITS-Maßnahmen) und -Maßnahmenbündeln ermöglicht.
Im Zentrum von MEBITS stand vor allem die Realisation der ersten beiden Bausteine – des multikriteriellen Entscheidungsmodells und der erweiterten Prozessmodellierungssprache –, die es ermöglichen, unter Berücksichtigung verschiedener Prozesseinflussgrößen, kosten- und nutzenorientierter Bewertungsdimensionen sowie praktischer Anforderungen, alternative ITS-Maßnahmen(-bündel) zu analysieren. Entscheider kleinerer, mittlerer und großer Unternehmen wurden und werden damit in die Lage versetzt, anfallende Kosten, prozessuale Aufwände und Nutzen multikriteriell abzuwägen, um Entscheidungen bezüglich der Auswahl von und Investition in ITS-Maßnahmen(-bündel) fundiert treffen zu können.

Angelehnt an die übergreifenden Ziele des Gesamtvorhabens ProBITS lassen sich die Teilziele für das Teilvorhaben MEBITS wie folgt zusammenfassen:

- Aufbau und Etablierung eines Kompetenzbereichs zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln)
- Identifikation von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen
- Identifikation von praktischen Anforderungen und Anwendungsbarrieren multikriterieller Ansätze zur Bewertung von ITS-Maßnahmen (mit besonderem Fokus auf KMU)
- Identifikation/Analyse von Potentialen und Grenzen traditioneller Verfahren zur Bewertung von ITS-Maßnahmen
- Konzeption eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln), das die zuvor identifizierten Prozesseinflussgrößen und Bewertungsdimensionen berücksichtigt, sowie Bereitstellung von notwendigen Unterstützungsleistungen für die praktische Anwendung und Umsetzung in Form der
  - Erweiterung/Anpassung der Geschäftsprozessmodellierungssprache Business Process Model and Notation 2.0 (BPMN 2.0) und des Standards für eXtensible Event Streams 2.0 (XES 2.0) durch entsprechende Extensions,
  - Integration des multikriteriellen Entscheidungsmodells sowohl in das skalierbare Vorgehensmodell als auch in das IT-Werkzeug und Ableitung zugehöriger technischer und fachlicher Anforderungen sowie
  - Erarbeitung von Umsetzungs- und Anwendungshilfen für das multikriterielle Entscheidungsmodell
- Demonstration und Evaluation der retrospektiven und prospektiven Anwendbarkeit des multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)
- Diffusion und Verstetigung des multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)
- Erzeugung eines adäquaten, an aktuellen Anforderungen ausgerichteten ITS-Bewusstseins und Steigerung der Qualifikation von Unternehmen (insb. KMUs), Mitarbeitenden, Studierenden und Doktoranden im Bereich der Informations- und ITS-Bewertung (im Allgemeinen) und der multikriteriellen Bewertung von ITS-Maßnahmen (im Speziellen)

Betrachtet man den Stand der Forschung und Technik zu Bewertungsverfahren von IT-Sicherheit zum Projektbeginn, so zeigten sich traditionell drei zentrale Richtungen von Ansätzen: (1) Ansätze basierend auf dem Return on Investment (ROI), (2) Ansätze basierend auf der Real Options Theory und (3) Ansätze basierend auf der Utility Maximization Theory. Diese Ansätze wurden im Bereich der Informations- und IT-Sicherheit aus einer investitionstheoretischen Sichtweise betrachtet, wie beispielsweise anhand der Spezifikation des ROI für Sicherheitsmaßnahmen – dem Return on Security Investment (RoSI) – sichtbar wird. Diese Ansätze sind jedoch technologischen Neuerungen, der zunehmenden Vernetzung und Digitalisierung in vielen Lebens- und Arbeitsbereichen und den damit einhergehenden Anforderungen an Datenschutz und Informationssicherheit, nicht mehr gewachsen. Für die Erfüllung derartiger Anforderungen ist zumeist ein komplexes Bündel von ITS-Maßnahmen nötig, das sowohl hohe Investitionskosten mit sich bringt, als auch in einem hohen Grad die Geschäftsprozesse von Unternehmen beeinflusst. Aus dem Bereich des Geschäftsprozessmanagements waren zum Zeitpunkt des Projektbeginns bereits Ansätze bekannt, die sich der Kostenrechnung und Geschäftserfolgsmessung widmen. Diese waren jedoch auf monetäre Werte ausgelegt und nicht spezifiziert für mehrdimensionale Bewertungen einerseits und die Bewertung von ITS-Maßnahmen andererseits.

Summa Summarum fehlt es den traditionellen Verfahren der Wissenschaft und Technik an Mehrdimensionalität, Skalierbarkeit, Prozessorientierung und der Möglichkeit, Wechselwirkungen zwischen Maßnahmenbündeln mit einbeziehen zu können, woraus die Motivation zur Neukonzeption eines adäquaten Bewertungsansatzes entsprang. Das Teilvorhaben MEBITS nutzte den Stand der Forschung als Informationsquelle, knüpfte daran an und erzielte signifikante Fortschritte durch die Entwicklung eines modernen, multikriteriellen und prozessorientierten Entscheidungsmodells zur Bewertung von ITS-Maßnahmen(-bündeln).

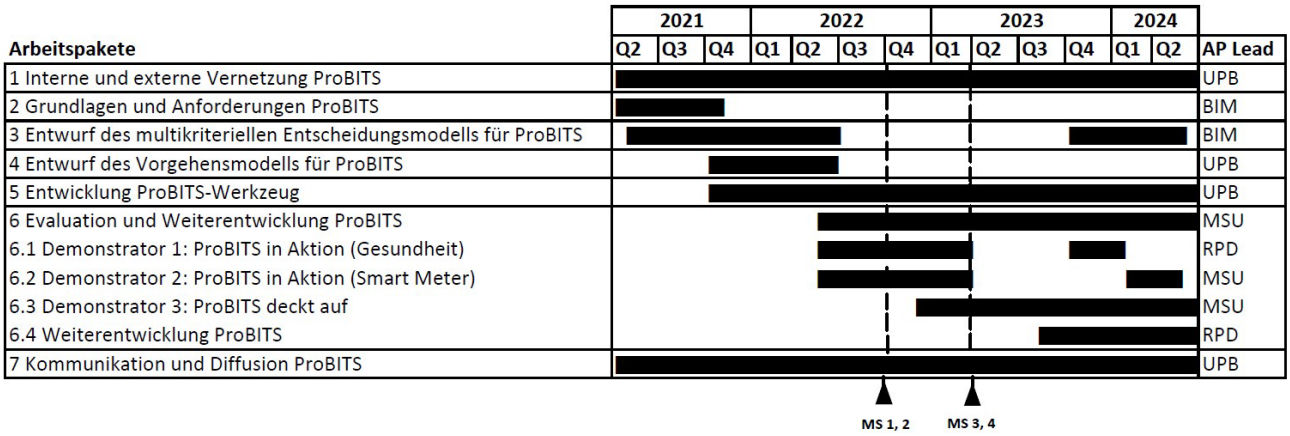
Die Geschäftsprozessorientierung im Zusammenspiel mit ITS-Investitionen stellt dabei einen besonders innovativen Aspekt des Bewertungsansatzes dar. Die aus Geschäftsprozessen abgeleiteten Prozesseinflussgroßen und Bewertungsdimensionen gehen sowohl in Form monetärer als auch nicht-monetärer Faktoren in die Entscheidungsfindung über ITS-Investitionen ein, was aktuellen praktischen Bedürfnissen und Anforderungen entspricht. Zudem wurden im Rahmen des Teilvorhabens (neben dem innovativen, multikriteriellen Ansätzen zur Bewertung von ITS-Maßnahmen) auch traditionelle Verfahren, wie beispielsweise der Return on Security Investment (RoSI), vergleichend untersucht. Ziel dessen war, eine möglichst umfangreiche Sicht auf die ITS-Bewertung zu erlangen und aus den Schwächen und Anwendungshürden traditioneller Verfahren zu lernen.

Die Einbeziehung von Praxispartnern und anderen Stakeholdern war im Teilvorhaben ein ebenso wichtiger Aspekt wie die Berücksichtigung des Standes der Forschung und Technik. Einerseits wurden von den Partnern wichtige Bedürfnisse und kritische fachliche Anforderungen erhoben, die sich aus dem Projektkontext ergaben, anderseits konnten wichtige Einblicke in die gelebte Praxis gewonnen werden (z.B. real eingesetzte Techniken und Entscheidungsverfahren). Dadurch konnte die Überführung der Projektergebnisse in die praktische Anwendung sichergestellt und iterativ verbessert werden.

Die im Teilvorhaben MEBITS entstandenen wissenschaftlichen Publikationen in Tagungsbänden und Fachjournalen trugen nicht nur zur Schließung der identifizierten Forschungslücke bei, sondern dienten auch der Verstetigung und Diffusion der entstandenen Ergebnisse. Auf wissenschaftlichen Fachtagungen wurden neue Diskurse über die ITS-Bewertung initiiert und neue Forschungsrichtungen diskutiert. Darüber hinaus trug und trägt MEBITS durch das errichtete Kompetenzzentrum nachhaltig zur Vernetzung von Forschung und Praxis bei und unterstützt damit den Wissenstransfer im Bereich der Informations- und IT-Sicherheit. Zusammenfassend geben die Resultate des Teilvorhabens MEBITS einen differenzierten und umfangreichen Überblick über die komplexen Bewertungs- und Entscheidungssituationen in der Informations- und IT-Sicherheit und stimulieren den Einsatz des im Projekt neu entwickelten, multikriteriellen, skalierbaren und an Geschäftsprozessen orientierten Entscheidungsmodells in realen Geschäftsszenarien.

2. Ablauf des Vorhabens

Der gesamte Arbeitsplan von ProBITS umfasste 7 Arbeitspakete (AP 1-7). Die Professur für Wirtschaftsinformatik, insb. Betriebliches Informationsmanagement der Martin-Luther-Universität Halle-Wittenberg (MLU) trug die Hauptverantwortung für AP 2 und AP 3, die zugleich den Kern von MEBITS ausmachten.



Tab.1: Überblick über den Projektverlauf anhand der Arbeitspakete

Zu Beginn des ProBITS-Projekts wurde die Vernetzung mit internen und externen Partnern durch den Aufbau eines Kommunikations- und Kompetenzzentrums in AP 1 sichergestellt; im Teilprojekt MEBITS wurde dafür ein Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln) eingerichtet und verstetigt. In AP 2 wurden im Teilprojekt aus systematischen Literaturanalysen und Experteninterviews (1) Prozesseinflussgrößen und Bewertungsdimensionen für ITS-Maßnahmen abgeleitet; über Zielgruppeninterviews wurden anhand von Fallstudien zudem (2) kritische Anforderungen erhoben, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden. (1) und (2) wurden validiert und anschließend katalogisiert/dokumentiert. Zudem wurden in AP 2 traditionelle Verfahren der ITS-Investitionskostenrechnung im Hinblick auf Potentiale und Grenzen konzept-zentrisch ausgewertet. Aufbauend auf den kosten- und nutzenbasierten Bewertungsdimensionen aus AP 2 wurden im Teilprojekt MEBITS in AP 3 zugehörige BPMN- und XES-Erweiterungen entwickelt und praktisch evaluiert. Daran anschließend wurden Kosten- und Nutzenmodelle konstruiert, in ein multikriterielles Entscheidungsmodell zur Bewertung von ITS-Maßnahmen(-bündeln) transformiert und evaluiert. In AP 4 wurde das skalierbare Vorgehensmodell und in AP 5 das IT-Werkzeug entwickelt. In diesem Kontext wurde im Teilprojekt MEBITS eine Ablaufbeschreibung für das multikriterielle Entscheidungsmodell ausgearbeitet sowie zugehörige technische und fachliche Anforderungen katalogisiert. Zudem wurde die Integration sowohl in das Vorgehensmodell als auch in das IT-Werkzeug sichergestellt und anschließend getestet. In AP 6 wurde das implementierte multikriterielle Entscheidungsmodell anhand verschiedener Fallstudien prospektiv, retrospektiv und vergleichend (unter Anwendung der Demonstratoren) erprobt. Die gewonnenen Erkenntnisse wurden zur iterativen Verbesserung verwendet. In AP 7 wurden zur Diffusion im Teilprojekt MEBITS beispielgetriebene Anwendungshilfen für das multikriterielle Entscheidungsmodell entwickelt. Zudem wurden die Resultate der Arbeitspakete in regelmäßigen Ergebnisberichten festgehalten, in Tagungsbänden und Fachjournalen veröffentlicht, in Lehr- und Weiterbildungsmaterialien überführt und auf Fachtagungen und Konferenzen präsentiert und diskutiert.

3. Wesentliche Ergebnisse

Die wesentlichen Ergebnisse lassen sich wie folgt zusammenfassen:

- Etablierter und verstetigter Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln), ausgerichtet auf Zusammenarbeit und Wissensaustausch zwischen den Projektpartnern, assoziierten Partnern und externen Interessierten
- Validierter Katalog von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen
- Validierter Katalog von kritischen fachlichen Anforderungen, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden
- Konzeptmatrix der traditionellen Verfahren zur ITS-Bewertung
- Prozessbasiertes Kosten-/Nutzenmodell zur Bewertung von ITS-Maßnahmen
- Zugehörige validierte BPMN- und XES-Extensions zur Erweiterung/Anpassung bestehender Prozessmodellierungskonventionen
- Evaluiertes, skalierbares, multikriterielles, prozessorientiertes Entscheidungsmodell als Methoden-Artefakt zur Bewertung von ITS-Maßnahmen(-bündeln).
- Ausformulierte Ablaufbeschreibungen und Katalog an fachlichen und technischen Anforderungen für das Entscheidungsmodell zur Implementierung in das IT-Werkzeug und Vorgehensmodell
- Fallstudiengetriebene Testung des multikriteriellen Entscheidungsmodells mit den entwickelten Demonstratoren und Erkenntnisdokumentation der prospektiven, retrospektiven und vergleichenden Anwendung
- Ausformulierte beispielgetriebene Anwendungshilfen für das multikriterielle Entscheidungsmodell
- Lehr- und Weiterbildungsmaterialien zur Informations- und IT-Sicherheitsbewertung (im Allgemeinen) und der multikriteriellen Bewertung von ITS-Maßnahmen (im Speziellen)
- Ergebnisdiffusion durch Publikationen in Tagungsbänden und Fachjournalen sowie Präsentationen auf Fachtagungen und Konferenzen

Bundesministerium
für Bildung
und Forschung

ProBITS

19.12.2024

Multikriterielles Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von IT-Sicherheitsmaßnahmen (MEBITS)

Eingehende Darstellung zum Teilvorhaben im Verbundprojekt
“Prozessorientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen (ProBITS)”

Martin-Luther-Universität Halle-Wittenberg
Lehrstuhl für Wirtschaftsinformatik,
insb. Betriebliches Informationsmanagement

Autorinnen und Autoren:

Dr. Stephan Kühnel
Laura Bauer
Leonard Nake
Prof. Dr. Stefan Sackmann

1. Motivation und Zielstellung des Teilvorhabens

Das Teilvorhaben „Multikriterielles Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von IT-Sicherheitsmaßnahmen“ (MEBITS) zielte als Teil des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Verbundprojekts „Prozessorientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen“ (ProBITS) darauf ab, die vier zentralen ProBITS-Bausteine (1. Erweiterte Prozessmodellierungssprache, 2. Multikriterielles Entscheidungsmodell, 3. Vorgehensmodell und 4. IT-Werkzeug) gemeinsam mit den Verbundpartnern zu entwickeln. Durch die Realisierung der Bausteine wurde im Gesamtprojekt ein innovativer, skalierbarer und werkzeuggestützter Ansatz bereitgestellt, der eine mehrdimensionale, geschäftsprozessorientierte Bewertung von IT-Sicherheitsmaßnahmen (ITS-Maßnahmen) und -Maßnahmenbündeln ermöglicht.
Im Zentrum von MEBITS stand vor allem die Realisation der ersten beiden Bausteine – des multikriteriellen Entscheidungsmodells und der erweiterten Prozessmodellierungssprache –, die es ermöglichen, unter Berücksichtigung verschiedener Prozesseinflussgrößen, kosten- und nutzenorientierter Bewertungsdimensionen sowie praktischer Anforderungen, alternative ITS-Maßnahmen(-bündel) zu analysieren. Entscheider kleinerer, mittlerer und großer Unternehmen wurden und werden damit in die Lage versetzt, anfallende Kosten, prozessuale Aufwände und Nutzen multikriteriell abzuwägen, um Entscheidungen bezüglich der Auswahl von und Investition in ITS-Maßnahmen(-bündel) fundiert treffen zu können.

1.1. Motivation

Technologische Neuerungen wie bspw. Cloud-Computing oder Big-Data-Analytics bieten einerseits erhebliches Potential für den Erhalt und die Stärkung der Wettbewerbsposition. Andererseits birgt die Einführung solcher Technologien neue Risiken, bspw. in Verbindung mit Data-Security, Cloud-Hacking oder Datenschutz. Um solche Risiken beherrschbar zu machen, definieren sowohl der Gesetzgeber als auch die Unternehmen selbst weitreichende und übergreifende Anforderungen an die Informations- und IT-Sicherheit. Beispiele hierfür finden sich sowohl in unternehmenseigenen Vorgaben zur Governance der Informationssicherheit (bspw. allg. Richtlinien zur Authentifizierung oder Vorgaben zur Klassifizierung von und zum Umgang mit Daten und Informationen), in sektorspezifischen Vorschriften (bspw. PSD2 für Banken oder KRITIS für Betreiber von kritischer Infrastruktur), als auch in sektorübergreifenden Gesetzen und Verordnungen (bspw. Datenschutz-Grundverordnung (DSGVO) oder IT-Sicherheitsgesetz) (Kühnel et al. 2021). Diese Anforderungen gilt es im Unternehmenskontext durch adäquate ITS-Maßnahmen umzusetzen.

Die Umsetzung solcher Anforderungen verlangt zumeist ein komplexes Bündel von ITS-Maßnahmen, das sowohl hohe Investitionskosten mit sich bringt, als auch in einem hohen Grad die Geschäftsprozesse von Unternehmen beeinflusst (Kühnel et al. 2021). Es sind sowohl technische Vorkehrungen erforderlich, wie bspw. Verschlüsselung und Pseudonymisierung personenbezogener Daten, als auch prozessuale Konfigurationen, wie bspw. Kontrollen zur Sicherstellung von Compliance oder Konsequenzen für die Verfügbarkeit von Informationen in Prozessschritten. Derartige technische Vorkehrungen und prozessuale Konfigurationen führen zu hohen Aufwänden (Kühnel et al. 2017; Sonnenreich et al. 2006), weshalb die Einhaltung von ITS-Anforderungen als kostenintensive Aufgabe (Sadiq und Governatori 2015; La Rosa 2015) und sogar als “heftiger Kostentreiber” (Becker et al. 2016) bezeichnet wird. Damit die Profitabilität sowohl von kleinen und mittlernen als auch von großen Unternehmen nicht durch den Einsatz von ITS-Maßnahmen(-bündeln) beeinträchtigt wird, gilt es daher, verschiedene Handlungsalternativen zu identifizieren und unter Berücksichtigung von wirtschaftlichen Kriterien die am besten geeignete auszuwählen.

Betrachtet man den Stand der Forschung und Technik zu Bewertungsverfahren von IT-Sicherheit zum Projektbeginn, so zeigten sich traditionell drei zentrale Richtungen von Ansätzen (Schatz und Bashroush 2017): (1) Ansätze basierend auf

dem Return on Investment (ROI), (2) Ansätze basierend auf der Real Options Theory und (3) Ansätze basierend auf der Utility Maximization Theory. Diese Ansätze wurden im Bereich der Informations- und IT-Sicherheit aus einer investitionstheoretischen Sichtweise betrachtet, wie beispielsweise anhand der Spezifikation des ROI für Sicherheitsmaßnahmen – dem Return on Security Investment (RoSI) – sichtbar wird (Sonnenreich et al. 2006). Diese Ansätze sind jedoch technologischen Neuerungen, der zunehmenden Vernetzung und Digitalisierung in vielen Lebens- und Arbeitsbereichen und den damit einhergehenden Anforderungen an Datenschutz und Informationssicherheit, nicht mehr gewachsen. Für die Erfüllung derartiger Anforderungen ist zumeist ein komplexes Bündel von ITS-Maßnahmen nötig, das sowohl hohe Investitionskosten mit sich bringt, als auch in einem hohen Grad die Geschäftsprozesse (und dadurch auch den Geschäftserfolg) von Unternehmen beeinflusst. Aus dem Bereich des Geschäftsprozessmanagements waren zum Zeitpunkt des Projektbeginns bereits Ansätze bekannt, die sich der Kostenrechnung und Geschäftszielmessung widmen (Magnani und Montesi 2007; Sampathkumaran und Wirsing 2013). Diese wurden jedoch zentriert auf monetäre Werte und somit nicht spezifiziert für mehrdimensionale Bewertungen einerseits und die Bewertung von ITS-Maßnahmen andererseits.

Summa Summarum fehlt es den traditionellen Verfahren der Wissenschaft und Technik an Mehrdimensionalität, Skalierbarkeit, Prozessorientierung und der Möglichkeit, Wechselwirkungen zwischen Maßnahmenbündeln mit einbeziehen zu können, woraus die Motivation zur Neukonzeption eines adäquaten Bewertungsansatzes entsprang. In eigenen Vorarbeiten (Kuehnel und Zasada 2018; Kühnel et al. 2019) wurde bereits für Compliance-Maßnahmen vielversprechend gezeigt, dass Prozessfragmente aktivitätsbasiert ökonomisch bewertet und optimiert werden können. Das Teilvorhaben MEBITS nutze den Stand der Forschung und die eigenen Vorarbeiten als Informationsquelle, knüpfte daran an und erzielte signifikante Fortschritte durch die Entwicklung eines modernen, multikriteriellen und prozessorientierten Entscheidungsmodells zur Bewertung von ITS-Maßnahmen(-bündeln).

1.2. Zielstellung

Wie bereits erwähnt, umfasste das Verbundprojekt ProBITS insgesamt vier Bausteine: neben einem multikriteriellen Entscheidungsmodell, mit dem sich ITS-Maßnahmen(-bündel) bewerten und auswählen lassen, waren dies drei Unterstützungsleistungen in Form der Erweiterung einer Prozessmodellierungssprache, eines Vorgehensmodells und eines IT-Werkzeugs.

Wie der Name von MEBITS schon vermuten lässt, bestand das Hauptziel des Teilprojekts in der Entwicklung eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen. Zur Sicherstellung der Prozessorientierung bestand ein zweites wesentliches Ziel darin, die Erweiterung einer Prozessmodellierungssprache zu entwickeln. Darüber hinaus trug MEBITS auch essentiell zu den verbliebenen zwei Bausteinen (Vorgehensmodell und IT-Werkzeug) und damit zum Erreichen aller Gesamtziele von ProBITS bei.

Die konkreten wissenschaftlichen und technischen Arbeitsziele von MEBITS lassen sich wie folgt zusammenfassen:

- Aufbau und Etablierung eines Kompetenzbereichs zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln)
- Identifikation von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen
- Identifikation von praktischen Anforderungen und Anwendungsbarrieren multikriterieller Ansätze zur Bewertung von ITS-Maßnahmen (mit besonderem Fokus auf KMU)
- Identifikation/Analyse von Potentialen und Grenzen traditioneller Verfahren zur Bewertung von ITS-Maßnahmen

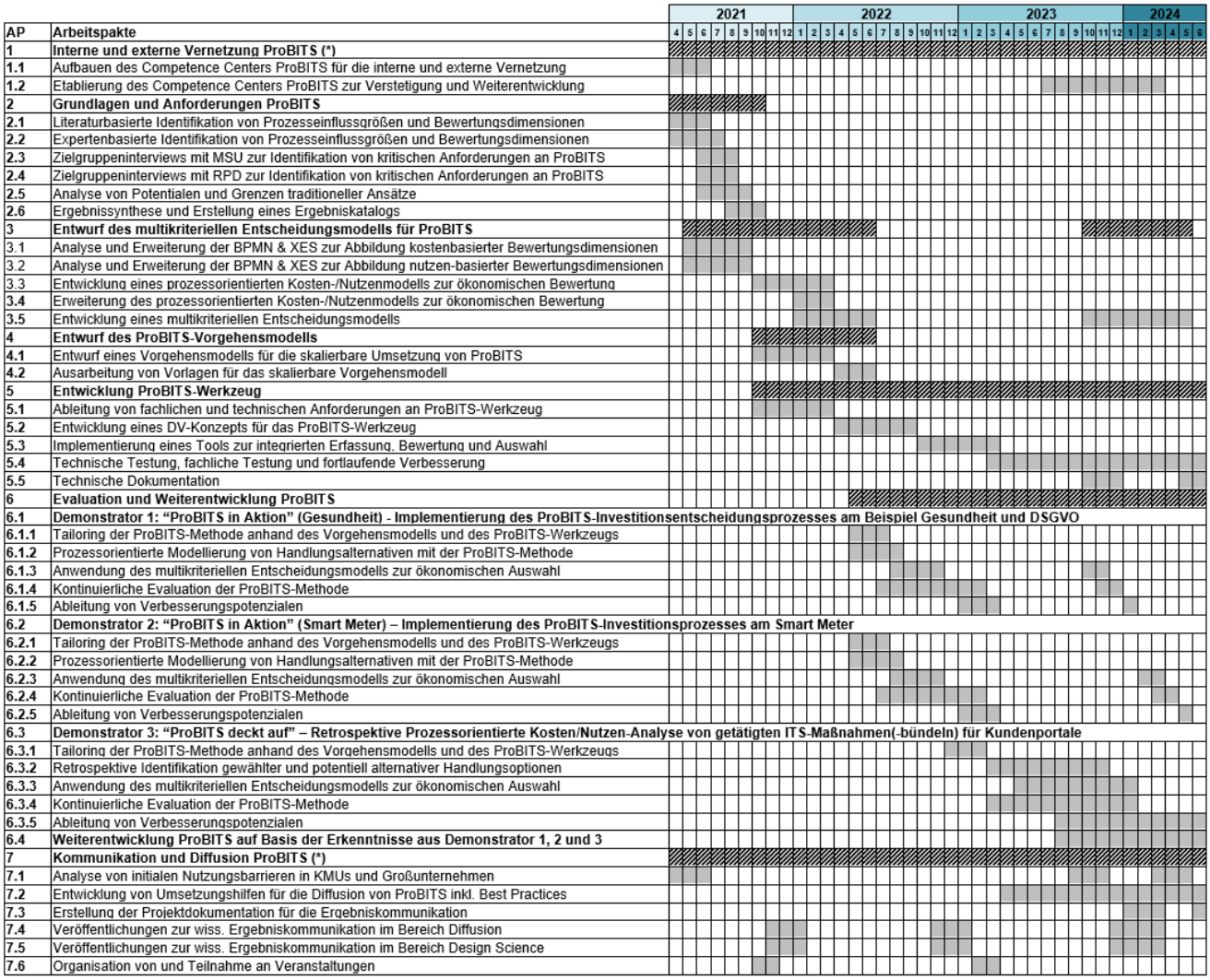
- Konzeption eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln), das die zuvor identifizierten Prozesseinflussgrößen und Bewertungsdimensionen berücksichtigt, sowie Bereitstellung von notwendigen Unterstützungsleistungen für die praktische Anwendung und Umsetzung in Form der
  - Erweiterung/Anpassung der Geschäftsprozessmodellierungssprache Business Process Model and Notation 2.0 (BPMN 2.0) und des Standards für eXtensible Event Streams 2.0 (XES 2.0) durch entsprechende Extensions,
  - Integration des multikriteriellen Entscheidungsmodells sowohl in das skalierbare Vorgehensmodell als auch in das IT-Werkzeug und Ableitung zugehöriger technischer und fachlicher Anforderungen sowie
  - Erarbeitung von Umsetzungs- und Anwendungshilfen für das multikriterielle Entscheidungsmodell
- Demonstration und Evaluation der retrospektiven und prospektiven Anwendbarkeit des multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)
- Diffusion und Verstetigung des multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)
- Erzeugung eines adäquaten, an aktuellen Anforderungen ausgerichteten ITS-Bewusstseins und Steigerung der Qualifikation von Unternehmen (insb. KMUs), Mitarbeitenden, Studierenden und Doktoranden im Bereich der Informations- und ITS-Bewertung (im Allgemeinen) und der multikriteriellen Bewertung von ITS-Maßnahmen (im Speziellen)

2. Ablauf des Vorhabens

2.1. Überblick

Der gesamte Arbeitsplan von ProBITS umfasste sieben Arbeitspakete (AP), die in Abbildung 1 dargestellt sind. Die Professur für Wirtschaftsinformatik, insb. Betriebliches Informationsmanagement der Martin-Luther-Universität Halle-Wittenberg (MLU) trug die Hauptverantwortung für AP 2 und AP 3 sowie die zugehörigen Unterarbeitspakete (UAPs), die zugleich den Kern von MEBITS ausmachten. Zudem war die MLU für UAP 7.5 zuständig. Die Juniorprofessur für Informationssicherheit und Compliance der Georg-August-Universität Göttingen (GAU) war Konsortialführer/Verbundkoordinator und trug die Hauptverantwortung für AP 1, AP 4, AP 5 und AP 7. Während der Projektlaufzeit änderte sich die Konsortialführung/Verbundkoordination durch einen Ruf von JProf. Dr. Trang auf die Professur für Wirtschaftsinformatik, insb. Nachhaltigkeit der Universität Paderborn (UPB). Die msu solutions GmbH (MSU) trug die Hauptverantwortung für AP 6. Darunter war die Rezeptprüfstelle Duderstadt GmbH (RPD) für UAP 6.1 und UAP 6.4 zuständig. Die zugewiesenen Hauptverantwortungen/Zuständigkeiten dienten als organisatorische Richtschnur für das Gesamtvorhaben und reflektieren die konkreten operativen Tätigkeiten und geleisteten Beiträge der Projektpartner in den verschiedenen APs und UAPs nicht in Gänze. Eine detaillierte Beschreibung der operativen Tätigkeiten der übrigen Konsortialpartner ist den jeweiligen Abschlussberichten zu entnehmen.

Im Folgenden werden die Aktivitäten von MEBITS entlang der Arbeitspakete zunächst zusammenfassend dargestellt und auf den erzielten Meilenstein eingegangen. In den Kapiteln 2.2 bis 2.8 erfolgt anschließend eine detailliertere Darstellung der Aktivitäten und Resultate des Teilprojektes von AP 1 bis AP 7.



AP	Arbeitspakte
1	**Interne und externe Vernetzung ProBITS (*)**
1.1	Aufbauen des Competence Centers ProBITS für die interne und externe Vernetzung
1.2	Etablierung des Competence Centers ProBITS zur Verstetigung und Weiterentwicklung
2	**Grundlagen und Anforderungen ProBITS**
2.1	Literaturbasierte Identifikation von Prozesseinflussgrößen und Bewertungsdimensionen
2.2	Expertenbasierte Identifikation von Prozesseinflussgrößen und Bewertungsdimensionen
2.3	Zielgruppeninterviews mit MSU zur Identifikation von kritischen Anforderungen an ProBITS
2.4	Zielgruppeninterviews mit RPD zur Identifikation von kritischen Anforderungen an ProBITS
2.5	Analyse von Potentialen und Grenzen traditioneller Ansätze
2.6	Ergebnissynthese und Erstellung eines Ergebniskatalogs
3	**Entwurf des multikriteriellen Entscheidungsmodells für ProBITS**
3.1	Analyse und Erweiterung der BPMN & XES zur Abbildung kostenbasierter Bewertungsdimensionen
3.2	Analyse und Erweiterung der BPMN & XES zur Abbildung nutzen-basierter Bewertungsdimensionen
3.3	Entwicklung eines prozessorientierten Kosten-/Nutzenmodells zur ökonomischen Bewertung
3.4	Erweiterung des prozessorientierten Kosten-/Nutzenmodells zur ökonomischen Bewertung
3.5	Entwicklung eines multikriteriellen Entscheidungsmodells
4	**Entwurf des ProBITS-Vorgehensmodells**
4.1	Entwurf eines Vorgehensmodells für die skalierbare Umsetzung von ProBITS
4.2	Ausarbeitung von Vorlagen für das skalierbare Vorgehensmodell
5	**Entwicklung ProBITS-Werkzeug**
5.1	Ableitung von fachlichen und technischen Anforderungen an ProBITS-Werkzeug
5.2	Entwicklung eines DV-Konzepts für das ProBITS-Werkzeug
5.3	Implementierung eines Tools zur integrierten Erfassung, Bewertung und Auswahl
5.4	Technische Testung, fachliche Testung und fortlaufende Verbesserung
5.5	Technische Dokumentation
6	**Evaluation und Weiterentwicklung ProBITS**
6.1	**Demonstrator 1: "ProBITS in Aktion" (Gesundheit) - Implementierung des ProBITS-Investitionsentscheidungsprozesses am Beispiel Gesundheit und DSGVO**
6.1.1	Tailoring der ProBITS-Methode anhand des Vorgehensmodells und des ProBITS-Werkzeugs
6.1.2	Prozessorientierte Modellierung von Handlungsalternativen mit der ProBITS-Methode
6.1.3	Anwendung des multikriteriellen Entscheidungsmodells zur ökonomischen Auswahl
6.1.4	Kontinuierliche Evaluation der ProBITS-Methode
6.1.5	Ableitung von Verbesserungspotenzialen
6.2	**Demonstrator 2: "ProBITS in Aktion" (Smart Meter) – Implementierung des ProBITS-Investitionsprozesses am Smart Meter**
6.2.1	Tailoring der ProBITS-Methode anhand des Vorgehensmodells und des ProBITS-Werkzeugs
6.2.2	Prozessorientierte Modellierung von Handlungsalternativen mit der ProBITS-Methode
6.2.3	Anwendung des multikriteriellen Entscheidungsmodells zur ökonomischen Auswahl
6.2.4	Kontinuierliche Evaluation der ProBITS-Methode
6.2.5	Ableitung von Verbesserungspotenzialen
6.3	**Demonstrator 3: "ProBITS deckt auf" – Retrospektive Prozessorientierte Kosten/Nutzen-Analyse von getätigten ITS-Maßnahmen(-bündeln) für Kundenportale**
6.3.1	Tailoring der ProBITS-Methode anhand des Vorgehensmodells und des ProBITS-Werkzeugs
6.3.2	Retrospektive Identifikation gewählter und potentiell alternativer Handlungsoptionen
6.3.3	Anwendung des multikriteriellen Entscheidungsmodells zur ökonomischen Auswahl
6.3.4	Kontinuierliche Evaluation der ProBITS-Methode
6.3.5	Ableitung von Verbesserungspotenzialen
6.4	**Weiterentwicklung ProBITS auf Basis der Erkenntnisse aus Demonstrator 1, 2 und 3**
7	**Kommunikation und Diffusion ProBITS (*)**
7.1	Analyse von initialen Nutzungsbarrieren in KMUs und Großunternehmen
7.2	Entwicklung von Umsetzungshilfen für die Diffusion von ProBITS inkl. Best Practices
7.3	Erstellung der Projektdokumentation für die Ergebniskommunikation
7.4	Veröffentlichungen zur wiss. Ergebniskommunikation im Bereich Diffusion
7.5	Veröffentlichungen zur wiss. Ergebniskommunikation im Bereich Design Science
7.6	Organisation von und Teilnahme an Veranstaltungen

(*) Obwohl für die Arbeitspakete 1 und 7 nur bestimmte Monate veranschlagt wurden, wurde über den gesamten Projektverlauf kontinuierlich daran gearbeitet (siehe graue Schraffur)

Abb 1: Überblick des Projektverlaufs anhand der Arbeitspakete

Zu Beginn des ProBITS-Projekts wurde die Vernetzung mit internen und externen Partnern durch den Aufbau eines Kommunikations- und Kompetenzzentrums in **AP 1** sichergestellt; im Teilprojekt MEBITS wurde dafür ein Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln) eingerichtet und verstetigt. In **AP 2** wurden im Teilprojekt aus systematischen Literaturanalysen und Experteninterviews (1) Prozesseinflussgrößen und Bewertungsdimensionen für ITS-Maßnahmen abgeleitet; über Zielgruppeninterviews wurden anhand von Fallstudien zudem (2) kritische Anforderungen erhoben, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden. (1) und (2) wurden validiert und anschließend katalogisiert/dokumentiert. Zudem wurden in AP 2 traditionelle Verfahren der ITS-Investitionskostenrechnung im Hinblick auf Potentiale und Grenzen konzept-zentrisch ausgewertet. Aufbauend auf den kosten- und nutzenbasierten Bewertungsdimensionen aus AP 2 wurden im Teilprojekt MEBITS in **AP 3** zugehörige BPMN- und XES-Erweiterungen entwickelt und praktisch evaluiert. Daran anschließend wurden Kosten- und Nutzenmodelle konstruiert, in ein multikriterielles Entscheidungsmodell zur Bewertung von ITS-Maßnahmen(-bündeln) transformiert und evaluiert. In **AP 4** wurde das skalierbare Vorgehensmodell und in **AP 5** das IT-Werkzeug entwickelt. In diesem Kontext wurde im Teilprojekt MEBITS eine Ablaufbeschreibung für das multikriterielle Entscheidungsmodell ausgearbeitet sowie zugehörige technische und fachliche Anforderungen katalogisiert. Zudem wurde die Integration sowohl

in das Vorgehensmodell als auch in das IT-Werkzeug sichergestellt und anschließend getestet. In **AP 6** wurde das implementierte multikriterielle Entscheidungsmodell anhand verschiedener Fallstudien prospektiv, retrospektiv und vergleichend (unter Anwendung der Demonstratoren) erprobt. Die gewonnenen Erkenntnisse wurden zur iterativen Verbesserung verwendet. In **AP 7** wurden zur Diffusion im Teilprojekt MEBITS beispielgetriebene Anwendungshilfen für das multikriterielle Entscheidungsmodell entwickelt. Zudem wurden die Resultate der Arbeitspakete in regelmäßigen Ergebnisberichten festgehalten, in Tagungsbänden und Fachjournalen veröffentlicht, in Lehr- und Weiterbildungsmaterialien überführt und auf Fachtagungen und Konferenzen präsentiert und diskutiert.

Insgesamt beinhaltete ProBITS vier **Meilensteine** (MS 1 - MS 4, siehe Abbildung 2), worunter **MS 1** in den Verantwortungsbereich des Teilvorhabens MEBITS fiel. MS 1 lautete wie folgt: *„Das multikriterielle Entscheidungsmodell für ProBITS als Methoden-Artefakt zur wirtschaftlichen Bewertung und Analyse alternativer IT-Sicherheitsmaßnahmen(-bündel) liegt vor und die Evaluation bzw. iterative Verbesserung gemeinsam mit den Praxispartnern hat begonnen."*

Der Meilenstein wurde erreicht. Das multikriterielle Entscheidungsmodell lag planmäßig vor und wurde zum Zeitpunkt der Fälligkeit von MS 1 mit den Praxispartnern MSU und RPD bereits prospektiv angewendet (anhand der Fallstudien „Smart Meter" und „Gesundheit"), initial evaluiert und der Prozess zur iterativen Anpassung angestoßen. Zusätzlich wurde das Modell zu diesem Zeitpunkt bereits im Rahmen einer Fallstudie von dem assoziierten Partner Volkswagen Financial Services AG (VWFS) erfolgreich praxisnah zum Einsatz gebracht. Dabei wurde bei VWFS ein Anwendungsfall für Intrusion Detection Systeme in einem realen Leasing-Prozess identifiziert.

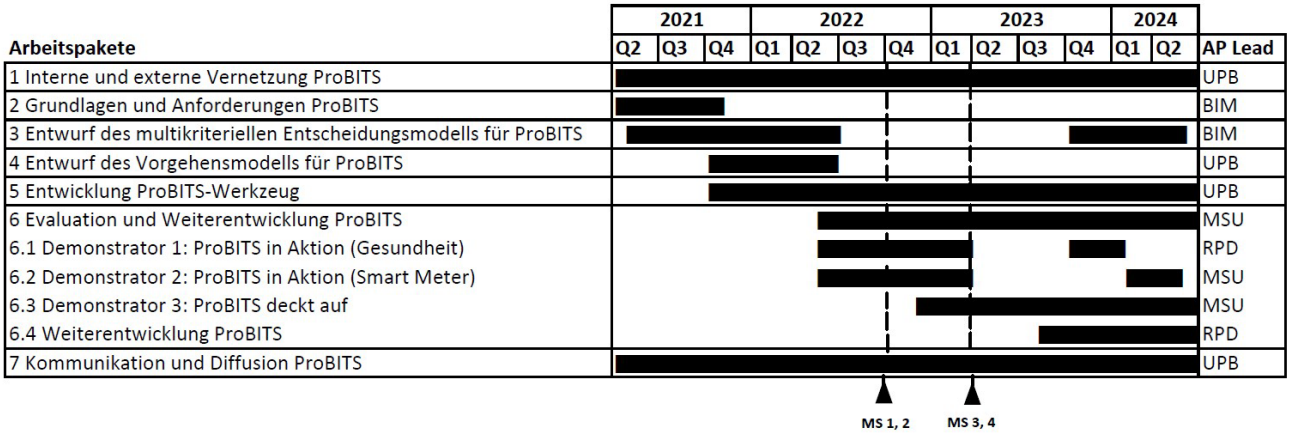


Abb. 2: Übersicht der Meilensteine im Projektplan

Die Meilensteine der anderen Projektpartner – MS 2 von der UPB, MS 3 von der MSU und MS 4 von der RPD – wurden ebenfalls planmäßig erreicht (siehe dafür die Abschlussberichte der jeweiligen Projektpartner).

2.2 AP 1 – Interne und externe Vernetzung ProBITS

Eine zentrale Aufgabe im Rahmen des Gesamtprojekts bestand in der Etablierung und dem Betrieb eines Projektnetzwerks. Dieses war ausgerichtet auf die Förderung der Zusammenarbeit zwischen den Konsortialpartnern einerseits und den assoziierten Partnern andererseits sowie die Etablierung eines strukturierten Kommunikationsprozesses, der regelmäßige Jours Fixes (online) sowie Netzwerktreffen beinhaltete. Das MEBITS-Team berichtete in diesem Rahmen regelmäßig über den Projektfortschritt, erreichte Ziele und mögliche Herausforderungen. Die Zusammenarbeit und Kommunikation zwischen den Konsortialpartnern und assoziierten Partnern verlief reibungslos und war sehr zielorientiert.

Ein wesentlicher Bestandteil der internen und insbesondere auch der externen Vernetzung und Kommunikation war der Aufbau eines Kompetenzzentrums (auch: Competence Center). Im Rahmen des Teilprojekts wurde ein Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln) eingerichtet und verstetigt, der einen kontinuierlichen und strukturierten Austausch über bewertungsbezogene Themen innerhalb des Projektkonsortiums und darüber hinaus ermöglicht (z. B. mit assoziierten Partnern und externen Dritten).

Community Days (summit) bei den Leipziger Softwareforen

Im Mai 2023 fanden die Community Days zu „Governance, Risk und Compliance in der IT" und „IT- Security-Management" der Softwareforen Leipzig statt. Das ProBITS-Team nahm an der Tagung teil und referierte über das Thema: „*IT- Sicherheit: (K)eine Frage des Geldes? Wie Sie Prozesse nutzen können, um wirtschaftliche Entscheidungen zu IT- Sicherheitsmaßnahmen zu treffen*". Der inhaltliche Fokus lag zum einen auf der Vorstellung einer realen Fallstudie, im Rahmen derer das multikriterielle Entscheidungsmodell der ProBITS-Methode bei unserem assoziierten Partner Volkswagen Financial Services AG angewendet wurde, sowie zum anderen auf allgemeinen Adoptionsbarrieren von Bewertungsverfahren für IT-Sicherheitsinvestitionen.

Die Softwareforen vereinen im Rahmen der Community Days (bzw. unter dem neuen Namen „summit") Unternehmen unterschiedlicher Branchen aus dem deutschsprachigen Raum. Dadurch ermöglicht die Tagung den Austausch zu aktuellen Entwicklungen aus dem IT-Bereich über verschiedenste Wirtschaftssektoren hinweg. Während, sowie im Anschluss an den Vortrag, wurde sich lebendig über das Vortragsthema sowie das Projekt ProBITS ausgetauscht. Insgesamt konnte das ProBITS-Team viele neue Erkenntnisse gewinnen, die zur Weiterentwicklung der ProBITS-Methode beitragen.

Aktuelle ProBITS News

Abb. 3: Beispiel eines Berichts aus dem Teilprojekt MEBITS (Auszug aus ProBITS-Newsletter 05 – 2023)

UNIVERSITÄT PADERBORN
Sprache Deutsch · Kontakt · Menü

Anmeldung Newsletter

ProBITS → News

Anmeldung Newsletter

Melden Sie sich jetzt hier zu unserem Newsletter an, um kein Update zu verpassen! (Sie verlassen die Website der Uni Paderborn und gelangen zu einem Formular des Anbieters Brevo).

ProBITS Newsletter 12 – 2023

Der letzte Newsletter des Jahres 2023 wurde an die Mitglieder des Kompetenzzentrums ITSECURITY verschickt.

Newsletter (.pdf) hier herunterladen: ProBITS Newsletter 12 - 2023

ProBITS Newsletter 05 – 2023

ProBITS

Der erste Newsletter des Jahres 2023 wurde an die Mitglieder des Kompetenzzentrums ITSECURITY verschickt.

Newsletter (.pdf) hier herunterladen: ProBITS Newsletter 05 - 2023

Abb. 4.: Newsletter-Anmeldung und -archiv auf der offiziellen ProBITS-Website

Der Kompetenzbereich des Teilprojektes trat regelmäßig aktiv nach außen in Erscheinung. MEBITS war und ist immer noch Teil der „Special Interest Group on Information Security and Privacy" (SIGSEC) der Association for Information Systems (AIS), einer Institution, die auf internationale Netzwerkbildung und globale Wissensdiffusion ausgerichtet ist. Auf zugehörigen Konferenzen der AIS (z. B. Americas' Conference on Information Systems (AMCIS)) und Workshops (z. B. Workshop on Information Security and Privacy (WISP)) wurden Ergebnisse aus dem Teilprojekt präsentiert und mit externen diskutiert. Auch national boten sich regelmäßig Optionen zur Repräsentation des Kompetenzbereichs, z. B. auf der „Nationalen Konferenz der IT-Sicherheitsforschung", den Community Days "Governance, Risk, Compliance in der IT" und "IT-Security-Management" der Leipziger Softwareforen oder dem „International Workshop on Current Information Security and Compliance Issues in Information Systems Research" (CIISR). Letzterer fand jährlich als Teil des Rahmenprogramms

der Internationalen Tagung Wirtschaftsinformatik statt und bot eine Bühne für die Präsentation von Ergebnissen, den gemeinsamen Austausch über projektrelevante Themen und Networking.

Ein weiteres Medium zur Wissensvermittlung aus dem Kompetenzbereich war der regelmäßige Newsletter des ProBITS-Projektes. Darin konnte das MEBITS-Team über aktuelle Resultate, Vorträge und Publikationen berichten (siehe bspw. Abb. 3). Die Anmeldung zum Newsletter und ein Archiv sind über die offizielle ProBITS-Webseite zugänglich (siehe Abb. 4).

Das Team des Teilprojektes fungierte im Competence Center als zentraler Ansprechpartner für Fachfragen rund um MEBITS und zum Thema der prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln). Eine Kontaktaufnahme war und ist immer noch über die E-Mail-Adresse probits@wiwi.uni-halle.de möglich. Über die Webadressen https://probits.uni-paderborn.de/ und https://probits.wiwi.uni-halle.de gelangt man zur offiziellen ProBITS-Website, die an die UPB angegliedert ist (siehe Abb. 5) und zahlreiche Informationen über das Projekt, die Konsortialpartner, Veröffentlichungen usw. bereitstellt.

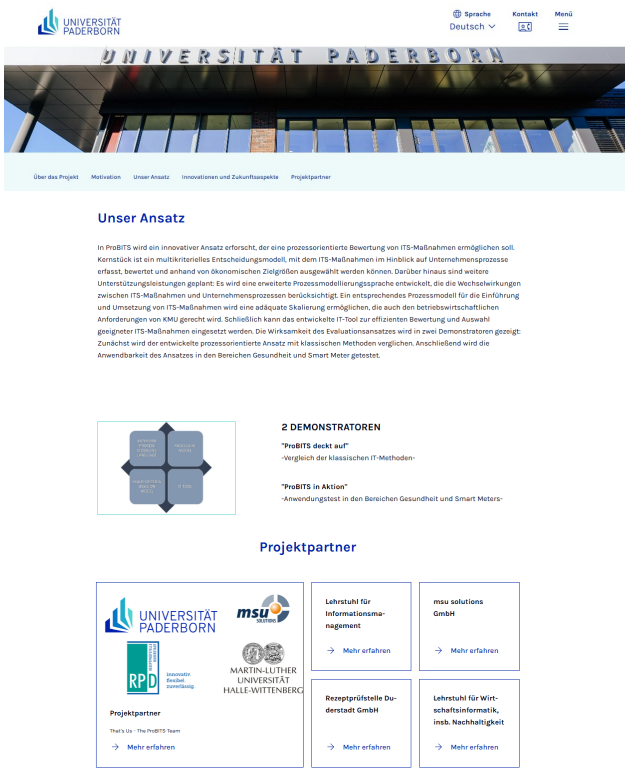


Abb. 5: Offizielle ProBITS-Website, angegliedert an die Universität Paderborn, Stand: 06.12.2024 (Screenshot)

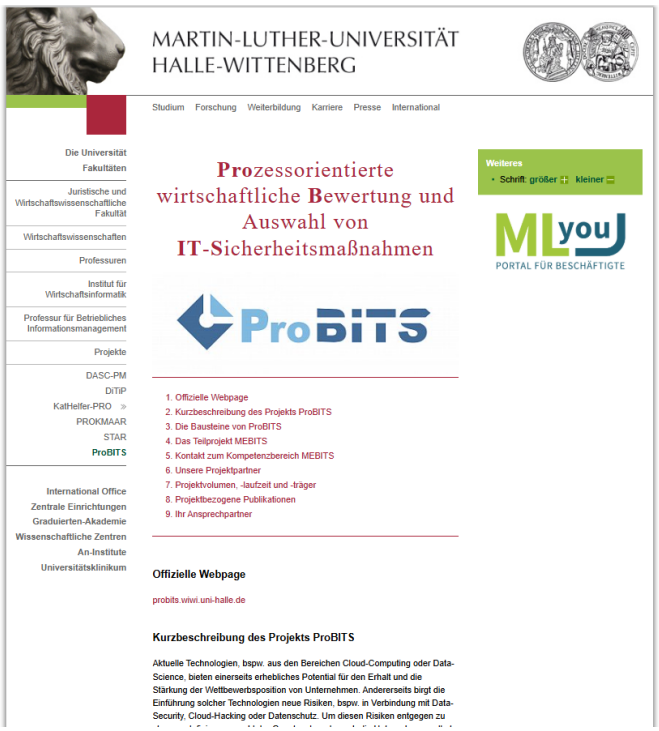


Abb. 6: Website von ProBITS und dem Teilprojekt MEBITS, angegliedert an die Martin-Luther-Universität, Stand: 06.12.2024 (Screenshot)

Auf der Website des Lehrstuhls für Wirtschaftsinformatik, insb. Betriebliches Informationsmanagement ist zudem eine Unterseite für das Projekt ProBITS und das Teilprojekt MEBITS angelegt und projektbegleitend gepflegt worden (https://informationsmanagement.wiwi.uni-halle.de/projekte/probits/, siehe Abb. 6). Darauf sind ebenfalls notwendige Kontaktinformationen zur Erreichbarkeit des Kompetenzbereichs enthalten. Auf weiteren Kanälen des Lehrstuhls (in verschiedenen sozialen Netzwerken, wie bspw. LinkedIn und Instagram) wurde regelmäßig über wichtige Resultate, Veröffentlichungen und Vorträge aus dem Teilprojekt MEBITS berichtet und Ergebnisse geteilt (siehe bspw. Abb. 7, links). Zudem wurde vom MEBITS-Team eine eigene Projektseite auf LinkedIn angelegt (siehe Abb. 7, rechts), um den Zugang zum Competence Center weiter zu

erleichtern (über die Nachrichtenfunktion von LinkedIn) und um ein nachhaltiges Mentioning/Tagging des Projekts in Beiträgen zu ermöglichen.

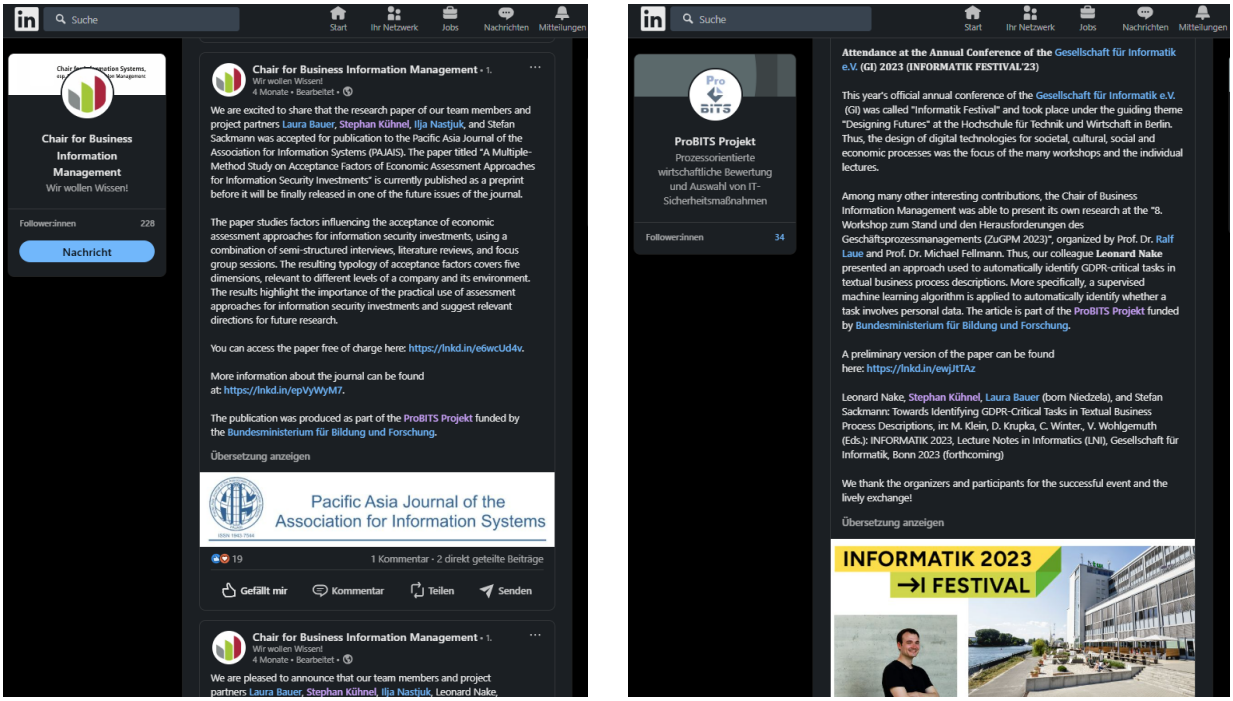


Abb. 7, links: Screenshot eines LinkedIn-Beitrags vom Lehrstuhl für Wirtschaftsinformatik, insb. Betriebliches Informationsmanagement über einen Journal-Artikel, der vom MEBITS-Team veröffentlicht wurde, rechts: Screenshot des vom MEBITS-Team betriebenen LinkedIn-Accounts für das ProBITS-Projekt

Der Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln) hat zudem die Ausarbeitung und Weiterentwicklung von Lehr- und Weiterbildungsmaterialien aktiv stimuliert, wovon sowohl Unternehmen als auch die akademische Lehre profitierten und weiterhin profitieren können.

Insgesamt trugen die einzelnen Maßnahmen maßgeblich zur Etablierung und Verstetigung des Kompetenzbereichs von MEBITS, zu einem schnellen Wissenstransfer und zur reibungslosen Kommunikation bei.

2.3 AP 2 - Grundlagen und Anforderungen ProBITS

Zur Erarbeitung der Grundlagen von ProBITS wurden zunächst drei systematische Literaturanalysen durchgeführt. Die ersten beiden dienten der Identifikation von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen(-bündeln), die dritte zur Identifikation von traditionellen (insb. ROSI-basierten) Ansätzen und Verfahren der Investitionskostenrechnung, die bereits für die Bewertung von ITS-Maßnahmen Verwendung fanden. Die Ergebnisse dieser Analysen wurden jeweils in einer ersten Version katalogisiert bzw. dokumentiert.

Zur Erweiterung, Validierung und Konsolidierung der literaturbasierten Kataloge von Prozesseinflussgrößen und Bewertungsdimensionen wurden 25 Experteninterviews mit Vertretern der assoziierten Partner im Rahmen einer Delphi-Befragung (auch Delphi-Studie) durchgeführt. Bei dieser Befragungsform werden Experten in mehreren Runden befragt und dabei das Ziel verfolgt, deren Einschätzungen zu sammeln und iterativ zu konsolidieren. Die Experten wurden in diesem Zuge zunächst darum gebeten, die Relevanz der in der Literatur identifizierten Prozesseinflussgrößen und Bewertungsdimensionen zu beurteilen und weitere zu benennen, die Ihnen aus der Praxis bekannt sind. Die Ergebnisse daraus wurden über mehrere

Runden sukzessive konsolidiert und erneut katalogisiert sowie zugehörige Arbeitsdefinitionen abgeleitet. Daran anschließend wurden die Dimensionen und Einflussgrößen einander zugeordnet und – auf Wunsch der assoziierten Partner – durch jeweils mehrere spezifische Beispiele ergänzt (siehe auszugsweise Tab. 1). Nach der Durchführung der Delphi-Studie trugen Fokusgruppenworkshops bei der RPD und der MSU zur weiteren Verfeinerung und Validierung der Ergebnisse bei.

Dimension	Definition	Einfuss der IT-Sicherheitsmaßnahme auf Dimension	Spezifische Beispiele
Abstimmungs- und Planungsaufwand	Beschreibt die Koordination und Abstimmung mit verschiedenen Stakeholdern zur Initiierung und/oder Steuerung eines Prozesses.	Abstimmung der IT-Sicherheitsmaßnahmen und Rahmenbedingungen mit externen Dienstleistern und Lieferanten.	Durch die IT-Sicherheitsmaßnahmen muss zum Beispiel vor der Einführung einer Cloud-Plattform erst mit dem Anbieter abgestimmt werden, ob über diese verschlüsselt kommuniziert werden kann.
Datenverfügbarkeit	Beschreibt die Menge und Qualität der Daten, die für die Initiierung bzw. Durchführung des Prozesses notwendig sind.	Einfluss der IT-Sicherheitsmaßnahmen auf die Quantität von prozessrelevanten Daten.	Durch IT-Sicherheitsmaßnahmen, wie zum Beispiel Datenklassifizierung (öffentliche vs. vertrauliche Daten) oder Zugriffskontrollen, kann es sein, dass weniger Daten für den Prozess zur Verfügung stehen.
Dokumentationsaufwand	Beschreibt den zur Anfertigung von Dokumentationen benötigten Aufwand.	IT-Sicherheitsmaßnahmen können den Umfang der Dokumenation (bzgl. der IT-Sicherheitsmaßnahme) bedingen.	IT-Sicherheitsmaßnahmen können implementiert werden, um sicherzustellen, dass prozessrelevante Daten gesichert und im Falle einer Katastrophe oder eines Datenverlusts wiederhergestellt werden können. Diese IT-Sicherheitsmaßnahmen können sich jedoch auf den Umfang der Dokumentation auswirken, da zusätzliche Informationen in die Dokumentation aufgenommen werden müssen, um den Status der Datensicherung und -wiederherstellung wiederzugeben.
Prozessdurchlaufzeit	Beschreibt die Zeit zwischen Prozessbeginn und Prozessende oder einen veränderten Zeitpunkt des Prozessbeginns.	IT-Sicherheitsmaßnahmen können die Dauer von Prozessschritten beeinflussen.	IT-Sicherheitsmaßnahmen wie Multi-Faktor-Authentifizierung und rollenbasierte Zugangskontrollen können sich auf die Dauer von Prozessschritten auswirken, da sie zusätzliche Zeit für Authentifizierungs- und Autorisierungsprüfungen erfordern.
Prozessflexibilität/ -anpassungsfähigkeit	Beschreibt, inwiefern es möglich ist, den Prozess möglichst schnell, einfach und/oder kostengünstig zu verändern.	IT-Sicherheitsmaßnahmen können den Aufwand für Prozessanpassungen beeinflussen.	Durch die Implementierung von IT-Sicherheitsmaßnahmen können technische Abhängigkeiten entstehen und daraus resultierende Wechselkosten, die die Anpassung des Prozesses teurer machen.
Innovationsfähigkeit	Beschreibt die Fähigkeit des Unternehmens oder der Mitarbeiter, innovative Lösungen bzw. Ideen hervorzubringen.	IT-Sicherheitsmaßnahmen können den verfügbaren Funktionsumfang von IT-Systemen beeinflussen.	IT-Sicherheitsmaßnahmen wie Geräteverschlüsselung, Gerätesperrung und Mobile Device Management (MDM) können den verfügbaren Funktionsumfang von IT-Systemen einschränken, indem sie den Zugriff auf und die Sicherung von Daten auf Geräten wie Laptops, Smartphones und Tablets kontrollieren.
IT-Sicherheitsbewusstsein (Awareness)	Beschreibt das Bewusstsein und die Achtsamkeit der Mitarbeiter des Unternehmens gegenüber IT-Sicherheitsbedrohungen, -Sicherheitsmaßnahmen und Konsequenzen.	IT-Sicherheitsmaßnahmen können die Sensibilisierung von Mitarbeiten für Sicherheitsthemen beeinflussen.	IT-Sicherheitsmaßnahmen, die das Primärziel haben, das IT-Sicherheitsbewusstsein zu steigern (z.B. Awareness-Trainings), können zu einer sinkenden Anzahl an erfolgreichen Phishing-Attacken führen. Aber auch IT-Sicherheitsmaßnahmen, die nicht das Primärziel haben, das IT-Sicherheitsbewusstsein zu steigern (z.B. Passwort-Policy oder Spam-Filter), können zu einem gesteigerten IT-Sicherheitsbewusstsein von Mitarbeitern führen und somit zu einer sinkenden Anzahl an erfolgreichen Phishing-Attacken.
Prozesskompatibilität	Beschreibt das Zusammenspiel bzw. Verträglichkeit	IT-Sicherheitsmaßnahmen können die Schnittstellen	IT-Sicherheitsmaßnahmen wie Datenschutzbestimmungen können die Schnittstellen

Tab. 1: Ausschnitt aus dem konsolidierten Katalog von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen(-bündeln)

Zur Identifikation kritischer (praktischer) Anforderungen, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden, wurden im Rahmen von MEBITS Zielgruppeninterviews mit Experten von der MSU und RPD durchgeführt und induktiv ausgewertet (siehe Tabelle 2). Durch die Interviews konnten bereits frühzeitig Informationen über konkrete (fachliche) Erwartungen der Praxispartner an das Modell und über die lokalen Voraussetzungen/Gegebenheiten (bspw. Daten, Systeme, IT) gewonnen werden, welche der späteren reibungslosen Anwendung und Integration des Entscheidungsmodells dienten.

	Kritische Anforderungen an ein multikriterielles Entscheidungsmodell	
Kategorie	**msu Solutions GmbH**	**Rezeptprüfstelle Duderstadt**
Quantifizierung und Bewertung (im Allgemeinen)	Gewichtung der Bewertungsdimensionen durch die Unternehmensführung, wobei ein Ausgleich zwischen kostenorientierten und kunden-/mitarbeiterorientierten Prioritäten geschaffen wird. Ein Administrator kann hier unterstützend tätig werden.	Dimensionen sollten je nach Informationslage bewertet werden können; bei Bedarf können Subdimensionen ausgeblendet werden.
	Qualitative/Non-monetäre Dimensionen sollten nicht abstrakt bleiben, sondern durch konkrete Zahlen gewichtet werden können und quantifizierbar sein.	Subdimensionen können separat bewertet und auf die übergeordnete Dimension aggregiert werden, wobei auf Konsistenz der Bewertung geachtet werden muss.
	Das Modell ermöglicht die Eingabe konkreter Maßnahmen, die Einfluss auf Dimensionen nehmen und darauf basierend erfolgt die Bewertung.	Die Entscheidung zur Bewertung muss individuell getroffen werden.
	Eine Gewichtung der Dimensionen durch Expertenschätzungen ist sinnvoll, besonders bei unklarer Datenlage.	Die Durchführung der Bewertung liegt bei der IT-Abteilung. Die Ergebnisse der Bewertung werden an Experten wie Datenschutzbeauftragte, Geschäftsführung oder Betriebsrat weitergeleitet.
	Bei ITS-Maßnahmen ist die Zeit ein kritischer Faktor; Maßnahmen sollten regelmäßig neu bewertet werden und nicht unbeachtet bleiben. Eine Neubewertung ist notwendig bei externen Einflüssen oder Kontextänderungen (z.B. neue Gesetzeslage).	Iterative Entscheidungsfindung sollte ermöglicht werden, um Gewichtungen und die Auswahl an Maßnahmen und Dimensionen anzupassen. Dabei sind klare Kriterien und Grenzen der Iteration anzuwenden, um Missbrauch zu vermeiden.
Bewertungsdimensionen und KPI	Klärung der Motivation hinter einer Dimension und des Ziels, das mit der Dimension erreicht werden soll; Ziele müssen klar formuliert werden.	Anhand der Anzahl der Bewertungsdimensionen soll die Objektivität der Bewertung gesichert und eine Einseitigkeit der Kriterien vermieden werden.
	Die Bewertung von ITS-Maßnahmen sollte sowohl Kosten (zeitlich und finanziell) als auch Nutzen berücksichtigen. Der Nutzen ist fallabhängig und es müssen die relevanten Dimensionen für die Bewertung bestimmt werden.	Dimensionen sollten auf fachlicher Ebene in der IT-Abteilung festgelegt werden.
	IT-Sicherheitsmaßnahmen beeinflussen und bedingen verschiedene Dimensionen und KPIs.	
	Möglichkeit zur Definition von KPIs bzw. übergeordneten Zielen, wie z.B. der Kundenzufriedenheit, die auf viele Beteiligte im Prozess Einfluss hat.	
	Eine Dimension kann mehreren KPIs zugeordnet werden.	
	Für Rückblickende Analysen: Transparenz darüber, auf welche KPI eine Dimension einzahlt. D.h. Anpassungen einer Dimension haben Auswirkungen auf andere KPIs sowie deren Performance.	
Prozessorientierung	Geschäftsprozesse umfassen viele verschiedene Maßnahmen und Aktivitäten. Eine Maßnahme kann sich auf mehrere Prozesse beziehen; es muss hinterfragt werden, ob sie auch auf weitere Aktivitäten Einfluss hat.	Flexibilität in der Anzahl der Dimensionen, abhängig von der jeweiligen ITS-Maßnahme und dem Geschäftsprozess.
	Klarheit darüber, an welchem Prozessschritt die Bewertung von KPIs oder Zielen erfolgt, insbesondere im Hinblick auf IT-Sicherheit, ohne den Prozess unnötig zu verlängern oder die Kosten zu erhöhen (z.B. im Home-Office-Betrieb).	
Struktur	Ein hierarchisches Modell, das den Entscheidungsprozess abbildet: Ziele stehen oben, Maßnahmen unten.	Eine hierarchische Struktur ist vorteilhaft, um Dimensionen und Gruppen auszuwählen.
		Das Tool sollte verschiedene Rollen bedienen: detaillierte Ansichten für Abteilungen wie IT und eine klar strukturierte, einfach aufbereitete Ergebnispräsentation für die Geschäftsführung.
Systemeinbindung	Kompatibilität der Bewertungsmethode für Energielieferanten/Netzbetreiber mit bestehenden IT-Systemen (z.B. Windows-Authentifizierung und MSU-Systeme).	
	Sicherstellung der Datensicherheit des Endkunden durch einen sicheren Systemzugang, der sich positiv auf das Unternehmensimage auswirkt.	

Tab. 2: Kritische Anforderungen der msu Solutions GmbH und der Rezeptprüfstelle Duderstadt an das multikriterielle Entscheidungsmodell

Zusätzlich wurden im Rahmen von weiteren Fokusgruppenworkshops mit der MSU und RPD geeignete Case Studies bzw. Fallstudien aus der Geschäftspraxis diskutiert und dokumentiert, die für eine spätere Anwendung und Evaluation des multikriteriellen Entscheidungs- und Vorgehensmodells geeignet erschienen. Ein geeignetes Beispiel der MSU aus dem Bereich

der Marktkommunikation war bspw. der „Sperrungs- und Entsperrungsprozess“. Ein Beispiel der RPD war der „Verarbeitungs-/Dateneingangsprozess“. Diese Fallstudien wurden im Laufe des Projekts immer wieder flexibel adaptiert, um wechselnden Umweltbedingungen und dynamischen Anforderungen stets gerecht werden zu können und die praktische Anwendung des Modells abzusichern.

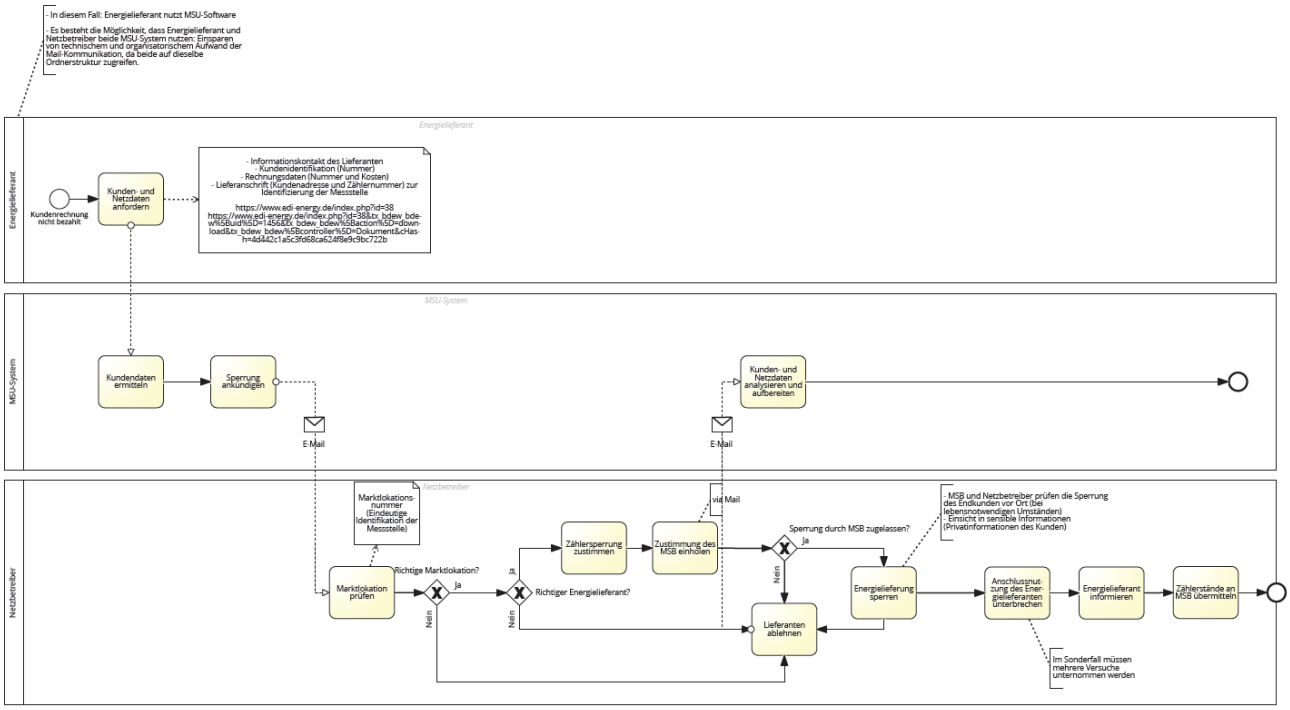


Abb. 8: Sperrungsprozess (Bereich: Marktkommunikation) der msu solutions GmbH

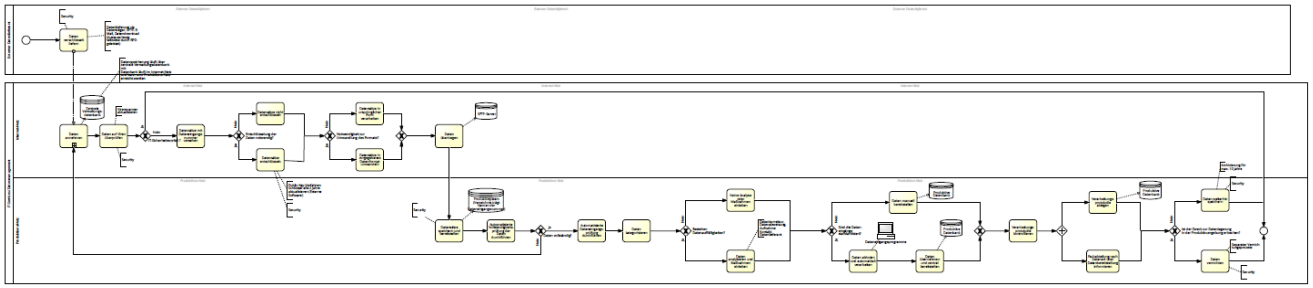


Abb. 9: Verarbeitungs-/Dateneingangsprozess der Rezeptprüfstelle Duderstadt

Die Ergebnisse der eingangs dieses Kapitels erwähnten, dritten systematischen Literaturanalyse (zur Identifikation von traditionellen (insb. ROSI-basierten) Ansätzen und Verfahren der Investitionskostenrechnung), wurden an dieser Stelle wieder aufgegriffen und im Lichte der bisherigen Erkenntnisse aus AP 2 einer tiefgehenden Synthese unterzogen. Ziel war dabei insbesondere, einen strukturierten Überblick über Potentiale und Grenzen dieser Ansätze zur Bewertung prozessorientierter Aufwände und Nutzen zu identifizieren. Dies erfolgte unter Berücksichtigung der kritischen Anforderungen aus den Zielgruppeninterviews mit MSU und RPD.

Die Ergebnisse wurden in einer Konzeptmatrix dokumentiert (siehe auszugsweise Tab. 3), die einen systematischen Überblick über die identifizierten, traditionellen Verfahren und deren spezifische Potentiale und Limitationen im Projektkontext gibt. Zum einen haben die Ergebnisse abermals verdeutlicht, dass die im Vorhaben anvisierten Aspekte der Bewertung

von ITS-Maßnahmen (Mehrdimensionalität und Skalierbarkeit bei gleichzeitiger Prozessorientierung und der Berücksichtigung von Wechselwirkungen zwischen Maßnahmenbündeln) durch keinen Ansatz aus der bestehenden Forschung adressiert werden.

Autoren	Titel	Ansatz/Verfahren	Potentiale	Grenzen
Alireza Shameli-Sendi; Rouzbeh Aghababaei-Barzegar; Mohamed Cheriet	Taxonomy of Information Security Risk Assessment (ISRA)	• Analyse von 125 Fachpublikationen zur Klassifizierung von ISRA-Methoden • Entwicklung einer neuen Taxonomie mit Fokus auf Abstraktionsebenen, Ressourcenbewertung und Angriffspropagation	• Ermöglicht den Vergleich und die Auswahl passender Risikobewertungsverfahren • Liefert einen Überblick über traditionelle und moderne Ansätze • Regt zur Weiterentwicklung des Forschungsfelds an	• Konzeptuell und teils abstrakt – Umsetzung in der Praxis kann herausfordernd sein • Mögliche Lücken bei der Darstellung aktueller Bedrohungsszenarien
Eleni Philippou; Sylvain Frey; Awais Rashid	Contextualising and Aligning Security Metrics and Business Objectives: A GQM-based Methodology	• Ableitung von Sicherheitsmessgrößen mittels eines GQM-basierten (Goal-Question-Metric) Modells • Einsatz systematischer Templates zur Verknüpfung von Geschäfts- und Sicherheitszielen	• Stellt sicher, dass Sicherheitsmetriken an den individuellen Geschäftsprozessen orientiert sind • Ermöglicht eine dynamische Anpassung der Metriken durch Rückkopplungsschleifen • Verbessert die Relevanz von Messgrößen in realen Organisationskontexten	• Beschränkt sich auf die Modellierung der Ziele und Messgrößen – weitere operative Aspekte bleiben unberücksichtigt • Abhängigkeit von korrekter Anwendung der Templates und qualitativer Daten
Alireza Shameli-Sendi	An Efficient Security Data-driven Approach for Implementing Risk Assessment	• Daten- und Geschäftsprozess-basierte Risikoanalyse • Einbeziehung des Sicherheitsdaten-Lebenszyklus und hierarchischer Pyramiden zur Priorisierung von Sicherheitsbedürfnissen • Verbesserung klassischer Verfahren (z. B. CVSS, OWASP) durch Integration von Sicherheitsdaten	• Präzisere Risikobewertung durch Verknüpfung mit den Kernprozessen • Berücksichtigt den dynamischen Charakter von Sicherheitsdaten • Ermöglicht eine differenzierte Betrachtung von Risiken entlang des Datenlebenszyklus	• Erfordert detaillierte Modellierung und umfassende Erfassung von Geschäftsprozessen • Komplexität bei der praktischen Umsetzung und Datenextraktion
Ram Kumar; Sungjune Park; Chandrasekar Subramaniam; Tae-Sung Kim	A Framework for Assessing IT Security Investment Portfolios	• Entwicklung eines Bewertungsrahmens, der auf Finanzmodellen zur Asset-Bewertung basiert • Simulation verschiedener Bedrohungsszenarien unter Berücksichtigung von Angriffsfrequenz, Schadenspotenzial und Wiederherstellungszeiten	• Ermöglicht die quantitative Bewertung von Sicherheitsinvestitionen • Unterstützt Entscheidungen bei Portfolio-Investitionen in unterschiedliche Technologien • Liefert handlungsorientierte Empfehlungen für Kosten-Nutzen-Analysen	• Modellannahmen und Simulationsparameter sind komplex und datenintensiv • Ergebnisse sind stark abhängig von der Genauigkeit der Eingangsdaten und Marktbedingungen
Huseyin Cavusoglu; Birendra Mishra; Srinivasan Raghunathan	Assessing the Value of Detective Control in IT Security	• Einsatz eines spieltheoretischen Modells zur Bewertung des Wertes von Intrusion Detection Systemen (IDS) • Vergleich von organisatorischen Payoffs mit und ohne Einsatz von IDS, inklusive Deterrenzeffekten	• Verdeutlicht den doppelten Nutzen (Erkennung und Abschreckung) von Detektionsmaßnahmen • Bietet wirtschaftliche Entscheidungsunterstützung für den Einsatz von IDS • Trägt zur Priorisierung von Sicherheitskontrollen im Gesamtarchitekturkonzept bei	• Vereinfachende Annahmen des spieltheoretischen Modells können reale Komplexitäten nicht vollständig abbilden • Modellparameter sind teils schwer exakt zu quantifizieren und erfordern empirische Validierung
Piya Shedden; Atif Ahmad; Wally Smith; Heidi Tscherning; Rens Scheepers	Asset Identification in Information Security Risk Assessment: A Business Practice Approach	• Einführung des „Rich Description Method" (RDM) zur Identifikation von Informations- und Wissens-Assets • Betrachtung formaler und informeller Aspekte von Geschäftsprozessen zur Erfassung kritischer Daten	• Erhöht die Granularität und Reichweite bei der Identifikation von Assets • Schließt auch schwer quantifizierbare, wissensbasierte Assets ein • Verbessert die Genauigkeit der Risikoabschätzung durch detailliertere Asset-Erfassung	• Erfordert intensiven qualitativen Analyseaufwand und Fallstudien • Mögliche Herausforderungen bei der Standardisierung und Übertragbarkeit der Methode auf andere Organisationen
Wei Qu; De-Zheng Zhang	Security Metrics Models and Application with SVM in Information Security Management	• Entwicklung von quantitativen Sicherheitsmetriken unterstützt durch Machine-Learning-Methoden (SVM – Support Vector Machine) • Modellierung der Sicherheitslage mittels numerischer Bewertung und statistischer Analysen	• Liefert objektive, datenbasierte Beurteilungen der Sicherheitslage • Ermöglicht automatisierte und skalierbare Sicherheitsbewertung • Unterstützt die Identifikation von Mustern und Schwachstellen	• Abhängigkeit von der Verfügbarkeit und Qualität der Daten • Komplexität im Aufbau und der Kalibrierung von SVM-Modellen • Potenzial für Fehlalarme oder Überanpassung bei geringem Datensatzumfang
Jan vom Brocke; Christian Buddendick;	Return on Security	• Anwendung kapitalbudgetierungstheoretischer	• Ermöglicht langfristige, ökonomische Bewertung von	• Hoher Modellierungsaufwand und Komplexität in der praktischen

Tab. 3: Ausschnitt der Konzeptmatrix zu Potentialen und Grenzen traditioneller Ansätze der Investitionskostenrechnung

Zum anderen hat sich gezeigt, dass die zuvor erhobenen kritischen Anforderungen von den bestehenden Ansätzen nicht in Gänze abgedeckt werden können. Nichtsdestotrotz bieten die Ergebnisse einen umfassenden Überblick über die vorhandenen Bewertungsmethoden und dienten als Informationsquelle und Inspiration für die Entwicklung eines modernen, multikriteriellen und prozessorientierten Entscheidungsmodells zur Bewertung von ITS-Maßnahmen(-bündeln).

Am Ende des Arbeitspakets wurden die Ergebnisse gemeinsam mit der UPB, MSU und RPD nochmals diskutiert, synthetisiert und ein finaler Ergebniskatalog erstellt. Dieser bietet einen detaillierten Überblick über Bewertungsdimensionen und Prozesseinflussgrößen von ITS-Maßnahmen(-bündeln) sowie kritische fachliche Anforderungen an ein multikriterielles Entscheidungsmodell. Der Katalog bildet die Grundlage für den Entwurf, die Entwicklung und die Anwendung eines fundierten multikriteriellen Entscheidungsmodells für ProBITS

2.4 AP 3 - Entwurf des multikriteriellen Entscheidungsmodells für ProBITS

Arbeitspaket 3 beinhaltete zwei zentrale Aufgaben: (1) die Konzeption eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln), das die zuvor identifizierten Prozesseinflussgrößen und Bewertungsdimensionen berücksichtigt, (2) die Bereitstellung von notwendigen Unterstützungsleistungen für die praktische Anwendung und Umsetzung in Form der Erweiterung bzw. Anpassung der Geschäftsprozessmodellierungssprache Business Process Model and Notation 2.0 (BPMN 2.0) und des Standards für eXtensible Event Streams 2.0 (XES 2.0) durch entsprechende Extensions.
Dem Ablaufplan folgend wurde mit (2) gestartet. Da es bereits eine Fülle von bestehenden BPMN-Erweiterungen (sog. Extensions) gab, wurde zunächst eine strukturierte Literatursuche durchgeführt. So konnten bereits existierende Erweiterungen, die Aspekte der IT-Sicherheit in Geschäftsprozessmodelle integrieren, identifiziert werden. Tabelle 4 zeigt die Ergebnisse dieser Literaturanalyse, aufbereitet als Taxonomie. In dieser werden die identifizierten BPMN-Extensions in Abhängigkeit von fünf IT-Sicherheits- und Funktionalitätskategorien klassifiziert (für nähere Informationen zur Taxonomie, siehe Nake (2023)). Aufbauend darauf zeigte sich, dass zwar durch die Verwendung bestehender Erweiterungen einzelne ITS-Aspekte in BPMN Modelle integriert werden können, jedoch nicht alle der in AP 2 identifizierten Bewertungsdimensionen und Einflussgrößen, auf denen das multikriterielle Entscheidungsmodell aufbaut.

Category	Characteristics		
Risk Assessment	*Reliability (5)*	*Risk Objective (5)*	*Risk Information (5)*
	Vulnerabilities (4)	*Asset Value (5)*	*None (12)*
Task Execution Rules	*Separation of Duty (5)*	*Binding of Duty (5)*	
	Non-delegation (3)	*None (13)*	
Security Goal	*Accountability (8)*	*Auditability (6)*	*Authenticity (10)*
	Confidentiality (10)	*Integrity (11)*	*Availability (11)*
	Non-repudiation (7)	*Privacy (8)*	*None (5)*
Domain Specificity	*Domain Specific (3)*	*Generic (15)*	
Extended BPMN Element	*Activity (18)*	*Event (4)*	*Gateway (3)*
	Pool (6)	*Message Flow (7)*	*Data Object (12)*
	Process (2)	*Subprocess (2)*	*Other (6)*

Legende: (#) = Anzahl der gefundenen BPMN-Erweiterungen, die den jeweiligen Aspekt abbilden

Tab. 4: Taxonomie der BPMN-Erweiterungen zur Integration von Aspekten der IT-Sicherheit in Geschäftsprozesse

Demnach mussten BPMN-Elemente und -Attribute für jede Bewertungsdimension des Ergebniskatalogs aus AP2 in einer neuen BPMN-Extension definiert werden. Diese Extension ermöglicht die Integration und Speicherung von kosten- und nutzenbasierten Bewertungsdimensionen aus dem Bereich IT-Sicherheit und unterstützt dadurch die Anwendung des multikriteriellen Entscheidungsmodells auf Basis von Soll- und Ist-Prozessmodellen. Die Bewertungsdimensionen wurden dafür anhand ihres Gültigkeitsbereichs in drei Ebenen aufgeteilt (Unternehmensebene, Mitarbeiterebene, Prozessebene). Die erstellte BPMN-Erweiterung wurde standardmäßig als XSD-Datei angelegt. Zur besseren Darstellbarkeit wurde zusätzlich ein BPMN+X-Modell nach Stroppi et al. (2011) entwickelt (siehe Abbildung 10), um die Struktur der Erweiterung darzustellen, also die drei Ebenen sowie die dazugehörigen Dimensionen.

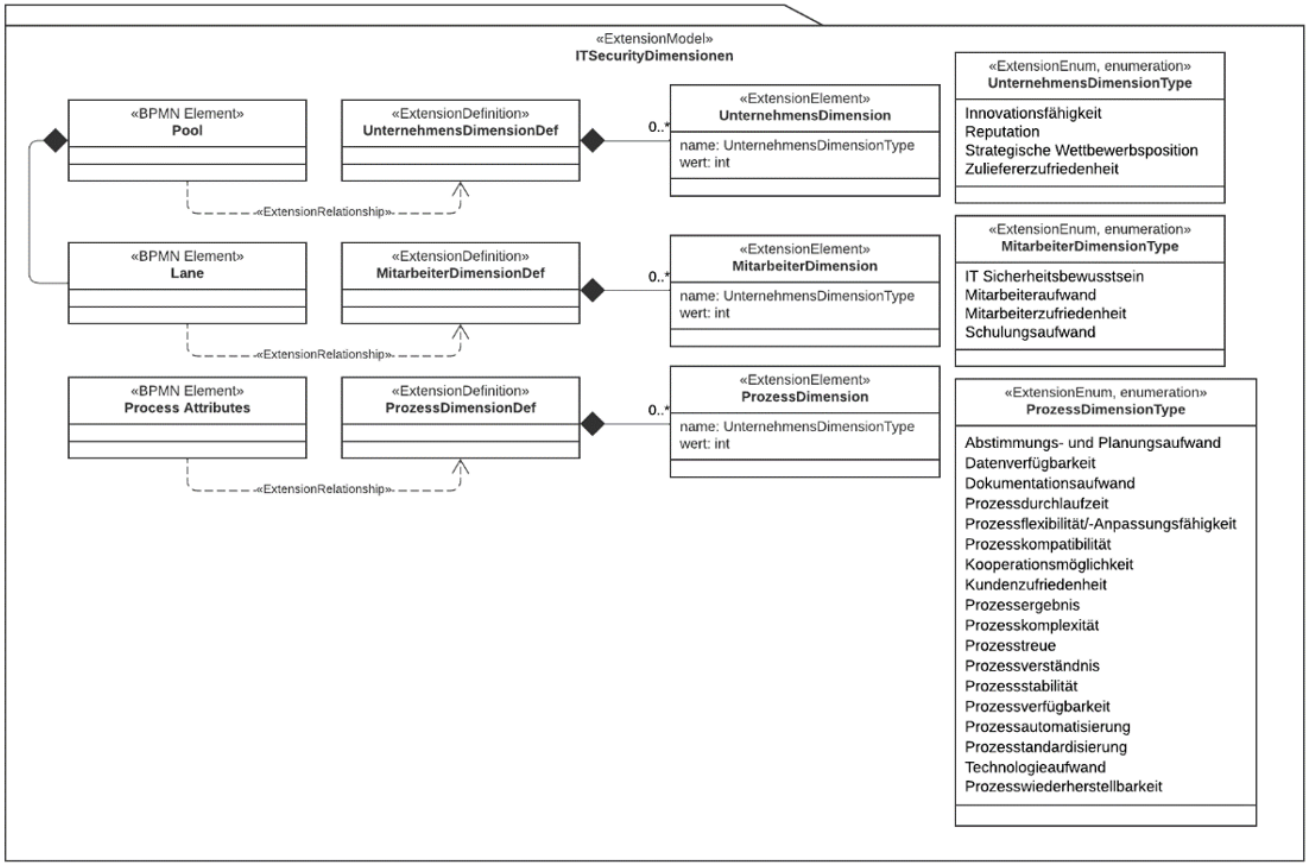


Abb. 10: BPMN+X-Modell der ProBITS-Erweiterung

Analog wurde eine XES-Erweiterung entwickelt, die die verschiedenen Bewertungsdimensionen in Protokolldateien abbilden und speichern kann. XES 2.0 ist ein Standard für Logfiles, der von der IEEE Task Force on Process Mining herausgegeben wurde. Er definiert ein allgemein anerkanntes Format für den Austausch von Protokolldaten zwischen Informationssystemen sowie für die Bereitstellung von Daten für Analysewerkzeuge (Günther und Verbeek 2014) und stellt damit eine Grundlage für die Anwendung von Process-Mining-Verfahren dar. Die Anwendung solcher Verfahren bietet für die Praxis den Vorteil, dass automatisch Prozessmodelle aus Protokolldateien rekonstruiert werden können, auch wenn noch keine modellierten Geschäftsprozesse im Unternehmen vorliegen (Kuehnel et al. 2022). Da es auf der Website des XES-Standards (https://www.xes-standard.org/) eine Auflistung der verfügbaren Erweiterungen gibt, war hierfür keine zusätzliche Literaturanalyse notwendig. Analog zu BPMN zeigte sich auch für die XES-Erweiterungen, dass bereits einzelne projektrelevante Aspekte abgebildet werden konnten (bspw. Prozessdurchlaufzeit durch die Time-Extension oder Kosten für ITS-Maßnahmen

durch die Cost-Extension), jedoch nicht alle der in AP2 identifizierten Bewertungsdimensionen und Einflussgrößen, auf denen das multikriterielle Entscheidungsmodell aufbaut. Die XES-Erweiterung, die erforderliche Elemente und Attribute für jede Bewertungsdimension des Ergebniskatalogs aus AP 2 enthält, wurde standardmäßig als XESEXT-Datei angelegt (basierend auf der Extensible Markup Language).

Die Erweiterungen wurden zuerst anhand synthetischer Daten und danach anhand der Case Studies aus UAP 2.3 und UAP 2.4 getestet und formativ zwischenevaluiert. Für das Testen der XES-Erweiterung musste ein spezifischer Demonstrator entwickelt werden, der in Abbildung 11 als Komponentendiagramm und in Abbildung 12 (a) und (b) in Form von Screenshots einer R-Applikation dargestellt ist.

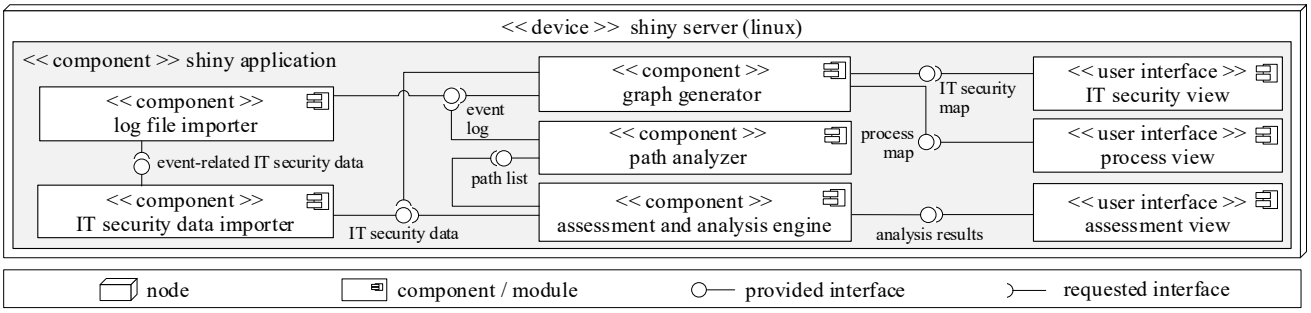
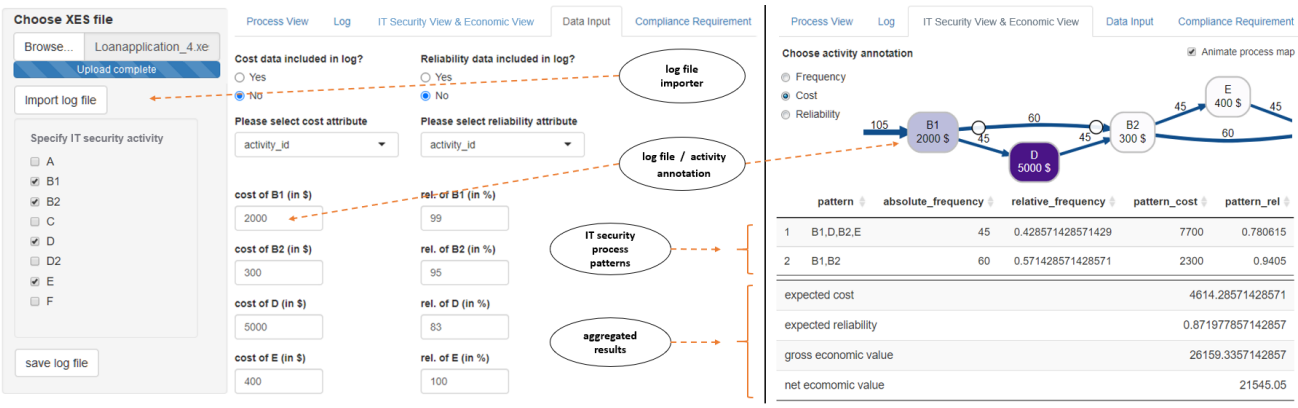


Abb. 11: Komponentendiagramm des Demonstrators für den Test der XES-Erweiterung



(a) Screenshot des "log file importers" und des "IT security data importers"

(b) Screenshot des dimensionserweiterten Prozesses und der Bewertungsergebnisse

Abb. 12: Benutzeroberfläche des Demonstrators für den Test der XES-Erweiterung

Als Feedback aus der Zwischenevaluation ergaben sich zwei zentrale Ergebnisse. Zum einen wurde festgestellt, dass nicht alle Bewertungsdimensionen auf dem gleichen Abstraktionslevel angesiedelt sind. Ein Teil der Dimensionen ist direkt anhand der Geschäftsprozesspfade verrechenbar, bspw. immer dann, wenn die enthaltenen ITS-Maßnahmen(-bündel) als Tasks oder Subprozesse repräsentiert bzw. modelliert sind (niedriges Abstraktionslevel). Dies ist z. B. bei Kosten, Zuverlässigkeiten oder Durchlaufzeiten von ITS-Maßnahmen der Fall, die als Aktivitäten in Prozessen enthalten sind und entsprechend spezifiziert werden können. Andere Dimensionen, wie bspw. die Prozesswiederherstellbarkeit (nach einem IT-Sicherheitsvorfall) oder die Kundenzufriedenheit (die sich durch eine Datenschutzmaßnahme erhöhen kann), beziehen sich auf den Geschäftsprozess als Ganzes bzw. die Unternehmensebene (hohes Abstraktionslevel). Daraus folgte die Erkenntnis, dass man die Bewertungsdimensionen immer im Zusammenspiel mit den zu implementierenden ITS-Maßnahmen(-bündeln) analysieren und je nach Anwendungsfall spezifizieren muss. Unternehmen müssen definieren, welche Dimensionen für die Bewertung relevant sind und welche alternativen ITS-Maßnahmen zur Verfügung stehen bzw. in Frage kommen.

Zum anderen wurde die Frage aufgeworfen, ob sich unabhängig von den BPMN- und XES-Extensions auch stärker softwarespezifische Lösungen zur Abbildung der Bewertungsdimensionen und zugehöriger Prozesseinflussgrößen umsetzen lassen. Hierbei zielte die MSU konkret auf eine Implementierung in der Software Signavio ab. Um dem nachzukommen, wurden die Dimensionen als Attribute in Signavio angelegt. Im Vergleich zur Nutzung der beiden Erweiterungen ist die Verwendung der Signavio-internen Attribute unkomplizierter, jedoch nur, wenn der Benutzer diese Software besitzt. Falls den Prozessmodellen ein oder mehrere Attribute der Bewertungsdimensionen zugewiesen sind, werden diese als Icons dargestellt (siehe Abbildung 13, oben links). Durch die zusätzliche Definition der Dimensionen als Attribute am Beispiel von Signavio wurde die softwarespezifische Anwendbarkeit des Ansatzes gezeigt und gleichzeitig die Zugänglichkeit weiter erhöht. Demgegenüber sind die Erweiterungen von BPMN und XES softwareübergreifend und demnach universell nutzbar.

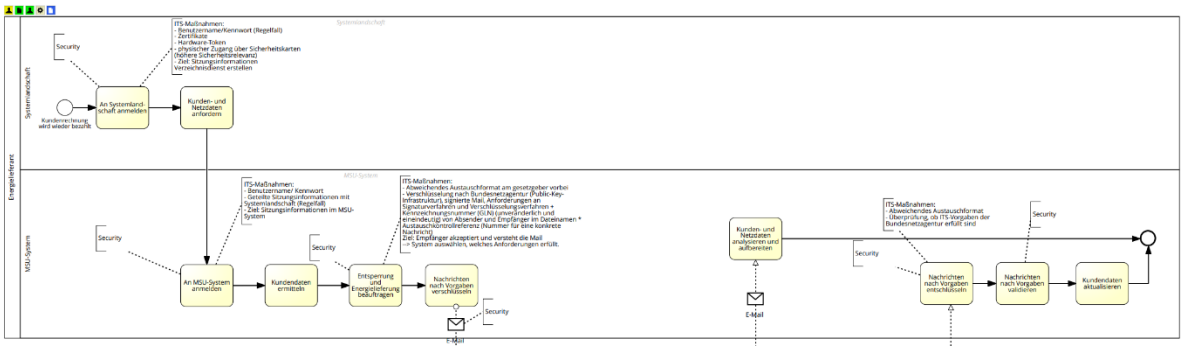


Abb. 13: Darstellung der definierten Attribute in Signavio am Beispiel eines Prozesses der msu solutions GmbH

Die gewonnenen Erkenntnisse, Fortschritte und Anpassungen der formativen Zwischenevaluation der BPMN- und XES-Erweiterungen wurden in einem Bericht dokumentiert. Anschließend wurden Kosten-/Nutzenmodelle zur wirtschaftlichen Bewertung von ITS-Maßnahmen entwickelt. Dazu gehörte die Definition erforderlicher prozessorientierter Bewertungsgrößen bzw. Variablen für alle Bewertungsdimensionen aus AP 2. Das war für quantitative Bewertungsdimensionen, wie bspw. Durchlaufzeiten von ITS-Aktivitäten (in Sekunden, Minuten und Stunden) oder monetäre Aufwände zur Einrichtung und zum Betrieb von ITS-Maßnahmen (in Euro und Cent) problemlos möglich. Für stärker qualitative Bewertungsdimensionen, wie bspw. die Auswirkung von ITS-Maßnahmen auf Prozessflexibilität oder -stabilität, wurden jeweils ordinale Bewertungsskalen zur Kosten- und Nutzenbewertung herangezogen. Für die Entwicklung von aggregierten Kosten- und Nutzenfunktionen (über alle Bewertungsdimensionen hinweg) musste darauf geachtet werden, dass Einheiten und Skalierung gleichartig sind, weil andernfalls keine sinnvolle Verrechnung möglich gewesen wäre. Ein Großteil der Bewertungsdimensionen musste zu diesem Zweck auf ein niedrigeres Skalenniveau transformiert werden.

Für erste Tests der Modelle orientierten wir uns an der Arbeit von Chen et al. (2013). Die Autoren nutzen eine ordinalskalierte linguistische Skala in Kombination mit Fuzzy-Zahlen (von 0 – sehr gering bis 100 – sehr hoch) jeweils für die Kosten- und die Nutzendimensionen einer ITS-Maßnahme. Die Einschätzung der Dimensionen je Sicherheitsmaßnahme erfolgte durch mehrere Probanden (Experten), wobei für die Berechnung jeder Dimension (über alle Experten hinweg) das geometrische Mittel von Chen et al. (2013) vorgeschlagen wurde. Unserer Berechnung lagen zwei Annahmen zu Grunde: 1. Alle ITS-Maßnahmen sollten im Kosten- und Nutzenmodell gleichermaßen auf das IT-Sicherheitsniveau eines Geschäftsprozesses einzahlen; 2. Die Bewertungsdimensionen gehen gleichgewichtet und nicht hierarchisch in die Bewertung ein. Das Kosten-/Nutzenmodell und die Aggregationsfunktionen wurden am Beispiel der Case Studies aus UAP 2.3 und UAP 2.4 getestet und formativ zwischenevaluiert (siehe beispielhaft Tabelle 5), um deren Anwendbarkeit zu erproben, Herausforderungen zu identifizieren und Erkenntnisse für die Weiterentwicklung zu gewinnen.

Hr. Powering Nutzen	1.Prozesskomplexität	2.Mitarbeiteraufwand	3.Prozessflexibilität/Anpassungsfähigkeit	4.Stabilität/verfügbarkeit	5.Technologieaufwand	6.Abstimmungs- und Planungsaufwand
Zwischen Netzwerken geschalteter PTP-Server	50	25	25	25	0	25
Direktes Kopieren durch Freigabe	75	25	25	75	25	50
Physischer Datenträger	25	0	0	75	75	0

Linguistic Scale	Number
Very High	100
High	75
Medium	50
Low	25
very Low	0

Hr. Bachmann Nutzen	1.Prozesskomplexität	2.Mitarbeiteraufwand	3.Prozessflexibilität/Anpassungsfähigkeit	4.Stabilität/verfügbarkeit	5.Technologieaufwand	6.Abstimmungs- und Planungsaufwand
Zwischen Netzwerken geschalteter PTP-Server	75	25	50	75	75	75
Direktes Kopieren durch Freigabe	100	50	50	75	75	100
Physischer Datenträger	25	0	0	0	0	0

Hr. Powering Kosten	1.Prozesskomplexität	2.Mitarbeiteraufwand	3.Prozessflexibilität/Anpassungsfähigkeit	4.Stabilität/verfügbarkeit	5.Technologieaufwand	6.Abstimmungs- und Planungsaufwand
Zwischen Netzwerken geschalteter PTP-Server	50	25	50	50	50	50
Direktes Kopieren durch Freigabe	50	25	50	25	75	75
Physischer Datenträger	25	75	25	0	25	25

Hr. Bachmann Kosten	1.Prozesskomplexität	2.Mitarbeiteraufwand	3.Prozessflexibilität/Anpassungsfähigkeit	4.Stabilität/verfügbarkeit	5.Technologieaufwand	6.Abstimmungs- und Planungsaufwand
Zwischen Netzwerken geschalteter PTP-Server	50	25	50	50	50	50
Direktes Kopieren durch Freigabe	25	25	50	25	25	25
Physischer Datenträger	0	100	75	0	25	75

Tab. 5: Auszug der Bewertung von IT-Sicherheitsmaßnahmen mithilfe des Kosten-/Nutzenmodells bei der RPD

Aus der Anwendung der Modelle und Zwischenevaluationen bei den Projektpartnern gingen nach induktiver Auswertung zahlreiche Erkenntnisse hervor (siehe Tabelle 6). Diese wurden in 3 Kategorien eingeteilt: 1. Kosten- und Nutzenbewertung, 2. Hilfestellung und Transparenz und 3. Kenntnis/Expertise der Bewertenden. Während die Inhalte der Kategorien 2 und 3 eher für den Entwurf des Vorgehensmodells (AP 4) und die Entwicklung von Umsetzungs- und Anwendungshilfen (UAP 7.2) wichtig waren und in den entsprechenden Arbeitspaketen auch genutzt wurden, waren die Inhalte der Kategorie 1 konkret auf das Kosten-/Nutzenmodell bezogen. So zeigte sich, dass eine Differenzierung von Kosten und Nutzen für die Bewertungsdimensionen der ITS-Maßnahmen nicht immer zielführend ist. Insbesondere bei den nicht-monetären, nicht-monetarisierbaren und den eher qualitativen Dimensionen stieß die Interpretierbarkeit in der Praxis an ihre Grenzen. Auch die fehlende Berücksichtigung der Relevanz einer Bewertungsdimension (im Vergleich zu anderen Bewertungsdimensionen) trug zu sehr heterogenen Einschätzungen der Kosten- und Nutzeneffekte von ITS-Maßnahmen bei.

Die gewonnenen Erkenntnisse wurden dazu genutzt, den multikriteriellen Ansatz zu verbessern und die Bewertung zweistufig (in Anlehnung an die Methode des Analytic Hierarchy Process (AHP) von Saaty (2008)) aufzubauen: Zuerst werden die von den Unternehmen ausgewählten und als relevant klassifizierten Bewertungsdimensionen paarweise Verglichen und darauf aufbauend Gewichte für die Dimensionen berechnet. Anschließend werden die ITS-Maßnahmen im Hinblick auf die Bewertungsdimensionen anhand einer eindimensionalen ordinalen Skala (anstatt zwei Skalen für Kosten und Nutzen) bewertet. Die Bewertung erfolgt jeweils vergleichend. Bei Einzelmaßnahmen wird der Zustand vor der Einführung einer ITS-Maßnahme (Status Quo) als Vergleichsobjekt herangezogen (bspw. Vergleich der Prozessdurchlaufzeit und -stabilität vor der Einführung einer ITS-Maßnahme und danach). Bei zu treffenden Auswahlentscheidungen zwischen zwei alternativen ITS-Maßnahmen werden einfach die jeweiligen Maßnahmen als Vergleichsobjekte herangezogen, wobei auch in diesem Fall immer eine zusätzliche Unterlassungsalternative (Status Quo wird beibehalten) mit aufgenommen werden kann. ITS-Maßnahmenbündel können ebenfalls berücksichtigt werden, indem die Kombination zweier Maßnahmen als zusätzliche alternative Handlungsoption mit in den Entscheidungsraum einbezogen wird (bspw. Alternative 1: Network Intrusion Detection System (NIDS), Alternative 2: Security Information and Event Management (SIEM), Alternative 3: NIDS & SIEM).

	Zwischenevaluation des Kosten-/Nutzenmodells	
Kategorie	**msu Solutions GmbH**	**Rezeptprüfstelle Duderstadt**
1. Kosten- und Nutzenbewertung	Getrennte Kosten-/Nutzenbewertung nicht für alle Dimensionen praktikabel	Interpretation von Kosten und Nutzen der qualitativen Bewertungsdimensionen ist teilweise schwierig
	Bewertungsdimensionen sollten nach Bedeutung für das Unternehmen ausgewählt und sortiert werden können; das sollte entsprechend bei der Bewertung berücksichtigt werden	Gewichtungsfaktoren für Bewertungsdimensionen definieren (Relevanzklassifizierung)
	Vorschlag: Quantitative Werte auf linearer Skala abbilden • Bewertung einer ITS-Maßnahme sollte möglichst auf einer linearen Skala festgelegt werden (von "sehr hoch" bis "sehr niedrig") • Es sollten Richtwerte definiert werden, um Interpretationen zu erleichtern	Bewertungsskalen für Kosten/Nutzen: • keine Trennung in 2 Skalen für Kosten und Nutzen • verbal beschriebene Bewertungsskalen verwenden (5-Punkte-Likert-Skala könnte ausreichend sein)
	Dynamische Anpassung der Skala sollte ermöglicht werden	Zukünftige Chancen und Risiken für jede ITS-Maßnahme optional berücksichtigen
	Was tun, wenn zwei Anbieter die gleiche Leistung anbieten, die sich nur in wenigen quantitativen Dimensionen unterscheiden?	
2. Hilfestellung und Transparenz	Es sollten erläuternde Beispiele bereitgestellt werden: Besonders für verschiedenartige ITS-Maßnahmen und Maßnahmenvergleiche	Hilfestellungen bieten: Beschreibungen zu Dimensionen, Skalen und Bewertungsmethoden bereitstellen, um den Bewertungsprozess zu erleichtern.
		Klarheit und Verständlichkeit der Bewertung: • Alle Bewertungen und Beschreibungen sollen klar und verständlich formuliert sein • Sicherstellen, dass alle Beteiligten dieselben Begriffe gleich verstehen
		Einsicht am Ende des Bewertungsprozesses: • Summierte Übersicht mit der Möglichkeit, detailliertere Ebenen einzusehen, um Entscheidungen nachzuvollziehen • Es sollte die Möglichkeit geben, die Bewertungen anderer einzusehen
3. Kenntnis/Expertise der Bewertenden	Unterschiedliche Bewertung von Dimensionen und ITS-Maßnahmen je nach Typ/Rolle der Person: • Bsp.: Techniker und Personaler gewichten Dimensionen unterschiedlich => das sollte sich bei der finalen Verrechnung ausgleichen • Unterschiedliche Maßnahmen oder Dimensionen sollten von unterschiedlichen Personen bewertet werden, um Vergleichbarkeit sicherzustellen	Fachliche Expertise nutzen: Für verschiedene Dimensionen sollen unterschiedliche Ansprechpartner mit entsprechender Expertise eingebunden werden
	Nicht alle Befragten/Experten kennen jede Maßnahme oder Dimension im Detail	

Tab. 6: Ergebnisdokumentation der formativen Zwischenevaluation des Kosten-/Nutzenmodells bei der msu Solutions GmbH und der Rezeptprüfstelle Duderstadt

Die Artefakt-Entwicklung und -Erweiterung wurde zusammen mit den Ergebnissen aus mehreren Zwischenevaluationen fortlaufend dokumentiert und als Grundlage für die Konzeption des finalen multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln) genutzt. Dieses ist hierarchisch strukturiert (siehe Abb. 14): Auf der ersten Hierarchiebene („Objective“) werden die Geschäftsprozesse, die von der zu bewertenden ITS-Maßnahme betroffenen sind, zuerst identifiziert und dann die für den Geschäftsprozess relevanten Bewertungsdimensionen abgeleitet. Auf der zweiten Hierarchiebene („Criteria“) werden die Bewertungsdimensionen manuell von den teilnehmenden Experten in reziproken Matrizen mit Hilfe von paarweisen Vergleichen gewichtet. Das Ergebnis ist ein Prioritätsvektor der Bewertungsdimensionen pro Experten (Bodin et al. 2005). Für die Aggregation der Gewichtungen der Bewertungsdimensionen über alle Experten hinweg, wird das geometrische Mittel verwendet. Als Ergebnis erhält man die relativen Gewichte pro Bewertungsdimension, welche einen Prioritätsvektor bilden.

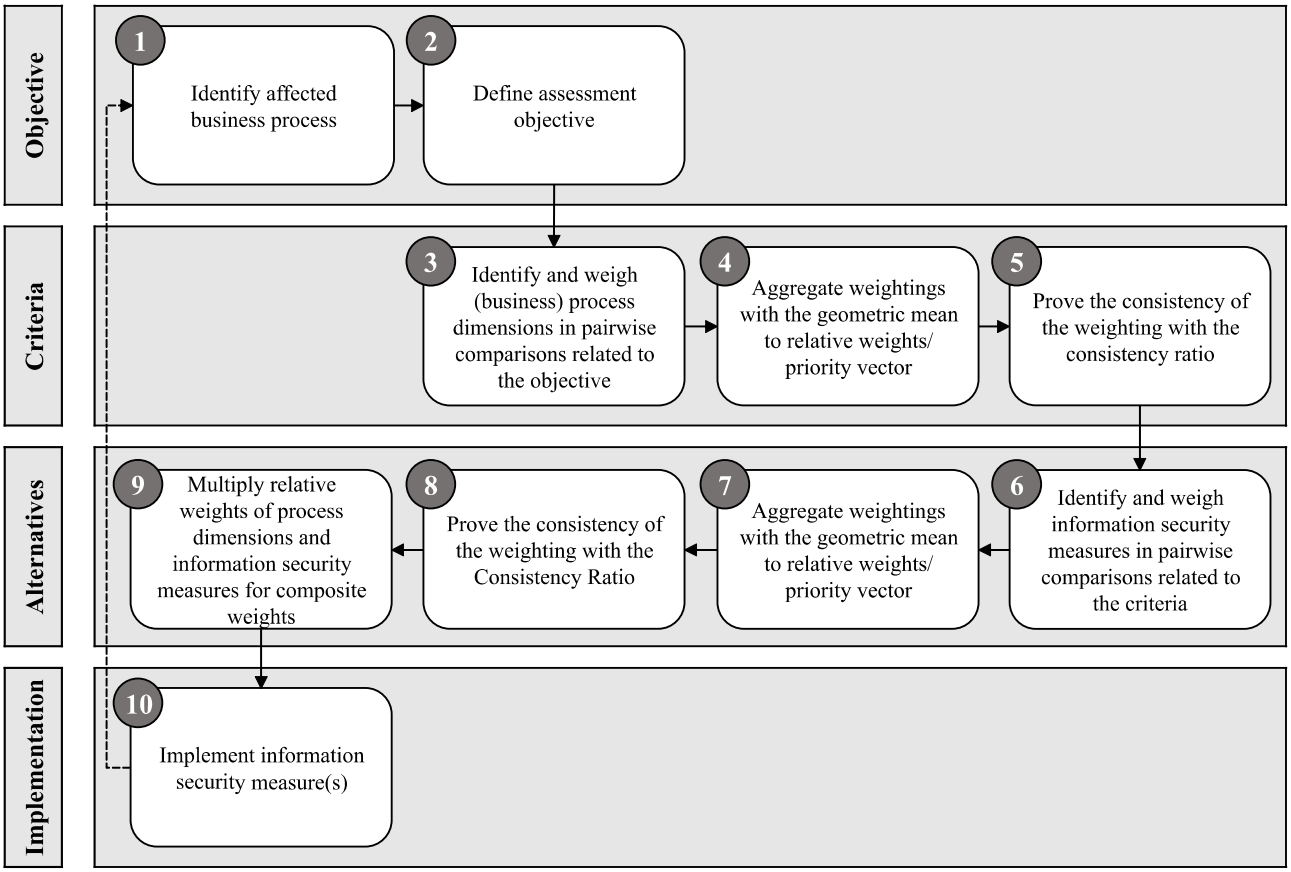


Abb. 14: Struktur des finalen multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)

Auf der dritten Hierarchieebene („Alternatives“) werden die zur Auswahl stehenden ITS-Maßnahmen ebenfalls in reziproken Matrizen aufgeführt und von den Experten durch einen paarweisen Vergleich gewichtet. Dabei wird berücksichtigt, inwieweit eine Alternative gegenüber einer anderen Alternative (in Bezug auf die oben aufgeführten Bewertungsdimensionen) bevorzugt wird (Bodin et al. 2005; Mayer et al. 2018). Wie bei den Kriterien wird auch für die Alternativen ein Prioritätsvektor berechnet. Um ein zusammengesetztes Gewicht für jede ITS-Maßnahme zu erhalten, wird der Prioritätsvektor einer ITS-Maßnahme mit dem Prioritätsvektor der Bewertungsdimensionen multipliziert (Benlian 2010). Die ITS-Maßnahme mit dem höchsten Gesamtwert kann dann implementiert werden (Hierarchieebene: „Implementation“). Diese Struktur wurde am Beispiel der Case Studies aus UAP 2.3 und UAP 2.4 sowie anhand einer Fallstudie des assoziierten Partners VWFS erfolgreich getestet und positiv abschlussevaluiert. Ein Einblick in die Bewertungsprozedur anhand der VWFS-Fallstudie ist in Abbildung 15 zu finden (am Beispiel von NIDS und SIEM). Einen konkreten Überblick über das Modell, notwendige Berechnungen und das in Abbildung 15 ersichtliche Anwendungsbeispiel sind in Bauer et al. (2024a) zu finden.

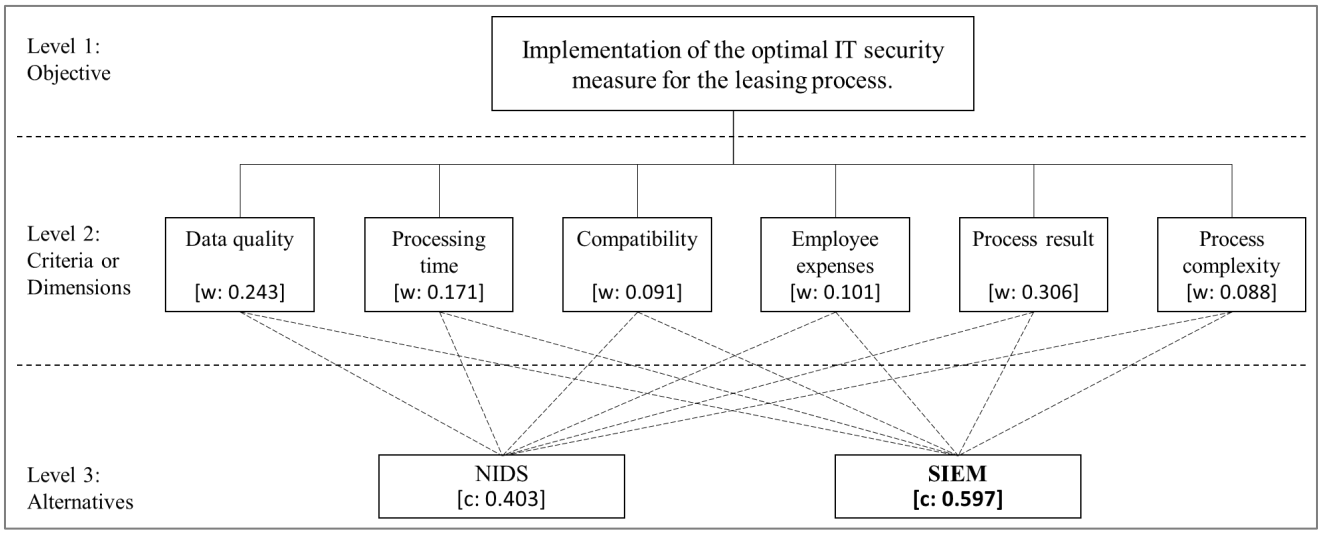


Abb. 15: Exemplarische Entscheidungshierarchie des multikriteriellen prozessorientierten Entscheidungsmodells bei der Volkswagen Financial Services AG

2.5 AP 4 - Entwurf des ProBITS-Vorgehensmodells

Im Rahmen des Arbeitspakets 4 wurde das multikriterielle Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln) vom MEBITS-Team in das von der UPB entwickelte skalierbare Vorgehensmodell integriert. Der Entwurf des Vorgehensmodells erfolgte parallel zur Entwicklung des Entscheidungsmodells, wodurch sichergestellt werden konnte, dass die beiden Modelle nicht klassisch aufeinander aufbauen, sondern sich vielmehr gegenseitig ergänzen. Durch enge Kollaboration und Kommunikation, insbesondere zwischen MLU und UPB, aber auch mit dem restlichen Projektkonsortium, konnte die nahtlose Integration sichergestellt werden. Beispielsweise wurden die Ergebnisse der Zwischenevaluationen aus AP 3 (siehe Tabelle 6) an die UPB weitergegeben und insbesondere über die Möglichkeiten diskutiert, wie die Aspekte der Kategorien 2 und 3 aus Tabelle 6 im Vorgehensmodell adressiert werden können.

Im Rahmen des Teilprojektes MEBITS wurde als Ergebnis von AP 4 eine ausformulierte Vorgehens- bzw. Ablaufbeschreibung für die Implementierung und Anwendung des multikriteriellen Entscheidungsmodells dokumentiert. Die Dokumentation wurde, im Einklang mit den Ergebnissen der Zwischenevaluationen aus AP 3 (siehe Tabelle 6), mit Beispielen unterlegt und führt Schritt für Schritt durch die einzelnen Phasen, die zur Anwendung des multikriteriellen Entscheidungsmodells erforderlich sind. Dadurch wird sichtbar, wie beide Instrumente zusammenwirken, um eine fundierte und praxisnahe Bewertung von ITS-Maßnahmen und -bündeln zu ermöglichen. Für eine detailliertere Beschreibung der Ergebnisse des AP 4 verweisen wir auf den Abschlussbericht des Konsortialpartners UPB, der die Hauptverantwortung für das Arbeitspaket trägt.

Die beispielgetriebene Vorgehens- bzw. Ablaufbeschreibung des multikriteriellen Entscheidungsmodells wurde vom MEBITS-Team als Teil eines wissenschaftlichen Beitrags im Tagungsband der renommierten Internationalen Tagung Wirtschaftsinformatik publiziert (siehe Bauer et al. (2024a)).

2.6 AP 5 – Entwicklung ProBITS-Werkzeug

Auf der Grundlage des Ergebniskatalogs aus AP2, der Zwischenevaluationen aus AP 3 und des multikriteriellen Entscheidungsmodells als zentrales Methoden-Artefakt des Teilprojektes MEBITS, wurden erforderliche technische und fachliche Anforderungen für das ProBITS-Werkzeug katalogisiert. Die wichtigsten Anforderungen wurden, angelehnt an das gestaltungsorientierte Forschungsparadigma der Wirtschaftsinformatik, überblicksartig in Form einer Design-Theorie dargestellt (siehe Abbildung 16) und eingehend beschrieben (siehe Bauer (2024)).

A multiple-criteria assessment tool for information security investments should…

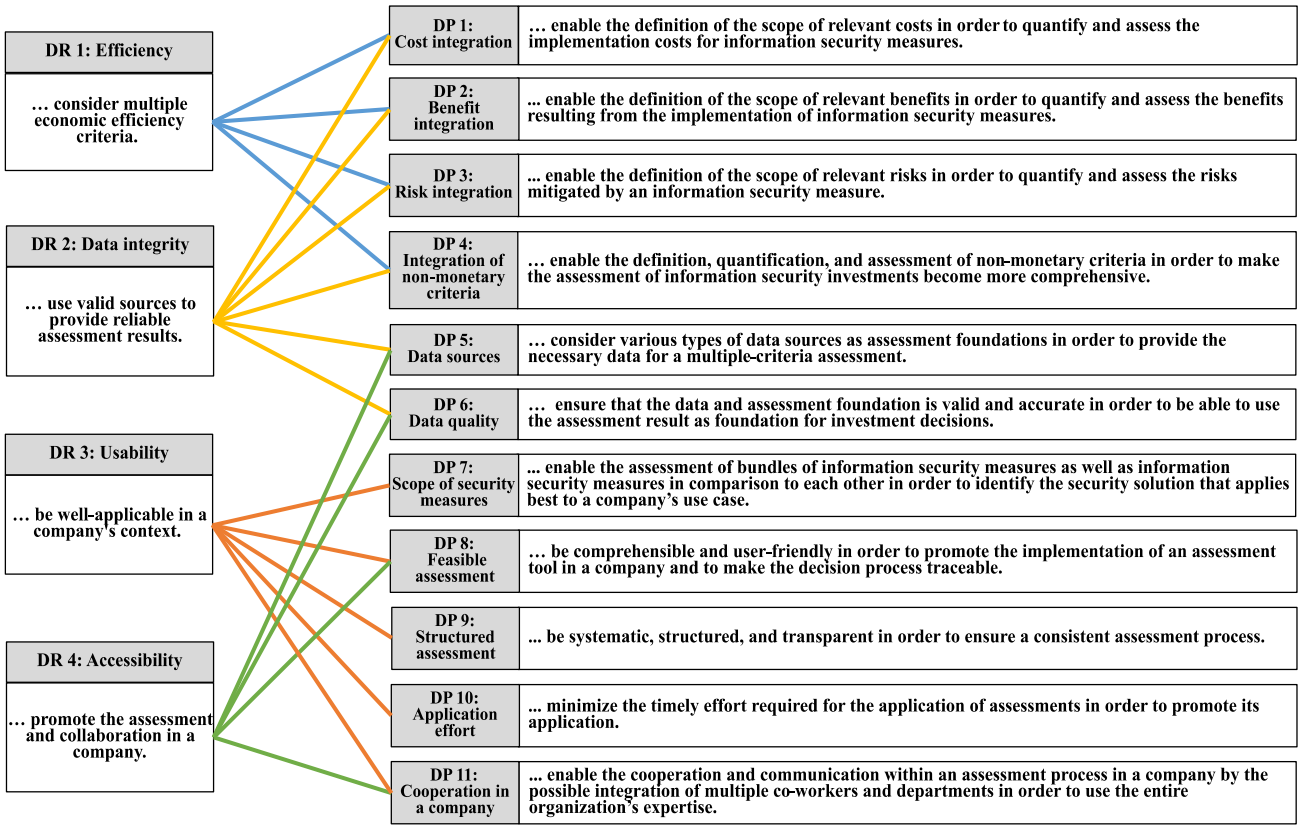


Abb. 16: Fachliche und technische Anforderungen an das ProBITS-Werkzeug, die sich aus dem multikriteriellen Entscheidungsmodell ergeben (dargestellt als Design-Theorie, siehe Bauer (2024))

In Abbildung 16 (links) sind Design-Anforderungen (engl. Design Requirements (DR)) abgebildet. Im Allgemeinen beschreiben DR übergeordnete Ziele, die ein Informationssystem bzw. IT-Werkzeug erfüllen soll (Baskerville und Pries-Heje 2010). In unserem Fall beschreiben DR1 – DR4 Anforderungen, die an ein IT-Werkzeug für ein multikriterielles Entscheidungsmodell gestellt werden. In Abbildung 16 (rechts) befinden sich zugehörige Design-Prinzipien (engl. Design Principles (DP)). Diese Prinzipien (DP 1 – DP 11) dienen als Leitlinien zur Erreichung der Ziele für den Entwicklungsprozesses des IT-Werkzeugs (Fu et al. 2016).

Der Katalog an fachlichen und technischen Anforderungen sowie die Design-Theorie dienten als Grundlage für die weitere Entwicklung und Implementierung des ProBITS-Werkzeugs. Damit wurde sichergestellt, dass die relevanten Aspekte und Bedürfnisse, die im Verlauf des Teilvorhabens MEBITS identifiziert wurden, angemessen berücksichtigt werden.

Im Rahmen eines ersten technischen und fachlichen Tests wurde das ProBITS-Werkzeug (im Allgemeinen) und die informationstechnische Integration des multikriteriellen Entscheidungsmodells (im Speziellen) geprüft. Dabei wurde zunächst besonderes Augenmerk auf technische Funktionalität und Effektivität der Bewertung gelegt. Das IT-Tool wurde dazu von drei Mitgliedern des MEBITS-Teams installiert und einem Alpha-Test unterzogen. Dafür wurden zuerst fiktive, später auch realitätsnahe Bewertungsszenarien durchgespielt. Im Ergebnis zeigte sich, dass es einerseits schon bei der Installation des Tools zu Problemen kam, woraus geschlossen wurde, dass Bedarf an einer Installationsanleitung besteht. Zum anderen wurde ersichtlich, dass die Struktur des hierarchischen Entscheidungsmodells (siehe Abb. 14) noch nicht vollständig in der Oberfläche des IT-Werkzeugs abgebildet wurde, was partiell zu Verständnisproblemen führte. Die detaillierten Ergebnisse der Tests wurden in einem Ergebnisbericht zusammengefasst und gezielte Verbesserungsmaßnahmen

umgesetzt. Für eine detailliertere Beschreibung der Ergebnisse des AP 5 verweisen wir auf den Abschlussbericht des Konsortialpartners UPB, der die Hauptverantwortung für das Arbeitspaket trägt.

2.7 AP 6 – Evaluation und Weiterentwicklung ProBITS

Im Rahmen des Arbeitspakets 6 wurde vom MEBITS-Team, unter Anwendung der IT-Demonstratoren 1, 2 und 3, das multikriterielle Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln) angewendet und evaluiert. IT-Demonstrator 1 (siehe Abb. 1, AP 6.1: „ProBITS in Aktion“) wurde anhand einer prospektiven Fallstudie der RPD aus dem Bereich „Gesundheit“ angewendet; IT-Demonstrator 2 (siehe Abb. 1, AP 6.2: „ProBITS in Aktion“) an einem prospektiven Fallbeispiel der MSU aus dem Bereich „Smart Metering“. Die retrospektive Anwendung (siehe Abb. 1, AP 6.3: „ProBITS deckt auf“) fand ebenfalls bei der MSU mit dem IT-Demonstrator 3 statt. In diesem Rahmen wurden zudem ausgewählte traditionelle Verfahren zur investitionstheoretischen Bewertung von ITS-Maßnahmen vergleichend zum multikriteriellen Modell angewendet. Nach allen drei Anwendungsszenarien wurden vom MEBITS-Team jeweils Erkenntnisse, Herausforderungen und ggf. Verbesserungspotentiale dokumentiert, die insbesondere das multikriterielle Entscheidungsmodell betrafen. Ein Auszug der Dokumentation ist in Tabelle 7 zu finden. Auf Basis der identifizierten Verbesserungspotentiale wurde eine zweite, aktualisierte Version des multikriteriellen Entscheidungsmodells entwickelt.

Kategorie	Erkenntnis / Herausforderung / Problem	Verbesserung / Anpassung
Skalen und Skalierung	Linguistische Skala für Bewertungsdimensionen nicht ausreichend feingranular	Granularität angepasst
	Skalenausprägungen der linguistischen Skala nicht eineindeutig	zusätzliche Erläuterungen (Bedeutung der Skalenausprägungen) hinzugefügt
Bewertungsdimensionen	Klarheit der Dimensionen und Dimensionsbeschreibungen	Wording überarbeitet
	Definitionen für Dimensionen bereitstellen	Definitionen bereitgestellt
	Wichtigste Dimensionen (nach Rangfolge) vorab im Tool bereitstellen	Dimensionskatalog implementiert
Funktionalitäten	Schnittstelle zum Upload von beliebigem Geschäftsprozess gewünscht	Upload-Funktion für Geschäftsprozess umgesetzt
	Alte Bewertungsprojekte und Prioritätsvektoren sollten einseh-, abruf- und nachnutzbar sein	Speicher-/Exportfunktion hinzugefügt
	Exportfunktion gewünscht, um Daten/Ergebnisse auch außerhalb des Tools verwenden zu können (bspw. in Excel)	
	Rollen- und Berechtigungskonzept gewünscht: nicht jeder sollte Zugriff auf alle Prozessinformationen und Dimensionen haben (bspw. Experten, die nur bewerten sollen)	Rollen- und Berechtigungskonzept umgesetzt

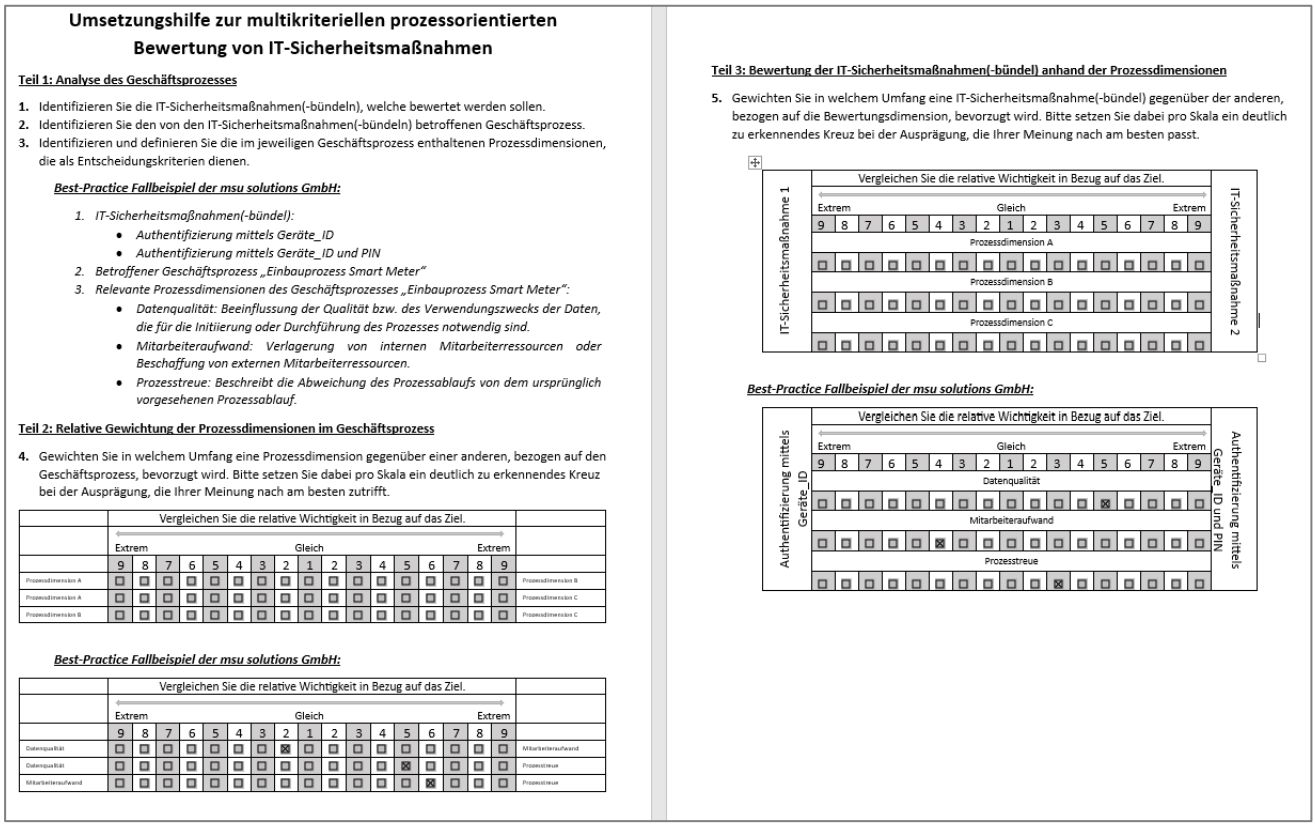
Tab. 7: Auszug der Ergebnisdokumentation aus der prospektiven und retrospektiven Modellanwendung

Aus der vergleichenden retrospektiven Betrachtung des multikriteriellen Modells mit traditionellen Verfahren zur investitionstheoretischen Bewertung von ITS-Maßnahmen gingen zudem spannende Erkenntnisse hervor. Ein großes Problem der MSU bestand zunächst darin, notwendige Daten zur investitionstheoretischen ITS-Bewertung zu beschaffen, die für die Anwendung der traditionellen Verfahren notwendig war. Während angefallene Kosten für ITS-Maßnahmen und Schäden von aufgetretenen Sicherheitsvorfällen relativ einfach zu beziffern waren, stellte es eine Herausforderung dar, die verhinderten Schäden monetär abzuschätzen, da keine konkreten Anhaltspunkte dazu vorlagen. Am Beispiel des RoSI zeigte sich zudem, dass auch die zur Berechnung benötigte Effektivität der ITS-Maßnahme deshalb schwer abschätzbar war. Ein zweites Problem bestand in der Entscheidung, welche monetären Auswirkungen der ITS-Maßnahme zuzuschreiben sind und welche nicht. Die Datenbeschaffung für die traditionellen Verfahren zur investitionstheoretischen Bewertung von ITS-Maßnahmen war summa summarum sehr aufwendig und zugleich von großer Vagheit geprägt. Die Kalkulation selbst ist einfach und intuitiv nachvollziehbar. Im Vergleich zur multikriteriellen Bewertung ist die Aussagekraft der traditionellen Verfahren durch die Fokussierung auf monetäre Werte jedoch deutlich limitiert. Sie berücksichtigen einen wesentlichen Teil der Bewertungsdimensionen aus AP 2 nicht und ermöglichen damit kein realistisches Abbild der vielfältigen Auswirkungen, die mit dem

Einsatz von ITS-Maßnahmen einhergehen. Das verdeutlichte insbesondere auch die vergleichende retrospektive Anwendung des RoSI und des multikriteriellen Modells bei der MSU am Beispiel „Clearswift Secure Gateway“. Während der RoSI ein negatives Ergebnis hervorbrachte (was bedeutet, dass sich eine Investition in die ITS-Maßnahme monetär nicht lohnt), war das Ergebnis der Anwendung des multikriteriellen Modells für die ITS-Maßnahme größer als die Unterlassungsalternative, was bedeutet, dass sich die Investition unter Berücksichtigung der Bewertungsdimensionen lohnt. Für eine detailliertere Beschreibung der Ergebnisse des AP 6 verweisen wir auf den Abschlussbericht des Konsortialpartners MSU, der die Hauptverantwortung für das Arbeitspaket trägt.

2.8 AP 7 – Kommunikation und Diffusion ProBITS

Im Rahmen des Arbeitspakets 7 wurden vom MEBITS-Team Umsetzungshilfen und Best-Practice-Beschreibungen zu den Demonstratoren entwickelt, um die Kommunikation und Diffusion des ProBITS-Ansatzes (im Allgemeinen) und des prozessorientierten multikriteriellen Entscheidungsmodells (im Speziellen) weiter zu unterstützen. Dafür wurde unter anderem auf die Ergebnisse der Zwischenevaluationen aus AP 3 (Tabelle 6) und die Erkenntnisse aus den APs 4 und 6 zurückgegriffen. Abbildung 17 zeigt die Umsetzungshilfe für Demonstrator 2.



Umsetzungshilfe zur multikriteriellen prozessorientierten Bewertung von IT-Sicherheitsmaßnahmen

Teil 1: Analyse des Geschäftsprozesses

1. Identifizieren Sie die IT-Sicherheitsmaßnahmen(-bündeln), welche bewertet werden sollen.
2. Identifizieren Sie den von den IT-Sicherheitsmaßnahmen(-bündeln) betroffenen Geschäftsprozess.
3. Identifizieren und definieren Sie die im jeweiligen Geschäftsprozess enthaltenen Prozessdimensionen, die als Entscheidungskriterien dienen.

Best-Practice Fallbeispiel der msu solutions GmbH:

1. *IT-Sicherheitsmaßnahmen(-bündel):*
   - *Authentifizierung mittels Geräte_ID*
   - *Authentifizierung mittels Geräte_ID und PIN*
2. *Betroffener Geschäftsprozess „Einbauprozess Smart Meter“*
3. *Relevante Prozessdimensionen des Geschäftsprozesses „Einbauprozess Smart Meter“:*
   - *Datenqualität: Beeinflussung der Qualität bzw. des Verwendungszwecks der Daten, die für die Initiierung oder Durchführung des Prozesses notwendig sind.*
   - *Mitarbeiteraufwand: Verlagerung von internen Mitarbeiterressourcen oder Beschaffung von externen Mitarbeiterressourcen.*
   - *Prozesstreue: Beschreibt die Abweichung des Prozessablaufs von dem ursprünglich vorgesehenen Prozessablauf.*

Teil 2: Relative Gewichtung der Prozessdimensionen im Geschäftsprozess

4. Gewichten Sie in welchem Umfang eine Prozessdimension gegenüber einer anderen, bezogen auf den Geschäftsprozess, bevorzugt wird. Bitte setzen Sie dabei pro Skala ein deutlich zu erkennendes Kreuz bei der Ausprägung, die Ihrer Meinung nach am besten zutrifft.

Vergleichen Sie die relative Wichtigkeit in Bezug auf das Ziel.
Extrem — Gleich — Extrem
9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9
Prozessdimension A | Prozessdimension B
Prozessdimension A | Prozessdimension C
Prozessdimension B | Prozessdimension C

Best-Practice Fallbeispiel der msu solutions GmbH:

Vergleichen Sie die relative Wichtigkeit in Bezug auf das Ziel.
Extrem — Gleich — Extrem
9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9
Datenqualität | Mitarbeiteraufwand
Datenqualität | Prozesstreue
Mitarbeiteraufwand | Prozesstreue

Teil 3: Bewertung der IT-Sicherheitsmaßnahmen(-bündel) anhand der Prozessdimensionen

5. Gewichten Sie in welchem Umfang eine IT-Sicherheitsmaßnahme(-bündel) gegenüber der anderen, bezogen auf die Bewertungsdimension, bevorzugt wird. Bitte setzen Sie dabei pro Skala ein deutlich zu erkennendes Kreuz bei der Ausprägung, die Ihrer Meinung nach am besten passt.

Vergleichen Sie die relative Wichtigkeit in Bezug auf das Ziel.
IT-Sicherheitsmaßnahme 1 — IT-Sicherheitsmaßnahme 2
Extrem — Gleich — Extrem
9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9
Prozessdimension A
Prozessdimension B
Prozessdimension C

Best-Practice Fallbeispiel der msu solutions GmbH:

Vergleichen Sie die relative Wichtigkeit in Bezug auf das Ziel.
Authentifizierung mittels Geräte_ID — Authentifizierung mittels Geräte_ID und PIN
Extrem — Gleich — Extrem
9 8 7 6 5 4 3 2 1 2 3 4 5 6 7 8 9
Datenqualität
Mitarbeiteraufwand
Prozesstreue

Abb. 17: Umsetzungshilfe des prozessorientierten multikriteriellen Entscheidungsmodells bezüglich Demonstrator 2

Darüber hinaus sind Umsetzungs- und Anwendungshilfen in den vom MEBITS-Team veröffentlichten Beiträgen Bauer (2024) (Umsetzungshilfe in Form einer Design-Theorie für Tool-Entwickler) und Bauer et al. (2024a) (Anwendungshilfe als ausformuliertes eines Fallbeispiel) zu finden. Zahlreiche zusätzliche Kommunikations- und Diffusionsaktivitäten sind auch bereits in AP 1 beschrieben worden, auf die an dieser Stelle nochmals verwiesen werden soll. Zudem sind fortlaufend Lehr- und Weiterbildungsmaterialien zur Informations- und IT-Sicherheitsbewertung (im Allgemeinen) und der multikriteriellen Bewertung von ITS-Maßnahmen (im Speziellen) entwickelt worden. Diese fanden und finden noch Eingang in die universitäre Lehre (z. B. in das Modul „Forschungsmethoden der Wirtschaftsinformatik“ an der MLU) und in Weiterbildungsinitiativen (z. B. in den Summit „IT-Security“ in Leipzig; siehe: https://summit-community.de/thema/it-security/).

Weitere Kommunikations- und Diffusionsmaßnahmen umfassten die durchgängig projektbegleitende Arbeit an Ergebnisberichten, Forschungsbeiträgen und Tagungspräsentationen. Auf die einzelnen Ergebnisberichte, Dokumentationen und Kataloge, die aus dem Teilvorhaben MEBITS hervorgingen, wurde in den jeweiligen Arbeitspaketen bereits detailliert eingegangen. Darüber hinaus wurden das Projekt ProBITS, das Teilprojekt MEBITS und die wichtigsten Ergebnisse öffentlichkeitswirksam auf Tagungen, Forschungs- und Praxiskongressen sowie nationalen und internationalen Konferenzen vorgestellt. Die wissenschaftliche Ergebniskommunikation umfasste sowohl die Organisation und Leitung eigener Workshops, als auch die Teilnahme an Konferenzen und Tagungen mit dem Ziel des Networkings und der Präsentation von Erkenntnissen aus dem Teilprojekt. Die nachfolgende Liste bietet Überblick über einige der zur wissenschaftlichen Ergebniskommunikation vorgenommenen Tätigkeiten und Aktivitäten (chronologisch geordnet):

- Organisation, Durchführung und Leitung des projektthemenspezifischen „First International Workshop on Current Information Security and Compliance Issues in Information Systems Research“ (CIISR 2021), der im Rahmen der 16. Internationalen Konferenz Wirtschaftsinformatik (WI 2021) stattfand (virtueller Workshop wegen der COVID-19-Pandemie, ursprünglich geplant: Duisburg)
- Organisation, Durchführung und Leitung des projektthemenspezifischen „Second International Workshop on Current Information Security and Compliance Issues in Information Systems Research“ (CIISR 2022), der im Rahmen der 17. Internationalen Konferenz Wirtschaftsinformatik (WI 2022) stattfand (virtueller Workshop wegen der COVID-19-Pandemie; ursprünglich geplant: Nürnberg)
- Teilnahme an und Präsentation von einem Beitrag bei der 17. Internationalen Konferenz Wirtschaftsinformatik (WI 2022) im Februar 2022 (virtuell wegen der COVID-19-Pandemie; ursprünglich geplant: Nürnberg)
- Poster- und Tool-Präsentation bei der 20th International Conference on Business Process Management (BPM 2022) in Münster im September 2022
- Teilnahme an und Beteiligung bei dem Karikaturenwettbewerb der Nationalen Konferenz für IT-Sicherheitsforschung, ausgerichtet vom Bundesministerium für Bildung und Forschung in Berlin im März 2023
- Vortrag zum Thema „IT-Sicherheit - (K)eine Frage des Geldes? Wie Sie Prozesse nutzen können, um wirtschaftliche Entscheidungen zu IT-Sicherheitsmaßnahmen zu treffen“ und anschließende formative Evaluation des multikriteriellen Entscheidungsmodells mit Praktikern bei den COMMUNITY DAYS "Governance, Risk, Compliance in der IT" und "IT-Security-Management" in Leipzig im Mai 2023
- Teilnahme an und Präsentation von Konferenzbeiträgen bei der Americas Conference on Information Systems (AMCIS 2023) in Panama City, Panama sowie Beteiligung am dortigen Community-Meeting der Expertengruppe für Information Security und Privacy (SIGSEC) im August 2023
- Organisation, Durchführung und Leitung des projektthemenspezifischen „Third International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR 2023)“, der im Rahmen der 18. Internationalen Konferenz Wirtschaftsinformatik (WI 2023) in Paderborn im September 2023 stattfand
- Teilnahme an und Präsentation von einem Beitrag bei der 18. Internationalen Konferenz Wirtschaftsinformatik (WI 2023) in Paderborn im September 2023
- Teilnahme an und Präsentation von einem Konferenzbeitrag auf dem INFORMATIK Festival 2023, der Jahrestagung der Gesellschaft für Informatik im September 2023 in Berlin
- Organisation, Durchführung und Leitung des projektthemenspezifischen „Fourth International Workshop on Current Information Security and Compliance Issues in Information Systems Research“ (CIISR 2024), der im Rahmen der 19. Internationalen Konferenz Wirtschaftsinformatik (WI 2024) in Würzburg im September 2024 stattfand
- Teilnahme an und Präsentation von Konferenzbeiträgen bei der 19. Internationalen Konferenz Wirtschaftsinformatik (WI 2024) in Würzburg im September 2024

Darüber hinaus wurden zur Ergebnisverstetigung und Langzeitarchivierung wissenschaftliche Artikel über die Ergebnisse des Teilprojektes in Tagungsbänden und Journalen veröffentlicht. Dabei wurde darauf geachtet, dass die Beiträge möglichst frei zugänglich sind. Zum Teil wurden die Artikel zusätzlich im digitalen universitären Repositorium Share_it der MLU zur Archivierung zweitveröffentlicht. Die nachfolgende Liste bietet einen wesentlichen Überblick über die Artikel, die Ergebnisse aus dem Teilprojekt (und darüber hinaus) enthalten (chronologisch geordnet):

- Kühnel, S.; Sackmann, S.; Trang, S. T.-N.; Nastjuk, I.; Matschak, T.; Niedzela, L.-M.; Nake, L. (2021): Towards a Business Process-based Economic Evaluation and Selection of IT Security Measures, Proceedings of the First International Workshop on Current Compliance Issues in Information Systems Research (CIISR'21), co-located with the 16th International Conference on Wirtschaftsinformatik (WI'21), Essen, Germany (online), CEUR Workshop Proceedings Vol-2966, urn:nbn:de:0074-2966-1, ISSN 1613-0073. http://ceur-ws.org/Vol-2966/paperkey.pdf.
- Niedzela, L.-M.; Nake, L.; Matschak, T. (2022): Categories of Approaches for IT Security Investment Decisions: A Systematic Literature Review, 17th International Conference on Wirtschaftsinformatik (WI'22), Wirtschaftsinformatik 2022 Workshop Proceedings, paper 4. https://aisel.aisnet.org/wi2022/workshops/workshops/4.
- Kuehnel, S.; Sackmann, S.; Damarowsky, J.; Böhmer, M. (2022): "EconBPC: A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes", 20th International Conference on Business Process Management (BPM 2022), Proceedings of the Best Dissertation Award, Doctoral Consortium, and Demonstration & Resources Track, CEUR-WS Vol. 3216, Münster, Germany, pp. 127-131, DOI: 10.25673/92371, http://ceur-ws.org/Vol-3216/paper_252.pdf.
- Nake, L.; Kuehnel, S.; Bauer, L.; Sackmann, S. (2023): „Towards Identifying GDPR-Critical Tasks in Textual Business Process Descriptions", in: M. Klein, D. Krupka, C. Winter., V. Wohlgemuth (Hrsg.): INFORMATIK 2023, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn, Germany, DOI: 10.18420/inf2023_191, S. 1895-1908, https://doi.org/10.18420/inf2023_191.
- Matschak, T.; Nastjuk, I.; Niedzela, L.; Kuehnel, S.; Trang, S. (2023): „A Process-Based Approach to Information Security Investment Evaluation: Design, Implementation, and Evaluation", Proceedings of Americas Conference on Information Systems (AMCIS 2023), Panama City, Panama, https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/30.
- Niedzela, L.; Kuehnel, S.; Nastjuk, I.; Matschak, T.; Sackmann, S.; Trang, S. (2023): „A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions", Proceedings of Americas Conference on Information Systems (AMCIS 2023), Panama City, Panama https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/16.
- Nake, L. (2023): „Integrating IT Security Aspects into Business Process Models: A Taxonomy of BPMN Extensions", Proceedings of the 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR 2023), Co-located with the 18th International Conference on Wirtschaftsinformatik (WI). Paderborn, Germany, https://ceur-ws.org/Vol-3512/fullpaper3.pdf.
- Hengstler, S.; Kuehnel, S.; Masuch, K.; Nastjuk, I.; Trang, S. (2023): „Should I Really do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior", Computers & Security, Volume 133, https://doi.org/10.1016/j.cose.2023.103370.
- Bauer, Laura (2024): A Literature-Driven Design Theory for Multiple-Criteria Assessment Tools for Information Security Investments, 19th International Conference on Wirtschaftsinformatik, 4th International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR 2024), September 2024, Würzburg, Germany. https://aisel.aisnet.org/wi2024/125/.

- Bauer, Laura; Kuehnel, Stephan; Nastjuk, Ilja; Nake, Leonard; Seidel, Heiko (2024): Multiple-Criteria Decisions for Information Security - A Case Study of Volkswagen Financial Services AG, Wirtschaftsinformatik 2024 Proceedings, 19th International Conference on Wirtschaftsinformatik, September 2024, Würzburg, Germany. https://aisel.aisnet.org/wi2024/56/
- Bauer, L.; Kuehnel, S.; Nastjuk, I.; Sackmann, S. (2024): „A Multiple-Method Study on Acceptance Factors of Economic Assessment Approaches for Information Security Investments“, Pacific Asia Journal of the Association for Information Systems (PAJAIS), Vol. 16, Iss. 4, Article 2. https://aisel.aisnet.org/pajais/vol16/iss4/2/.

3. Wesentliche Ergebnisse

Eine detaillierte Darstellung der Resultate ist in Kapitel 2 (Beschreibung des Ablaufs des Teilvorhabens MEBITS) dieses Berichts zu finden. Die wesentlichen Ergebnisse können nochmals wie folgt zusammengefasst werden:

- Etablierter und verstetigter Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln), der innerhalb des Competence Centers von ProBITS geschaffen wurde und auf Zusammenarbeit und Wissensaustausch zwischen den Projektpartnern, assoziierten Partnern und externen Interessierten ausgerichtet wurde
- Validierter Katalog von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen
- Validierter Katalog von kritischen fachlichen Anforderungen, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden
- Konzeptmatrix der traditionellen Verfahren zur ITS-Bewertung
- Prozessbasiertes Kosten-/Nutzenmodell zur Bewertung von ITS-Maßnahmen
- Zugehörige validierte BPMN- und XES-Extensions zur Erweiterung/Anpassung bestehender Prozessmodellierungskonventionen
- Evaluiertes, skalierbares, multikriterielles, prozessorientiertes Entscheidungsmodell als Methoden-Artefakt zur Bewertung von ITS-Maßnahmen(-bündeln).
- Ausformulierte Ablaufbeschreibungen und Katalog an fachlichen und technischen Anforderungen für das Entscheidungsmodell zur Implementierung in das IT-Werkzeug und Vorgehensmodell
- Fallstudiengetriebene Testung des multikriteriellen Entscheidungsmodells mit den entwickelten Demonstratoren und Erkenntnisdokumentation der prospektiven, retrospektiven und vergleichenden Anwendung
- Ausformulierte beispielgetriebene Anwendungshilfen für das multikriterielle Entscheidungsmodell
- Lehr- und Weiterbildungsmaterialien zur Informations- und IT-Sicherheitsbewertung (im Allgemeinen) und der multikriteriellen Bewertung von ITS-Maßnahmen (im Speziellen)
- Ergebnisdiffusion durch Publikationen in Tagungsbänden und Fachjournalen sowie Präsentationen auf Fachtagungen und Konferenzen

4. Vorläufige Auskunft über die wichtigsten Positionen des zahlenmäßigen Nachweises

Da uns zum Zeitpunkt der Einreichung dieses Abschlussberichts noch kein finaler Kontenstand vorliegt, basieren die hier aufgelisteten Positionen und Zahlen auf dem Kontenstand vom 03.12.2024. Eine finale Auskunft ist dem zahlenmäßigen Verwendungsnachweis zu entnehmen.

Im Projekt wurden folgende Kosten verausgabt (Stand 03.12.2024):

Ausgabeart		
Nummer	**Bezeichnung**	**Ausgabe**
0812	Wissenschaftler	*208.126,39*
0822	Hilfskräfte	*14.222,67*
0843	Verbrauchsmaterial SK	*3.501,90*
0844	Dienstreisen Inland	*4.765,89*
0888	Projektpauschale	*45.839,03*

5. Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten

Das Teilvorhaben MEBITS war ein wesentlicher Bestandteil des Verbundprojekts ProBITS, das darauf abzielte, die vier zentralen ProBITS-Bausteine gemeinsam mit den Verbundpartnern zu entwickeln. Durch die Konzeption und Umsetzung dieser Bausteine konnte im Verbundprojekt ein innovativer, skalierbarer und werkzeuggestützter Ansatz bereitgestellt werden, der eine mehrdimensionale, geschäftsprozessorientierte Bewertung von ITS-Maßnahmen und -Maßnahmenbündeln ermöglicht.

Im Rahmen des Verbundprojekts nahm MEBITS eine zentrale Rolle ein, da es mit der Konzeption des Herzstücks von ProBITS – dem multikriteriellen Entscheidungsmodell – betraut worden war. Dessen Realisierung war für das Verbundprojekt notwendig, da die Arbeit an den weiteren Unterstützungsleistungen (erweiterte Prozessmodellierungssprache, Vorgehensmodell, IT-Werkzeug) darauf aufbaute oder davon abhängig war und ansonsten nicht möglich gewesen wäre. Dies wurde auch durch Meilenstein 1 reflektiert (*„Das multikriterielle Entscheidungsmodell für ProBITS als Methoden-Artefakt zur wirtschaftlichen Bewertung und Analyse alternativer IT-Sicherheitsmaßnahmen(-bündel) liegt vor […]“*), der planmäßig erreicht wurde.

Für die Konzeption eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln) war es notwendig, zuerst relevante Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen sowie kritische fachliche Anforderungen, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden, zu erheben. Es erschien darüber hinaus als angemessen, bestehende traditionelle Verfahren der ITS-Bewertung vergleichend zu untersuchen und deren Grenzen aufzuzeigen, um die zum Zeitpunkt des Projektantrags bestehende Forschungslücke weiter zu untermauern. Es zeigte sich, dass die Aussagekraft der traditionellen Verfahren durch die eindimensionale Fokussierung auf monetäre Werte deutlich limitiert ist. Traditionelle Verfahren berücksichtigen einen wesentlichen Teil der in AP 2 identifizierten Bewertungsdimensionen nicht und ermöglichen damit kein realistisches Abbild der vielfältigen Auswirkungen, die mit dem Einsatz von ITS-Maßnahmen(-bündeln) einhergehen. Mit dem prozessorientierten multikriteriellen Entscheidungsmodell und den Unterstützungsleistungen konnte die erwähnte Forschungslücke geschlossen werden.

Eine dieser Unterstützungsleistungen war die Erweiterung der Prozessmodellierungssprache, die ebenfalls in den Aufgabebereich von MEBITS fiel und durch Extensions des Standards XES 2.0 und der Geschäftsprozessmodellierungssprache BPMN 2.0 realisiert wurde. Diese Erweiterungen bildeten nicht nur eine notwendige Grundlage für die Prozessorientierung

der Bewertung von ITS-Maßnahmen(-bündeln), sondern fungieren zugleich als Quelle von Prozessdaten/-informationen und als Schnittstelle zur Geschäftspraxis.

Die Integration des multikriteriellen Entscheidungsmodells sowohl in das skalierbare Vorgehensmodell als auch in das IT-Werkzeug war aus praktischer Sicht besonders wichtig, da es Praktikern den Zugang zum Entscheidungsmodell erleichterte und den manuellen Bewertungsaufwand so gering wie möglich hielt. Zusätzlich boten die erarbeiteten Umsetzungs- und Anwendungshilfen für das multikriterielle Entscheidungsmodell eine angemessene Hilfestellung für den praktischen Einsatz. Darüber hinaus war die Begleitung und Durchführung von Fallstudien nötig, um das Modell in realistischen Anwendungsszenarien zu erproben und praxisnah an den spezifischen Bedürfnissen und Anforderungen von Unternehmen auszurichten.

Die Arbeit im Teilvorhaben MEBITS und die Kollaboration zwischen den Projektpartnern waren in hohem Maße zielorientiert. Dies trug maßgeblich zur Sicherung des Projekterfolgs, zur Erreichung der gesetzten Meilensteine und zur Ergebnisrealisierung bei. Wie bereits erwähnt, konnte der Meilenstein 1, der im Verantwortungsbereich der MLU lag, problemlos und vollumfänglich eingehalten werden. Auch die Meilensteine 2, 3 und 4, deren Verantwortlichkeit bei den Projektpartnern der UPB, MSU und RPD lag, wurden allesamt eingehalten und können in den jeweiligen Abschlussberichten eingesehen werden.

6. Verwertbarkeit der Ergebnisse

Im Rahmen des Teilvorhabens MEBITS wurden zahlreiche Ergebnisse erzielt, die auch zukünftig von großem theoretischem und praktischem Nutzen sein werden und auf die sich mithilfe zukünftiger Forschung sinnvoll aufbauen lässt. Konkret lassen sich aus unserer Perspektive sechs Aspekte der Verwertbarkeit der Ergebnisse aus dem Teilvorhaben ableiten:

1. **Nutzung und Erweiterung des Katalogs von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen sowie von kritischen fachlichen Anforderungen, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden:** Der im Projekt entwickelte Katalog bietet eine solide Basis für den Einsatz von Bewertungsverfahren zur multikriteriellen ITS-Bewertung. In der Praxis kann dieser Katalog bereits eingesetzt und individuell, je nach Unternehmensgröße, Branche und in Abhängigkeit der jeweiligen Ziele, spezifiziert werden. Der Katalog kann zudem in zukünftiger Forschung um weitere Einflussgrößen, Dimensionen und Anforderungen ergänzt werden.
2. **Nutzung, Anpassung und Erweiterung des multikriteriellen Entscheidungsmodells:** Das multikriterielle Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln) kann praktisch bereits eingesetzt und individuell angepasst werden. Anhand der erfolgreichen Fallstudien mit MSU (Smart Meter) und RPD (Gesundheit) konnte praktisch gezeigt werden, dass ein Einsatz auch in völlig unterschiedlichen Branchen problemlos möglich ist. Die zukünftige Anwendung in weiteren Branchen und Szenarien offenbart vielversprechende Potentiale.
3. **Nutzung, Anpassung und Erweiterung der Extensions von BPMN 2.0 und XES 2.0:** Die entwickelten Extensions sind praktisch nutzbar und können, im Einklang mit Punkt 1 dieser Liste, um weitere Dimensionen erweitert werden. Auch eine Adaption innerhalb bestehender Prozessmodellierungs-Tools ist möglich, wie am Beispiel von Signavio gezeigt wurde.
4. **Förderung von Akzeptanz und Anwendung:** Durch die Integration des multikriteriellen Entscheidungsmodells in das Vorgehensmodell und das IT-Werkzeug sowie durch die Erstellung von Umsetzungshilfen konnte die Akzeptanz in der Praxis (bei den Konsortialpartnern und den assoziierten Partnern) gesichert werden. Durch gezielte

Maßnahmen könnte die Akzeptanz und Anwendung noch weiter gefördert werden, wie z.B. durch praxisnahe Schulungen, die Anwendern die Funktionsweise des Modells näherbringt. Regelmäßige Workshops mit Praxispartnern können zudem dazu beitragen, die Bereitschaft zur Nutzung noch weiter zu erhöhen.

5. **Langfristige Nutzung des ProBITS-Competence Centers**: Das verstetigte ProBITS-Competence-Center und der darin etablierte Kompetenzbereich zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen bieten eine wertvolle Plattform für den fortlaufenden Wissensaustausch. Unternehmen können das Kompetenzzentrum langfristig nutzen, um neue Erkenntnisse und Weiterentwicklungen des Entscheidungsmodells zu teilen sowie fachlichen Support zu erhalten, was die nachhaltige Verwertung der Projektergebnisse fördert.
6. **Übertragung des Ansatzes auf andere Themen (abseits der IT-Sicherheit):** Die Vorgehensweise im Gesamtprojekt und der entwickelte prozessorientierte Ansatz ließen sich auch auf andere Themenbereiche (außerhalb der IT-Sicherheit) übertragen. Alle Aktionen, Geschehnisse und Umweltfaktoren, die Auswirkungen auf die Geschäftstätigkeit und damit auch auf Geschäftsprozesse haben, können theoretisch multikriteriell und prozessorientiert bewertet werden. Das projektübergreifende Vorgehen kann somit als Blaupause für neue Anwendungsfelder dienen.

Planungen für die nähere Zukunft (im Sinne eines fortgeschriebenen Verwertungsplans) sind die Folgenden:

- Journal-Publikation der in AP 2 erhobenen Bewertungsdimensionen (erweitert um eine quantitative Relevanzklassifizierung)
- Weitere Forschung im Bereich „Förderung von Akzeptanz und Anwendung“ durch Frau Laura Bauer, M. Sc. und Abschluss einer darauf aufbauenden Dissertation
- Weitere Forschung zu projektnahen Themen (automatische Identifikation von datenschutzrelevanten Aktivitäten in Geschäftsprozessen mit Hilfe von Machine Learning und KI) durch Herrn Leonard Nake, M. Sc. und Abschluss einer darauf aufbauenden Dissertation
- Aufrechterhaltung des Kompetenzbereichs zur prozessorientierten wirtschaftlichen Bewertung von ITS-Maßnahmen(-bündeln)
- Verstetigung der Projektergebnisse in der universitären Lehre (sowohl in wirtschaftsinformatischen als auch in betriebswirtschaftlichen Studiengängen) und Nutzung der aus diesen Ergebnissen entstandenen, neuen Forschungsoptionen für Abschlussarbeiten, (Praxis-)Seminare und Experimente
- Verstetigung der Zusammenarbeit mit MSU und UPB, um die Entwicklung der Demonstratoren zu einem einsetzbaren Produkt weiter voranzutreiben
- Sondierung weiterer praxisnaher Verwertungsoptionen

7. Stand der Wissenschaft & Fortschritt auf dem Gebiet des Vorhabens

Zu Projektbeginn war der Stand der Wissenschaft und Technik im Bereich der ITS-Bewertung traditionell von drei zentralen Strömungen geprägt (Schatz und Bashroush 2017): (1) Ansätze basierend auf dem Return on Investment (ROI), (2) Ansätze basierend auf der Real Options Theory und (3) Ansätze basierend auf der Utility Maximization Theory. Diese Ansätze wurden im Bereich der Informations- und IT-Sicherheit aus einer investitionstheoretischen Sichtweise betrachtet, wie beispielsweise anhand der Spezifikation des ROI für Sicherheitsmaßnahmen – dem Return on Security Investment (RoSI) – sichtbar wird (Sonnenreich et al. 2006). Diese Ansätze sind jedoch technologischen Neuerungen, der zunehmenden Vernetzung und Digitalisierung in vielen Lebens- und Arbeitsbereichen und den damit einhergehenden Anforderungen an Datenschutz und Informationssicherheit, nicht mehr gewachsen. Für die Erfüllung derartiger Anforderungen ist zumeist ein komplexes Bündel von ITS-Maßnahmen nötig, das sowohl hohe Investitionskosten mit sich bringt, als auch in einem hohen Grad die Geschäftsprozesse (und dadurch auch den Geschäftserfolg) von Unternehmen beeinflusst. Aus dem Bereich

des Geschäftsprozessmanagements waren zum Zeitpunkt des Projektbeginns bereits Ansätze bekannt, die sich der Kostenrechnung und Geschäftszielmessung widmen (Magnani und Montesi 2007; Sampathkumaran und Wirsing 2013). Diese wurden jedoch zentriert auf monetäre Werte und somit nicht spezifiziert für mehrdimensionale Bewertungen einerseits und die Bewertung von ITS-Maßnahmen andererseits.

Der zum Zeitpunkt des Projektbeginns bestehende Überblick über den Stand der Wissenschaft wurde in UAP 2.5 durch eine systematische Analyse von Potentialen und Grenzen traditioneller (insb. ROSI-basierter) Ansätze zur ITS-Investitionskostenrechnung ergänzt (siehe Tabelle 3). Zum einen haben die daraus resultierenden Ergebnisse abermals verdeutlicht, dass traditionelle Verfahren einen wesentlichen Teil der in AP 2 identifizierten Bewertungsdimensionen und kritischen fachlichen Anforderungen nicht reflektieren und damit kein realistisches Abbild der vielfältigen Auswirkungen, die mit dem Einsatz von ITS-Maßnahmen einhergehen, erzeugen können. Zum anderen wurde ersichtlich, dass die im Vorhaben anvisierten Aspekte der Bewertung von ITS-Maßnahmen (Mehrdimensionalität und Skalierbarkeit bei gleichzeitiger Prozessorientierung und der Berücksichtigung von Wechselwirkungen zwischen Maßnahmenbündeln) durch keinen Ansatz aus der bestehenden Forschung adressiert und in keinem anderen Projekt aufgegriffen wurden. Nichtsdestotrotz gaben die Ergebnisse aus AP 2.5 einen umfassenden Überblick über die vorhandenen Bewertungsmethoden und wurden als Informationsquelle und Inspiration für die Konzeption des multikriteriellen und prozessorientierten Entscheidungsmodells zur Bewertung von ITS-Maßnahmen(-bündeln) genutzt.

Aus dem Teilprojekt MEBITS gingen zahlreiche Ergebnisse und Implikationen für Wissenschaft und Praxis hervor, die als Fortschritte auf dem Gebiet des Vorhabens klassifiziert werden können:

1. Der in AP 2 neu entwickelte Katalog von Prozesseinflussgrößen und Bewertungsdimensionen von ITS-Maßnahmen sowie von kritischen fachlichen Anforderungen, die an ein multikriterielles Entscheidungsmodell für ITS-Maßnahmen(-bündel) gestellt werden, gibt einen kondensierten Überblick über relevante Aspekte der ITS-Bewertung. Wissenschaft und Praxis können diesen Katalog nutzen, um sich einen Überblick über die Vielzahl von Dimensionen, Einflussgrößen und Anforderungen zu verschaffen, um jeweils individuell relevante Aspekte abzuleiten und darauf aufbauend eigene Verfahren und Ansätze zu entwickeln.
2. Das in AP 3 neu entwickelte, multikriterielle Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln), das die in AP 2 identifizierten Prozesseinflussgrößen und Bewertungsdimensionen berücksichtigt, erweitert den Fokus der traditionellen ITS-Bewertungsverfahren deutlich.
3. Die in AP 3 neu entwickelte Erweiterung von BPMN 2.0 verbessert die Anwendung der Geschäftsprozessmodellierungssprache im Bereich der ITS-Bewertung für Wissenschaft und Praxis.
4. Die in AP 3 neu entwickelte Erweiterung von XES 2.0 erleichtert die Rekonstruktion bewertungsrelevanter Geschäftsprozesse aus Protokolldateien und ermöglicht die Annotation bewertungsrelevanter Daten.
5. Die in AP 4, 5 und 6 vorgenommene Integration des multikriteriellen Entscheidungsmodells sowohl in das skalierbare Vorgehensmodell als auch in das IT-Werkzeug erleichtert die praktische Anwendung und ermöglicht eine aufwandsarme Bewertung von ITS-Maßnahmen(-bündeln).

Der Fortschritt auf dem Gebiet des Vorhabens konnte auch insbesondere noch einmal anhand der vergleichenden retrospektiven Anwendung des RoSI und des multikriteriellen Modells bei der MSU verdeutlicht werden. Am Beispiel des „Clearswift Secure Gateway“ wurde für den RoSI retrospektiv ein negatives Ergebnis berechnet, was bedeutet, dass sich eine Investition in die ITS-Maßnahme monetär eigentlich nicht lohnt. Die MSU hatte die ITS-Maßnahme jedoch schon erfolgreich im Betrieb. Bei Anwendung des multikriteriellen Modells für die ITS-Maßnahme war das Ergebnis größer als das Ergebnis für die Unterlassungsalternative, was bedeutet, dass sich die Investition unter Berücksichtigung der für die MSU relevanten Bewertungsdimensionen lohnt.

8. Erfolgte und geplante Veröffentlichungen

Im Zuge des Teilvorhabens wurden zum Zeitpunkt des Verfassens dieses Abschlussberichts bereits 11 Publikationen veröffentlicht. Eine ausführliche Auflistung ist in Abschnitt 2 dieses Berichts unter “AP 7 – Kommunikation und Diffusion ProBITS” zu finden.

Eine weitere Publikation über die in AP 2 erhobenen Bewertungsdimensionen (erweitert um eine quantitative Relevanzklassifizierung) ist derzeit noch in Planung. Die notwendigen Ergebnisse und Erkenntnisse liegen vor, müssen aber noch in einen Journal-Artikel überführt werden.

9. Das MEBITS-Projekt-Team

Dr. Stephan Kühnel

Dr. Stephan Kühnel ist Habilitand am Lehrstuhl für Wirtschaftsinformatik, insbesondere Betriebliches Informationsmanangement und Leiter einer Forschungsgruppe mit Schwerpunkt auf Design Science Research (DSRG) am Institut für Wirtschaftsinformatik und Operations Research der Martin-Luther-Universität Halle-Wittenberg. Dort arbeitet er als Dozent, Forscher und Evaluationsbeauftragter. Er promovierte 2019 im Fach Wirtschaftsinformatik über Ansätze zur ökonomischen Bewertung von Compliance-Maßnahmen auf Basis von Geschäftsprozessen. Die Ergebnisse seiner Dissertation bildeten die Grundlage für das Projekt ProBITS, im Rahmen dessen er das Teilprojekt MEBITS beantragte, leitete und operativ unterstützte. Neben der Leitung weiterer drittmittelfinanzierter Projekte umfasst seine praktische Erfahrung die Arbeit als Data Analyst und Data Scientist, sowie die Beratung von Start-ups, Kleinunternehmen und Verbänden bei der Umsetzung regulatorischer Anforderungen. Zu seinen Forschungsinteressen gehören aktuelle Herausforderungen in den Bereichen Informationssicherheit und Compliance, Data-Science-Projektmodelle sowie Design-Science-Forschung in einer Vielzahl von Anwendungsbereichen (z. B. Augmented Reality, Cloud Computing, E-Health). Seine Forschungsarbeiten wurden in Zeitschriften wie ACM Computing Surveys, Business & Information Systems Engineering, Computers & Security, Journal of Decision Systems und Pacific Asia Journal of the Association for Information Systems sowie in führenden, begutachteten Tagungsbänden wie der European Conference on Information Systems, der International Conference on Conceptual Modeling und der International Conference on Business Process Management veröffentlicht.

Laura Bauer (geb. Niedzela), M. Sc.

Laura Bauer ist Doktorandin, wissenschaftliche Mitarbeiterin und Projektmanagerin am Lehrstuhl für Wirtschaftsinformatik, insbesondere Betriebliches Informationsmanagement an der Martin-Luther-Universität Halle-Wittenberg. Ihre Forschungsschwerpunkte liegen im Bereich der Informationssicherheit und IT-Governance. Konkret forscht sie zu Bewertungs- und Entscheidungsmodellen für Informationssicherheitsinvestitionen in Verbindung mit Akzeptanzforschung. Sie integriert die Ergebnisse ihrer Forschung in Herausforderungen des Design Science Research. Ihre Arbeit wurde in zahlreichen von wissenschaftlichen Experten begutachteten Tagungsbänden, wie der Internationalen Konferenz für Wirtschaftsinformatik (WI), Americas Conference on Information Systems (AMCIS), Pacific-Asia Conference on Information Systems (PACIS), sowie im anerkannten Pacific Asia Journal of the Association

for Information Systems (PAJAIS) veröffentlicht. Im Projekt ProBITS war Laura Bauer als IT-Projektmanagerin für das Teilvorhaben MEBITS zuständig. In dieser Rolle übernahm sie sowohl strategische als auch operative Aufgaben und koordinierte die Aktivitäten des Teilprojekts.

Leonard Nake, M. Sc.

Leonard Nake ist Doktorand und wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik, insbesondere Betriebliches Informationsmanagement an der Martin-Luther-Universität Halle-Wittenberg. Er forscht über unterschiedliche Aspekte des Geschäftsprozessmanagements, unter anderem zu Compliance in Geschäftsprozessen oder Process Mining. Er veröffentlichte bereits auf internationalen Konferenzen wie der European Conference on Information Systems (ECIS), der Internationalen Konferenz für Wirtschaftsinformatik (WI) oder der Australasian Conference on Information Systems (ACIS).

Prof. Dr. Stefan Sackmann

Prof. Dr. Sackmann hat seit 2009 die Professur für Wirtschaftsinformatik, insbesondere Betriebliches Informationsmanagement an der Martin-Luther-Universität Halle-Wittenberg inne. Der Lehrstuhl und sein Team forscht und lehrt seit mehreren Jahren in den Bereichen Geschäftsprozess- und Workflow-Management mit einem dezidierten Fokus auf Compliance und wirtschaftliche Bewertung sowie der Erweiterung von Workflow-Management-Systemen. Im Kern stehen in allen Projekten – und so auch im Projekt ProBITS – die effektive und effiziente Steuerung von Prozessen, aber auch der Transfer der gewonnenen Erkenntnisse in die betriebliche Praxis im Fokus. Mehrere der von Prof. Sackmann entwickelten und geleiteten Projekte wurden bislang durch das BMBF und die DFG gefördert (siehe https://informationsmanagement.wiwi.uni-halle.de/projekte/).

10. Literaturverzeichnis

Baskerville, Richard; Pries-Heje, Jan (2010): Explanatory Design Theory. In: *Bus Inf Syst Eng* 2 (5), S. 271–282. DOI: 10.1007/s12599-010-0118-4.

Bauer, L.; Kuehnel, S.; Nastjuk, I.; Nake, L.; Seidel, H. (2024a): Multiple-Criteria Decisions for Information Security - A Case Study of Volkswagen Financial Services AG. In: *Wirtschaftsinformatik 2024 Proceedings, 19th International Conference on Wirtschaftsinformatik*, Artikel 56. Online verfügbar unter https://aisel.aisnet.org/wi2024/56/.

Bauer, Laura (2024): A Literature-Driven Design Theory for Multiple-Criteria Assessment Tools for Information Security Investments. In: *Wirtschaftsinformatik 2024 Proceedings*, Artikel 125.

Bauer, Laura; Kühnel, Stephan; Nastjuk, Ilja; Sackmann, Stefan (2024b): A Multiple-Method Study on Acceptance Factors of Economic Assessment Approaches for Information Security Investments. In: *Pacific Asia Journal of the Association for Information Systems* 16 (4), Artikel 2. Online verfügbar unter ttps://aisel.aisnet.org/pajais/vol16/iss4/2.

Becker, Jörg; Delfmann, Patrick; Dietrich, Hanns-Alexander; Steinhorst, Matthias; Eggert, Mathias (2016): Business process compliance checking – applying and evaluating a generic pattern matching approach for conceptual models in the financial sector. In: *Information Systems Frontiers* 18 (2), S. 359–405. DOI: 10.1007/s10796-014-9529-y.

Benlian, Alexander (2010): Which Type of Software Model is First Choice? An AHP-based Comparison of Traditional, Open-Source, and On-Demand Office Suites on the Fulfillment of Evaluation Criteria. In: *ECIS 2010 Proceedings*, Artikel 149. Online verfügbar unter https://aisel.aisnet.org/ecis2010/149.

Bodin, Lawrence D.; Gordon, Lawrence A.; Loeb, Martin P. (2005): Evaluating information security investments using the analytic hierarchy process. In: *Commun. ACM* 48 (2), S. 78–83. DOI: 10.1145/1042091.1042094.

Chen, Pei-Chi; Chern, Ching-Chin; Chen, Chung-Yang; and Tzeng, Gwo-Hshiung (2013): IT Portfolio Investment Evaluation on E-Commerce Solution Alternatives. In: *PACIS 2013 Proceedings.*, Artikel 122. Online verfügbar unter https://aisel.aisnet.org/pacis2013/122.

Fu, Katherine K.; Yang, Maria C.; Wood, Kristin L. (2016): Design Principles. Literature Review, Analysis, and Future Directions. In: *J. Mech. Des* 138 (10), S. 101103. DOI: 10.1115/1.4034105.

Günther, Christian W.; Verbeek, Eric (2014): XES Standard Definition 2.0. 2. Aufl. Eindhoven. Online verfügbar unter http://www.xes-standard.org/_media/xes/xesstandarddefinition-2.0.pdf, zuletzt geprüft am 27.02.2019.

Hengstler, Sebastian; Kuehnel, Stephan; Masuch, Kristin; Nastjuk, Ilja; Trang, Simon (2023): Should i really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior. In: *Computers & Security* 133, S. 103370. DOI: 10.1016/j.cose.2023.103370.

Kuehnel, S.; Sackmann, S.; Damarowsky, J.; Böhmer, M. (2022): EconBPC: A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes. In: *20th International Conference on Business Process Management (BPM 2022), Proceedings of the Best Dissertation Award, Doctoral Consortium, and Demonstration & Resources Track* (3216), S. 127–131. Online verfügbar unter http://ceur-ws.org/Vol-3216/paper_252.pdf.

Kuehnel, Stephan; Zasada, Andrea (2018): An Approach Toward the Economic Assessment of Business Process Compliance. In: Carson Woo, Jiaheng Lu, Zhanhuai Li, Tok Wang Ling, Guoliang Li und Mong Li Lee (Hg.): Advances in Conceptual Modeling. ER 2018 Workshops Emp-ER, MoBiD, MREBA, QMMQ, SCME, Xi'an, China, October 22-25, 2018, Proceedings. Cham: Springer International Publishing (11158), S. 228–238.

Kühnel, Stephan; Sackmann, Stefan; Seyffarth, Tobias (2017): Effizienzorientiertes Risikomanagement für Business Process Compliance. In: *HMD* 54 (1), S. 124–145. DOI: 10.1365/s40702-016-0284-z.

Kühnel, Stephan; Sackmann, Stefan; Trang, Simon; Nastjuk, Ilja; Matschak, Tizian; Niedzela, Laura; Nake, Leonard (2021): Towards a Business Process-based Economic Evaluation and Selection of IT Security Measures. In: *Proceedings of the First International Workshop on Current Compliance Issues in Information Systems Research (CIISR'21), Co-located with the 16th International Conference on Wirtschaftsinformatik (WI'21)', Essen, Germany (online), CEUR-WS Vol-2966*, S. 7–21. Online verfügbar unter https://ceur-ws.org/Vol-2966/paper1.pdf.

Kühnel, Stephan; Trang, Simon; Lindner, Sebastian (2019): Conceptualization, Design, and Implementation of EconBPC – A Software Artifact for the Economic Analysis of Business Process Compliance. In: Alberto H. F. Laender, Barbara Pernici und Ee-Peng Lim (Hg.): Conceptual Modeling. 38th International Conference, ER 2019, Salvador, Brazil, November 4–7, 2019, Proceedings. 1st ed. 2019 (Information Systems and Applications, incl. Internet/Web, and HCI), S. 378–386.

La Rosa, Marcello (2015): Strategic business process management. In: *International Conference on Software and Systems Process (ICSSP)*. DOI: 10.1145/2785592.2785620.

Magnani, Matteo; Montesi, Danilo (2007): BPMN. How Much Does It Cost? An Incremental Approach. In: Gustavo Alonso, Peter Dadam und Michael Rosemann (Hg.): Business process management. 5th international conference, BPM 2007, Brisbane, Australia, September 24 - 28, 2007 ; proceedings, Bd. 4714. Berlin: Springer (Lecture Notes in Computer Science, 4714), S. 80–87.

Matschak, Tizian; Nastjuk, Ilja; Niedzela, Laura; Kuehnel, Stephan; Trang, Simon (2023): A Process-Based Approach to Information Security Investment Evaluation: Design, Implementation, and Evaluation. In: *AMCIS 2023 Proceedings*, Artikel 30. Online verfügbar unter https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/30.

Mayer, Joerg Hans; Quick, Reiner; Friedrich, Christian (2018): Towards a more situated IS design by prioritizing use situations. In: *Proceedings of the European Conference on Information Systems (ECIS)*, Artikel 64.

Nake, Leonard (2023): Integrating IT Security Aspects into Business Process Models: A Taxonomy of BPMN Extensions. In: *Proceedings of the 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR 2023), Co-located with the 18th International Conference on Wirtschaftsinformatik (WI 2023)*, S. 38–48.

Nake, Leonard; Kuehnel, Stephan; Bauer, Laura; Sackmann, Stefan (2023): Towards Identifying GDPR-Critical Tasks in Textual Business Process Descriptions. In: *INFORMATIK 2023 - Designing Futures: Zukünfte gestalten*, S. 1895–1908. DOI: 10.18420/INF2023_191.

Niedzela, Laura; Kuehnel, Stephan; Nastjuk, Ilja; Matschak, Tizian; Sackmann, Stefan; Trang, Simon (2023): A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions. In: *AMCIS 2023 Proceedings*, Artikel 16. Online verfügbar unter https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/16.

Niedzela, Laura; Nake, Leonard; Matschak, Tizian (2022): Categories of Approaches for IT Security Investment Decisions: A systematic literature review. In: *Wirtschaftsinformatik 2022 Proceedings*, Artikel 4. Online verfügbar unter https://aisel.aisnet.org/wi2022/workshops/workshops/4.

Saaty, Thomas L. (2008): Decision making with the analytic hierarchy process. In: *International Journal of Services Sciences* 1 (1), S. 83–98. Online verfügbar unter https://doi.org/10.1504/IJSSci.2008.01759.

Sadiq, Shazia; Governatori, Guido (2015): Managing Regulatory Compliance in Business Processes. In: Jan Vom Brocke und Michael Rosemann (Hg.): Handbook on Business Process Management 2. Strategic Alignment, Governance, People and Culture. 2nd ed. 2015. Berlin, Heidelberg, s.l.: Springer Berlin Heidelberg (International Handbooks on Information Systems), S. 265–288.

Sampathkumaran, Partha B.; Wirsing, Martin (2013): Financial Evaluation and Optimization of Business Processes. In: *IJISMD* 4 (2), S. 91–120. DOI: 10.4018/jismd.2013040105.

Schatz, Daniel; Bashroush, Rabih (2017): Economic valuation for information security investment: a systematic literature review. In: *Information Systems Frontiers* 19 (5), S. 1205–1228. DOI: 10.1007/s10796-016-9648-8.

Sonnenreich, Wes; Albanese, Jason; Stout, Bruce (2006): Return On Security Investment (ROSI): A Practical Quantitative Model. In: *Journal of Research and Practice in Information Technology* 38 (1), S. 45–56.