MASTERARBEIT

zur Erlangung des akademischen Grades

MASTER OF SCIENCE (M.SC.)

Hochschule Zittau/Görlitz Fakultät für Natur- und Umweltwissenschaften

Studiengang Integrierte Managementsysteme

In Kooperation mit dem Fraunhofer-Institut für Organische Elektronik, Elektronenstrahl- und Plasmatechnik FEP Dresden

Integration neuer Anforderungen in ein bestehendes Managementsystem

Am Beispiel der Informationssicherheit im Projektgeschäft am Fraunhofer-Institut FEP Dresden

Vorgelegt von:	Patric Gerö
Matrikelnummer:	212310
Betreuer der Hochschule:	Prof. Dr. rer. pol. Jana Brauweiler
Zweitgutachter/Betrieblicher Betreuer:	M. Sc. Sabine Nolting
Bearbeitungszeitraum	01.09.2020
Abgabedatum	01.03.2021

I Inhaltsverzeichnis

II Abbildungsverzeichnis

III Tabellenverzeichnis

IV Abkürzungsverzeichnis

AMS ..... Arbeitssicherheitsmanagementsystem
EMB ..... Energiemanagementbeauftragter
EMS ..... Energiemanagementsystem
FhG ..... Fraunhofer Gesellschaft
HLS ..... High Level Structure
IMS ..... integriertes Managementsystem
IS ..... Informationssicherheit
ISB ..... Informationssicherheitsbeauftragter
ISMS ..... Informationssicherheitsmanagementsystem
IT ..... Informationstechnik
KVP ..... Kontinuierlicher Verbesserungsprozess
MS ..... Managementsystem
PDCA-Zyklus ..... Plan-Do-Check-Act-Zyklus
PM ..... Projektmanagement
QMB ..... Qualitätsmanagementbeauftragter
UK ..... Unternehmenskommunikation
UMS ..... Umweltmanagementsystem
ZV ..... Zentralverwaltung

1 Einleitung und Zielsetzung der Arbeit

1.1 Motivation

Aufgrund der kontinuierlichen Weiterentwicklung in Management und Geschäftsprozessen, wird es immer notwendig sein, neue Anforderungen bestmöglich und nachhaltig zu integrieren. Das kann von der Einführung eines ganzen Managementsystems (MS), über die Implementierung von bereichsspezifischen Anforderungen, bis hin zur Veränderung eines einzelnen Prozesses oder Prozessschritts sein. Die vorliegende Arbeit, soll das Fraunhofer-Institut FEP bei der Integration neu vorgegebener Anforderungen der Fraunhofer Zentralverwaltung unterstützen. Die Umsetzung der neuen Anforderungen zur Informationssicherheit (IS) und zum Datenschutz, sollen gleichzeitig zur Einführung eines zertifizierungsfähigen Informationssicherheitsmanagementsystems (ISMS) beitragen.

Aufgrund spezieller Bedingungen in jeder Organisation, ist die praktische Umsetzung neuer Anforderungen schwierig. Je mehr Bedingungen beachtet werden müssen, desto komplexer gestaltet sich die Aufgabe der Integration. In der vorliegenden Arbeit soll geprüft werden, welche Methoden helfen ein Managementsystem zu untersuchen. Auf Basis dieser Ergebnisse sowie dem Beachten wichtiger Bedingungen, soll eine Möglichkeit zur Implementierung neuer Anforderungen in ein bereits bestehendes integriertes Managementsystem (IMS) entwickelt werden.

Die Motivation dieser Arbeit ist es eine Nachhaltige Leistung in Form einer Richtlinie bzw. Vorlage zu entwickeln, wie neue Anforderungen in ein bestehendes integriertes Managementsystem implementiert werden können. Neue Anforderungen sollen so, durch eine normierte Wiederholbarkeit, zukünftig mit gleichem Erfolg umgesetzt werden können.

1.2 Ziel der Arbeit

Das Ziel der Arbeit ist es die neuen Anforderungen der Fraunhofer Zentralverwaltung zur Informationssicherheit und zum Datenschutz in das bestehende integrierte

Managementsystem am Fraunhofer FEP zu implementieren. Aus diesem Ziel ergibt sich folgende Forschungsfrage:

- Gibt es eine Möglichkeit einer standardisierten Wirksamkeitsbewertung auf Prozessebene nach der Integration neuer Anforderungen?

Neben diesem Hauptziel, gibt es weitere Soll- und Kann-Ziele. Ein Soll-Ziel ist die Entwicklung der bereits im vorherigen Kapitel erwähnten Richtlinie, zur Integration neuer Anforderungen in ein bestehendes IMS, in Form eines Leitfadens. Dieses Ziel führt zu folgenden zwei Forschungsfragen:

- Kann ein Methodenbaukasten zur Analyse von Managementsystemen zur Verfügung gestellt werden?
- Gibt es eine Möglichkeit zur Normierung der Umsetzung neuer Anforderungen in Organisationen?

Das zweite Soll-Ziel ist es, das Projektmanagement (PM) am Fraunhofer FEP zu untersuchen und die ermittelten Verbesserungsmöglichkeiten umzusetzen. Zu den Kann-Zielen gehören das Erstellen von Schulungsunterlagen für Informationssicherheit und Datenschutz sowie das Entwickeln einer Intranetseite für das ISMS. Die eben vorgestellten Ziele, zählen zu den Ergebniszielen dieser Arbeit. Zusätzlich wurden Ziele festgelegt, welche im Verlauf der Arbeit erreicht werden sollen. Diese Hauptvorgehensziele, sind die Ermittlung geeigneter Analysemethoden für ein IMS, die Analyse des IMS mit diesen geeigneten Methoden, das Ableiten von Maßnahmen und die Umsetzung dieser Maßnahmen. Mit dem Umsetzen der Maßnahmen wird die Integration der neuen Anforderung der Fraunhofer Zentralverwaltung (ZV) durchgeführt. Ein Soll-Vorgehensziel ist das Zusammentragen von Informationen zum Projektmanagement am Fraunhofer FEP und als Kann-Vorgehensziel wird die Entwicklung eines Verfahrens zur Priorisierung der Umsetzung von Maßnahmen festgelegt. Das Ziel der Priorisierung der Umsetzung von Maßnahmen führt zu einer weiteren Forschungsfrage:

- Wie kann die Komplexität in der Priorisierung der Umsetzung der Maßnahmen mit einbezogen werden?

Nicht-Ziele sind, das Verändern von Prozessen im Projektmanagement, welche keinen Bezug zu Informationssicherheit und Datenschutz haben und Dokumente sowie andere Anpassungen in englischer Sprache zu verfassen. Ein weiteres Nicht-Ziel ist das durchführen weiterer Audits nach der Integration durch den Verfasser der Arbeit.

1.3 Methodik und Vorgehensweise

Nach dem Abschluss der einleitenden Worte in Kap. 1, sind in Kap. 2 wichtige Grundlagen im Zusammenhang mit Managementsystemen vorgestellt. Dazu werden in Kap. 2.1 wichtige Fachausdrücke Definiert und in Kap. 2.2 die High-Level-Structure, der Plan-Do-Check-Act-Zyklus (PDCA-Zyklus) und der Kontinuierliche Verbesserungsprozess beschrieben. Kap. 2.3 handelt von integrierten Managementsystemen. Im ersten Teil dieses Kapitels, wird erläutert, dass die Anwendung verschiedene Managementsystemstandards nicht zu mehreren Managementsystemen in einer Organisation führt (Kap. 2.3.1). Als nächstes werden die Ziele von integrierten Managementsystemen vorgestellt (Kap.2.3.2). In Kap. 2.3.3 wird neben der Addition, welche ein vorläufiges Integrationskonzept ist, das Integrationskonzept der partiellen Integration, der systemübergreifenden Integration und der prozessorientierten Integration erläutert. Zum Schluss wird im Kap. 2.3.4 über mögliche Kritik an integrierten Managementsystemen berichtet.

Weil bei der Integration neuer Anforderung in ein bestehendes integriertes Managementsystem auf viele verschiedene Faktoren und Bedingungen geachtet werden muss, wird im Kap. 3 das Thema Komplexität behandelt. Dazu werden zuerst wichtige Begriffe abgegrenzt (Kap. 3.1). Daraufhin werden die Ziele des Managements in Bezug auf Komplexität erläutert (Kap. 3.2). Ein wesentlicher Punkt dieses Kapitels ist es zu ermitteln, welche Treiber von Komplexität in Managementsystemen eine Rolle spielen (Kap. 3.3) und welche Methoden angewendet werden können, die Komplexität zu reduzieren (Kap. 3.4).

Im Kap. 4 findet eine Vorstellung des Fraunhofer FEP statt (Kap. 4.1). Weil die neuen Anforderungen integriert werden sollen, wird im gleichen Zug, dessen integriertes Managementsystem vorgestellt (Kap. 4.2). Die von der Fraunhofer Zentralverwaltung gestellten Anforderungen, werden im Kap. 4.3 beschrieben. Im letzten Punkt von Kap. 4,

dem Kap. 4.4 werden erste Betrachtungen zur bevorstehenden Aufgabe der Integration vorgenommen. Neben dem Durchführen verschiedener Vorbetrachtungen, wird hier auch auf die Forschungsfrage eingegangen, ob ein Methodenbaukasten zur Analyse von Managementsystemen zur Verfügung gestellt werden kann.

Im nächsten Kapitel (Kap. 5), werden mögliche Analysemethoden zur Untersuchung von (integrierten) Managementsystemen vorgestellt (Kap. 5.1 bis 5.8). Weil sich nicht alle Methoden zur Analyse von (integrierten) Managementsystemen eignen, wird im Kap. 5.9 eine Prüfung durchgeführt, welche Methoden für die Erfüllung der Aufgabe der Integration genutzt werden sollen.

Im Kapitel der Datenerhebung und Auswertung (Kap. 6) wird beschrieben, wie die Analysemethoden, welche sich in Kap. 5 als geeignet zur Analyse von (integrierten) Managementsystemen herausgestellt haben, angewendet werden (Kap. 6.1 bis 6.4). Neben der Anwendung wird gleichzeitig eine Auswertung der Analysen vorgenommen. Aus der Analyse des integrierten Managementsystems am Fraunhofer FEP, wurden mehrere Maßnahmen abgeleitet (Kap. **Fehler! Verweisquelle konnte nicht gefunden werden.**). Diese Maßnahmen werden in einem Maßnahmenkatalog zusammengefasst. Neben dem Erstellen des Maßnahmenkatalogs, wird eine Möglichkeit zur Berechnung der Priorisierung zur Umsetzung der Maßnahmen vorgestellt. Damit wird der Forschungsfrage, ob Komplexität in der Priorisierung der Maßnahmen mit einbezogen werden kann, nachgekommen.

Kap. 7 handelt von der Integration der neuen Anforderungen. Im Kap. 7.1 werden die Verbesserungen im Projektmanagement des Fraunhofer FEP beschrieben. Im nächsten Schritt (Kap. 7.2), wird beschrieben wie die abgeleiteten Maßnahmen umgesetzt werden. Die Bewertung der Wirksamkeit der Integration ist Gegenstand von Kap. 7.3. Des Weiteren wird ein Ausblick auf die geplante Einführung von SAP im Jahr 2022 gegeben.

Im vorletzten Kapitel, wird die Entwicklung des Leitfaden zur Integration neuer Anforderungen in ein bestehendes (integriertes) Managementsystem, behandelt (Kap. 8). Dabei werden zuerst die Ziele und darauffolgend der Aufbau beschrieben (Kap. 8.1). Kap 8.2 handelt über die Anwendung des Leitfadens.

Im letzten Kapitel (Kap. 9) werden die Ergebnisse der vorliegenden Arbeit zusammengefasst und kritisch hinterfragt. Zusätzlich werden die vorgegebenen Ziele und Forschungsfragen aus Kap. 1.2 aufgegriffen und diskutiert. Die Arbeit wird mit einem Ausblick zur weiterführenden Bearbeitung des Themas und der Ableitung weiteren Forschungsbedarfs abgeschlossen.

2 Grundlagen

2.1 Definition und Ziele von Management und Managementsystemen

Der internationale Begriff Management hat seinen Ursprung im lateinischen „manus“ (=Hand), aus dem sich das italienische Wort „maneggiare“ (=Handhaben) entwickelte.[1] Im Rahmen des betriebswirtschaftlichen Sprachgebrauchs wird Management allgemein für die ‚Leitung‘ und ‚Führung‘ eines Unternehmens oder einer Organisation gebraucht.[2] Aber für heutige Verhältnisse ist die Anwendung dieser Begriffe nicht mehr geeignet. Mit diesen Bezeichnungen werden unerwünschte Assoziationen, wie Autorität, Bürokratie oder mystische Fähigkeiten hervorgerufen, was immer weniger überzeugt, wenn es um Lösungen komplexer Probleme geht. Zahlenmechanik und rechtliche Bestimmungen dienen längst nicht mehr als einzige Grundlage des Managements. Alle Bereiche des Wissens wie Psychologie, Soziologie, Ethik, Technik, Biologie, etc. werden bei Bedarf herangezogen. Der Term Management wird also zur Vermeidung unerwünschter Assoziationen und als kulturelle Alternative zur Bezeichnung des administrativen Umgangs mit komplexen Gebilden genutzt. Management kann als eine personelle bzw. organisatorische Einrichtung (Institution) und als eine Rollenausübung (Funktion) angesehen werden.[3]

Das **Management als Institution** umfasst den Personenkreis, der in der Organisation leitende Aufgaben übernimmt. Im weiten Sinne vertritt ‚das Management‘ die Interessen des Arbeitgebers gegenüber den Arbeitnehmern. ‚Das Management‘ bildet keine eigene Berufsgruppe und i.Allg. werden die oberen und obersten Führungskräfte zum Management gezählt.

Zum **Management als Funktion** gehören Tätigkeiten wie Führung und Leitung in allen Bereichen der Organisation, Personalwirtschaft, Umgang mit Kunden und anderen

[1] Vgl. Pischon und Liesegang, 1999, S. 96.

[2] Vgl. Springer Fachmedien Wiesbaden GmbH, 2013, S. 229.

[3] Vgl. Remer, 2009, S. 15.

Interessengruppen (s. Kap. 5.3), Beschaffung, Absatz, Verwaltung, Finanzierung etc. Oft wird zwischen Planung, Durchführung, und Kontrolle unterschieden. Zur Planung gehören Problem- und Aufgabendefinition, Zielsetzung, Risiken- und Chancenbetrachtung und das Festlegen von Entscheidungen. Zur Durchführung zählen die Organisation, Kommunikation, Information, Motivation und Koordination der Mitarbeiter und Prozesse in der Organisation. Kontrolle umfasst Soll-/Ist-Vergleiche und Rückmeldung für weitere Planung, Steuerung und Verbesserung.[4]

Unter dem Begriff **Managementsystem** versteht man das Organisieren von Prozessen, Ressourcen, Produkten/Dienstleistungen und von Verantwortlichkeiten nach einer bestimmten Struktur, um die Ziele eines Unternehmens zu erreichen.[5] Darunter zählen Systeme zur Gestaltung Lenkung und Entwicklung von Unternehmen und anderen Organisationen. Beispiele sind bekannte Vertreter, wie das Qualitätsmanagementsystem (QMS), Arbeitssicherheitsmanagementsystem (AMS), Umweltmanagementsystem (UMS) und das Energiemanagementsystem (EMS), als auch solche, welche zur allg. betriebswirtschaftlichen Praxis zuzuordnen sind, wie Personal- und Wertmanagementsysteme.

Das Ziel eines Managementsystems ist es, dass vorrausschauende Verhalten einer Organisation so zu beeinflussen, dass es lebens- und entwicklungsfähig ist und zukünftig bleibt. Managementsysteme sollen die Findung und Realisierung von Zielen wirksam unterstützen.[6]

2.2 High-Level-Structure, Deming-Zyklus und kontinuierlicher Verbesserungsprozess

Mit der großen Revision der Norm für Qualitätsmanagementsysteme im Jahr 2015 wurde eine neue Struktur für die Qualitätsmanagementsystemnorm eingeführt. Die EN ISO 9001:2015 wurde erstmals nach der High Level Structure (HLS) aufgebaut. Die HLS

[4] Vgl. Springer Fachmedien Wiesbaden GmbH, 2013, S. 229–230.

[5] Vgl. Brauweiler, 2019b.

[6] Vgl. Schwaninger, 1994, S. 15–16.

wurde 2012 eingeführt[7] und in Zukunft sollen weitere Normen nach dieser Struktur aufgebaut werden. Bei der HLS handelt es sich um eine spezifische Gliederung der Normabschnitte zur Einführung, Aufrechterhaltung und Verbesserung von Managementsystemen. Des Weiteren sind einheitliche Artikelnummern, einheitliche Bezeichnungen von Überschriften und Fachbegriffen, sowie eine identische Wortwahl für gleiche Anforderungen inbegriffen.[8] Die HLS besteht aus 10 Kapiteln, wie in Abb. 1 zu sehen ist. Von Kapitel 1 bis 3 erstreckt sich der einleitende Teil und von Kapitel 4 bis 10 werden die inhaltlichen Anforderungen an das Managementsystem unter Berücksichtigung des Deming-Zyklus beschrieben.[9]

Abb. 1: High Level Structure (HLS)[10]

Der Deming-Zyklus wurde nach dem US-amerikanischen Qualitätsmanager William Edwards Deming bezeichnet. Er ist auch unter den Namen Plan-Do-Check-Act-Zyklus bekannt. Dieser Zyklus ist ein Werkzeug, welcher aus den vier Phasen Planen, Ausführen, Überprüfen, Anpassen besteht und einen Verbesserungsprozess beschreibt. Die Planphase besteht aus der Problembeschreibung und dem Erheben des Ist-Zustands. Es wird ein Ziel-Zustand formuliert und Maßnahmen sowie Messgrößen zum Erreichen des

[7] Vgl. Brauweiler et al., 2018b, S. 2.

[8] Vgl. Harmeier, 2016

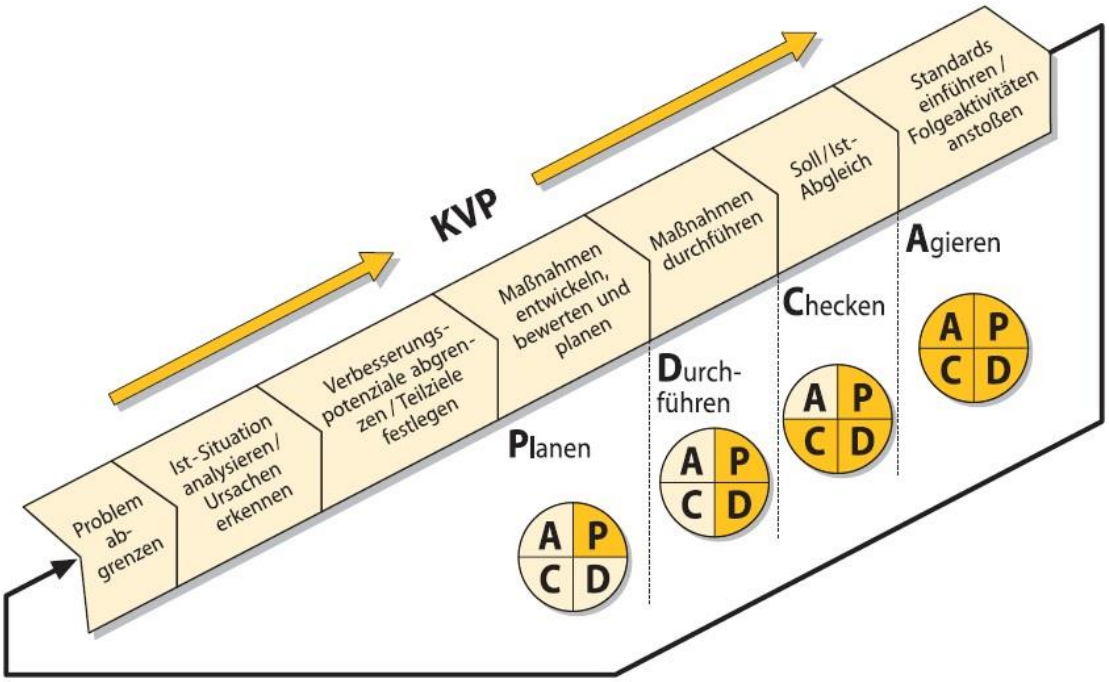
[9] Vgl. Brauweiler et al., 2018b, S. 1.

[10] Brauweiler, 2019a, S. 4.

Ziel-Zustands definiert. In der Phase des Ausführens werden die zuvor festgelegten Maßnahmen unter Einhaltung des Ressourcenplans umgesetzt. Gleichzeitig werden die durchgeführten Maßnahmen dokumentiert. In der nächsten Phase werden die gesammelten Ergebnisse im Hinblick auf die Zielsetzung überprüft. Sollten Abweichungen auftreten, werden die Maßnahmen nochmals angepasst und nachjustiert. In der Letzten Phase werden die Erfahrungen, welche im Prozess der Problemlösung gesammelt wurden, reflektiert und es können Standards für künftige Vorgehen abgeleitet werden.[11]

Der Deming-Zyklus wird genutzt, um dem Streben nach nie endender kontinuierlicher Verbesserung nachzugehen (s. Abb. 2).[12]

Abb. 2: Kontinuierlicher Verbesserungsprozess (KVP)[13]



[11] Vgl. Kudernatsch, 2018, S. 38–39.

[12] Vgl. Kamiske, 2015, S. 39.

[13] Kostka und Kostka, 2017, S. 9.

Kontinuierlicher Verbesserungsprozess (KVP) ist ein Begriff, welcher sich Ende der 1980er-Jahre etabliert hat.[14] Ursprünglich geht dieser Begriff auf das japanische Wort Kaizen „kai“ (=Veränderung) und „zen“ (=zum Besseren oder zur Meisterschaft) zurück. Kaizen ist eine aus Japan stammende Verhaltensphilosophie, welche davon ausgeht, dass alle Handlungen von Menschen, ständig weiterentwickelt werden können und dass das Erschaffene dem Verfall preisgegeben ist, wenn es nicht ständig verbessert bzw. erneuert wird. [15] Seit über 60 Jahren ist Kaizen das Leitmotiv des japanischen Automobilunternehmens Toyota. Viele Unternehmen, die dieses Prinzip konsequent und geduldig verfolgt haben, waren damit erfolgreich. Der KVP erfordert Zeit, Nachhaltigkeit sowie Transparenz und ist nicht für kurzfristige Erfolge ausgelegt. Mit dem KVP können in allen Unternehmensbereichen kontinuierliche Verbesserungen erreicht werden. Dazu gehört die Reduktion von Verschwendungen, das Optimieren von Prozessen, Kostensenkungen, Qualitätssteigerung, etc.[16]

2.3 Integrierte Managementsysteme

2.3.1 Ein Managementsystem

Wie im Kap. 2.2 beschrieben, versteht man unter ein Managementsystem, das Organisieren von Prozessen, Ressourcen, Produkten/Dienstleistungen und von Verantwortlichkeiten nach einer bestimmten Struktur um die Ziele eines Unternehmens zu erreichen. Der Begriff Integration, leitet sich vom lateinischen „integratio“ (=die Erneuerung) ab, wird jedoch zumeist im Sinne von „Wiederherstellung eines Ganzen“ oder Eingliederung in ein größeres Ganzes“ verwendet. [17] „Integrierte Managementsysteme“ sind Managementsysteme, welche mehrere Managementstandards gleichzeitig anwenden.[18] Die einzelnen Standards sind also in ein größeres Ganzes eingegliedert.

[14] Vgl. Kamiske, 2015, S. 131.

[15] Vgl. Kostka und Kostka, 2017, S. 6.

[16] Vgl. Kamiske, 2015, S. 131.

[17] Vgl. Pertsch, 2001, S. 628.

[18] Vgl. Koubek und Pölz, 2014, S. 76.

Von integrierten Managementsystemen wird oft im Rahmen der „zertifizierten Managementsysteme“ gesprochen. Dort wird jedem Bereich wie Qualität, Arbeitssicherheit oder Informationssicherheit ein eigenes Regelwerk zugeordnet. I. Allg. werden diese Standards getrennt betrachtet, um klare Abgrenzungen bei der Überprüfung der Erfüllung der Anforderungen zu schaffen. Dies führt dazu, dass diese Bereiche in Organisationen fälschlicherweise oft als eigenständige Managementsysteme angesehen werden. Diese Abgrenzung der einzelnen Standards ist jedoch primär für eine Überprüfung oder Zertifizierung erforderlich [19] Von außen betrachtet hat jedes Unternehmen ein einziges Managementsystem in dem alle Bereiche, wie z.B. Qualität, Arbeitssicherheit oder Informationssicherheit abgebildet sind. Das Qualitätsmanagementsystem oder Arbeitssicherheitsmanagementsystem sind keine einzelnen, abgegrenzten und eigenständigen Systeme, sondern sie sind Teil des gesamten Managementsystems eines Unternehmens.[20]

2.3.2 Ziele der Integration von Managementsystemen

Die Integration unterschiedlicher Managementstandards erfolgt aus der Idee heraus, dass bestimmte Unternehmensziele mit einem integrierten Managementsystem besser erreicht werden können als mit unabhängig voneinander aufgebauten Managementsystemen.

Integrationsziele werden in Basisziele, Effizienzziele, Sicherungsziele und Innovationsziele eingeteilt (s. Abb. 3). Zu den Basiszielen gehören die ursprünglichen Ziele der einzelnen Managementstandards. [21] Beispiele für ein Informationssicherheitsmanagementsystem, sind der adäquate Schutz von Informationen vor Missbrauch, Offenlegung, Verlust und Manipulation in allen Geschäftsprozessen und die Optimierung der IT-Landschaft und der Infrastruktur.[22] Typische Basisziele für das Qualitätsmanagement sind beständige Produkte und Dienstleistungen zu liefern, welche gesetzliche, behördliche und Kundenanforderungen erfüllen und die

[19] Vgl. Koubek und Pölz, 2014, S. 74–75.

[20] Vgl. Koubek und Pölz, 2014, S. 52–53.

[21] Vgl. Pischon und Liesegang, 1999, S. 294.

[22] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, S. 5, 37.

Kundenzufriedenheit zu steigern.[23]Für Arbeitssicherheit und Gesundheitsschutz sind die Ermittlung von Risiken und Chancen in Bezug auf Gefährdungen der Mitarbeiter am Arbeitsplatz, das Ausführen gefährlicher Tätigkeiten oder der Umgang mit Gefahrstoffen Basisziele.[24]

Unter Effizienzziele werden die Nutzung von Synergie- und Einsparpotentialen bei Aufbau, Pflege, Dokumentation, Betrieb und Zertifizierung eines integrierten Managementsystems zusammengefasst. Mit diesen Zielen soll die Leistung der einzelnen Teilsysteme auf möglichst kostensparende Weise erreicht werden. Beispiele sind Kostenreduzierung durch Redundanzreaktion, die Anwendung einer einheitlichen Sprache und die Minimierung des Auditierungsaufwands.

Sicherungsziele dienen der Wahrung der Rechtskonformität (legal compliance) und der Minimierung von Haftungsrisiken. Mit ihnen sollen die Beziehungen zwischen Banken, Behörden, Versicherungen und der Öffentlichkeit verbessert werden. Besonders für Unternehmen mit besonderen Risikopotentialen wie z.B. gefährliche Tätigkeiten, Anlagen oder Chemikalien sind Sicherungsziele von großem Interesse. Sicherungssziele sind Einhaltung der Rechtskonformität, „Gerichtsfeste“ Organisation und das Abwenden potentieller Imageschäden.

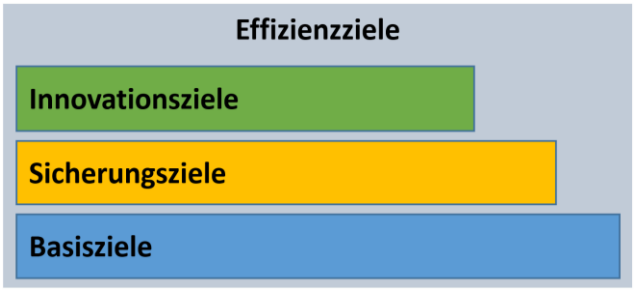
Innovationsziele schließen die Verbesserung der gesamten Systemleistung sowie das Aufbauen einer Wissensbasis zur Entscheidungsunterstützung mit ein. Dazu gehören das Optimieren von Managementinstrumenten und Methoden, Organisationsprozesse, Technologien, Produkte und Dienstleistungen. Auch die Anpassungsfähigkeit des Unternehmens an sich ändernde Umfeldbedingungen muss beachtet werden. Ein flexibles anpassungsfähiges Unternehmen hat gegenüber einem unflexiblen Unternehmen höhere Erfolgschancen.[25]

[23] Vgl. DIN EN ISO 9001:2015, S. 8.

[24] Vgl. Brauweiler et al., 2018a, S. 36.

[25] Vgl. Pischon und Liesegang, 1999, S. 294–296.

Abb. 3: Ziele von integrierten Managementsystemen[26]



2.3.3 Integrationskonzepte

Um ein integriertes Managementsystem zu erhalten, werden in der Praxis zumeist die bereits bestehenden Teilsysteme verbunden. Wenn erforderlich werden dann weitere Extras ergänzt. Es gibt drei Integrationskonzepte, womit dieser Weg realisiert werden kann. Die partielle Integration, die systemübergreifende Integration und die prozessorientierte Integration. Zusätzlich gibt es noch die Addition, welche als Ansatz zur vorläufigen Integration angesehen wird. [27] Dieser Ansatz und die drei Integrationskonzepte werden nachfolgend näher erläutert.

Addition

Ein Ansatz zur vorläufigen Integration ist die Addition. Bei der Addition handelt es sich um ein Zusammenfügen der Dokumentation der zu integrierenden Themengebiete. Eine inhaltliche Abstimmung erfolgt jedoch nicht. Hierbei findet keine Abstimmung der Aufbau- bzw. Ablauforganisation statt, und Konflikte und Wiedersprüche werden größten Teils nicht erkannt oder nicht beachtet. Mit der Addition bleiben die Teilsysteme einzeln bestehen, was nicht mit der inhaltlichen Integration von Managementsystemen gleichgesetzt werden kann. Außer einer übersichtlicheren Dokumentation und erste Konfliktlösungsansätze lassen sich durch die Addition kaum weitere Verbesserungen erkennen. In der Praxis hat die Methode der Addition jedoch häufig die positive Wirkung der Sensibilisierung, wodurch i.d.R. weitere Implementierungsaktivitäten angestoßen

[26] Eigene Darstellung

[27] Vgl. Pischon und Liesegang, 1999, S. 302.

werden. Ein Beispiel ist die Zusammenfassung der Handbücher der zu integrierenden Themengebiete in einer Dokumentation, ohne weiterer inhaltlicher Abstimmung. [28]

Partielle Integration

Zur formalen Abstimmung der Anforderungen verschiedener Normen bzw. Verordnungen dient die Methode der partiellen Integration. Bei dieser Methode werden nicht alle Normelemente eines Anwendungsbereiches bedingungslos zusammengefasst. Aufgrund der Komplexität eines Unternehmens und des Managementsystems (s. Kap. 3), kann so fallweise entschieden werden welche Elemente zusammengefügt werden und welche lieber separat behandelt werden sollen. Ein Beispiel ist die Zusammenfassung der Handbücher der zu integrierenden Themengebiete in einer Dokumentation, mit inhaltlicher Abstimmung. [29]

Systemübergreifende Integration

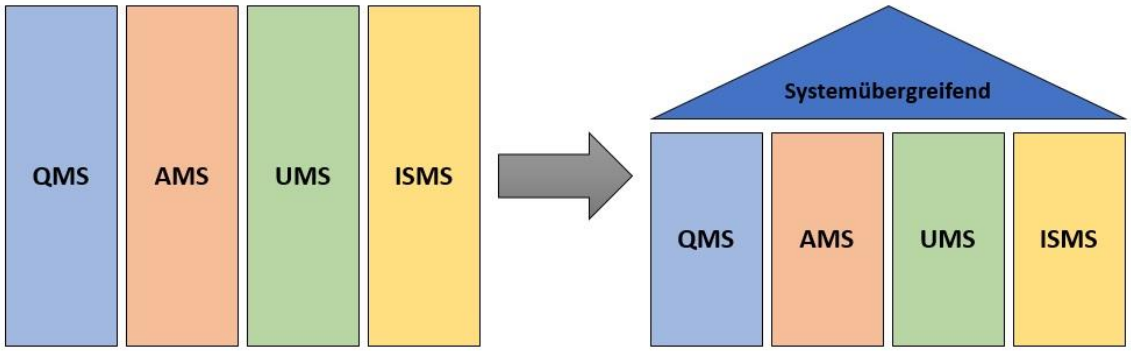
Bezüglich der High Level Structure kann eine bestimmte Grundstruktur der Management-Modelle erkannt werden. Jedes Managementsystem hat bestimmte Elemente, die sich zu Managementfunktionen, zum Produktionsprozess oder in übergeordnete Querschnittsfunktionen zuordnen lassen. Bei der systemübergreifenden Integration sollen die Elemente, welche zu den Managementfunktionen und den übergeordneten Querschnittsfunktionen gehören, von den Elementen der prozess- oder ablauforientierten Funktionen getrennt werden. Bei der Durchführung einer systemübergreifenden Integration werden die relevanten Managementstandards zunächst gegenübergestellt umso die systemübergreifenden Elemente des geplanten IMS identifizieren zu können. Als nächstes können die ermittelten Elemente zusammengefasst werden. Die anderen fachspezifischen sowie prozess- und ablauforientierten Elemente der einzelnen Managementstandards werden in einzelnen untergeordneten Modulen angeordnet. Bildlich formen sie das Grundgerüst und die systemübergreifenden Elemente das Dach

[28] Vgl. Pischon und Liesegang, 1999, S. 305.

[29] Vgl. Pischon und Liesegang, 1999, S. 311.

(s. Abb. 4). Die systemübergreifenden Elemente werden auch als das „Management der Managementsysteme“ bezeichnet.[30]

Abb. 4: Systemübergreifende Integration[31]



Pischon beschrieb bereits 1999 sieben systemübergreifende Aspekte für Managementsysteme. Diese Themen spiegeln sich größtenteils in der HLS, welche 2012 eingeführt wurde, wider. Nachfolgend werden diese Aspekte mit Vermerk auf den entsprechenden Kapiteln der HLS aufgezählt.[32] Der letzte Punkt wurde zu den von Pischon beschriebenen Aspekten, durch den Autor der Masterarbeit ergänzt, da er auch systemübergreifend ist und nicht vergessen werden darf.

1. **Die Zielsetzung, Politik und Vision des Unternehmens**
   Die Ziele spiegeln sich in der Politik, Vision und der festgelegten Programme wider. Außerdem wird festgelegt, wer Ziele formuliert, freigibt und fortschreibt. (entspr. HLS. Kap. 5.2 Politik und 6.2 Ziele und Planung zu deren Erreichung)
2. **Die Beschreibung des integrierten Managementsystems**
   Hierzu zählt die Definition der internen und externen Systemgrenzen sowie das Festlegen von Verantwortungen, Befugnisse und Delegationen. (entspr. HLS Kap. 4 Kontext der Organisation und 5.3 Rollen, Verantwortlichkeiten und Befugnisse in der Organisation)
3. **Das Erstellen und der Umgang mit dokumentierten Informationen**

[30] Vgl. Pischon und Liesegang, 1999, S. 320.

[31] Angelehnt an Pischon und Liesegang, 1999, S. 320.

[32] Vgl. Pischon und Liesegang, 1999, S. 321–322.

Hierzu gehören bestimmte Muster nachdem Dokumente erstellt werden, welche Inhalte enthalten sein müssen und welche nicht, auch die Lenkung von internen und externen dokumentierten Informationen sowie Aufbewahrungsort und -dauer. (entspr. HLS. Kap. 7.5 Dokumentierte Informationen)

4. **Die Bewertung und Kontrolle des integrierten Managementsystems**
   Das Bewertungs- und Kontrollsystem ist dreistufig aufgebaut. Es besteht aus der Überprüfung der Wirksamkeit des IMS durch die oberste Leitung (Managementbericht oder auch Management-Review). Regelmäßiger Planung, Durchführung, Auswertung und Dokumentation von Audits und den Überprüfungen der Beauftragten des Unternehmens. (entspr. HLS. Kap. 9 Bewertung der Leistung)
5. **Das Vorantreiben der kontinuierlichen Verbesserung**
   Hierunter wird eine Bündelung von Zielen und Maßnahmen verstanden, wie Effizienzsteigerung, Vorbeugemaßnahmen, Motivation, Schulungen etc. (entspr. HLS. Kap. 10 Verbesserung)
6. **Bindende Verpflichtungen**
   Bindende Verpflichtungen werden unterteilt in rechtliche Verpflichtungen z.B. Arbeitsschutzgesetz (ArbSchG) oder Kreislaufwirtschaftsgesetz (KrWG) und andere nicht-hoheitliche und nicht-rechtliche Anforderungen z.B. freiwillige Selbstverpflichtungen, Branchenstandards oder DIN-Normen.[33]
7. **Weitere Aspekte**
   Asset-, Risiko-, und Versicherungsmanagement, statistische Methoden und Öffentlichkeitsarbeit sind hier beispielsweise zu nennen.[34]
8. **Kommunikation**
   Managementsysteme hängen besonders von der Kommunikation der Menschen miteinander ab.[35] (entspr. HLS. Kap. 7.4 Kommunikation)

Diese acht Aspekte in Kombination mit der HLS bieten sich hervorragend dazu an, die Managementsystemnormen gegenüberzustellen und zu vergleichen. Aus dieser

[33] Vgl. Brauweiler et al., 2018b, S. 15.

[34] Vgl. Pischon und Liesegang, 1999, S. 321–322.

[35] Vgl. Koubek und Pölz, 2014, S. 26.

Gegenüberstellung (s. Anhang_01_Entsprechungsmatrix) der Managementsysteme QMS, EMS, und ISMS wird nochmal deutlich, welche Punkte systemübergreifend sind und welche zu prozess- und ablauforientierten Funktionen zu zählen sind.

Prozessorientierte Integration

Eine weitere Möglichkeit zur Integration verschiedener Managementstandards bieten die Prozesse, welche im Unternehmen anzutreffen sind.[36] Laut der DIN EN ISO 14001:2015 ist ein Prozess ein „Satz zusammenhängender und sich gegenseitig beeinflussender Tätigkeiten, der Eingaben in Ergebnisse umwandelt“.[37] Ein Prozess hat also ein Ziel und ein Ergebnis. Jeder Prozess besteht dabei aus Eingabe (z.B. Material, Informationen), Verarbeitung (z.B. Tätigkeiten, Verfahren, Einzelschritte) und Ausgabe (z.B. Produkte, Dienstleistungen, Informationen).[38] Um einen Ansatz zur Integration zu schaffen, bietet es sich an eine Prozessstruktur aufzubauen. Im ersten Schritt werden übergeordnete Prozessarten definiert. Diese können Management-, Ressourcen-, Leistungserstellungs-, kunden- und unterstützende Prozesse sein. Darauf aufbauend, kann eine zweite Ebene festgelegt werden, wo einzelne Unternehmensprozesse oder Prozessschritte konkretisiert und benannt werden.[39]

Alle Prozesse orientieren sich an den Bedürfnissen von Kunden. Dabei gibt es interne Kunden, wie z.B. ein darauffolgender Prozess und externe Kunden, wie z.B. ein externer Käufer eines Produkts oder einer Dienstleistung. Zum Durchführen der Integration auf Prozessebene, können diese vier Schritte durchlaufen werden:[40]

1. Eine Analyse des Prozesses in Bezug auf die zu implementierenden Managementstandards.
2. Eine Revision der Prozessbeschreibung. Diejenigen Aktivitäten, welche zu den zu implementierenden Managementstandards gehören, werden ergänzt.

[36] Vgl. Pischon und Liesegang, 1999, S. 323.

[37] Zit. DIN EN ISO 14001:2015, S. 20.

[38] Vgl. Kamiske, 2015, S. 137.

[39] Vgl. Pischon und Liesegang, 1999, S. 324.

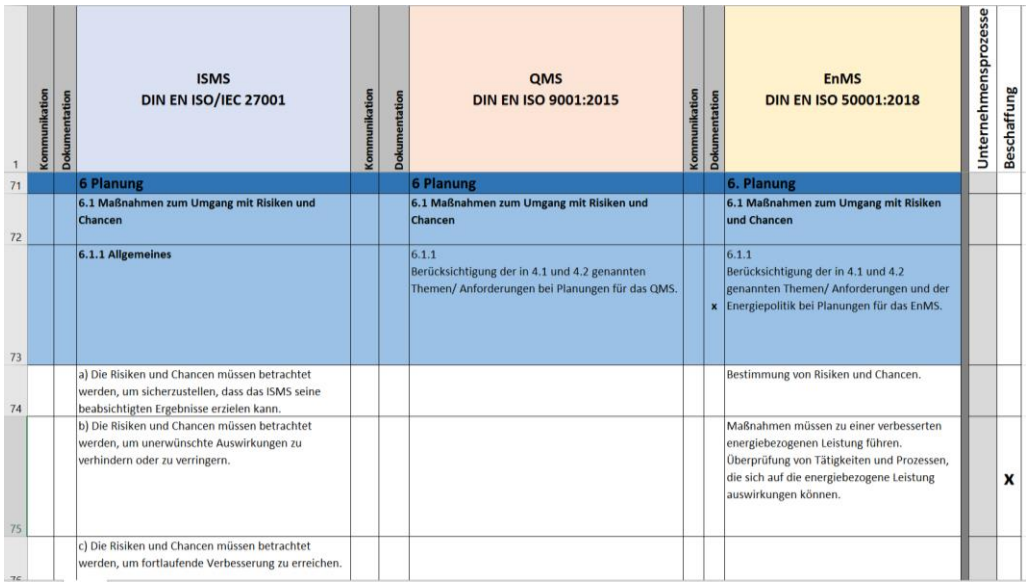
[40] Vgl. Pischon und Liesegang, 1999, S. 325.

3. Kontrolle jeder einzelnen Anforderung der zugrundeliegenden Vorgaben z.B. Normen, Verordnungen, Leitfäden, Organisationsanweisungen etc. im Hinblick auf die Erfüllung des Prozesses.
4. Das Erstellen von Prüfmatrizen für die einzelnen zu integrierenden Managementstandards, um zu dokumentieren in welchem Prozess, welcher Standard implementiert ist.

In der Literatur, wird geraten für jeden Bereich eine eigene Prüfmatrix zu nutzen. Um jedoch den Charakter der Integration aufrecht zu halten bietet es sich an, eine einzige Prüfmatrix über alle Anforderungen und Standards zu erstellen. Um dies zu realisieren, wird die Entsprechungsmatrix, welche bereits beim Konzept der Systemübergreifenden Integration eine Rolle gespielt hat, um den zu implementierenden oder zu verändernden Prozess erweitert. Im nächsten Schritt wird ermittelt, in welchen Punkten der Prozess involviert ist. Das Ergebnis ist eine integrierte Prüfmatrix. Weil die neuen Anforderungen teilweise prozessorientiert sind, wird ein Beispiel gezeigt, wie solche Anforderungen integriert werden können. Abb. 5 zeigt das Beispiel am Prozess der Beschaffung. Hier wird der Zusammenhang des Beschaffungsprozesses mit dem Kap. 6 Planung der HLC deutlich. Im Beschaffungsprozess wird geprüft, ob Informationssicherheitsrisiken bestehen (ISMS), bestimmte Kundenanforderungen erfüllt sind (QMS) und ob energierelevante Aspekte existieren (EMS). Die Vorlage der integrierten Prüfmatrix ist im Anhang (s. Anhang_02_Integrierte_Prüfmatrix) zu finden.

Neben der Integration von Prozessen, können zwei weitere Möglichkeiten genutzt werden, um die Prüfmatrix anzuwenden. Zum einen ist es möglich bereits bestehende Prozesse auf ihren Integrationsgrad zu untersuchen, indem die Zusammenhänge eines Prozesses mit den Normen ermittelt wird. Und zum anderen kann die Wirksamkeit nach der Integration neuer Anforderungen in einem Prozess bewertet werden. Diese Möglichkeiten zur Nutzung der integrierten Prüfmatrix, müssen jedoch erst überprüft werden und sind nicht Thema dieser Arbeit.

Abb. 5: Auszug integrierte Prüfmatrix mit Beispiel[41]



1	Kommunikation	Dokumentation	ISMS DIN EN ISO/IEC 27001	Kommunikation	Dokumentation	QMS DIN EN ISO 9001:2015	Kommunikation	Dokumentation	EnMS DIN EN ISO 50001:2018	Unternehmensprozesse	Beschaffung
71			**6 Planung**			**6 Planung**			**6. Planung**		
72			**6.1 Maßnahmen zum Umgang mit Risiken und Chancen**			**6.1 Maßnahmen zum Umgang mit Risiken und Chancen**			**6.1 Maßnahmen zum Umgang mit Risiken und Chancen**		
73			**6.1.1 Allgemeines**			6.1.1 Berücksichtigung der in 4.1 und 4.2 genannten Themen/ Anforderungen bei Planungen für das QMS.		x	6.1.1 Berücksichtigung der in 4.1 und 4.2 genannten Themen/ Anforderungen und der Energiepolitik bei Planungen für das EnMS.		
74			a) Die Risiken und Chancen müssen betrachtet werden, um sicherzustellen, dass das ISMS seine beabsichtigten Ergebnisse erzielen kann.						Bestimmung von Risiken und Chancen.		
75			b) Die Risiken und Chancen müssen betrachtet werden, um unerwünschte Auswirkungen zu verhindern oder zu verringern.						Maßnahmen müssen zu einer verbesserten energiebezogenen Leistung führen. Überprüfung von Tätigkeiten und Prozessen, die sich auf die energiebezogene Leistung auswirkungen können.		x
			c) Die Risiken und Chancen müssen betrachtet werden, um fortlaufende Verbesserung zu erreichen.								

Nach der Durchführung einer prozessorientierten Integration, liegt die Verantwortung zur Umsetzung der Aktivitäten bei den jeweiligen Prozesseigentümern („Prozess Owner“). Demnach liegen die Aufgaben der Managementbeauftragten in der Beratung und Unterstützung der Prozessgruppen und ggf. der Kontrolle und Bewertung der Prozesse. Ein Vorteil dieser Methode ist die schnelle Sensibilisierung der Mitarbeiter, weil die Managementstandards, wie z.B. Qualität, Energie und Informationssicherheit in die alltäglichen Entscheidungsprozesse mit eingebunden sind.[42]

2.3.4 Mögliche Kritik an integrierten Managementsystemen

Nachdem die Ziele und Vorteile von integrierten Managementsystemen erläutert sind, werden nun mögliche Kritikpunkte aufgezählt. Die Ablehnung gegenüber integrierten Managementsystemen basiert häufig auf subjektiver Basis. Aufgrund von Abteilungsdenken und der Konkurrenz zwischen Fachbereichen, werden mit der Integration mögliche individuelle Machteinbußen gefürchtet. Als Ergebnis der Integration wird mit diversen Kürzungen gerechnet. Gleichzeitig steigt die Angst, den eigenen Arbeitsplatz infolge dieser Kürzungen verlieren zu können. Beide Fälle können

[41] Angelehnt an Pischon und Liesegang, 1999, S. 326.

[42] Vgl. Pischon und Liesegang, 1999, S. 325–326.

theoretisch eintreten, jedoch sind sie in der Praxis nicht zu beobachten. Ein weiterer möglicher Kritikpunkt ist, dass die Integration zu einem unüberschaubaren, inflexiblen, bürokratischen und komplexen System führt. Die Gefahr einer Erhöhung der Komplexität besteht grundsätzlich. Auch bei der internen und externen Auditierung integrierter Managementsysteme scheint im ersten Moment die Komplexität zu steigen, da der Auditierungsaufwand erhöht wird und die Auditoren speziell ausgebildet sein müssen.[43] Aus diesen Gründen geht es im nächsten Kapitel um die Komplexität. Dazu werden wichtige Begriffe festgelegt, die Treiber von Komplexität aufgezählt und Methoden aufgezeigt Komplexität in integrierten Managementsystemen zu verringern.

[43] Vgl. Pischon und Liesegang, 1999, S. 327–329.

3 Komplexität von (integrierten) Managementsystemen

Die Komplexität einer Organisation und dessen (integrierten) Managementsystem, hängt von vielen Faktoren ab. Zum einen gibt es eine äußere, lebendige Welt der Organisation wozu z.B. die Wirtschaftswelt, wie Geschäftspartner, Konkurrenz, Kunden oder auch das Umfeld, wie die Umwelt oder Nachbarn eine Rolle spielen. Zum anderen ist die Organisation an sich ein komplexes System. Interne Strukturen und Prozesse, welche durch das Management vorgegeben sind, werden immer komplizierter. Gleichzeitig ist eine Organisation und ihr (integriertes) Managementsystem, ein soziales System. Die Eigenschaften sozialer Systeme hängen davon ab, wie die Menschen verbunden sind und zusammen agieren. Die Kommunikation zwischen den Menschen ist entscheidend. Faktoren wie, Grundwerte, Ethik, Unternehmenskultur, toleriertes und erwünschtes Verhalten sind maßgebend, was zur Erhöhung der Komplexität beiträgt. Systeme sind nicht nur Ansammlungen von Personen oder Dingen. Systeme schließen viele Elemente ein, die zusammenhängen und sich gegenseitig beeinflussen, um ein oder mehrere Ziele zu erreichen. Anders ausgedrückt, jede Organisation zeigt ihr eigenes Verhalten gegenüber verschiedenen Einflüssen und reagiert unterschiedlich auf Veränderungen.[44]

3.1 Begriffe

Zum besseren Verständnis werden im Folgendem die Begriffe einfach, kompliziert und komplex unterschieden.

Tab. 1: Begriffserklärung einfach, kompliziert und komplex[45]

einfach
Einfache Sachverhalte benötigen kein Expertenwissen zur Erfassung und lösen wenig Kontroversen aus.

[44] Vgl. Koubek und Pölz, 2014, S. 25–26.

[45] Vgl. Koubek und Pölz, 2014, S. 243.

Beispiel: Das Backen von Brot ist einfach. Mit einem Rezept und den nötigen Zutaten und Hilfsmitteln kann nicht viel schiefgehen. Es bestehen auch keine unterschiedlichen Lehrmeinungen oder Kontroversen zum Thema Backen.

kompliziert

Komplizierte Sachverhalte sind nur mit Expertenwissen zu erfassen und besitzen eine Vielzahl von Variablen, wobei jedoch bei der richtigen Zusammensetzung der Variablen vorhersagbare Ergebnisse entstehen. Ist der Weg zur Lösung eines komplizierten Problems bekannt, kann dieser wiederholt werden und liefert dasselbe Ergebnis.

Beispiel: Der Bau einer Rakete ist kompliziert. Es wird Expertenwissen, eine detaillierte Anleitung und neueste Technik benötigt, um erfolgreich eine Rakete zu bauen.

komplex

Komplexe Sachverhalte bestehen aus bekannten und unbekannten Variablen, deren Kombination und Auswirkung nicht oder nur in geringem Maße vorhersagbar ist.

Zur Lösung komplexer Probleme gibt es keinen einzig wahren Weg. Weil komplexe Sachverhalte auch durch Intransparenz und Dynamik gekennzeichnet sind.[46]

Beispiel: Zu komplexen Sachverhalten kommt es, wenn Menschen interagieren. Kindererziehung ist z.B. ein komplexes Thema. Es gibt kein eins zu eins Rezept Kinder am besten zu erziehen. Es gibt so viele Situationen und Faktoren, die eine Rolle spielen, so dass eine Checkliste oder Wenn-Dann-Anleitung nicht ausreichend ist.

[46] Vgl. Dörner, 2002

3.2 Ziele des (integrierten) Managements in Bezug auf Komplexität

Ziel eines (integrierten) Managementsystems ist es die Komplexität durch bestmöglich entwickelte und zueinander optimierte Prozesse, Tätigkeiten und Werkzeuge zu verringern, um den Menschen in der Organisation zu ermöglichen, die enorme Menge von Anforderungen erfüllen zu können. Das Modell muss anpassungsfähig, veränderbar und schlank sein. Beim Aufbauen und Integrieren von Managementsystemen können vermeintlich notwendige oder nützliche Zusätze die Flexibilität und Schlankheit gefährden und gleichzeitig dazu führen, dass die Leistungsfähigkeit und Reaktionsfähigkeit der Organisation darunter leidet.[47] Letztendlich gilt der Grundsatz, dass das Managementsystem der Organisation dienen muss und nicht die Organisation dem Managementsystem.[48]

3.3 Treiber von Komplexität in (integrierten) Managementsystemen[49]

Nachfolgend werden verschiedene Punkte aufgeführt, die dazu beitragen können, die Komplexität von Managementsystemen zu erhöhen.

1. **Die Berücksichtigung interessierter Parteien**

Wenn die Menge von interessierten Parteien steigt oder diese neu betrachtet werden müssen, steigen auch die Anforderungen an das Management und demzufolge an die Organisation. So werden beim Einführen spezieller Anforderungen oder Managementsysteme zusätzliche Analysen, Aktivitäten und Dokumentationen erforderlich, die zur Erhöhung der organisationalen Komplexität beitragen.

2. **Weiterentwicklung von Prozessen**

[47] Vgl. Koubek und Pölz, 2014, S. 252.

[48] Vgl. Kuntsche und Börchers, 2017, S. 447.

[49] Vgl. Koubek und Pölz, 2014, S. 252–256.

Bei der Weiterentwicklung von Prozessen gibt es vier Punkte, die eine Erhöhung der Komplexität bewirken können:

- Zur Überprüfung von Wechselwirkungen und Anforderungen werden Kontroll- und Abstimmungsschleifen eingeführt
- Es besteht die Gefahr, dass sich die Menschen in der Organisation zu sehr auf die Funktion der Prozesse verlassen und negative Veränderungen im Prozessverlauf aufgrund zu hoher Komplexität und mangelnder Aufmerksamkeit nicht oder zu spät wahrgenommen werden.
- Wenn die Festlegungen und Regelungen zu stark ausgeprägt sind, ist ein flexibles Reagieren auf viele, teilweise ungeplante Situationen nicht möglich. So müssen Regeln gebrochen werden, was sich dann aufsummiert und dazu führt, dass das System zu erodieren beginnt.
- In der Organisation werden bereichsspezifische Variationen der Prozesse abgebildet.

3. Compliance

Compliance ist ein schwieriger Themenbereich. Es gibt eine riesige Anzahl verschiedener Gesetze und Regelungen. Diese können sich ändern, aufgehoben werden und es können neue hinzukommen. Meist sind es unumgängliche Anforderungen, die bei der Implementierung zusätzliche Arbeits- und Prüfschritte benötigen. Bei der Umsetzung von Compliance-Anforderungen wird oft keine Diskussion geführt, sondern die erstbeste Variante, welche meist einfach zu implementieren aber auf Dauer nicht die Beste ist, bevorzugt.

4. Risikomanagement

Beim Risikomanagement besteht die Gefahr, Risiken welche eine niedrige Eintrittswahrscheinlichkeit bzw. wenig Einfluss auf die Organisation haben, eine zu hohe Aufmerksamkeit beizumessen. Arbeits- und Prüfschritte für un- oder wenig wahrscheinliche Risiken, die jeden Tag angewendet werden, blähen einen Prozess unnötig auf.

5. Korrekturmaßnahmen

Um einen wichtigen Prozess am Laufen zu halten, sind schnell durchgeführte Korrekturmaßnahmen kurzfristig sinnvoll aber auf Dauer ein potentieller Treiber für Komplexität. Hier gilt auch, dass die schnellste und billigste Lösung nicht immer die beste ist, zumal oft nur die Symptome bekämpft werden und nicht die eigentliche Fehlerquelle. Ein Lösungsweg ist es, die bekannten Qualitätstools anzuwenden und beim Auftreten des Problems ausreichend Zeit für Analyse und Problemlösung zu nehmen.

6. Kundenorientierung

Kundenanforderungen unüberlegt zu übernehmen und zu erfüllen sorgt dafür, dass weitere Prozesse, Kompetenzen und Informationen notwendig sind. Die Organisation sollte eine klare Grenze ziehen wo der Aufwand nicht den Nutzen übersteigt, um so einen weiteren Treiber von Komplexität zu eliminieren.

7. Dokumentierte Informationen

Allein aus Gründen der Compliance ist es wichtig dokumentierte Informationen aufzubewahren. Relevante Arbeitsschritte müssen dokumentiert sein, für relevante Tätigkeiten müssen Arbeitsanweisungen und Checklisten vorliegen und Prozesse müssen schriftlich abgebildet sein. So weiß jede Person, was ihre Aufgabe ist und alle wichtigen Prozesse und Tätigkeiten können, wenn nötig nachvollzogen werden.

8. Kontinuierlicher Verbesserungsprozess

Wenn eine Sache verbessert wird, heißt das nicht automatisch, dass sie vereinfacht wird. Eine Verbesserung eines Prozessschrittes ist auf den ersten Blick positiv. Jedoch sollte beachtet werden, dass aus ganzheitlicher Sicht die Komplexität nicht unbewusst steigt oder sogar bewusst in Kauf genommen wird die Komplexität zu fördern.

Ein einfaches Beispiel ist die Verbesserung eines Antragsdokuments mittels Microsoft Office. Ein kreativer und engagierter Mitarbeiter programmiert ein interaktives Dokument, welches für die spezifische Arbeitsumgebung im ersten Moment eine Verbesserung darstellt. Jedoch ist es nicht selten, dass neue Anforderungen umgesetzt werden müssen. D.h. das Dokument muss auch angepasst werden. Wenn dies nun der

Mitarbeiter aus irgendeinem Grund nicht kann, sei es wegen Krankheit oder Abteilungswechsel oder nicht mehr in der Organisation ist und niemand sonst die Programmiersprache beherrscht und zuzüglich das alte Dokument nicht mehr existiert, dann kann die neue Anforderung nicht oder nur mit großem Aufwand umgesetzt werden. Letztendlich war die Einführung dieses neuen interaktiven Dokuments keine Verbesserung, sondern eher eine „Verschlimmbesserung".

9. Striktes Anwenden des PDCA-Zyklus'

Wenn der PDCA-Zyklus zur systematischen Verbesserung und Weiterentwicklung in übertriebener Form angewendet wird, kann dies zur Erhöhung der Komplexität führen.

Tab. 2: Treiber von Komplexität im PDCA-Zyklus[50]

Phase	Treiber von Komplexität
Planung	Genauigkeit und Umfang bei der Planung von Prozessen und Projekten haben einen entscheidenden Einfluss auf die Komplexität.
Umsetzung	Das rigorose Umsetzen aller geplanten Schritte, selbst wenn sich während des Umsetzens herausstellt, dass Verbesserungen bzw. Anpassungen nötig sind.
Überprüfen	Umfangreiche Datenmengen von Kennzahlen und andere Daten sind „nice to have" aber treiben die Komplexität nur unnötig in die Höhe, wenn kein erkennbarer Nutzen vorliegt.
Handeln	Das Nachverfolgen und Analysieren jeder Kleinigkeit führt zu Unmengen von Maßnahmen, welche den Aufwand erhöhen aber nur minimal Nutzen.

3.4 Simplicity als Lösung

Um die Komplexität zu reduzieren hilft nur eines – „Simplicity". Simplicity bedeutet gezielte Vereinfachung von Prozessen, Strukturen, Strategien, Portfolios und anderen Sachverhalten.[51]

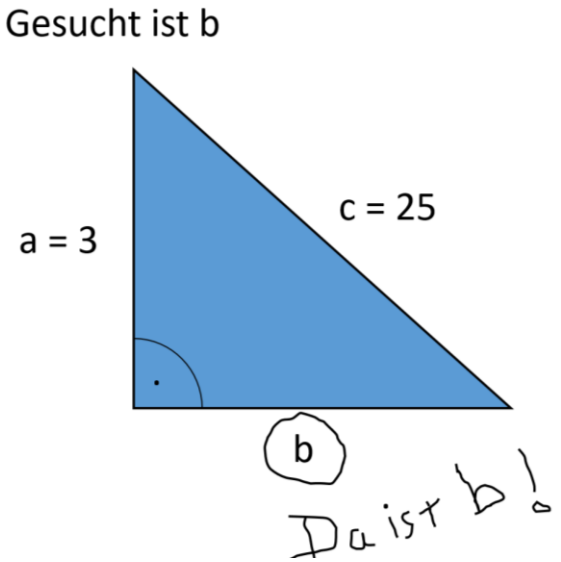
Bei einer Vereinfachung können zwei potentielle Gefahren auftreten. Zum einen kann eine Vereinfachung formal korrekt sein aber wichtige Wechselwirkungen und

[50] Vgl. Koubek und Pölz, 2014, S. 255–256.

[51] Vgl. Koubek und Pölz, 2014, S. 242.

Einflussfaktoren können nicht betrachtet worden sein. Ein Beispiel solch einer Vereinfachung ist die Mathematische Aufgabe in Abb. 6.

Abb. 6: Falsch verstandene Lösung[52]



Die Aufgabe wurde gelöst. Einfach und formal korrekt aber solch eine Lösung war nicht das Ziel. Das Ziel war es einen Wert für b zu erhalten. Und genauso verhält es sich auch bei der Vereinfachung eines Sachverhalts im Unternehmen. Das Ziel ist nicht bloß die reine Vereinfachung. Die Grundziele des Sachverhalts z.B. eines Prozesses müssen bestehen bleiben. D.h. Bei einer Vereinfachung eines Sachverhalts darf dieser nur soweit verändert werden, dass er seine Hauptfunktion erfüllen oder sogar verbessert kann.

Zum anderen besteht die Gefahr Know-how also Wissen und Fortschritt zu verlieren. Ein Beispiel ist ein Unternehmen, welches führend im Herstellen von Tintenstrahldruckern war. Dieses Unternehmen hatte in eigenes Forschungslabor mit 14 Mitarbeitern. Während einer Krise mussten 40% der Mitarbeiter eingespart werden und das Forschungslabor verlor sieben Mitarbeiter. Als Ergebnis fehlten wichtige Kernkompetenzen und ein ganzes Marktsegment ging verloren. Ein wichtiger Wettbewerbsvorteil kam damit unwiderruflich abhanden. Zusammenfassend sollte beim „Vereinfachen“ ein klares Bild des Sachverhalts bestehen. Es bietet sich eine Risiko- und Chancenanalyse an, worin

[52] Angelehnt an Koubek und Pölz, 2014, S. 247.

Wechselwirkungen und Einflussfaktoren herausgearbeitet und betrachtet werden können. Nur so kann am Ende das Ergebnis einer zukunftsorientierten, zuverlässigen und einfachen Lösung erreicht werden.[53]

Es gibt verschiedene Simplicity-Methoden. Diese Ansätze zur Vereinfachung in Bezug auf Managementsysteme sind in Tab. 3 zusammengetragen. Bei der Anwendung dieser Methoden ist immer der Kontext ausschlaggebend. Methoden die falsch oder zum falschen Zeitpunkt angewendet werden, können das Gegenteil nämlich eine Komplexitätssteigerung bewirken.

Tab. 3: Simplicity-Methoden[54]

Methode	**Beschreibung**
Historischer Rückblick	Beim historischen Rückblick; wird jeder Teil eines Prozesses, Produkts, oder Themas im Hinblick auf dessen Entstehung und den damaligen Motiven und Beweggründen untersucht. Es werden wichtige Fragen geklärt, wie z.B.: Warum wurde es so eingeführt? Was für Ziele bzw. Probleme gab es und sind diese heute noch aktuell oder gibt es ganz andere Anforderungen oder Voraussetzungen? Der historische Rückblick dient auch zur Beseitigung von Widerstand. Denn dem Argument „Das haben wir schon immer so gemacht.“, kann so durch fundiertem Aufzeigen warum „Das“ so eingeführt wurde und warum „Das“ nicht mehr zeitgemäß ist, dem Widerstand Schritt für Schritt entgegengetreten werden.
Weglassen	Bei Themen mit wenig Einflussfaktoren und wo die Auswirkungen überschaubar sind, kann auf ein Historical Review verzichtet werden und die Methode des Weglassens angewendet werden.

[53] Vgl. Koubek und Pölz, 2014, S. 246–248.

[54] Vgl. Koubek und Pölz, 2014, S. 260–270.

Methode	Beschreibung
	Beispiele sind Arbeitsanweisungen oder Dokumentationen. Von vertraglichen und gesetzlichen Verpflichtungen abgesehen, kann das, was nicht genutzt oder gebraucht wird weggelassen werden.
Funktionen verstecken	In der täglichen Arbeit werden bestimmte Funktionen, Dokumente, Daten, etc. nicht regelmäßig benötigt. Um trotzdem die Übersichtlichkeit zu gewähren, können wichtige aber nicht ständig genutzte Funktionen versteckt werden. Beispielsweise können in Antragsformularen die wichtigsten Funktionen auf einem Blick vorhanden sein und untergeordnete oder selten genutzte Funktionen erst auf Befehl eingeblendet werden.
Provokatives Amputieren	Beim provokativen Amputieren geht es darum wesentliche Elemente in Frage zu stellen um herauszufinden, was passiert, wenn diese weggelassen werden. Wesentliche Elemente können z.B. Prozesse, Produkte, Dienstleistungen, Abteilungen, etc. sein. Diese werden nicht wirklich weggelassen, sondern sollen potenziell unnötige Teilbereiche identifizieren. Beispielsweise könnte hinterfragt werden, was passiert, wenn keine Audits mehr durchgeführt werden. Solche extremen Fragen können zu unbekannten und innovativen Lösungen führen. Bei dieser Methode sind Vorsicht und ein vertrauensvolles Arbeitsklima wichtig, weil sonst schnell auf Widerstand gestoßen werden kann.
Zeit sparen	Zeit ist eine wertvolle Ressource. Beim Vereinfachen von Prozessen muss darauf geachtet werden, die Durchlaufzeit und die Arbeitsschritte der Mitarbeiter gering zu halten. Anstelle von zeitaufwändigen Kontrollschleifen die, vielleicht sogar mehrmals durchlaufen werden müssen, sollte versucht werden den Prozess so

Methode	Beschreibung
	zu gestalten, dass keine Kontrollschleifen mehr nötig sind oder diese zumindest minimiert. Hier bietet es sich an, eine präzise Ursachenanalyse für mögliche Fehler / Fehlerquellen durchzuführen.
Zuhören/ Zuschauen	Oftmals haben Mitarbeiter, die am Ort des Geschehens arbeiten, die besten Ideen zur Verbesserung eines Prozesses, einer Tätigkeit, etc. Da in Managementsystemen normalerweise regelmäßige Audits stattfinden, ist diese Methode recht gut abgedeckt. Recht gut, weil der Grundgedanke eines Audits auf die Überprüfung von Konformitäten aufbaut und es vom Auditor abhängt, inwiefern die Verbesserung eine Rolle spielt.
Nutzen erhöhen	Wenn eine Anwendung oder ein Gerät sowieso schon existiert, bietet es sich an weitere Funktionen hinzuzufügen, um dessen Nutzen zu erhöhen. Einer Armbanduhr wird heute z.B. zusätzlicher Nutzen hinzugefügt, indem sie als Wecker, Stoppuhr und Timer genutzt werden kann und zusätzlich noch eine integrierte Beleuchtung eingebaut ist. Dasselbe Prinzip kann in Managementsystemen genutzt werden um Prozessen, Geräten, Dokumenten, usw. zusätzlichen Nutzen hinzuzufügen. Gleichzeitig lässt sich so möglicherweise auch Zeit, Platz und Speicherkapazität einsparen. Kontextabhängig kann so durch Hinzufügen die Komplexität verringert werden.
Konzepte übertragen	Funktionierende Konzepte zu übertragen ist eine Methode mit mehreren Vorteilen. Zum einen ist es einfacher ein bereits in der Praxis angewendetes und Vertrautes Konzept zu übernehmen, als eines neu entwickeln zu müssen. Bei einem bereits genutzten Konzept sind i.d.R. Risiken und Chancen bekannt. Zum anderen beherbergen Methoden die durchgängig angewendet werden, eine

Methode	Beschreibung
	höhere Sicherheit bei der Anwendung und Akzeptanz bei den Mitarbeitern, was wiederum zu zuverlässigen Ergebnissen führt. Als Beispiel dient die Vereinheitlichung der ISO-Normen durch die HLS und die Anwendung des PDCA-Zyklus.
Masse und Ausnahme	Beim Entwickeln von Prozessen und Systemen werden Spezialfälle oft mit einbezogen. Aber Spezialfälle sind meist kompliziert zu handhaben. Jede Ausnahme bei der Entwicklung zu betrachten wird auch als „Over-Engineering“ bezeichnet. Um Komplexität und Ressourcen zu sparen, sollte die Masse von der Ausnahme getrennt werden. Diese Methode widerspricht dem Prinzip kombinieren, jedoch ist die Betrachtung des Kontextes wichtig.
Kombinieren und Reorganisieren	Kombinieren und Reorganisieren ist die Kernidee beim Integrieren von Managementsystemen. Prozesse, Abläufe und andere Dinge werden so kombiniert und erneuert oder verändert, bis sie einfacher in der Umsetzung sind und der Konformität entsprechen. Beispiele sind die Erstellung einer integrierten Unternehmenspolitik, das Zusammenfassen von Audits oder das Vereinheitlichen von Dokumentenablagen.
Modularisieren	Beim Modularisieren geht es darum, Dinge in kleinere Einheiten zu zerlegen. Weitläufige Prozesse können bspw. in Teilprozesse zerlegt werden. Vorteile dieser Methode können eine höhere Übersichtlichkeit und damit ein leichteres Arbeiten, schnellere Durchlaufzeiten und eine niedrigere Fehleranfälligkeit sein.
Energie verlagern	Bei Prozessoptimierungen und Restrukturierungen spielt die Energieverlagerung eine zentrale Rolle. Im Zuge der Automatisierung wird die Energie von Menschen auf Maschinen verlagert. Dieses Prinzip kann auch auf Prozessen angewendet

Methode	Beschreibung
	werden. Zu beachten ist, dass beim Anwenden dieser Methode die Arbeit bei dem einen vereinfacht wird, bei einem anderen dafür erschwert.

Im Kapitel 7 Integration der neuen Anforderungen, soll bei der Implementierung darauf geachtet werden, was Treiber von Komplexität sein können und wenn notwendig versucht werden mögliche Simplicity-Methoden anzuwenden, um die Komplexität im integrierten Managementsystem des Fraunhofer FEP zu verringern.

Nachfolgend werden im Kapitel 4 das Fraunhofer FEP, dessen integriertes Managementsystem und die von der Fraunhofer Zentralverwaltung vorgegebenen neuen Anforderungen vorgestellt.

4 Fraunhofer FEP

4.1 Kurzportrait

Die Fraunhofer Gesellschaft wurde nach dem Münchner Gelehrten Joseph von Fraunhofer (1787–1826) benannt, welcher erfolgreicher Forscher, Erfinder und Unternehmer war.[55] Joseph von Fraunhofer war ein bedeutender Wegweiser in den Bereichen der Optik und Feinmechanik.[56]

Die 1949 gegründete Fraunhofer Gesellschaft ist die weltweit führende Institution für anwendungsorientierte Forschung. Der Forschungsschwerpunkt liegt auf zukunftsorientierte Technologien und die Verwertung der Ergebnisse in Wirtschaft und Industrie. Die Fraunhofergesellschaft mit ihrem Hauptsitz in München, betreibt derzeit 74 Institute und Forschungseinrichtungen in ganz Deutschland. Es werden ca. 28 Tausend Mitarbeiter mit vorwiegend natur- oder ingenieurwissenschaftlicher Ausbildung beschäftigt. Das Projektgeschäft ist der Wertschöpfungsprozess des Fraunhofer-Instituts. Das jährliche Forschungsvolumen beträgt 2,8 Milliarden Euro, wovon 2,3 Milliarden Euro auf den Leistungsbereich Vertragsforschung anfallen.[57]

Das Fraunhofer-Institut für organische Elektronik, Elektronenstrahl- und Plasmatechnik FEP entwickelt innovative Technologien, Prozesse und Lösungen im Bereich der Oberflächenveredelung und der organischen Elektronik. Zur Lösung von Problemen in der Oberflächenbehandlung, Vakuumbeschichtung sowie der organischen Halbleiter werden wichtige Kernkompetenzen auf den Feldern der Elektronenstrahltechnologie, Rolle-zu-Rolle-Technologie, der plasmagestützten Großflächen- und Präzisionsbeschichtung, organischen Elektronik sowie der Entwicklung technologischer Schlüsselkomponenten genutzt.[58]

[55] Vgl. Eitner, 2021b

[56] Vgl. Thum, 2013, S. 7.

[57] Vgl. Eitner, 2021b

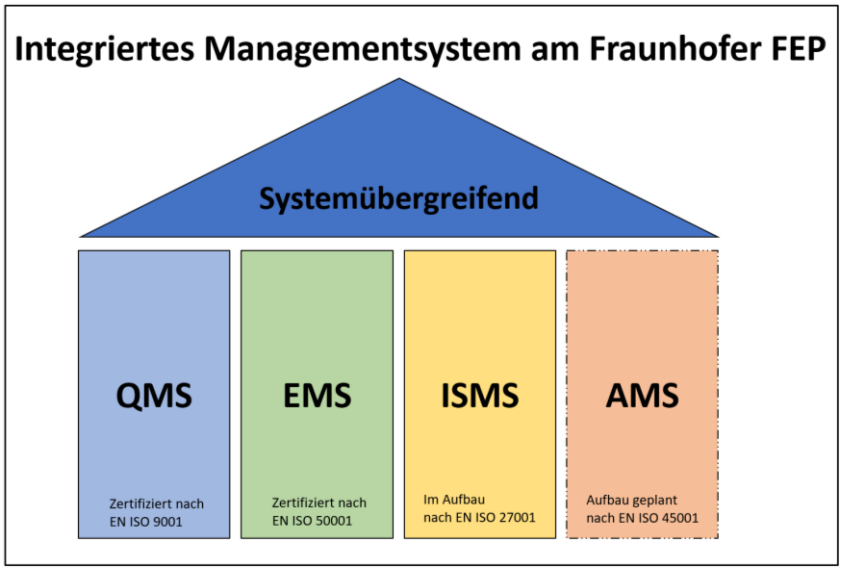
[58] Vgl. Eitner, 2021a

4.2 Management am Fraunhofer FEP

Integriertes Management

Das integrierte Managementsystem am Fraunhofer FEP besteht aus den vier Managementstandards Qualität, Energie, Informationssicherheit und Arbeitsschutz. Das Qualitätsmanagementsystem ist nach der DIN EN ISO 9001:2015 und das Energiemanagementsystem nach der DIN EN ISO 5001:2018 zertifiziert. Das Informationsmanagementsystem (ISMS) nach der DIN EN ISO 27001:2017 befindet sich gerade im Aufbau und das Arbeitsschutzmanagementsystem wird im Sinne des KVP weiterentwickelt, um in Zukunft das systemische Level der DIN EN ISO 45001:2018 zu erreichen. Das integrierte Managementsystem am Fraunhofer FEP wird nach dem Konzept der systemübergreifenden Integration geführt. Wie in Kapitel 2.3.3 beschrieben findet die Zusammenführung der einzelnen Standards über die systemübergreifenden Aspekte statt und die prozess- und ablauforientierten Funktionen werden getrennt betrachtet. Systemübergreifend wird die Politik umgesetzt, findet die Kommunikation über das Intranet und finden Schulungen statt und werden Stakeholder überprüft. Währenddessen pro Managementstandard ein Beauftragter berufen ist. Z.B. wird im Beschaffungsprozess geprüft, ob bestimmte Kundenanforderungen erfüllt sind (QMS), ob energierelevante Aspekte existieren (EMS), ob Informationssicherheitsrisiken bestehen (ISMS) und ob bei der Beschaffung von Gefahrstoffen der Gefahrstoffbeauftragte mit einbezogen wird (AMS). In Abb. 7 ist die Übersicht des integrierten Managementsystems am Fraunhofer FEP bildlich dargestellt.

Abb. 7: Übersicht integriertes Management am Fraunhofer FEP[59]



Projektmanagement

Weil die neuen Anforderungen zu Informationssicherheit und Datenschutz in den Projektprozess integriert werden müssen, ist es wichtig zu untersuchen, wie das Projektmanagement am Fraunhofer FEP aufgebaut ist und gelebt wird. Mögliche Lücken oder Verbesserungsmöglichkeiten im Projektmanagement aufzudecken ist einer der ersten Schritte zur Implementierung der neuen Anforderungen. Durch Beobachtungen, Recherchen und Rücksprache mit den Managementbeauftragten sind folgende Schwächen bzw. Verbesserungsmöglichkeiten ermittelt worden:

- Es fehlt ein Gesamtüberblick über die Prozesse des PM.
- Es gibt eine Intranetseite zu Qualitätsmanagement und Energiemanagement aber nicht zu Projektmanagement.
- Die Anforderungen und Regelungen zum Durchführen von Projekten sind vorhanden, jedoch in vielen verschiedenen Dokumenten und an unterschiedlichen Orten.
- Es gibt keine Vorlage einer systemübergreifenden Risikobetrachtung im Projektgeschäft, zur Sicherung der Assets (Vermögenswerte) des Fraunhofer FEP.

[59] Angelehnt an Pischon und Liesegang, 1999, S. 320.

Im gleichen Zuge zur Implementierung der neuen Anforderungen in das Projektgeschäft sollen die Verbesserungsmöglichkeiten im Projektmanagement umgesetzt werden, um so gleichzeitig die Wirksamkeit der Integration zu erhöhen. Die Umsetzung dieser Verbesserungen wird in Kap. 7.1 beschrieben.

4.3 Neue Anforderungen zur Informationssicherheit

Informationssicherheitsmanagementsysteme dienen zum Schutz wertvoller Informationen und Werte von Unternehmen und Behörden. Informationen müssen in allen Phasen von Geschäftsprozessen vor Manipulation, Offenlegung und Zerstörung geschützt werden. Die Einführung eines ISMS bietet verschiedene Vorteile. Neben Kosteneinsparungen sind eine Steigerung der Arbeitsqualität und des Kundenvertrauens sowie die Optimierung der IT-Struktur und weiterer organisatorischer Abläufe positive Nebeneffekte.[60]

Die Fraunhofergesellschaft hat sich gemäß ihrer vom Vorstand verabschiedeten Informationssicherheitspolitik an die DIN EN ISO/IEC 27001:2017 orientiert.[61] Die ISO 2700x-Reihe sind die von den Normungsorganisationen ISO und IEC zusammengeführten Standards zur Informationssicherheit. Dazu gehört die ISO 27000, welche einen zusammenfassenden Überblick über ISMS und wichtige Definitionen, Begriffe, Prinzipien und Konzepte gibt. Die ISO 27001, gilt als internationaler Standard zum Management von Informationssicherheit. Sie enthält allgemeine Empfehlungen zur Einführung, zum Betrieb und zur Verbesserung eines dokumentierten und zertifizierungsfähigen ISMS. Die ISO 27002 ist eine Hilfe mit Möglichkeiten und Empfehlungen zur praktischen Umsetzung in der Organisation.[62]

2019 wurden wichtige Anforderungen an Informationssicherheit und Datenschutz von der Fraunhofer-Zentralverwaltung bekannt gegeben, welche das Fraunhofer FEP im Projektgeschäft umsetzen muss. Es handelt sich um neun allgemeine Anforderungen,

[60] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, S. 5.

[61] Persönliche Kommunikation, 15. September 2020

[62] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2008, S. 8–9.

welche wissenschaftliche Projekte erfüllen müssen (s. Tab. 4). Projekte sind die Wertschöpfungsprozesse am Fraunhofer-Institut. Veränderungen im Projektprozess sind also mit großer Sorgfalt durchzuführen und dürfen das tägliche Projektgeschäft nicht negativ beeinflussen. Aus diesem Grund ist eine umfangreiche Analyse des komplexen Systems und des Projektprozesses notwendig, um herauszufinden, wie die neuen Anforderungen am besten implementiert werden können.

Tab. 4: Neue Anforderungen an Projekte[63]

Nr.	Anforderung
A1	**Sicherheitsanforderungen von Auftraggebern rechtzeitig erkennen, prüfen und erfüllen** Auftraggeber verlangen immer öfter, dass bestimmte Sicherheitsrichtlinien umgesetzt werden. Das können z.B. Sicherheitszertifikate, Fragebögen zur Eigenbewertung der Sicherheit im Institut oder die Zulassung von externen Sicherheits-Auditierungen sein. Diese Anforderungen müssen rechtzeitig erkannt werden, um zu prüfen inwieweit diese erfüllt werden können.
A2	**Informationssicherheits-Risiken bewerten** Das Risiko durch Vernichten, veröffentlichen, verfälschen oder durch anderweitigen Missbrauch von Informationen muss über Wahrscheinlichkeit und Schadensausmaß bewertet werden. Eine Risikobewertung bildet die Grundlage zur Planung von Sicherheitsmaßnahmen.
A3	**Datenschutzrisiken bewerten und ggf. Datenschutzfolgenabschätzung durchführen** Es ist zu bewerten, welche Datenschutzrisiken für betroffene Personen entstehen können. Besteht ein hohes Risiko für Betroffene oder werden besonders viele personenbezogene Daten in einem Projekt genutzt, ist es gesetzlich vorgeschrieben eine Datenschutzfolgeabschätzung durchzuführen.
A4	**Angemessene Sicherheitsmaßnahmen für genutzte IT treffen** Das Sicherheitskonzept des Instituts und die IT-Benutzungsordnung bilden grundlegende Sicherheitsmaßnahmen für genutzte IT in Projekte. Ja nach Projekt, kann es notwendig sein, dass ergänzende Maßnahmen, wie z.B. Anonymisierung oder Sicherheitsmaßnahmen für Kooperationsplattformen getroffen werden.

[63] Internes Dokument FhG: Informationssicherheit und Datenschutz im Projektmanagement, S. 5-6, 2019

Nr.	Anforderung
A5	**Informationsklassifizierung** Informationen müssen nach bestimmten Regeln klassifiziert werden. Dazu müssen die Vorgaben des Fraunhofer-Instituts und ggf. die des Kunden eingehalten werden.
A6	**Verarbeitungstätigkeiten melden (Verfahrensmeldung)** Bei der Sammlung einer größeren Menge oder sensiblen personenbezogenen Daten in einem gesonderten Verfahren im Projekt, ist es erforderlich diese Verarbeitungstätigkeit zu melden.
A7	**Rechtsgrundlagen der Datenverarbeitung sicherstellen** Zur Verarbeitung personenbezogener Daten muss ein Erlaubnisbestand vorliegen. Das kann die Einwilligung der betroffenen Personen, lebenswichtige, öffentliche oder berechtigte Interessen oder rechtliche Vorgaben sein.
A8	**Betroffenenrechte sicherstellen** Sollen personenbezogene Daten verarbeitet werden, müssen die betroffenen Personen in Kenntnis gesetzt werden. Hierzu zählen z.B. Projekte, die eine Internetpräsenz aufbauen, Projekte die Umfragen durchführen oder Personen für wissenschaftliche Projekte anwerben.
A9	**Sorgfältige Auswahl von Web- und Cloud-Diensten und Dienstleistern** Die Zulässigkeit der Anbieter und der Verarbeitungen mit diesen Medien muss überprüft werden.

4.4 Vorbetrachtungen zur Integration der neuen Anforderungen in das bestehende integrierte Managementsystem

Vor der eigentlichen Integration der neuen Anforderungen der Fraunhofer Zentralverwaltung werden verschiedene Betrachtungen durchgeführt. Diese Vorbetrachtungen werden nachfolgend in der Reihenfolge der Durchführung aufgezählt und sind im Anhang zu finden.

- Ideensammlung: Verschaffen eines groben Überblicks über die Aufgabe der Integration neuer Anforderungen (s. Anhang_03_Ideensammlung).
- Zielkatalog: Festlegen von Ist-, Soll-, Kann- und Nicht-Zielen (s. Anhang_04_Zielkatalog).

- Machbarkeitsanalyse: Machbarkeit der Aufgabe der Integration der neuen Anforderungen ermitteln (s. Anhang_05_Machbarkeitsanalyse).
- Risikoanalyse: Ermitteln potentieller Risiken welche die Aufgabe der Integration behindern, bzw. gefährden können (s. Anhang_06_Risikoanalyse).

Diese Vorbetrachtungen können als Teil eines Methodenbaukastens für zukünftige Untersuchungen angesehen werden. Aus diesem Grund werden sie Teil des Leitfadens sein. Zu den näheren Erläuterungen dieser Methoden sei deshalb auf den entwickelten Leitfaden verwiesen. Weil Vorbetrachtungen allein nicht ausreichen werden, um die Aufgabe der Integration bewältigen zu können, sollen im nächsten Kapitel verschiedene Analysemethoden zur Untersuchung von (integrierten) Managementsystemen vorgestellt werden. Nach der Darstellung dieser Methoden, erfolgt eine Prüfung zur Eignung der Analyse von (integrierten) Managementsystemen.

5 Methoden zur Analyse von (integrierten) Managementsystemen

5.1 Audits

Das Wort Audit hat seinen Ursprung vom lateinischen Wort *audire*, welches übersetzt „hören“ bedeutet. Demzufolge handelt es sich bei einem Audit um eine Anhörung bzw. Inspektion, wobei bestimmte Prozesse oder Gegebenheiten beobachtet oder Überwacht werden können.[64]

Laut dem Leitfaden zur Auditierung von Managementsystemen DIN EN ISO 19011:2018, wird ein Audit wie folgt definiert: „… systematischer, unabhängiger und dokumentierter Prozess zum Erlangen von objektiven Nachweisen und zu deren objektiver Auswertung, um zu bestimmen, inwieweit Auditkriterien erfüllt sind.“[65]

Durch Audits kann geprüft werden, ob ein Managementsystem bestehende Anforderungen erfüllt bzw., in welchem Maße diese erfüllt sind. Anforderungen an ein Managementsystem können verschiedenen Ursprungs sein. Mögliche Anforderungen sind die Normen, nach der das Managementsystem ausgerichtet ist, Gesetze und Branchenstandards, Kundenanforderungen und Ergebnisse vorangegangener Audits. Eine weitere wichtige Funktion von Audits ist es, Schwachstellen zu identifizieren und Verbesserungs- und Lösungsvorschläge aufzuzeigen umso den Kontinuierlichen Verbesserungsprozess voran zu treiben.[66]

Um ein Audit durchzuführen, werden Auditkriterien, zur Prüfung der Auditnachweise herangezogen. Auditkriterien können Verfahren, Vorgehensweisen oder Anforderungen sein. Auditnachweise sind für die Auditkriterien relevante, zutreffende und verifizierbare

[64] Vgl. Brauweiler et al., 2015, S. 3.

[65] Zit. DIN EN ISO 19011:2018, S. 11.

[66] Vgl. Brauweiler et al., 2015, S. 3.

Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen.[67] In der folgenden Tabelle sind Beispiele für Auditkriterien und Nachweise aufgelistet:

Tab. 5: Beispiele Auditkriterien und Nachweise[68]

Beispiele für Auditkriterien	**Auditnachweise**
Regelmäßige Beurteilung von Informationssicherheitsrisiken	Durchgeführte und dokumentierte Informationssicherheitsrisikobeurteilung
Rechtskonformität	Rechtskataster
Regelmäßige Schulungen der Mitarbeiter	Schulungsnachweise, Schulungsplan
Regelmäßige Kommunikation und Information	Kommunikationsmatrix

Bevor Audits durchgeführt werden, wird i.d.R. ein Auditprogramm erstellt. Ein Auditprogramm ist ein Plan, in dem festgelegt ist wann die Audits stattfinden, welche Arten von Audits durchgeführt werden, welche Unternehmensbereiche auditiert werden und wer auditiert. Abb. 8 zeigt wie ein Auditprogramm aufgebaut sein kann. Auch während der Audittätigkeiten wird das Auditprogramm regelmäßig überprüft und ggf. überarbeitet, um sicherzustellen, dass Audits zielorientiert und nicht zum Selbstzweck durchgeführt werden. Das Auditprogramm wird von den Managementbeauftragten erstellt und vorm Verteilen im Unternehmen von der obersten Leitung genehmigt.[69]

[67] Vgl. DIN EN ISO 19011:2018, S. 11–18.

[68] Eigene Darstellung

[69] Vgl. Brauweiler et al., 2015, S. 9–10.

Abb. 8: Vorlagebeispiel eines Auditprogramms[70]

Jahr	Auditart und -bereich	Auditor	Jan	Feb	…	Nov	Dez	Zeitpunkt (Datum) Erledigt (Signum)

Zur Durchführung eines Audits wird ein Auditplan erstellt, welcher folgende Punkte beinhaltet:

- Die Auditziele
- Den Umfang
- Die Auditkriterien
- Die zu prüfenden Dokumente
- Der zu prüfende Bereich bzw. Standort
- Methoden
- Rollen und Verantwortlichkeiten

Dieser Plan begleitet das Audit und hilft dem Auditor das Audit strukturiert durchzuführen. Da ein Audit zeitbeschränkt ist, muss zwischen genauer und detaillierter Betrachtung aller Einzelheiten und dem Erreichen eines umfassenden Überblicks abgewogen und das richtige Mittelmaß gefunden werden.[71]

[70] Brauweiler et al., 2015, S. 10.

[71] Vgl. Brauweiler et al., 2015, S. 15–16.

Abb. 9: Beispiel eines Auditplans[72]

Zeit	Thema	Bereich	Beteiligte	Elemente ISO 14001
8.15–8.30	Einführungsgespräch			–
08.30–09.00	Verantwortung der Obersten Leitung (Umweltpolitik, -ziele und -programm, KVP, Managementbewertung Rechtskonformität, Notfallmanagement, Gefahrstoffe)			4.2, 4.3.2, 4.3.3, 4.4.7, 4.5.1, 4.5.3, 4.6; 4.4.4, 4.4.5, 4.5.4
09.00–10.30	Notfallmanagement, Gefahrstoffmanagement, Wartung und IH, Verantwortlichkeiten, Pflichtenübertragung, Beauftragte,			4.4.1, 4.4.6, 4.4.7, 4.5.1; 4.4.4, 4.4.5, 4.5.4
10.30–11.30	Betriebsbegehung, Teil 1			4.4.1, 4.4.6, 4.4.7, 4.5.1; 4.4.4, 4.4.5, 4.5.4
11.30–12.00	Rechtskonformität, Bewertung der Einhaltung von Rechtsvorschriften und anderen Anforderungen, Schulungen, Kommunikation			4.3.2, 4.5.2, 4.4.2,4.4.3; 4.4.4, 4.4.5, 4.5.4

Nachdem das Audit durchgeführt wurde, wird ein Auditbericht, der eine Auswertung des Audits enthält erstellt. Ein Auditbericht soll kurz und knapp aber trotzdem prägnant sein. Inhalte des Auditberichts sind dieselben wie die des Auditplans plus:

- Der Umfang des Audits z.B. auditierte Prozesse, Themen
- Auditfeststellungen und ggf. Nachweise
- Informationen inwieweit die Auditkriterien erfüllt wurden sind
- Auditschlussfolgerungen

Abb. 10 zeigt eine mögliche Gliederung eines Auditberichts. Auf Basis der Auditfeststellungen lassen sich Maßnahmen zur Beseitigung und Vorbeugung von Abweichungen oder zur Verbesserung ableiten. Für die Umsetzung der Maßnahmen ist die Organisation verantwortlich. Die Umsetzung der terminierten Maßnahmen wird daraufhin in Folgeaudits überprüft.[73]

[72] Brauweiler et al., 2015, S. 17.

[73] Vgl. Brauweiler et al., 2015, S. 24.

Abb. 10: Beispiel zur Gliederung eines Auditberichtes[74]

1. Informationen zum durchgeführten Audit

Auditierter Bereich		**Datum:**	
Regelwerk	DIN EN ISO 14001:2009		
Auditor			
Auditziel	Beurteilung des Umweltmanagementsystems in der xy-GmbH auf Konformität mit den Anforderungen der DIN EN ISO 14001:2009 (internes Systemaudit)		
Dokumentation	UMHB, Revision xxx		
Auditplan	siehe Anlage		

2. Vorgehen

3. Grundsätzliche und zusammenfassende Einschätzungen

4. Auditfeststellungen (Auszug am Beispiel des Normkapitels 4.3 „Planung“)

Norm kap.	Benennung	Konformitätsbewertung					Korrektur- oder Vorbeugemaßnahme
		1	2	3	NZ	Erläuterung	
4.3	**Planung**						
4.3.1	Umweltaspekte						
4.3.2	Rechtliche Verpflichtungen und andere Anforderungen						
4.3.3	Zielsetzungen, Einzelziele und Programm(e)						

Erläuterungen:
1 = Erfüllt, 2 = Nebenabweichung, 3= Hauptabweichung, NZ = Nicht zutreffend

5. Abschließende Hinweise

Auditor, Unterschrift
Ort, Datum

6. Anlage: Auditplan

5.2 Beobachtung

Zu den mit am häufigsten genutzten Methoden empirischer Forschung gehören Beobachtungsverfahren. Sowohl in den Naturwissenschaften als auch in den Sozialwissenschaften werden mittels Beobachtungen Erkenntnisse erlangt, um bestimmte Fragen beantworten zu können. Da der Mensch seine Umgebung ständig durch

[74] Brauweiler et al., 2015, S. 25.

Beobachtungen wahrnimmt und diese bewusst und unbewusst interpretiert und analysiert, ist diese Methode ein sinnvolles Mittel, um Informationen zu gewinnen.[75] In dieser Arbeit werden Recherche und Gespräche zur Beobachtung gezählt.

5.3 Stakeholderanalyse

Um zu zeigen, was eine Stakeholderanalyse ist, wie sie aufgebaut ist und welche Ergebnisse zu erwarten sind, ist es von Vorteil den Begriff Stakeholder zu definieren. Stakeholder ist ein Synonym für Interessierte Partei oder Interessengruppe. [76]

Definition: Stakeholder sind Personen oder Personengruppen, innerhalb oder außerhalb einer Organisation, die durch das Managementsystem beeinflusst werden oder es beeinflussen können.[77]

Stakeholder werden in intern (innerhalb der Organisation) und extern (außerhalb der Organisation) unterteilt. Interne Stakeholder sind z.B. Mitarbeiter, Führungskräfte, Beauftragte z.B. aus Qualitäts-, Arbeitssicherheit- und Energiemanagement, Betriebs- und Personalräte, Gewerkschaftsvertreter und die Geschäftsführung. Zu den externen Stakeholdern gehören Kunden, Lieferanten, Behörden, die Öffentlichkeit wie Nachbarn Bürgerinitiativen, Vereine und Verbände, regionale und überregionale Medien, der Grundstückseigentümer, Wettbewerber, etc.

Es ist sinnvoll die Stakeholder einer Organisation zu betrachten. Sind die Erwartungen und Erfordernisse der interessierten Parteien bestimmt, kann daraus abgeleitet werden, welche bindenden Verpflichtungen sich daraus für die Organisation ergeben.

Die Analyse der Stakeholder dient dazu, Erfordernisse und Erwartungen der interessierten Gruppen zu identifizieren. So werden zum einen rechtliche Verpflichtungen ermittelt und zum anderen Anforderungen, die sich die Organisation auf Basis der Stakeholderanalyse selbst auferlegen kann. Beispiele hierfür sind Vertragsbeziehungen,

[75] Vgl. Drinck, 2013, S. 182.

[76] Vgl. Brauweiler et al., 2018b, S. 13.

[77] Vgl. DIN EN ISO 14001:2015, S. 16.

gesellschaftliche und ethische Standards, Organisations- und Branchenstandards, etc. Ziel ist es bindende Verpflichtungen aus den Erwartungen und Interessen der Stakeholder abzuleiten. [78]

Es gibt verschiedene Ansätze, eine Analyse der Interessengruppen durchzuführen. Zu allererst sollten die Stakeholder und ihre Rolle definiert werden. I.d.R. werden die Stakeholder wie oben beschrieben in intern und extern geteilt.

Je nach Struktur der Organisation können auch weitere Unterteilungen vorgenommen werden. Sollte eine Organisation beispielsweise einen Produktionsprozess auslagern, sog. Outsourcing können die Stakeholder, die mit diesem Prozess verbunden sind, extra betrachtet werden. Wenn der Prozess z.B. im Ausland abläuft, bietet sich solch eine gesonderte Betrachtung an, weil sich Interessen und Befürchtungen stark unterscheiden können.

Als nächstes werden die Erwartungen und Befürchtungen der einzelnen Stakeholder notiert. Mit diesen Informationen kann dann die eigentliche Bewertung durchgeführt werden. Als praktikabel hat sich herausgestellt, auf Grundlage von Einfluss/Macht und Konfliktpotenzial zu bewerten. Dazu eignet sich ein einfaches Punktesystem, indem die Bewertungszahlen addiert werden, um so die einzelnen Stakeholder zu priorisieren. Diese Priorisierung dient dazu die Interessengruppen in wichtige, weniger wichtige und nicht wichtige Gruppen aufzuteilen. Auf dieser Basis ist dann bekannt, welche Stakeholder besonders beachtet und welche bindenden Verpflichtungen eingegangen werden müssen.

[78] Vgl. Brauweiler et al., 2018b, S. 15.

Abb. 11: Beispiel einer Stakeholderanalyse[79]

Externe Stakeholder	Thema	Einfluss/Macht*	Konfliktpotenzial*	Bedeutung**	Auswirkungen auf das UMS/ erforderliche Regelungen	Bindende Verpflichtung
Umweltamt, Gewerbeaufsichtsamt	• Einhaltung der behördlichen Informationspflichten z. B. nach BImschG	3	3	A (6)	• Aufnahme der Informationspflichten in das Kataster der bindenden Verpflichtungen	ja
A-Kunde	• Vorgaben für die Konservierung von Zwischenprodukten	3	3	A (6)	• Prozessregelung	ja
Anwohner	• Beschwerden über Lärmemissionen nachts	1	1	C (2)	• Regelungenzu Fenster- und Türöffnungen in der Nacht • regelmäßige Lärmmessung	nein

Interne Stakeholder	Thema	Einfluss/Macht*	Konfliktpotenzial*	Bedeutung**	Auswirkungen auf das UMS/erforderliche Regelungen	Bindende Verpflichtung
Eigentümer	• Konzentration auf kurzfristigen Erfolg	3	3	A (6)	• Bedeutung des UMS für die Erzielung von Einspareffekten hervorheben	nein
Mitarbeiter	• Zunahme der Krankmeldungen durch ergonomisch ungünstige Verpackungstätigkeiten	3	2	A (5)	• Suche nach einer technologischen Alternative	ja

* Punktbewertung:
3 = hoch
2 = mittel
1 = niedrig

** Summe aus Einfluss/Macht + Konfliktpotenzial
A – Stakeholder (6-5)
B – Stakeholder (4-3)
C – Stakeholder (2-1)

5.4 ABC-Analyse

Ein Haupteinsatzgebiet der ABC-Analyse ist die Materialwirtschaft. Dort wird sie schon seit langem erfolgreich eingesetzt um herausfinden, welche Artikel und Lieferanten wichtig sind und welche weniger zu beachten sind.[80] Allgemein werden in der ABC-Analyse wichtige von unwichtigen Sachverhalten getrennt. Im ursprünglichen Einsatzgebiet sollen verschiedene Bereiche der Beschaffung transparent dargestellt werden, um Ansatzpunkte für eine Effizienzsteigerung ermitteln zu können.

[79] Brauweiler et al., 2018b, S. 16.

[80] Vgl. Tiedtke, 2007, S. 321.

In der Beschaffung wird bei der ABC-Analyse ein Bezug zum Wert eines Gutes und dessen Menge hergestellt. Dabei weisen A-Materialien den höchsten Wert auf und die C-Materialien den geringsten. Mengenmäßig verhält es sich gegenteilig. Die A-Materialien weisen die geringste Menge auf und die C-Materialien die höchste.[81]

Um eine ABC-Analyse durchführen zu können, müssen vergleichbare Daten, wie z.B. Kunden/Umsatz oder Ressourcen/Kosten vorhanden sein. Um eine ABC-Analyse durchzuführen, werden zuerst die Merkmale z.B. Umsatz pro Kunde festgelegt. Dazu wird eine Tabelle erstellt, in der die Elemente nach dem Merkmal sortiert und die Werte in einer weiteren Spalte kumuliert werden (s. Abb. 12). Im nächsten Schritt werden die Merkmale in die A, B und C Kategorie geteilt und grafisch aufbereitet (s. Abb. 13).[82]

Abb. 12: Beispieltabelle einer ABC-Analyse[83]

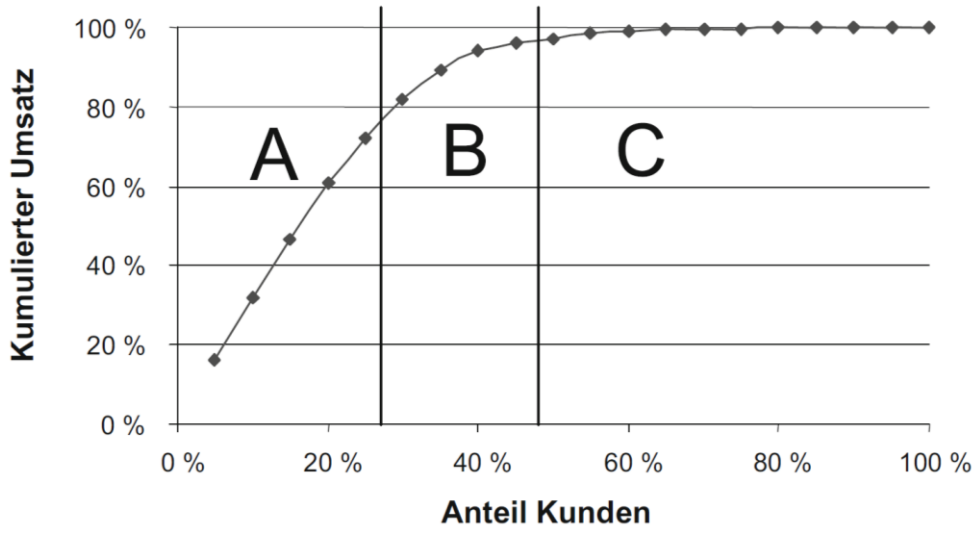
Nr.	Prozent Kunden	Kunde	Umsatz 2004 (in Euro)	Kumulierter Umsatz
1	5 %	Schawel GmbH	100.000	16,4 %
2	10 %	Billing GmbH	95.000	31,9 %
3	15 %	Hartenstein GmbH	90.000	46,7 %
4	20 %	Grein GmbH	85.000	60,6 %
...	...	...	...	...
20	100 %	Maurer GmbH	300	100 %
			610.400	

[81] Vgl. Brecht, 2012, S. 81.

[82] Vgl. Schawel und Billing, 2018, S. 16.

[83] Schawel und Billing, 2018, S. 16.

Abb. 13: Beispieldiagramm einer ABC-Analyse[84]



5.5 Checklisten

Mithilfe von Checklisten lassen sich Aufgaben Strukturieren, Lösen und Kontrollieren. Sie helfen keine Punkte zu vergessen und diese zu ordnen und zu priorisieren. Checklisten können als eine Ansammlung verschiedener Kriterien zum Erreichen eines Ziels verstanden werden.[85]

5.6 Verbal-argumentative Bewertung

Die verbal-argumentative Methode ist eine subjektive Bewertung. Mit ihr können Vor- und Nachteile, Schaden und Nutzen sowie Stärken und Schwächen eines Bewertungsgegenstands gegenübergestellt und abgewogen werden. Da die Eigenschaften schnell und einfach erfasst werden, ist dies Methode zeit- und kostengünstig. Das Ergebnis ist oft eine Bilanz von pro und contra Argumenten, die meist eine rein verbale Übersicht bilden.[86]

[84] Schawel und Billing, 2018, S. 17.

[85] Vgl. Hurtz und Flick, 2002, S. 165.

[86] Vgl. Deimer, 2005, S. 27.

5.7 SWOT-Analyse

Die SWOT-Analyse ist eine beliebte Methode, um Situationen im Management und Marketing untersuchen zu können. Des Weiteren kann sie auch in der Personal- und Führungskräfteentwicklung eingesetzt werden. Ursprünglich sollte die SWOT-Analyse die Hauptfrage beantworten, wie ein Unternehmen seine Existenz langfristig sichern kann. Diese Kernfrage wurde wiederum in kleinere Fragen unterteilt:

- Was funktioniert aktuell sehr gut? (engl. **S**trengths – Stärken)
- Welche weiteren Möglichkeiten und Chancen gibt es? (engl. **O**pportunities – Gelegenheit)
- Was läuft schlecht? (engl. **F**ault – Fehler)
- Was kann schiefgehen? (engl. **T**hreat – Gefahren oder Risiken)

Bei Volkswagen wurde das Akronym „**SOFT**“ zu „**TOWS**“ indem Fehler mit Schwächen (engl. Weaknesses) ersetzt wurde. Aus „**TOWS**“ wurde letztendlich „**SWOT**“.[87]

Mit der SWOT-Analyse soll die Ausgangslage möglichst zuverlässig und realistisch eingeschätzt werden. Dazu wird das interne und externe Umfeld untersucht. Zum internen Umfeld gehören die Stärken und Schwächen der Organisation z.B. Motivation, Führungsqualität, Mitarbeiterzufriedenheit, Finanzen, Patente, Image, Erfahrung, etc. Zum externen Umfeld gehören die Chancen und Risiken. Das können Trends und Veränderungen in verschiedenen Bereichen wie Technologie, Politik, internationale Beziehungen usw. sein. Nachdem die SWOT-Analyse durchgeführt wurde, können Maßnahmen und Strategien abgeleitet werden, um in Zukunft den Erfolg der Organisation sicherzustellen.[88]

[87] Vgl. Pelz, 2018, S. 2.

[88] Vgl. Pelz, 2018, S. 4–5.

Abb. 14: Beispiel einer SWOT-Analyse der Organisation Google[89]

Chancen	Risiken
▸ Marktwachstum bei Tablets und Smartphones ▸ Wachstum des Marktes für mobile Werbung ▸ Wachsender Unterhaltungsmarkt bei Videos (Streaming)	▸ Starker Wettbewerb durch Amazon, Facebook und Netflix ▸ Wachsendes Bewusstsein für Datenschutz in der Bevölkerung ▸ Gesetzgebung (Marktmacht, Urheberrecht)
Stärken	**Schwächen**
▸ Globaler Marktführer bei Suchmaschinen ▸ Android als Treiber des Wachstums im Mobil-Markt ▸ Hohe Liquidität und Produktivität	▸ Sehr starke Abhängigkeit vom Werbemarkt ▸ Kaum Fortschritte beim Ausbau des eigenen sozialen Netzwerks ▸ Wenig Innovation im Werbemarkt

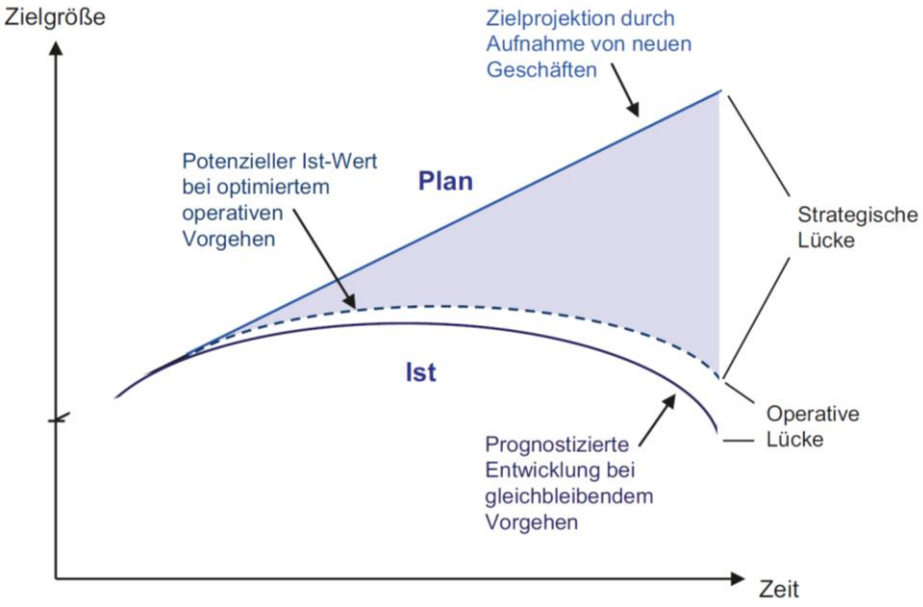
5.8 Gap-Analyse

Die Gap-Analyse auch Fit-Gap-Analyse, Lückenanalyse oder Ist-Soll-Analyse ist ein Instrument zur Beschreibung und Beurteilung eines Untersuchungsgegenstandes, wie z.B. Organisationen, Managementsysteme, Prozesse, etc. Bei dieser Analyse wird ermittelt ob vorgegebene Soll-Zustände vorhanden sind. Diese Soll-Zustände werden den Ist-Zuständen gegenübergestellt. Stimmt der Soll-Zustand nicht mit dem Ist-Zustand überein, ist ein „Gap“ also eine Lücke nachgewiesen. Gaps werden in operative und strategische Lücken unterschieden. Operative Lücken sind jene Gaps, zwischen prognostizierter Entwicklung ohne Veränderung und potenzieller Entwicklung mit Veränderung und daraus resultierendem optimierten Vorgehen. Strategische Lücken sind die Abweichungen, zwischen der potentiell besten Entwicklung und dem zu erwartenden Ergebnisziel. In Abb. 15 ist das Prinzip der Gap-Analyse dargestellt.[90]

[89] Pelz, 2018, S. 6.

[90] Vgl. Schifferer und Reitzenstein, 2018, S. 17–18.

Abb. 15: Prinzip der Gap-Analyse[91]



Das Identifizieren, Strukturieren sowie eine qualitative und nach Möglichkeit auch quantitative Beschreibung ist das Ziel der Gap-Analyse. Auf Basis der identifizierten Lücken, lassen sich im nächsten Schritt die Gründe der ermittelten Abweichungen analysieren. Die Gap-Analyse ist vielseitig einsetzbar. Mit ihr lassen sich z.B. die Planwerte, also die Ist-Größen und die vordefinierten Soll-Größen von Umsatz- und Absatzzahlen vergleichen. Ein weiteres Anwendungsbeispiel ist eine Mitarbeiterbefragung zu Arbeitszeiten oder Arbeitsklima, wobei dann jedoch keine quantifizierte Auswertung möglich ist.[92]

Um die Gap-Analyse durchzuführen ist es zweckmäßig, die Ist- und Soll-Werte also den Status quo zu ermitteln. Das kann mit einer oder mehreren vorausgehenden Analysemethoden geschehen. Nach der Gegenüberstellung der beiden Werte und der Identifizierung der Gaps, können Hinweise auf Fehlentwicklungen oder Versäumnisse vorliegen. Bei der Einführung oder Veränderung von Systemen, Prozessen o.ä. kann die Gap-Analyse zur Konformitätsprüfung genutzt werden. Als Ergebnis entsteht eine Übersicht, welche Schritte zur vollständigen Konformität noch getätigt werden müssen.

[91] Schifferer und Reitzenstein, 2018, S. 15.

[92] Vgl. Schifferer und Reitzenstein, 2018, S. 17–18.

Gleichzeitig kann der Grad der Zielerreichung abgeschätzt werden. Bei einer Konformitätsprüfung wird nicht in operative und strategische Lücken unterschieden, sondern ob Konformität vorliegt oder nicht.[93]

5.9 Eignung der Methoden zur Analyse von (integrierten) Managementsystemen

Nachdem die möglichen Analysemethoden vorgestellt sind, wird nun eine Argumentenbilanz aufgestellt, um zu bewerten welche Methode zur Analyse von Managementsystemen und dessen Prozessen geeignet ist (s. Tab. 6).

Eine Argumentenbilanz ist ein Verfahren zur Auflistung von Vor- und Nachteilen verschiedener Alternativen in verbaler Form. Diese Bewertungsmethode eignet sich für die Erstbewertung. Sollte sich herausstellen, dass eine detailliertere Bewertungsmethode notwendig ist, kann diese im Nachgang noch durchgeführt werden.[94]

Tab. 6: Vor- und Nachteile der vorgestellten Analysemethoden[95]

Methode	Pro	Contra
Beobachtungen	- Objektiv - Kann als Grundlage zur Gap-Analyse genutzt werden. - Maßnahmen lassen sich direkt ableiten.	- Detailtreue hängt vom Engagement und der Kompetenz des Beobachters ab
ABC-Analyse	- Leicht und übersichtlich	- Benötigt Daten, die verarbeitet werden können - Quantitative Auswertung selten qualitativ - Subjektive Bewertungsgrenzen - Nicht zur Bewertung komplexer Systeme geeignet
SWOT-Analyse	- Objektiv - Gute Nachvollziehbarkeit	- Detaillierte Analysen sind nicht möglich, es können nur allgemeine Aussagen getroffen werden

[93] Vgl. Schifferer und Reitzenstein, 2018, S. 14–17.

[94] Vgl. VDI-Gesellschaft Produkt- und Prozessgestaltung, 2011, S. 144–146.

[95] Eigene Darstellung

Methode	Pro	Contra
Verbal-argumentative Bewertung	- Maßnahmen lassen sich direkt ableiten	- Sehr subjektiv - Es erfolgt keine Dokumentation - Nicht zur Bewertung komplexer Systeme geeignet
Stakeholder-analyse	- Interessen der Stakeholder sind von zentraler Bedeutung im Management - Die Interessen der Beteiligten und die eigenen Interessen werden in Einklang gebracht - Maßnahmen lassen sich direkt ableiten	- Stakeholder müssen bekannt sein
Audits	- Direktes in Kontakt treten mit den betreffenden Personen - Hilft die Institution besser kennen zu lernen - Kann als Grundlage zur Gap-Analyse genutzt werden - Positive Akzeptanz gegenüber Audits im Unternehmen, weil Zusatzinformationen erhalten werden können - Das Durchführen von Audits ist fester Bestandteil im Managementgeschäft - Bewertung komplexer Systeme möglich	- Zeit- und Ressourcenaufwändig - Negative Akzeptanz gegenüber Audits im Unternehmen, kann zu möglicher Befangenheit führen
Checklisten	- Objektiv - Gut geeignet zur Überprüfung der Einhaltung bestehender Regelungen	- Geregelter Ablauf der Aufgabe / Tätigkeit muss schon bekannt sein - Nicht geeignet zur Analyse von Managementsystemen, nur für die Bewertung von Einzelprozessen geeignet
Gap-Analyse	- Objektiv - Detailgetreu - Gewährleistet vollständige Betrachtung des gesamten Managementsystems - Konformitätsstatus gegenüber den Vorgaben (Normanforderungen Organisationsanweisungen, etc.) wird geprüft und bewertet - Bewertung komplexer Systeme möglich	- Sehr zeitaufwändig - Durch Detaillierungsgrad können Einbußen an der Übersichtlichkeit, Vollständigkeit und der Priorisierung auftreten

Als nächstes werden die Vorteile addiert und davon die Nachteile subtrahiert. Das Ergebnis ist in Form einer Bewertung in Tab. 7 zusammengefasst. Die Analysemethoden mit einer Bewertung von minus drei bis eins, werden in nicht geeignet für die Analyse von Managementsystemen eingeteilt und die Methoden, welche eine Bewertung von zwei bis drei aufweisen gelten als geeignet. Nicht geeignet sind die ABC-Analyse, die SWOT-

Analyse, die verbal-argumentative Bewertungsmethode und Checklisten. Geeignet sind Beobachtungen, die Stakeholderanalyse, Audits und die Gap-Analyse.

Um den maximalen Nutzen aus der Untersuchung des Managementsystems am Fraunhofer-Institut zu ziehen, bietet es sich an, die Analysemethoden aufeinander aufzubauen. Da die Gap-Analyse den Ist- und Soll-Zustand gegenüberstellt und die Beobachtungen und Audits den Ist-Zustand ermitteln, ist es von Vorteil erst die Audits durchzuführen und Beobachtungen anzustellen und mithilfe dieser Ergebnisse die Gap-Analyse durchzuführen. Das heißt aber nicht, dass die Beobachtung des Managementsystems an einem bestimmten Punkt abgeschlossen ist. Es wird ständig und aufmerksam auf dessen Verhalten und Entwicklung geachtet, um potentielle Chancen und Risiken ad hoc erkennen zu können.

Tab. 7: Bewertung der Analysemethoden[96]

Methode	Anzahl Vorteile	Anzahl Nachteile	Bewertung*	Eignung zur Analyse von MS
Beobachtungen	3	1	2	geeignet
ABC-Analyse	1	4	-3	nicht geeignet
SWOT-Analyse	2	1	1	nicht geeignet
Verbal-argumentative Bewertung	1	3	-2	nicht geeignet
Stakeholder-analyse	3	1	2	geeignet
Audits	6	2	4	geeignet
Checklisten	2	2	0	nicht geeignet
Gap-Analyse	5	2	3	geeignet

* -3 bis 1: nicht für Analyse von Managementsystemen geeignet
2 bis 3: für die Analyse von Managementsystemen geeignet

[96] Eigene Darstellung

6 Datenerhebung und Auswertung

In diesem Kapitel wird zum einem die Überprüfung der Erfüllung von Informationssicherheits- und Datenschutzanforderungen im Projektgeschäft (prozessorientierter Ansatz) und zum anderen die Analyse des Informationssicherheitsmanagementsystems (systemorientierter Ansatz) behandelt. Der Grund dieser Einteilung liegt darin, dass es bei der Einführung der neuen Anforderungen nicht ausreicht, ausschließlich zu wissen wie mit Informationssicherheit und Datenschutz im Projektgeschäft umgegangen wird. Vielmehr spielen die Prozesse, Tätigkeiten und Vorgaben im Hintergrund eine wesentliche Rolle. Weil die neuen Anforderungen aus dem Bereich der Informationssicherheit und des Datenschutzes kommen, muss auch das dazugehörige System überprüft werden. Dieses System bildet den Rahmen und ist essentiell zur dauerhaften Umsetzung der neuen Anforderungen. Zurzeit befindet sich das ISMS im Aufbau und noch bestehende Lücken müssen geschlossen werden. Mit dem erfolgreichen Einführen des ISMS, ist die Grundstruktur zur Umsetzung der Anforderungen gelegt. Worauf hin im nächsten Schritt, die einzelnen Prozesse im Hinblick auf die vorgegebenen Anforderungen nochmals optimiert werden müssen.

6.1 Audits

Die Audits dienen hauptsächlich zur Überprüfung inwieweit bereits die Informationssicherheits- und Datenschutzanforderungen in den Projekten umgesetzt werden. Da Audits ein fester Bestandteil im Management sind, gab es am Fraunhofer FEP bereits eine Vorlage eines Auditplans. Dessen Vorteil war, dass er nach dem Durchführen eines Audits gleichzeitig als Auditbericht genutzt werden konnte. Für die Datenerhebung zur Untersuchung des Managementsystems und für zukünftige Audits am FEP wurde diese Vorlage um folgende Punkte erweitert, bzw. angepasst:

- es wurde eine Nummerierung der Fragen zur besseren Strukturierung, Nachverfolgung und Auswertung eingeführt
- Anpassung der Kopf und Fußzeile
- Änderungen der Formatierung von Tabellen und Schrift

- um Platz zu sparen wurden die Bezüge zu den Managementsystemnormen unter die Agenda positioniert
- weitere kleine Änderungen

Die Daten wurden zusätzlich zu den regulären internen Audittätigkeiten am Fraunhofer FEP ermittelt. Insgesamt fanden vier Audits zur Untersuchung der Erfüllung von Anforderungen zur Informationssicherheit und Datenschutz im Projektgeschäft statt. In Tab. 8 ist eine Übersicht zu den durchgeführten Audits dargestellt. Die Auditfragen orientierten sich an die Norm DIN EN ISO/IEC 27001:2017 mit Fokus auf den von der Fraunhofer Zentralverwaltung vorgegebenen Anforderungen. Die DIN EN ISO/IEC 27001:2017 wurde als Vorlage zur Fragenentwicklung gewählt, weil so ermittelt werden konnte, wie weit der Aufbau des Informationssicherheitsmanagementsystems war und wo ggf. noch Maßnahmen ergriffen werden mussten. Neben dem Ermitteln des aktuellen Stands, war ein weiterer wichtiger Teil der Audits, in Erfahrung zu bringen welche Erwartungen und Befürchtungen die Projektleiter zur Implementierung der neuen Anforderungen haben. So konnten gleichzeitig Informationen für die Stakeholderanalyse gesammelt werden, um bei der Einführung der neuen Anforderungen auf dessen Interessen eingehen zu können. Es hat sich herausgestellt, dass einige Auditfragen optimiert werden konnten, um somit mehr Informationen von den Projektleitern zu erhalten. Aus diesem Grund können die Audits nicht quantitativ ausgewertet werden. In Tab. 9 sind die Auditfragen aus einem durchgeführten Audit zusammengestellt. Die Daten der systemrelevanten Fragen wurden zur Erstellung der Gap-Analyse genutzt. Ein Zentrales Ergebnis ist, dass standardisierte Prozesse, wie z.B. für die Informationssicherheitsrisikobeurteilung / Datenschutzrisikobeurteilung eingeführt werden müssen.

Die prozessorientierten Fragen wurden gestellt, um zu ermitteln inwieweit die neuen Anforderungen der Fraunhofer Zentralverwaltung bereits im Projektgeschäft umgesetzt werden. Tab. 10 zeigt das Ergebnis. Es ist zu erkennen, dass die meisten Anforderungen bereits oder teilweise umgesetzt sind. Der Grund dafür ist, dass Projekte schon bevor die neuen Anforderungen von der Zentralverwaltung gestellt wurden, gewisse Informationssicherheitsstandards erfüllen mussten.

Tab. 8: Durchgeführte Audits[97]

Termin	Auditart	Bereich	Inhalt	Auditoren	Auditierte
01.07.2020	Prozessaudit	Anlage A	Umsetzung von Anforderungen der Informations-sicherheit / Datenschutz im Projektmanagement	Auditoren: Autor der Masterarbeit, QMB, ISB	Abteilungsleitung, Mitarbeiter
03.07.2020	Prozessaudit	Anlage B	Umsetzung von Anforderungen der Informations-sicherheit / Datenschutz im Projektmanagement	Auditoren: Autor der Masterarbeit, QMB, ISB	Gruppenleitung, Mitarbeiter
03.07.2020	Prozessaudit	Anlage C	Umsetzung von Anforderungen der Informations-sicherheit / Datenschutz im Projektmanagement	Auditoren: Autor der Masterarbeit, QMB, ISB	Gruppenleitung, Mitarbeiter
09.07.2020	Prozessaudit	Anlage D	Umsetzung von Anforderungen der Informations-sicherheit / Datenschutz im Projektmanagement	Auditoren: Autor der Masterarbeit, QMB, ISB	Gruppenleitung, Mitarbeiter

[97] Eigene Darstellung

Tab. 9: Ergebniszusammenfassung Audits[98]

Anforderung	Auditfrage	Fragentyp	Erfüllt?	Erfüllungsgrad*	Bemerkung
DIN EN ISO 27001:2017 6.1.1; Anforderungen der ZV: A1, A2, A3, A4, A6, A7, A8 (Kap. 4.3)	Wie wird mit Risiken und Chancen in Bezug auf Informationssicherheit/Datenschutz im Projekt umgegangen? *(Benutzung IT-Infrastruktur wie, Messenger-, Webdienste, Personenbezogene Daten, Informationsklassifizierung, Exportkontrolle, Geheimhaltung (NDA), Löschkonzept, gesicherter Projektordner, begrenzter Personenkreis, Nutzung VPN, Verschlüsselung, usw.)*	prozess-orientiert	ja	50%	Es werden Maßnahmen geplant und umgesetzt, jedoch werden diese Maßnahmen i.d.R. nicht bewusst dokumentiert.
DIN EN ISO 27001:2017 6.1.1, A9 (Kap. 4.3)	Wie gehen sie z.B. mit Risiken um, welche von Clouddiensten ausgehen? *(Fraunhofer-interne Cloud-Dienste sind vorzuziehen. Für andere Clouddienste muss eine Risikobewertung vorgenommen werden.)*	prozess-orientiert	ja	100%	Es werden die IT-Richtlinien für interne Dokumente genutzt. Daten werden nicht auf private Geräte abgelegt. USB-Sticks (ausgegeben von IT) sind verschlüsselt.
DIN EN ISO 27001:2017 6.1.2	Gibt es einen Prozess zur Informationssicherheitsrisikobeurteilung und wird dieser angewendet? (Standardisierte Abläufe? Gibt es eine Hilfestellung und wird diese genutzt? Hätten sie gerne eine Hilfestellung?)	system-orientiert	teilweise	50%	Es gibt eine Informationssicherheitsrisikobeurteilung von der ZV, welche jedoch noch nicht verwendet wird.
DIN EN ISO 27001:2017 6.1.2	Gibt es ein Bewertungsschema ab welcher Risikohöhe/Risikoart Maßnahmen eingeleitet werden müssen?	system-orientiert	teilweise	50%	Es gibt ein Bewertungsschema, welches jedoch noch nicht genutzt wird.

[98] Eigene Darstellung

Anforderung	Auditfrage	Fragentyp	Erfüllt?	Erfüllungsgrad*	Bemerkung
DIN EN ISO 27001:2017 6.1.1	Wie werden die Risiken und Maßnahmen in den einzelnen Projektphasen dokumentiert? (Projektplanung, -durchführung, -abschluss)	prozess-orientiert	ja	100%	Aktuelle Regelungen zur Risikobewertung gelten im gesamten Projektablauf.
DIN EN ISO 27001:2017 7.2	Wurden sie (Projektleiter/Projektteam) zur Umsetzung von Informationssicherheit/Datenschutz im Projektgeschäft unterrichtet bzw. geschult?	system-orientiert	ja	100%	
DIN EN ISO 27001:2017 10.1	Wie wird mit Nichtkonformitäten umgegangen? Werden Maßnahmen zur Überwachung und Korrektur ergriffen? *(Falsche Dokumentenklassifizierung, nicht sichere Clouddienste, nicht sichere Kommunikation)*	system-orientiert	teilweise	50%	Es ist bekannt, dass es eine Meldeprozedur gibt, aber nicht wie diese Prozedur funktioniert.
DIN EN ISO 27001:2017 10.1	Werden Nichtkonformitäten, dessen Maßnahmen und die Überprüfung der Maßnahmen dokumentiert?	prozess-orientiert	ja	100%	Dokumentation erfolgt über E-Mails.
A5 (Kap. 4.3)	Sind ihnen die drei Schutzklassen und deren Bedeutung für papiergebundene und digitale Informationen bekannt. *(Es gibt 3 Schutzklassen.)*	prozess-orientiert	ja	100%	Schutzklassen sind bekannt und können genannt werden. Schutzklassen sollten jedoch besser an die Projektmitarbeiter kommuniziert werden.
A5 (Kap. 4.3)	Werden die Vorgaben der Organisationsanweisung Informationsklassifizierung kommuniziert und angewendet? *(Kommuniziert an alle im Projekt intern und extern beteiligten Parteien, wie Projektpartner, Kunden, Lieferanten?)*	prozess-orientiert	ja	75%	Schutzklassen werden angewendet jedoch nicht kommuniziert.
DIN EN ISO 27001:2017 8.3	Werden Dokumente im Projektmanagement regelmäßig auf ihre Schutzbedürftigkeit überprüft und ggf. angepasst? *(Austausch mit Kunden, Messdaten, Projektablaufpläne, Kalkulationen, Berichte, etc.)*	prozess-orientiert	ja	100%	Vertrauliche Dokumente werden regelmäßig auf ihre Schutzbedürftigkeit überprüft. Es wird gezielt überprüft, welche Dokumente veröffentlicht werden können.

Anforderung	Auditfrage	Fragentyp	Erfüllt?	Erfüllungsgrad*	Bemerkung
DIN EN ISO 27001:2017 8.3	Welche Unterstützung stellen sie sich für die Umsetzung für Informationssicherheit/Datenschutz im Projektmanagement vor?	-	-	-	Kurzes Informationsblatt mit Fallstricken und Erläuterungen wird gewünscht. Mit klaren Handlungsanweisungen z.B.: Google Cloud soll nicht genutzt werden, Auflistung welche Clouds nicht genutzt werden sollen.

*Kriterien Erfüllungsgrad:

100% Die Anforderung ist vollständig umgesetzt und etabliert oder es existieren noch wenige begründete Ausnahmen oder Sonderfälle.
75% Bis zur vollständigen Umsetzung der Anforderung sind nur noch wenige Schritte erforderlich.
50% Die Umsetzung der Anforderung läuft, bis zur vollständigen Umsetzung sind noch nennenswerte Schritte erforderlich.
25% Die Umsetzung der Anforderung wurde begonnen, bis zur vollständigen Umsetzung sind aber noch erhebliche Schritte erforderlich.
0% Die Umsetzung der Anforderung hat noch nicht begonnen.

Tab. 10: Bereits umgesetzte Anforderungen[99]

Nr.	Anforderung	Umgesetzt ja/nein/teilweise	Bemerkung
A1	Sicherheitsanforderungen von Auftraggebern rechtzeitig erkennen, prüfen und erfüllen	ja	- Deliverable (Vorgaben) in EU Projekten - Sonst Vertragsbedingungen
A2	Informationssicherheits-Risiken bewerten	teilweise	- Risiken werden bewertet aber es wird kein standardisierter Prozess genutzt
A3	Datenschutzrisiken bewerten und ggf. Datenschutzfolgenabschätzung durchführen	teilweise	- Risiken werden bewertet aber es wird kein standardisierter Prozess genutzt
A4	Angemessene Sicherheitsmaßnahmen für genutzte IT treffen	ja	- Es gibt Organisationsanweisungen und ISB steht beratend zur Verfügung
A5	Informationsklassifizierung	ja	- Wird von Projektleitern angewendet, sollte jedoch besser an Projektmitarbeiter kommuniziert werden
A6	Verarbeitungstätigkeiten melden (Verfahrensmeldung)	-	- Keine Informationen aus dem Audit
A7	Rechtsgrundlagen der Datenverarbeitung sicherstellen	-	- Keine Informationen aus dem Audit
A8	Betroffenenrechte sicherstellen	teilweise	- Es werden Schulungen zu Informationssicherheit und Datenschutz durchgeführt
A9	Sorgfältige Auswahl von Web- und Cloud-Diensten und Dienstleistern	ja	- Es finden Schulungen statt und ISB steht für Beratung zur Verfügung

6.2 Stakeholderanalyse

Bei der Durchführung der Stakeholderanalyse wurde die ursprüngliche Vorlage aus dem Modul Projektmanagement an der Hochschule Zittau/Görlitz etwas angepasst. Um leichter Konfliktursachen oder auch Potenziale erkennen zu können, wurde eine Spalte mit den eigenen Interessen und Befürchtungen hinzugefügt. Die angepasste Stakeholderanalyse befindet sich im Anhang (s. Anhang_07_Stakeholderanalyse). Zum Erstellen dieser Analyse wurden auch Ergebnisse aus Audits und zusätzlichen Gesprächen herangezogen.

[99] Eigene Darstellung

Nach der formellen Auswertung sind in jeder Gruppe A, B und C; Stakeholder vertreten (s. Tab. 11). Die Gruppe A umfasst fünf, die Gruppe B neun und die C-Gruppe enthält vier Stakeholder.

Aus dieser Analyse lässt sich ableiten, dass die Interessen der Projektleiter, Institutsleitung, Führungskräfte, Zentralverwaltung und Kunden besondere Beachtung finden müssen. Die Erwartungen der Projektleiter und der Institutsleitung sind, dass das Projektgeschäft in Vorbereitung, Durchführung und Nachbereitung vereinfacht und verbessert wird. Projektleiter möchten kurze Informationen, klare Handlungsanweisungen und keinen Mehraufwand. Eine Befürchtung der Führungskräfte ist, dass mehr Verantwortung und Arbeit, die evtl. nicht bewältigt werden kann auf sie zukommt. Die Fraunhofer Zentralverwaltung erwartet die Umsetzung der von ihr gestellten Anforderungen zur Informationssicherheit und Datenschutz im Projektgeschäft und die Kunden erwarten dies ebenfalls.

Tab. 11: Auswertung Stakeholderanalyse[100]

Stakeholder	Einfluss/Macht	Konfliktpotenzial	Bedeutung	Kategorie
Projektleiter im FEP	3	3	6	A
Institutsleitung	3	3	6	
Führungskräfte	3	3	6	
Zentralverwaltung	3	3	6	
Kunden	3	2	5	
Informations-sicherheits-beauftragter (ISB)	3	1	4	B
Stabsfunktionen (Controlling, UK, Verwaltung, IT, Schutzrechte, …)	2	2	4	
Weitere Beauftragte (EMB, QMB)	2	1	3	
Ämter	3	1	4	
Kooperationspartner	2	2	4	
Mitarbeiter	2	1	3	

[100] Eigene Darstellung

Stakeholder	Einfluss/Macht	Konfliktpotenzial	Bedeutung	Kategorie
Lieferanten	2	1	3	
Versicherungen	2	1	3	
Studenten, Schüler	1	1	2	C
Gäste	1	1	2	
Nachbarn	1	1	2	
Presse	1	1	2	

6.3 Beobachtung

Beobachtungen fanden im gesamten Zeitraum des Aufenthalts am Institut statt. Mit der Methode der Beobachtung, wozu auch Recherche und Gespräche gezählt werden, wurden verschiedene Informationen zur Analyse des ISMS zusammengetragen. D.h., dass die systemorientierten Anforderungen betrachtet wurden. Als Informationsquelle dienten Dokumente, wie Präsentationen, Schulungsunterlagen, Auditunterlagen, Organisationsanweisungen, etc. Die meisten Informationen wurden aus Gesprächen mit den Beauftragten für Informationssicherheit und Qualität zusammengetragen. In Tab. 12 befinden sich die Informationen, welche durch Beobachtungen gewonnen wurden. Diese Tabelle ist ein Ausschnitt aus der Gap-Analyse.

Tab. 12: Beobachtung und Recherche[101]

DIN EN ISO/IEC 27001:2017	Quelle/Art der Information	Erfüllt?	Erfüllungs-grad*	Ergebnis
4.1 – 4.3	Dokumentation	ja	100%	Anforderungen in Kapitel 4 sind von der Fraunhofer Zentralverwaltung erfüllt worden.
4.4	Gespräch mit ISB	teilweise	50%	Das ISMS befindet sich gerade in der Einführung.
5.1	Dokumentation und Gespräche mit ISB	ja	100%	Anforderungen sind weitestgehend umgesetzt.
5.2	Dokumentation	ja	100%	Informationssicherheitspolitik existiert bereits. Und Fraunhofer FEP Politik ist integriertes Dokument, da Ziele für

[101] Eigene Darstellung

DIN EN ISO/IEC 27001:2017	Quelle/Art der Information	Erfüllt?	Erfüllungs-grad*	Ergebnis
				Qualität-, Energie und Informationssicherheit definiert sind.
5.3	Gespräche mit ISB, QMB und Intranet	ja	100%	ISB wurde am Fraunhofer FEP berufen.
6.1.1	Dokumentation und Gespräche mit ISB	ja	75%	Risiken und Chancen werden weitestgehend durch ein systematisches Fraunhofer weites Risikomanagement abgedeckt.
6.1.2	Dokumentation	ja	75%	Vorlage zu Informations-sicherheitsbeurteilung ist vorhanden
6.2	Gespräch mit ISB	teilweise	50%	Es gibt Informationssicherheitsziele, welche jedoch allgemein gehalten sind.
7.1 – 7.5.3	Dokumentation und Gespräche mit ISB	teilweise	50%	Das ISMS befindet sich gerade in der Einführung.
8.1	Dokumentation und Gespräche mit ISB	teilweise	50%	Das ISMS befindet sich gerade in der Einführung aber verschiedene Prozesse wie Informationsklassifizierung, Einweisungsveranstaltungen, ISMS Audits, jährliche Belehrungen/ Auffrischungen sind schon eingeführt.
8.2 – 8.3	Gespräche mit ISB, QMB	teilweise	50%	Informationssicherheitsrisikobeurteilungen werden nur operativ durchgeführt und es gibt keinen Prozess dafür.
9.1	Gespräche mit ISB	nein	0%	Es findet noch keine Überwachung, Messung, Analyse und Bewertung der Informationssicherheitsleistung statt.
9.2	Dokumentation und Gespräche mit ISB, QMB	ja	100%	Informationssicherheitsaudits werden bereits durchgeführt.
9.3	Gespräche mit ISB, QMB	ja	100%	Managementbewertungen werden bereits durchgeführt.
10.1	Gespräche mit ISB	teilweise	50%	Das ISMS befindet sich gerade in der Einführung.
10.2	Gespräche mit ISB	ja	100%	Das ISMS befindet sich gerade in der Einführung.

*Kriterien Erfüllungsgrad:

100% Die Anforderung ist vollständig umgesetzt und etabliert oder es existieren noch wenige begründete Ausnahmen oder Sonderfälle.

75% Bis zur vollständigen Umsetzung der Anforderung sind nur noch wenige Schritte erforderlich.

50% Die Umsetzung der Anforderung läuft, bis zur vollständigen Umsetzung sind noch nennenswerte Schritte erforderlich.

25% Die Umsetzung der Anforderung wurde begonnen, bis zur vollständigen Umsetzung sind aber noch erhebliche Schritte erforderlich.

0% Die Umsetzung der Anforderung hat noch nicht begonnen.

6.4 Gap-Analyse

Mithilfe der Gap-Analyse wird das Informationssicherheitsmanagementsystem am Fraunhofer FEP Analysiert (s. Anhang_08_GAP-Analyse). Die Gap-Analyse ist das finale Analyseinstrument, um festzustellen welche Anforderungen an das Managementsystem umgesetzt sind und welche nicht. Um daraus schlussfolgern zu können, wo Maßnahmen ergriffen werden müssen, um mögliche die Lücken zu schließen. Wie in Abb. 16 zu erkennen ist, sind in der Spalte ganz links die Soll-Zustände eingetragen. Diese Soll-Zustände sind von den Anforderungen der DIN EN ISO/IEC 27001:2017 abgeleitet. In der nächsten Spalte wird der Ist-Zustand abgefragt. Hier wird eingetragen ob die Anforderungen erfüllt, nicht erfüllt, teilweise erfüllt oder nicht anwendbar sind. Grundlage des Ist-Zustands bilden die durchgeführten Beobachtungen und Audits. Des Weiteren sind der Erfüllungsgrad, Bemerkungen, eine Datenquelle, Verantwortliche und zweckmäßige Dokumente ergänzt.

Abb. 16: Ausschnitt Gap-Analyse[102]

GAP-Analyse zu den Anforderungen zur EN ISO 27001:2017							
Anforderungen der DIN EN ISO 27001:2017	erfüllt?	Erfüllungsgrad	Integrationsgrad	Bemerkung	Datenquelle	Prozess / Verantwortliche	zwecl Doku
Einleitung							
1 Anwendungsbereich							
2 Normative Verweisungen							
3 Begriffe							
4 Kontext der Organisation							
4.1 Verstehen der Organisation und ihres Kontextes							
Hat die Organisation externe und interne Themen bestimmt?							
Sind diese für ihren Zweck relevant?							
Wirken sich diese auf ihre Fähigkeit aus, die beabsichtigten Ergebnisse ihres ISMS zu erreichen?							
4.2 Verstehen der Erfordernisse und Erwartungen Interessierter Parteien							
a) Wurden Interessierte Parteien, die für das ISMS relevant sind bestimmt?							
b) Wurden die Anforderungen dieser interessierten Parteien mit Bezug zur Informationssicherheit bestimmt?							
4.3 Festlegen des Anwendungsbereichs des ISMS							
Sind die Grenzen und die Anwendbarkeit des ISMS bestimmt, um dessen Anwendungsbereich festzulegen?							
Wurden bei der Festlegung des Anwendungsbereiches:							
a) die externen und internen Themen,							

6.5 Maßnahmen

Als Ergebnis der vorhergehenden Analysen ist ein Maßnahmenkatalog mit 16 Maßnahmen entstanden (s. Tab. 13) Neben der Nichtkonformität und der Angabe des

[102] Eigene Darstellung

entsprechenden Kapitels in der Norm ist die Maßnahme beschrieben und das zu erwartende Ergebnis notiert. Für eine bessere Übersichtlichkeit wurden die Maßnahmen in Kommunikation, Dokumentation und Prozess kategorisiert. Ein weiterer Vorteil dieser Kategorisierung liegt darin, dass Gemeinsamkeiten bei der Umsetzung der Maßnahmen erkannt werden können. Hier z.B. ist deutlich, dass die Maßnahmen, die zur Kommunikation zählen gleichzeitig mit dem Einführen einer Intranetseite zur Informationssicherheit umgesetzt werden können. Um eine Reihenfolge zur Umsetzung der Maßnahmen festlegen zu können, werden die Maßnahmen zusätzlich auf Dringlichkeit und Umsetzbarkeit bewertet. Aus den beiden Kriterien wird die Priorität ermittelt. Dabei gilt, je niedriger die Punktzahl, desto höher die Priorität.

Festlegung des Dringlichkeitsgrades

Zur Festlegung der Dringlichkeit bieten sich zwei Kriterien an. Zum einen das geplante Datum an denen die Maßnahme spätestens umgesetzt werden soll und zum anderen inwieweit die Maßnahme dazu beiträgt, die neuen Anforderungen der Fraunhofer Zentralverwaltung aus Kap. 4.3 im Projektgeschäft umzusetzen.

Spätestens mit dem Fertigstellen der Masterarbeit, sollen die Maßnahmen umgesetzt sein. D.h., dass für alle Maßnahmen die gleiche Frist gilt. Demnach ist das Kriterium der Terminierung für alle Maßnahmen gleich und wird zur Bildung der Priorität ausgeklammert. Zur Umsetzung der neuen Anforderungen im Projektgeschäft dienen in erster Linie die prozessorientierten Maßnahmen. Die systemorientierten Maßnahmen bilden die Grundstruktur der Prozesse, um das System lebensfähig und nachhaltig zu gestalten. Eine prozessorientierte Maßnahme ist demnach dringlicher einzustufen als eine systemorientierte. Folgend werden die prozessorientierten Maßnahmen mit einem (höhere Priorität) und die systemorientierten Maßnahmen mit zwei Punkten (niedrigere Priorität) bewertet.

Festlegung der Umsetzbarkeit

Die Umsetzbarkeit wird daran festgelegt, wie viele Bereiche des Fraunhofer-Instituts hinzugezogen werden müssen, um die Maßnahme umsetzen zu können. Das können z.B. Informationssicherheit, Qualität, IT, oberste Leitung oder Beschaffung sein. Die

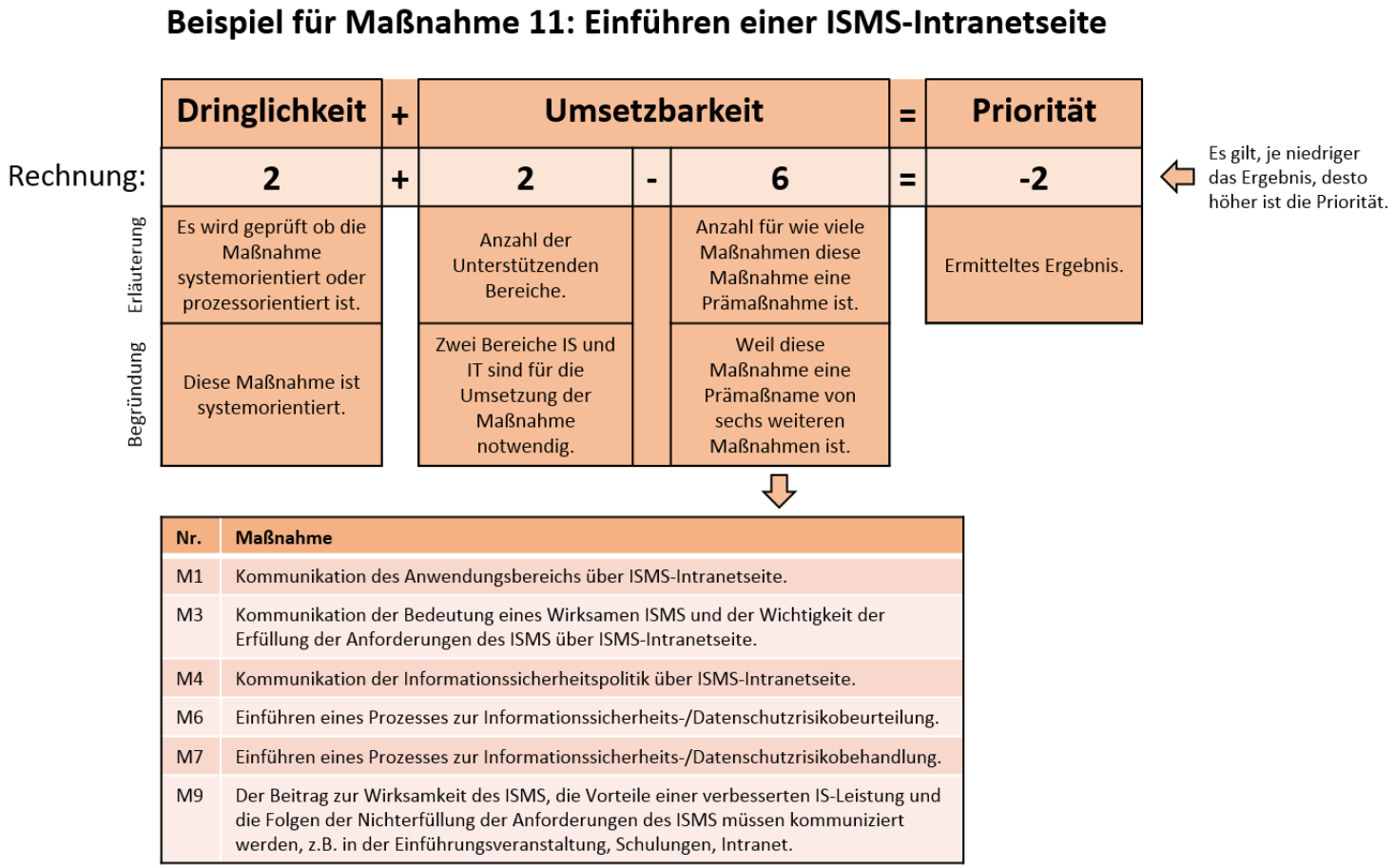
Punktzahl ist die Summe aus der Anzahl der benötigten Bereiche. Bei der Erstellung der Informationssicherheits-Intranetseite werden z.B. die Bereiche Informationssicherheit und die IT benötigt. Daraus ergibt sich eine Punktzahl von zwei.

Bei der Festlegung der Umsetzbarkeit können zwei Sonderfälle auftreten, die wie folgt behandelt werden. Ist die Anzahl der Bereiche, die bei der Umsetzung einer Maßnahme hinzugezogen werden müssen, besonders hoch, dann werden grundsätzlich 5 Punkte vergeben. Und zweitens, ist zum Umsetzen einer Maßnahme die Umsetzung einer oder mehrerer vorherigen Maßnahmen (Prämaßnahme) notwendig, dann wird die Punktzahl der Prämaßnahme mit der Anzahl der Maßnahmen, die diese Maßnahme voraussetzen subtrahiert.

Berechnungsbeispiel

Als Beispiel wird die Ermittlung der Priorität an Maßnahme 11 gezeigt. Das Einführen einer ISMS-Intranetseite ist eine systemorientierte Maßnahme. Damit wird für die Dringlichkeit die Punktzahl zwei vergeben. Zur Realisierung werden zwei Bereiche benötigt. Die Informationssicherheit in Form des ISB und die IT zur Bereitstellung und Freischaltung der Intranetseite. Demnach wird ein Wert von zwei addiert. Zum Schluss wird überprüft, ob diese Maßnahme eine Prämaßnahme ist. Maßnahme 11 ist eine Prämaßnahme von 6 weiteren Maßnahmen. In Abb. 17 ist das Beispiel Übersichtlich dargestellt.

Abb. 17: Berechnungsbeispiel zur Priorisierung der Maßnahmen[103]



[103] Eigene Darstellung

Tab. 13: Maßnahmenkatalog[104]

Nr.	Anforderung/ Nichtkonformität	ISO 27001 Kapitel	Beschreibung der Maßnahme	Ergebnis	Verantwortliche	Kategorie*	Art der Umsetzung	Dringlichkeit	Umsetzbarkeit (Bereiche – Prämaßnahmen von = Differenz)			Priorität
									Bereiche	*Prämaß-nahme von*	Differenz	
1	Der Anwendungsbereich des ISMS muss verfügbar sein für interessierte Parteien.	4.3	Kommunikation des Anwendungsbereichs über ISMS- Intranetseite.	ISMS-Intranetseite mit Information zum Anwendungsbereich	ISB, Autor der Masterarbeit	K	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
2	Das ISMS muss aufgebaut, verwirklicht, aufrechterhalten und fortlaufend verbessert werden.	4.4	Aufbau und Verwirklichung: Vollständige Einführung des ISMS in das Projektgeschäft und die unterstützenden Prozesse des FEP.	Integriertes Informationssicherheits managementsystem	ISB, Autor der Masterarbeit	P	System-orientiert	2	*5 (un-bekannt)*	*0*	5	7
3	Die Bedeutung eines wirksamen ISMS sowie die Wichtigkeit der Erfüllung der Anforderungen des ISMS muss vermittelt werden.	5.1	Kommunikation der Bedeutung eines Wirksamen ISMS und der Wichtigkeit der Erfüllung der Anforderungen des ISMS über ISMS-Intranetseite.	Intranetseite mit Information zur Bedeutung eines Wirksamen ISMS und der Wichtigkeit der Erfüllung der Anforderungen des ISMS	ISB, Autor der Masterarbeit	K	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
4	Die Informationssicherheitspolitik muss innerhalb des FEP kommuniziert werden.	5.2	Kommunikation der Informationssicherheitspolitik über ISMS-Intranetseite.	Intranetseite mit Informationspolitik	ISB, Autor der Masterarbeit	K	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2

[104] Eigene Darstellung

Nr.	Anforderung/ Nichtkonformität	ISO 27001 Kapitel	Beschreibung der Maßnahme	Ergebnis	Verantwortliche	Kategorie*	Art der Umsetzung	Dringlichkeit	Umsetzbarkeit (Bereiche – Prämaßnahmen von = Differenz)			Priorität
									Bereiche	*Prämaß-nahme von*	Differenz	
5	Risiken und Chancen müssen regelmäßig überprüft werden.	6.1.1	Einführung eines Prozesses zur regelmäßigen Überprüfung von Risiken und Chancen im ISMS.	Eintrag in den ISMS-Kalender, in dem daran erinnert wird, Risiken und Chancen regelmäßig zu betrachten.	ISB, Autor der Masterarbeit	P	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
6	Es muss ein Prozess zur Informationssicherheitsrisikobeurteilung / Datenschutzrisikobeurteilung in Projekten eingeführt werden.	6.1.2 u. 8.2	Auf PM-Intranetseite wird die Informationssicherheitsrisikobeurteilung / Datenschutzrisikobeurteilung in der Projektanbahnung thematisiert. Auf der ISMS-Intranetseite wird diese Beurteilung bereitgestellt.	Informationssicherheitsrisikobeurteilung ist kommuniziert und für Projektleiter bereitgestellt.	ISB, Autor der Masterarbeit	P	Prozess-orientiert (A2, A3)	1	*2 (IS, Projekte)*	*0*	2	3
7	Es muss ein Prozess zur Informationssicherheitsrisiko- / Datenschutzrisikobehandlung in Projekten eingeführt werden.	6.1.3 u. 8.2	Da die Informationssicherheitsrisiko- / Datenschutzrisikobeurteilung eine Risikobehandlung enthält, wird mit Maßnahme 6 gleichzeitig Maßnahme 7 umgesetzt.	Anwendbarer Prozess	ISB, Autor der Masterarbeit	P	Prozess-orientiert (A4, A8, A9)	1	*2 (IS, Projekte)*	*0*	2	3
8	Es müssen Informationssicherheitsziele für relevante Funktionen und Ebenen festgelegt werden.	6.2	Erstellen eines Zielkataloges, welcher als dokumentierte Information gilt.	ISMS-Zielkatalog	ISB, Autor der Masterarbeit	D	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2

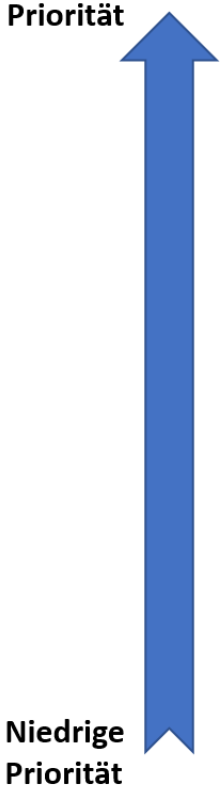
Nr.	Anforderung/ Nichtkonformität	ISO 27001 Kapitel	Beschreibung der Maßnahme	Ergebnis	Verantwortliche	Kategorie*	Art der Umsetzung	Dringlichkeit	Umsetzbarkeit (Bereiche – Prämaßnahmen von = Differenz)			Priorität
									Bereiche	*Prämaß-nahme von*	Differenz	
9	PL und MA müssen sich über die - ihren Beitrag zur Wirksamkeit des ISMS - der Vorteile einer verbesserten IS-Leistung und - über die Folgen der Nichterfüllung der Anforderungen des ISMS bewusst sein.	7.3	Der Beitrag zur Wirksamkeit des ISMS, die Vorteile einer verbesserten IS-Leistung und die Folgen der Nichterfüllung der Anforderungen des ISMS müssen kommuniziert werden, z.B. in der Einführungsveranstaltung, Schulungen, Intranet.	Information über ISMS-Intranetseite	ISB, Autor der Masterarbeit	K	System-orientiert	2	*2 (IS, Projekte)*	*1 (M2)*	1	3
10	Die interne und externe Kommunikation in Bezug auf das ISMS muss bestimmt werden; einschließlich worüber, wann, mit wem und wer.	7.4	Erstellen einer Kommunikationsmatrix mit den geforderten Inhalten.	Kommunikationsmatrix	Autor der Masterarbeit	D	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
11	Ein Prozess zur Bewerkstelligung der Kommunikation muss etabliert werden.	7.4	Einführung einer ISMS-Intranetseite	funktionstüchtige ISMS-Intranetseite	ISB, Autor der Masterarbeit	P	System-orientiert	2	*2 (IS, IT)*	*6 (M1, M3, M4, M6, M7 M9)*	-4	-2
12	Die für das ISMS erforderliche und von der internationalen Norm geforderte dokumentierte Informationen müssen gelenkt werden.	7.5.3	Es muss ein Prozess zur Dokumentenlenkung eingeführt werden.	Dokumentenlenkungs-prozess	ISB	P	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2

Nr.	Anforderung/ Nichtkonformität	ISO 27001 Kapitel	Beschreibung der Maßnahme	Ergebnis	Verantwortliche	Kategorie*	Art der Umsetzung	Dringlichkeit	Umsetzbarkeit (Bereiche – Prämaßnahmen von = Differenz)			Priorität
									Bereiche	*Prämaß-nahme von*	Differenz	
13	Geplante und ungeplante Änderungen müssen beurteilt und ggf. Maßnahmen ergriffen werden um, um jegliche negativen Auswirkungen zu vermindern.	8.1	Bei geplanten und ungeplanten Änderungen müssen ggf. mittels Risiken und Chancenkataloges, für den bestimmten Bereich, Maßnahmen abgeleitet, bewertet und evtl. angepasst werden.	Eintrag in den ISMS-Kalender indem Risiken und Chancen regelmäßig betrachtet werden, wenn Änderungen eintreten.	Autor der Masterar beit	P	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
14	Ausgegliederte Prozesse müssen bestimmt und gesteuert werden.	8.1	Ausgegliederte Prozesse müssen bestimmt und entsprechend gesteuert (Chancen- und Risikobetrachtung, ggf. Prozessanpassungen, Schulungen, etc.) werden.	Ausgegliederte Prozesse sind in Bezug zur Informationssicherheit und Datenschutz betrachtet worden. Eintrag in ISMS-Kalender.	ISB, Autor der Masterar beit	P	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
15	Der Umgang mit Nichtkonformitäten muss geklärt werden.	10.1	Ein Prozess zum Umgang mit Nichtkonformitäten muss erstellt werden. Der Prozess muss eingeführt und angewandt werden.	Erweitertes Ticketsystem	ISB	P	System-orientiert	2	*1 (IS)*	*1 (M2)*	0	2
16	Die Eignung Angemessenheit und Wirksamkeit des ISMS muss fortlaufend verbessert werden.	10.1	Erstellen einer Checkliste, welche zeigt in welchen Abständen Überprüfungen / Aktualisierungen stattfinden müssen, um den KVP voranzutreiben.	ISMS-Kalender	Autor der Masterar beit	P	System-orientiert	2	*5 (un-bekannt)*	*3 (M2, M5, M13)*	2	4

*D = Dokumentation, K = Kommunikation, P = Prozess

Nach der Ermittlung der Priorität, ist folgende Reihenfolge zur Umsetzung gem. den Maßnahmen aus Tab. 13 entstanden. Diese Reihenfolge richtet sich absteigend nach der Priorität, Kategorie und dem entsprechenden Normkapitel.

Abb. 18: Maßnahmenpriorisierung[105]



Priorität	Kategorie*	Kapitel ISO 27001	Maßnahme
-2	P	7.4	Einführung einer ISMS-Intranetseite, zur Bewerkstelligung der Kommunikation.
2	D	6.2	Erstellen eines Zielkatalogs.
2	D	7.4	Erstellen einer Kommunikationsmatrix.
2	K	4.3	Kommunikation des Anwendungsbereichs über ISMS-Intranetseite.
2	K	5.1	Kommunikation der Bedeutung eines Wirksamen ISMS und der Wichtigkeit der Erfüllung der Anforderungen des ISMS über ISMS-Intranetseite.
2	K	5.2	Kommunikation der Informationssicherheitspolitik über ISMS-Intranetseite.
2	P	6.1.1	Einführung eines Prozesses zur regelmäßigen Überprüfung von Risiken und Chancen im ISMS.
2	P	7.5.3	Einführen eines Prozesses zur Dokumentenlenkung.
2	P	8.1 c	Einführen eines Prozesses zur Beurteilung von Änderungen.
2	P	8.1 d	Bestimmen und Steuern von ausgegliederten Prozessen.
2	P	10.1	Einführung eines Prozesses zum Umgang mit Nichtkonformitäten.
3	K	7.3	Der Beitrag zur Wirksamkeit des ISMS, die Vorteile einer verbesserten IS-Leistung und die Folgen der Nichterfüllung der Anforderungen des ISMS müssen kommuniziert werden.
3	P	6.1.2 u. 8.2	Einführung eines Prozesses zur Informationssicherheits-/Datanschutzrisikobeurteilung.
3	P	6.1.3 u. 8.2	Einführung eines Prozesses zur Informationssicherheits-/Datanschutzrisikobehandlung.
4	P	10.1	Die Eignung Angemessenheit und Wirksamkeit des ISMS muss fortlaufend verbessert werden.
7	P	4.4	Vollständige Einführung des ISMS in das Projektgeschäft und die unterstützenden Prozesse des FEP.

*D = Dokumentation, K = Kommunikation, P = Prozess

[105] Eigene Darstellung

7 Integration der neuen Anforderungen

7.1 Verbesserung des Projektmanagements

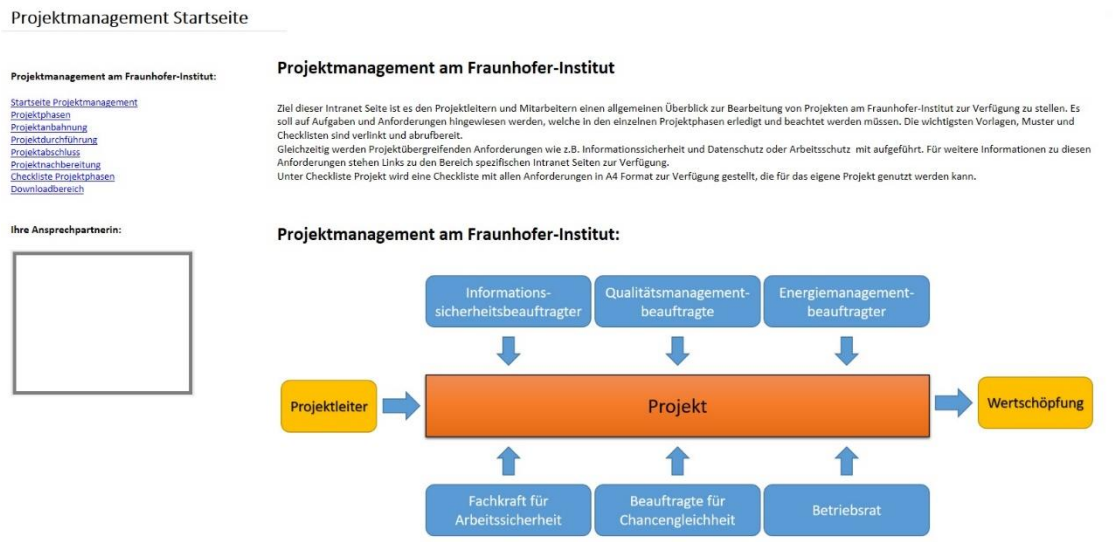
Wie in Kapitel 4.2 beschrieben muss vor der Umsetzung der entwickelten Maßnahmen und der damit einhergehenden Implementierung der neuen Anforderungen, das Projektmanagement am Fraunhofer FEP verbessert werden. Um die in Kapitel 4.2 genannten Verbesserungsmöglichkeiten umzusetzen, wurde eine Intranetseite für das Projektmanagement entwickelt. Die Intranetseite ist in Zusammenarbeit mit den Beauftragten für Qualität und Informationssicherheit und der IT-Abteilung des Fraunhofer FEP entstanden (s. Abb. 19).

Folgende Vorteile bietet das Einführen der Intranetseite für Projektmanagement:

- Es wird ein umfassender Überblick der Phasen und der einzelnen Schritte des Projektmanagements zur Verfügung gestellt.
- Die Anforderungen aller Managementsysteme / Bereiche sind auf einem Blick zusammengefasst. Über einen Link sind die jeweiligen Intranetseiten (Qualität, Energie, Informationssicherheit, Arbeitsschutz) erreichbar (integrierte Kommunikation).
- Durch die Verlinkung zu den einzelnen Bereichen, bleibt die Verantwortung der Inhalte bei den jeweiligen Beauftragten. Somit entsteht kein Mehraufwand für Eintrag, Pflege und Verantwortung.
- Es werden nur die wichtigsten Dinge angezeigt, um Komplexität zu verringern und Übersichtlichkeit zu gewährleisten.
- Bei zukünftigen Veränderungen oder neuen Anforderungen können diese einfach implementiert werden.

Mit dem Einführen dieser Intranetseite soll die Wirksamkeit der Integration der neuen Anforderungen zu Informationssicherheit und Datenschutz erhöht werden. Zusätzlich wurde eine integrierte Risikobewertung vom Autor der Arbeit entwickelt, die den Projektleitern in Zukunft über die PM-Intranetseite zur Verfügung gestellt wird. Die Risikobewertung ist im Anhang zu finden (s. Anhang_09_Integrierte_Risikobewertung).

Abb. 19: PM-Intranetseite

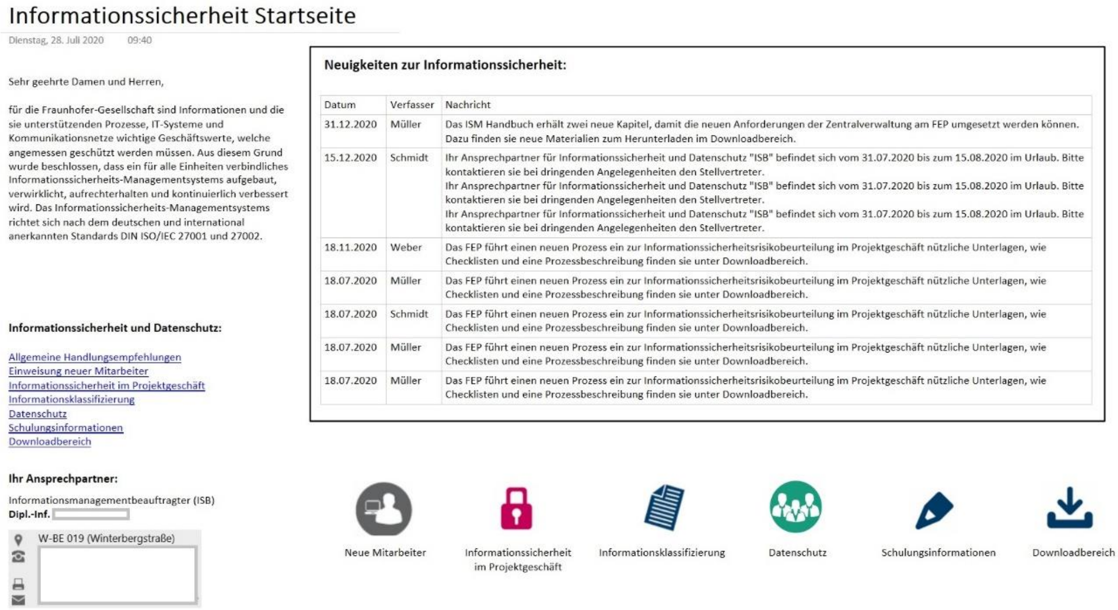


7.2 Umsetzung der Maßnahmen zur Einführung eines ISMS und Integration der neuen Anforderungen

Intranetseite Informationssicherheitsmanagement

Eine Möglichkeit zur Kommunikation im Fraunhofer FEP bietet das Intranet. Im integrierten Managementsystem wird diese Form der Kommunikation bereits für das Qualitäts- und Energiemanagement genutzt. Um den Kommunikationsprozess für das ISMS zu etablieren (M11) bietet es sich deshalb an diese Methode zu übernehmen (Simplicity-Methode: „Konzepte übertragen“). Abb. 20 zeigt die Startseite einer entwickelten ISMS-Intranetseite. Die Startseite enthält einen Einführungstext zur Notwendigkeit eines ISMS und dessen Vorteilen, die Kontaktinformationen des ISB und ein Feld mit Neuigkeiten, wo aktuelle Themen und Informationen zum ISMS zur Verfügung gestellt werden. Zusätzlich gibt es eine Linkspalte zu weiteren Inhalten wie allgemeine Handlungsempfehlungen, Einweisung neuer Mitarbeiter, Informationssicherheit im Projektgeschäft, Informationsklassifizierung, Datenschutz, Schulungsinformationen sowie einen Downloadbereich.

Abb. 20: ISMS-Intranetseite[106]



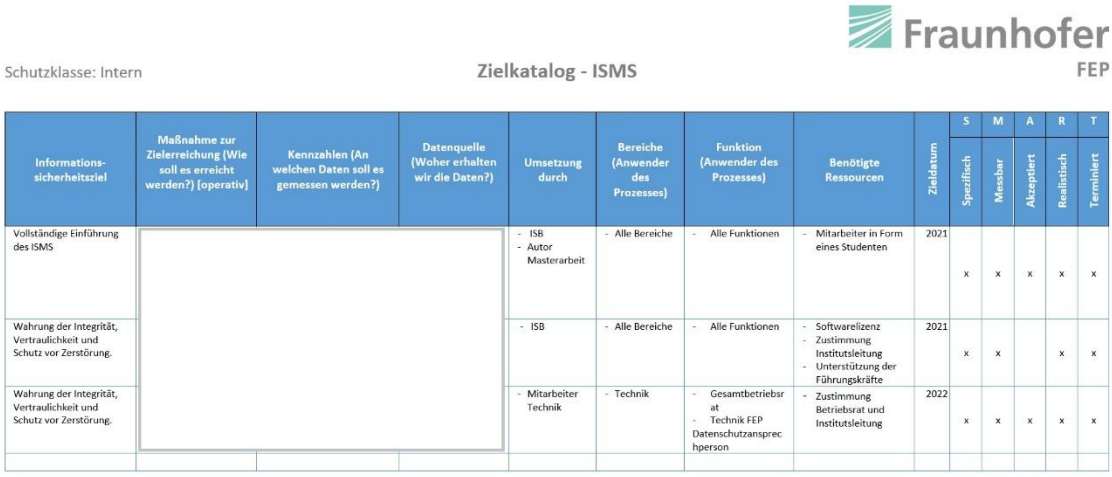
Zielkatalog

Um Maßnahme 8 umzusetzen wurde ein Zielkatalog erstellt (s. Anhang_10_Zielkatalog_ISMS). In diesem Katalog sind Informationssicherheitsziele für relevante Funktionen und Ebenen festgelegt worden. Der Katalog ist eine dokumentierte Information. Dieses Dokument entspricht allen notwendigen Anforderungen an dokumentierten Informationen, wie Schutzklasse, Verantwortlichkeiten, letzte Änderung, etc. Des Weiteren wurde am Ende des Dokuments ein Abkürzungsverzeichnis eingefügt, um neuen Mitarbeitern oder Studenten die Arbeit mit diesem Dokument zu erleichtern. Aus Informations- und Datenschutzgründen wurden einige Bereiche in Abb. 21 abgedeckt.

---

[106] Eigene Darstellung

Abb. 21: Auszug Zielkatalog[107]



Schutzklasse: Intern

Zielkatalog - ISMS

Fraunhofer FEP

Informations-sicherheitsziel	Maßnahme zur Zielerreichung (Wie soll es erreicht werden?) [operativ]	Kennzahlen (An welchen Daten soll es gemessen werden?)	Datenquelle (Woher erhalten wir die Daten?)	Umsetzung durch	Bereiche (Anwender des Prozesses)	Funktion (Anwender des Prozesses)	Benötigte Ressourcen	Zieldatum	S	M	A	R	T
									Spezifisch	Messbar	Akzeptiert	Realistisch	Terminiert
Vollständige Einführung des ISMS				- ISB - Autor Masterarbeit	- Alle Bereiche	- Alle Funktionen	- Mitarbeiter in Form eines Studenten	2021	x	x	x	x	x
Wahrung der Integrität, Vertraulichkeit und Schutz vor Zerstörung.				- ISB	- Alle Bereiche	- Alle Funktionen	- Softwarelizenz - Zustimmung Institutsleitung - Unterstützung der Führungskräfte	2021	x	x		x	x
Wahrung der Integrität, Vertraulichkeit und Schutz vor Zerstörung.				- Mitarbeiter Technik	- Technik	- Gesamtbetriebsrat - Technik FEP Datenschutzansprechperson	- Zustimmung Betriebsrat und Institutsleitung	2022	x	x	x	x	x

Kommunikation

Mit dem Einführen der Intranetseite zur Informationssicherheit sind vier Maßnahmen, die das ISMS betreffen gleichzeitig mit umgesetzt. Auf dieser ISMS-Intranetseite sind die Informationen,

- zum Anwendungsbereich des ISMS (M1),
- die Bedeutung eines wirksamen ISMS sowie die Wichtigkeit der Erfüllung der Anforderungen des ISMS (M3),
- die Informationssicherheitspolitik (M4) sowie
- der Vorteile einer verbesserten IS-Leistung (M9)

kommuniziert.

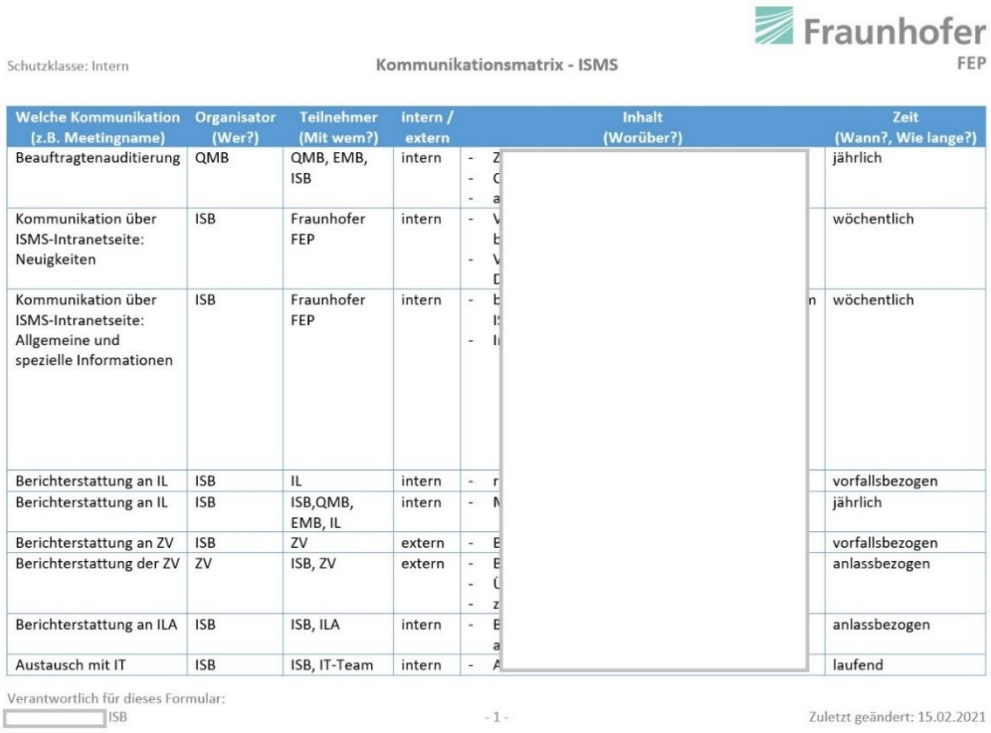
Kommunikationsmatrix

Inhalt der Maßnahme 10 ist es eine Kommunikationsmatrix zu erstellen. In dieser Matrix ist ersichtlich wie intern und extern, worüber, wann, wer und mit wem kommuniziert wird. Abb. 22 zeigt einen Auszug aus der erstellten Kommunikationsmatrix. Dieses Dokument entspricht allen notwendigen Anforderungen an dokumentierten Informationen, wie Schutzklasse, Verantwortlichkeiten, letzte Änderung, etc. Des Weiteren wurde am Ende

[107] Eigene Darstellung

des Dokuments ein Abkürzungsverzeichnis eingefügt, um neuen Mitarbeitern oder Studenten die Arbeit mit diesem Dokument zu erleichtern. Aus Informations- und Datenschutzgründen wurden einige Bereiche in der Abbildung abgedeckt. Die Vollständige Kommunikationsmatrix befindet sich im Anhang (s. Anhang_11_Kommunikationsmatrix_ISMS).

Abb. 22: Auszug Kommunikationsmatrix[108]



Fraunhofer FEP

Schutzklasse: Intern

Kommunikationsmatrix - ISMS

Welche Kommunikation (z.B. Meetingname)	Organisator (Wer?)	Teilnehmer (Mit wem?)	intern / extern	Inhalt (Worüber?)	Zeit (Wann?, Wie lange?)
Beauftragtenauditierung	QMB	QMB, EMB, ISB	intern	- Z - C - a	jährlich
Kommunikation über ISMS-Intranetseite: Neuigkeiten	ISB	Fraunhofer FEP	intern	- V - V	wöchentlich
Kommunikation über ISMS-Intranetseite: Allgemeine und spezielle Informationen	ISB	Fraunhofer FEP	intern	- B - I	wöchentlich
Berichterstattung an IL	ISB	IL	intern	- r	vorfallsbezogen
Berichterstattung an IL	ISB	ISB,QMB, EMB, IL	intern	- M	jährlich
Berichterstattung an ZV	ISB	ZV	extern	- B	vorfallsbezogen
Berichterstattung der ZV	ZV	ISB, ZV	extern	- B - Ü - z	anlassbezogen
Berichterstattung an ILA	ISB	ISB, ILA	intern	- B a	anlassbezogen
Austausch mit IT	ISB	ISB, IT-Team	intern	- A	laufend

Verantwortlich für dieses Formular:
ISB

- 1 -

Zuletzt geändert: 15.02.2021

Prozess zur regelmäßigen Überprüfung von Risiken und Chancen im ISMS

Die Umsetzung des Prozesses zur regelmäßigen Überprüfung von Risiken und Chancen im ISMS (M5) wird umgesetzt indem in dem erstellten ISMS Kalender (M16) ein Eintrag hinzugefügt wird die Risiken und Chancen des ISMS regelmäßig zu überprüfen.

Prozess zur Dokumentenlenkung

Die Umsetzung des Prozesses zur Dokumentenlenkung (M12) wird vom ISB des Fraunhofer FEP durchgeführt. Es ist geplant die Software „Verinice“ einzusetzen.

[108] Eigene Darstellung

Prozess zur Beurteilung von Änderungen

Um den Prozess zur Beurteilung von Änderungen (M13) umzusetzen wird ein Eintrag in den ISMS-Kalender hinzugefügt, welcher mit Maßnahme 16 entwickelt wird. So ist gewährleistet, dass die Beurteilung von Änderungen regelmäßig durchgeführt und nicht vergessen wird.

Prozess zum Bestimmen und Steuern von ausgegliederten Prozessen

Um einen Prozess zum Bestimmen und Steuern von ausgegliederten Prozessen einzuführen (M14), wurde ein Dokument erstellt, in dem Ausgegliederte Prozesse bestimmt und mögliche Maßnahmen zur Steuerung dokumentiert werden (s. Anhang_12_Ausgegliederte_Prozesse_ISMS). Mit dem Eintrag in den ISMS-Kalender zur regelmäßigen Aktualisierung, ist der Prozess etabliert.

Prozess zum Umgang mit Nichtkonformitäten

Um den Prozess zum Umgang mit Nichtkonformitäten (M15) umzusetzen, ist geplant das Fraunhofer interne Ticketsystem zu erweitern. Diese Erweiterung wird vom ISB des Fraunhofer FEP durchgeführt.

Einführen eines Prozesses zur Informationssicherheits- / Datenschutzrisiko-beurteilung

Um den Prozess zur Informationssicherheits- / Datenschutzrisikobeurteilung (M6) einzuführen, wird die bereits erstellte ISMS-Intranetseite genutzt. Auf der ISMS-Intranetseite ist die Informationssicherheitsrisikobeurteilung / Datenschutzrisikobeurteilung kommuniziert und wird dem Projektleiter zur Verfügung gestellt.

Einführen eines Prozesses zur Informationssicherheits- / Datenschutzrisiko-behandlung

Mit dem Umsetzen von Maßnahme 6 wird gleichzeitig diese Maßnahme umgesetzt, da das vorgegebene Dokument von der Fraunhofer Zentralverwaltung auch eine

Risikobehandlung enthält. Hierbei wird eine wie in Kap. 3.4 beschriebene Simplicity-Methode zur Reduzierung der Komplexität verwendet, die Methode „Nutzen erhöhen“.

Fortlaufende Verbesserung

Die Maßnahme 16 dient dem Zweck den KVP regelmäßig voranzutreiben. Ein entwickelter Kalender, mit Einträgen und Erinnerungen in welchen Abständen bestimmte Überprüfungen und Aktualisierungen bezüglich des ISMS vorzunehmen sind, ist das Ergebnis dieser Maßnahme (s. Abb. 23). Der ISB wird dadurch regelmäßig angehalten eine strukturierte Kontrolle durchzuführen. Der Vorteil dieser Checkliste ist nicht nur, dass keine Punkte vergessen werden, sondern auch, dass Einträge beliebig angepasst, ergänzt, oder entfernt werden können (s. Anhang_13_Kalender_ISMS).

Abb. 23: ISMS-Kalender[109]

ISMS - Kalender

Schutzklasse: intern - nicht für die Öffentlichkeit bestimmt

Aktualisierung /Überprüfung	In welchem Abstand?	Überprüfun am	Überprüfung durchgeführt
Neuigkeiten im Intranet Kommunizieren			
Iaktualität der Intranetseite Überprüfen			
Überprüfung von Risiken und Chancen im ISMS			
- Beurteilung von Änderungen im ISMS			
Kommuikationsmatrix aktualisieren			
Zielkatalog aktualisieren			
Schulungsunterlagen aktualisieren			
Bestimmen ausgegliederter Prozesse			
Weitere Aufgaben			
Weitere Aufgaben			

7.3 Wirksamkeitsbewertung und Ausblick hinsichtlich der Einführung von SAP

Zur Bewertung der Wirksamkeit, sollten mindestens die zwei folgenden Verfahren genutzt werden. Der erste Weg ist ein aktives Zugehen des ISB auf die Projektleiter. Der ISB sollte das Gespräch suchen, um in Erfahrung zu bringen inwieweit die neuen

[109] Eigene Darstellung

Anforderungen im Projektgeschäft umgesetzt und akzeptiert werden. Hierbei besteht die Chance, frühzeitig bestehende Lücken oder mögliche Verbesserungsvorschläge in Erfahrung bringen zu können. Das aktive Zugehen auf die Projektleiter bringt einen weiteren Vorteil. Wie in Kap. 3 beschrieben, ist ein (integriertes) Managementsystem auch ein soziales System. Kommuniziert der ISB Auge zu Auge mit den Projektleitern, besteht die Chance, die soziale Zufriedenheit zu erhöhen. Wenn die Projektleiter das Gefühl haben gehört und ernst genommen zu werden, ist es wahrscheinlicher, dass die neuen Anforderungen akzeptiert und im Projektgeschäft umgesetzt werden.

Der zweite Weg zur Bewertung der Wirksamkeit, ist die Nutzung der nächsten regulären internen Audits. Dazu sollten Auditfragen entwickelt werden, welche sowohl die Integration der neuen Anforderungen überprüfen, als auch die Zufriedenheit der Projektleiter mit den neu implementierten Anforderungen ermittelt.

Eine weiteres Mittel, welches ins Auge gefasst werden kann, ist die Anwendung der in Kap. 2.3.3 vorgestellten Prüfmatrix (s. Anhang_02_Integrierte_Prüfmatrix). Mit dieser Matrix kann kontrolliert werden, ob die Prozesse nach der Integration, den neuen Anforderungen aus Kap. 4.3 gerecht werden. Das Anwenden und Testen der Prüfmatrix ist aufgrund des Umfangs nicht Gegenstand der Arbeit, kann aber als Möglichkeit zur Wirksamkeitsbewertung Betracht gezogen werden.

Es ist geplant, dass im Jahr 2022 die Software SAP zum Einsatz kommen soll. Diese Software dient zur Abwicklung von Geschäftsprozessen. Wenn die Software eingeführt wird und sich neue Anforderungen ergeben, dann kann der in Kap. 8 entwickelte Leitfaden genutzt werden. In diesem Fall, muss je nach Umfang der neuen Anforderungen, entschieden werden, ob der Leitfaden ausreichend ist oder ggf. weitere Schritte durchgeführt werden müssen.

8 Leitfaden zur Integration neuer Anforderungen

8.1 Entwicklung des Leitfadens

Der Leitfaden zur Integration neuer Anforderung, soll das nachhaltige Element dieser Arbeit sein. Bevor der Aufbau entwickelt wird, sind im folgenden wichtige Ziele des Leitfadens zusammengetragen:

- Der Leitfaden dient als Allgemeine Handlungsempfehlung zum Integrieren neuer Anforderungen.
- Es wird ein Methodenbaukasten für Vorbetrachtungen und zur Analyse des Systems bzw. Prozesses vorgegeben.
- Es soll gleichzeitig als Ablaufprotokoll dienen können, indem das Eintragen von Notizen und Bemerkungen möglich ist.
- Eine Checklistenfunktion soll enthalten sein.
- Kurzer, kompakter und aussagekräftiger Aufbau.

Der Aufbau des Leitfadens gliedert sich in fünf Phasen. In der ersten Phase, sollen wichtige Vorbetrachtungen durchgeführt werden, um einen allgemeinen Überblick über den Umfang zu erlangen und die Aufgabe der Integration zu verbildlichen. Wichtige Methoden sind das Sammeln von Ideen, das Erstellen eines Zielkatalogs, das Durchführen einer Machbarkeitsanalyse, das Betrachten von Risiken und Chancen, das Festlegen von Referenzbezügen und die Bewertung der neuen Anforderungen (s. Kap. 4.4).

In der zweiten Phase werden wichtige Analysen durchgeführt, um das System oder den Prozess zu untersuchen. Dazu gehört die Ist-Analyse, Beobachtungen, Gespräche, Recherche, Audits, die Stakeholderanalyse und die Gap-Analyse (s. Kap. 5).

Phase drei, behandelt das Ableiten von Maßnahmen und die dazu gehörenden Aufgaben, wie Prüfung auf Umsetzbarkeit und Angemessenheit, Kategorisierung, Priorisierung, etc.

In der vierten, der vorletzten Phase, werden vor dem Umsetzen der Maßnahmen nochmals Risiken und Chancen betrachtet. Auch das Nachverfolgen des Umsetzungsstands der

Maßnahmen, das Achten auf Komplexität und die Bewertung von Änderungen während der Umsetzung gehören zu dieser Phase.

Phase fünf dreht sich um die Wirksamkeitsbewertung. Methoden wie Beobachtungen, Gespräche und Audits spielen hier wieder eine Rolle.

8.2 Anwendung des Leitfadens

Der Leitfaden kann bei der Integration von neuen Anforderungen in ein bestehendes Managementsystem, integriertes Managementsystem, einen Prozess oder eines Prozessschrittes angewendet werden. Es ist wichtig, dass in der Phase der Vorbetrachtung, ermittelt wird, ob die zu integrierenden Anforderungen system- oder prozessorientiert sind. Wie sich im Verlauf der vorliegenden Arbeit herausgestellt hat, ist bei prozessorientierten Anforderungen, parallel zu überprüfen, ob das dazugehörige System angepasst werden muss. Da Prozesse, wie in der Einleitung von Kap. 6 beschrieben, von dem entsprechenden System, welches als Grundgerüst dient, beeinflusst werden.

Die Grenzen dieses Leitfadens können, aufgrund fehlender Tests, bloß geschätzt werden. Es wird geschätzt, dass die Integration sehr komplexer Anforderungen, wie die Integration ganzer Managementsysteme mit dem Leitfaden allein nicht realisiert werden können. Bei sehr komplexen Aufgaben müssen wahrscheinlich weitere und umfangreichere Analysemethoden hinzugezogen werden. Bei sehr einfachen Anforderungen wiederum, muss Aufwand und Nutzen abgewogen werden, diesen Leitfaden extra hinzuzuziehen.

Zu den potenziellen Nutzern dieses Leitfadens gehört jeder, der neue Anforderungen in Systeme oder Prozesse integrieren muss. Weil der Leitfaden in Zusammenhang mit der vorliegenden Arbeit entstanden ist, wird dem Nutzer des Leitfadens nahegelegt, ihn für seine persönlichen Bedürfnisse anzupassen und zu optimieren.

9 Zusammenfassung

Die Zusammenfassung gliedert sich in vier Teile auf. Im ersten Teil werden die wesentlichen Ergebnisse der Arbeit zusammengefasst und vorgestellt. Gleichzeitig erfolgt eine kritische Betrachtung der Ergebnisse und des methodischen Vorgehens. Im zweiten Teil, werden die in Kap. 1.2 festgelegten Ziele behandelt, ob diese erfüllt sind, welche Schwierigkeiten es gab und ob sich Änderungen bezüglich der ursprünglich festgelegten Zielsetzung ergeben haben. Parallel zur Behandlung der Zielerreichung, wird auf die festgelegten Forschungsfragen und ob diese während der Bearbeitung des Themas beantwortet werden konnten, eingegangen. Zum Schluss erfolgt ein Ausblick zur weiterführenden Bearbeitung des Themas und die Ableitung weiteren Forschungsbedarfs.

Zu den Ergebnissen dieser Arbeit, gehören zum einen die Verbesserungen im Projektmanagement (s. Kap. 7.1). Das Projektmanagement am Fraunhofer FEP hat jetzt eine eigene Intranetseite. Mithilfe dieser Intranetseite, wurden die ermittelten Möglichkeiten zur Verbesserung umgesetzt. Dazu gehört, dass ein Gesamtüberblick des Projektmanagements zur Verfügung gestellt wird, einschl. Projektphasen, Meilensteine, wichtige Dokumente, Anforderungen der einzelnen Managementbereiche, etc. Eine weitere Verbesserung im Projektmanagement, ist die entwickelte integrierte Risikobetrachtung, welche den Projektleitern auf der PM-Intranetseite, zur Verfügung gestellt werden kann.

Zum anderen konnte das ISMS am Fraunhofer FEP analysiert und ein Beitrag zum vollständigen Aufbau geleistet werden. Um das ISMS zu analysieren, wurde untersucht welche Methoden sich zur Analyse von MS eignen (s. Kap. 5.9). Aus acht Methoden, haben sich vier Methoden, als geeignet herausgestellt, Audits, Beobachtungen, die Stakeholderanalyse und die Gap-Analyse. Die verwendete Methode der Argumentenbilanz kann jedoch kritisch betrachtet werden, da Argumente stark subjektiv geprägt sein können und somit das Ergebnis verzerrt werden kann. Mit den ermittelten Methoden konnte das ISMS vom Fraunhofer FEP untersucht werden (s. Kap. 6). Auf den Audits und Beobachtungen, bauten die Stakeholderanalyse und die Gap-Analyse auf.

Auf Basis der Gap-Analyse, wurden unter Berücksichtigung der Stakeholderanalyse, 16 Maßnahmen (s. Tab. 13) abgeleitet. Nach der Ableitung dieser Maßnahmen, konnte eine Berechnung zur Priorisierung der Umsetzung der Maßnahmen entwickelt werden (s. Abb. 17). Die Priorität ergibt sich aus der Dringlichkeit und der Umsetzbarkeit. Diese Berechnung ist auf die Maßnahmen aus dem Maßnahmenkatalog angepasst und führte zu einem sinnvollen Ergebnis.

Das Ergebnis der Umsetzung der Maßnahmen sind, eine ISM-Intranetseite, ein Zielkatalog für das ISMS, eine funktionierende Kommunikation über die in der EN ISO 27001:2018 geforderten Punkte, eine Kommunikationsmatrix für das ISMS, ein Prozess zur regelmäßigen Überprüfung von Risiken und Chancen im ISMS, ein Prozess zur Beurteilung von Risiken und Chancen und ein ISMS Kalender zum Zweck der fortlaufenden Verbesserung. Das waren die Ergebnisse der systemorientierten Maßnahmen. Die Ergebnisse der zwei prozessorientierten Maßnahmen, sind ein funktionierender Prozess zur Informationssicherheits- / Datenschutzrisikobeurteilung und zur Informationssicherheits- / Datenschutzrisikobehandlung.

Mit dem Umsetzen der Maßnahmen wurde versucht, die in Kap. 3.4 vorgestellten Simplicity-Metoden zur Reduzierung von Komplexität im IMS anzuwenden. Diese Anwendung gelang an zwei Stellen. Zum einen bei der Einführung der ISMS-Intranetseite indem die Simplicity-Metode „Konzept übertragen“ angewendet wurde. Und zum anderen beim Einführen des Prozesses zur Informationssicherheits- / Datenschutzrisikobehandlung. Hier wird die Simplicity-Metode „Nutzen erhöhen“ angewendet, da ein Dokument für zwei Prozesse genutzt werden kann. Um die Komplexität weiter zu reduzieren, war es ein Wunsch, noch mehr Simplicity-Metoden nutzen zu können, jedoch konnten keine weiteren geeigneten Stellen zur Anwendung ausgemacht werden.

Mit dem Umsetzen der Maßnahmen, wurden gleichzeitig die von der Fraunhofer ZV vorgegebenen Anforderungen (s. 4.3) in das Projektgeschäft integriert. Anforderung A1, A2, A3, A4, A6, A7, A8 wurden parallel mit der Einführung der Prozesse zur Informationssicherheits- / Datenschutzrisikobeurteilung und zur Informationssicherheits- / Datenschutzrisikobehandlung implementiert. Die Anforderung A5 Informationsklassifizierung, war bereits in die Projektgeschäfte integriert. Die

Kommunikation der Schutzklassen, ist nun mit der Einführung der ISMS-Intranetseite verbessert. Anforderung A9, die sorgfältige Auswahl von Web- und Cloud-Diensten und Dienstleistern war auch schon implementiert. Dieses Thema, war bereits Inhalt von Schulungen. Es wurden jedoch Verbesserungen erreicht, indem Informationen zur Auswahl von Web- und Cloud-Diensten und Dienstleistern auf der ISMS-Intranetseite zur Verfügung gestellt werden und der ISMS-Kalender regelmäßig an die Aktualisierung der Intranetseite und Schulungsunterlagen erinnert.

Ein weiteres Ergebnis der Arbeit ist ein Leitfaden zum Integrieren neuer Anforderungen in ein bestehendes (integriertes) Managementsystem. Die Ziele des Leitfadens konnten erreicht werden. Es ist ein Methodenbaukasten zur Verfügung gestellt, dieser Leitfaden kann als Ablaufprotokoll dienen, eine Checklistenfunktion ist enthalten und es wurde auf einen kurzen, kompakten sowie aussagekräftigen Aufbau geachtet.

Das Muss-Ziel der Arbeit, war es die neuen Anforderungen der Fraunhofer ZV zur Informationssicherheit und zum Datenschutz (A1 bis A9) in das bestehende integrierte Managementsystem am Fraunhofer-Institut zu implementieren. Dieses Ziel wurde wie oben beschrieben, unter Beachtung der Interessen der Stakeholder, erreicht. Die mit diesem Ziel zusammenhängende Forschungsfrage, ob es eine Möglichkeit einer standardisierten Wirksamkeitsbewertung auf Prozessebene, nach der Integration neuer Anforderungen gibt, wurde mit der Vorgabe einer Möglichkeit in Kap. 7.3 beantwortet. Um die Wirksamkeitsbewertung auf Prozessebene durchzuführen, kann die entwickelte integrierte Prüfmatrix genutzt werden (s. Anhang_02_Integrierte_Prüfmatrix). Mit dieser Matrix können die Prozesse nach der Integration gegengeprüft werden. Ein Soll-Ziel war es, einen Leitfaden zur Integration neuer Anforderungen in ein bestehendes (integriertes) MS zu entwickeln. Dieser Leitfaden konnte erstellt werden. Mit der Realisierung des Leitfadens, wurde die Forschungsfrage, ob ein Methodenbaukasten zur Analyse von Managementsystemen zur Verfügung gestellt werden kann und ob es eine Möglichkeit zur Normierung der Umsetzung neuer Anforderungen in Organisationen gibt, beantwortet. Der Leitfaden bestätigt die beiden Forschungsfragen positiv. Er enthält einen Methodenbaukasten und die Umsetzung neuer Anforderungen ist normiert. Das zweite Soll-Ziel, die Untersuchung des Projektmanagements und mögliche Verbesserungen umzusetzen, wurde auch erreicht. Zu den Kann-Zielen gehörte ursprünglich das

Entwickeln einer ISMS-Intranetseite. Während der Arbeit jedoch, um genauer zu sein, beim Ableiten und Priorisieren der Maßnahmen, hat sich herausgestellt, dass dieses Ziel kein Kann-Ziel, sondern ein Muss-Ziel ist, da die Umsetzung der Maßnahmen und die Integration der neuen Anforderungen der Fraunhofer ZV, davon abhängig gewesen sind. Ein weiteres Kann-Ziel, war die Entwicklung von Schulungsunterlagen. Dieses Ziel wurde aufgrund des Umfangs der Arbeit nicht erreicht. Wie aus den oben beschriebenen Ergebnissen der Arbeit zu erkennen ist, sind die Vorgehensziele, wie die Ermittlung geeigneter Analysemethoden für ein IMS, die Analyse des IMS mit diesen geeigneten Methoden, das Ableiten von Maßnahmen und die Umsetzung dieser Maßnahmen, erreicht wurden. Das Soll-Vorgehensziel, das Zusammentragen von Informationen zum Projektmanagement am Fraunhofer FEP und das Kann-Vorgehensziel, die Entwicklung eines Verfahrens zur Priorisierung der Umsetzung von Maßnahmen konnten ebenfalls erreicht werden. Mit der Entwicklung der Berechnung, zur Priorisierung der Umsetzung der Maßnahmen, konnte die letzte Forschungsfrage, wie die Komplexität in der Priorisierung der Umsetzung der Maßnahmen mit einbezogen werden kann, beantwortet werden. Mithilfe der Dringlichkeit und der Umsetzbarkeit wurde versucht die Komplexität in der Priorisierung der Umsetzung der Maßnahmen einzubeziehen. Da eine sinnvolle Reihenfolge zur Umsetzung der Maßnahmen entstanden ist, wird somit die Frage beantwortet.

Im letzten Teil dieser Zusammenfassung erfolgt ein Ausblick auf eine weiterführende Bearbeitung des Themas und die Ableitung weiteren Forschungsbedarfs.

Eine weiterführende Bearbeitung des Themas bietet sich im Hinblick auf die integrierte Prüfmatrix an. Die Wirksamkeitsbewertung mit dieser Matrix in Kap. 7.3, kann gleichzeitig als Test angesehen werden, um herauszufinden ob die Matrix anwendbar ist oder optimiert werden muss. Als Beispiel kann die Kontrolle der Datenschutzanforderungen mit der integrierten Prüfmatrix dienen. Dazu müssen die jeweiligen Referenzen im Dokument ergänzt werden. Daraus lässt sich weiterer Forschungsbedarf ableiten. Fragen in Bezug auf Anwendung und Grenzen zur Wirksamkeitsbewertung können z.B. untersucht werden. Des Weiteren bedarf die Nutzung dieser Prüfmatrix zur prozessorientierten Integration, zusätzlicher Forschung. Aus der Methode zur Priorisierung der Maßnahmen, lässt sich auch weiterer

Forschungsbedarf ableiten. Zu untersuchen ist, ob die Berechnung bei einer höheren Anzahl von Maßnahmen, weiterhin sinnvolle Ergebnisse liefert. Vielleicht müssen weitere Kriterien definiert oder die aktuellen Kriterien, können optimiert werden. Eine weitere Bearbeitung ist bezüglich der integrierten Risikobetrachtung notwendig. Die ausschließliche Vorlage zur Anwendung dieser neu erstellten Risikobetrachtung, würde das Ziel verfehlen. Die Risikobetrachtung muss getestet, Projektleiter sollten zur Anwendung geschult und es muss auf die Rückmeldung der Projektleiter eingegangen werden. Eine mögliche kritische Frage ist, ob die integrierte Risikobetrachtung zu allgemein gehalten ist oder sie managementspezifischer gestaltet werden muss. Indem z.B. Mess- und Prüfmittel thematisiert werden, was nur im Qualitätsmanagement zu finden ist.

V Literaturverzeichnis

Brauweiler, J. (2019a). *2. UMS nach ISO 14001:2015* [Vorlesungsfolien]. Hochschule Zittau/Görlitz. Modul "Umweltmanagementsysteme".

Brauweiler, J. (2019b). [Vorlesung]. Hochschule Zittau/Görlitz. Modul "Umweltmanagementsysteme".

Brauweiler, J., Will, M. & Zenker-Hoffmann, A. (2015). *Auditierung und Zertifizierung von Managementsystemen: Grundwissen für Praktiker*. *Essentials* Wiesbaden: Springer Gabler http://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&AN=1055060

Brauweiler, J., Will, M., Zenker-Hoffmann, A. & Wiesner, J. (2018a). *Arbeitsschutzrecht: Ein Einstieg in die Materie* (2. Aufl.). *Essentials* Wiesbaden: Springer Gabler http://dx.doi.org/10.1007/978-3-658-21468-5 https://doi.org/10.1007/978-3-658-21468-5

Brauweiler, J., Zenker-Hoffmann, A. & Will, M. (2018b). *Umweltmanagementsysteme Nach ISO 14001: Grundwissen Für Praktiker* (2. Aufl.). *Essentials Ser* Wiesbaden: Gabler https://ebookcentral.proquest.com/lib/gbv/detail.action?docID=5224856

Brecht, U. (2012). *BWL für Führungskräfte: Was Entscheider im Unternehmen wissen müssen* (2., überarb. und erw. Aufl. 2013) Wiesbaden: Springer http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10607536 https://doi.org/10.1007/978-3-8349-3850-3

Bundesamt für Sicherheit in der Informationstechnik. (2008). *BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjDgL3Q5ITvAhX1wQIHHWrQABoQFjAAegQIARAD&url=https%3A%2F%2Fwww.dhge.de%2Fdms%2Fdhge%2Fhochschule%2Fweiterbildungsangebote%2Fz

ertifizierung%2FBSI_Standard_100-1.pdf&usg=AOvVaw2Xm21XaqQWcOxqc00aXmsg

Deimer, C. (2005). *Honorierungsansätze für Umweltleistungen in der Landwirtschaft - Genese, Trends und Bewertung* [Dissertation] Halle-Wittenberg, Deutschland. Martin-Luther-Universität, Halle-Wittenberg, Landwirtschaftliche Fakultät https://opendata.uni-halle.de/bitstream/1981185920/9257/1/prom.pdf

DIN EN ISO 9001 (2015). *Qualitätsmanagementsysteme – Anforderungen* (DIN EN ISO 9001:2015).

DIN EN ISO 14001 (2015). *Umweltmanagementsysteme – Anforderungen mit Anleitung zur Anwendung* (DIN EN ISO 14001:2015).

DIN EN ISO 19011 (2018). *Leitfaden zur Auditierung von Managementsystemen* (DIN EN ISO 19011:2018).

Dörner, D. (2002). *Die Logik des Mißlingens: Strategisches Denken in komplexen Situationen* (15. Aufl.). *rororo rororo-Sachbuch rororo science: Bd. 19314* Reinbek bei Hamburg: Rowohlt.

Drinck, B. (Hg.). (2013). *utb-studi-e-book: Bd. 3776. Forschen in der Schule: Ein Lehrbuch für (angehende) Lehrerinnen und Lehrer.* Verlag Barbara Budrich http://www.utb-studi-e-book.de/9783838537764

Eitner, J. (2021a). *Über uns: Fraunhofer FEP im Profil.* Fraunhofer-Gesellschaft e.V. https://www.fep.fraunhofer.de/de/ueber-uns.html#7

Eitner, J. (2021b). *Zahlen und Fakten: Auftragsforschung für Wirtschaft und Staat.* Fraunhofer-Gesellschaft e.V. https://www.fraunhofer.de/de/ueber-fraunhofer/profil-struktur/zahlen-und-fakten.html

Harmeier, J. (2016). *High Level Structure.* azm cert https://www.azm-cert.de/impuls_aktuell_High%20Level%20Structure.pdf

Hurtz, A. & Flick, D. (2002). *Verbesserungsmanagement: Was gute Unternehmen erfolgreich macht* Wiesbaden: Gabler Verlag http://dx.doi.org/10.1007/978-3-322-90247-4 https://doi.org/10.1007/978-3-322-90247-4

Kamiske, G. F. (Hg.). (2015). *Handbuch QM-Methoden: Die richtige Methode auswählen und erfolgreich umsetzen* (3., aktualisierte und erweiterte Auflage). Hanser.

Kostka, C. & Kostka, S. (2017). *Der kontinuierliche Verbesserungsprozess: Methoden des KVP* (7. Auflage) München: Hanser http://dx.doi.org/10.3139/9783446452411 https://doi.org/10.3139/9783446452411

Koubek, A. & Pölz, W. (2014). *Integrierte Managementsysteme: Von komplexen Anforderungen zu zielgerichteten Lösungen* München: Hanser.

Kudernatsch, D. (2018). Probleme lösen mit dem PDCA-Zyklus. *wirtschaft + weiterbildung,* 2018 (01), S. 38–41 https://www.kudernatsch.com/fileadmin/fachartikel-hoshin-kanri-lean-leadership/053-PDCA-Zyklus-einfuehren.pdf

Kuntsche, P. & Börchers, K. (2017). *Qualitäts- und Risikomanagement im Gesundheitswesen: Basis- und integrierte Systeme, Managementsystemübersichten und praktische Umsetzung* Berlin: Springer Gabler http://dx.doi.org/10.1007/978-3-642-55185-7 https://doi.org/10.1007/978-3-642-55185-7

Pelz, W. (2018). *SWOT-Analyse: Definition, Beispiele und Vorlagen zum Erstellen einer SWOT-Analyse.* Institut für Management-Innovation https://docplayer.org/104929073-Swot-analyse-von-prof-dr-waldemar-pelz-definition-beispiele-und-vorlagen-zum-erstellen-einer-swot-analyse.html

Pertsch, E. (2001). *Langenscheidts Großes Schulwörterbuch Lateinisch - Deutsch* (15. Aufl.) Berlin: Langenscheidt.

Pischon, A. & Liesegang, G. (Hg.). (1999). *Integrierte Managementsysteme für Qualität, Umweltschutz und Arbeitssicherheit: Mit 10 Tabellen.* Springer.

Remer, A. (2009). *Grundlagen des Management: Instrumente und Strategien*. *Grundzüge der BWL* Stuttgart: Kohlhammer.

Schawel, C. & Billing, F. (2018). *Top 100 Management Tools: Das wichtigste Buch eines Managers: von ABC-Analyse bis Zielvereinbarung* (6. Auflage) Wiesbaden: Springer Gabler.

Schifferer, S. & Reitzenstein, B. v. (2018). *Tools und Instrumente der Organisationsentwicklung: Erfolgreiche Umsetzung von Organisationsprojekten* Berlin: Springer Gabler http://dx.doi.org/10.1007/978-3-662-55560-6 https://doi.org/10.1007/978-3-662-55560-6

Schwaninger, M. (1994). *Managementsysteme*. *St. Galler Management-Konzept: Bd. 4* Frankfurt, New York: Campus.

Springer Fachmedien Wiesbaden GmbH (Hg.). (2013). *Kompakt-Lexikon Management: 2.000 Begriffe nachschlagen, verstehen, anwenden* Wiesbaden: Springer Gabler http://dx.doi.org/10.1007/978-3-658-03025-4 https://doi.org/10.1007/978-3-658-03025-4

Thum, M. (2013). *Joseph von Fraunhofer: Forscher und Unternehmer.* Fraunhofer-Gesellschaft e.V. https://www.fraunhofer.de/content/dam/zv/de/publikationen/broschueren/Joseph-von-Fraunhofer.pdf

Tiedtke, J. R. (2007). *Allgemeine BWL: Betriebswirtschaftliches Wissen für kaufmännische Berufe - Schritt für Schritt* (2., überarbeitet Auflage) Wiesbaden: Betriebswirtschaftlicher Verlag Dr. Th. Gabler | GWV Fachverlage GmbH Wiesbaden http://dx.doi.org/10.1007/978-3-8349-9168-3 https://doi.org/10.1007/978-3-8349-9168-3

VDI-Gesellschaft Produkt- und Prozessgestaltung. (2011). *Wertanalyse - das Tool im Value Management* (6. Aufl.). *VDI-Buch* Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10470740 https://doi.org/10.1007/978-3-540-79517-9

Eidesstattliche Erklärung

Ich versichere an Eides statt, dass ich die nachstehende Arbeit eigenständig und ohne fremde Hilfe angefertigt und mich anderer als der in der Arbeit angegebenen Hilfsmittel nicht bedient habe. Alle Stellen, die sinngemäß oder wörtlich aus Veröffentlichungen übernommen wurden, sind als solche kenntlich gemacht.

Name, Vorname: _____

Matrikelnummer: _____

Ort/ Datum: _____ Unterschrift: _____