

30.12.2024

# **ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen**

Kurzbericht zum Teilvorhaben im Verbundprojekt  
“Prozess-orientierte wirtschaftliche Bewertung und Auswahl von IT-  
Sicherheitsmaßnahmen (ProBITS)”

msu solutions GmbH

Autoren:  
Jennifer Arndt  
Erik Schulz

# 1. Motivation und Zielstellung des Teilvorhabens

Das Teilvorhaben ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen im BMBF geförderten Verbundprojekt Prozess-orientierte wirtschaftliche Bewertung und Auswahl von IT-Sicherheitsmaßnahmen (ProBITS) zielte darauf ab, die vier zentralen Bausteine für ProBITS (ProBITS-Prozessmodellierungssprache, -Methode, -Vorgehensmodell, IT-Werkzeug) gemeinsam mit den Verbundpartnern zu entwickeln. Dadurch wurde ein innovativer Ansatz bereitgestellt werden, der eine geschäftsprozessorientierte Bewertung von IT-Sicherheitsmaßnahmen ermöglicht. Somit wurden Entscheider in die Lage versetzt, prozessuale Aufwände und Nutzen von IT-Sicherheitsmaßnahmen abzuwägen, um wirtschaftliche Entscheidungen bei der Auswahl von ITS-Maßnahmen 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 diesen Risiken entgegen zu steuern, definieren sowohl der Gesetzgeber als auch die Unternehmen selbst weitreichende und übergreifende Anforderungen an die IT-Sicherheit. Beispiele hierfür finden sich sowohl in unternehmenseigenen Vorgaben zur Governance der Informationssicherheit (bspw. allg. Richtlinien zur Authentifizierung oder Richtlinien zur Datenklassifizierung und zum -umgang), in sektorspezifischen Richtlinien (bspw. PSD2 für Banken oder KRITIS für Betreiber von kritischer Infrastruktur), als auch in sektorübergreifenden Vorgaben (bspw. DSGVO oder IT-Sicherheitsgesetz). 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. 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 IT-Sicherheitsanforderungen als kostenintensive Aufgabe (Sadiq und Governatori 2015; La Rosa 2015) und sogar als "heftiger Kostentreiber" (Becker et al. 2016) bezeichnet wird. Damit die Profitabilität eines Unternehmens nicht durch die Umsetzung von ITS-Maßnahmen(-bündeln) beeinträchtigt wird, gilt es daher, geeignete Handlungsalternativen zu identifizieren und basierend auf wirtschaftlichen Kriterien auszuwählen.

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. Außerdem zeigt sich, dass in der Praxis bislang keine hohe Akzeptanz von Bewertungsmethoden besteht. So hat sich auf breiter Linie bislang keiner der bestehenden Ansätze durchgesetzt. Daher sind Ansätze zur ganzheitlichen Bewertung und Auswahl solch komplexer Bündel von ITS-Maßnahmen und deren Wechselwirkungen mit Geschäftsprozessen notwendig, um Unternehmen die Auswahl der effektivsten ITS-Maßnahme unter ökonomischen Gesichtspunkten überhaupt zu ermöglichen.

Die Energiebranche stellt die Entwicklung einer solchen Bewertungsmethode vor besondere Herausforderungen. Die Energiebranche gehört nach EU-Richtlinie 2008/114/EG zu den „Kritischen Infrastrukturen“ und ist vom Gesetzgeber verpflichtet, umfangreiche Maßnahmen für die IT-Sicherheit, aber auch für die Sicherheit von Erzeugungsanlagen, Netzen und Messtechnik umzusetzen. Genau hier wäre eine an Geschäftsprozessen orientierte IT-Sicherheit und der Einsatz eines Systems wie ProBITS zwingend geboten. Allerdings fehlt es in der Praxis vielfach an Bereitschaft, die Umsetzung der ITS-Maßnahmen(-bündeln) mit der Unterstützung der Entwicklung geeigneten Tools für die IT-Sicherheit vorzubereiten und umzusetzen. Bei der msu solutions GmbH bezogen sich die bisherigen Verfahren und Tools zur IT-Sicherheit jedoch insbesondere auf Zugriffsfreigaben und -beschränkungen von Daten in den IT-Systemen für die Energiewirtschaft, sowie auf die verschlüsselte Übertragung von Marktkommunikationsdaten an Marktpartner, wie Netzbetreiber, Messstellenbetreiber, Stromlieferanten, etc. Die Einbeziehung von Tools und Verfahren für die Bewertung von ökonomischen Kriterien erfolgt bisher demnach nur unzureichend, wird aber zunehmend von Unternehmen der Energiewirtschaft gefordert.

## 1.2. 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. Im Rahmen des Teilprojekts Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen wurde daher bei der Entwicklung eines innovativen Ansatzes unterstützt, der die geschäftsprozessorientierte Bewertung von ITS-Maßnahmen methodisch, mehrdimensional, skalierbar und werkzeuggestützt ermöglicht. Dadurch werden KMUs und Entscheider in die Lage versetzt, Kosten, prozessuale Aufwände und Nutzen von ITS-Maßnahmen abzuwägen, um Entscheidungen bei der Auswahl von ITS-Maßnahmen unter Berücksichtigung ökonomischer Auswirkungen treffen zu können.

Die msu solutions GmbH (MSU) trug essentiell zum Erreichen aller Gesamtziele von ProBITS bei. Hierbei wird explizit das Ziel verfolgt, die Anwendbarkeit von Verfahren zur Bewertung und Auswahl von ITS-Maßnahmen zu demonstrieren. Hierfür wurde zum einen der Demonstrator ProBITS in Aktion: Smart Meter umgesetzt, der aufzeigte, wie ProBITS aus Sicht eines Beratungsunternehmens eingesetzt werden kann. Zum anderen wurde in diesem Teilvorhaben „ProBITS deckt auf“ umgesetzt, welches Erkenntnisse zur Effektivität von Verfahren zur Bewertung und Auswahl von ITS-Maßnahmen lieferte.

Im Rahmen der übergreifenden Gesamtziele des Gesamtvorhabens von ProBITS, ergaben sich folgende Ziele für das Teilvorhaben:

- 1. Analyse und Evaluation der Effektivität bisheriger Verfahren zur Bewertung von IT-Sicherheitsmaßnahmen:** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu das Aufzeigen von Stärken und Schwächen traditioneller investitionstheoretischer Verfahren zur ökonomischen Bewertung und Auswahl von ITS-Maßnahmen (insb. ROSI-basierter Verfahren) durch Anwendung auf Realszenarien im Rahmen von „ProBITS deckt auf“. Außerdem wurden die Ergebnisse traditioneller investitionstheoretischer Verfahren zur ökonomischen Bewertung und Auswahl von ITS-Maßnahmen (insb. ROSI-basierter Verfahren) mit den Ergebnissen des multikriteriellen Entscheidungsmodells von ProBITS verglichen.
- 2. Identifikation von Prozesseinflussgrößen, fachlichen Anforderungen, Bewertungsdimensionen und Anwendungsbarrieren von Verfahren zur Bewertung von IT-Sicherheitsmaßnahmen mit einem Fokus auf KMUs:** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu die Durchführung von Zielgruppeninterviews gemeinsam mit der Martin-Luther-Universität Halle-Wittenberg (MLU). Dabei wurden Experten von der MSU durch die MLU interviewt um praktische Anforderungen, die an ein multikriterielles Entscheidungsmodell für IT-Sicherheitsmaßnahmen(-bündel) und an ein skalierbares Vorgehensmodell gestellt werden, zu identifizieren. Zusätzlich wurden Case Studies der MSU zur Absicherung der Relevanz und Anwendbarkeit theoretischer Zwischenergebnisse diskutiert und konzeptioniert.
- 3. Bereitstellung eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln):** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu die Anwendung und formative Zwischenevaluation von Ergebnissen des Projektkonsortiums mit Hilfe von Case Studies bei der MSU. Diese beinhalteten die Erweiterung der Business Process Model and Notation 2.0 (BPMN) und des Standards für eXtensible Event Streams (XES) zur Abbildung kosten- und nutzenbasierter Bewertungsdimensionen von IT-Sicherheitsmaßnahmen(-bündeln), der Kosten-/Nutzenmodelle zur wirtschaftlichen Bewertung von IT-Sicherheitsmaßnahmen(-bündeln) und des multikriteriellen Entscheidungsmodells zur wirtschaftlichen Bewertung und Analyse von alternativen IT-Sicherheitsmaßnahmen(-bündeln).
- 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:** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu die Durchführung von Workshops gemeinsam mit der MLU, um Vorgehens-relevante Aspekte sowie Tailoring-Faktoren für das ProBITS-Vorgehensmodell zu identifizieren. Außerdem wurde das ProBITS-Vorgehensmodell an die spezifischen Bedürfnisse von Anwendern aus dem Bereich der Energiewirtschaft angepasst.
- 5. Demonstration der Anwendbarkeit und Effektivität von ProBITS:** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu die Demonstration der prospektiven Anwendbarkeit und der Effektivität von ProBITS im Kontext von Smart Metering sowie die der retrospektiven Anwendbarkeit und der Effektivität von ProBITS.
- 6. Verstetigung eines multikriteriellen Entscheidungsmodells zur prozessorientierten wirtschaftlichen Bewertung und Analyse von ITS-Maßnahmen(-bündeln):** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu die Verstetigung des ProBITS-Ansatzes durch Einführung des ProBITS Competence Centers als zentrale Koordinationsstelle für die interne und externe Kommunikation. Im Rahmen dessen als auch darüber hinaus wurde zur Erreichung dieses Ziels außerdem das gewonnene praktische Wissen und Anwendungswissen vermittelt.

7. **Steigerung der Qualifikation und Awareness von Unternehmen (insb. KMUs), Mitarbeitern, Studierenden und Doktoranden im Bereich IT-Sicherheit:** Im Rahmen des Teilprojekts der msu solutions GmbH zählte dazu die Qualifizierung von Mitarbeitern und Mitarbeiterinnen, speziell von Mitarbeitern aus dem Bereich der IT-Sicherheit, für die Anwendung von Modellen und IT-Werkzeugen von ProBITS durch interne Schulungen bei der MSU sowie durch das Angebot externer Schulungen für andere KMU.

Und der Meilenstein M3: **Demonstrator 2 – ProBITS in Aktion (Smart Meter):** ProBITS wurde im Bereich SmartMeter im Rahmen einer IT-Sicherheitsmaßnahme angewendet, evaluiert und dokumentiert.

## 2. Ablauf des Vorhabens

Die Hauptpositionen des Teilvorhabens ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen setzen sich im Wesentlichen aus der Ermittlung der Anwendbarkeit, einer Überprüfung auf Korrektheit und der tatsächlichen Anwendung von proBITS zusammen. Diese werden im Folgenden entsprechend den Arbeitspaketen im zeitlichen Ablauf der Aktivitäten gegliedert und detailliert beschrieben. Dabei stimmen Arbeitsplan und Tätigkeitsverlauf im Folgenden weitestgehend überein, wobei etwaige Verschiebungen im Projektverlauf durch einen schriftlichen und visuellen Verweis im ursprünglichen Arbeitsplan sowie die genaue Erläuterung des tatsächlich erfolgten Leistungszeitraums erläutert werden.

### 2.1. Überblick

AP	Arbeitspakete	2021				2022				2023				2024															
		4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	
1	<b>Interne und externe Vernetzung ProBITS</b>																												
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	<b>Grundlagen und Anforderungen ProBITS</b>																												
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	<b>Entwurf des multikriteriellen Entscheidungsmodells für ProBITS</b>																												
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	<b>Entwurf des ProBITS-Vorgehensmodells</b>																												
4.1	Entwurf eines Vorgehensmodells für die skalierbare Umsetzung von ProBITS																												
4.2	Ausarbeitung von Vorlagen für das skalierbare Vorgehensmodell																												
5	<b>Entwicklung ProBITS-Werkzeug</b>																												
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	<b>Evaluation und Weiterentwicklung ProBITS</b>																												
6.1	<b>Demonstrator 1: "ProBITS in Aktion" (Gesundheit) - Implementierung des ProBITS-Investitionsentscheidungsprozesses am Beispiel Gesundheit und DSGVO</b>																												
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	<b>Demonstrator 2: "ProBITS in Aktion" (Smart Meter) - Implementierung des ProBITS-Investitionsprozesses am Smart Meter</b>																												
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	<b>Demonstrator 3: "ProBITS deckt auf" - Retrospektive Prozessorientierte Kosten/Nutzen-Analyse von getätigten IT-S-Maßnahmen(-bündeln) für Kundenportale</b>																												
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	<b>Weiterentwicklung ProBITS auf Basis der Erkenntnisse aus Demonstrator 1, 2 und 3</b>																												
7	<b>Kommunikation und Diffusion ProBITS</b>																												
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																												

Abbildung 2: Überblick des Projektverlaufs anhand der Arbeitspakete, Personenmonate und Meilensteine für das Teilvorhaben.  
 Legende: x = keine Aktivität trotz Planung; pastellfarbene Felder = Aktivität über die ursprüngliche Planung hinausgehend.

Das Vorhaben lässt sich in drei Phasen unterteilen (siehe Abbildung 1). In der ersten Phase "Design" (AP 2-5) werden die vier zentralen Bausteine für ProBITS (ProBITS-Prozessmodellierungssprache, -Methode, -Vorgehensmodell, IT-Werkzeug) gemeinsam mit den Verbundpartnern in einer ersten Version (ProBITS V.1) entwickelt. In der zweiten Phase "Demonstration" (AP 6) wird ProBITS in Form von drei Demonstratoren angewendet. Dies dient zum einen dazu, die Effektivität der Methode aufzuzeigen ("ProBITS in Aktion"). Zum anderen soll mit einer retrograden Betrachtung die Effektivität der Methode im Vergleich zu bestehenden Verfahren wie dem ROSI aufgezeigt werden ("ProBITS deckt auf"). Im Laufe der Entwicklung und Testung aller drei Demonstratoren wird eine kontinuierliche Verbesserung von ProBITS durchgeführt. Schließlich wird aufbauend auf den Erkenntnissen aus der Anwendung von ProBITS V.1 eine Version ProBITS V.2 formal weiterentwickelt. In der dritten Phase "Projektleitung/Diffusion" wird parallel zum Vorhaben durch AP 1 und AP 7 das Gesamtvorhaben gesteuert sowie die Ergebnisse kommuniziert und in Wissenschaft und Praxis übertragen. In den folgenden Tabellen werden die geplanten Arbeitspakete inkl. den entsprechenden personellen Aufwänden (PM: Personenmonat), der Unterarbeitspakete (UAP) und der Meilensteine skizziert.

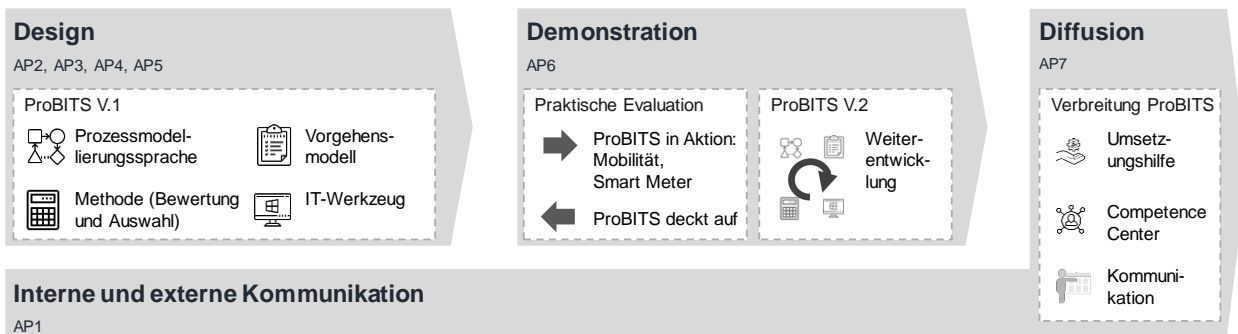


Abbildung 1. Übersicht der Arbeitspakete

Der Meilenstein des Teilvorhabens bestand im Demonstrator – ProBITS in Aktion (Smart Meter). Dieser wurde durch die erfolgreiche Anwendung, Evaluation und Dokumentation der ProBITS-Bausteine im Bereich Smart Meter erfolgreich erreicht. Hierfür nutzten wir die Fallstudie "Anschluss eines Smart Meters" und erarbeiteten den Meilenstein gemeinsam mit den Partnern der MLU und RPD.

Arbeitspakete	2021			2022				2023				2024		AP Lead
	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	
1 Interne und externe Vernetzung ProBITS	[Aktivität]													UPB
2 Grundlagen und Anforderungen ProBITS	[Aktivität]													BIM
3 Entwurf des multikriteriellen Entscheidungsmodells für ProBITS	[Aktivität]													BIM
4 Entwurf des Vorgehensmodells für ProBITS	[Aktivität]													UPB
5 Entwicklung ProBITS-Werkzeug	[Aktivität]													UPB
6 Evaluation und Weiterentwicklung ProBITS														MSU
6.1 Demonstrator 1: ProBITS in Aktion (Gesundheit)														RPD
6.2 Demonstrator 2: ProBITS in Aktion (Smart Meter)														MSU
6.3 Demonstrator 3: ProBITS deckt auf														MSU
6.4 Weiterentwicklung ProBITS														RPD
7 Kommunikation und Diffusion ProBITS	[Aktivität]													UPB

▲ MS 1, 2      ▲ MS 3, 4

Arbeitsstand zu den geplanten Meilensteinen:

- Meilenstein 1 wurde erreicht.
- Meilenstein 2 wurde erreicht.
- Meilenstein 3 wurde erreicht.

- Meilenstein 4 wurde erreicht.

## AP 1 – Interne und externe Vernetzung ProBITS

### UAP 1.1 - Aufbauen des Competence Centers ProBITS für die interne und externe Vernetzung

- Erproben des technischen Setups einer Microsoft TEAMS-Plattform für die interne Vernetzung aller Teilnehmer
- Einrichten eines sicheren Dateiaustausches für Dateien über eine NextCloud-Plattform
- Start des laufenden Betriebs der TEAMS-Plattform der UPB für die interne Kommunikation und Datentransfer zwischen MSU und anderen Projektteilnehmern über NextCloud-Plattform

### UAP 1.2 - Etablierung des Competence Centers ProBITS zur Verstetigung und Weiterentwicklung der Projektergebnisse

- Einbringen von benutzeroptimierten Vorgaben zum Aufbau eines Competence Centers und Bereitstellung der Auskünfte zur aktuellen Entwicklung und zum gemeinsamen Datenaustausch
- Aufbau des Kompetenzbereichs "Praktische Anwendung des Entscheidungs- und Vorgehensmodells sowie des IT-Werkzeugs von ProBITS"
- Vermittlung des im Rahmen des Teilprojekts gewonnenen Wissens
- die externe Kommunikation und Vernetzung des ProBITS-Projekts wurde im weiteren Verlauf des Fördervorhabens vorrangig durch die Partner der Universität Paderborn betrieben.
- Gestaltung des Logos für das gemeinsame Competence Center



Bild 1 – Logo des Competence Center

## AP 2 - Grundlagen und Anforderungen ProBITS

### UAP 2.3 - Zielgruppeninterviews mit MSU zur Identifikation von kritischen Anforderungen, die an ein multikriterielles Entscheidungsmodell gestellt werden

- Zielgruppeninterviews mit Experten von der MSU zur Identifikation von praktischen Anforderungen, die an ein multikriterielles Entscheidungsmodell für IT-Sicherheitsmaßnahmen(-bündel) gestellt werden, wie bspw. Anforderungen hinsichtlich der Anpassung von Geschäftsprozessen in **msu.energie**
- Fokusgruppenworkshops zur Erarbeitung einer Fallstudie, die zur Anwendung und Evaluation des Entscheidungs- und Vorgehensmodells dient und im Laufe des Projekts flexibel erweitert und präzisiert werden kann
- Ziel der Entwicklung einer Fallstudie wurde erreicht, weiterführend sollen weitere Fallstudien aufgestellt werden, um die Thematik des DSGVO-Moduls und der Prozessbearbeitung im Bereich intelligente Messsysteme stärker mit einzubeziehen. Bisherige Praxisfälle wurden in den Workshops besprochen und mit der Fallstudie in Verbindung gebracht
- Unterstützung der MLU & ISC bei Unterarbeitspaketen, durch den Austausch aus der Praxisperspektive zu Dimensionen, Einflussgrößen und Entscheidungsfaktoren von IT-Sicherheitsmaßnahmen.
- so soll die Bewertungsmethode für kompatibel mit den interagierenden Systemen der msu solutions GmbH gestaltet sein, um eine einfache und dennoch sichere Methode zum Einsatz bringen zu können

### UAP 2.6 - Ergebnissynthese und Erstellung eines Ergebniskatalogs für

#### Prozesseinflussgrößen, Bewertungsdimensionen und kritische fachliche Anforderungen

- Abgleich der bisherigen Ergebnisse mit vergangenen Praxisfällen aus ausgewählten Geschäftsprozessen von **msu.energie**
- Ergebnisdiskussion mit der MLU<sup>^</sup>
- Teilnahme an der Delphi-Studie zur Weiterentwicklung von Prozesseinflussdimensionen sowie konkreten Praxisbeispielen zu Prozessdimensionen
- Kategorisierung der Einflussdimensionen wurde erarbeitet und eine Priorisierung der Dimensionen durchgeführt

Definition	IT-Sicherheitsmaßnahmen – Wie beeinflusst die ITSM die Dimension auf Metaebene?	SpM (spezifische Beispiele aus den Interviews)	Neu
1 Beschreibe 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.	Durch die IT-Sicherheitsmaßnahmen muss zum Beispiel vor der Einführung einer Cloud-Plattform sich erst mit dem Anbieter die Plattform eingedringt wird, ist es wichtig sicherzustellen, dass die Kommunikation zwischen dem Unternehmen und der Verschlüsselung der Daten zu gewährleisten in diesem Fall muss das Unternehmen zunächst mit dem Cloud-Anbieter für eine verschlüsselte Kommunikation abstimmen. Weiterhin muss zum Beispiel der Cloud-Anbieter bestimmte zusätzliche Anforderungen, um eine verschlüsselte Kommunikation zu ermöglichen. Das Unternehmen müsste dann mit dem Anbieter dazu verhandeln und aushandeln.
2 Beschreibe 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.	Für die Implementierung der IT-Sicherheitsmaßnahmen müssen häufiger Technologiepezialisten hinzugezogen werden, um die Komplexität der Umsetzung der IT-Sicherheitsmaßnahmen zu managen, fehlendes Wissen in das Unternehmen zu integrieren oder mit externen Neutralität die Entscheidungsprozesse zu begleiten.	Für die Implementierung der IT-Sicherheitsmaßnahmen müssen häufiger Technologiepezialisten hinzugezogen werden. Sicherheitsmaßnahmen zu managen, fehlendes Wissen in das Unternehmen zu integrieren oder mit externen Neutralität. Z.B. wenn die IT-Infrastruktur modernisiert wird und im Rahmen dieser Modernisierung zusätzliche IT-Sicherheitsmaßnahmen Technologiepezialisten wie IT-Sicherheitsbetreuer oder Penetrationstester hinzugezogen werden. Diese Experten haben für IT-Sicherheitsstandards, -protokolle und -technologien und können dabei helfen, die besten Lösungen für das Unternehmen zu identifizieren.
3 Beschreibe die Koordination und Abstimmung mit verschiedenen Stakeholdern zur Initiierung und/oder Steuerung eines Prozesses.	Interne Abstimmung der IT-Sicherheitsmaßnahmen und Rahmenbedingungen.	Zum Beispiel müssen alternative Backup-Lösungen und deren potenzielle Auswirkungen auf die Prozesse und IT-Systeme analysiert werden.	Bevor die IT-Sicherheitsmaßnahmen implementiert werden können, müssen verschiedene Angebote von externen Anbietern intern abgestimmt werden. Z.B. wenn ein Unternehmen die Implementierung einer effizienten Backup-Lösung plant, um die verschiedenen Angebote von Backup-Anbietern eingeholt, geprüft und intern abgestimmt werden (z.B. potenzielle Auswirkungen auf die Prozesse und IT-Systeme analysiert werden).
4 Beschreibe die Koordination und Abstimmung mit verschiedenen Stakeholdern zur Initiierung und/oder Steuerung eines Prozesses.	Interne Abstimmung der IT-Sicherheitsmaßnahmen und Rahmenbedingungen.	Vor der Einführung der IT-Sicherheitsmaßnahmen müssen zu vergebenen Rechte/Rollen abgestimmt werden (z.B. wer darf auf welche Daten oder IT-Systeme zugreifen).	Vor der Einführung der IT-Sicherheitsmaßnahmen müssen zu vergebenen Rechte/Rollen abgestimmt werden. Z.B. um Systeme zu kontrollieren und zu schützen, müssen die zu vergebenen Rechte und Rollen intern sorgfältig abgestimmt und autorisierte Benutzer auf bestimmte Daten oder IT-Systeme zugreifen können. Das Unternehmen muss analysieren, wie Benutzer Zugriff auf welche Daten oder IT-Systeme benötigen, um ihre jeweiligen Aufgaben zu erfüllen.
5 Beschreibe die Koordination und Abstimmung mit verschiedenen Stakeholdern zur Initiierung und/oder Steuerung eines Prozesses.	Abstimmung der IT-Sicherheitsmaßnahmen und Rahmenbedingungen mit Kunden.	Durch die Implementierung der IT-Sicherheitsmaßnahmen kann es erforderlich sein, den Kunden einzulassen, insbesondere wenn der Prozess von Kundendaten abhängt (z.B. zum Beispiel, wenn bestimmte Daten von Kunden (z.B. IP-Adresse zur Zugriffserfassung auf IT-Systeme des Unternehmens) benötigt werden.	Durch die Implementierung der IT-Sicherheitsmaßnahmen kann es erforderlich sein, den Kunden einzulassen, insbesondere wenn der Prozess von Kundendaten abhängt. Ein konkretes Beispiel dafür könnte die Erhebung der IP-Adresse des Kunden zur Zugriffserfassung auf IT-Systeme sein. Ein konkretes Beispiel dafür könnte die Erhebung der IP-Adresse des Kunden zur Zugriffserfassung auf IT-Systeme sein. Ein konkretes Beispiel dafür könnte die Erhebung der IP-Adresse des Kunden zur Zugriffserfassung auf IT-Systeme sein. Ein konkretes Beispiel dafür könnte die Erhebung der IP-Adresse des Kunden zur Zugriffserfassung auf IT-Systeme sein.

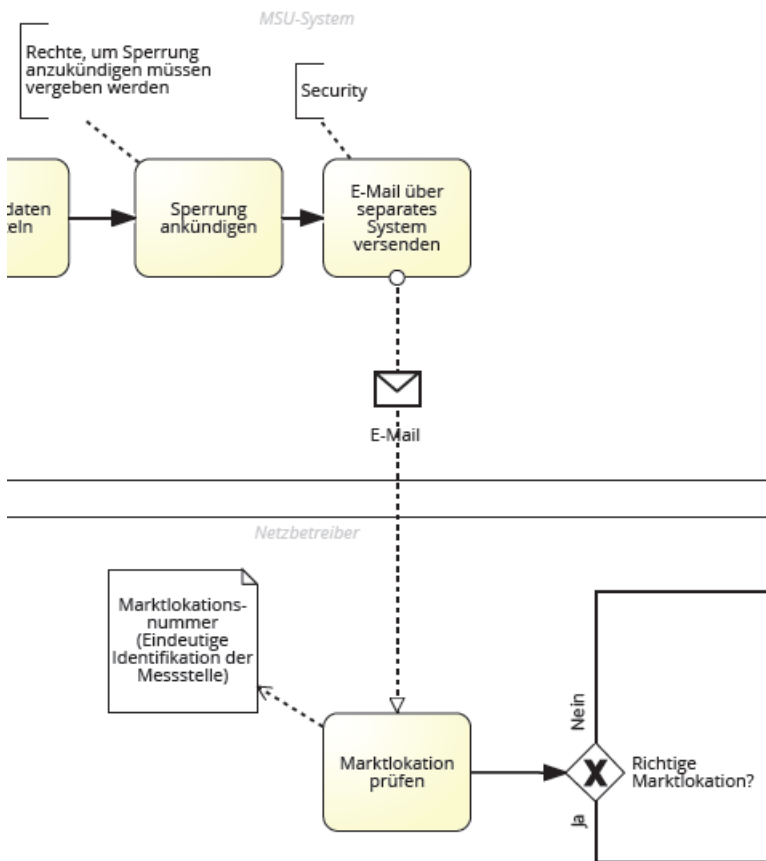
**Bild – Beispiele für die aus der Delphi-Studie entwickelten Dimensionen und Subdimensionen**

- Die ermittelten Dimensionen sind in der nachfolgenden Tabelle zusammengefasst. Es wird der Begriff der Dimension genannt und eine Definition zur näheren Erklärung beigefügt. Zusätzlich wird die Dimension einer Oberkategorie zugeordnet, um das Wirkungsumfeld der Dimension zu klassifizieren. Hierzu zählt die Kategorie Input für notwendige Tätigkeiten, die zur Erfüllung investiert werden müssen, Aktivität, welche den Prozessablauf bedingt und der Outcome, welches Dimensionen sind, die die Auswirkungen nach Außen zeigen.

## AP 3- Entwurf des multikriteriellen Entscheidungsmodells für ProBITS

### UAP 3.3 - Entwicklung von prozessorientierten Kosten-/Nutzenmodellen zur wirtschaftlichen Bewertung von IT-Sicherheitsmaßnahmen auf Grundlage von BPMN 2.0 und XES

- Formative Zwischenevaluation und iterative Weiterentwicklung des von der MLU entwickelten prozessorientierten Kosten-/Nutzenmodells auf Basis der Case Studies aus UAP 2.3
- Nähere Betrachtung der Prozessgestaltung in msu.energie hinsichtlich kundenrelevanter Abläufe im Bereich Stammdaten, Abrechnung und Smart Metering
- Entwicklung einer weiteren Fallstudie, welche die Durchführung der Marktkommunikation am Beispiel des „Sperr- und Entsperrungsprozesses“ thematisiert, sowie zugehörige Anforderungen, welche für die Anwendung und Evaluation des Entscheidungs- und Vorgehensmodells und des ProBITS-Tools notwendig sind
- diese wurde mithilfe der Durchführung der Delphi-Studie evaluiert und datenschutzrelevante Aspekte in dem Prozess visualisiert
- Beispielhaft wird das Ergebnis der Kosten- und Nutzenanalyse für den Geschäftsprozess Marktkommunikation für die Sperrung und Entsperrung erläutert
  - zur besseren Einschätzung der Sicherheitsmaßnahmen wurde der Prozess vorab skizziert, wobei wir hier nur einen der relevanten Ausschnitte darstellen



**Bild – Ausschnitt aus dem skizzierten Sperrprozess mit sicherheitsrelevanten Übertragungsweg vom System der msu solutions GmbH an den ausführenden Netzbetreiber**

- für die Kosten- und Nutzenanalyse wurden folgende Dimensionen paarweise in nxn Matrizen verglichen, um die Gewichtung dieser ermitteln zu können:
  - Mitarbeiterzufriedenheit entspricht w1
  - Kundenzufriedenheit entspricht w2
  - Datenschutz entspricht w3
  - Datenintegrität entspricht w4
  - Stabilität und Verfügbarkeit entspricht w5
- als Ergebnis erhielten wir folgende Fuzzy Gewichtungen:
  - w1= (0,094; 0,157; 0,219)
  - w2= (0,119; 0,170; 0,220)
  - w3= (0,314; 0,245; 0,189)
  - w4= (0,267; 0,224; 0,184)
  - w5= (0,211; 0,198; 0,189)
- folgende Sicherheitsmaßnahmen wurden mithilfe dieser Gewichtung im nachfolgenden Schritt miteinander verglichen
  - Benutzername/Kennwort entspricht ITSM A
  - Integrierte AD- Anmeldung entspricht ITSM B
  - Externe Verzeichnisanmeldung entspricht ITSM C
  - Manuelle AD-Anmeldung entspricht ITSM D
- das Ergebnis der Kosten- und Nutzenanalyse ergab sich daraufhin mit folgenden Werten:
  - ITSM A → 42,176
  - ITSM B → 62,241
  - ITSM C → 66,068
  - ITSM D → 46,416
- somit schneidet die externe Verzeichnisanmeldung in dieser Analyse am besten ab

Die hier ermittelten Werte decken sich mit den Experteneinschätzungen. Allerdings zeigte sich im weiteren Verlauf des Projektes, dass eine Kosten-Nutzen-Analyse nicht zielführend ist, da in allen probierten Fällen die Zahlen nur geschätzt werden konnten. Das Verfahren ist deutlich zu unpräzise und damit für einen Praxiseinsatz ungeeignet.

### UAP 3.5 - Entwicklung eines multikriteriellen Entscheidungsmodells zur wirtschaftlichen Bewertung und Analyse alternativer IT-Sicherheitsmaßnahmen(-bündel)

- Formative Zwischenevaluation des multikriteriellen Entscheidungsmodells anhand der Case Studies
- Iterative Verbesserung des multikriteriellen Entscheidungsmodells auf Basis der Erkenntnisse aus den Case Studies und des Feedbacks aus der Zwischenevaluation
  - auf der Grundlage der Kosten- und Nutzenanalyse wurde das multikriterielle Entscheidungsmodell entwickelt, welches anhand einfacherer Vergleiche ebenfalls die Sicherheitsmaßnahmen gegenüberstellt und bewertet
  - dieses wurde zur Bewertung des Marktkommunikationsprozesses zur Sperrung und Entsperrung eingesetzt
  - um die Bewertung für die Fachberater verständlich zu gestalten, wurden von dem Projektteilnehmern der MLU (BIM) Fragebögen entwickelt, die die einzelnen Mitarbeiter der MSU für sich ausfüllen konnte und die dann für die Auswertung herangezogen wurden
  - die nachfolgenden Bildausschnitte zeigen eine der Gegenüberstellung zur Einschätzung der Gewichtung der Dimensionen, die für die Bewertung herangezogen wurden, und eine Gegenüberstellung von zwei ausgewählten Sicherheitsmaßnahmen zur Bewertung der einzelnen vorher festgelegten Maßnahmen

	Mitarbeiter-zufriedenheit	Kunden-zufriedenheit	Datenschutz	Datenintegrität	Stabilität und Verfügbarkeit
<b>Experte/ Expertin</b>					
Mitarbeiterzufriedenheit	1				
Kundenzufriedenheit		1			
Datenschutz			1		
Datenintegrität				1	
Stabilität und Verfügbarkeit					1

Bild – Gewichtungstabelle zur Gegenüberstellung der einzelnen, vorab bestimmten Dimensionen

Benutzername/ Kennwort	Compare the relative importance related to the goal.																Externe Verzeichnisanmeldung	
	←-----→																	
	Extremely			Equally										Extremely				
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
	Mitarbeiterzufriedenheit																	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Kundenzufriedenheit																	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Datenschutz																	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Datenintegrität																	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	Stabilität und Verfügbarkeit																	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

**Bild – Gegenüberstellung von zwei der insgesamt vier bestimmten Sicherheitsmaßnahmen als Verdeutlichung innerhalb des Fragebogens**

- als Ergebnis der Gegenüberstellung zeigte sich eine Gewichtung von

Dimensionen	Gewichtung
Mitarbeiterzufriedenheit	0,034
Kundenzufriedenheit	0,064
Datenschutz	0,375
Datenintegrität	0,392
Stabilität und Verfügbarkeit	0,134
Summe	0,999

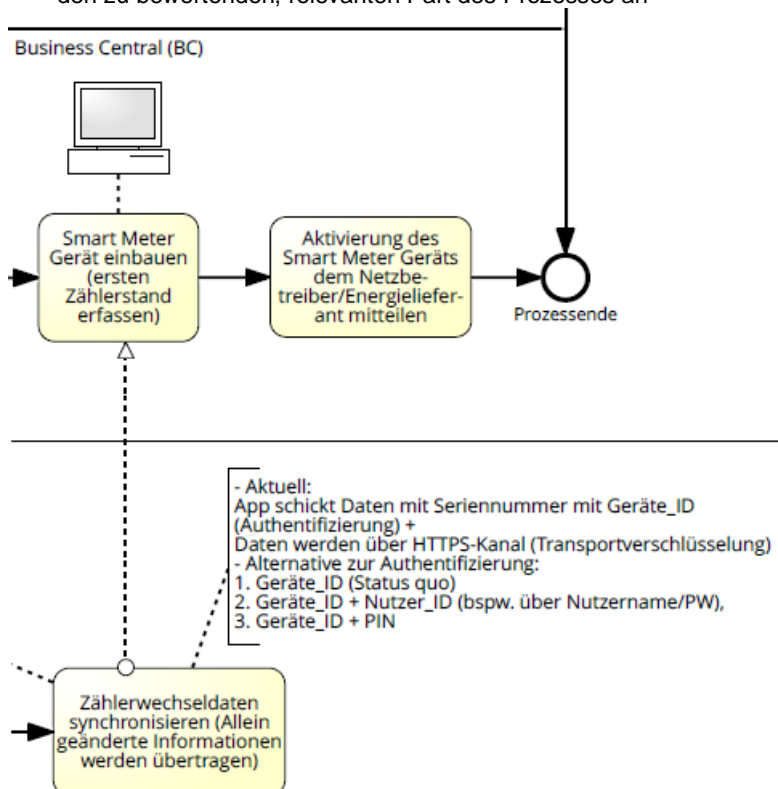
**Tabelle – Gewichtung der einzelnen Dimensionen**

mithilfe dieser Gewichtung ließen sich die Maßnahmen gegenüberstellen und vergleichen  
hierbei schneidet ebenfalls die externe Verzeichnisanmeldung am besten ab

Maßnahme/ Dimension	Mitarbeiter-zufriedenheit	Kunden-zufriedenheit	Datenschutz	Daten-integrität	Stabilität und Verfügbarkeit	TOTAL
Benutzername/ Kennwort	0,092	0,086	0,066	0,127	0,378	<b>0,134</b>
Integrierte AD-Anmeldung	0,555	0,531	0,289	0,301	0,376	<b>0,329</b>
Externe Verzeichnisanmeldung	0,270	0,306	0,545	0,390	0,087	<b>0,398</b>
Manuelle AD-Anmeldung	0,083	0,077	0,100	0,183	0,159	<b>0,138</b>
Summe	1,000	1,000	1,000	1,000	1,000	0,999

**Tabelle – Ergebnis der Gegenüberstellung der einzelnen Sicherheitsmaßnahmen**

- selbiges Verfahren wurde ebenfalls auf den Smart Meter Anwendungsfall angewandt
- hierfür wurde der Einbauprozess des Smart Meter genutzt und ebenfalls vorab skizziert, der Bildausschnitt zeigt den zu bewertenden, relevanten Part des Prozesses an



**Bild – Ausschnitt aus dem skizzierten Einbauprozess für das Smart Meter mit sicherheitsrelevanten Übertragungsweg vom System des Messstellenbetreibers der MSU APP an das Business Central (BC) System der msu solutions GmbH**

- es wurden für das Entscheidungsmodell die folgenden Sicherheitsmaßnahmen verglichen:
  - Authentifizierung mittels Geräte\_ID
  - Authentifizierung mittels Geräte\_ID und Nutzer\_ID
  - Authentifizierung mittels Geräte\_ID und PIN
  
- dabei kamen folgende Dimensionen für den Vergleich zum Einsatz
  - Abtimungs- und Planungsaufwand entspricht M1
  - Datenqualität entspricht M2
  - Flexibilität/ Anpassungsfähigkeit entspricht M3
  - Kompatibilität entspricht M4
  - Kooperationsmöglichkeit entspricht M5
  - Mitarbeiteraufwand entspricht M6
  - Mitarbeiterzufriedenheit entspricht M7
  - Prozessstreuung entspricht M8
  - Technologieaufwand entspricht M9
  - IT-Sicherheit entspricht M10
  
- die Gewichtung der Dimensionen wurde wie folgt ermittelt

Dimensionen	Gewichtung
Abtimungs- und Planungsaufwand	0,024
Datenqualität	0,27
Flexibilität/ Anpassungsfähigkeit	0,045
Kompatibilität	0,097
Kooperationsmöglichkeit	0,026
Mitarbeiteraufwand	0,051
Mitarbeiterzufriedenheit	0,054
Prozessstreuung	0,14
Technologieaufwand	0,041
IT-Sicherheit	0,252

**Tabelle – Gewichtung der einzelnen Dimensionen**

- daraus ergab sich nach Durchlauf des Entscheidungsmodells folgendes Ergebnis:

Maßnahme/ Dimension	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	TOTAL
Authentifizierung mittels Geräte_ID	0,4326	0,3333	0,5890	0,5328	0,3333	0,3751	0,5722	0,3579	0,3541	0,0754	<b>0,3209</b>
Authentifizierung mittels Geräte_ID und Nutzer_ID	0,1655	0,3333	0,1226	0,2000	0,3333	0,1612	0,1590	0,2841	0,2211	0,6584	<b>0,3591</b>
Authentifizierung mittels Geräte_ID und PIN	0,4019	0,3333	0,2883	0,2671	0,3333	0,4637	0,2687	0,3579	0,4248	0,2663	<b>0,3200</b>
Summe	1	1	1	1	1	1	1	1	1	1	1

**Tabelle – Ergebnis der Gegenüberstellung der einzelnen Sicherheitsmaßnahmen**

## AP 4 - Entwurf des ProBITS-Vorgehensmodells

### UAP 4.1 - Entwurf eines Vorgehensmodells für die skalierbare Umsetzung von ProBITS

- Definieren von Anforderungen und anschließende Evaluation des Vorgehensmodells für die Beratertätigkeit zur Vorgabe einer praxisorientierten Lösung hinsichtlich der Arbeit eines Energieversorgungsunternehmens auf der Grundlage von aufgetretenen Fallbeispielen und der Entwicklung der rechtlichen Grundlagen am Energiemarkt
- Berücksichtigung von einschlägigen Kosten- und Nutzendimensionen

### UAP 4.2 - Ausarbeitung von Vorlagen für das skalierbare Vorgehensmodell

- Definition von Evaluationskriterien aus der Perspektive eines Beratungsunternehmens
- Unterstützung bei der Identifizierung von Dimensionen und Dimensionsausprägungen von IT-Sicherheitsmaßnahmen auf IT-Investments über eine interviewbasierte Delphi-Studie.

- Es wurden quantitative und qualitative Dimensionen identifiziert
- Die msu solutions GmbH hat hierfür an mehreren Experteninterviews teilgenommen und damit direkt zur Identifizierung der Dimensionen beigetragen.
- Ein Auszug aus den identifizierten Dimensionen inkl. Definition sind:
  - Abstimmungsaufwand/Planung: Beschreibt die Koordination und Abstimmung zur Steuerung des Prozesses
  - Akzeptanz: Bereitschaft, etwas oder Personen zu akzeptieren
  - Automatisierungsgrad/Standardisierung: Beschreibt, inwiefern die Prozesse vereinheitlicht sind
  - Digitalisierungsgrad: Beschreibt, inwiefern der Prozess von der Sicherheitstechnologie abhängt bzw. inwiefern der Prozess ohne die Technologie überhaupt ausgeführt werden kann
  - Workaround: Umweg zur Vermeidung eines bekannten Fehlverhaltens eines Prozesses oder Systems
  - Dokumentationsaufwand: Beschreibt den Aufwand, Dokumentationen anfertigen zu müssen
- Review des Vorgehensmodells und der Vorlagen (insb. der Tailoring-Faktoren) aus der Perspektive eines Beratungsunternehmens

## **AP 5 – Entwicklung ProBITS-Werkzeug**

### **UAP 5.1 - Ableitung von fachlichen und technischen Anforderungen an ProBITS-IT-Werkzeug aus AP3 und AP4**

- Ableitung technischer und fachlicher Anforderungen aus der Unternehmenspraxis der MSU
  - Nutzung der zusammengetragenen Informationen und Vorgaben bei der Anwendung des ProBITS-Werkzeugs
- Einnahme der Rolle des Unternehmensberaters der Energieversorgung in den stattfindenden Workshops

### **UAP 5.2 - Entwicklung eines DV-Konzepts für das ProBITS-IT-Werkzeug**

- Bewertung des von den Verbundpartnern entwickelten DV-Konzepts für das ProBITS-Werkzeug
- Ableiten von Verbesserungsvorschlägen in Bezug auf das DV-Konzept

### **UAP 5.4 - Technische Testung, fachliche Testung und fortlaufende Verbesserung des ProBITS-IT-Werkzeugs**

- Entwurf und Durchführung von technischen Tests
  - Fachliches Testen des ProBITS-Werkzeugs in den von den MSU Kunden angewandten Geschäftsprozessen mit den zugrunde gelegten Praxisfällen
  - Fachliches Testen des ProBITS-Werkzeugs auf das von der MSU entwickelte und derzeit angewandte DSGVO-Modul
- Fachliches Testen des ProBITS Werkzeuges für das zukunftsrelevante Thema der intelligenten Messsysteme (Smart Metering) ohne zugrunde gelegte Altfälle

### **UAP 5.5 – Technische Dokumentation**

- Überarbeitung und Bewertung der von den Verbundpartnern entwickelten technischen Dokumentation

## **AP 6 – Evaluation und Weiterentwicklung ProBITS**

### **UAP 6.2 - Demonstrator 2: “ProBITS in Aktion” (Smart Meter) – Implementierung des ProBITS-Investitionsentscheidungsprozesses am Smart Meter (MSU)**

Der erste wesentliche Schritt zur Evaluation und Weiterentwicklung von proBITS war die Auswahl und Modellierung eines geeigneten Prozesses. Zur Auswahl konnte nur ein Prozess gewählt werden, der bereits in ähnlicher Form durchgeführt wurde, um die realen Entscheidungen an denen von proBITS zu messen. Ziel dieser Maßnahme ist es, den Prozess hinter proBITS auf mögliche Unschärfen und Fallstricke zu untersuchen.

Als geeigneter Prozess wurde der Einbauprozess SmartMeter bei der MSU ausgewählt. Dieser Prozess ist durch gesetzliche Vorgaben gut strukturiert und erlaubt an bestimmten Stellen eine dedizierte Auswahl von Sicherheitsmaßnahmen.

Als zweiter Punkt stand die Modellierung des Prozesses an. Hier wurde gemeinsam mit der MLU der Prozess in einem Geschäftsprozessdiagramm mittels BPNM erstellt:



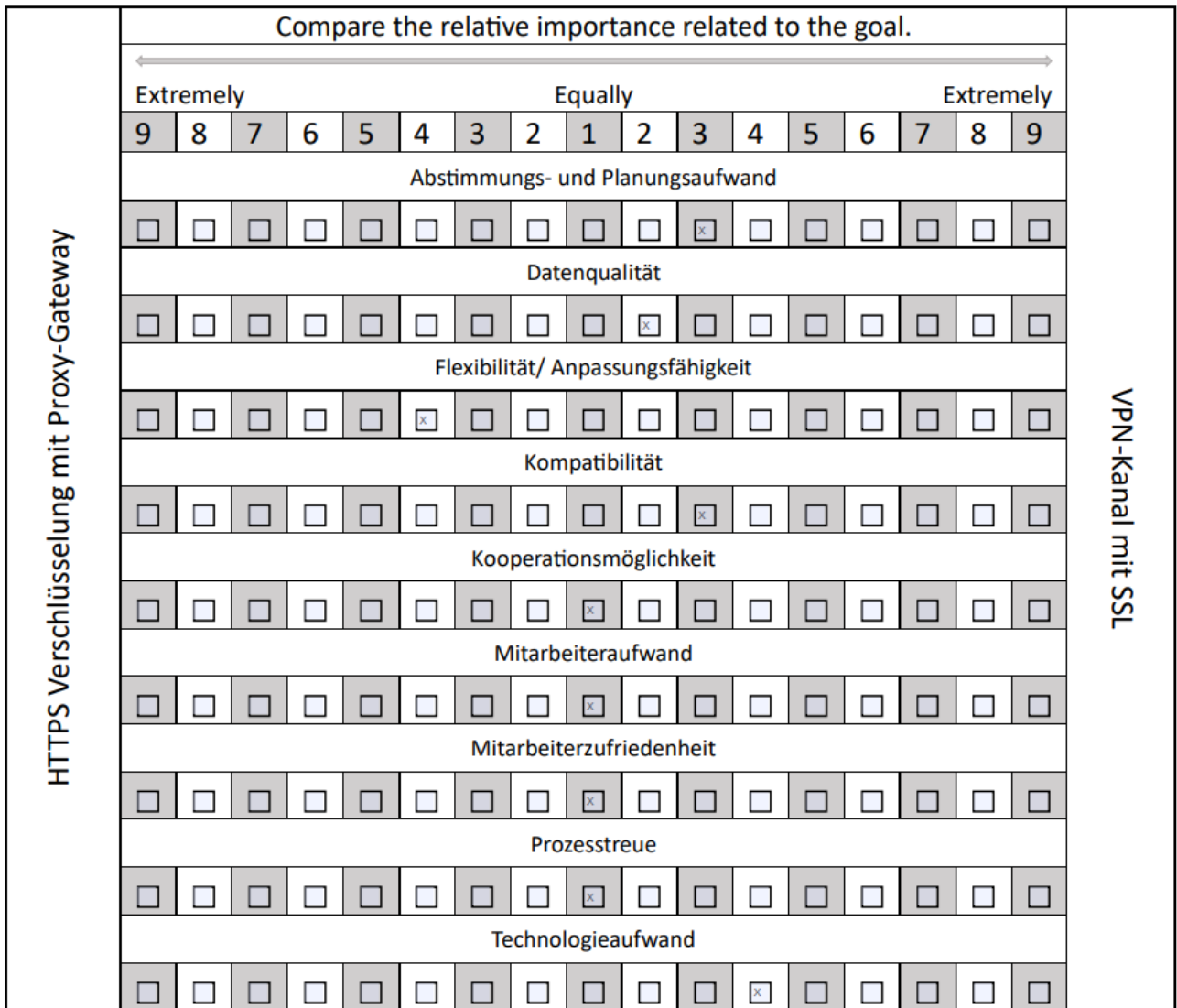


Bild –Gegenüberstellung von 2 Maßnahmen anhand aller gewählter Dimensionen

Die Auswertung der Ergebnisse hat die MLU (BIM) übernommen. Der gesamte Prozess ist recht aufwändig durchzuführen, allerdings lassen sich sämtliche Schritte nach der Bewertung sehr gut automatisieren:

Gesamt Abstimmungs- und Planungsaufwand				Gesamt Kooperationsmöglichkeit				Gesamt Mitarbeiterzufriedenheit				Gesamt Prozessreife			
HTTPS mit Proxy	VPN mit SSL	VPN mit IPsec	VPN mit WireGuard	HTTPS mit Proxy	VPN mit SSL	VPN mit IPsec	VPN mit WireGuard	HTTPS mit Proxy	VPN mit SSL	VPN mit IPsec	VPN mit WireGuard	HTTPS mit Proxy	VPN mit SSL	VPN mit IPsec	VPN mit WireGuard
1,000	0,815	2,000	3,152	1,000	1,000	1,000	1,000	1,000	0,500	0,447	0,378	1,000	1,414	1,414	1,414
1,225	1,000	2,445	0,707	1,000	1,000	1,000	1,000	2,000	1,000	0,577	0,378	0,707	1,000	1,414	2,236
0,500	0,408	1,000	0,408	1,000	1,000	1,000	1,000	2,236	1,732	1,000	0,378	0,707	0,707	1,000	1,414
0,315	1,414	2,445	1,000	1,000	1,000	1,000	1,000	2,646	2,646	2,646	1,000	0,707	0,447	0,707	1,000
<b>Geometrisches Mittel</b>				<b>Dimensionen</b>				<b>Priority Vector</b>							
HTTPS mit Proxy				Abstimmungs- und Planungsaufwand				0,036							
VPN mit SSL				Datenqualität				0,287							
VPN mit IPsec				Flexibilität				0,034							
VPN mit WireGuard				Anpassungsfähigkeit				0,338							
Summe				Kompatibilität				0,034							
				Kooperationsmöglichkeit				0,034							
				Mitarbeiteraufwand				0,032							
				Mitarbeiterzufriedenheit				0,034							
				Prozessreife				0,25							
				Technologieaufwand				0,087							
<b>Priority Vector</b>				<b>TOTAL</b>											
HTTPS mit Proxy				0,221											
VPN mit SSL				0,268											
VPN mit IPsec				0,234											
VPN mit WireGuard				0,285											
Summe				1											

Bild – Bewertungstabelle proBITS

Die Ergebnisse zeigen hier nur minimale Unterschiede der verschiedenen Handlungsoptionen. Dies deckt sich mit den tatsächlichen Beobachtungen. Allerdings stellten sich hier direkt 3 wesentliche Vorteile gegenüber einer Kosten-Nutzen-Bewertung heraus:

1. Es brauchte keine zuverlässigen Zahlen mehr. Durch die relativen Bewertungen sind Unschärfen

- unproblematisch und führen nicht zu einer Verzerrung. Auch ist der Bewertungsprozess dadurch insgesamt konsistenter, da kein einheitliches Zahlmaß mehr notwendig ist
2. Der Prozess ist pausierbar. Wo bei der Kosten-Nutzen-Bewertung ein pausieren der Analyse und späteres Fortsetzen kaum möglich ist, da sonst möglicherweise subjektive Schätzungen nicht mehr konsistent ausfallen, kann der Bewertungsprozess hier beliebig unterbrochen und später fortgesetzt werden. Das lässt den proBITS-Bewertungsprozess sehr viel nahtloser in den Arbeitsalltag integrieren.
  3. Es braucht nicht mehr ausschließlich Expertenmeinungen. Durch die Auswahl der Dimensionen aus verschiedenen Teilbereichen können auch Nicht-Experten zur Bewertung beitragen und so auch subjektive bzw. nicht geldlich abschätzbare Einflüsse bewertet werden. Der Prozess ist damit deutlich näher an den Menschen als an den Finanzen.

Das macht den Prozess insgesamt sehr solide und praxisnah. Dennoch zeigte sich hier bereits Verbesserungspotential. Einerseits ist eine Gewichtung einzelner Personengruppen nützlich, denn wenn bei einem Prozess die IT-Sicherheit im Fokus liegt, dann sollten Fachfremde Bewerber erhört, aber nicht so stark gewichtet werden. Ein weiterer Verbesserungsaspekt betrifft nicht den proBITS-Prozess selbst, sondern die Anwendung dessen: Eine hohe Auswahl an Dimensionen führt zu sehr ausgiebigen Fragebögen und entsprechend zu einem hohen Bearbeitungsaufwand.

Mit diesen Erkenntnissen kann der Prozess nun für eine reale Entscheidung angewendet werden um zu prüfen, ob er ohne Kenntnis des Ergebnisses funktioniert.

Derselbe Vorgang wurde für denselben Prozess aber einen anderen Aspekt, namentlich die Authentifizierung der Anwender des Messstellenbetreibers gegen das MSU-System durchgeführt. Dabei blieben die Dimensionen gleich, der Prozess ist ja noch derselbe, aber die Handlungsoptionen änderten sich und auch die bewertenden Personen – es wurden Entwickler, die an der Umsetzung beteiligt sind mit befragt. Die Optionen waren eine Authentifizierung mittels GeräteID, eine Authentifizierung mittels GeräteID und NutzerID und eine Authentifizierung mittels GeräteID und PIN. Hierbei wurden 2 Auswertungen gefahren: Einmal die Auswertung rein ohne Berücksichtigung von ITS, einmal mit Berücksichtigung der ITS.

Die Ergebnisse sind dabei plausibel. Für Anwender ist die Verwendung der GeräteID ohne Berücksichtigung der ITS die beste Methode, da diese am einfachsten auszuführen ist. Außerdem empfangen die Personen eine PIN leichter zu merken als eine Benutzerkennung.

Unter Einbeziehung der ITS drehten sich die Ergebnisse dann. Die zusätzliche Eingabe einer Benutzerkennung wurde als beste Option empfunden, obwohl diese von Anwendern als unangenehmste Option empfunden wurde. Dadurch, dass die Abstimmung der Anwender nicht nur zu den Teilaspekten untereinander, sondern auch zu deren Gewichtung stattfand, ist hier eine Verzerrung durch falsche Parameterwahl eher nicht gegeben.

Auch aus dieser Anwendung lassen sich Erkenntnisse gewinnen:

1. Die Gewichtung der einzelnen Aspekte scheint wichtig, wird aber durch die Anwender selbst vorgegeben. Die Bewertung bleibt konsistent, selbst wenn Teilaspekte sich zu widersprechen scheinen. Der proBITS-Prozess wird als sehr robust wahrgenommen
2. Die Auswahl der Dimensionen ist entscheidend. Da einzelne Dimensionen das Ergebnis sehr stark drehen können, ist es wichtig, dass initial bei der Dimensionsauswahl nichts vergessen wird.

### **UAP 6.3 - Demonstrator 3: “ProBITS deckt auf” – Retrospektive prozessorientierte Kosten/Nutzen-Analyse von getätigten ITS-Maßnahmen(-bündeln) für Kundenportale; Vergleich tatsächlich genutzte Verfahren, ROSI und ProBITS (MSU)**

Der nächste wesentliche Schritt zur Bewertung von proBITS ist die Gegenüberstellung mit einem anderem Bewertungsmodell anhand tatsächlich genutzter Verfahren. Gewählt ist hier ROSI als Alternativmodell.

Die Bearbeitungsschritte für proBITS waren wieder identisch. Der Prozess wurde ausgewählt und mittels BPMN modelliert, bevor die eigentliche Bewertung durchgeführt wurde. Dabei wurde der Prozess ausgewählt, der die Bearbeitung von Kundenthemen mithilfe von Supporttickets darstellt.

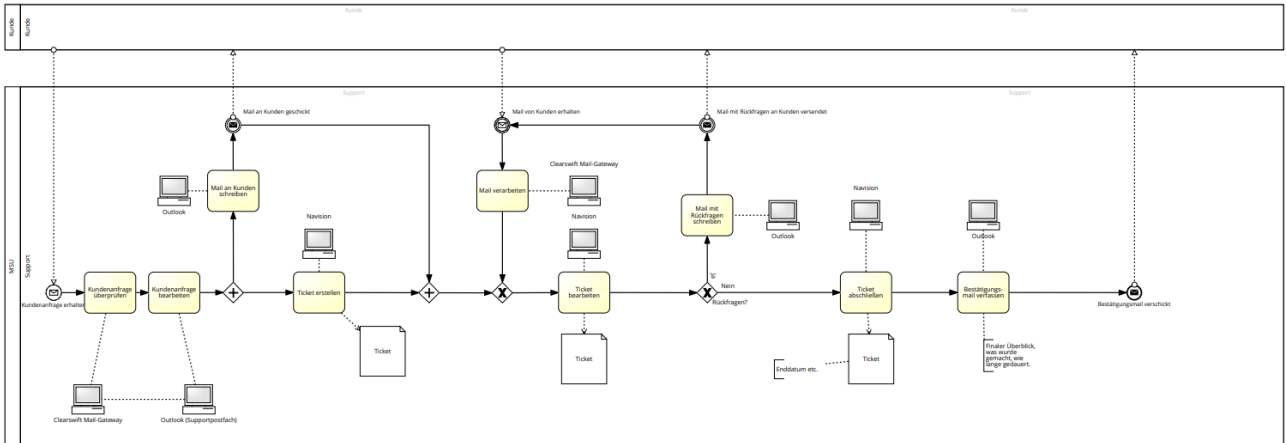


Bild – BPMN-Prozess MSU Supporttickets

Der betrachtete ITS-Aspekt der Bewertung ist die E-Mail-Kommunikation mit dem Kunden bzw. deren Absicherung. Zur Absicherung standen hier nur 2 Optionen: Ein sicheres E-Mail-Gateway einführen, oder nicht. Die gewählten Dimensionen sind in diesem Beispiel deutlich zahlreicher, da der Prozess fast alle Abteilungen und Bereiche betreffen kann und maßgeblich die tägliche Arbeit des Supports der MSU beschreibt. Dies führte zu einer zeitaufwendigen Gewichtung der Dimensionen gegeneinander, wohingegen die eigentliche Bewertung der Maßnahmen gegeneinander eher kurz ausfällt. Das ist soweit auch wenig Verwunderlich, wenn man betrachtet, wie weitreichend die Auswirkungen der Maßnahme sind.

	Compare the relative importance related to the goal.																	
	←-----→																	
	Extremely			Equally										Extremely				
	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Datenverfügbarkeit
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Dokumentationsaufwand
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozessdurchlaufzeit
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	IT-Sicherheitsbewusstsein
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Kundenzufriedenheit
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Mitarbeiteraufwand
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozessergebnis
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozessverständnis
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Schulungsaufwand
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozessstabilität
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozessverfügbarkeit
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozessstandardisierung
Abstimmungs- und Planungsaufwand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Prozesswiederherstellbarkeit

Bild – Auszug aus Bewertung E-Mail-Gateway, zeigt alle Dimensionen

Die mathematische Auswertung des proBITS-Modells übernahm wieder die MLU (BIM). Das Ergebnis war eine deutliche

Bevorzugung der Handlungsoption Einführung E-Mail-Gateway.

Als zweites wurde ein ITS-Prozess nach ROSI bewertet. Hierbei zwei Prozesse gewählt, um keine Verfälschung der Ergebnisse durch ein schlechtes Beispiel zu haben. Es wurde sich dafür entschieden, den Zählerwechselprozess (Einbauprozess Smart Meter), der auch schon im UAP 6.2 Anwendung fand, zu verwenden sowie die Einführung des sicheren E-Mail-Gateways, der ebenfalls in UAP 6.2 beschrieben wurde.

Der erste Schritt bestand darin, die benötigten Werte für ROSI zu schätzen. Hier offenbart sich aber schon eine sehr große Schwäche von ROSI: Wo die Anschaffung und Investition noch gut ermittelbar sind, sind Schadenskosten bestenfalls Schätzungen. Neben dieser großen Unschärfe sind außerdem weitere Modelle nötig, um verschiedene Schadensfälle berücksichtigen zu können. Obwohl ROSI damit von weniger Parametern abhängt, ist die Arbeit, die für die Anwendung des Modells nötig ist, keinesfalls geringer.

Nachdem mit viel Aufwand die Parameter von 4 verschiedenen Personen geschätzt und deren Mittelwerte für die Berechnung von ROSI herangezogen wurden, hat die MLU (BIM) die mathematische Auswertung getätigt und die Ergebnisse wurden gemeinsam analysiert. Um eine sinnvolle Entscheidung fällen zu können, wurden dabei für die Maßnahme Authentifizierung der Nutzer aus dem Prozess die einzelnen Maßnahmen separat bewertet. Außerdem wurden 3 Szenarien, nämlich best case, most common case und worst case berücksichtigt. Das führe zu einer großen Anzahl an ROSI-Bewertungen, Beispielhaft ist hier eine der 3 Maßnahmen als Bild aufgeführt.

Min					Mittel					Max				
Teilnehmer	Einzel	Einzel	ALE		Teilnehmer	Einzel	Einzel	ALE		Teilnehmer	Einzel	Einzel	ALE	
	P	W				P	W				P	W		
Erik	1600	0,45	720		Erik	18.600	0,45	8370		Erik	281.600	0,45	126720	
Jennifer	1600	0,1	160		Jennifer	18.600	0,1	1860		Jennifer	281.600	0,1	28160	
Jan	1600	0,03	48		Jan	18.600	0,03	558		Jan	281.600	0,03	8448	
Hfuchs	1600	0,02	32		Hfuchs	18.600	0,02	372		Hfuchs	281.600	0,02	5632	
Summe			240		Summe			2790		Summe			42240	
Teilnehmer	ALE	E	K_Ges	ROSI	Teilnehmer	ALE	E	K_Ges	ROSI	Teilnehmer	ALE	E	K_Ges	ROSI
Erik	240	0,91	1	217,4	Erik	2790	0,91	1	2537,9	Erik	42240	0,91	1	38437,4
Jennifer	240	0,1	1	23	Jennifer	2790	0,1	1	278	Jennifer	42240	0,1	1	4223
Jan	240	0,9	1	215	Jan	2790	0,9	1	2510	Jan	42240	0,9	1	38015
Hfuchs	240	0	1	-1	Hfuchs	2790	0	1	-1	Hfuchs	42240	0	1	-1
Summe				133,6	Summe				1331,225	Summe				20168,6

**Bild – Bewertung ROSI, Fall „GeräteID“, 3 verschiedene Schadensfälle**

Die Auswertung der Ergebnisse zeigt, das ROSI nicht nur im Vergleich mit proBITS, sondern sogar generell nicht zur Bewertung von ITS-Maßnahmen zu empfehlen ist. Die Ergebnisse selbst unterscheiden sich gar nicht so stark von den proBITS-Ergebnissen ohne Berücksichtigung der ITS-Maßnahmen, jedoch sehr sobald die ITS Teil der Bewertung ist. So hat ROSI die Authentifizierungsoption „nur GeräteID“ bevorzugt, proBITS unter Berücksichtigung von ITS hingegen die Option „GeräteID + NutzerID“. Diese Option kam bei ROSI hingegen am schlechtesten weg. Auch kam bei ROSI eine Empfehlung GEGEN das E-Mail-Gateway heraus.

Eine Analyse der Ergebnisse zeigte, dass ROSI sich auf rein finanzielle Aspekte stützt. Dabei sind ausschließlich Investitions- und Implementierungskosten zuverlässig möglich anzugeben, alle anderen Werte sind reine Schätzwerte. Es ist also möglich, dass hier komplett falsche Werte angenommen wurden und es gibt keinerlei Kontrollmöglichkeit.

Zusammenfassend sind folgende Ergebnisse festzuhalten:

- proBITS ist in der Bedienung sehr viel leichter, da deutlich mehr Eingabewerte deutlich weniger Schätzfehler produzieren
- proBITS kann mehrere Optionen gegeneinander abwägen, ROSI nur durch mehrfache Anwendung und Vergleich der Ergebnisse. Dabei gibt es in ROSI keine Möglichkeit die Ergebnisse konsistent zu halten, durch Verfahrensfehler oder Pausen in der Durchführung sind die Ergebnisse anfällig für Fehler
- proBITS hat eine gewisse Selbstkorrektur, da widersprüchliche Angaben erkannt werden können
- proBITS ist ohne Kenntnis der Zahlen durchführbar. Das führt nicht nur dazu, dass es mehr Personen zugänglich ist, sondern auch dass proBITS von Anwendern und nicht nur von Buchhaltern durchführbar ist
- proBITS berücksichtigt nicht nur finanzielle Aspekte, sondern ist auch in der Lage die Einflüsse auf die zugrundeliegenden Prozesse zu bewerten
- proBITS und ROSI sind in der Durchführung ähnlich schnell.

Neben den analytischen Prozessen fühlte sich ROSI in der Durchführung auch sehr schwammig und unpräzise an, man hatte selbst bei gewissenhafter Vorbereitung kein Vertrauen in die Zahlen. proBITS hingegen wirkte nicht nur schlüssiger, sondern auch robuster und lässt sich durch seine Pausierbarkeit sehr gut in den Arbeitsalltag integrieren. Im direkten Vergleich mit ROSI ist es das eindeutig überlegene Modell.

## **AP 7 – Kommunikation und Diffusion ProBITS**

### **UAP 7.2 - Entwicklung von Umsetzungshilfen für die Diffusion von ProBITS inkl. Best Practice Beschreibungen bzgl. Demonstrator 1 und 2**

Erstellung von Umsetzungs- und Anwendungshilfen sowie von Best Practices auf Basis der gewonnenen Erkenntnisse aus AP6

### **UAP 7.3 - Erstellung der Projektdokumentation für die Ergebniskommunikation**

- Praktische und fachliche Prüfung der von den Verbundpartnern verfassten Ergebniskommunikation
- Teilnahme an Fokusgruppenworkshops und Expertenbefragungen zu Dimensionen, Einflussgrößen und Entscheidungsfaktoren von IT-Sicherheitsmaßnahmen und zur Erarbeitung der Fallstudie für ProBITS

### **UAP 7.6 - Organisation von und Teilnahme an öffentlichkeitswirksamen (regionalen) Veranstaltungen, Präsentation auf Fachtagungen, Messen, etc.**

- Fachliche Vorbereitung und Realisierung einer speziellen Praktiker-Fachtagung zu den ProBITS-Bausteinen und dem ProBITS-Werkzeug
- Informationsdiffusion im Rahmen weiterer (regionaler) Praktiker-Fachtagungen

## **3. Wesentliche Ergebnisse**

Die detaillierte Darstellung der Ergebnisse wurde in Kapitel 2 und der Beschreibung des Ablaufs des Teilvorhabens ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen dargestellt. Die wesentlichen Ergebnisse des Projektes können daher nochmals wie folgt zusammengefasst werden:

- proBITS hat die Möglichkeit, ITS-Entscheidungen zu vereinfachen und mehr Unternehmen zugänglich zu machen. Die Kenntnisse, die für eine erfolgreiche Anwendung nötig sind, lassen sich durch Schulungen vermitteln und die Bewertungen sind intuitiv und von jederman ausführbar.
- proBITS ist im Vergleich mit anderen Bewertungsmethoden besser in den Arbeitsalltag integrierbar und nicht so anfällig für einzelne Fehler. Die Entscheidungen sind robuster und nachvollziehbarer.
- proBITS ermöglicht einen Vergleich verschiedener Maßnahmen und ist nicht nur auf die Qualität einer Maßnahme bezogen. proBITS ermöglicht außerdem die Bewertung von Maßnahmen im Prozesskontext, nicht losgelöst als reine ITS-Maßnahme. Das macht die Bewertungen deutlich wertvoller als rein finanzielle Analysen.

## **4. Wichtigste Positionen des zahlenmäßigen Nachweises**

Dieses Dokument ist separat eingereicht.

## **5. Notwendigkeit und Angemessenheit der geleisteten Projektarbeiten**

Das Teilvorhaben ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen war ein wesentlicher Bestandteil des ProBITS-Gesamtprojekts, mit dem Ziel, einen innovativen Ansatz zu entwickeln, der eine geschäftsprozessorientierte Bewertung von IT-Sicherheitsmaßnahmen ermöglicht. Im Folgenden werden die Angemessenheit und Notwendigkeit der geleisteten Arbeiten zum Erfolg und Ablauf des Projekts diskutiert.

Im Zentrum des Projekts stand die Erarbeitung eines Bewertungsmodells von ITS-Maßnahmen welches sich in den Arbeitsalltag von Unternehmen integrieren lässt und dabei nicht nur rein finanzielle Aspekte berücksichtigt.

Die Arbeit im Teilvorhaben ProBITS in Aktion & ProBITS deckt auf: Demonstration der Anwendbarkeit sowie vergleichende retrograde Analysen war in hohem Maße zielorientiert, um den Projekterfolg zu sichern und adäquat zu kommunizieren. Die Kombination aus bedarfsorientierter Technologieentwicklung, nutzerzentriertem Design, interdisziplinärer Forschung und dem Fokus auf Skalierbarkeit und Nachhaltigkeit zeichnet die Qualität und Relevanz der geleisteten Arbeit aus. Damit wurde ein wesentlicher Beitrag zum Projekterfolg und -verlauf geleistet.

## 6. Verwertbarkeit der Ergebnisse

Die in proBITS erzielten Ergebnisse sind ein Bewertungsmodell von ITS-Maßnahmen, welches die Prozesse in Unternehmen berücksichtigt und sich nicht ausschließlich auf finanzielle Aspekte stützt. Außerdem ist die Bewertung fehlerunanfällig und kann von „jedermann“ durchgeführt werden. Auch Unternehmen ohne ausgeprägte IT-Buchhaltung können proBITS anwenden und so ihre Maßnahmen zur IT-Sicherheit effizienter planen. Die Hürden zur Nutzung sind überaus gering, die Anwendbarkeit ist gegeben und sie lässt sich mit dem Arbeitsalltag vereinbaren.

## 7. Erfolge und geplante Veröffentlichungen

Die MSU plant keine eigenen Veröffentlichungen zum Thema.

## 8. „Einhaltung der Ausgaben- und Zeitplanung“ des Erfolgskontrollberichts:

Das Teilvorhaben der MSU wurde kostenneutral um drei Monate (04/2024 – 06/2024) verlängert. Grund dafür war die verzögerte Einführung des Smart Meter Rollouts sowie das zeitliche Zusammentreffen des Projektstarts mit der Covid-19-Pandemie. Dies führte zu einer mehrmonatigen Verzögerung bei der Erarbeitung der Arbeitspakete 3, 6 und 7. Im Rahmen der Projektlaufzeit (inkl. dreimonatiger kostenneutraler Verlängerung) kam es daher zu kleineren Verschiebungen der Arbeitspakete. Abschließend konnten jedoch alle Projektziele von proBITS vollumgänglich und in der angestrebten Qualität erreicht werden. Die Ausgabenplanung wurde eingehalten. Siehe hierzu Kapitel 4 des Abschlussberichts.

## 8. Projekt-Team

Prof. Dr. Stefan Sackmann



Prof. Dr. Sackmann hat seit 2009 die Professur für Wirtschaftsinformatik, insb. Betriebliches Informationsmanagement an der Martin-Luther-Universität HalleWittenberg inne. Sein Forschungsschwerpunkt liegt unter anderem auf der zivilen Sicherheitsforschung (Katastrophenmanagement) und der Digitalen Transformation im Pflege- und Gesundheitskontext. Im Kern stehen in allen Projekten – und so auch im Projekt KEVALiS – die Zusammenarbeit von Menschen und Computern sowie 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 (<https://informationsmanagement.wiwi.uni-halle.de/projekte/>).

## Dr. Stephan Kühnel



Dr. Stephan Kühnel ist Habilitand, Dozent und Projektleiter an der Professur für Wirtschaftsinformatik, insb. Betriebliches Informationsmanagement der MartinLuther-Universität Halle-Wittenberg und Evaluationsbeauftragter am dortigen Wirtschaftswissenschaftlichen Bereich. 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 vom BMBF geförderte Projekt „Prozess-orientierte wirtschaftliche

Bewertung und Auswahl von IT-Sicherheitsmaßnahmen“ ([ProBITS](#)), in dem er eine leitende Funktion ausübt. In der Forschung beschäftigt er sich unter anderem mit Informationssicherheit sowie der Konzeption und Evaluation von Informationssystemen, insbesondere im AR-Umfeld. Seine Forschungsergebnisse wurden in zahlreichen Journalen und Tagungsbänden, wie bspw. ACM Computing Surveys, Computers & Security, Journal of Decision Systems, European Conference

on Information Systems und International Conference on Conceptual Modeling veröffentlicht. Als Experte im Bereich Design Science Research, Informations- und Geschäftsprozessmanagement war er wesentlich an der Ideenfindung, Konzeption und Antragstellung/-ausarbeitung des Verbundprojektes ALiS beteiligt und hat im Teilprojekt KEVALiS an der Erforschung, Evaluation und Publikation der DesignTheorie und Referenzarchitektur mitgewirkt.

Usw.