

Prozess-orientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen (ProBITS)

Sachbericht zum Abschlussnachweis

Zuwendungsempfänger:	Förderkennzeichen:
Rezeptprüfstelle Duderstadt GmbH (RPD)	16KIS1333
Titel des Teilvorhabens:	
Demonstration der Effektivität von ProBITS am Beispiel Gesundheit und Datenschutz	
Projektleiter: Robert Schmidthals	
E-Mail: robert.schmidthals@rpd.de	Tel.: 05527/9852-74
Laufzeit des Vorhabens:	
von: 01.04.2021 bis: 30.06.2024	
Berichtszeitraum des Vorhabens:	Berichtsdatum:
von: 01.04.2023 bis: 30.06.2024	vom: 19.12.2024

1 Übersicht Projektstruktur

Das Konsortium setzte sich aus folgenden Partnern zusammen: Universität Paderborn (UPB), Martin-Luther-Universität Halle-Wittenberg (MLU), Rezeptprüfstelle Duderstadt GmbH (RPD) und msu solutions GmbH (MSU). Die Zusammenarbeit erfolgte konstruktiv, ergebnisorientiert und verlief somit sehr gut.

Prof. Dr. Simon Trang ist im Projektverlauf mit dem ehemaligen Lehrstuhl für Informationssicherheit und Compliance der Georg-August-Universität Göttingen (GAU) an den Lehrstuhl für Wirtschaftsinformatik, insbesondere Nachhaltigkeit der UPB gewechselt.

Die einzelnen Partner waren entsprechend ihrer Kompetenzen im Projektvorhaben verordnet. Prof. Dr. Sackmann und Dr. Kühnel hatten gemeinsam mit dem Team des Lehrstuhls für Betriebliches Informationsmanagement der MLU die Leitung der

Arbeitspakete (AP) 2 und AP 3 inne. Prof. Dr. Trang und sein Team des Lehrstuhls für Wirtschaftsinformatik, insbesondere Nachhaltigkeit an der UPB leiteten die APs 1, 4, 5 und 7. Die Praxispartner RPD und MSU waren hauptsächlich bei der Anwendung, Evaluation und Weiterentwicklung von ProBITS involviert (AP 6).

2 Motivation und Zielstellung

IT-Sicherheitsmaßnahmen (ITS-Maßnahmen), die einen weitreichenden Einfluss auf Geschäftsprozesse haben, lassen sich mit "klassischen" Bewertungsansätzen der Investitionskostenrechnung, wie bspw. dem Return on Security Investment (ROSI), nur unzureichend bewerten. ProBITS wird hierfür einen innovativen Ansatz bereitstellen, um zukünftig eine geschäftsprozessorientierte Bewertung von ITS-Maßnahmen methodisch, mehrdimensional, skalierbar und werkzeuggestützt zu ermöglichen. Mit ProBITS werden insbesondere Entscheider*innen und KMUs in die Lage versetzt, Entscheidungen über die Auswahl von ITS-Maßnahmen unter Berücksichtigung von Kosten, prozessualen Aufwänden und Nutzen treffen zu können.

Hierfür umfasst ProBITS insgesamt vier Bausteine: (1) ein multikriterielles Entscheidungsmodell, mit dem sich ITS-Maßnahmen bewerten und auswählen lassen, sowie drei Unterstützungsleistungen in Form der (2) Erweiterung einer Prozessmodellierungssprache, (3) eines Vorgehensmodells und (4) eines IT-Werkzeugs. Das ProBITS-Vorhaben umfasst zudem mehrere Demonstratoren. Mit „ProBITS deckt auf“ wird die Effektivität existierender Verfahren (wie dem ROSI) auf Basis vergangener ITS-Maßnahmen analysiert. „ProBITS in Aktion“ dient hingegen der Demonstration der Effektivität der ProBITS-Bausteine sowie deren kontinuierlicher Weiterentwicklung.

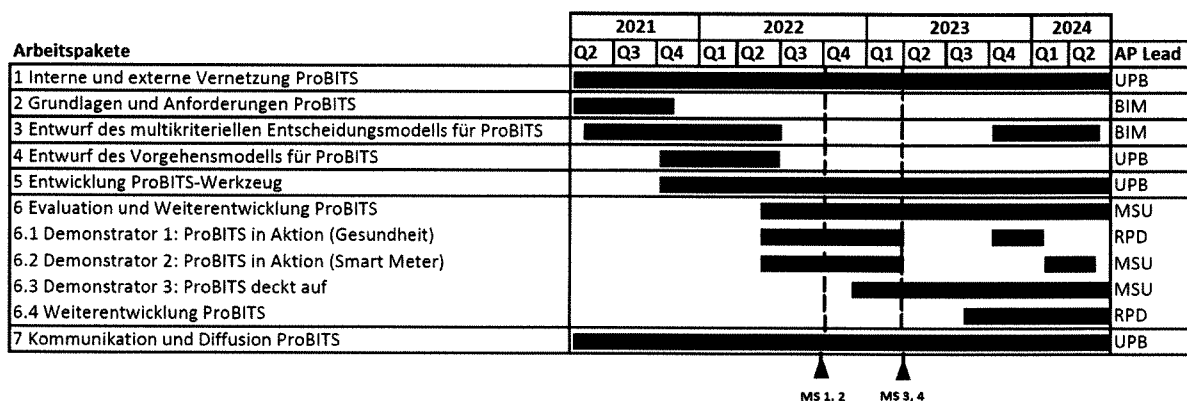


Abbildung 1: Übersicht zum Vorhaben „ProBITS: Prozess-orientierte wirtschaftliche Bewertung und Auswahl von ITS-Maßnahmen

Das Verbundvorhaben ProBITS setzt sich aus vier Teilvorhaben zusammen. Während sich die zwei universitären Teilvorhaben (UPB, MLU) primär mit der Entwicklung von ProBITS beschäftigen, befassen sich die zwei Teilvorhaben der Anwendungspartner (MSU, RPD) mit der Demonstration und Evaluation:

- TVB 1 (Uni Halle Wittenberg): Multikriterielles Entscheidungsmodell zur prozessorientierten wirtschaftlichen Bewertung und Analyse von IT-Sicherheitsmaßnahmen

- TVB 2 (Uni Paderborn): ProBITS einfach gemacht: Analyse von Adaptionsbarrieren und Entwicklung von Werkzeugen zur effektiven Einführung und Umsetzung
- TVB 3 (MSU consulting): ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen
- TVB 4 (RPD): ProBITS in Aktion: Demonstration der Effektivität von ProBITS am Beispiel Gesundheit und Datenschutz

2.1 Motivation

Technologische Innovationen wie Cloud-Computing und Big Data-Analytics bieten erhebliches Potenzial zur Erhaltung und Stärkung der Wettbewerbsfähigkeit. Gleichzeitig bringen diese Technologien neue Risiken mit sich, wie etwa Probleme bei der Datensicherheit, Cloud-Hacking oder Datenschutz. Um diesen Risiken entgegenzuwirken, legen sowohl Gesetzgeber als auch Unternehmen umfangreiche Anforderungen an die IT-Sicherheit fest. Diese Anforderungen finden sich in internen Vorgaben zur Informationssicherheits-Governance (wie bspw. allgemeine Richtlinien zur Authentifizierung oder zur Datenklassifizierung und -handhabung), in branchenspezifischen Regelungen (wie bspw. PSD2 für Banken oder KRITIS für Betreiber kritischer Infrastrukturen) sowie in branchenübergreifenden Vorschriften (wie bspw. DSGVO oder IT-Sicherheitsgesetz). Diese Anforderungen müssen im Unternehmenskontext durch geeignete ITS-Maßnahmen umgesetzt werden.

Die Umsetzung solcher Anforderungen erfordert meist ein komplexes Bündel von ITS-Maßnahmen, das sowohl hohe Investitionskosten verursacht als auch die Geschäftsprozesse von Unternehmen erheblich beeinflusst. Artikel 32 (1) der DSGVO verlangt beispielsweise, dass geeignete technische und organisatorische Maßnahmen ergriffen werden, um die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit bei der Verarbeitung personenbezogener Daten zu gewährleisten. Für die Umsetzung dieser Anforderungen sind sowohl technische Maßnahmen, wie etwa die Verschlüsselung und Pseudonymisierung personenbezogener Daten, als auch prozessuale Konfigurationen, wie Kontrollen zur Sicherstellung von Compliance oder Regelungen zur Verfügbarkeit von Informationen in Prozessschritten, notwendig. Solche technischen und prozessualen Maßnahmen führen zu hohen Aufwänden (Kühnel et al. 2017; Sonnenreich et al. 2006), weshalb die Einhaltung von IT-Sicherheitsanforderungen als kostenintensive Aufgabe (La Rosa 2015; Sadiq and Governatori 2015) und sogar als „heftiger Kostentreiber“ (Becker et al. 2016) gilt. Um die Profitabilität eines Unternehmens durch die Umsetzung von ITS-Maßnahmen(-bündeln) nicht zu beeinträchtigen, müssen daher geeignete Handlungsalternativen identifiziert und anhand wirtschaftlicher Kriterien ausgewählt werden. Ansätze zur ganzheitlichen Bewertung und Auswahl solcher komplexer Bündel von ITS-Maßnahmen und deren Wechselwirkungen mit Geschäftsprozessen sind daher notwendig, um Unternehmen die Auswahl der effektivsten ITS-Maßnahmen unter ökonomischen Gesichtspunkten zu ermöglichen.

Betrachtet man den aktuellen Stand der Forschung zu Bewertungsverfahren für IT-Sicherheit, lassen sich drei zentrale Ansätze identifizieren, die in Kapitel 6 ausführlich behandelt werden. Diese Ansätze basieren auf der Investitionstheorie und konzentrieren sich auf die eindimensionale Bewertung einzelner ITS-Maßnahmen (wie bspw. die Implementierung einer Firewall), wobei direkt zurechenbare und rein monetäre Kosten- und Nutzenaspekte berücksichtigt werden. Bestehende Verfahren

stoßen jedoch an ihre Grenzen, wenn es darum geht, ITS-Maßnahmen zur Erfüllung aktueller IT-Sicherheitsanforderungen und deren Wechselwirkungen mit Geschäftsprozessen zu bewerten.

2.2 Zielstellung

Das Projekt ProBITS zielt darauf ab, die Grenzen bestehender Verfahren bei der Bewertung komplexer ITS-Maßnahmen(-bündel) zu überwinden und stützt sich dabei auf die Methoden des modernen Geschäftsprozessmanagements. Dabei bieten Geschäftsprozessmodelle einen detaillierten Einblick in die Ablauf- und Organisationsstrukturen, die den ITS-Maßnahmen(-bündeln) zugrunde liegen, und eröffnen somit neue Möglichkeiten zur Analyse und Verbesserung. Die Bewertung von prozessbasierten ITS-Maßnahmen (d.h. ITS-Aktivitäten und ITS-Aktivitätssequenzen innerhalb der Geschäftsprozesse) im Hinblick auf ihre Wirtschaftlichkeit erfordert einen spezifischen Bewertungsansatz, um Ineffizienzen zu identifizieren und Prozessverbesserungen aufzuzeigen. Im Rahmen des Projekts ProBITS wird ein solcher Ansatz konzipiert, evaluiert und als Software-Artefakt implementiert.

Da sowohl Großunternehmen als auch KMUs von ITS-Anforderungen betroffen sind, KMUs jedoch häufig nur begrenzte Ressourcen (in den Bereichen Finanzen, Personal und Daten) zur Verfügung stehen, wird ProBITS explizit unter Berücksichtigung der Skalierbarkeit für verschiedene Unternehmensgrößen entwickelt. Neben der multidimensionalen werkzeuggestützten Bewertungsmethode soll ein Vorgehensmodell realisiert werden, das die Implementierung des ProBITS-Ansatzes in Unternehmen unterschiedlicher Größe unterstützt. Die Entwicklung und Evaluation von ProBITS erfolgt daher in enger Zusammenarbeit mit KMUs als Projektpartner und Großunternehmen als assoziierte Partner. Bei der Evaluation werden zwei Szenarien berücksichtigt:

1. **Demonstration der Anwendbarkeit:** Entlang des Vorgehensmodells wird der ProBITS Ansatz am Beispiel der Implementierung einer komplexen ITS-Anforderung in KMUs demonstriert. Dabei erfolgt sowohl die Anwendung des Bewertungsverfahrens auf die verfügbaren ITS-Maßnahmen(-bündel) als auch die Auswahl der besten Handlungsalternative unter Berücksichtigung ökonomischer Kriterien.
2. **Vergleichende Evaluation (retrospektiv):** Auf Basis historischer Daten werden vergangene ITS-Maßnahmen(-bündel) sowohl mit bestehenden investitionstheoretischen Verfahren wie dem ROSI-Ansatz als auch mit dem ProBITS-Ansatz retrospektiv bewertet. Die Ergebnisse der Bewertungen werden dann zu Evaluationszwecken miteinander verglichen.

Die Entwicklung und Evaluation von ProBITS erfolgen in den Kontexten Gesundheit und Datenschutz sowie Smart Meter. Der Gesundheits- und Datenschutzbereich eignet sich aus den folgenden zwei Gründen: Erstens zeichnet sich die Gesundheitsbranche durch einen besonders hohen Schutzbedarf der verarbeiteten Informationen aus, da es sich meist um Patientendaten handelt. Gleichzeitig ist die Gesundheitsbranche durch einen hohen Anteil an KMUs geprägt. Daher spielt die ökonomische Auswahl von ITS-Maßnahmen eine entscheidende Rolle für viele Unternehmen und Organisationen in dieser Branche. Somit ist die Gesundheitsbranche besonders geeignet. Es wird erwartet, dass bereits während der Projektphase andere KMUs in der Gesundheitsbranche von den gewonnenen

Erkenntnissen und Design-Artefakten profitieren können. Der zweite Fokus liegt auf dem Bereich Smart Meter. Smart Meter Anwendungen sind vernetzte Produkte, die kritische Informationen üblicherweise über öffentliche Netze austauschen. Auch hier besteht ein hoher Schutzbedarf für die verarbeiteten Informationen. ITS-Maßnahmen betreffen nicht nur interne Prozesse, sondern sind auch bei der Produktentwicklung von großer Bedeutung. Darüber hinaus repräsentieren Smart Meter-Technologien andere IoT-Technologien und die Digitalisierung der deutschen Industrie.

Das Verbundvorhaben verfolgt bei der Umsetzung des Projekts sieben übergreifende Gesamtziele (GZ), die in der folgenden Tabelle dargestellt sind. Die Gesamtziele dienen als Rahmen für den Arbeitsplan und werden im folgenden Kapitel auf wissenschaftliche und technische Arbeitsziele bezogen.

Tabelle 1. Übersicht zu den Gesamtzielen des Vorhabens

Übergreifende Gesamtziele des Gesamtvorhabens der Verbundpartner	
GZ 1	Analyse und Evaluation der Effektivität bisheriger Verfahren zur Bewertung von ITS-Maßnahmen
GZ 2	Identifikation von Prozesseinflussgrößen, fachlichen Anforderungen, Bewertungsdimensionen und Anwendungsbarrieren von Verfahren zur Bewertung von ITS-Maßnahmen mit einem Fokus auf KMUs
GZ 3	Bereitstellung eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)
GZ 4	Bereitstellung von notwendigen Unterstützungsleistungen für die Einführung eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln) mit einem Fokus auf KMUs
GZ 5	Demonstration der Anwendbarkeit und Effektivität von ProBITS
GZ 6	Verstetigung eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln)
GZ 7	Steigerung der Qualifikation und Awareness von Unternehmen (insb. KMUs), Mitarbeitern, Studierenden und Doktoranden im Bereich IT-Sicherheit

3 Ablauf des Vorhabens

Das Projekt ProBITS wurde durch die RPD über einen Zeitraum von 3 Jahren und 3 Monaten bearbeitet. Eine Übersicht über die Arbeitspakete und ihre Bearbeitungsdauer, kann der nachfolgenden Grafik entnommen werden. In den darauffolgenden Unterkapiteln werden jeweils die Kern-Tätigkeiten und Ergebnisse der einzelnen Arbeitspakete beschrieben.

AP 1 – Interne und externe Vernetzung durch das Competence Center (CC) ProBITS

Bezug zu Gesamtziel: GZ 1 - GZ 5

Ziel der RPD als Praxispartner war es, durch aktive Mitarbeit am Aufbau des Competence Centers die Grundlagen für eine gemeinsame Kommunikation zu schaffen und ProBITS nachhaltig zu etablieren. Dazu wurde durch die RPD an internen und externen Projekttreffen teilgenommen, um Projektergebnisse auszutauschen und zu diskutieren. Dieses Vorgehen wurde zielorientiert durchgeführt, um die Aktualität sowie die Erfüllung der Praxisanforderungen an ProBITS zu gewährleisten.

Das Arbeitspaket fand über die gesamte Projektdauer hinweg statt und das Ziel wurde aus Sicht der RPD erreicht.

Die externe Kommunikation und Vernetzung des ProBITS-Projekts wurde vorrangig durch die Partner der UPB betrieben.

Zur Vermeidung von Redundanzen verweisen wir daher auf den Sachbericht zum Abschlussnachweis der UPB.

AP 2 – Grundlagen und Anforderungen ProBITS

Bezug zu Gesamtziel: GZ 1, GZ 2

Ein Ziel der RPD als Praxispartner war die Identifikation von praxistauglichen und ökonomischen Anforderungen, die an ProBITS gestellt werden. Ein weiteres Ziel war es, die Stärken und Schwächen (Nutzungsbarrieren) bisheriger Verfahren zur Bewertung von ITS-Maßnahmen aus Perspektive eines KMU-Anwenders zu identifizieren.

Durch den Austausch und die Einblicke in die Praxisperspektive zu Dimensionen, Einflussgrößen und Entscheidungsfaktoren von ITS-Maßnahmen wurden die MLU & Prof. Dr. Trang und sein Team des Lehrstuhls für Wirtschaftsinformatik, insbesondere Nachhaltigkeit bei der Bearbeitung von Unterarbeitspaketen unterstützt. Außerdem wurde im Rahmen von Fokusgruppenworkshops eine Fallstudie erarbeitet, die zur Anwendung und Evaluation des Entscheidungs- und Vorgehensmodells diente und im Laufe des Projekts flexibel erweitert werden konnte.

Aus der Sicht des Praxispartners RPD wurden die Ziele im Jahr 2021 erreicht. Vgl. dazu auch die im Abschnitt 4 „Wichtige Ergebnisse“ dargestellten Ergebnisse.

Durch die im Verlauf des Jahres 2022 erarbeiteten Ergebnisse in AP 4 und AP 5 wurde allerdings festgestellt, dass Anpassungen an den in AP 2 bereits identifizierten Prozessdimensionen nötig waren, damit diese erfolgreich im Vorgehensmodell und IT-Tool zur Anwendung gebracht werden konnten. Vor diesem Hintergrund hat die RPD die Weiterentwicklung von Prozesseinflussdimensionen sowie konkreten Praxisbeispielen (zu Prozessdimensionen) durch die Teilnahme an der Delphi-Studie unterstützt. Darüber hinaus wurde eine Kategorisierung der Einflussdimensionen erarbeitet und eine Priorisierung der Dimensionen durchgeführt.

Diese Prozessdimensionen wurden an einem ersten Prototyp des IT-Tools (V.1) getestet. Es wurde davon ausgegangen, dass weitere Anpassungen der Prozessdimensionen auf Basis der IT-Tool Entwicklung und Evaluation nötig sein könnten.

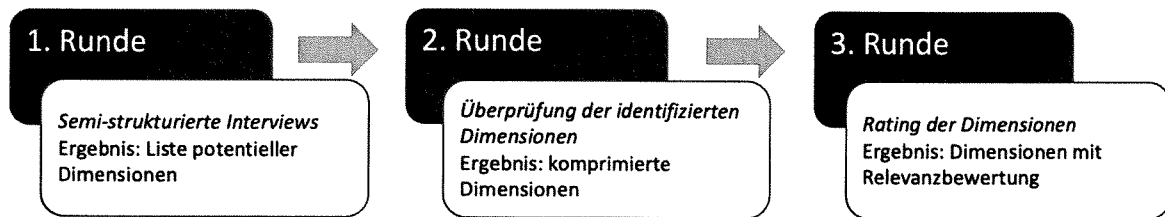


Abbildung 3: Ablauf der Delphi-Studie

AP 3 - Entwurf des multikriteriellen Entscheidungsmodells für ProBITS

Bezug zu Gesamtziel: GZ2, GZ3

In AP 3 wurde in UAP 3.5 das multikriterielle Entscheidungsmodell entwickelt und evaluiert. Dabei ist es zu personellen Engpässen und veränderndem Anwendungskontext gekommen. Da das Entscheidungsmodell das Herz der ProBITS-Methode bildet, wurde das Ziel verfolgt, hier alle relevanten Aspekte umzusetzen, auch wenn dies zu einer Verzögerung des Arbeitspaketes führte. Entsprechend wurde im November 2023 ein Verlängerungsantrag gestellt.

Zur Vermeidung von Redundanzen verweisen wir für weitere Details zum AP 3 auf den Sachbericht zum Abschlussnachweis der MLU.

AP 4 – Entwicklung des ProBITS-Vorgehensmodells

Bezug zu Gesamtziel: GZ 4

Ziel der RPD als Praxispartner war es, die praxisorientierte Sicht eines KMU in die Entwicklung des ProBITS-Vorgehensmodells einzubringen und die (Zwischen-) Ergebnisse des Vorgehensmodells zu evaluieren.

Dazu wurde mit Unterstützung der RPD ein Grobkonzept des Vorgehensmodells erstellt. Hierbei unterstützte die RPD primär mit Praktiker-Interviews, um eine Grundlage an Anforderungen für die weitere Entwicklung des Vorgehensmodells zu liefern. Konkret wurden hier die Anforderungen aus den unterschiedlichen Blickwinkeln eines KMUs betrachtet, sodass die langfristige Etablierung und Diffusion der ProBITS-Methode unterstützt wird.

Vgl. dazu auch die im Abschnitt 4 „Wichtige Ergebnisse“ dargestellten Ergebnisse. Die RPD stand in den folgenden Schritten für einen weiteren Austausch und für die Evaluation der Ergebnisse zur Verfügung.

Durch weitere Tiefen-Interviews anhand konkreter Fallstudien konnte die RPD die Sicht und Anforderungen eines mittelständischen Unternehmens an das Vorgehensmodell zur Erfassung und Bewertung von Prozessdimensionen einbringen. Diese Anforderungen wurden im Rahmen von mehreren Workshops konkretisiert und experimentell erprobt. Die aus der Entwicklung des IT-Tool-

Prototypen gewonnenen Erkenntnisse hatten einen Einfluss auf das initial entwickelte Vorgehensmodell. Im Konkreten gab es eine Diskrepanz zwischen den konzeptionellen Ablaufaktivitäten der Prozessbewertung im Vorgehensmodell und den tatsächlich erforderlichen Schritten (aus Praxissicht und der Integration des Tools in den Arbeitsablauf der Mitarbeiter*innen) für die Bewertung im IT-Tool. Dies konnte zuvor aufgrund der Komplexität und Innovativität einer solchen prozessbasierten Bewertung und die damit verbundene begrenzte theoretische Herleitbarkeit von Anforderungen nicht vorhergesehen werden.

Es war notwendig, das Vorgehensmodell kontinuierlich basierend auf den Entwicklungen des IT-Tools anzupassen.

Das ProBITS-Vorgehensmodell wurde mit den Projektpartnern der UPB in mehreren Workshops beispielhaft und praxisnah angewendet und evaluiert. Dabei konnte die RPD ihr Feedback zur Weiterentwicklung und Finalisierung des Vorgehensmodells beitragen und ist zur Überzeugung gekommen, dass die erzielten Ergebnisse einen Mehrwert für die effiziente Anwendung der ProBITS-Methode liefern.

Zur Vermeidung von Redundanzen vgl. die detaillierte Beschreibung des AP 4 im Sachbericht zum Abschlussnachweis des UPB.

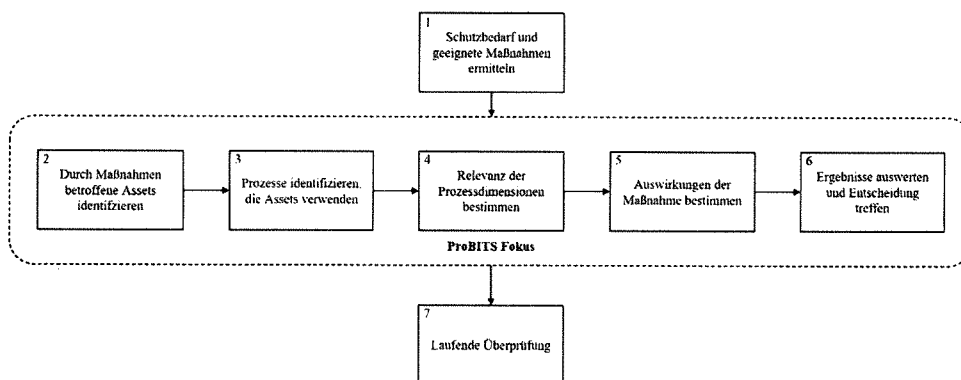


Abbildung 4: ProBITS-Vorgehensmodell

AP 5 – Entwicklung ProBITS-IT-Werkzeug

Bezug zu Gesamtziel: GZ 4

Ziel der RPD als Praxispartner war es, die praxisorientierte Sicht eines KMU in die Entwicklung des ProBITS-Werkzeugs einzubringen. Dadurch sollte ein effizientes Tool entwickelt werden, welches die Grundlage der Entwicklung eines Demonstrators (AP 6) bildete. Aus Unternehmenssicht bestehende fachliche und technische Anforderungen an das ProBITS-Werkzeug sollten in die Entwicklung eingebracht werden.

Zur Bearbeitung des Arbeitspaktes 5 wurde durch Unterstützung bei der Erhebung fachlicher und technischer Anforderungen beigetragen. Dazu wurden entsprechende Interviewpartner*innen zur Verfügung gestellt und weitere Expert*inneninterviews für den Projektverlauf geplant. Die enge Verzahnung von Forschung und Praxis zielte dabei auf möglichst niedrige Adoptionschürden für die ProBITS-Methode und dem dazugehörigen Tool ab.

Die RPD unterstützte weiterhin durch aktive Teilnahme an Workshops sowie durch einen Probelauf und Evaluation der (Zwischen-) Ergebnisse.

Im Rahmen eines iterativen Entwicklungsprozesses wurden relevante Adoptionshürden der ProBITS-Methode und des dazugehörigen IT-Tool identifiziert und dementsprechend konkrete Handlungsempfehlungen abgeleitet. Dadurch wurde sichergestellt, dass relevante Usability-Aspekte sowie die funktionale Integration in den bestehenden Arbeitsalltag von Mitarbeiter*innen (höhere Akzeptanz des Tools) bei der Entwicklung des IT-Tools Anwendung gefunden haben. Zudem hat die RPD bei der Fallstudien-basierten Evaluation des Prototyp V.1 mitgewirkt.

Aus dieser Evaluation sind einige neue Features und Vorschläge für Funktionalitäten und Verbesserungspotenziale hervorgekommen. Diese wurden dann in den weiteren Evaluationszyklen im Rahmen der gegebenen Möglichkeiten umgesetzt.

Im Rahmen des AP 5 unterstützte die RPD zudem bei der technischen und fachlichen Testung des ProBITS-Werkzeugs und bei der daran angeschlossenen technischen Dokumentation. In dem Zuge führte die RPD die bereits im Jahr 2022 begonnene kontinuierliche Evaluation und Weiterentwicklung des IT-Tools fort. Aufgrund der verzögerten Einführung des E-Rezeptes, diese wurde bereits im Verlängerungsantrag aus November 2023 beschrieben, ergaben sich jedoch unvorhersehbare Verzögerungen in der praktischen Testung, Evaluation und Dokumentation des ProBITS-Werkzeugs. Dennoch ermöglichte die gemeinsame Evaluation mit der UPB wie oben beschrieben einige Anpassungen am ProBITS IT-Tool vorzunehmen.

Zur Vermeidung von Redundanzen vgl. für weitere Details zum AP 5 auf den Sachbericht zum Abschlussnachweis der UPB.

ID	Name der Dimension	Kategorie der Dimension	Erstellt am
1	Abstimmungs-/Planungsaufwand	Aktivität	15.11.2023, 11:52:48
2	Durchlaufzeit	Aktivität	15.11.2023, 11:52:48
3	Flexibilität/Anpassungsfähigkeit	Aktivität	15.11.2023, 11:52:48
4	Prozesskomplexität	Aktivität	15.11.2023, 11:52:48
5	Prozessstreuung	Aktivität	15.11.2023, 11:52:48
6	Stabilität/Verfügbarkeit	Aktivität	15.11.2023, 11:52:48
7	Datenqualität	Input	15.11.2023, 11:52:48
8	Datenquantität	Input	15.11.2023, 11:52:48

Abbildung 5: ProBITS IT-Tool V2

AP 6 – Evaluation und Weiterentwicklung ProBITS

zu Gesamtziel: GZ 1, GZ 3, GZ 4, GZ 5, GZ 7

Im AP 6 war die RPD hauptsächlich für die UAPs 6.1 und 6.4 verantwortlich. Das Ziel von UAP 6.1 war die Anwendung und Evaluation der ProBITS-Methode anhand

von Demonstrator 1 „ProBITS in Aktion“ (Gesundheit) – Implementierung des ProBITS-Investitionsentscheidungsprozesses am Beispiel Gesundheit und DSGVO. Ursprünglich war hier eine Demonstration am Fall des E-Rezeptes im Projektplan vorgesehen.

Durch unvorhergesehene Änderungen von Seiten des Gesetzgebers in Bezug auf den bundesweiten Rollout (und Verpflichtung) von E-Rezepten musste jedoch eine alternative Fallstudie entwickelt werden. Dies hat zu zusätzlichem, unvorhergesehenen Arbeitsaufwand geführt.

Auf Basis der Fallstudie des AP2 im Bereich Gesundheit „Datenverarbeitung“ wurde der zu dem Zeitpunkt aktuelle Stand des in AP 4 entwickelten Vorgehensmodells für den Kontext der RPD angepasst und angewendet. In enger Abstimmung mit Mitarbeiter*innen der RPD wurde eine prozessorientierte Modellierung von Handlungsempfehlungen (via BPMN) durchgeführt und das multikriterielle Entscheidungsmodell angewendet. Entlang dieser Arbeitsschritte wurden kontinuierlich Verbesserungspotenziale in Bezug auf das Vorgehensmodell, Entscheidungsmodell, sowie deren Umsetzung im IT-Tool identifiziert, dokumentiert und in den zugehörigen Arbeitspakete widerspiegelt.

Im Rahmen von UAP 6.1 wurde die ProBITS-Methode dabei mithilfe des Demonstrators 1: „ProBITS in Aktion“ (Gesundheit) – Implementierung des ProBITS-Investitionsentscheidungsprozesses am Beispiel Gesundheit und DSGVO (RPD) weitergehend evaluiert. Wie bereits im Verlängerungsantrag von November 2023 beschrieben, gab es in dem Zusammenhang jedoch unvorhersehbare Änderungen des Gesetzgebers bezüglich des E-Rezept-Rollouts, weswegen das Entscheidungs- und Vorgehensmodell auf die alternative Fallstudie im Bereich Gesundheit „Datenverarbeitung“ mit Verspätung angewendet wurde. Dies hatte wiederum zur Folge, dass die abschließende Evaluation der ProBITS-Bausteine durch eine exemplarische praxisnahe Integration, später als zuvor erwartet durchgeführt werden konnte. Mit den Evaluationsrunden konnten einige Verbesserungspotenziale an den ProBITS-Bausteinen abgeleitet werden. Der finale Erkenntnisaustausch und -dokumentation konnte fristgerecht und vollumfänglich zum Projektende abgeschlossen werden.

Durch die Verzögerung im UAP 6.1 verzögerte sich auch der Start des UAP 6.4, in welchem die ProBITS-Methode aufgrund der in der Anwendung gesammelten Erkenntnisse und Erfahrungen weiterentwickelt und verbessert wurde. Mithilfe der Projektverlängerung konnten wir die Ergebnisse aus AP 6 mit Abschluss des Projektes in hoher Qualität fertigstellen.

AP 7 – Kommunikation und Diffusion ProBITS

Bezug zu Gesamtziel: GZ 5, GZ 7

Ziel der RPD als Praxispartner war die Erstellung einer Best Practice-Beschreibung zum Einsatz von ProBITS in der Praxis aus der Sicht eines KMU. Durch interne und externe Kommunikation wurde das erlangte Anwendungswissen als Hilfestellung an die anderen Verbundpartner sowie externe Anwender*innen weitergegeben. Die eigene Qualifikation im Unternehmen in Bezug auf ITS-Maßnahmen wurde durch die Kommunikation mit anderen Beteiligten gestärkt.

Im Kontext des AP 7 hat die RPD in Form der Teilnahme an Fokusgruppenworkshops und Expert*innenbefragungen zu den erzielten Projektergebnissen beigetragen.

Zentral ist hier die Bereitstellung von Erfahrungen und Einblicken bezüglich Nutzungsbarrieren von Bewertungsmethoden für Investments in ITS-Maßnahmen im Allgemeinen und im Speziellen bezüglich der ProBITS-Methode zu nennen. Das Forschungsprojekt wurde zudem innerhalb der RPD kommuniziert.

In AP 7 wurde während des gesamten Projektverlaufs kontinuierlich gearbeitet. Es fanden regelmäßige Treffen und Austausch zur ProBITS-Methode, vor allen Dingen mit den Partnern der UPB und der MLU, statt. Darüber hinaus unterstützte die RPD die Partner der UPB und der MLU dabei, die Diffusion und Anwendbarkeit der ProBITS-Methode durch die Identifikation von Adoptionsbarrieren im Rahmen von Interviews und Fokusgruppen zu erhöhen. Durch die Projektverlängerung wurde es uns ermöglicht, diese bis zum Projektende vollumfänglich abzuschließen und damit die Anwenderfreundlichkeit der ProBITS-Methode zu steigern.

Für weitere Details zur Kommunikation und Verbreitung von ProBITS-Inhalten referenzieren wir an dieser Stelle gerne auf den Sachbericht zum Abschlussnachweis der UPB.



Abbildung 6: Dritter Internationaler Workshop zu Compliance-Anforderungen im Information Systems Research Kontext (CIISR 2023)

4 Wichtige Ergebnisse

- Identifikation von Prozesseinflussfaktoren von ITS-Maßnahmen im Rahmen von vier Interview-basierten Runden mit 28 Praktikern und Forschern (Delphi-Studie):

Die RPD stand als Praxispartner für Interviews zur Verfügung und konnte den im Projekt beteiligten Universitäten einen praktischen Einblick in die Umsetzung von ITS-Maßnahmen und IT-Investments im Unternehmensalltag vermitteln. Hierbei lag der Fokus auf Herausforderungen von KMUs im Allgemeinen sowie auf ITS-Maßnahmen im Gesundheitsbereich im Speziellen. Konkret haben hierbei zwei Mitarbeiter*innen an der Erhebung und Entwicklung relevanter Prozessdimensionen aus der Sicht eines mittelständischen Unternehmens mitgewirkt.

- Erhebung von Anforderungen an ein ProBITS-Tool:

Die RPD stand als Praxispartner für Interviews und Diskussionsrunden zur Verfügung und konnte den im Projekt beteiligten Universitäten ihre Anforderungen aus dem Unternehmensalltag an das ProBITS-Tool vermitteln (welche Entscheidungskriterien und Nutzungsbarrieren gibt es?). Zur Nutzung eines solchen Tools gibt es Voraussetzungen (bspw. eine vorhandene Prozessdokumentation), die im praktischen Alltag in sehr heterogener Form, Umfang und Qualität vorliegen. Das ProBITS-Tool muss dieses entsprechend berücksichtigen. Die Nutzung des Tools muss ohne große Vorarbeiten und Einarbeitungszeiten möglich sein. Diese Anforderungen wurden durch die RPD übermittelt.

- Entwicklung einer Fallstudie zur Durchführung der Marktkommunikation am Beispiel der Dateneingangs- und Datenausgangsprozesse der RPD, welche für die Anwendung und Evaluation des ProBITS Entscheidungs- und Vorgehensmodells notwendig ist:

Die RPD hat gemeinsam mit der MLU und der UPB zwei Prozesse aus ihrem Unternehmensalltag identifiziert (Dateneingang und Datenausgang der Rezeptprüfung). Diese Prozesse wurden vorgestellt und ein Prozessdiagramm (BPML) erarbeitet. Da diese Prozesse sowohl externe (zu Datenlieferanten und -empfängern) als auch interne Schnittstellen (Trennung in unterschiedliche unternehmensinterne Netzwerksegmente) besitzen, spielt IT-Sicherheit eine wesentliche Rolle. Die aktuelle Risikoanalyse hat zur Implementierung komplexer ITS-Maßnahmenbündel geführt. Vor diesem Hintergrund ist die RPD der Überzeugung, dass die Prozesse Ansatzpunkte für Effizienzsteigerungen (durch Vereinfachung der Schnittstellen) besitzen, die jedoch immer unter dem Aspekt der IT-Sicherheit analysiert und umgesetzt werden müssen. Daher eignete sich die Fallstudie, um im Verlauf das ProBITS-Modell und das ProBITS-Tool aufbauen und testen zu können.

Die Fallstudien konnten bei der RPD als Basis des Arbeitspaketes 6.1 (Entwicklung eines Demonstrators am Beispiel DSGVO und Gesundheit) dienen.

- Entwicklung des ProBITS-Vorgehensmodells:

Durch mehrere Tiefen-Interviews anhand konkreter Fallstudien konnte die RPD die Sicht und Anforderungen eines KMUs an das Vorgehensmodell zur Erfassung und Bewertung von Prozessdimensionen einbringen.

- Prototypische Implementierung und Evaluation des ProBITS IT-Tools:
Auf Basis der Ergebnisse aus dem Jahr 2021 stand die RPD als Praxispartner für Interviews und Diskussionsrunden zur Verfügung und konnte den im Projekt beteiligten Universitäten zusätzliche kritische Anforderungen aus dem Unternehmensalltag an das ProBITS-Tool vermitteln. Darüber hinaus wirkte die RPD bei der Evaluation und dem grafischen Design der IT-Tool Mockups sowie des Prototypen V.1 und V.2 mit.
- Teilnahme an finaler Delphi Runde zur Relevanzbewertung der Prozessdimensionen, um darauf aufbauend einen Tailoring Bedarf zu identifizieren.
- Evaluation und Dokumentation des multikriteriellen Entscheidungsmodells im Rahmen des Demonstrators 1 „*ProBITS in Aktion*“.
- Ableitung von Tailoring-Faktoren auf das ProBITS-Vorgehensmodell nach Unternehmensgröße und Industrie.
- Modellierung von Handlungsalternativen und ITS-Maßnahmen im Anwendungskontext „Netzwerktrennung Datenverarbeitung“, „Awareness“ und „ISMS“ für den Demonstrator 1.
- Prototypische Implementierung und kontinuierliche Evaluation des verbesserten ProBITS IT-Tools V2.

5 Wichtigste Positionen des zahlenmäßigen Nachweises

Es wurden hauptsächlich Personalmittel verwendet, um die durchführenden Mitarbeiter*innen, Herr Powering (später Frau Reimann) und Herrn Bachmann, zu finanzieren. Diese erhielten bei der Bearbeitung der im Projekt anfallenden Aufgaben Unterstützung durch Herrn Schmidhals, Frau Schneider, Frau Eckold, Frau Kaufhold und Frau Senger, die ebenfalls über die Personalmittel des Projektes finanziert wurden.

Vor dem Hintergrund der angespannten Personalsituation in der hauseigenen IT-Abteilung und unter der Prämisse, dass die Stelle des Informationssicherheitsexperten unbesetzt blieb, wurde im Zuge der kostenneutralen Projektverlängerung das Restbudget für die Unterstützung des AP 6.1 und AP 6.4 durch externe Informationssicherheitsexperten genutzt. In Abstimmung mit dem zuständigen Projektträger sahen wir dies als erfolgskritisch an, um die ausstehenden Aufgaben rund um die ProBITS Fallstudie e-Rezept abschließen zu können, da dies mit den verfügbaren internen Ressourcen nicht abbildbar war.

6 Stand der Wissenschaft & Forschung auf diesem Gebiet

Existierende Ansätze für die ökonomische Bewertung von ITS-Maßnahmen

Der theoretische Hintergrund bestehender Verfahren zur ökonomischen Bewertung von ITS-Maßnahmen ist die Investitionstheorie (Schatz and Bashroush 2017). Dabei

werden die direkten Kosten für die Einführung und den Betrieb einzelner, isolierter ITS-Maßnahmen (z.B. Kosten für Software, Hardware oder Personal) als Investition betrachtet, von der ein direkter Kapitalrückfluss (monetärer Nutzen) erwartet wird (Davis 2005). Die bestehende Literatur zur Bewertung von ITS-Maßnahmen wird von drei Hauptströmungen dominiert (Schatz and Bashroush 2017):

1. Return on Investment (ROI) Ansätze: Diese bewerten den Kapitalrückfluss, der durch eine isolierte ITS-Maßnahme erzeugt wird, im Verhältnis zum eingesetzten Kapital (Phillips and Phillips 2009).
2. Real Options Theory (ROT) Ansätze: Diese berücksichtigen bei der Investitionsbewertung die zeitabhängige Veränderlichkeit des zugrunde liegenden IT-Risikos (Miller and Park 2002).
3. Utility Maximization Theory (UMT) Ansätze: Diese zielen darauf ab, den Kapitalrückfluss eines IT-Sicherheitsinvestments zu maximieren (Strotz 1955).

Allen drei Kategorien liegt die Annahme zugrunde, dass der Kapitalrückfluss durch den erwarteten Anteil des monetären Schadens eines potenziellen IT-Sicherheitsvorfalls repräsentiert wird, der durch den Einsatz einer ITS-Maßnahme verhindert werden kann. Ein Beispiel hierfür sind die verhinderten Betriebsausfall- und Wiederherstellungskosten bei einer DDoS-Attacke (Soo Hoo 2000). In Tabelle 2 werden gängige Ansätze zur ökonomischen Bewertung von ITS-Maßnahmen dargestellt und zusammengefasst.

Tabelle 2. Existierende Ansätze zur ökonomischen Bewertung von ITS-Maßnahmen

Ansatz	Beschreibung
ROSI (Fox 2011; Soo Hoo 2000; Wei et al. 2001)	Der Return on Security Investment (ROSI) hat seine Wurzeln in der Investitionskostenrechnung und basiert auf dem Return on Investment (ROI). Dabei wird die Wirtschaftlichkeit einer Maßnahme durch das Verhältnis von Ertrag zu Kosten berechnet. Im Kontext von ITS-Maßnahmen werden beim ROSI typischerweise vier Komponenten berücksichtigt: die Eintrittswahrscheinlichkeit eines IT-Sicherheitsvorfalls und die Schadenshöhe des IT-Sicherheitsvorfalls. Die Kosten einer ITS-Maßnahme entsprechen den Investitionskosten, während der „Gewinn“ sich aus der Reduktion der Eintrittswahrscheinlichkeit und der Schadenshöhe durch die ITS-Maßnahme ergibt.
Mizzi-Modell (Mizzi 2005)	Das Mizzi-Modell, entwickelt von Adrian Mizzi, erweitert den ROSI um den Aspekt einer Kosten-Nutzen-Betrachtung des Angreifers. Ein rationaler Angreifer wird nur dann einen Angriff durchführen (was im Sinne des ROSI die Eintrittswahrscheinlichkeit beeinflusst), wenn der erwartete Nutzen die entstehenden Kosten überwiegt. Eine ITS-Maßnahme beeinflusst diese Entscheidungsfaktoren, indem sie beispielsweise die Angriffskosten erhöht oder den Zugang zu potenziell wertvollen Informationen einschränkt.
SecureMark System	Das SecureMark System erweitert den ROSI-Ansatz um ein Score Assessment, das Produktivitätsgewinne und -verluste berücksichtigt (Sonnenreich et al. 2006). Es identifiziert zentrale

	Einflussfaktoren des ROSI und beschreibt Methoden, wie diese gemessen werden können. Um beispielsweise den Nutzen einer ITS-Maßnahme zu erfassen, wird empfohlen, Produktivitätsgewinne durch Umfragen in der Belegschaft zu ermitteln. Die Nutzung von Score Assessments soll sicherstellen, dass die Ergebnisse reproduzierbar sind und somit die Ergebnisse verschiedener Alternativen besser vergleichbar machen.
Lockstep-Ansatz (New South Wales. Department of Commerce. Government Chief Information Office and New South Wales. Department of Commerce. Office of Information and Communications Technology 2004)	Der Lockstep-Ansatz erweitert den ROSI-Ansatz durch die Einführung stochastischer Verteilungen für die Eintrittswahrscheinlichkeit und ermöglicht dadurch Sensitivitätsanalysen. Anstelle fixer Eintrittswahrscheinlichkeiten werden mithilfe von Monte-Carlo-Simulationen verschiedene Ereignisse und deren potenzielle Schäden für ein Unternehmen simuliert. Grundlage dieser Simulationen sind Zufallsvariablen, die bestimmten Verteilungen folgen. Durch diese Simulationen kann das Risikomanagement um den Aspekt der Unsicherheit bei der Vorhersage erwarteter Schäden erweitert werden.
QUANTSEC (Chehrazi et al. 2015)	QUANTSEC ist eine ökonomische Wirkungsanalyse, die darauf abzielt, die Kosten und den Nutzen von ITS-Maßnahmen zu quantifizieren. Es berücksichtigt direkte Kosten, Einsparungen durch die frühzeitige Behandlung von Schwachstellen und schätzt die Schadensminderung durch ITS-Maßnahmen. Dieses Modell erweitert die Perspektive des ROSI und bietet ein umfassendes Bewertungsmodell für Sicherheitsmaßnahmen, das auf messbaren Unternehmenskennzahlen basiert.
CIAM (Llansó 2012)	CIAM ist ein datengetriebener Ansatz, der Cyber-Sicherheitsingenieuren eine erste Priorisierung der Sicherheitskontrollen ermöglicht. Dieser Ansatz berücksichtigt Daten zu Sicherheitsvorfällen, ausgenutzten Schwachstellen, geschäftlichen Auswirkungen und Kosten der Sicherheitskontrollen bei der Bewertung und Auswahl von ITS-Maßnahmen.

Die Spezifikation von Investitionen und Kapitalrückflüssen im Bereich der IT-Sicherheit erleichtert zwar die Anwendung investitionstheoretischer Ansätze in diesem Kontext, bringt jedoch mindestens drei zentrale Probleme mit sich, die in der bestehenden Literatur nicht behandelt werden:

1. **Fehlende Mehrdimensionalität.** ITS-Maßnahmen haben neben monetären auch nicht-monetäre Effekte, wie die Beeinflussung der Prozesskomplexität und -flexibilität, Produktivität oder Reputation (Kühnel et al. 2017; Sonnenreich et al. 2006). Solche Effekte werden in den aktuellen investitionstheoretischen Bewertungsansätzen nicht erfasst (Schatz and Bashroush 2017). Es ist daher

notwendig, den Fokus dieser Methoden zu erweitern, um auch die Auswirkungen von ITS-Maßnahmen auf unternehmerische Kernprozesse und die Wertschöpfung zu berücksichtigen.

2. **Datengetriebenheit und fehlende Skalierbarkeit.** Ansätze, die auf ROI, ROT und UMT basieren, sind datengetrieben, obwohl die notwendigen Inputdaten oder genauen Schätzfunktionen oft nicht verfügbar sind (Davis 2005; Schatz and Bashroush 2017). Zudem fehlt eine Methode, wie Kosten- und Nutzenaspekte verschiedener ITS-Maßnahmen vergleichbar erfasst und modelliert werden können. Diese mangelnde ökonomische Vergleichbarkeit erschwert die Auswahl der wirtschaftlich besten Alternative. Insbesondere die fehlende Skalierbarkeit bestehender Berechnungsverfahren wird kritisiert (z. B. Cavusoglu et al. 2004; Schatz and Bashroush 2017), da sie in KMUs aufgrund der begrenzten Datenverfügbarkeit oft nicht anwendbar sind.
3. **Fehlende Berücksichtigung von Maßnahmenbündeln und Wechselwirkungen.** ROI-, ROT- und UMT-basierte Ansätze sind auf die Bewertung einzelner, isolierter ITS-Maßnahmen ausgerichtet. Diese Verfahren stoßen jedoch bei der Bewertung von Maßnahmenbündeln an ihre Grenzen und können die Wechselwirkungen zwischen verschiedenen ITS-Maßnahmen und Geschäftsprozessen nicht berücksichtigen.

7 Verwertbarkeit der Ergebnisse

Im Rahmen des Teilvorhabens *ProBITS in Aktion: Demonstration der Effektivität von ProBITS am Beispiel Gesundheit und Datenschutz*, konnte die Effektivität eines Verfahrens zur Bewertung und Auswahl von ITS-Maßnahmen am Beispiel Gesundheit und Datenschutz demonstriert werden. Auch wenn angrenzende Forschungs- und Förderprojekte existieren, die die Wichtigkeit des Themas unterstreichen, schließt dieses Vorhaben eine zentrale Forschungslücke im Bereich der Forschung zu IT-Sicherheitsinvestitionen. Existierende Forschungs- und Förderprojekte fokussierten sich auf hypothetischen Beispielrechnungen, Großkonzerne und auf Verfahren mit stark vereinfachter Modellrechnung. Eine ganzheitliche Analyse und Demonstration eines Verfahrens zur Bewertung von ITS-Maßnahmen für KMUs im deutschsprachigen Raum ist nicht bekannt und öffentlich zugänglich. Darüber hinaus existierte keine Demonstration eines Verfahrens, das die Kernprobleme aktueller Verfahren zur Bewertung von ITS-Maßnahmen adressiert: fehlende Mehrdimensionalität, Datengetriebenheit, fehlende Skalierbarkeit, fehlende Berücksichtigung von Maßnahmenbündeln und Wechselwirkungen.

Mit Abschluss des Vorhabens (Projektende) sollen die Ergebnisse in den praktischen Unternehmensalltag einfließen. Die ProBITS-Methode soll ab diesem Zeitpunkt bei zukünftigen Unternehmensentscheidungen zur Umsetzung von Datenschutz- und ITS-Maßnahmen zum Einsatz kommen.

Gegenüber den Kunden der RPD soll ProBITS außerdem dafür genutzt werden, ITS-Maßnahmen zu priorisieren und ggf. bei Preisverhandlungen und Preiskalkulationen zum Einsatz kommen.

Durch ProBITS selbst, aber auch durch die im Rahmen des Projektes erworbenen Fachkenntnisse der Beschäftigten der RPD wird insgesamt eine langfristige

Steigerung der IT-Sicherheit im Unternehmen erwartet. Das gilt auch für den im Rahmen des Projektes stattfindenden Informationsaustausch mit anderen Verbundpartnern und den universitären Einrichtungen.

7.1 Wissenschaftliche Erfolgsaussichten

Basierend auf den Ergebnissen des ProBITS-Teilvorhabens lassen sich folgende wissenschaftliche Erfolgsaussichten identifizieren:

1. **Interdisziplinärer Ansatz:** Die Kombination von prozessorientierter und wirtschaftlicher Bewertung erfordert Kenntnisse aus verschiedenen Disziplinen, darunter Informatik, Wirtschaftswissenschaften und Risikomanagement. Dieses Projekt konnte daher die interdisziplinäre Forschung fördern und einen innovativen Ansatz entwickeln, der über traditionelle Sicherheitsbewertungen hinausgeht.
2. **Methodologische Innovation:** Die Entwicklung neuer Methoden und Modelle zur Bewertung der Wirtschaftlichkeit und Effektivität von ITS-Maßnahmen stellt einen wichtigen wissenschaftlichen Beitrag dar. Diese Methoden können helfen, fundierte Entscheidungen über Investitionen in der IT-Sicherheit zu treffen und damit die Ressourcenzuteilung zu optimieren.
3. **Praxisrelevanz und Anwendungsorientierung:** Ein prozessorientierter Ansatz zur Bewertung von ITS-Maßnahmen ermöglicht es, Sicherheitsstrategien direkt in die Geschäftsprozesse zu integrieren. Dies erhöht die Praxisrelevanz des Forschungsprojekts und verbessert die Chancen, dass die entwickelten Modelle und Methoden in der Industrie Anwendung finden.
4. **Unterstützung durch Technologie und Tools:** Mit Hilfe des entwickelten IT-Werkzeugs kann eine IT-gestützte Bewertung und Auswahl angemessener ITS-Maßnahmen erfolgen. Dies erhöht nicht nur die Effizienz, sondern sorgt außerdem für niedrige Adoptions- und Nutzungsbarrieren bei der Entscheidung zum Einsatz der ProBITS-Methode. Das ProBITS-IT-Tool ist damit die technische Unterstützung der ProBITS-Prozessmodellierungssprache, des ProBITS-multikriteriellen Entscheidungsmodells sowie des ProBITS-Vorgehensmodells.

7.2 Fortgeschrittener Verwertungsplan

Aufgrund der technisch und methodisch offenen Gestaltung sowie der vielfältigen Anwendungsmöglichkeiten werden die Ergebnisse des Projekts ProBITS als äußerst relevant für zukünftige Projekte im Bereich der ökonomisch orientierten Sicherheitsforschung des BMBF angesehen. Diese Ergebnisse können direkt und unmittelbar genutzt werden. Alle Methoden, Vorgehensmodelle und Erkenntnisse aus ProBITS werden und wurden sowohl in der Lehre (z.B. Vorlesungen, Projektseminare und Abschlussarbeiten) als auch in der Forschung (z.B. Konferenzen, Publikationen und Promotionen) wissenschaftlich genutzt und der Öffentlichkeit sowie dem Fachpublikum frei zugänglich gemacht. Die wissenschaftlichen Mitarbeiter*innen, die am Projekt ProBITS beteiligt waren, hatten die Möglichkeit, sich im Fachgebiet zu etablieren, wertvolle Projekterfahrungen zu sammeln, eigenständig zu forschen, ihre Ergebnisse international zu veröffentlichen und sich zu vernetzen. Darüber hinaus wird durch die Beteiligung der Transferpartner MSU und RPD sowie der assoziierten

Partner in ihren jeweiligen Anwendungsdomänen eine direkte wirtschaftliche Anschlussfähigkeit gewährleistet.

Im Verlauf des Projekts wurde das Competence Center ProBITS unter Leitung der universitären Partner etabliert, um die Nachhaltigkeit zu gewährleisten. Das Competence Center steht darüber hinaus allen interessierten Unternehmen offen und fungiert als Leuchtturm für den Kompetenzaufbau. Es dient als zentrale Schnittstelle für die Weiterentwicklung und Verbreitung des Ansatzes sowohl in der Wissenschaft als auch in der Praxis über die Projektlaufzeit hinaus. Das Ziel des Verbunds ist es, eigene sowie weitere durch Drittmittel geförderte Projekte zu initiieren und in Zusammenarbeit mit den Gründungszentren der Universitäten beispielsweise Ausgründungen zu unterstützen.

Die praxisnahe Entwicklung und Evaluierung bilden eine wesentliche Grundlage für die Umsetzung in der Praxis. Die entwickelten Bausteine von ProBITS werden von uns und möglicherweise von weiteren interessierten assoziierten Partnern genutzt, um ihr eigenes Toolset und Fähigkeiten im Bereich IT-Sicherheit zu erweitern. In Zeiten von steigenden Anforderungen bei kontinuierlich hoher Belastung der Mitarbeitenden in Unternehmen, bietet sich die Nutzung der ProBITS Methode besonders an, um Reibungsverluste zu vermeiden und Effizienzen (von Investition) zu steigern. Unser Fokus liegt dabei darauf, prozessorientierte ITS-Maßnahmen effektiv zu bewerten und auszuwählen und dies künftig als zusätzlichen Baustein unseres Informationssicherheits-Management-Systems zu nutzen.

7.3 Planungen für die nähere Zukunft

Um die nachhaltige Nutzung und Weiterentwicklung der ProBITS-Methode sicherzustellen, sind mehrere strategische Ansätze überlegt worden, die das Projekt auch über die Laufzeit hinaus stärken und verbreiten können. Dabei sollen sowohl die bestehenden Strukturen genutzt als auch neue Partnerschaften und Forschungsinitiativen ins Leben gerufen werden.

Weiterentwicklung zu ProBITS 2.0: Es wird vorgeschlagen, die ProBITS-Methode weiterzuentwickeln und zu einer verbesserten Version, ProBITS 2.0, auszubauen. Diese Version könnte erweiterte Funktionen und verbesserte Algorithmen zur Bewertung und Integration von ITS-Maßnahmen bieten. Insbesondere sollen die folgenden Bereiche adressiert werden:

- **Erweiterung der Dimensionen:** Integration zusätzlicher Dimensionen, wie etwa die Berücksichtigung von Umweltaspekten und sozialen Auswirkungen von ITS-Maßnahmen.
- **Verbesserte Benutzerfreundlichkeit:** Weiterentwicklung der Benutzeroberfläche und der Usability des IT-Tools, um die Handhabung für Unternehmen weiter zu erleichtern.
- **Erweiterte Analytik:** Implementierung fortgeschrittener Analysetools, die auf maschinellem Lernen basieren, um präzisere Vorhersagen und Empfehlungen zu ermöglichen.

Kooperation mit Forschungsgruppen und Vereinen: Die Zusammenarbeit mit etablierten Forschungsgruppen und Fachvereinen, die sich mit IT-Sicherheit und ökonomischen Bewertungen beschäftigen, soll intensiviert werden. Mögliche Partner könnten unter anderem folgende Institutionen sein:

- **Forschungsinstitute und Universitäten:** Kooperationen mit führenden Universitäten und bundesweiten Forschungsinstituten, die sich mit IT-Sicherheit, Wirtschaftsinformatik und Prozessmanagement befassen.
- **Fachverbände und Netzwerke:** Zusammenarbeit mit Fachverbänden wie dem Bundesverband IT-Sicherheit e.V. (TeleTrust) oder dem Verband der Internetwirtschaft e.V. (eco), um die ProBITS-Methode in der Breite der Wirtschaft bekannt zu machen und zu verbreiten.

Gründung von Spin-offs und Start-ups: Es wird erwogen, die ProBITS-Methode durch die Gründung von Start-ups weiter zu kommerzialisieren. Hierzu könnten spezielle Inkubatorprogramme an der MLU und UPB genutzt werden, um interessierte Gründer*innen zu unterstützen. Unterstützung durch Programme wie dem EXIST-Gründerstipendium oder den universitären Gründungszentren, um innovative Ideen aus dem ProBITS-Projekt in marktfähige Produkte und Dienstleistungen zu überführen.

Aufbau eines Netzwerks von ProBITS-Anwendern: Ein weiteres Ziel ist der Aufbau eines Netzwerks von Unternehmen und Organisationen, die die ProBITS-Methode anwenden. Dieses Netzwerk könnte durch regelmäßige Treffen, Workshops und Konferenzen gefördert werden.

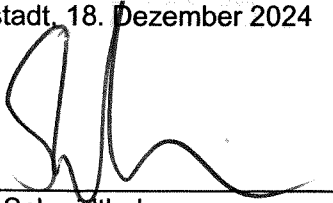
Diese Planungen bieten eine solide Grundlage, um die erfolgreiche Arbeit des ProBITS-Projekts weiterzuführen und seine Ergebnisse nachhaltig in die Praxis zu überführen. Durch die enge Zusammenarbeit mit verschiedenen Stakeholdern und die Nutzung vielfältiger Unterstützungsangebote kann die Verbreitung und Weiterentwicklung der ProBITS-Methode auch in naher Zukunft sichergestellt werden.

Referenzen

- Becker, J., Delfmann, P., Dietrich, H.-A., Steinhorst, M., and Eggert, M. 2016. "Business Process Compliance Checking – Applying and Evaluating a Generic Pattern Matching Approach for Conceptual Models in the Financial Sector," *Information Systems Frontiers* (18:2), pp. 359–405. (<https://doi.org/10.1007/s10796-014-9529-y>).
- Cavusoglu, Hasan, Cavusoglu, Huseyin, and Raghunathan, S. 2004. "Economics of IT Security Management: Four Improvements to Current Security Practices," *Communications of the Association for Information Systems* (14:1), pp. 65–75.
- Chehrazi, G., Schmitz, C., and Hinz, O. 2015. "QUANTSEC - Ein Modell Zur Nutzenquantifizierung von IT-Sicherheitsmaßnahmen," in *Wirtschaftsinformatik Proceedings 2015*, Osnabrück, March 4, pp. 1131–1145. (<https://aisel.aisnet.org/wi2015/76>).
- Davis, A. 2005. "Return on Security Investment – Proving It's Worth It," *Network Security* (2005:11), pp. 8–10. ([https://doi.org/10.1016/S1353-4858\(05\)70301-9](https://doi.org/10.1016/S1353-4858(05)70301-9)).
- Fox, D. 2011. "Betriebswirtschaftliche Bewertung von Security Investments in der Praxis," *Datenschutz und Datensicherheit - DuD* (35:1), pp. 50–55. (<https://doi.org/10.1007/s11623-011-0014-1>).
- Kühnel, S., Sackmann, S., and Seyffarth, T. 2017. "Efficiency-Oriented Risk Management for Business Process Compliance," *HMD Praxis Der Wirtschaftsinformatik* (54), Springer, pp. 124–145.
- La Rosa, M. 2015. "Strategic Business Process Management," in *Proceedings of the 2015 International Conference on Software and System Process, ICSSP 2015*, New York, NY, USA: Association for Computing Machinery, August 24, pp. 177–178. (<https://doi.org/10.1145/2785592.2785620>).
- Llansó, T. 2012. "CIAM: A Data-Driven Approach for Selecting and Prioritizing Security Controls," in *2012 IEEE International Systems Conference SysCon 2012*, Vancouver, BC, Canada, March, pp. 1–8. (<https://doi.org/10.1109/SysCon.2012.6189500>).
- Miller, L. T., and Park, C. S. 2002. "Decision Making Under Uncertainty—Real Options to the Rescue?," *The Engineering Economist* (47:2), Taylor & Francis, pp. 105–150. (<https://doi.org/10.1080/00137910208965029>).
- Mizzi, A. 2005. "Return on Information Security Investment. Are You Spending Enough? Are You Spending Too Much," *Posted in ACM IT Security Toolbox*.
- New South Wales. Department of Commerce. Government Chief Information Office, and New South Wales. Department of Commerce. Office of Information and Communications Technology. 2004. *A Guide for Government Agencies Calculating Return on Security Investment [Electronic Resource] / Lockstep*

- Consulting [for] Government Chief Information Office*, (Government Chief Information Office, ed.). (<https://catalogue.nla.gov.au/catalog/4808007>).
- Phillips, P. P., and Phillips, J. J. 2009. "Return on Investment," in *Handbook of Improving Performance in the Workplace: Volumes 1-3* (Vol. 1–3), John Wiley & Sons, Ltd, pp. 823–846. (<https://doi.org/10.1002/9780470592663.ch53>).
- Sadiq, S., and Governatori, G. 2015. "Managing Regulatory Compliance in Business Processes," in *Handbook on Business Process Management 2: Strategic Alignment, Governance, People and Culture*, J. vom Brocke and M. Rosemann (eds.), Berlin, Heidelberg: Springer, pp. 265–288. (https://doi.org/10.1007/978-3-642-45103-4_11).
- Schatz, D., and Bashroush, R. 2017. "Economic Valuation for Information Security Investment: A Systematic Literature Review," *Information Systems Frontiers* (19:5), pp. 1205–1228. (<https://doi.org/10.1007/s10796-016-9648-8>).
- Sonnenreich, W., Albanese, J., and Stout, B. 2006. "Return on Security Investment (ROSI) - A Practical Quantitative Model," *Journal of Research and Practice in IT* (38:1), Australian Computer Society, pp. 45–56. (<https://doi.org/10.3316/ielapa.937199632104879>).
- Soo Hoo, K. J. 2000. *How Much Is Enough: A Risk Management Approach to Computer Security*, Stanford University.
- Strotz, R. H. 1955. "Myopia and Inconsistency in Dynamic Utility Maximization," in *Readings in Welfare Economics*, M. J. Farrell (ed.), London: Macmillan Education UK, pp. 128–143. (https://doi.org/10.1007/978-1-349-15492-0_10).
- Wei, H., Frinke, D., Carter, O., and Ritter, C. 2001. *Cost-Benefit Analysis for Network Intrusion Detection Systems*, presented at the CSI 28th Annual Computer Security Conference, Washington, DC, pp. 29–31.

Duderstadt, 18. Dezember 2024

A handwritten signature in black ink, consisting of a large, stylized 'R' followed by a series of loops and a long horizontal stroke.

Robert Schmidhals
Geschäftsführer RPD

Prozess-orientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen (ProBITS)

Kurzbericht zum Abschlussnachweis

Zuwendungsempfänger:	Förderkennzeichen:
Rezeptprüfstelle Duderstadt GmbH (RPD)	16KIS1333
Titel des Teilvorhabens:	
Demonstration der Effektivität von ProBITS am Beispiel Gesundheit und Datenschutz	
Projektleiter: Robert Schmidthals	
E-Mail: robert.schmidthals@rpd.de	Tel.: 05527/9852-74
Laufzeit des Vorhabens:	
von: 01.04.2021 bis: 30.06.2024	
Berichtszeitraum des Vorhabens:	Berichtsdatum:
von: 01.04.2023 bis: 30.06.2024	vom 19.12.2024

Aufgabenstellung

Ziel des Projekts ProBITS war es, eine methodisch fundierte und werkzeuggestützte prozessorientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen (ITS-Maßnahmen) zu ermöglichen. Ausgangspunkt waren die Limitationen bestehender Bewertungsansätze, die sich oft auf eindimensionale, monetäre Aspekte konzentrieren. Insbesondere kleine und mittlere Unternehmen (KMUs) benötigen eine skalierbare Methode, die die Auswirkungen von ITS-Maßnahmen auf Geschäftsprozesse umfassend berücksichtigt. Basierend auf aktuellem Wissen und Technologie (z. B. DSGVO, IT-Sicherheitsgesetz) sollte ProBITS ein multikriterielles Entscheidungsmodell und unterstützende Tools entwickeln.

Wissenschaftlicher und technischer Stand

Bereits bestehende Ansätze zur Bewertung von ITS-Maßnahmen, wie der Return on Security Investment (ROSI), fokussieren sich primär auf monetäre Aspekte und berücksichtigen weder die komplexen Wechselwirkungen von ITS-Maßnahmen mit Geschäftsprozessen noch deren nicht-monetäre Auswirkungen. Zudem sind diese Ansätze oft datengetrieben und für KMUs schwer umsetzbar. ProBITS setzte auf Methoden des modernen Geschäftsprozessmanagements auf, um diese Lücken zu schließen, und integrierte innovative Elemente wie ein multikriterielles Entscheidungsmodell, ein Vorgehensmodell und ein IT-Tool.

Ablauf des Vorhabens

Das Projekt lief von April 2021 bis Juni 2024 und umfasste sieben Arbeitspakete. Es wurde von einem Konsortium aus Forschungseinrichtungen und Praxispartnern durchgeführt, darunter die Universität Paderborn (UPB), die Martin-Luther-Universität Halle-Wittenberg (MLU), die Rezeptprüfstelle Duderstadt GmbH (RPD) und die msu solutions GmbH (MSU).

Die Hauptaktivitäten umfassten:

1. Analyse und Definition von Anforderungen an ITS-Bewertungsverfahren.
2. Erweiterung einer Prozessmodellierungssprache und Entwicklung eines multikriteriellen Entscheidungsmodells und eines Vorgehensmodells.
3. Prototypische Implementierung des multikriteriellen Entscheidungsmodells und des Vorgehensmodells in einem IT-Tool.
4. Evaluation und Demonstration der Methodik anhand praxisnaher Szenarien, z. B. im Gesundheitssektor.

Wesentliche Ergebnisse

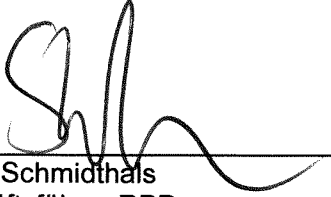
1. **Multikriterielles Entscheidungsmodell:** Ein Modell zur Bewertung und Auswahl von ITS-Maßnahmen basierend auf ökonomischen, prozessualen und sicherheitstechnischen Kriterien wurde entwickelt.
2. **Vorgehensmodell:** Ein praxistaugliches Framework unterstützt Unternehmen bei der Implementierung und Nutzung des Entscheidungsmodells.
3. **Erweiterung einer Prozessmodellierungssprache:** Die Prozessmodellierungssprache BPMN wurde erweitert, um spezifische Einflussdimensionen und Anforderungen von ITS-Maßnahmen abzubilden. Dies ermöglicht eine prozessorientierte Betrachtung und Bewertung der Auswirkungen von ITS-Maßnahmen auf Geschäftsprozesse. Unternehmen können dadurch die Wechselwirkungen zwischen Maßnahmen und Prozessen besser visualisieren und optimieren.
4. **IT-Tool:** Ein Prototyp wurde erstellt und erfolgreich evaluiert. Dieses Tool ermöglicht Unternehmen, komplexe ITS-Maßnahmenbündel effizient zu bewerten.
5. **Demonstration der Anwendbarkeit:** Im Rahmen von Fallstudien (z. B. zur DSGVO-Compliance) wurde die Effektivität der ProBITS-Bausteine gezeigt.

Zusammenarbeit und Mehrwert

Das Projekt profitierte von der interdisziplinären Zusammenarbeit zwischen Forschung und Praxis. Die RPD und MSU trugen zur praktischen Validierung bei, während die Universitäten die methodischen Grundlagen legten. ProBITS schließt

eine Forschungslücke, indem es die Mehrdimensionalität, Skalierbarkeit und Wechselwirkungen von ITS-Maßnahmen umfassend berücksichtigt. Die Ergebnisse können Unternehmen langfristig bei der Entscheidungsfindung unterstützen und zu einer Steigerung der IT-Sicherheit und Effizienz beitragen.

Duderstadt, 19.12.2024

A handwritten signature in black ink, consisting of a large, stylized 'S' followed by a series of loops and a long horizontal stroke extending to the right.

Robert Schmidhals
Geschäftsführer RPD