Hochschule
Bonn-Rhein-Sieg
University
of Applied Sciences

Fachbereich Informatik
Department of Computer Sciences

Abschlussarbeit

Studiengang Master Informatik

Informationssicherheitsmanagementsysteme aus einer systemtheoretischen Sicht

von

Jonathan Theis

Erstprüfer	Prof. Dr. Petra Haferkorn
Zweitprüfer	Prof. Dr. Thorsten Bonne

eingereicht am 18.07.2024

https://doi.org/10.18418/opus-8902

Danksagung

Ich danke

meiner Erstprüferin Frau Prof. Dr. Petra Haferkorn und
meinem Zweitprüfer Herrn Prof. Dr. Thorsten Bonne

sowie

allen weiteren Personen, die mich während der Anfertigung meiner Abschlussarbeit unterstützt haben.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Diese Thesis befasst sich mit dem Thema: Informationssicherheitsmanagementsysteme (ISMS) und zwar zunächst aus Sicht der klassischen Managementtheorie, um dann die Vorzüge einer systemtheoretischen Sicht herauszustellen. Die Thesis erarbeitet auf Basis der neueren Systemtheorie nach Niklas Luhmann [Luh11] [Luh21] eine systemtheoretische Betrachtung ausgewählter Aspekte des ISMS. Dieses Kapitel leitet die vorliegende Arbeit ein und unterteilt sich hierfür in drei Abschnitte:

- Motivation
- Problemstellung
- Lösungsansatz

1.1 Motivation

Die Motivation für das Thema dieser Arbeit lässt sich auf zwei Hauptkomponenten herunterbrechen: eine praktische und eine wissenschaftliche (Abb. 1).

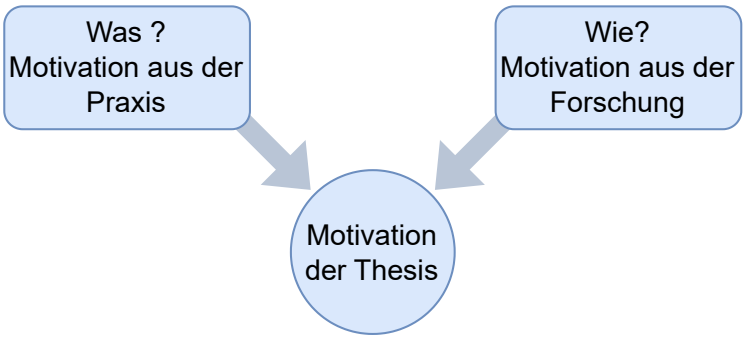

Abbildung 1: Die Motivation des Themas (Kreis) ergibt sich sowohl aus einer praktischen als auch einer wissenschaftlichen Komponente.

Die praktische Sichtweise motiviert hierbei insbesondere, warum das ISMS in dieser Arbeit betrachtet wird und begründet damit den Gegenstand der Betrachtungsweise, das „Was“ dieser Thesis. Die wissenschaftliche Perspektive erklärt, warum diese Arbeit das Thema ISMS auf Basis einer Theorie betrachtet und somit die Betrachtungsweise, das „Wie“, das ISMS in dieser Thesis untersucht wird.

1.1.1 Praktische Motivation

Im Kontext der zunehmenden Digitalisierung von Unternehmen und Behörden wächst auch die Cyberkriminalität [Eur22] [Eur23], und der Schutz digitaler Informationen ge-

winnt zunehmend an Bedeutung. Organisationen müssen daher physische, technische und organisatorische Sicherheitsmaßnahmen implementieren, die entsprechenden Aufgaben koordinieren und die zu treffenden Entscheidungen aufeinander abstimmen. Tätigkeiten, die sich mit dieser Thematik beschäftigen, subsumieren sich unter dem Begriff ISMS.

Die Notwendigkeit für ein ISMS kann sich aus unterschiedlichen Gründen ergeben. Culot et al. fassen diese Gründe in ihrer Literaturrecherche [Cul+21] beispielsweise in zwei Kategorien zusammen: Institutionalistische und Funktionalistische Motivationen. Mit dieser Zweiteilung orientieren sie sich an der Kategorisierung in [NP09].

Die „institutionalistischen“ Motivationen umfassen neben gesetzlichen Rahmenbedingungen erwartete Wettbewerbsvorteile gegenüber anderen Organisationen, beispielsweise als positives Herausstellungsmerkmal gegenüber der Konkurrenz oder als zu erfüllende Anforderung, um überhaupt für eine Zusammenarbeit mit einem anderen Unternehmen in Betracht gezogen zu werden.

Ein Beispiel für solche gesetzlichen Rahmenbedingungen in Deutschland wäre das IT-Sicherheitsgesetz [Bun15] [Bun21] in Verbindung mit der KRITIS-Sicherheitsverordnung [Bun16]. Diese rechtlichen Vorgaben legen für bestimmte Organisationen im Bereich der kritischen Infrastrukturen (kurz KRITIS) fest, dass diese Sicherheitsmaßnahmen für ihre Informationstechnik zu ergreifen haben.

Neben dieser ersten Motivationskategorie gibt es noch die Kategorie der „funktionalistischen“ Motivationen. In dieser Kategorie fassen die Autoren von [Cul+21] die Veröffentlichungen zusammen, welche als Motivation für die Einführung eines ISMS die Verbesserung der Informationssicherheit angeben. Hierzu zählt beispielsweise die Verbesserung der Dokumentation oder der Sicherheitsprozesse.

Als gemeinsamen Fixpunkt für die Diskussion über das ISMS sticht aktuell die Begriffsdefinition der ISO 27000 Reihe, insbesondere der ISO 27001, heraus. Die Internationale Organisation für Standardisierung (ISO) veröffentlichte zur Verbreitung des ISO 27001 seit 2018 bis 2022 jährlich offizielle Zahlen [ISO22]. Diesen Zahlen nach ist der ISO 27001 und allgemeiner das Thema ISMS kein landes- oder sektorspezifisches, sondern eine branchenübergreifendes, weltweite beachtetes Thema.

Zusammenfassend lässt sich sagen, dass das Interesse an ISMS in der Praxis vorhanden ist und es daher ein geeignetes Thema für die Thesis darstellt.

1.1.2 Wissenschaftliche Motivation

Nachdem die Motivation für den Betrachtungsgegenstand dieser Arbeit herausgearbeitet ist, gilt es noch die Frage zu beantworten, wieso diese Thesis einen theoriegeleiteten

Ansatz verfolgt?

Es könnte auch argumentiert werden, dass die Begriffsbildung der ISO 27000 Reihe ausreichend komplex sei, um den wissenschaftlichen Diskurs darauf auszurichten und keinen Bedarf an einer expliziten wissenschaftlichen Theorie bedürfe. Hierfür bietet es sich an, den bisherigen Forschungsdiskurs zum Thema ISMS zu betrachten.

Ungleichgewicht der aktuellen Veröffentlichungen Den Auswertungen der bereits angeführten Literaturrecherche [Cul+21] nach diskutiert die Forschung das Thema ISMS seit mindestens 2005 aktiv (vgl. Zeitstrahl von wissenschaftlichen Veröffentlichungen in [Cul+21]). Der Diskurs der insgesamt 96 Veröffentlichungen konzentriert sich dabei vornehmlich auf eine praktische, anwendungsorientierte Perspektive. Dies lässt sich sowohl an den Themenschwerpunkten der wissenschaftlichen Artikel erkennen als auch an dem Verhältnis von Veröffentlichungen, die eine Theorie oder theoriebasierte Methodik heranziehen.[1]

Der aktuelle thematische Schwerpunkt liegt laut Culot et al. auf der Vergleichbarkeit und Integration des ISMS mit anderen Standards und Rahmenwerken. Ein Beispiel hierfür ist die Arbeit von [Yas+20], welche das IT-Governance Framework „COBIT“ im Zusammenhang mit dem ISMS betrachtet. Oder die Veröffentlichungen von [MB19] und [Axe19], die das „Information Technology Infrastructure Library (ITIL)“ [Axe19] betrachten.

Diese Arbeiten nehmen die Begriffsbildung der ISO 27000 als gegeben an und arbeiten weitestgehend ohne theoretischen Unterbau. Von den 96 betrachteten Arbeiten beziehen lediglich sechs eine Theorie oder theoriebasierte Methodik mit ein. Im aktuellen Diskurs existiert somit ein Ungleichgewicht zwischen theoretisch fundierten Veröffentlichungen und Veröffentlichungen ohne Theoriebezug. Das Korrigieren dieses Ungleichgewichts kann somit ein erster Motivationsgrund für die theoretische Natur dieser Thesis verstanden werden.

Motivation des theoretischen Ansatzes Eine allgemeine Betrachtung des ISMS anhand einer Theorie ist sinnvoll, da sie eine gesteigerte Erklärbarkeit ermöglicht. Erklärbarkeit bedeutet in dieser Thesis, inwieweit sich beobachtete Dynamiken innerhalb einer Theorie beschreiben lassen, ohne aus dieser ausbrechen zu müssen. Die Vorteile einer solchen gesteigerten Erklärbarkeit lassen sich an verschiedenen Beispielen festmachen:

In [Win09] diskutieren vier Vertreter der Wirtschaftsinformatik die Notwendigkeit von

[1] Diese Arbeit versteht Theorien als Erklärungsmodelle der Grundlagenforschung und theoriebasierte Methodiken als Resultate anwendungsbasierter Forschung, im Sinne der später eingeführten Diskussion von [Win09].

theoretischen Grundlagen in ihrer Disziplin. Sie grenzen dabei die Grundlagenforschung von der angewandten Forschung wie folgt ab:

> Der Begriff der Grundlagenforschung ist nur sinnvoll in Abgrenzung zum Begriff der angewandten Forschung. Während letzterer Forschungsaktivitäten eng mit der Lösung aktueller Probleme in der wirtschaftlichen, gesellschaftlichen oder kulturellen Praxis verknüpft, legt die Grundlagenforschung den Fokus auf die Erklärung von Phänomenen in Natur und Gesellschaft, ohne einen konkreten Anwendungszusammenhang vorauszusetzen. Grundlagenforschung liefert dabei Erklärungsmodelle für die Strukturen und Zusammenhänge des jeweiligen Erkenntnisobjekts. Grundlagenforschung endet bei einem zufrieden stellenden Erklärungsmodell für das untersuchte Phänomen, während die angewandte Forschung diese Modelle anwendet, um eine Nutzen stiftende Lösung für ein gegebenes, bisher unzureichend gelöstes Problem zu entwickeln (S.224 [Win09]).

Demnach ermöglichen grundlegende Theorien (Erklärungsmodelle) erst die Untersuchung von gewissen Phänomenen. Zu einem ähnlichen Ergebnis kommt die Publikation von [Nil15] aus dem Bereich der „Implementation Science“. Deren Publikation befasst sich mit dem Mehrwert von Theorien für die Übertragung von wissenschaftlichen Erkenntnissen in die Praxis. Die „classic theories“ (dt. klassische Theorien) leisten in diesem Zusammenhang einen Beitrag, indem sie ein umfassenderes Verständnis der zugrundeliegenden Mechanismen einer Thematik ermöglichen.

Reflektiert auf das Ungleichgewicht aus dem letzten Abschnitt bedeutet dies, dass die aktuellen Erkenntnisse im Bereich ISMS weitestgehend auf die Erklärbarkeit der Begriffsbildung der ISO 27000 Reihe, insbesondere dem ISO 27001, beschränkt sind.

Damit weitreichendere Erkenntnisse gewonnen werden können, ist es notwendig, das ISMS vor dem Hintergrund einer oder mehrerer Theorien zu betrachten. Diese Erkenntnisse befruchten dann wiederum die Adressierung von Problemstellungen, die mit der aktuellen Begriffsbildung des ISMS nicht abzubilden sind.

Motivation für die Systemtheorie nach Luhmann Wie bereits zu Beginn dieses Kapitels erwähnt, zieht diese Arbeit die Systemtheorie nach Niklas Luhmann als zugrundeliegende Theorie für ihre Betrachtung heran. Eine differenzierte Begründung für diese Wahl wird im Laufe der Arbeit geliefert. Dennoch lässt sich an dieser Stelle bereits die initiale Motivation für diese Wahl skizzieren.

Zunächst einmal führen die Autoren von [Cul+21] am Ende ihrer Literaturrecherche, als Vorschlag für eine theoretisch fundierte Forschungsagenda zum ISMS, die Theorie von „Collaborative systems“ [SWM17] an. Diese Theorie fußt auf der englischen Übersetzung von Luhmanns Systemtheorie [LBL05].

Zusätzlich merken die Autoren der bereits referenzierten Veröffentlichung aus der Implementation Science [Nil15] an, dass klassische Theorien, welche Organisationen in den Fokus stellen, besonders für die Übertragung von Forschungsergebnissen in die Praxis relevant sind. Die Relevanz dieser Theorien ergibt sich aus ihrer Fähigkeit, die Organisationen, in denen praktische Lösungen implementiert werden, abbilden zu können. Als Theorie, die es insbesondere ermöglicht, Organisationen, aber auch andere soziale Phänomene zu beschreiben, erfüllt die Systemtheorie nach Luhmann genau diese Anforderungen.

1.2 Problemstellung und Lösungsansatz

Nachdem der letzte Abschnitt die Motivation für das Thema dieser Thesis ausführlich dargelegt hat, widmet sich dieser Abschnitt der zu behandelnden Problemstellung und dem Lösungsansatz.

Im Rahmen der Motivation wurde bereits darauf hingewiesen, dass der aktuelle Forschungsdiskurs weitgehend auf Theorien verzichtet und sich dessen Erklärbarkeit somit auf die des Industriestandards begrenzt.

Die daraus folgende Problemstellung, mit der sich diese Thesis befasst, lautet: „Wie kann eine systemtheoretische Sicht auf das ISMS die Erklärbarkeit gegenüber der aktuellen Forschung verbessern?“.

Damit die Problemstellung beantwortbar ist, differenziert dieser Abschnitt diese weiter aus. Es gilt folgende Teilfragen zu beantworten:

- Was bietet die aktuelle Forschung an Erklärbarkeit bezogen auf ISMS?
- Wie grenzen sich die Erklärungen auf Basis der Systemtheorie nach Luhmann von Erklärungen auf Basis keiner oder anderer Theorien ab?
- Welche Dynamiken sind insbesondere mit der Systemtheorie nach Luhmann erklärbar?

Die drei Fragen werden in der vorliegenden Arbeit beantwortet. Dabei ist das Ziel dieser Thesis insbesondere, die umfassende und differenzierte Erklärbarkeit der Systemtheorie nach Niklas Luhmann für relevante Dynamiken des ISMS nachvollziehbar

darzulegen. Um dies zu erreichen, grenzt die Thesis die Betrachtung des ISMS anhand der Systemtheorie gegenüber anderen theoretischen Betrachtungsweisen ab. Für die Abgrenzung verwendet die Thesis insbesondere die klassische Managementtheorie nach Schreyögg et al. [SK20]. Diese bezieht sich ebenfalls auf Organisationen, trifft dabei allerdings grundlegend andere Annahmen als die Systemtheorie nach Luhmann.[2]

1.3 Aufbau der Arbeit

Die Arbeit strukturiert sich zur Beantwortung der drei Teilfragen in insgesamt sieben Kapitel, welche im folgenden kurz dargestellt werden:

Kapitel 2 adressiert vor allem die erste und zweite Teilfrage der Problemstellung, indem es den Kontext der Arbeit aufzeigt.

Zum Kontext der Arbeit gehört die gegenwärtige Begriffsbildung des ISMS gemäß der ISO 27000 Reihe, auf die sich ein Großteil der Veröffentlichungen bezieht. Mit dieser Darstellung lässt sich bereits erkennen, welchen konzeptionellen Rahmen das ISMS umspannt, wodurch das Kapitel die erste Teilfrage adressiert.

Zudem gehören zum Kontext dieser Arbeit Veröffentlichungen, die sich auf einer theoretischen Basis mit ISMS oder Informationssicherheitsmanagement im Allgemeinen auseinandersetzen. Hierzu betrachtet das Kapitel beispielhaft die sechs Veröffentlichungen aus [Cul+21] sowie verschiedene Veröffentlichungen aus der Organisationspsychologie und eine Arbeit des Berufsverbands ISACA. Auch hierbei wird die erste Frage zur Erklärbarkeit der aktuellen Forschung zum Thema ISMS beantwortet.

Dieses Kapitel grenzt außerdem die verwendeten Theorien und deren Nutzen für das ISMS von der Systemtheorie nach Luhmann ab und adressiert somit ebenfalls die zweite Teilfrage. Die Abgrenzung erfolgt dabei im Vergleich zur späteren Abgrenzung der Erklärbarkeit von klassischer Managementtheorie nach [SK20] bewusst prägnanter.

Das anschließende Kapitel 3 führt die wesentlichen Grundlagen ein, die für einen tiefgreifenderen Vergleich der Systemtheorie als theoretische Grundlage mit anderen Theorien nötig sind. Zu diesen Grundlagen gehört eine tiefere Auseinandersetzung mit den Inhalten des ISO 27000, ISO 27001 und ISO 27002. Außerdem gibt das Kapitel eine Einführung in die klassische Managementtheorie nach [SK20].

Kapitel 4 verwendet die eingeführte klassische Managementtheorie und die Inhalte

[2] Siehe hierzu insbesondere Kapitel 6

der ISO 27000 Reihe aus dem vorherigen Kapitel, um einen klassischen ISMS-Begriff zu erarbeiten. Hierbei reflektiert das Kapitel das Erklärungsmodell der „Organisation als Maschine“ auf das ISMS und dessen Umwelt. Demnach behandelt dieses Kapitel insbesondere die erste Teilfrage.

Darauf folgend beschäftigt sich Kapitel 5 mit den inhärenten Limitationen eines solchen klassischen ISMS-Begriffs. Hierfür zieht das Kapitel verschiedene Beispiele heran, welche sich mit dem Erklärungsmodell der klassischen Managementtheorie nicht hinreichend differenziert beobachten lassen.

Nachdem die Limitationen der klassischen Managementtheorie in Sachen Erklärbarkeit von relevanten Dynamiken der Organisation und ihrer Umwelt aufgezeigt sind, führt Kapitel 6 die Systemtheorie nach Luhmann als Theorie mit höherer Erklärbarkeit ein. Hierfür greift das Kapitel die Kritikpunkte des vorherigen Kapitels auf und demonstriert, wie die Systemtheorie insbesondere an diesen Stellen differenziertere Betrachtungen ermöglicht. Mit dem Aufgreifen der Kritikpunkte beantwortet das Kapitel die zweite Teilfrage, inwieweit sich die Erklärbarkeit der Systemtheorie nach Luhmann von anderen Theorien unterscheidet. Anhand der Reflexionen von systemtheoretischen Erkenntnissen auf das ISMS beantwortet das Kapitel ebenfalls die dritte Teilfrage der Problemstellung, welche Dynamiken insbesondere mit der Systemtheorie nach Luhmann erklärt werden können.

Kapitel 7 konkludiert dann die Arbeit mit einer kritischen Reflexion des Arbeitsergebnisses, dem Aufzeigen weiterer Entwicklungsmöglichkeiten für zukünftige Arbeiten und einer abschließenden Zusammenfassung.

2 Kontext der Arbeit

Wie das vorherige Kapitel aufgezeigt hat, beschäftigt sich diese Thesis insbesondere mit den Vorzügen der Systemtheorie nach Luhmann als geeignete theoretische Basis zur umfassenden und differenzierten Betrachtung des ISMS.

Um diese Vorzüge herauszustellen, stellt diese Kapitel den aktuellen Stand der Forschungsdebatte dar. Genauer geht es in diesem Kapitel darum, die Erklärbarkeit bisheriger theoretischer Rahmenwerke und Methodiken kurz zu veranschaulichen, und die Nutzung der Systemtheorie nach Luhmann in dieser Arbeit abzugrenzen.

Dabei ist es relevant anzumerken, dass der Kontext, in dem sich diese Arbeit bewegt, auf mehrere Weisen interdisziplinär ist. Dies hat zur Folge, dass bereits verschiedene Publikationen aus unterschiedlichen Fachrichtungen existieren, die ausgewählte Aspekte des ISMS mit einem theoretischen Rahmenwerk oder einer theoretischen Methodik untersuchen.

Weiterhin führt dieses Kapitel die gegenwärtige Begriffsbildung des ISMS gemäß der ISO 27000 Reihe ein, da diese als gemeinsamer Fixpunkt für den aktuellen Diskurs zum ISMS dient.

2.1 Interdisziplinarität dieser Arbeit

Die Betrachtung des ISMS mittels der in diesem Kapitel aufgeführten Theorien ist auf mannigfaltige Weisen interdisziplinär. Die erste Weise, auf welche das Thema dieser Arbeit interdisziplinär ist, liegt im Informationssicherheitsmanagementsystem selbst begründet. Wie die ausgeschriebene Form erkennen lässt, setzt es sich nämlich aus zwei Anteilen zusammen: Informationssicherheit und Management.

Die Informationssicherheit wird vorrangig aus der Informatik betrachtet und in bestimmten Bereichen, wie der Kryptographie, auch aus der Mathematik. Entsprechend ist es wenig verwunderlich, dass die ISO 27000 Reihe im DIN-Normausschuss Informationstechnik und Anwendungen verortet ist (vgl. S.2 [ISO20]). Der Themenbereich des Managements ist in seiner angewandten Form hingegen insbesondere der Betriebswirtschaftslehre zuzuordnen. Das ISMS lässt sich entsprechend als Schnittstellenthema zwischen der Informatik (Informationssicherheit) und der Betriebswirtschaftslehre (Management) darstellen. Diese Eigenschaft teilt das ISMS mit der Wirtschaftsinformatik, als Schnittstellendisziplin zwischen denselben Themenbereichen. Dies lässt die Vermutung zu, dass die in [Win09] angeführten Vorteile von Grundlagenforschung in der Wirtschaftsinformatik respektive auch für den Bereich des ISMS gelten.

Neben dieser ersten, dem Thema inhärenten Weise der Interdisziplinarität, ist das Thema dieser Arbeit noch auf eine zweite Weise interdisziplinär. Zur Analyse des ISMS lassen sich Theorien und Methodiken aus anderen wissenschaftlichen Disziplinen heranziehen. Beispielsweise lässt sich das Thema Management ebenfalls aus der Perspektive der Psychologie, insbesondere im Teilgebiet der Arbeits- und Organisationspsychologie [PJF17], erforschen. Einige beispielhafte Veröffentlichungen aus dieser Disziplin betrachtet Kapitel 2.4. Weiter betrachtet Kapitel 2.3 die in der Einführung bereits erwähnten sechs theoriebasierten Veröffentlichungen, welche Culot et al. im Rahmen ihrer Literaturrecherche [Cul+21] identifizieren konnten. Eine weitere Möglichkeit, das ISMS interdisziplinär zu betrachten, ist die Systemtheorie. Ein Beispiel hierfür ist die in der Einleitung erwähnte Arbeit des Berufsverbands ISACA, der die Systemtheorie nach Bertalanffy [Ber09] heranzieht. Die vorliegende Thesis nutzt die Systemtheorie von Luhmann zur Betrachtung des ISMS, vgl. Kapitel 6. Den Unterschied zwischen den beiden systemtheoretischen Ansätzen zeigt Kapitel 2.5 auf und befasst sich mit der Abgrenzung zwischen der Sichtweise von Luhmanns Systemtheorie und der Modellbildung der ISACA in [ISA09].

2.2 Bisherige Begriffsbildung zum ISMS

Der aktuelle Bezugspunkt der Begriffsbildung des ISMS ist die ISO 27000 Reihe. Dies gilt sowohl für den aktuellen Diskurs in der Forschung als auch in der Praxis, wie die Einleitung des letzten Kapitel 1 ausgeführt hat. Besonders relevant für die Begriffsbildung sind die ISO 27000, ISO 27001 und ISO 27002, da sie die Anforderungen und das Grundverständnis für die Funktionsweise eines der Reihe entsprechenden ISMS definieren sowie zahlreiche Hinweise für dessen Umsetzung bieten.

Diese drei Standards fördern eine spezifische Begriffsbildung des ISMS, die es Industrie und Forschung ermöglicht, ihren Diskurs an einem gemeinsamen Verständnis auszurichten. Die Begriffsbildung schürt sozusagen eine Erwartungshaltung, welche Themenbereiche und Perspektiven *im* Rahmen des ISMS liegen und *außerhalb* der Konzeption liegen.[3]

Die spezifischen Inhalte dieser Standards werden im nächsten Kapitel detaillierter erläutert, damit theoretische Betrachtungen des ISMS mittels der klassischen Managementtheorie und der Systemtheorie nach Luhmann in den kommenden Kapiteln an diese anknüpfen können. Dieser Abschnitt befasst sich auf einer abstrakteren Ebene mit der Frage, welche Aspekte des Managements die ISO 27000 Reihe für das ISMS besonders

[3] Für eine allgemeine Betrachtung des Prozesses der Begriffsbildung siehe [SG89] mit der Diskussion über „Boundary Objects“ als kooperationsermöglichende Übereinkunft für Begrifflichkeiten.

hervorhebt.

In den Standards ISO 27000 und ISO 27001 sind das Risikomanagement sowie das Qualitäts- bzw. Change-Management besonders prominent vertreten. Der Risikobegriff nimmt beispielsweise eine zentrale Rolle im formulierten Managementprozess des ISO 27000 ein (vgl. Abb. 4). Auch das Qualitätsmanagement ist im Rahmen der „Fortlaufenden Verbesserung “ (Kapitel 4.5.7 [ISO20]) Teil dieses Managementprozesses.

Diese Schwerpunktbildung lässt sich auch an den Themen verschiedener Forschungsarbeiten erkennen, die sich sowohl mit dem Risikomanagement [TH23] [TGG19] als auch dem Qualitätsmanagement [Saf+20] im Rahmen des ISMS befassen.

Die Grenzen des Risikomanagements zu anderen Managementaspekten sind jedoch nicht immer klar zu trennen und überschneiden sich je nach Auffassung. Die Autoren in [MB19] argumentieren beispielsweise, dass das Risikomanagement ebenso wie die IT-Governance Teil der gemeinsamen Obermenge IT-Management ist. Power geht in seinem Buch „The Risk Management of Everything “ [Pow10] einen Schritt weiter und versteht Risikomanagement als eine Managementpraxis, die sich potenziell über die gesamte Organisation erstreckt. Ihr Herausstellungsmerkmal ist die Fähigkeit, bisher unorganisierbare Gefahren strukturieren zu können (vgl. S.10 [Pow10]).

Mit diesem umfassenden Verständnis des Risikomanagements lässt sich erklären, warum sich die ISO 27000 Reihe nicht nur mit dem Qualitäts- und Risikomanagement der Informationstechnik einer Organisation und deren technische Schwachstellen befasst. Wie die folgende Aufzählung demonstriert, nimmt die Standardreihe ebenfalls andere Gefahren für die Informationssicherheit der Organisation in den Blick:

- Der ISO 27001 betont beispielsweise an verschiedenen Stellen das Personal bzw. das Personalmanagement [ISO23]. Auch in der Forschung befassen sich Publikationen mit dem Thema „Personal“ im Zusammenhang mit dem ISMS. So evaluieren die Autoren in [AQ21], welche Techniken der „Open Source Intelligence“ (OSINT) für Hintergrundüberprüfungen von potenziellen neuen Mitarbeitern verwendet werden. Durch die verbesserte Überprüfung der Bewerber erhoffen sich die Autoren eine erhöhte Wahrscheinlichkeit, dass die gegenseitigen Erwartungen von potenziellem Mitarbeitern und der Organisation übereinstimmen (siehe hierzu auch S.82 [ISO22]).

- Auch das Thema „Budgetierung“, beispielsweise in Form von Kosten für Maßnahmen und Kosten zur Behebung von möglichen Schadensfällen, spielt im ISMS eine Rolle (vgl. Abschnitt 4.5.5 im ISO 27000 [ISO20]). Im Bereich der Versicherungen

etwa spielt das Thema Prognose von Schadensfällen anhand von Risikomodellen eine vergleichbare Rolle (siehe beispielsweise [Pai23] oder allgemein für die Finanzbranche [Hul23]).

- Zudem hat das Informationssicherheitsmanagementsystem verschiedene Implikationen auf das Projektmanagement, indem die Anforderungen des ISMS ebenfalls in den Projektanforderungen Berücksichtigung finden sollten (vgl. Abschnitt 4.5.5 [ISO20]).

Dies bedeutet jedoch nicht, dass die Standardreihe keine technische Schwachstellen und Lösungen für diese thematisiert. Der ISO 27002 weist an einigen Stellen technische Lösungen als IT-Sicherheitsmaßnahmen aus, wie unter anderem in Kapitel acht „Technologische Maßnahmen“ [ISO22]. Für diese Thesis sind jedoch insbesondere die Managementaspekte relevant, da die technischen Aspekte im Rahmen der soziologischen Systemtheorie als „Maschinen“ ohne eigene Komplexität nicht im Fokus stehen (vgl. S.16 [Luh21]).

Die Betrachtung der angeführten Managementaspekte im Verbund ist auch deswegen sinnvoll, weil sie sich in deren Zielsetzung teilweise orthogonal entgegenstehen. Beispielsweise könnte der Finanzbereich der Organisation im Rahmen eines Sparprogramms darauf drängen, die Ausgaben zu minimieren.

Währenddessen hat das Informatinossicherheitsteam o.Ä. Organisationseinheiten das Ziel die Informationssicherheit zu verbessern und möchte hierfür ein möglichst hohes Budget zur Verfügung haben.

Eine mögliche Illustration für diese entgegengesetzten Ziele ist das Zieldreieck des Projektmanagements, wie beispielsweise in Abbildung 2-3 von [WDB23] dargestellt. Das Zieldreieck des Projektmanagements visualisiert die Balance zwischen den entgegengesetzten Zielen der Optimierung von Zeit, Qualität bzw. Informationssicherheit und Kosten an den Ecken eines Dreiecks, wie in Abb. 2 dargestellt.

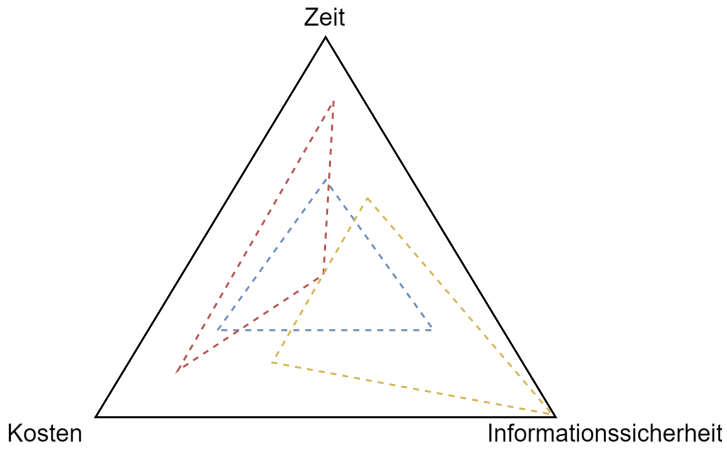

Abbildung 2: Zieldreieck des Projektmanagements angelehnt an Abbildung 2-3[WDB23]. Blau: optimiert alle Faktoren gleichermaßen. Rot: optimiert insbesondere Zeit und Kosten. Gelb: optimiert vor allem Informationssicherheit.

Änderungen an einem Faktor führen zwangsläufig zu Anpassungen bei den anderen, da eine Erhöhung oder Verringerung eines Aspekts Kompromisse in den übrigen Bereichen erfordert. In der Grafik sorgt die Maximierung der Informationssicherheit beispielsweise für einen mittleren bis hohen Zeitaufwand und Kosten.

Als Fazit dieses Abschnitts lässt sich festhalten, dass die Begriffsbildung der ISO 27000 Reihe weit über das Management von Informationstechnik hinausgeht. Sie versteht ISMS insbesondere auch als Risiko- und Qualitätsmanagement, welche sich über verschiedene Dimensionen erstrecken. Hierzu gehören beispielsweise Personal, die Umsetzung von (technischen) Sicherheitsmaßnahmen sowie Kosten. Diese stehen sich in ihren Zielsetzungen teilweise orthogonal gegenüber. Eine Theorie sollte somit in der Lage sein, nicht nur vereinzelte Aspekte aus diesem Wirkungsgefüge zu erklären, wenn sie eine umfassende Erklärungsbasis für das ISMS bieten soll.

Im Folgenden werden nun einige ausgewählte Veröffentlichungen angeführt, die das ISMS anhand von Theorien und theoriebasierten Methodiken betrachten. Dabei untersuchen die Abschnitte insbesondere, wie sich diese Methodiken von einer umfassenden Theorie unterscheiden.

2.3 Theoriebasierte Forschung zum ISMS

Die Einleitung verweist bereits auf die Literaturrecherche von Culot et al. [Cul+21], welche den aktuellen Stand der Forschung zum ISMS auf Basis des ISO 27001 erarbeitet. Hierbei stellen die Autoren heraus, dass von 96 betrachteten Veröffentlichungen lediglich sechs ihre Forschung auf eine theoretische Basis stellen:

> It should be noted that research on ISO/IEC 27001 is characterized by a relatively low theoretical underpinning: six papers built on established theories, i.e. the circuit of power framework in [Smi+10], the resource-based view (RBV) and the crisis management theory in [BYU15], the technology acceptance model (TAM) in [KCY09][sic], [VWYDV11] and [Fer+18], the theory of cultural differences in [AH10] and the technology–organization–environment (TOE) framework in [MKB21].

.

Die folgenden Absätze fassen diese sechs Arbeiten prägnant zusammen und grenzen deren Gebrauch von Theorien gegenüber dem Gebrauch der neueren soziologischen Systemtheorie in dieser Thesis ab: Die Publikation von [Smi+10] untersucht, wie Informationssicherheitssysteme in Regierungsorganisationen umgesetzt werden, wenn deren Einführung von einem Staatsoberhaupt vorgeschrieben wird. Als theoretische Basis wählen die Autoren das „circuit of power framework“ [Cle02]. Wie der Name des Rahmenwerkes bereits andeutet, stellt sich das ISMS aus dieser Perspektive in erster Linie als die Manifestation von Machtstrukturen dar. Die Autoren konkludieren die aus dieser Perspektive gewonnenen Erkenntnisse sinngemäß wie folgt:

- Eine an die Organisationseinheit angepasste Strategie für die Einführung eines ISMS hat positive Auswirkungen auf dessen Umsetzung.
- Das Diktat zur Einführung eines ISMS „von oben“ wirkt sich negativ auf die Allokation von Ressourcen und das Commitment der obersten Führungseben aus.
- Die Unternehmenskultur, von den Autoren beschrieben als Gruppennormen und kultureller Bias, wirkte sich ebenfalls negativ auf die Umsetzung aus.

Versteht man den Begriff „Macht“ als Vorgaben durch Autorität, wie es im Beispiel der Veröffentlichung durch das Dekret des Staatsoberhauptes zur Einführung eines ISMS der Fall ist, so findet sich dies auch in der Systemtheorie als ein Aspekt wieder.

Luhmanns Systemtheorie bildet Macht beispielsweise in Form von Hierarchien ab, in denen Personen auf höheren Ebenen der Hierarchie Weisungsbefugnis über die ihnen unterstellten Personen besitzen. Eine weitere Form von Macht findet sich in der Systemtheorie nach Luhmann in den Mitgliedschaftsbedingungen, denen sich eine Person fügen muss, um Teil der Organisation zu werden. Zu diesen Bedingungen zählt beispielsweise die Anerkennung der Weisungsbefugnis des disziplinarischen Vorgesetzten

und somit die Anerkennung der Hierarchie.[4]. Im Gegensatz zum „circuit of power framework“ sind diese Aspekte von Macht zwar ein Teil der Theorie, sie begrenzt sich jedoch nicht darauf. Die Systemtheorie nach Luhmann baut grundlegend auf Kommunikation und der Autopoiesis von Organisationen auf, wie in Kapitel 6 weiter ausführt wird. Mit diesem weiteren Rahmen kann die Systemtheorie eine umfangreichere Erklärungsbasis bieten als der auf Macht beschränkte Fokus des „circuit of power framework“.

In ihrer Veröffentlichung greifen die Autoren von [Fer+18] auf zwei Theorien zurück, um den konzeptionellen Rahmen für ihre Studie zu bereiten. In ihrer Studie versuchen die Autoren eine positive Beziehung zwischen dem ISMS und der Leistung der Organisation empirisch zu belegen. Dabei betrachten sie das ISMS primär als ein Instrument zur Sicherung der Geschäftskontinuität (englisch „Business Continuity Managements“ oder BCM). Um den Nutzen des ISMS als BCM zu messen, ziehen die Autoren die erste von beiden Theorien heran: Die „ressource-based view“ von [Bar91]. Im Lichte dieser Theorie lässt sich das ISMS als interne „Ressource“ verstehen, welche der Organisation einen Wettbewerbsvorteil gegenüber Konkurrenten verschafft.[5] Die zweite Theorie mit dem Namen „crisis management theory“ [PC98] verwenden die Autoren wiederum, um die Notwendigkeit mit unerwarteten Krisen umzugehen, abzubilden.

Somit sind die Autoren in der Lage, sowohl die kontinuierliche Verbesserung als auch das Risikomanagement im Zusammenhang mit dem ISMS abzubilden. Im Gegensatz zur Nutzung der Systemtheorie in der vorliegenden Arbeit verwenden die Autoren diese theoretische Basis allerdings nicht für eine umfassende theoretische Untersuchung, sondern vielmehr zur Strukturierung ihrer empirischen Ergebnisse in Bezug auf den Zusammenhang zwischen dem ISMS und der Organisationsleistung.

Ähnlich verhält es sich mit der Studie von [MKB21]. In dieser Veröffentlichung verwenden die Autoren das „Technology-Organization-Environment framework“, basierend auf [TF90], als konzeptionellen Rahmen ihrer empirischen Studie. Sie untersuchen die Verbreitung und Umsetzung von Informationssicherheitsmanagementsystemen in Deutschland. Dabei setzen sie die im Rahmenwerk definierten Einflussfaktoren bei der Verbreitung von Innovationen ein, um die Verbreitung des ISMS zu erklären. Auf Basis dieser Faktoren wertet die Studie Daten von Unternehmen in Deutschland aus und erstellt eine „Landkarte“ anhand derer sie verschiedene Erkenntnisse ableiten.

[4] Siehe für eine Übersicht zu Hierarchien, Mitgliedschaftsbedingungen und Zweckrationalität Kapitel 2 [Kü11]

[5] Siehe zu solchen extrinsischen Motivationen zur Einführung eines ISMS auch die institutionalistische Motivation in [Cul+21] oder in Kapitel 1.1.1

Abschließend nutzen zwei weitere Veröffentlichungen noch das „technology acceptance model (TAM)“ [Dav89]. Die Autoren von [AH10] verwenden die in dem Modell beschriebenen Einflussfaktoren zur Akzeptanz von Technologien, um die Akzeptanz des ISMS bei den Mitarbeitern einer Organisation zu erheben. Auch die Autoren von [VWYDV11] ziehen das TAM heran. In diesem Fall allerdings, um die Unterschiede zwischen chinesischen und europäischen Organisationen bei der Umsetzung eines ISMS zu vergleichen.

Die Veröffentlichung von [KCY09] wird in der Literaturrecherche [Cul+21] als eine der Veröffentlichungen aufgeführt, die das TAM ebenfalls als theoretische Basis heranziehen. Allerdings referenziert die Arbeit von [KCY09] keine Theorie, was auf einen Formatierungsfehler in der Arbeit von [Cul+21] schließen lässt. Ohne die Arbeit von Ku et al. [KCY09] stimmt die Anzahl der zitierten theoriebasierten Arbeiten – sechs statt sieben – mit der genannten Anzahl überein.

Als Zwischenfazit dieses Abschnitts lässt sich festhalten, dass die bisherigen Veröffentlichungen mit einem Theoriebezug eher der angewandten Forschung im Sinne der Unterscheidung aus Kapitel 1.1.2, und somit nicht der Grundlagenforschung zuzuschreiben sind. Dabei konzentrieren sich die herangezogenen Theorien meist auf einzelne Aspekte wie die Einflussfaktoren von Innovation oder Macht und bieten dadruch eine deutlich selektivere Sicht auf das ISMS, als es diese Thesis mit der Systemtheorie nach Luhmann anstrebt.

2.4 Arbeits- und Organisationspsychologisch basierte Forschung zum Thema ISMS

Neben den Arbeiten aus [Cul+21] existieren weitere theoriegeleitete Forschungsarbeiten zum Thema Informationssicherheit. Der Beginn dieses Kapitels hat bereits die Arbeits- und Organisationspsychologie sowie die Verhaltenspsychologie als weitere Fachgebiete benannt, aus denen sich das (Informationssicherheits-)Management betrachten lässt. Dieser Abschnitt führt, ähnlich wie der vorherige, beispielhaft einige dieser Veröffentlichungen an und grenzt diese erneut von dem Vorhaben in dieser Thesis ab.

Ein bedeutender Forschungsbereich scheint hierbei die Compliance der Organisationsmitglieder mit den erlassenen Sicherheitsmaßnahmen zu sein [Men+22]. Ein Unterthema in diesem Forschungsbereich, das sich aus den folgenden Veröffentlichungen herauskristallisiert, ist die Kritik an Awareness-Kampagnen, Trainings und nicht auf die Organisationsmitglieder abgestimmten Sicherheitsmaßnahmen, vor dem Hintergrund psy-

chologischer Modelle:

So entwickeln die Autoren von [BSW08] ein Modell zur Veranschaulichung der Compliance-Bereitschaft von Mitarbeitern: das sogenannte „Compliance Budget“. Dieses Budget spiegelt die Bereitschaft der Mitarbeiter wider, Sicherheitsrichtlinien zu befolgen. Das Budget wird durch das Erlassen von Sicherheitsrichtlinien erschöpft, und ist es erschöpft, tendieren die Mitarbeiter dazu, die Maßnahmen zu umgehen. Das Modell stützt sich auf die Annahme, dass jeder Mitarbeiter eine persönliche Kosten-Nutzen-Rechnung für Compliance besitzt.

In eine ähnliche Richtung gehen die Autoren von [PSF14] in ihren Untersuchungen zur Mitarbeiter-Compliance. Sie stützen ihre Überlegungen auf das Verständnis des Menschen als „Homo oeconomicus“, der versucht, seine persönliche Kosten-Nutzen-Rechnung zu optimieren.

Über die Nutzung in den respektiven Veröffentlichungen hinaus ermöglicht das Erklärungsmodell zur Compliance ebenfalls die Einordnung der Bestrebungen des Forschungsfeldes „Usable Security and Privacy“. Betrachtet man diese vor dem besagten Hintergrund, so versucht die Forschung dieses Bereichs, die mit der Compliance von Sicherheitsmaßnahmen verbundenen „Kosten“ für den einzelnen Mitarbeiter zu verringern.

Eine etwas andere Perspektive auf das Thema Sicherheitsrichtlinien bietet die Veröffentlichung von [Hie+22], die sich mit dem Prozess des Erlassens neuer Sicherheitsmaßnahmen befasst. Ausgehend davon, dass die Sicherheitsmaßnahmen umsetzbar sind, stellen die Autoren das sogenannte „Intentional Forgetting “ in den Mittelpunkt der erfolgreichen Umsetzung von Sicherheitsmaßnahmen. Sie leiten her, dass Routinen, die die Organisationsmitglieder durchlaufen, aktiv durch einen Lernprozess vergessen werden müssen. Nur so können neue Routinen, die in Übereinstimmung mit den Sicherheitsmaßnahmen stehen, etabliert werden.

Neben diesen Veröffentlichungen existieren noch zahlreiche weitere Publikationen mit einer auf das Individuum ausgerichteten Perspektive im Bereich des ISMS. Zur Vervollständigung dieses Abschnitts werden einige kurz benannt:

- [BS14] hinterfragen anhand von fünf verschiedenen psychologischen Modellen die Wirksamkeit von Awareness-Kampagnen in Bezug auf die Verhaltensänderung.
- Die Autoren in [BBS15] stützen sich auf drei verschiedene psychologisch motivierte Methodiken, um die Selbst- und Fremdwahrnehmung, den emotionalen Zustand sowie schnelles und langsames Denken in die Erstellung von Sicherheitsmaßnahmen mit einzubeziehen.

- Die Veröffentlichung [Sas15] ergänzt die bisher behandelten Veröffentlichungen mit Erkenntnissen aus diagnostischen Untersuchungen. Diese deuten darauf hin, dass wiederholte Warnungen auf Dauer ihre Wirksamkeit bezüglich der Verhaltensänderung der Mitarbeiter verlieren. Es tritt eine Art Gewöhnungseffekt ein.

- [IS10] bespricht die Anwendung von Methoden aus dem Bereich der Therapie zur Verbesserung der Beziehungen zwischen IT-Sicherheitsverantwortlichen und anderen Organisationsmitgliedern, um so die Informationssicherheit in der Organisation zu verbessern.

Zusammenfassend lässt sich festhalten, dass Untersuchungen des ISMS auf einer theoretischen Basis aus der Arbeits- und Organisationspsychologie ebenfalls tiefere Erkenntnisse liefern können, als Betrachtungen die nicht explizit Theorien als Erklärungsmodell nutzen. Die herangezogenen Theorien werden von den Autoren, ähnlich wie im vorherigen Abschnitt, zur Untersuchung ausgewählter Dynamiken des ISMS verwendet. Eine umfassendere Theorie, die möglichst viele Dynamiken des ISMS einfangen kann, bieten die hier angeführten Veröffentlichungen jedoch nicht. Demnach unterscheidet sich das Ziel dieser Thesis, die Systemtheorie nach Luhmann als eine solche Grundlage darzustellen, von den hier angeführten Publikationen.

Es sei an dieser Stelle jedoch darauf hingewiesen, dass die hier gewonnenen Erkenntnisse bezüglicher der Beispiele aus der Praxis in der nachfolgenden systemtheoretischen Betrachtung des ISMS erklärt werden können. Dies lässt sich aus systemtheoretischer Sicht vor allem dadurch begründen, dass die Organisation auf die Mitarbeiter als psychische Systeme angewiesen ist (siehe [Luh11] Seiten 397ff. oder [BCE97] Seite 187ff.).

2.5 Business Model for Information Security

Das „Business Model for Information Security“ ist ein Erklärungsmodell des Berufsverbands von IT-Revisoren, Information Security Managern und IT-Governance Experten für das Informationssicherheitsmanagement [ISA09]. Es basiert auf dem „Critical Information Infrastructure Protection (ICIIP) Modell“ von Kiely et al. [KB06]. Die grafischen Darstellungen beider Modelle sind praktisch identisch, was die Ähnlichkeit der beiden Modelle unterstreicht.

Es ist wichtig zu beachten, dass keines der beiden Modelle in einem wissenschaftlichen Journal veröffentlicht wurde. Somit ist das BMIS kein wissenschaftliches Modell, sondern eines, das aus der Praxis stammt. Dennoch sollte das BMIS im Kontext dieser

Arbeit eingeführt werden, da es ähnliche Ansätze zur Motivation, Problemstellung und Lösungsentwicklung aufweist. Darüber hinaus wählt das BMIS ebenfalls eine, wenn auch andere, systemtheoretische Basis. Entsprechend relevant ist es, im Folgenden die Unterschiede und Gemeinsamkeiten zwischen dem BMIS und der Betrachtung in Kapitel 6 der vorliegenden Arbeit herauszuarbeiten, um beide Arbeiten klar voneinander abzugrenzen.

BMIS Das Modell, dargestellt in Abb. 3, erweitert gemäß Kiely [KB06] die bisher vorherrschende Perspektive auf das Informationssicherheitsmanagement in Organisationen. Vor der Veröffentlichung des Modells konzentrierte sich die Betrachtung des Informationssicherheitsmanagements auf drei Hauptbereiche: Technologie, Menschen und Prozesse, die im Modell als Knoten konzipiert sind. Das Modell erweitert diese drei um einen vierten Knoten, der die Organisation selbst repräsentiert.

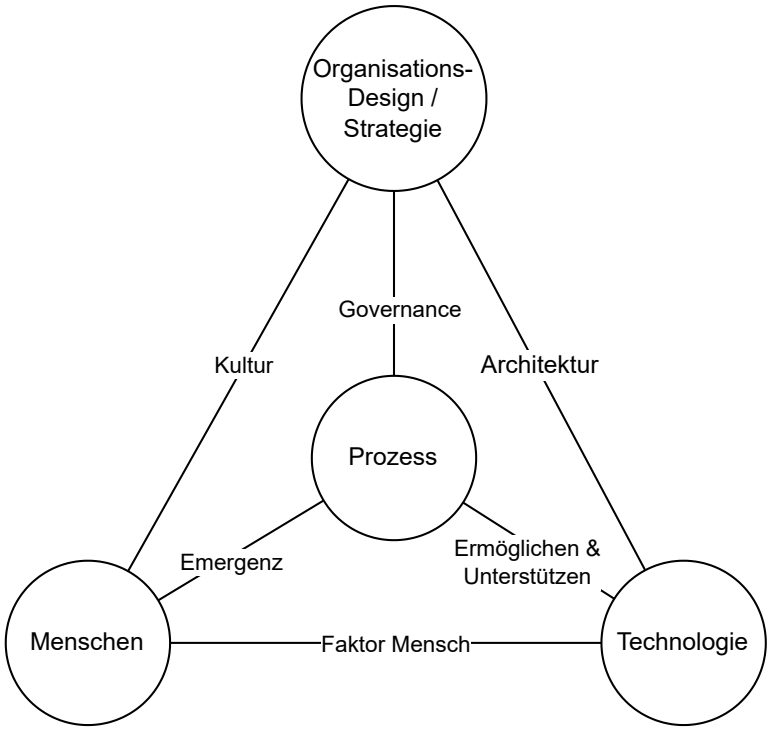

Abbildung 3: ICIIP Modell angelehnt an die Darstellung in [KB06] S.3

Darüber hinaus bilden die Autoren die Wechselwirkungen zwischen diesen Knoten explizit als Kanten ab. Diese Kanten stellen die fortwährende Spannung zwischen den Knoten dar, die aus einer kontinuierlichen Konkurrenz resultiert. Diese Spannungen müssen durch Entscheidungen ausbalanciert werden, wobei eine endgültige Balance nie erreicht werden kann:

> In such a system, and especially when it comes to security, we ought to achieve perfect balance, however impossible. It's impossible, because of the forces of entropy and dynamism that are always at work, but we strive for it. To use a metaphor from a linear model, it's like spinning plates... just as you get one plate to spin nicely; the others you spun earlier are slowing down and in danger of crashing. (S.4f. [KB06].)

Diese Übersicht genügt zum Zweck einer kurzen Einführung des Modells, da dessen genaue Spezifikation für die Abgrenzung vom Vorhaben dieser Thesis nicht herangezogen wird.

Es ist allerdings relevant anzumerken, dass das Modell seit seiner Veröffentlichung im Jahr 2009 nicht weiterentwickelt wurde. Trotz gegenteiliger Ankündigungen, dass die Entwicklung des Modells fortgesetzt würde, [6] konnten seit 2009 keine entsprechende Veröffentlichung gefunden werden. Die Recherchen dieser Arbeit konnten zwar einige Publikationen identifizieren, die das Modell entweder als konzeptionellen Rahmen oder als ergänzende Quelle heranziehen. [7] Eine tiefgreifende theoretische Weiterentwicklung des BMIS konnte über die Publikation im hauseigenen Onlinejournal der ISACA [VR10] jedoch nicht festgestellt werden.

Abgrenzung zur Thesis Nachdem das Modell und dessen Entwicklung hinreichend beleuchtet wurden, gilt es nun, das BMIS von der Theoriebildung in dieser Thesis abzugrenzen. Zunächst geht der Abschnitt auf die Gemeinsamkeiten ein, die vor allem in der Kritik der aktuellen Betrachtung der ISMS-Begriffsbildung und dem Verständnis der Rolle einer Theorie liegen. Die Autoren von [ISA09] verstehen die Rolle des BMIS ähnlich wie diese Thesis die Bedeutung der Systemtheorie für das ISMS:

> The Business Model for Information Security provides the context in which frameworks such as Control Objectives for Information and related Technology (CobiT) and standards that enterprises currently use to structure information security program activities come together (S.6 [ISA09]).

Die Autoren betrachten ihr Modell demnach als einen umfassenden Rahmen für das Management von Informationssicherheit, der die aktuellen Praktiken erfassen und erklären kann. Diese Auffassung ähnelt den beschriebenen Vorzügen klassischer Theorien

[6] Siehe S.19 [ISA09]

[7] Beispielsweise zwei spezifische Arbeiten zum Thema Internet der Dinge (IoT), die das BMIS für die Formulierung einer Roadmap [RS+18] und die Betrachtung der Ergebnisse einer Case Study [SCC17] verwenden

aus der Einleitung in Kapitel 1.1.2 und Erklärungsmodellen aus der Grundlagenforschung beschrieben in [Nil15].

Später präzisieren die Autoren die Rolle des BMIS weiter:

> The Business Model for Information Security does not replace the many sources of security program best practices. It does, however, provide a view of information security program activities within the context of the larger enterprise, to integrate the disparate security program components into a holistic system of information protection (S.9 [ISA09] bzw. siehe auch S.38f. [VR10]).

Diese Annahme stimmt mit den Aussagen in [Nil15] über die Vorteile klassischer Theorien überein, die in der Einleitung dieser Thesis zur Motivation der Systemtheorie nach Luhmann benannt werden. Anhand dieser Aussagen zeigt sich, dass das Verständnis der Autoren von [ISA09] darüber, was das BMIS leisten soll, mit den Auffassungen dieser Thesis übereinstimmt, was die Systemtheorie für das ISMS leisten kann.

Und nicht nur in diesem Punkt gibt es Überschneidungen zwischen dieser Thesis und der Veröffentlichung [ISA09]. Auch einige der von den Autoren vorgebrachten Kritikpunkte stimmen mit der späteren Kritik an der klassischen Managementtheorie in Kapitel 5 überein.

So kritisieren die Autoren von [ISA09] beispielsweise, dass aktuelle Modelle zu statisch und simpel sind, um die Dynamik einer sich wandelnden Umwelt zu adressieren: „Current models tend to be static and simple, while environments are continuously changing.“ (S.7 [ISA09]) Was sie unter „aktuellen Modellen“ verstehen, lassen die Autoren jedoch offen. Diese Kritik äußert die Thesis später in Kapitel 5.2.2 auf ähnliche Weise in Bezug auf die Darstellung der Umwelt in der klassischen Managementtheorie.

Die Autoren von [ISA09] kritisieren darüber hinaus auch die mangelnde Beachtung von Organisationen und deren Dynamiken in aktuellen Modellen: „Of the few models that do exist, even fewer consider how the enterprise changes, how the culture adapts, and what may or may not emerge as a result. “ (S.7 [ISA09]). Auch in diesem Punkt deckt sich deren Kritik mit der in dieser Thesis. Kapitel 5.1 kritisiert ebenfalls die Idealisierung einer Organisation als Maschine und die damit einhergehende Unterschätzung einer Vielzahl von organisationseigenen Dynamiken.

Über die Übereinstimmungen in Zielsetzung und Kritik am „Status quo“ hinaus überschneiden sich die Veröffentlichungen ebenfalls in der Annahme, dass die ISO 27000 Reihe ein relevanter Orientierungspunkt für den Diskurs über Informationssicherheitsmanagementsysteme ist. Dies zeigt sich daran, dass die Autoren von [VR10] das BMIS mit

der ISO 27000 Reihe in Verbindung bringen.

Nachdem die Gemeinsamkeiten der beiden Arbeiten aufgezeigt wurden, gilt es, die fundamentalen Unterschiede zwischen dieser Thesis und [ISA09] herauszustellen, namentlich die Wahl unterschiedlicher Systemtheorien. Während diese Thesis die Systemtheorie nach Niklas Luhmann für ihre Analyse heranzieht, wählen die Autoren von [ISA09] die allgemeine Systemtheorie von Bertalanffy [Ber09] als theoretische Grundlage des BMIS. Obwohl die Theorien nicht vollständig unabhängig voneinander sind – Luhmann bezieht sich in der Formulierung seiner Systemtheorie beispielsweise mehrfach auf Bertalanffys allgemeine Systemtheorie (vgl. z.B. S. 41 [LSK17] oder S. 11 [Luh21]) – sind die Schlussfolgerungen der Autoren von [ISA09] grundverschieden von denen dieser Thesis.

Die Autoren von [ISA09] sehen „die Antwort“ auf die in den Kritikpunkten erkennbare Komplexität eines ISMS in einer holistischen Sichtweise. Sie argumentieren, dass sich auf diese Weise die Komplexität einfangen lässt: „The essence of systems theory is that a system needs to be viewed holistically—not merely as a sum of its parts—to be accurately understood. A holistic approach examines the system as a complete functioning unit.“ (S.10 [ISA09]). Basierend auf dieser Annahme formulieren die Autoren das BMIS Abb. 3 als „Lösung“ für das Problem der Komplexität:

> Security-related problems are often complex and dynamic, yet all models (until now) have been simple and static. Problems have been viewed simplistically as straight-line cause and effect, when more complex (and circular) forces are generally in play. The Business Model for Information Security avoids this pitfall by employing systems thinking principles such as circular thinking, innovation, feedback and delay to help create synergy in an enterprise. (S.11 [ISA09]).

Luhmanns Systemtheorie erklärt eine solche holistische Betrachtungsweise, die eine Organisation als eine komplette Funktionseinheit auffasst, im Gegensatz dazu für unmöglich. Diese Unmöglichkeit ergibt sich aus Luhmanns Definition des Komplexitätsbegriffs: Komplexität bedeutet für Luhmann, dass nicht alle Elemente, aus denen ein System besteht, gleichzeitig miteinander verknüpft werden können (siehe S. 408 in [KE06], im Original S. 46 in [Luh21]). Dies bedeutet, dass eine vollumfängliche, simultane Vernetzung aller Elemente eines Systems unmöglich ist. Die Schlussfolgerung von [ISA09], auf die komplexe Dynamik konstruktiv mit einem komplexen holistischen Modell reagieren zu

können und somit die Komplexität einzufangen, ist somit grundlegend anders als die dieser Thesis.

Die vorliegende Arbeit vertritt entsprechend der Systemtheorie nach Luhmann die Auffassung, dass jegliche Modellbildung immer mit einer Selektion einhergeht, die gezwungenermaßen nicht alle relevanten Aspekte abbilden kann.[8] Es existiert somit immer eine unumgängliche Unsicherheit, die eine vollständige Modellbildung unmöglich macht.

Als Fazit lässt sich festhalten, dass das BMIS in seiner Kritik am Status quo und der Auffassung, was eine systemtheoretische Betrachtung des ISMS leisten kann, zwar mit dieser Thesis übereinstimmt. Die Wahl der allgemeinen Systemtheorie nach Bertalanffy und die daraus folgende Schlussfolgerung, der Komplexität des ISMS mit einem konstruktiven Modell zu begegnen, unterscheidet sich jedoch grundlegend von den Schlussfolgerungen dieser Thesis, die auf der Systemtheorie nach Luhmann basieren.

Gemeinsamkeit mit der klassischen Managementtheorie Die Annahme einer holistischen Betrachtungsweise, die das BMIS von der Analyse auf Basis der Systemtheorie nach Luhmann in dieser Thesis unterscheidet, begründet gleichzeitig eine Gemeinsamkeit mit der klassischen Managementtheorie, wie sie von Schreyögg et al. [SK20] eingeführt wird (siehe Kapitel 3.3).

Die klassische Managementtheorie geht ebenfalls davon aus, dass eine Organisation holistisch abgebildet werden kann. Im Fall der klassischen Managementtheorie geschieht dies in Form eines allumfassenden Plans, der hierarchisch in die Organisation heruntergebrochen werden kann. Neben dieser Gemeinsamkeit in der Annahme der Möglichkeit eines vollständigen Erfassens aller relevanten Aspekte des ISMS gibt es eine weitere Überschneidung zwischen der klassischen Managementtheorie und dem BMIS: der Bezug auf die allgemeine Systemtheorie nach Bertalanffy.

Um diesen Bezug zu verdeutlichen, muss zunächst erklärt werden, wie sich die klassische Managementtheorie auf die allgemeine Systemtheorie nach Bertalanffy bezieht. Hierfür ist es wichtig zu verstehen, dass die klassische Managementtheorie die Funktionsweise einer Maschine als das zu erreichende Optimum für die Managementdynamik in einer Organisation idealisiert, was die vorliegende Arbeit in Kapitel 3.3.4 später weiter ausführt. Schreyögg et al. führen in [SK20] die allgemeine Systemtheorie nach Bertalanffy als Ausgangspunkt für die Konzeption einer Organisation als kybernetischen Regelkreis ein (siehe hierzu S.58f [SK20]). Der kybernetische Regelkreis ist wiederum eine Möglichkeit, die Organisation maschinenartig darzustellen, wie nachfolgend in Kapi-

[8] Zum Begriff der Selektion und dessen Zusammenhang mit Komplexitätsreduktion siehe [BCE97], S.94.

tel 3.3.3 beleuchtet. Demnach bezieht sich die klassische Managementtheorie mit ihrer Idealisierung der Organisation als Maschine indirekt auf die allgemeine Systemtheorie nach Bertalanffy (edb). Relevanter für diese Thesis ist jedoch, dass sich das BMIS mit dem Bezug auf die allgemeine Systemtheorie nach Bertalanffy ebenfalls auf die Organisation als Maschine bezieht.

Für diesen Abschnitt lassen sich die Auswirkung dieser Gemeinsamkeiten wie folgt festhalten: Da die Kritik in Kapitel 5 auf denjenigen Annahmen der klassischen Managementtheorie fußt, welche das BMIS teilt, lässt sich diese Kritik auf das BMIS übertragen. Folgerichtig bietet die in der vorliegenden Arbeit angewandte Systemtheorie nach Luhmann, durch die Adressierung dieser Kritik in Kapitel 6, gegenüber dem BMIS ebenfalls eine umfassendere und differenziertere Erklärungsbasis für das ISMS.

2.6 Zusammenfassung

Dieses Kapitel hat sich mit dem Kontext, den das Thema dieser Arbeit umgibt, befasst. Als Ergebnis dieser Auseinandersetzung lässt sich prägnant festhalten: Ein Großteil der Forschung zum Thema ISMS fußt auf keiner theoretischen Grundlage (siehe [Cul+21]). Die wenigen Publikationen, die theoretische Ansätze nutzen, tun dies meist zur Konzeptionierung einer bestimmten Problemstellung, wie beispielsweise der Compliance von Mitarbeitern mit Sicherheitsmaßnahmen.

Zudem existiert mit dem BMIS [ISA09] ein allgemeines Modell, dass das ISMS im Kontext der Organisation betrachtet (vgl. Kapitel 2.5). Trotz einiger Gemeinsamkeiten in der Kritik des Status quo und der Auffassung, was eine Systemtheorie an Vorteilen für das Thema ISMS bieten kann, unterscheidet sich das BMIS durch die Wahl der allgemeinen Systemtheorie nach [Ber09] in den daraus resultierenden Schlussfolgerungen fundamental von denen in dieser Thesis.

Allerdings weisen die Annahmen, auf welche sich das BMIS stützt, Überschneidungen mit der klassischen Managementtheorie auf, was letztlich dafür sorgt, dass die Kritik an der klassischen Managementtheorie in den späteren Kapiteln auch auf das BMIS zutrifft. Folgerichtig setzt sich die Systemtheorie nach Niklas Luhmann durch die Adressierung der Schwächen des klassischen Managements ebenfalls positiv vom BMIS ab. Darüber hinaus zeigt der Umstand, dass das BMIS von einem Berufsverband stammt, dass die Relevanz einer allgemeinen Theorie des ISMS nicht nur für die Forschung, sondern insbesondere auch für die Praxis von großer Bedeutung ist.

3 Grundlagen

Nachdem das vorherige Kapitel den Kontext des Themas dieser Thesis umrissen hat, legt dieses Kapitel die notwendigen Grundlagen für den Rest der Arbeit. Zunächst führt das Kapitel hierfür die Inhalte der ISO 27000, ISO 27001 sowie Teile der ISO 27002 ein.

Anschließend legt das Kapitel die Grundzüge der klassischen Managementtheorie dar, indem es das Managementverständnis, den Managementprozess und die zugrunde liegenden Annahmen der Theorie bespricht.

Die formulierten Grundlagen zieht das nachfolgenden Kapitel dann heran, um ein klassisches ISMS zu begründen, das an die Begriffsbildung der ISO 27000 Reihe anschließt und mit der klassischen Managementtheorie übereinstimmt.

3.1 ISO 27000

Der ISO 27000 dient primär als Überblick über das Verständnis des ISMS im Sinne der Standardreihe sowie zur Festlegung der verwendeten Terminologie.

Der Industriestandard gliedert sich zu diesem Zweck in sechs Kapitel:

1. Einleitung
2. Normative Verweisungen
3. Anwendungsbereich
4. Begriffe
5. Managementsysteme für Informationssicherheit (ISMS)
6. Die ISMS-Normenfamilie

Von diesen sechs Kapiteln sind insbesondere die Kapitel drei und vier für die spätere Erarbeitung eines klassischen ISMS relevant, da sich diese speziell mit dem ISMS und dessen Wirkungszusammenhängen befassen: Kapitel drei legt die Bedeutung der verwendeten Terminologie fest und erweitert diese um erläuternde Anmerkungen, die ein tieferes Verständnis der Begriffe ermöglichen. Kapitel vier beschreibt, wie ein ISMS nach Einschätzung der ISO 27000 konzipiert werden sollte.

Nachdem die Struktur des ISO 27000 dargestellt und Kapitel drei und vier als besonders relevant für diese Thesis identifiziert wurden, befasst sich der folgende Abschnitt mit dem darin vermittelten Verständnis eines ISMS. Der ISO 27000 beschreibt ein ISMS grundsätzlich wie folgt: „Ein ISMS ist ein systematisches Modell für die Einführung, die

Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen.“. In Kapitel 4.5 [ISO20] konkretisiert der ISO 27000 dieses „systematische Modell“ als vierphasigen iterativen Prozess. Der Prozess ist in Abbildung Abb. 4 mit den vier Phasen graphisch dargestellt:

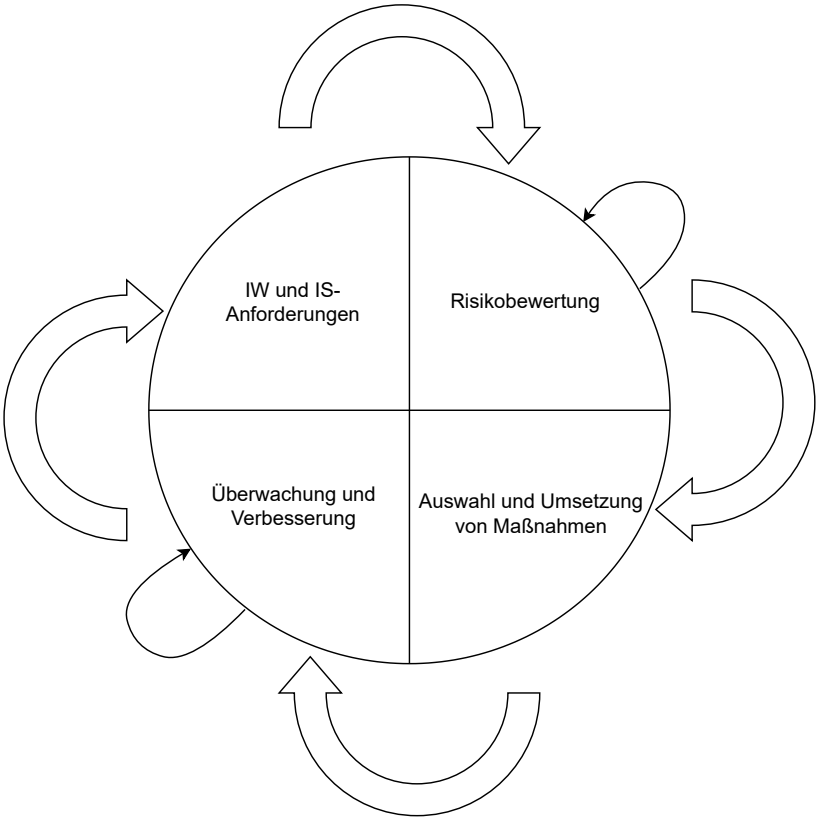

Abbildung 4: Prozess des ISMS nach ISO 27000. 1) Informationswerte (IW) und Informationssicherheits (IS) -anforderungen, 2) Risikobewertung, 3) Auswahl und Umsetzung von Maßnahmen, 4) Überwachung und Verbesserung. Jeweils aufeinander folgend (große Pfeile). 2) und 4) werden darüber hinaus in sich häufiger wiederholt.(kleine Pfeile)

Die erste Phase beschäftigt sich mit der Identifikation von Informationswerten und den damit verbundenen Informationssicherheitsanforderungen (siehe 4.5.2[ISO20]). Die Phase definiert hierfür Sicherheitsanforderungen für die identifizierten Informationswerte. Beispielsweise wäre in der Hochschule eine Sicherheitsanforderung im Bezug auf den Informationswert „Masterthesis“, dass diese unverfälscht an die Prüfer übertragen wird. Es geht bei Informationswerten und Sicherheitsanforderungen um das Verständnis dessen, was geschützt werden muss.

Die zweite Phase bestimmt Informationssicherheitsrisiken und entscheidet den Umgang mit diesen (siehe Kapitel 4.5.3 und 4.5.4). Risiken setzen sich dem Standard nach

aus einer Bedrohung, deren Eintrittswahrscheinlichkeit und den Auswirkungen bei deren Eintreten zusammen (siehe 3.61 [ISO20]). Diese gilt es zu identifizieren und entsprechend der drei Bestandteile zu bewerten. Nach der Bewertung wird für jedes Risiko entschieden, ob das Risiko als tragbar akzeptiert wird, oder ob Maßnahmen zur Risikobehandlung ergriffen werden sollen. Die Risikoanalyse und Beurteilung kann dabei nach unterschiedlichen Methoden erfolgen, beispielsweise nach [U.S49] verwendet in [WPO22].

Die dritte Phase wählt für die als zu hoch eingeschätzten Risiken bestimmte Maßnahmen aus und leitet deren Umsetzung an (siehe 4.5.5 [ISO20]). Diese Maßnahmen sollen sicherstellen, dass die Risiken auf ein akzeptables Niveau reduziert werden. Hierfür plant das Management spezifische Sicherheitsmaßnahmen für die Risiken und überwacht deren Implementierung.

Die vierte Phase beschäftigt sich mit der Überwachung, Wartung und Verbesserung der Wirksamkeit der Sicherheitsmaßnahmen in Zusammenhang mit den Informationswerten der Organisation (siehe 4.5.6 [ISO20]). Diese Phase beinhaltet die kontinuierliche Überwachung und Bewertung der implementierten Sicherheitsmaßnahmen, mit der Absicht ihre Wirksamkeit sicherzustellen und wo nötig, Verbesserungen vorzunehmen. Das Vorgehen zum Verbessern weist Ähnlichkeiten mit der Abweichungsanalyse, beispielsweise dargestellt für verschiedene Zwecke in [Bur18] auf.[9] Gemein haben die beiden Vorgehensweisen, dass ein Vergleich zwischen einem aktuellen IST-Zustand und einem angestrebten SOLL-Zustand durchgeführt wird. Die Ansätze unterscheiden sich allerdings darin, dass die Abweichungsanalyse von [Bur18] als Werkzeug zur Steuerung während des Projekts verwendet wird (S.425-432), oder zur Dokumentation des Projekts (S.621ff.). Der Standard nutzt die Abweichungsanalyse zur Identifikation von Verbesserungsmöglichkeiten und ist somit dem Projekt vorgeschaltet.

Die vier Phasen sollen in regelmäßigen Abständen wiederholt werden, um Veränderungen der Risiken, der Strategie oder den Geschäftszielen zu adressieren. Darüber hinaus soll die Risikobewertung und die Verbesserung häufiger wiederholt werden, um Veränderungen, die sich auf die Risiken auswirken, oder Verbesserungen des ISMS zu identifizieren.

Zusammenfassend spannt der ISO 27000 mit der Definition der Terminologie und des ISMS-Prozesses den konzeptionellen Rahmen des ISMS auf.

[9] Für eine kritische Einordnung der Abweichungsanalyse siehe [SK20] S.308ff.

3.2 ISO 27001 und ISO 27002

Der ISO 27001 baut auf dem zuvor in Kapitel 3.1 eingeführten Verständnis eines ISMS als systematischem Ansatz zur Verbesserung der Informationssicherheit einer Organisation auf.

Mein Masterprojekt [The23] führt den ISO 27001 und ISO 27002 bereits in Kapitel „Einführung in den ISO 27001“ ein. Dieses Unterkapitel orientiert sich insbesondere in den folgenden drei Abschnitten an dieser Einführung.

In seiner Version von 2022 spezifiziert der ISO 27001 diesen systematischen Ansatz auf 19 Seiten und in elf Kapiteln [The23]. Die ersten drei Kapitel dienen der Einleitung und der Einordnung des ISO 27001 in die Welt der ISO-Normen (edb). Die darauf folgenden Kapitel, auch Klauseln genannt, formulieren Anforderungen für Organisationen, die ein ISMS gemäß dem Verständnis der ISO 27000 Reihe umsetzen möchten. Dabei bezieht sich der ISO 27001 in erster Linie auf den systematischen Ansatz in Form des bereits in Kapitel 3.1 eingeführten Planungsprozesses. Darüber hinaus befasst sich der Standard ebenfalls mit Themen, die mit diesem Planungsprozess in Verbindung stehen. Beispielsweise schildert der ISO 27001, wie die Führung im Verhältnis zum ISMS stehen soll ([ISO23] Klausel 5.1).

Der folgende Abschnitt bietet einen kurzen Überblick über die besagten Klauseln. Dabei orientiert sich der folgende Abschnitt, wie bereits gesagt, an meinem Masterprojekt [The23]:

3.2.1 Klauseln

Die Anforderungen an ein erfolgreiches ISMS nach der ISO 27000 Reihe sind in den Kapiteln vier bis zehn des ISO 27001 detailliert beschrieben. Der Industriestandard bezeichnet diese Kapitel, wie bereits erwähnt, als **Klauseln**:

In Klausel **„Kontext der Organisation“** wird betont, dass das Umfeld der Organisation für die Entwicklung eines ISMS analysiert werden muss. Dabei sind sowohl interne als auch externe Faktoren zu berücksichtigen, die das ISMS beeinflussen können. Der Standard betrachtet die gesamte Organisation im jeweiligen Kontext, nicht nur einzelne Bereiche.

In Klausel **„Führung“** fordert der Standard, dass die Unternehmensleitung sich aktiv für das Informationssicherheitsmanagement einsetzt und die Verantwortung für dessen

Implementierung und Weiterentwicklung übernimmt. Dies beinhaltet auch die Bereitstellung der notwendigen Ressourcen und die Sicherstellung, dass entsprechende Sicherheitsregeln eingeführt sowie relevante Rollen innerhalb der Organisation geschaffen werden.

Die Klausel **„Planung“** legt fest, dass die Planung für die Informationssicherheit risikoorientiert erfolgen muss. Organisationen sollen die Risiken identifizieren, bewerten und entsprechende Maßnahmen zur Risikominderung ergreifen. Der Standard gibt spezifische Vorgaben für diesen Prozess und fordert die Formulierung von Sicherheitszielen sowie die Beachtung bestimmter Aspekte bei deren Planung.

Die Klausel **„Unterstützung“** behandelt unterstützende Maßnahmen und greift die in „Führung“ genannten Anforderungen auf, indem sie die Forderung nach ausreichenden Ressourcen für die Informationssicherheit wiederholt. Zudem müssen die nötigen Kompetenzen entwickelt und das Bewusstsein der Mitarbeiter für ihre Rolle in Bezug auf die Sicherheitsziele geschärft werden. Es wird auch betont, dass interne und externe Kommunikation bezüglich des ISMS identifiziert und gepflegt werden muss. Eine umfassende Dokumentation des ISMS ist ebenfalls erforderlich.

In **„Betrieb“** werden die in der Planung beschriebenen Schritte zur Risikobewertung und -behandlung wiederholt. Es müssen Kriterien für die Steuerung dieser Prozesse festgelegt und regelmäßige Risikobewertungen durchgeführt werden. Neue Risiken sind entsprechend zu behandeln, und die Dokumentationspflicht gilt auch für diese Prozesse.

Das Kapitel **„Bewertung der Leistung“** umfasst Anforderungen zur Überwachung, Messung, Analyse und Bewertung des ISMS. Es schreibt interne Audits vor, um die Einhaltung der Anforderungen der Organisation und des Standards zu überprüfen. Die Leistung des ISMS muss im Rahmen der Governance bewertet werden.

Die letzte Klausel **„Verbesserung“** legt fest, dass das ISMS fortlaufend verbessert werden muss.

Die Klauseln bieten somit einen tieferen Einblick in das Verständnis der Standardreihe, welche Aspekte ein ISMS umfasst.

3.2.2 Plan Do Check Act (PDCA) Zyklus

Auch dieser Abschnitt orientiert sich am gleichnamigen Abschnitt aus meinem Masterprojekt [The23]. Die Klauseln der ISO 27001 zeigen in ihrer Benennung, Reihenfolge und ihren Inhalten Überschneidungen mit dem Deming-Zyklus, auch bekannt als *„Plan Do Check Act" (PDCA) Zyklus* [Tag05]. Der folgende Abschnitt erläutert diese Überschneidungen kurz.

Der PDCA-Zyklus, ursprünglich aus dem Qualitätsmanagement, beschreibt einen iterativen Prozess mit vier Schritten zur kontinuierlichen Verbesserung der Qualität von Produkten:

- Im ersten Schritt werden die zu erreichenden Ziele festgelegt und geplant, wie diese zu erreichen sind.
- Im zweiten Schritt wird dieser Plan umgesetzt.
- Im dritten Schritt werden die Ergebnisse der Umsetzung mit den Zielen aus Schritt eins verglichen.
- Der vierte Schritt entscheidet, ob die Ziele erreicht wurden und neue Ziele für einen anderen Bereich formuliert werden können oder ob eine weitere Iteration zur Erreichung der ursprünglichen Ziele notwendig ist.

Nach diesem letzten Schritt beginnt der Prozess wieder bei Schritt eins.

Die Überschneidungen zwischen dem PDCA-Zyklus und den Klauseln der ISO 27001 sind auffällig. Obwohl die ISO 27001 den PDCA-Zyklus nicht explizit referenziert, lassen sich die Klauseln des Standards in die vier Phasen des PDCA-Zyklus einordnen: Plan entspricht der Planung, Do dem Betrieb, Check der Bewertung der Leistung und Act der Verbesserung. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist in seinem IT-Grundschutzstandard zur Etablierung eines ISMS nach ISO 27001 auf den PDCA-Zyklus als Orientierung für den Lebenszyklus des ISO 27001 hin [BSI17]. Darüber hinaus wird der PDCA-Zyklus in mehreren Veröffentlichungen verwendet, um den ISO 27001 mit anderen Standards zu vergleichen oder als Leitfaden für die Umsetzung eines ISMS zu dienen. [TPG20][Sun+20][HKR15][SSD22]. Dies zeigt, dass der PDCA-Zyklus als praktische und wissenschaftliche Orientierungshilfe zur Veranschaulichung des ISMS-Prozesses in Abb. 4 nützlich ist.

Im Gegensatz zum PDCA-Zyklus, der nur einen Hauptzyklus bietet, enthält der ISMS-Prozess zusätzliche Iterationen in der „Risikobewertung" und der „Überwachung und Verbesserung". Fernerhin lassen sich die Tätigkeiten in den Phasen des ISMS-Prozesses

nicht nahtlos auf die Tätigkeiten des PDCA-Zyklus übertragen. Beispielsweise ist die Einordnung der Tätigkeiten aus der dritten Phase des ISMS-Prozesses, „Auswahl und Umsetzung von Maßnahmen“, in die „Check“-Phase des PDCA-Zyklus nicht unmittelbar nachvollziehbar.

Trotz dieser Unterschiede wird der PDCA-Zyklus in den genannten Publikationen als konzeptioneller Rahmen für das ISMS verwendet. Dies deutet darauf hin, dass der PDCA-Zyklus im aktuellen Forschungsdiskurs als funktionsäquivalent zum ISMS-Prozess angesehen wird. Daher ist es für die systemtheoretische Analyse in Kapitel 6 unproblematisch, dass die aktuelle Forschung den PDCA-Zyklus als Rahmenmodell bevorzugt.

3.2.3 Anhang A und ISO 27002

Genauso wie die vorherigen zwei Abschnitte orientiert sich der vorliegende Abschnitt ebenfalls am gleichnamigen Abschnitt aus dem Masterprojekt [The23]. Neben den Klauseln und deren Ähnlichkeit mit dem PDCA-Zyklus beinhaltet der ISO 27001 den **Anhang A** (engl. Annex A), welcher wichtige Bereiche für die Umsetzung des Standards aufgreift. Diese Bereiche sind: organisatorische Maßnahmen, personenbezogene Maßnahmen, physische Maßnahmen und technologische Maßnahmen. Über diese Bereiche verteilt gibt Anhang A insgesamt 93 Maßnahmen an, die jeweils eine potenzielle Risikoquelle adressieren. Der ISO 27002 [ISO22] konkretisiert diese Maßnahmen mit Empfehlungen zu ihrer Umsetzung und bietet weitere Maßnahmen in den verschiedenen Bereichen.

3.3 Klassische Managementtheorie

Das vorangehende Unterkapitel befasst sich mit der Beschreibung des ISMS, dem ersten Baustein für die Erarbeitung des klassischen ISMS in Kapitel 4. Das nun folgende Unterkapitel widmet sich der Einführung der klassischen Managementtheorie, und damit dem zweiten notwendigen Baustein zur Erarbeitung des klassisch-interpretierten ISMS.

Hierfür orientiert sich der Abschnitt maßgeblich an dem im Einführungswerk zum Thema Management dargestellten klassischen Managementverständnis von Schreyögg et al. [SK20]. Insbesondere sind hierfür die Kapitel 1.1, 1.2, 1.3, 2.2.2.1 und 4.1 aus [SK20] relevant. Zur weiteren Anreicherung der Diskussion über die klassische Managementtheorie werden zusätzliche Quellen herangezogen, darunter vor allem das Werk zur Wirtschaftsinformatik von Ferstl und Sinz [FS13]. Das Unterkapitel teilt sich dabei in drei Abschnitte:

- Der erste Abschnitt stellt den Zweck von Management im Verständnis der klassischen Managementtheorie dar.
- Der zweite Abschnitt erläutert den klassischen Managementprozess.
- Der dritte Abschnitt schildert die konstituierenden Annahmen der klassischen Managementtheorie.

3.3.1 Zweck von Management

Zu Beginn ist es wesentlich, den Zweck des Managements innerhalb einer Organisation aus Sicht der klassischen Managementtheorie zu klären. Die Autoren von [SK20] beginnen in Kapitel 1.1 ihres Werkes damit, darauf aufmerksam zu machen, dass zwei unterschiedliche Perspektiven auf das Management existieren: die institutionelle und die funktionale Perspektive.

Die institutionelle Perspektive betrachtet „das Management“ als eine Gruppe von Personen bzw. eine Institution, die die Befugnis besitzt, Anweisungen an andere Mitglieder der Organisation zu formulieren und damit die Organisation zu „steuern“.

Die funktionale Perspektive sieht „das Management“ als eine Sammlung von Aufgaben, die darauf abzielen, die Organisationsmitglieder anzuleiten. Für die Klarheit im folgenden Text werden Aufgaben zur Steuerung der Organisation als Managementaufgaben bzw. Managementfunktionen bezeichnet. Diesen Managementfunktionen gegenüber stehen die zu steuernden betrieblichen Funktionen (Sachfunktionen). Die Sachfunktionen einer Organisation beinhalten unter anderem alle Tätigkeiten zur Leistungserstellung und die Ausführung der geplanten Maßnahmen (vgl. S.5-6 [SK20]).

Die Unterscheidung zwischen Managementfunktionen und Sachfunktionen führen die Autoren von [SK20] auf Frederick W. Taylor zurück, der als Begründer des„scientific managment“ (auch Taylorismus genannt) gilt (vgl. S. 38ff. [SK20]). Taylor versprach sich durch die Trennung von Planung (Managementfunktionen) und Ausführung (Sachfunktionen), dass beide Aufgabenfelder jeweils optimiert werden könnten. Die Entkopplung der Managementfunktionen sollte es ermöglichen, allgemeingültige wissenschaftlich fundierte Methoden für das Management nutzbar zu machen, während sich die Sachfunktionen vollständig auf die operativen Aufgaben spezialisieren könnten.[10]

Zusammenfassend kann Management in der klassischen Managementtheorie sowohl in seiner institutionellen als auch in seiner funktionalen Form als Steuerungsmechanismus der Organisation verstanden werden.

[10] Für eine Einführung in Taylors Publikationen zu „scientific management“ siehe [Tay04], ansonsten vgl. [SK20])

3.3.2 Klassischer Managementprozess

Dieser Abschnitt präsentiert den klassischen Managementprozess, der sich auf den „klassischen Fünferkanon von Managementfunktionen“ stützt. Der Fünferkanon wurde in [KO55] definiert und wird von Schreyögg et al. in Kapitel 1.2 [SK20] detailliert beschrieben. Dieser Abschnitt gibt einen vergleichsweise kurzen Überblick über den Kanon, der die folgenden wesentlichen Aufgaben zur Unternehmenssteuerung umfasst:

- Planung: Festsetzung der Ziele und Auswahl von Handlungsoptionen.
- Organisation: Schaffung planmäßiger Stellen und Abteilungen, Zuweisung von Kompetenzen.
- Personaleinsatz: Besetzung der Stellen mit Personal.
- Führung: Anleitung zur korrekten Umsetzung des Plans.
- Kontrolle: Abschließender Vergleich von geplantem SOLL und umgesetztem IST.

Die einzelnen Aufgaben des Fünferkanons bilden die Phasen des klassischen Managementprozess. Diese Durchläuft das Management während der Unternehmenssteuerung sequenziell. Zum Ende hin schließt die Kontrollphase der aktuellen Iteration an die Planungsphase der nächsten Iteration an, wodurch der Steuerungsprozess von neuen beginnt. Die Autoren von [SK20] führen diesen Prozess in Kapitel 1.3 aus. An dieser Stelle wird er prägnant zusammengefasst:

Der Managementprozess beginnt mit der Planungsphase, die durch die „Festsetzung von Zielen, Rahmenrichtlinien, Programmen und Verfahrensweisen zur Programmrealisierung für die Gesamtunternehmung oder einzelne ihrer Teilbereiche“ (S.9 [SK20]) in einem Plan beginnt. Diese Phase legt für die darauf folgenden Phasen einen „verbindlichen Handlungsrahmen, in den sich alle anderen Steuerungsaktivitäten einordnen“ (S. 120f. [SK20]) fest.

Die Organisationsphase konkretisiert die Ausgestaltung der Planung in Form von Abteilungen, Stellen und Kommunikationswegen. Darauf folgt die Besetzung der Stellen mit Personal. Die Führung befasst sich mit der Steuerung bzw. Feinsteuerung der Arbeitsausführung. Die Arbeitsausführung bezieht sich auf die Sachfunktionen, welche ebenfalls die neuen Maßnahmen berücksichtigen müssen.

Die Kontrollphase des klassischen Managementprozesses schließt, wie bereits gesagt, an die erste Phase an. Dabei führt sie einen SOLL/IST-Vergleich (vgl. Abweichungsanalyse in Kapitel 3.1 oder [Bur18] (S.425-432)) der Ergebnisse der Iteration (IST) mit dem geplanten Ergebnis (SOLL) durch.

Anhand des SOLL/IST-Vergleichs entscheiden die Verantwortlichen, „ob sie [die Abweichungen] die Einleitung von Korrekturmaßnahmen oder grundsätzliche Planrevisionen erfordern“ (S.10 [SK20]). Mit diesen Informationen begründet der Managementprozess eine neue Iteration, die wieder mit der Erstellung eines Plans beginnt.

So verlässt der Steuerungsprozess lediglich zu Beginn einer Iteration den Handlungsrahmen eines Plans. Ansonsten betrachtet der klassische Managementprozess die Organisation, vornehmlich aus der Perspektive des Plans, den es zu erreichen gilt.

Die Autoren visualisieren den entstehenden Managementprozess, angelehnt an [Mac69], als Zyklus und integrieren dabei auch die Sachfunktionen, die durch diesen Prozess gesteuert werden.

An dieser Stelle sei die Ähnlichkeit der bis hierhin beschriebenen Struktur des klassischen Managementprozesses mit dem PDCA-Zyklus aus Kapitel 3.2.2 und damit auch dem ISMS-Prozess des ISO 27000, illustriert in Abb. 4, angemerkt. Diese Ähnlichkeit erleichtert die Betrachtung des ISMS in Kapitel 4, da diese weitestgehend den klassischen Managementprozess für das klassische ISMS verwendet.

Die Autoren von [SK20] heben in ihrer Kritik die primäre Rolle der Planung im Gegensatz zu den nachgelagerten Managementaufgaben und Sachfunktionen im klassischen Managementprozess hervor (S. 120 ff. [SK20]). Eine detaillierte Diskussion dieser Unterteilung erfolgt in den späteren Abschnitten dieser Thesis, die sich mit den zugrundeliegenden Annahmen befassen. Dennoch gilt es, diesem Umstand auch im Rahmen des klassischen Managementprozesses Rechnung zu tragen.

Somit ergibt sich abschließend die in Abb. 5 dargestellte finale Struktur des klassischen Managementprozesses.

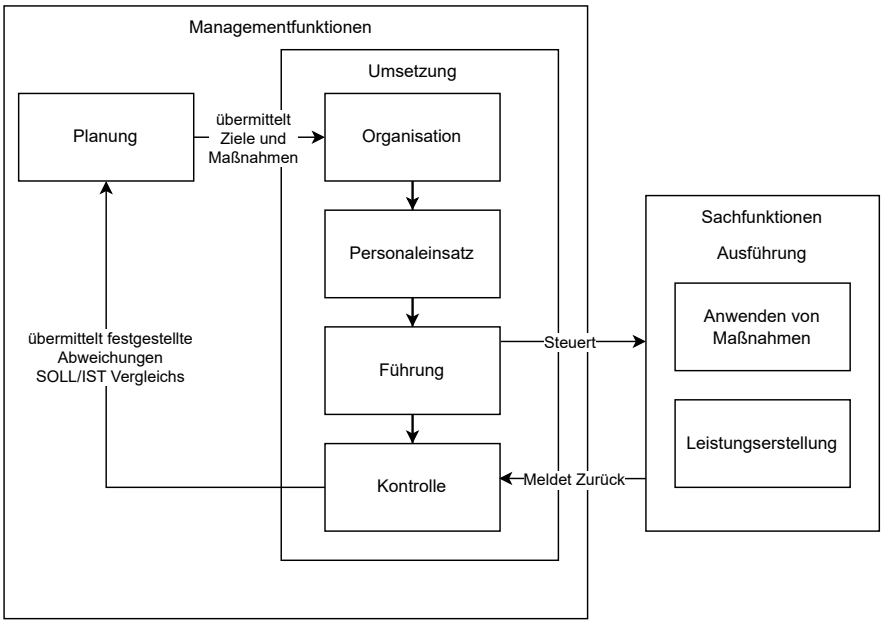

Abbildung 5: Interpretation des klassischen Managementprozesses nach [SK20]. Planungsphase: erstellt einen Plan, der die Ziele und Maßnahmen umfasst. Umsetzung: erfolgt durch die übrigen vier Managementfunktionen. Führung: koordiniert die Sachfunktionen entsprechend den neuen Maßnahmen. Sachfunktionen: informieren die Kontrolle über die Ergebnisse, woraufhin die Kontrollphase Abweichungen vom geplanten SOLL an die Planung rückmeldet.

3.3.3 Konstituierende Annahmen der klassischen Managementtheorie

Der klassische Managementprozess basiert auf einigen grundlegenden Annahmen, welche dieser Abschnitt im Folgenden herausarbeitet. Dies ist notwendig, da diese Annahmen die Ursache der Limitationen eines klassischen ISMS sind und somit die Hauptanknüpfungspunkte für die Kritik in Kapitel 5 darstellen.

Im Wesentlichen stützt sich die klassische Managementtheorie nach [SK20] auf vier konstituierende Annahmen: der Primärfunktion der Planung, der externen und internen Determiniertheit sowie der Steuerbarkeit der Organisation.

Die Primärfunktion der Planung ergibt sich aus den drei anderen Annahmen und wurde bereits im Zusammenhang mit der Ausführung des klassischen Managementprozesses in Kapitel 3.3.2 erwähnt.

Die Autoren von [SK20] beschreiben die restlichen drei Annahmen des klassischen Managements auf Seite 123 wie folgt:

- „Die Umwelt des Handlungssystems Unternehmung ist in ihren relevanten Wirkungszusammenhängen erfassbar, verstehbar und in ihrer Entwicklung prognostizierbar.“ (im folgenden „externe Determiniertheit“)

- „Das Handlungssystem Unternehmung lässt sich soweit „programmieren“, dass Planvorgaben weitgehend störungsfrei realisiert werden können, d. h., das System als solches ist vollständig durchdringbar und beherrschbar.“ (im folgenden „interne Determiniertheit“ und „Steuerbarkeit“)

Diese gilt es im folgenden noch einmal genauer darzustellen:

Determiniertheit Die Annahmen der inneren und äußeren Determiniertheit sind im Wesentlichen gleich, obwohl die äußere Determiniertheit als „erfassbar, verstehbar und prognostizierbar“ beschrieben wird, während die innere Determiniertheit diese Eigenschaften als „vollständig durchdringbar“ unter anderem Namen zusammenfasst (vgl. S.124 [SK20]).

Sowohl die Organisation als auch ihre Umwelt verhalten sich determiniert gemäß dem in der Planungsphase erstellten Plans. Daher beschreiben die Autoren von [SK20] diese Art der Unternehmensführung auf Seite 122 als „plandeterminiert“. Das Determinieren der Umwelt und der Organisation ist möglich, weil die Planungsphase in der Lage ist, alle für die Steuerung der Organisation relevanten Zusammenhänge vollständig zu durchdringen. Konkret erfasst, versteht und prognostiziert die Planungsphase alle wesentlichen Faktoren der Umwelt und der Organisation. Diese umfassenden Erkenntnisse werden dann in einem Plan zusammengeführt.

Da der Plan alle relevanten Aspekte der Organisation und Umwelt berücksichtigt, erübrigt sich die Notwendigkeit einer Betrachtung außerhalb dieses Rahmens. Aspekte, die nicht im Plan berücksichtigt sind, werden als für die Erreichung der Unternehmensziele vernachlässigbar angesehen. Wären sie relevant, wären sie im Plan entsprechend dargestellt.

Abweichungen vom Plan sind grundsätzlich als unerwünscht anzusehen. In diesem Zusammenhang führen die Autoren von [SK20] den Begriff des „Implementationsproblem“ als „Sammelbegriff für alle die Probleme, die notorisch auftreten, wenn in Organisationen Pläne realisiert werden sollen: Verdrängung, Fehlanpassungen, Widerstände durch neue aktuellere Probleme usw.“ (S.122 [SK20]) ein.

Auch im Standardwerk der Betriebswirtschaftslehre [WDB23] wird die Implementierung als Fehlerquelle thematisiert. Sollte die Ausführung des Plans nicht zu den prognostizierten Ergebnissen führen, liegt dies an den „Unzulänglichkeiten menschlichen Handelns“, die eine grundsätzlich richtige Planung nicht wie intendiert umsetzen (vgl. Ausführungen von [WDB23] auf S.98, oder im Original Kapitel 1.4 [Pic+20]).

In der klassischen Managementtheorie ist die Fehlerquelle somit vornehmlich die Um-

setzung des Plans oder dessen falsche Ausführung, nicht jedoch die Planung oder der Plan an sich.

Bei der Betrachtung des Business Model for Information Security [ISA09] wurde bereits darauf hingewiesen, dass eine solche vollständige Betrachtungsweise der Organisation und ihrer Umwelt aus Sicht der Systemtheorie nach Luhmann abzulehnen ist (vgl. Kapitel 2.5).

Steuerbarkeit Die letzte Annahme der Steuerbarkeit versetzt die Planung in die Lage, die Organisation zu steuern. Denn nur weil die Planungsphase einen allumfassenden Plan formuliert, muss dies noch nicht bedeuten, dass die Organisation diesen Plan auch entsprechend umsetzt.

Zur Veranschaulichung, wie das klassische Management die Steuerung konzipiert, zieht dieser Abschnitt das Standardwerk zur Wirtschaftsinformatik von Ferstl und Sinz [FS13] heran. Genauer gesagt, die Konzeptionierung einer Organisation als Regelkreis, wie in Abb. 6 abgebildet. Das Bildnis der Organisation als Regelkreis wurde bereits im Zusammenhang mit der allgemeinen Systemtheorie nach Bertalanffy [Ber09] als Basis des BMIS in Kapitel 2.5 eingeführt.

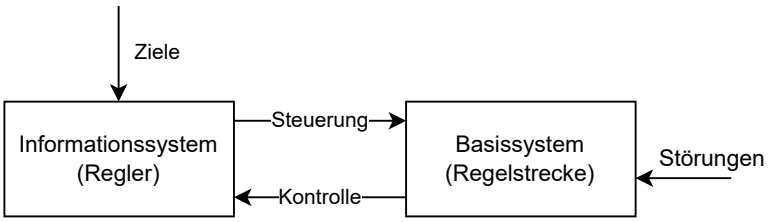

Abbildung 6: Organisation konzeptioniert als Regelkreis aus [FS13]

Der Regelkreis unterteilt das Unternehmen in zwei Systeme, die in einer Steuerungsbeziehung zueinander stehen. Das Informationssystem übernimmt die Rolle des Reglers. Es generiert Entscheidungswerte durch einen Entscheidungsprozess und übermittelt diese als Durchführungsauftrag an das Basissystem. Das Basissystem führt den Auftrag aus und sendet eine Durchführungsmeldung zurück an das Informationssystem.

Das Informationssystem erzeugt die Entscheidungswerte basierend auf den vorgegebenen Zielen. Das Basissystem kann jedoch bei der Durchführung gestört werden, was zu Abweichungen führen kann.

Vergleicht man die Beziehung zwischen Informationssystem und Basissystem mit der zwischen umsetzenden Managementfunktionen und Sachfunktionen in der grafischen Darstellung des Managementprozesses in Abb. 5, so werden Parallelen deutlich.

Die Phasen der Führung und Kontrolle sind in ihren Aufgaben mit denen des Informationssystems im Regelkreis vergleichbar. Die Sachfunktionen ähneln in ihrer Rolle als zu steuernde Instanzen dem Basissystem.

Die Autoren von [SK20] stellen auf den Seiten 124f. in ihrer Kritik ähnliche Parallelen her und vergleichen das Steuerungsverständnis der klassischen Managementtheorie mit dem einer trivialen Maschine. Die Organisation führt demnach die in der Planung festgelegten Maßnahmen aus, ähnlich wie das Basissystem im Regelkreis die Anweisungen des Informationssystems umsetzt.

Somit gestaltet sich die Steuerung der Organisation nach Erstellung des Plans als trivial, vergleichbar mit der Funktion einer Maschine, die angestellt wird (vgl. hierzu auch [Kü11] S.90ff.).

3.3.4 Organisation als Maschine

Ein wiederkehrendes Thema in allen bisherigen Abschnitten, das ebenfalls im Rahmen des BMIS in Kapitel 2.5 angesprochen wurde, ist die Idealisierung der Organisation als Maschine durch die klassische Managementtheorie. Diese Auffassung wird explizit hervorgehoben, da sie später zur Abgrenzung von der neueren, soziologischen Systemtheorie nach Luhmann herangezogen wird (vgl. insbesondere Kapitel 6.2.2).

Unter der Annahme der Determiniertheit lässt sich die Organisation in allen relevanten Aspekten darstellen, ähnlich einer technischen Zeichnung für eine Maschine.

Die Steuerung von Management und Organisation lässt sich in der klassischen Managementtheorie überspitzt anhand eines Regelkreises oder einer trivialen Maschine, innerhalb einer Ursache-Wirkungsbeziehung darstellen: Der Plan als Ursache bewirkt eine entsprechende Anpassung der Organisation.

Um das Bild der Organisation als Maschine zu vervollständigen, bleibt noch die Frage zu beantworten, aus welchen Bestandteilen diese Maschine besteht. Eine Antwort darauf liefert der deutsche Soziologe Max Weber mit seinem Konzept der bürokratischen Herrschaft.

Die Autoren von [SK20] stellen Weber als einen der drei Klassiker des Managements vor (vgl. S.45 [SK20]).

Seine bürokratische Herrschaft beschreiben die Autoren wie folgt:

> [Die] „Bürokratische Herrschaft“ist (idealtypisch) durch eine genaue Festlegung von Amtspflichten und präzise Abgrenzung von Autorität und Verantwortung gekennzeichnet, ferner durch ein festgelegtes System von Über- und Unterordnungen (Amtshierarchie), durch die nach festen, erlernbaren Regeln

> ablaufende Amtsführung und die Aktenmäßigkeit aller Vorgänge. In diesen (und weiteren) formalen Merkmalen findet die bürokratische Herrschaft ihren konkreten, für die Handlungskoordination bedeutsamen Niederschlag. (S.46 [SK20])

Diese formalen Merkmale, im Folgenden als **formale Strukturen** bezeichnet, sind laut Weber die Bestandteile einer Organisation, welche ihr die maschinenartige Eigenschaften verleihen: „Ein voll entwickelter bürokratischer Mechanismus verhält sich zu diesen genau wie eine Maschine zu den nicht mechanischen Arten der Gütererzeugung.“ (S.47 [SK20] bzw. im Original [WW72] S.561f.).

3.4 Zusammenfassung

Dieses Kapitel hat sich mit der Einführung der notwendigen Grundlagen für die Beschreibung eines klassischen ISMS im nächsten Kapitel beschäftigt. In den ersten beiden Kapiteln wurde das Verständnis des ISMS, wie es die ISO 27000 Reihe vermittelt, dargestellt. Dabei wurde insbesondere der ISMS-Prozess der ISO 27000 und dessen Zusammenhang mit dem PDCA-Zyklus erläutert.

Im Anschluss an die Einführung des ISMS beschäftigte sich das letzte Unterkapitel mit der klassischen Managementtheorie, einschließlich des Managementprozesses und der zugrundeliegenden Annahmen.

4 ISMS nach klassischer Managementtheorie

Nachdem das vorangegangene Kapitel mit der Einführung des ISMS und der klassischen Managementtheorie die nötigen Grundlagen gelegt hat, kann dieses Kapitel aufbauend darauf das klassische ISMS erarbeiten. Hierfür orientiert sich das Kapitel an den vier konstituierenden Annahmen der klassischen Managementtheorie: der Planung als Primärfunktion, der internen und externen Determiniertheit sowie der Steuerbarkeit der Organisation, die das vorherige Kapitel ausführlich besprochen hat.

Das Kapitel strukturiert sich zu diesem Zweck in drei Abschnitte, von denen jeder mit einer kurzen Zusammenfassung der entsprechenden theoretischen Annahmen beginnt und anschließend deren Implikationen für das ISMS diskutiert:

- Kapitel 4.1 erklärt das ISMS anhand der fünf Phasen des klassischen Managementprozesses aus Abb. 5 und widmet sich insbesondere der Annahme der Planung als Primärfunktion der klassischen Managementtheorie.
- Kapitel 4.2 widmet sich der Umwelt des ISMS und zeigt, wie sich diese auf Basis der externen Determiniertheit gestaltet.
- Kapitel 4.3 ergründet, wie sich die inneren Wirkungszusammenhänge des ISMS auf Basis der inneren Determiniertheit und Steuerbarkeit darstellen.

Es sei angemerkt, dass die klassische Managementtheorie in ihren Annahmen unterschiedlich strikt ausgelegt werden kann. Dies lässt sich an der ersten Annahme - Planung als Primärfunktion - beispielhaft demonstrieren: Eine strikte Auslegung dieser Funktion führt zu einer regelrechten Planungsdominanz, bei der die durch die Planung festgelegten Ziele und Maßnahmen so spezifisch sind, dass sie den anderen Managementfunktionen kaum Raum für gestalterische Freiheit und Ermessen bei der effizienten Implementierung lassen.

Da die klassische Managementtheorie in dieser Arbeit hauptsächlich zur Abgrenzung der Systemtheorie dient, um deren Vorzüge in der Erklärbarkeit hervorzuheben, wird die Dominanz der Planung strikt ausgelegt und die Flexibilität bei der Umsetzung somit vergleichsweise gering gehalten.

So gleicht die Beziehung zwischen Planung auf der einen Seite und Umsetzung sowie Ausführung der Maßnahmen auf der anderen Seite der Beziehung zwischen Informationssystem und Basissystem im Regelkreis, wie sie bereits in Kapitel 3.3.3 nach [FS13] beschrieben wurde.

4.1 Planung als Primärfunktion

Die Betrachtung des ISMS aus klassischer managementtheoretischer Sicht beginnt mit der Annahme, dass Planung die Primärfunktion im Unternehmenssteuerungsprozess ist. In dieser Arbeit wurden bereits verschiedene Unternehmenssteuerungsprozesse, wie beispielsweise der PDCA-Zyklus in Kapitel 3.2.2 oder der ISMS-Prozess in Abb. 4 eingeführt. In Kapitel 3.3.2 wurde erläutert, dass der ISMS-Prozess und der klassische Managementprozess weitestgehend vergleichbar sind. Da es in diesem Kapitel um die Darstellung des ISMS auf Basis der klassischen Managementtheorie geht, wird der klassische Managementprozess als konzeptioneller Rahmen für die Unternehmenssteuerung herangezogen.

In diesem plandeterminierten Steuerungsprozess ist die Planungsphase die einzige zielgebende Phase. Die weiteren vier Managementfunktionen zur Umsetzung des Plans sowie die Ausführung der Maßnahmen richten sich nach den von der Planung festgelegten Zielen und Vorgaben (siehe Abb. 5). Die Planungsphase trägt somit „Die gedankliche Last der Unternehmenssteuerung“ (S.120 [SK20]).

In der beschriebenen Funktion als Zielgeber kann die Planung als Informationssystem des Regelkreises „Steuerungsprozess ISMS“ verstanden werden, während die im nächsten Abschnitt thematisierten Aufgaben zur Umsetzung und Ausführung dem Basissystem zugeordnet werden können, angelehnt an [FS13].

Das verbleibende Unterkapitel widmet sich der Einbindung der Begriffsdefinition des ISMS in den klassischen Managementprozess, wie er in Abb. 4 dargestellt ist.

Beispiel Um den Einstieg in diese Thematik zu erleichtern, beginnt das Unterkapitel mit einem prägnanten Beispiel. Dieses illustriert, wie die Planung, Umsetzung und Ausführung einer Maßnahme zur Verbesserung der Informationssicherheit aus der Perspektive der klassischen Managementtheorie konzipiert werden.

In der Planungsphase entscheiden die Verantwortlichen des ISMS, die Maßnahme: „Sichern von Büros, Räumen und Einrichtungen“ (7.3 [ISO22]) umzusetzen. Wie bei allen Maßnahmen des ISO 27002 erhofft sich das Management, somit eine Verbesserung der Informationssicherheit zu erreichen. Die Maßnahme legt allgemein fest: „Die physische Sicherheit von Büros, Räumen und Einrichtungen sollte konzipiert und umgesetzt werden“ (7.3 [ISO22]).

Die weiterführende Anleitung im ISO 27002 zur Umsetzung der Maßnahme empfiehlt zudem: „Verzeichnisse, interne Telefonbücher und online zugängliche Karten, auf denen die Standorte von Einrichtungen zur Verarbeitung vertraulicher Informationen verzeichnet

sind, dürfen Unbefugten nicht ohne weiteres zugänglich gemacht werden.“ (7.3 Anleitung d) [ISO22]).

Die Verantwortlichen legen daraufhin spezifische Maßnahmen fest, die in der Organisation umgesetzt werden sollen. Eine dieser Maßnahmen ist eine neue Richtlinie. Diese untersagt es Personen in den betroffenen Einrichtungen, private Navigationsapps auf ihren Handys für die Navigation zum Betriebsgebäude zu verwenden. Dadurch soll die Gefahr minimiert werden, dass Standortinformationen durch Diebstahl dieser Geräte oder deren Nutzung durch Unbefugte offengelegt werden.

Die sich im Steuerungsprozess anschließenden Managementfunktionen nehmen diese (und weitere im Plan festgelegte Maßnahmen) auf und beginnen mit deren möglichst effizienter Umsetzung.

In der darauffolgenden Organisationsphase könnte die Verantwortung für die Überwachung der Umsetzung dem Facility Management der Einrichtung übertragen werden. Die Personaleinsatzphase teilt die Aufgabe der weiteren Umsetzung dann konkreten Personen des Facility Managements zu.

In der Führungsphase versammeln die für die Umsetzung zuständigen Mitarbeiter des Facility Managements die betroffenen Organisationsmitglieder zu einem Meeting. In diesem Meeting geben sie die neuen Richtlinien weiter. Die Verantwortlichen erläutern die Maßnahmen und deren Zweck, einschließlich der neuen Regelung, die den Gebrauch privater Navigationsanwendungen verbietet.

Gemäß dem Prinzip der Organisation als Maschinenmodell (vgl. Kapitel 3.3.4) setzen die Mitarbeiter anschließend die neuen Anweisungen um. Fortan nutzen sie keine privaten Geräte mehr zur Navigation zu den Einrichtungen.

Anhand des Beispiels lässt sich die Dreiteilung des klassischen Managementprozesses in Planung, Umsetzung und Ausführung für einen vereinfachten Fall nachvollziehen.

Der weitere Verlauf des Unterkapitels erarbeitet diese Dreiteilung noch einmal allgemeiner anhand der Ausführungen im ISO 27000. Dies ermöglicht das Aufzeigen der Konsequenzen einer klassischen managementtheoretischen Basis für die Erklärbarkeit eines solchen ISMS-Begriffs und bereitet somit die Kritik in Kapitel 5 vor.

Planung Dieser Abschnitt widmet sich der ersten Phase des Steuerungsprozesses: der Planungsphase. Als einzige zielgebende Phase im gesamten Steuerungsprozess hat sie die Primärfunktion, alle relevanten internen und externen Faktoren zu berücksichtigen, um Maßnahmen zur Verbesserung der Informationssicherheit in der Organisation effektiv zu gestalten. Sie muss explizit für die nachfolgenden Phasen der Umsetzung und

Ausführung „vorausdenken“, da diese die im Plan beschlossenen Maßnahmen nicht verändern dürfen (vgl. S.121f. [SK20]).

Die zahlreichen Aspekte, die bei der Planung von Sicherheitsmaßnahmen zu berücksichtigen sind, werden an verschiedenen Stellen innerhalb der Standards der ISO 27000 Reihe dargelegt.[11]

Es gilt beispielsweise allgemein: „[...] den Interessen und Anforderungen an die Informationssicherheit aller Stakeholder der Organisation, einschließlich Kunden, Lieferanten, Geschäftspartnern, Anteilseignern und anderen betroffenen Dritten, Rechnung zu tragen.“ (Kapitel 4.4 [ISO20]). Aus dieser Textpassage geht hervor, dass die Planung verantwortlich ist, die Erwartungen der vom ISMS betroffenen Personen und Institutionen, also des gesamten organisatorischen Umfelds zu berücksichtigen.

In Bezug auf die Umsetzung von Maßnahmen muss die Planung das Verhältnis von Kosten und Risikominderung unter gleichzeitiger Beachtung der Anforderungen und Beschränkungen der Organisationen wahren (Kapitel 4.5.5 d) [ISO20]). Außerdem müssen die nötigen Investitionen und die Verlusterwartungen in ein Gleichgewicht gebracht werden (4.5.5 f) [ISO20]). Hierbei sei an das magische Dreieck des Projektmanagements erinnert, das bereits in Abb. 2 als Werkzeug zur Visualisierung solcher entgegengesetzten Ziele angeführt wurde.

Auch in Bezug auf die Ausführung sind bereits in der Planung wichtige Aspekte zu beachten. So muss laut ISO 27000 auf eine Verträglichkeit von Sachfunktionen und Informationssicherheitsmaßnahmen geachtet werden, damit „die relevanten Informationssicherheitsmaßnahmen nahtlos in die Geschäftsprozesse der Organisation integriert werden.“ (Kapitel 4.2.3 [ISO20]). Dieser wurde bereits in Kapitel 2.4 durch verschiedene Publikationen erörtert.

Für eine erfolgreiche Umsetzung und Anwendung der Sicherheitsmaßnahmen ist es zudem laut ISO 27000 wichtig, dass die Informationssicherheitsziele mit der Unternehmenskultur übereinstimmen (vgl. Kapitel 4.6 b) [ISO20]). Die ISO 27000 Reihe definiert den Begriff der Unternehmenskultur nicht explizit. Sie kann jedoch, wie später in Kapitel 6.2 eingeführt, als Gegenstruktur zu den formalen Strukturen im Sinne Webers verstanden werden. Dies umfasst beispielsweise organisationsspezifische Traditionen, wie den kurzen Austausch über triviale Themen im Pausenraum.

Als Zwischenfazit lässt sich festhalten, dass die Faktoren, die die Planung als einzige zielgebende Phase in der klassischen Managementtheorie berücksichtigen muss,

[11] Eine vollständige Aufzählung aller relevanten Aspekte, Erwartungen und Wirkungszusammenhänge, sprengt den Umfang und die Intention der Masterarbeit , daher beschränkt sich dieser Abschnitt auf wesentliche Beispiele für zu berücksichtigende Faktoren in der Planung.

zahlreich und vielfältig sind. Der Anspruch an die Planung ist entsprechend hoch und wird dadurch erschwert, dass sich die Auswirkungen erst in späteren Phasen des Steuerungsprozesses abzeichnen.

Umsetzung und Ausführung Nachdem der vorherige Abschnitt die Planungsphase als steuerungsimpulsgebende Instanz im Sinne des Regelkreismodells von [FS13] behandelt hat, konzentriert sich dieser Abschnitt auf die gesteuerten Aufgaben: die Umsetzung und Ausführung.

Die Umsetzung und Ausführung verantworten die Realisation des Plans. Daher ist es sinnvoll, diese beiden Teile des Steuerungsprozesses gemeinsam zu betrachten.

In der Konzeption des Verhältnisses zwischen Planung und den übrigen Aufgaben im Managementprozess, die einem Regelkreis ähnelt, funktionieren die Umsetzung und Ausführung von Maßnahmen wie eine Maschine. Weitere Erläuterungen hierzu finden sich in den Ausführungen zur „Organisation als Maschine“ im vorherigen Kapitel 3.3.4.

In dieser Metapher erhält die „Maschine“ verschiedene „Befehle“, die sie dann ausführt. Diese Befehle in der Metapher sind Informationssicherheitsmaßnahmen, die von der Planung festgelegt, vom nachgelagerten Management umgesetzt und von den betroffenen Organisationsmitgliedern ausgeführt werden.

Der ISO 27000 formuliert dies ähnlich: „Das Management von Informationssicherheit findet Ausdruck in der Formulierung und Anwendung von Informationssicherheitspolitik, -verfahren und -richtlinien, die dann in der gesamten Organisation und von allen Personen, die der Organisation angehören, angewendet werden.“ (Kapitel 4.2.4 Management [ISO20]). Der in dem Zitat verwendete Begriff der „Anwendung“ umfasst die hier getrennt aufgeführten Begriffe der Umsetzung und Ausführung.

Von einer klassisch managementtheoretischen Perspektive aus betrachtet, ist besonders interessant, wie die beschriebene maschinenartige Funktionsweise der Organisation erreicht werden kann (vgl. S.91 [Kü11]). Die ISO 27000 Reihe bietet hierfür mehrere Ansatzpunkte.

Der ISO 27000 und der ISO 27001 halten beispielsweise allgemein dazu an, alle Führungsebenen zur erfolgreichen Etablierung des ISMS zu verpflichten (vgl. Kapitel 4.6 c) und Kapitel 4.2.1 c) in [ISO20] sowie 5.2, 5.3, 9.3.1 in [ISO20]). Aus der Sicht des Standards kommt ihr also eine besondere Rolle zu.

Der ISO 27001 formuliert zudem konkretere Anforderungen an die Managementfunktionen der Umsetzung in den Klauseln „Führung“, „Unterstützung“, „Betrieb“ und „Bewertung der Leistung“ (vgl. Kapitel 3.2).

Aus einer klassischen Perspektive soll mit diesen Anforderungen dafür gesorgt werden, dass „alle an einem Strang ziehen“, oder wie die Autoren in [SK20] auf Seite S.125 beschreiben, sich die Organisation wie ein Kollektivakteur verhält. Das Einbringen eigener Ziele der Mitarbeiter außerhalb der Planungsphase wird dadurch reduziert, um die im Plan festgelegten Ziele nicht zu konterkarieren (S.121f. [SK20]).

Ein weiterer, aus klassischer Sicht relevanter Baustein sind Awareness- (dt. Bewusstseins-), Schulungs- und Fortbildungsprogramme. Diese dienen dazu, neben der Umsetzung auch die planmäßige Ausführung der Maßnahmen zur Verbesserung der Informationssicherheit zu gewährleisten (vgl. Kapitel 4.6 e) [ISO20] und 7.2 [ISO22]). Aus klassischer Sicht zielen die Programme darauf ab, dass sich die Mitarbeiter gemäß der vorgesehenen Planung verhalten.

Beide Maßnahmen tragen aus der klassischen Perspektive somit auf ihre Weise dazu bei, dass die Organisation sich entsprechend des Plans wie eine triviale Maschine verhält.

Die Annahme, dass durch die obigen Programme das Verhalten der Organisation vorhersagbarer gemacht werden kann, wurde in verschiedenen psychologischen Publikationen bezüglich Informationssicherheit kritisiert (Kapitel 2.4) und bietet einen Ansatzpunkt für die spätere Nutzung der luhmannschen Systemtheorie als theoretische Grundlage in Kapitel 6.

Abweichungen von dieser maschinenartigen Funktionsweise werden im klassischen Managementverständnis durch den Abgleich der geplanten Ergebnisse (SOLL) mit den tatsächlich eingetretenen Ergebnissen (IST) festgestellt. Mögliche Ursachen für Abweichungen können sowohl innerhalb als auch außerhalb der Organisation liegen.[12]

Die klassische Managementtheorie reagiert auf Abweichungen von dieser mechanischen Funktionsweise mit dem Erstellen eines neuen Plans. [13]

Bis hierhin ließ sich die Begriffsbildung des ISMS aus der ISO 27000 Reihe in den klassischen Managementprozess, illustriert in Abb. 5, integrieren. Der ISMS-Prozess der ISO 27000, dargestellt in Abb. 4, weicht jedoch in einem Punkt vom klassischen Managementprozess ab: Neben der großen Iteration der vier Phasen des ISMS-Prozesses enthält dieser zusätzliche Iterationen der Phasen zwei zur Risikobewertung und vier zur Überwachung und Umsetzung des ISMS außerhalb der Hauptiteration. Wie in Kapitel 3.1 ausgeführt, sollen diese Iterationen mögliche Veränderungen der Risiken oder Verbesserungen erkennen.

[12] Vergleiche kurze Ausführung zur Bewertung von individueller Zielsetzung von Mitarbeitern im Planungsprozess in Kapitel 4.1, und Bewertung der Umwelt als nicht Steuerbar in Kapitel 4.2.

[13] Im Rahmen der iterativen Gestaltung des Managementprozesses, ebenfalls in Kapitel 4.1 erwähnt

Mit der strikten Auslegung der plandeterminierten Unternehmensführung lässt sich die Notwendigkeit für weitere Iterationen neben der Hauptiteration schwierig vereinbaren. Diese Nebeniterationen sind nämlich nur notwendig, wenn die Planung nicht alle relevanten Faktoren bereits vorausgesehen hat. Die Einführung zusätzlicher Überprüfungsmechanismen im Steuerungsprozess im Standard weist bereits auf die Zweifel der Praktiker hin, dass alles durch die Planung determinierbar ist.

Zusammenfassend lässt sich festhalten, dass das Verständnis von Umsetzung und Ausführung einen Großteil der Begriffsbildung des ISMS gemäß ISO 27001 integrieren kann. Allerdings weicht die in der klassischen Managementtheorie vertretene Konzentration der Steuerungskompetenz in der Planungsphase in Details von den im Standard vorgesehenen zusätzlichen Überprüfungsmechanismen in den späteren Phasen der Umsetzung und Ausführung ab.

Fazit Dieses Unterkapitel befasste sich mit der Planung als Primärfunktion des klassischen Steuerungsprozesses im Zusammenhang mit dem ISMS. Die klassische Managementtheorie von [SK20] konzipiert die Steuerung der Organisation weitestgehend maschinenartig. Hierbei übernimmt die Planung die Rolle, Anweisungen an die „Maschine“ zu formulieren und muss dabei verschiedenste Aspekte einbeziehen, die gemäß der ISO 27000 Reihe für das ISMS relevant sind.

Aus der Perspektive der klassischen Managementtheorie erscheint die darauf folgende Umsetzung und Ausführung der Maßnahmen vergleichsweise unkompliziert. Dies liegt vornehmlich daran, dass der Schwerpunkt dieser Aufgaben auf der getreuen Implementierung der detailliert geplanten Maßnahmen liegt.

Die so entwickelte Konzeption des Steuerungsprozesses fängt die in diesem Abschnitt angeführten Teile der Begriffsbildung der ISO 27000 Reihe größtenteils ein, auch wenn die Standards, vermutlich aufgrund berufspraktischer Erfahrung, an einigen Stellen darüber hinausweisen.

Nachdem dieses Unterkapitel die aktuelle Begriffsbildung des ISMS in den Steuerungsprozess der klassischen Managementtheorie integriert hat, befassen sich die folgenden Unterkapitel mit den Wirkungszusammenhängen der Organisationsumwelt und den inneren Wirkungszusammenhängen der Organisation aus klassischer managementtheoretischer Sicht.

4.2 Umwelt

Die Annahme der externen Determiniertheit lässt etwas sich verkürzt wie folgt zusammenfassen:

Die Umwelt ist in ihren für die Planung relevanten Aspekten vollständig erfassbar, erklärbar und prognostizierbar. Dies ermöglicht es, alle relevanten Umweltaspekte in der Planung zu berücksichtigen. Wäre dies nicht der Fall, könnte die Umwelt unvorhersehbar die Planung stören und somit aus dem formulierten Plan ausbrechen. Damit wäre die Steuerung der Organisation nicht mehr durch den Plan determiniert. Da sich der Managementprozess in seiner Struktur darauf stützt, dass die Planung als allumfassende vorbedenkende Instanz fungiert, würde der Prozess durch den Wegfall dieser Determiniertheit direkt gefährdet.

Im Kontext des ISMS bedeutet externe Determiniertheit, dass die Umwelt sorgfältig in der Planung berücksichtigt werden muss. Andernfalls könnte sie potenziell störend auf die Umsetzung oder Ausführung der Informationssicherheitsmaßnahmen einwirken und somit die Verbesserung der Informationssicherheit gefährden.

Nachdem die Umwelt des ISMS im klassischen Sinne allgemein eingeführt wurde, geht es nun an die Erarbeitung der Umwelt des ISMS. Die Umwelteinflüsse sind unter der Annahme der externen Determiniertheit in erster Linie als in der Planung zu beachtende Faktoren zu betrachten. Im Folgenden wird untersucht, wie sich die Begriffsbildung der Umwelt der ISO 27000 Reihe aus dieser Sicht gestaltet.

Vorab sei jedoch noch angemerkt, dass es für diese tiefere Betrachtung unvermeidlich ist, einige Details zu den Wirkungszusammenhängen innerhalb der Organisation vorwegzunehmen, um bestimmte Aspekte der Umwelt zu erläutern.

Der Glossar des ISO 27000 (Kapitel 3 [ISO20]) definiert selbst nicht den Begriff „Umwelt“, allerdings führt der Standard den Begriff des „externen Kontexts“, als Umfeld ein, in dem die Organisation versucht, ihre Ziele zu erreichen (Kapitel 3.22 [ISO20]).

Zusätzlich konkretisiert das Glossar die möglichen Bestandteile des externen Kontexts in der ersten Anmerkung zum Begriff. Zu den Bestandteilen gehören unter anderem die wettbewerbliche Umgebung, politische und gesetzliche Umgebungen und externe Stakeholder. Der Begriff „externer Kontext“ des ISO 27000 wird in diesem Kapitel synonym für den Begriff der Umwelt aus [SK20] verwendet.

Der Begriff des externen Kontexts selbst wird vom ISO 27000 lediglich in den Anmerkungen zur Definition der Risikokriterien verwendet. Als Risikokriterien bezeichnet der ISO 27000 Festlegungen, anhand derer die Signifikanz eines Risikos bewertet werden

kann. Hierauf geht der nächste Abschnitt Kapitel 4.3 detaillierter in der Beschreibung der internen Wirkungszusammenhänge ein.

An dieser Stelle sei festgehalten, dass als Quelle für solche Festlegungen neben dem internen Kontext und den Zielen der Organisation auch der externe Kontext einfließt (vgl. Anmerkung 1, 3.66 [ISO20]).

Auch wenn der Begriff des externen Kontexts nur an dieser Stelle verwendet wird, so verwendet der ISO 27000 dessen Bestandteile aus Anmerkung 1 an verschiedenen Stellen.

Der Begriff des Stakeholders (dt. Interessengruppe) wird selbst als eigener Begriff für eine Person oder Organisation, die von einer Entscheidung beeinflusst wird, eingeführt (Kapitel 3.37 [ISO20]) und an mehreren Stellen verwendet. Beispielsweise in dem bereits angeführten Zitat aus Kapitel 4.4 [ISO20], welches die Berücksichtigung der Anforderungen der Stakeholder für eine erfolgreiche Planung betont. Dies wird an einer weiteren Stelle erneut betont (vgl. Kapitel 4.2.5 a) [ISO20]). Die Planung muss demnach nicht nur die Interessengruppen in der Organisation einbeziehen, sondern ebenfalls die Interessen von „betroffenen Dritten“, die außerhalb der Organisation verortet sind.

Der ISO 27000 konkretisiert in einem späteren Kapitel weiter, dass die Risikobeurteilung und -behandlung „soweit erforderlich, eine Schätzung der Kosten und des Nutzens, die gesetzlichen Anforderungen, die Interessen der Stakeholder und andere Vorgaben und Variablen umfassen darf.“ (Kapitel 4.5.3 [ISO20]). Die Planung kann dementsprechend Interessen der Stakeholder bei der Risikoidentifikation heranziehen (vgl. Kapitel 3.68 Anmerkung 2 [ISO20]).

Darüber hinaus thematisiert der ISO 27000 weitere Bestandteile des externen Kontexts. Beispielsweise führt dieser die gesetzlichen Anforderungen an verschiedene Maßnahmen als zu berücksichtigende Regularien an (vgl. Kapitel 4.1, Kapitel 4.4 d), Kapitel 4.5.2 c) [ISO20]). Somit schränkt die Umwelt die Entscheidungsfreiheit bei der Planung ein.

Alle bis hierhin angeführten Zitate in Bezug auf den externen Kontext des ISMS und dessen Bestandteile dienen unter der klassischen Managementtheorie als zu berücksichtigende Faktoren in der Planung.

Über den externen Kontext hinaus gibt es im ISO 27000 weitere Stellen, an denen die Umwelt der Organisation thematisiert wird. Es geht um den Begriff der „Bedrohung“ der ebenfalls für die internen Wirkungszusammenhänge relevant ist (siehe Kapitel 4.3).

Den Begriff der Bedrohung führt der ISO 27000 als „mögliche Ursache eines un-

erwünschten Vorfalls, der zu Schaden für ein System oder eine Organisation (3.50 [ISO20]) führen kann“ ein (3.74 [ISO20]).

An späterer Stelle konkretisiert der ISO 27000, dass diese möglichen Ursachen insbesondere aus der Umwelt der Organisation stammen:„Organisationen und ihre Informationssysteme und Netzwerke sind mit Sicherheits*bedrohungen* aus einer Vielfalt von Quellen konfrontiert, einschließlich computergestütztem Betrug, Spionage, Sabotage, Vandalismus, Feuer und Überschwemmungen.“ (4.4 [ISO20])

Der ISO 27000 benennt darüber hinaus mögliche Quellen für Informationen, die von der Planung zur Identifikation von Bedrohungen genutzt werden können: „historische Daten, theoretische Analysen, fundierte Meinungen und Expertenmeinungen sowie Bedürfnisse von interessierten Parteien“ (3.68 Anmerkung 2 [ISO20]).

Die Bedrohungen sind unter der strikten Auslegung der externen Determiniertheit ebenfalls vollständig erfassbar. Die Planung kann die Bedrohungen demzufolge in die Planung einbeziehen und deren Eintreten somit verhindern.

Neben dem externen Kontext und der Bedrohung gibt es einen letzten Aspekt der Umwelt, den die Planung aus klassischer managementtheoretischer Sicht betrachten muss: Die unkontrollierte Veränderung der Umwelt über die Zeit.

Im Gegensatz zur Organisation, die die Managementfunktionen im plandeterministischen Verständnis steuert[14], unterliegt die Umwelt nicht dieser Steuerung.

Die Organisation verändert sich in der strikten Auslegung der plandeterminierten Unternehmensführung ausschließlich durch die Umsetzung und Ausführung des formulierten Plans (vgl. Organisation als Maschine Kapitel 3.3.4).

Dadurch, dass die Umwelt nicht der Kontrolle des Plans unterliegt, entwickelt sie sich im Laufe der Zeit. Der ISO 27000 führt als Beispiel die Veränderung von Angriffen als „häufiger, ehrgeiziger und immer raffinierter “ (4.4 [ISO20]) an. Hierdurch „Verändern sich Informationssicherheitsrisiken und die Wirksamkeit der Maßnahmen“ (4.1 [ISO20]).

In einer strikten Interpretation der klassischen Managementtheorie lässt sich diese Veränderung ebenfalls erfassen, erklären und in ihrer Entwicklung prognostizieren. Die Veränderung adressiert die Planung dann ggf. in der nächsten Iteration des Managementprozesses Abb. 5.

An den Ausführungen ist zu erkennen, dass sich die Umwelt des ISMS in der klassischen Managementtheorie in erster Linie als passive Sammlung von Faktoren verstehen lässt.

In einer strikten Auslegung der klassischen Managementtheorie ist die Planung im

[14]Siehe die Annahme der Steuerbarkeit in Kapitel 3.3.3 oder S.123 [SK20]

Zusammenhang zur Umwelt somit vornehmlich in der prognostizierenden Rolle. Die Planung erkennt Bedrohungen, die sich in der Umwelt entwickeln, bevor diese zu einem Schadensfall führen, und adressiert diese durch Maßnahmen.

Beim Eintreten von Sicherheitsvorfällen, also dem Ausbrechen aus der prognostizierenden Rolle, ist die Erklärbarkeit auf Basis der Annahmen der klassischen Managementtheorie stark limitiert. Im Grunde lässt die Theorie nur personelles Versagen als Erklärungsgrund zu. Die „Schuld“ kann dabei entweder bei der Planung oder bei den Umsetzenden liegen.

Die Planenden haben möglicherweise in ihrer Planung nicht alles bedacht, obwohl dies entsprechend der Annahme der Determinierbarkeit möglich wäre. Und die Umsetzenden könnten von den Sicherheitsmaßnahmen abgewichen sein, was bei einer korrekten Planung die einzige Möglichkeit ist, wie ein Informationssicherheitsvorfall eintreten kann.

Damit ist die klassische Managementtheorie in ihrer Erklärbarkeit gegenüber der Systemtheorie deutlich unterlegen. Diese versteht die Umwelt grundlegend anders, wie später in Kapitel 6.3 weiter ausgeführt wird.

Nachdem dieses Unterkapitel die Umwelt des ISMS in den Fokus gerückt hat, befasst sich das anschließende Unterkapitel mit den inneren Wirkungszusammenhängen des ISMS. Sowohl Kapitel 4.1 zur Primärfunktion der Planung als auch Kapitel 4.2 zur externen Determiniertheit beleuchten bereits Teilaspekte dieser inneren Wirkungszusammenhänge. In Kapitel 4.1 wird die Steuerungsannahme anhand der regelkreisähnlichen Dynamik der Managementaufgaben verdeutlicht. Kapitel 4.2 führt den Begriff der Bedrohung ein. Dieser wird im weiteren Verlauf als zentrales Element in den Wirkungszusammenhängen eines ISMS dargestellt.

4.3 Organisation

Die dritte und vierte Annahme der klassischen Managementtheorie - interne Determiniertheit und Steuerbarkeit - beziehen sich auf die Organisation selbst. Diese Annahme ist im Grunde dieselbe wie die der externen Determiniertheit. Der einzige Unterschied ist, dass sich die interne Determiniertheit auf die Organisation und die externe Determiniertheit auf die Umwelt der Organisation bezieht. Hinzu kommt die Annahme der Steuerbarkeit der Organisation.

An diese Erkenntnisse anschließend, befasst sich der folgende Abschnitt mit der Konstruktion der internen Wirkungszusammenhänge eines ISMS aus Sicht der internen De-

terminiertheit. Hierfür zieht der Abschnitt die Begriffsbildungen aus dem ISO 27000 heran und verbindet sie mit Bezug auf die klassische Managementtheorie. In Abb. 7 ist dieses Modell der Wirkungszusammenhänge eines ISMS grafisch dargestellt:

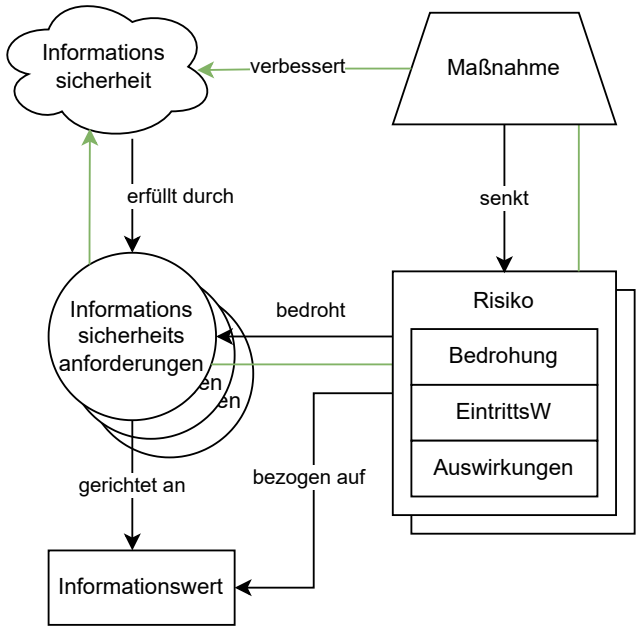

Abbildung 7: Die internen Wirkungszusammenhänge eines ISMS zur Verbesserung der Informationssicherheit auf Basis des ISO 27000 aus einer Perspektive der klassischen Managementtheorie nach Kapitel 3.3 original [SK20].

Die in der Grafik dargestellten Zusammenhänge führt der folgende Absatz aus. Die Begriffe und deren Zusammenhang stammen oder sind abgeleitet aus dem ISO 27000. Der Zweck des ISMS ist laut Definition in Kapitel 4.2.1 [ISO20] die Verbesserung der Informationssicherheit in einer Organisation. Die Informationssicherheit steht im Zusammenhang mit Informationswerten und den (Informations-)Sicherheitsanforderungen (3.56 [ISO20]). Dabei sind die Informationswerte die Entitäten, an welche die zu erfüllenden Erfordernisse oder Erwartungen (Informationssicherheitsanforderungen) gerichtet sind.

Eine beispielhafte Informationssicherheitsanforderung könnte im Bezug auf den Informationswert „Gesundheitsdaten“ lauten: „Die Gesundheitsdaten sind ausschließlich von dem betroffenen Patienten und dem behandelnden Arzt einzusehen.“.Diese Informationswerte unterliegen potenziellen Bedrohungen, welche bei einer Realisierung die Informationssicherheitsanforderungen des Informationswerts gefährden. Wie bereits in Kapitel 4.2 beschrieben, stammen diese Bedrohungen vornehmlich aus der Umwelt der Organisation.

Von Risiken spricht der ISO 27000, wenn eine Bedrohung mit einer bestimmten Ein-

trittswahrscheinlichkeit auf die Informationswerte trifft und zu negativen Auswirkungen führt (vgl. Abbildung, Pfeil rechts und 3.61 Anmerkung 3 und 4 und Ausführungen zur Beurteilung von Risiken 4.5.2 [ISO20]). Die Risiken stehen der Informationssicherheit gegenüber: Sinken die Risiken, steigt die Informationssicherheit und umgekehrt.

Aus Sicht der klassischen Managementtheorie sind formale Maßnahmen das entsprechende Mittel zur Verringerung der Risiken (vgl. Kapitel 3.3.4). Der ISO 27000 definiert die Maßnahmen ebenfalls als „Mittel zur Veränderung der Risiken". Maßnahmen umfassen hierbei laut ISO 27000 „[...] Prozesse (3.54 [ISO20]), Richtlinien, Geräte, Methoden oder anderweitige Handlungen." (3.14 Anmerkung 1 [ISO20]).

Da die Organisation aus klassischer Sicht im Optimum wie eine Maschine funktioniert und die Planung alle relevanten Aspekte für die Verbesserung der Informationssicherheit mit einbezieht, sorgt das Erlassen von Maßnahmen für eine Verringerung der Risiken und somit für eine Verbesserung der Informationssicherheit. Der ISO 27000 schreibt hierzu: „Informationssicherheit wird durch die Umsetzung eines geeigneten Maßnahmenkatalogs erreicht, der durch den festgelegten Risikomanagementprozess ausgewählt und mit Hilfe eines ISMS gesteuert wird" (4.2.3 [ISO20]).

Anders ausgedrückt, lässt sich die Informationssicherheit, deren Verbesserung das Ziel eines ISMS ist, an der Qualität des Maßnahmenkatalogs und dessen Umsetzung bemessen.

Kapitel 4.2 macht bereits darauf aufmerksam, dass sich die Umwelt im klassischen Managementverständnis zwar in die Planung integrieren lässt, allerdings nicht der Steuerung des Plans unterliegt. Somit verändert sich die Umwelt mit der Zeit.

Der ISO 27000 führt in diesem Zusammenhang den Begriff der „Wirksamkeit" als „Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden" (3.20[ISO20]) ein.

Die Veränderung der Wirksamkeit von Maßnahmen begründet der ISO 27000 an einer Stelle mit „wandelnden Umständen" (4.1 [ISO20]). An einer späteren Stelle im Text führt der ISO 27000 an: „Veränderungen der Risiken oder der Strategie und Geschäftsziele der Organisation" (4.5.1 [ISO20]).

Die Veränderung der Wirksamkeit von Maßnahmen adressiert der ISO 27000 wie bereits angemerkt auf zwei Arten: Zum einen ist der Planungsprozess des ISMS iterativ konzipiert (siehe Abb. 4), wodurch die Planung Veränderungen der Umwelt erfasst und in einem neuen Plan adressieren kann (vgl. Kapitel 4.5.1 [ISO20]). Zum anderen betont der ISO 27000 an mehreren Stellen die Notwendigkeit für die Überwachung (3.58 [ISO20]) und die fortlaufende Verbesserung der Wirksamkeit der Maßnahmen (vgl. 4.5.6

/ 7 [ISO20] und Klausel „Verbesserung“ [ISO22]).

4.4 Zusammenfassung

Dieses Kapitel beschäftigte sich mit der Konzeptionierung des ISMS nach der ISO 27000 Reihe auf Basis der klassischen Managementtheorie, wie in Kapitel 3.3 angerissen. In Kürze lässt sich das ISMS nach der ISO 27000 Reihe aus Sicht der klassischen Managementtheorie wie folgt darstellen:

Die Planung fungiert als erste Phase im Managementprozess. Sie bildet den externen Kontext und dessen Bedrohungen, als auch die Organisation in ihren relevanten Aspekten zur Verbesserung der Informationssicherheit ab. Auf Basis dieser Faktoren erstellt die Planung Vorgaben, die ausgehend von den inneren Wirkungszusammenhängen in Abb. 7 die Informationssicherheit verbessern sollen. Die Organisation setzt diesen Plan um und verhält sich größtenteils entsprechend der festgelegten Maßnahmen. Da die Umwelt nicht unter der Kontrolle der Organisation steht, verändert sich die Umwelt über die Zeit. Auch diese Veränderung erfasst das ISMS. Es führt den Planungsprozess iterativ aus und reagiert so mit der Anpassung von bereits eingeführten oder mit neuen Maßnahmen.

5 Limitationen der klassischen Managementtheorie

Das vorangegangene Kapitel 4 bietet eine Sichtweise auf das ISMS gemäß der ISO 27000 Reihe aus einer streng ausgelegten Perspektive der klassischen Managementtheorie.

Dieses Kapitel widmet sich der Kritik an dieser klassischen Theorie, um die Systemtheorie nach Luhmann als geeignetere theoretische Grundlage für das ISMS vorzustellen. Die Kritik basiert auf den Ausführungen im Werk von Schreyögg [SK20], welches sowohl die klassische Managementtheorie darstellt als auch in Kapitel 4.1 kritisiert. Diese Kritik soll einen auf Luhmanns Systemtheorie basierenden Managementprozess motivieren und spiegelt die in dieser Arbeit verfolgte Argumentationslinie für das ISMS wider.

Ein wesentlicher Unterschied liegt jedoch in der Allgemeinheit der Kritik. Während Schreyögg [SK20] die klassische Theorie breit kritisiert, fokussiert sich diese Arbeit konkret auf die Anwendung der Theorie auf das ISMS. Trotzdem lassen sich die allgemeinen Kritikpunkte von Schreyögg in die spezifischen Argumente dieser Arbeit integrieren und auf das ISMS übertragen.

Die folgenden Unterkapitel befassen sich mit jeweils einem zu kritisierenden Aspekt der klassischen Managementtheorie als theoretische Basis für das ISMS.

5.1 Organisation als Maschine

Dieses Unterkapitel kritisiert die Annahme der inneren Determiniertheit und Steuerbarkeit von Organisationen, die grundlegende Elemente der plandeterminierten Unternehmensführung darstellen. Diese beiden Annahmen werden unter dem Bild der „Organisation als Maschine“ zusammengefasst, wie in Kapitel 3.3.4 beschrieben.

Die Autoren von [SK20] kritisieren die Vorstellungen von vollständiger Durchdringbarkeit und Steuerbarkeit einer Organisation als unterkomplex. Sie argumentieren, dass komplexe Organisationen nur bedingt durch Top-down-Planung steuerbar sind (vgl. S. 124 [SK20]).

Um zu demonstrieren, warum diese Planung nicht alle relevanten Aspekte einer Organisation erfassen und gemäß eines solchen Plans steuern kann, zieht dieses Unterkapitel unter anderem die Ergebnisse der „Bank-Wiring Observation Room“-Studie [Han03] heran.

Diese Studie wird von den Autoren in [SK20] im Kontext der verhaltenswissenschaftlichen Schule des Managements vorgestellt (S. 48-56 [SK20]). Diese Richtung stellt eine mehr oder weniger radikale Abkehr von den klassischen Managementansätzen dar (S.

48 [SK20]) und dient somit als Gegenpol zu den Annahmen der klassischen Managementtheorie.

5.1.1 „Bank-Wiring Observation Room“-Studie

Zunächst wird die „Bank-Wiring Observation Room“-Studie mit ihrem Entstehungskontext, ihren Zielen und dem Versuchsaufbau eingeführt, um deren Ergebnisse im Anschluss zu reflektieren:

Die Studie ist Teil einer größeren Versuchsreihe bei Western Electric in Hawthorne, bekannt als die Hawthorne-Experimente. Ziel dieser Experimente war es, die Einflüsse der Arbeitsbedingungen auf die Produktivität von Mitarbeitern zu erforschen. Die verschiedenen Versuche der Hawthorne-Experimente bieten Einblicke in die Wechselwirkung zwischen Management und Ausführung, die oft den Annahmen der klassischen Managementtheorie widersprechen (vgl. Ausführungen zu den Hawthorne-Experimenten, S. 51ff. [SK20]). Für eine Übersicht über alle Hawthorne-Experimente siehe [Han03], S. 85-96.

Die „Bank-Wiring Observation Room“-Studie untersucht den Einfluss von sozialen Interaktionen auf die Arbeitsproduktivität. Der Versuchsaufbau umfasst drei Gruppen von Arbeitern in einem Raum, in dem diese Gruppen Wicklungen für Motoren produzieren, während sie von unparteiischen Beobachtern begleitet werden. Diese Beobachter interagieren weder mit dem Management noch nehmen sie am Produktionsprozess teil, sondern dokumentieren lediglich ausführlich das Verhalten der Mitarbeiter und der Manager.

Die Entlohnung basiert sowohl auf der individuellen als auch auf der Gruppenleistung eines Tages. Die Intention hinter dem Entlohnungssystem ist es, die Mitarbeiter dazu zu bewegen, ihren Tagesumsatz und damit den des Unternehmens zu maximieren (für eine ausführliche Zusammensetzung und Erläuterung des Entlohnungsmodells vgl. [Han03], S. 91-92).

5.1.2 Erkenntnisse aus der Studie

Nach der Erläuterung des Versuchsaufbaus und der damit verbundenen Ziele reflektiert dieser Abschnitt kurz die Ergebnisse hinsichtlich der Annahme der vollständigen Durchdringbarkeit und Steuerbarkeit.

Aus dem beschriebenen Versuchsaufbau heraus sollen die Mitarbeiter die vorgegebenen Maßnahmen umsetzen und somit eine Maximierung des Tagesumsatzes erreichen, zumindest wenn die Annahmen der inneren Determiniertheit und Steuerbarkeit zutreffen würden.

Entgegen diesen plandeterministischen Erwartungen streben die Mitarbeiter jedoch nicht danach, den Tagessatz an Wicklungen zu maximieren. Stattdessen zielen sie darauf ab, einen konstanten und deutlich niedrigeren Tagessatz zu produzieren (vgl. [Han03], S. 93ff.). Dies begründet sich durch die Annahme der Mitarbeiter, dass bei einer Überschreitung des niedrigeren Tagessatzes dieser entsprechend angepasst würde und sie für den gleichen Lohn mehr Wicklungen produzieren müssten. Gleichzeitig achten die Mitarbeiter darauf, dass jede Person die von der Gruppe erwartete Leistung bringt, um eine gerechte Bezahlung zu erwirken.

Um den Tagessatz möglichst konstant zu halten, entwickeln die Arbeiter eigene Mechanismen, wie das Verstecken von Überschüssen oder die physische Disziplinierung mittels „binging“ (starker Schlag gegen den Oberarm) von „Akkordbrechern“ (Arbeiter, die zu viel oder zu wenig Leistung bringen). Darüber hinaus verstoßen die Mitarbeiter gegen die von den Forschern festgelegten Regeln, beispielsweise durch gegenseitiges Unterstützen bei Aufgaben oder das Wechseln von Rollen.

Bis hierhin lässt sich festhalten: Die Organisation verhält sich deutlich komplizierter als eine triviale Maschine, sowohl in Bezug auf die vollständige Durchdringbarkeit als auch die Steuerbarkeit. Diese Aspekte sollen in den folgenden Abschnitten noch weiter vertieft werden.

5.1.3 Steuerbarkeit

In Bezug auf das Steuerungsverständnis der klassischen Managementtheorie lässt sich an den Beobachtungen der „Bank-Wiring-Observation-Room“-Studie erkennen, dass die Mitarbeiter den „Steuerungsimpulsen“ des Managements nur bedingt Folge leisten.

Zwar produzieren sie die von der Unternehmensleitung gewünschten Motorwicklungen, jedoch nicht in dem von den Maßnahmen des Managements vorgesehenen Umfang. Stattdessen bilden die Mitarbeiter ihre eigenen Strukturen, die mehr oder weniger im Einklang mit den Maßnahmen des Managements stehen und ihre eigenen Ziele und Bedürfnisse berücksichtigen. Die Umsetzung und Ausführung[15] der im Plan festgelegten Maßnahmen gestaltet sich somit deutlich komplexer, als es das maschinenartige Modell der klassischen Managementtheorie zu erklären vermag.

Darüber hinaus sei angemerkt, dass die Planung sich diesem Umstand nicht einmal bewusst sein muss. Das Management in der „Bank-Wiring Observation Room“-Studie ist beispielsweise nicht darüber informiert, dass die beschriebenen informellen Strukturen der Mitarbeiter existieren. Aus Sicht des Managements funktionieren die erlassenen

[15] Siehe die Phasen Umsetzung und Ausführung in Kapitel 4.1

Regelungen wie durch den Plan intendiert, wobei sich die Organisation wie in einem Regelkreis steuern lässt (vgl. Abb. 6).

Die klassische Managementtheorie geht somit davon aus, dass sie die Dynamiken mit ihrer Steuerungskonzeption von Ursache (Maßnahme) und daraus folgender Wirkung (Umsetzung und Verbesserung der Informationssicherheit) einfängt, obwohl sich die tatsächlichen Mechanismen deutlich komplexer darstellen.

Diese Begrenzung mag für ein pragmatisches, handlungsorientiertes Verständnis der Organisation in einem stabilen Umfeld ausreichen, jedoch limitiert dieser Pragmatismus die Erklärbarkeit der Theorie in Bezug auf die tatsächlichen Dynamiken des ISMS.

5.1.4 Informelle Strukturen

Die klassische Managementtheorie ignoriert die angesprochenen informellen Strukturen nicht, konzeptioniert sie jedoch in erster Linie als Abweichung von der intendierten Planung, unter dem Begriff „Implementationsprobleme“. Der Begriff umfasst nach den Autoren von [SK20] alle Abweichungen in der Umsetzung und Ausführung von der intendierten Planung.

Überspitzt formuliert stellen alle formalen Maßnahmen, die im Rahmen der Planung festgelegt werden, die „guten“ maschinenartigen Verhaltensweisen der Organisation dar.[16] Die informellen Strukturen hingegen sind Abweichungen von diesem durch die Planung vorgegebenen Verhalten und schwächen die maschinenartige Funktionsweise der Organisation ab. Da die Organisation als Maschine das zu erreichende Optimum darstellt, sind die informellen Strukturen somit als Problem „schlecht“ zu bewerten.

Folgerichtig gilt aus einer klassischen managementtheoretischen Sicht: „Informationssicherheit wird durch die Umsetzung eines geeigneten Maßnahmenkatalogs erreicht“ (4.2.3 [ISO20]).

Diese Konzeption mag, wie die oben erwähnte Simplifizierung der Organisationssteuerung auf einen Regelkreis, für ein pragmatisches, handlungsorientiertes Organisationsverständnis geeignet sein, jedoch ist sie in ihrer Erklärbarkeit als weite theoretische Basis eingeschränkt.

Die Autoren von [SK20] führen dazu aus:

> Alle konstitutiven Grundmerkmale sozialer Systeme, wie z. B. sich selbstverstärkende Dynamiken, die Vernetztheit der faktischen Arbeitsvollzüge, die vielfach divergierenden Interessen der Organisationsmitglieder, die systemintern vorfindbare und funktional erforderliche Bandbreite von Perspektiven

[16] Siehe auch Kapitel 3.3.4 für die Ausführung der Organisation als Maschine

und Orientierungsmustern etc., werden nicht nur ausgeblendet, sondern sogar negiert. (S.126 [SK20])

Die Vierfeldertafel in Abb. 8 visualisiert diese Einschränkung.

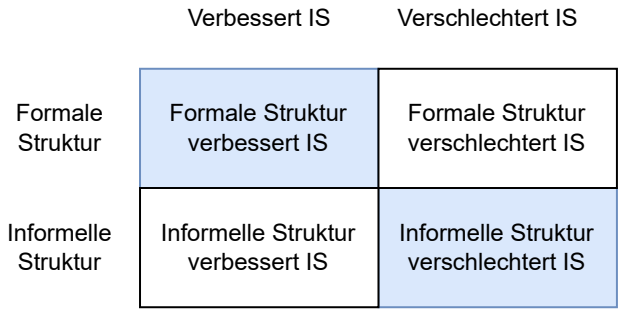

Abbildung 8: Vierfeldertafel mit allen möglichen Kombinationen von informellen/formalen Strukturen und Verschlechterung/Verbesserung der Informationssicherheit (IS). Hellblau sind die Kästen, welche das klassische Management im Rahmen ihres Maschinenmodells zugrundelegt.

Sie zeigt die möglichen Kombinationen von formalen und informellen Strukturen als Gegensätze, mit der Verbesserung und Verschlechterung der Informationssicherheit. Strukturen, die neutral zur Informationssicherheit stehen, betrachtet die Grafik bewusst nicht, da diese nicht im Fokus dieses Unterkapitels stehen.

Die klassische Managementtheorie erklärt mit ihrer Konzeption von Informationssicherheit durch die Umsetzung eines Maßnahmenkatalogs und Abweichungen von diesem als Implementationsprobleme in erster Linie die beiden hellblau hinterlegten Felder der Vierfeldertafel.

Die weiß hinterlegten Felder in Abb. 8 zeigen die Aspekte, die sich unter den obigen Annahmen der klassischen Managementtheorie schwer abbilden lassen. Hierzu gehören zum einen Fälle, in denen erlassene Sicherheitsmaßnahmen zu einer Verschlechterung der Informationssicherheit führen (rechtes oberes Feld). Zum anderen gehören hierzu Fälle, in denen informelle Strukturen kein Problem für die Verbesserung der Informationssicherheit darstellen, sondern diese potenziell sogar verbessern (linkes unteres Feld).

Die folgenden Abschnitte zeigen die Notwendigkeit auf, auch die von der klassischen Managementtheorie nur schwer abbildbaren Dynamiken einzufangen.

Formale Strukturen als Ursache für die Verschlechterung der Informationssicherheit Um zu veranschaulichen, warum formale Maßnahmen zur Verbesserung der Informationssicherheit paradoxerweise zu einer Verschlechterung derselbigen führen können,

zieht dieser Abschnitt das in Kapitel 2.4 von verschiedenen organisationspsychologischen Arbeiten [AS99] [IS10] [Hie+22] verwendete Beispiel der Passwortrichtlinien heran:

In dem Beispiel erlässt die Planung neue Passwortrichtlinien, die für eine Verbesserung der Informationssicherheit sorgen sollen. Die Mitarbeiter können sich diese neuen „komplizierten“ Passwörter nicht merken, weshalb sie sich gezwungen sehen, die Passwörter in Klartext auf Papier oder in Textdateien zu notieren.

Zwar würde sich gemessen an der Umsetzung der Maßnahme (Einführung der Passwortrichtlinie) die Informationssicherheit verbessern, allerdings ist fraglich, ob die informelle Struktur, also das Speichern der Passwörter auf unverschlüsselte Weise, wirklich zu einer besseren Informationssicherheit beiträgt.

Im PDCA-Zyklus aus Kapitel 3.2 könnte diese Abweichung durch einen tiefgreifenden CHECK, beispielsweise im Rahmen einer Prüfung, auffallen und auf eine sinnvolle Verbesserung drängen, woraufhin das Management in der ACT-Phase mit einer weiteren Maßnahme reagieren könnte, welche diese Praktiken untersagt.

Allerdings könnten die Mitarbeiter auch hierauf wieder reagieren, um das Problem des Merkens der komplexen Passwörter zu umgehen. Beispielsweise mit dem Neu-Beantragen über den „Passwort vergessen“-Knopf bei jedem Login oder schlicht dem Verstoß gegen die Maßnahme.[17]

Die Autoren von [SK20] machen auf Seite 54 ferner darauf aufmerksam, dass informelle Strukturen stets ein Teil der Organisation sind. Folgt man dieser Feststellung und betrachtet die negative Sicht der klassischen Managementtheorie auf informelle Strukturen als Probleme, so ergibt sich, dass die klassische Managementtheorie grundsätzlich gegen einen ständig vorhandenen Teil der Organisation ankämpft.

Dies kann im schlimmsten Fall zu einer stetigen Zunahme von Regulierungen innerhalb der Organisation führen, wie im Beispiel zu erkennen ist und später in Kapitel 6.2 weiter erläutert wird.

Die Autoren von [Hie+22] führen zur Überregulierung aus, dass eine Informations- und Compliance-Überlastung durch eine solche Überregulierung zu einer Verschlechterung der Informationssicherheit führen kann. Die Mitarbeiter möchten sich bei einer Überlastung an keine der Informationssicherheitsmaßnahmen mehr halten und versuchen, diese zu umgehen. Das „Compliance Budget“ [BSW08] der Mitarbeiter ist sozusagen überschritten.[18]

An den Beispielen lässt sich erkennen, dass das Erlassen von weiteren Informati-

[17] Für eine grundlegende Kritik an dem PDCA-Zyklus und dem modernen Managementverständnis siehe [Kri24], sowie [Min05].

[18] Siehe hierzu Kapitel 2.4

onssicherheitsmaßnahmen entgegen der Erwartung der klassischen Managementtheorie nicht zu einer Verbesserung der Informationssicherheit, sondern im Gegenteil zu einer Verschlechterung führt.

Die klassische Managementtheorie würde die „Schuld“ für die Verschlechterung der Informationssicherheit bei der mangelnden Umsetzung der erlassenen Maßnahmen und damit bei den informellen Strukturen sehen.

Diese Sichtweise vernachlässigt allerdings die Planung als Ursache dieser Probleme, wie beispielsweise durch die resultierenden unmerkbaren Passwörter oder die schlichte Überlastung der Organisation mit Richtlinien.

Für eine umfassende theoretische Basis des ISMS wäre es nötig, sowohl die formalen Maßnahmen als auch die informellen Maßnahmen als Verursacher für die Verbesserung und Verschlechterung der Informationssicherheit betrachten zu können.

Informelle Strukturen als Treiber der Verbesserung von Informationssicherheit Die bisher angeführten Beispiele der „Bank-Wiring-Observation-Room“-Studie und der Passwortrichtlinien können den Anschein erwecken, dass die informellen Strukturen aus späteren Phasen des Managementprozesses die Ziele der Planung tatsächlich nur konterkarieren. Somit wäre die vornehmlich negative Auslegung von Abweichungen des Plans gerechtfertigt. Um diesem Trugschluss zu begegnen, zieht der folgende Abschnitt erneut das Beispiel der Passwortrichtlinien heran:

Der gestiegene Aufwand durch die neuen Passwortrichtlinien könnte einige Mitarbeiter auf die Idee bringen, einen Passwortmanager zu verwenden (vgl. 4.1 [Hie+22]). Die Motivation der Mitarbeiter ist hierbei, dass sie sich nicht alle neuen, komplexeren Passwörter merken müssen, sondern lediglich das Passwort, mit dem sie die verschlüsselten Passwörter entschlüsseln. Dabei sorgt die Verschlüsselung gleichzeitig dafür, dass das Risiko einer unbefugten Einsicht geringer ist als bei einer Speicherung in einer unverschlüsselten Textdatei. Folgerichtig wird hierdurch die Informationssicherheit verbessert, was das übergeordnete Ziel eines ISMS nach ISO 27000 ist und damit auch der formalen Maßnahmen entspricht.

Dieses Beispiel zeigt, dass die bei der Umsetzung und Ausführung entstehenden informellen Strukturen nicht nur „Störfaktoren“ bei der Verbesserung der Informationssicherheit darstellen. Die informellen Strukturen können mit den Zielen der Planung koexistieren, ohne diese negativ zu beeinflussen. Weiterhin sind die Phasen der Umsetzung und Ausführung in der Lage, die Ziele der Planung sogar besser als die eigentlich beschlossenen Maßnahmen umzusetzen. Die Nutzung des Passwortmanagers geschieht

in diesem Beispiel nicht als Umsetzung einer in der Planungsphase definierten Maßnahme. Die Idee der Nutzung eines Passwortmanagers und die Umsetzung stammen von den Mitarbeitern selbst, um sowohl ihre eigenen Bedürfnisse als auch den Erwartungen der Organisation zu entsprechen.

Für eine umfassende theoretische Basis des ISMS benötigt es eine Theorie, welche diese Dynamiken abbilden kann.

5.1.5 Fazit

Zusammenfassend zeigt dieses Unterkapitel die Grenzen der klassischen Managementtheorie in der Erklärbarkeit von informellen Strukturen auf. Diese Begrenzung resultiert aus der Definition der Organisation als eine Entität, die vollständig durch einen Plan erfassbar und steuerbar ist, inkl. der daraus resultierenden Folgerungen. Die Steuerbarkeit setzt eine maschinenartige Befolgung des formulierten Plans voraus, was jegliche Abweichung von dem Plan als Implementationsproblem darstellt.

Die vergleichsweise simplen Dynamiken in den hier angeführten Beispielen zeigen, dass ein solches „Schwarz-Weiß-Denken“ von formalen Maßnahmen als die „Guten“, welche die Informationssicherheit verbessern, und informellen Strukturen als die „Schlechten“, welche die Informationssicherheit gefährden, die Erklärbarkeit der klassischen Managementtheorie stark beschränkt.

Sowohl die formalen Maßnahmen als auch die informellen Strukturen können zur Verbesserung der Informationssicherheit, aber auch zu deren Verschlechterung führen.

Eine umfassende theoretische Basis sollte in der Lage sein, auch die oben benannten Dynamiken abzubilden.

5.2 Passive Umwelt

Dieses Unterkapitel kritisiert die Konzeption der Umwelt aus klassisch managementtheoretischer Perspektive. Hierfür führt es zunächst die klassisch managenttheoretische Konzeption der Umwelt auf und zeigt, wie sich diese in den klassischen Managementprozess aus Abb. 5 einfügt. Anschließen kritisiert dieses Unterkapitel die Annahmen, welche dieser Umweltkonzeption stützen und zeigt deren Folgen für die Erklärbarkeit auf.

5.2.1 Die Umwelt in der klassischen Managementtheorie

Die Umwelt nimmt in der plandeterminierten Unternehmensführung in erster Linie die Rolle einer Quelle von in der Planung zu beachtenden Faktoren ein. Kapitel 4.2 fasst

zusammen, dass die Umwelt im ISMS zum einen stabile externe Faktoren (beispielsweise Gesetze) und zum anderen Bedrohungen liefert.

Beides erfasst, erklärt und prognostiziert die Planung genauso, wie sie dies in Bezug auf die Organisation tut. Somit lässt sich die Umwelt genauso in den Plan integrieren wie die relevanten Dynamiken der Organisation.

Im Gegensatz zur Organisation lässt sich die Umwelt zwar nicht durch die Planung steuern, wodurch sich deren Veränderung der Kontrolle des Plans entzieht. Allerdings verändert sich die Umwelt in der strikten Auslegung des letzten Kapitel 4.2 nur so, dass sich die Veränderungen mittels des Managementprozesses wieder einfangen und in die nächste Planung integrieren lassen.

Sollten die Ergebnisse am Ende des Managementprozesses nicht mit den geplanten Ergebnissen übereinstimmen, beispielsweise indem sich die Umwelt verändert, adressiert der klassische Managementprozess diese Abweichungen in der nächsten Iteration mit einem neuen Plan.[19]

5.2.2 Kritik an der Annahme der externen Determiniertheit

Das vorherige Kapitel 5.1 kritisiert ein solch allumfassendes Planungsverständnis in Bezug auf die Organisation als verkürzt. Die Ergebnisse der „Bank-Wiring-Observation-Room“-Studie demonstrieren beispielsweise, dass sich die Organisationsmitglieder nicht determiniert, entsprechend einer Planung verhalten.

Diese Kritik an diesem allumfassenden Anspruch greift ebenfalls bei der Umwelt. Denn auch die Umwelt besteht „zum erheblichen Teil aus handelnden Personen und Organisationen“ (S.123 [SK20]).

Zu den Akteuren der Umwelt gehören in der klassischen Interpretation nicht die Mitglieder der Organisation.[20]

Als Herausstellungsmerkmal gegenüber einer regulären Organisation- und Umweltbetrachtung befasst sich das ISMS insbesondere mit feindlich gesinnten Akteuren als Quelle von Bedrohungen. Beispielsweise definiert Eckert auf den Seiten 23ff. in [Eck23] verschiedene Angreifer-Typen zu denen unter anderem Hacker und Skript Kiddies, aber auch Wirtschaftsspionage und allgemeinen Kriminelle zählen.

Die benannten Umstände sorgen gleich auf zwei Arten dafür, dass sich die Umwelt gegenüber der Organisation potenziell noch weniger determinieren lässt.

[19] Siehe für eine ausführlichere Erklärung des klassischen Managementprozesses Kapitel 3.3.2

[20] Luhmann definiert auch die Mitglieder der Organisation als Teil der Umwelt und unterscheidet sich somit von der klassischen Auffassung. Siehe Kapitel 6.3.

Der erste Umstand ist, dass die Probanden aus der Studie als Mitglieder der Organisation den Zielen der Organisation verpflichtet sind (vgl. „Theory of Authority“ [BA02] Kapitel zwölf). Die Mitarbeiter haben entsprechend ein Interesse daran, die Maßnahmen zumindest scheinbar umzusetzen und tun dies, gemessen am Unwissen des Managements (vgl. Kapitel 5.1), erfolgreich über die informellen Strukturen.

Für Akteure der Umwelt gilt diese Verpflichtung gegenüber den Zielen der Organisation nicht. Insbesondere für Angreifer liegt es nicht in deren Interesse, mit dem Planungsprozess des Managements zu kooperieren. Denn dieser soll explizit dafür sorgen, dass die Angreifer von dem Erreichen ihrer Ziele, wie beispielsweise die Störung der IT-Systeme der Organisation, abgehalten werden.

Weiter ist das Handeln der feindlichen Akteure, als kriminelle Organisationen oder Personen, aller Wahrscheinlichkeit nach nur bedingt durch Gesetze limitiert.

Durch beide Umstände gestalten sich die Handlungsmöglichkeiten der Angreifer potenziell anders und vielfältiger als die der Organisationsmitglieder. Bereits in dem vergleichsweise einfachen Organisationsaufbau der „Bank-Wiring-Observation-Room“-Studie konnte das vorherige Kapitel 4.3 die Annahme der Determinierbarkeit als unterkomplex darstellen. Es ist somit fraglich, ob sich bei einer komplexeren Organisation die im Vergleich zu dieser Organisation komplexere Umwelt in den klassischen Managementprozess eingliedern lässt.

5.2.3 Folgen

Angenommen, die externe Determinierbarkeit wäre nicht gegeben, wie im vorherigen Abschnitt argumentiert. Dies hätte Implikationen für die Eignung der plandeterminierten Unternehmensführung und deren Managementprozess als konzeptionelle Basis für die Erklärung der Organisation.

Das Fehlen einer externen Determinierbarkeit bedeutet, dass sich relevante Aspekte der Umwelt nicht in der Planung abbilden lassen. Es bleiben somit immer relevante „blinde Flecken“ zurück, welche von der aktuellen Planung nicht bedacht wurden.

Das spätere Kapitel 6.3 reflektiert diese blinden Flecken und deren Implikationen auf die Verbesserung der Informationssicherheit tiefgreifender. Für die Kritik der klassischen Managementtheorie in diesem Abschnitt reicht es aus, darauf hinzuweisen, dass durch deren Existenz die dauerhafte Gefahr besteht, dass Informationssicherheitsvorfälle eintreten, obwohl alle von der Planung erfassten Schwachstellen mit Maßnahmen bedacht und diese korrekt umgesetzt und befolgt werden.

Kapitel 6 weist bereits darauf hin, dass das klassische ISMS vornehmlich eine präventive

Perspektive einnimmt und alle Herausforderungen im Vorhinein bedenkt und adressiert. Dass ein neuartiger Informationssicherheitsvorfall eintritt, kann die klassische Managementtheorie lediglich als eine Abweichung vom Maßnahmenkatalog abbilden, welche durch einen SOLL/IST-Vergleich identifiziert und dann mittels eines neuen Plans adressiert wird.

Diese Darstellung bietet zwar eine pragmatische Sichtweise für den Umgang mit solchen Situationen, limitiert allerdings stark die Erklärbarkeit der zugrunde liegenden Dynamiken, wie es bereits im vorherigen Kapitel 5.1 mehrfach dargestellt wurde.

Eine dieser Limitierungen zeigt sich beim Versuch, formale Maßnahmen zur Verbesserung der Informationssicherheit als potenzielle Quelle für die Verschlechterung der Informationssicherheit zu erfassen, wie in Kapitel 5.1.4 ausgeführt. Diese Limitation lässt sich ebenfalls im Hinblick auf die Limitation der Umwelt betrachten:

Ein Beispiel hierfür wäre die offizielle Zertifizierung einer Organisation nach ISO 27001. Damit wäre für Angreifer offengelegt, dass die Organisation einem dokumentierten Planungsprozess folgt. Diese Information kann der Angreifer in seinem Angriff nutzen und gezielt nach den Dokumenten für die hinterlegten Sicherheitsmaßnahmen suchen. Beispielsweise könnte der Angreifer die verabschiedeten Richtlinien zur Verbesserung der Informationssicherheit für Mitarbeiter für einen informierten Social-Engineering-Angriff verwenden.

Besonders kritisch wäre es, wenn Angreifer die Liste der abzustellenden Schwachstellen bzw. die Liste der zu implementierenden Maßnahmen finden. Der ISO 27000 macht selbst darauf aufmerksam, dass die Umsetzung von Maßnahmen Zeit benötigt (vgl. 4.5.5 [ISO20]). Bei einer relativ neuen Zertifizierung können Maßnahmen noch nicht vollständig umgesetzt worden sein, was die Organisation zu einem noch attraktiveren Ziel für Angreifer macht. Insbesondere wenn die Zertifizierung unter Auflagen geschehen ist und diese womöglich nicht nur in der zertifizierten Organisation, sondern auch bei der Zertifizierungsgesellschaft, dem BSI usw. vorliegen.

An diesen beiden Beispielen lässt sich erkennen, dass die klassische Managementtheorie die aktive Rolle der Umwelt kategorisch unterschätzt.

5.2.4 Fazit

Zu den vorangehenden Abschnitten lässt sich festhalten, dass die Annahme der externen Determiniertheit, wie auch schon die Annahme der internen Determiniertheit, eine zu starke Vereinfachung für eine umfassende theoretische Basis des ISMS darstellt. Eine solche Annahme erschwert insbesondere die differenzierte Betrachtung von eintretenden

Informationssicherheitsvorfällen und unterschätzt die aktive und dynamische Rolle der Umwelt des ISMS.

5.3 Zusammenfassung

Dieses Kapitel hat sich mit einigen ausgewählten Kritikpunkten befasst, die sich aus der Konzeptionierung des ISMS auf Basis der klassischen Managementtheorie ergeben. Alle Abschnitte befassen sich im Kern mit demselben Problem: „Eine Organisation in ihrer Umwelt lässt sich nicht vollständig mittels eines Plans beschreiben und infolgedessen auch nicht steuern“. Beide Abschnitte kommen über verschiedene Aspekte zum selben Ergebnis: Die Konzeptionierung des ISMS auf Basis der klassischen Managementtheorie ist für die Beschreibung der in der Praxis auftretenden Herausforderungen nicht hinreichend komplex und vernachlässigt wichtige Aspekte und dynamische Entwicklungen in und um die Organisation. Damit diese Aspekte ebenfalls abgebildet werden können, benötigt es eine andere theoretische Basis als die klassische Managementtheorie.

6 ISMS nach Luhmanns Systemtheorie

Dieses Kapitel behandelt die Systemtheorie nach Niklas Luhmann als theoretische Basis für das Thema ISMS.

Im Kontext dieser Arbeit ist dieses Kapitel das letzte Glied in einer Kette von drei Kapiteln:

- Kapitel 4 hat die Erklärbarkeit der klassischen Managementtheorie ausführlich dargestellt. Dabei wird deutlich, dass die klassische Managementtheorie einen Großteil der aktuellen Begriffsbildung des ISMS erfassen kann. Zudem betont sie mit ihrem pragmatischen Erklärungsansatz, der insbesondere auf einem umfassenden und detaillierten Plan basiert, die Handlungsfähigkeit des Managements zur Verbesserung der Informationssicherheit.

- Aufbauend auf der ausführlichen Darstellung des klassischen ISMS kritisiert Kapitel 5 diese Theorie als zu simpel. Relevante Dynamiken des ISMS werden durch die Annahmen der klassischen Managementtheorie nicht ausreichend erklärt.

- Dieses Kapitel greift die Kritikpunkte aus Kapitel 5 auf und zeigt, dass die Systemtheorie nach Luhmann in der Lage ist, auch diese Dynamiken abzubilden.

Dieses Kapitel behandelt sowohl die Frage, wie sich die Erklärbarkeit der Systemtheorie nach Luhmann von anderen Theorien unterscheidet, als auch die Frage, welche spezifischen Dynamiken des ISMS sich mit der Systemtheorie nach Luhmann abbilden lassen.[21]

Der Vorteil einer differenzierteren und umfangreicheren Erklärbarkeit durch die Systemtheorie liegt insbesondere darin, dass sich damit Herausforderungen der Praxis erfassen lassen, die sich sonst der Beobachtung entziehen würden. Dadurch dass diese Fragestellungen überhaupt erst beobachtet werden können, ist es ebenfalls möglich, für diese Lösungen zu entwickeln. [22] Dieses Kapitel zeigt insbesondere, wie die Systemtheorie besagte Herausforderungen und allgemeine Dynamiken des ISMS sichtbar macht. Die Entwicklung konkreter Handlungsmöglichkeiten wird im Rahmen dieser Arbeit nur skizziert und stellt eine mögliche Weiterentwicklung dieser Thesis dar (vgl. Kapitel 7.2).

Nachdem die Zielsetzung dieses Kapitels eingegrenzt ist, befasst sich der weitere Abschnitt mit der Struktur des Kapitels ein. Es gliedert sich in drei Unterkapitel, die sich mit unterschiedlichen Aspekten der Systemtheorie befassen:

[21] Vergleiche hierzu die Teilfragen zwei und drei der Problemstellung in Kapitel 1.2
[22] Siehe hierzu auch die Ausführungen zur Grundlagenforschung in Kapitel 1.1.2

1. zeigt Überlegungen, wie sich Management als Steuerungsaufgabe und Systemtheorie nach Luhmann mit selbststeuernden Systemen zusammenführen lassen.

2. greift die Kritikpunkte von Kapitel 5.1 zur limitierten Erklärbarkeit der klassischen Managementtheorie in Bezug auf die Organisation auf. Dabei zeigt das Kapitel, wie die Systemtheorie nach Luhmann die Lücken in der Erklärbarkeit der klassischen Managementtheorie schließen kann.

3. verfolgt dasselbe Ziel, die Limitationen der klassischen Managementtheorie durch die bessere Erklärbarkeit der Systemtheorie zu adressieren. Das Kapitel greift hierbei jedoch die Kritik aus Kapitel 5.2 auf, welche die Mängel in der Erklärbarkeit der Umwelt thematisiert.

Bevor die einführenden Überlegungen eingeleitet werden, muss kurz erläutert werden, warum es keine allgemeine Einführung zur Systemtheorie in Kapitel 3 gibt, wie dies beispielsweise für die klassische Managementtheorie in Kapitel 3.3 der Fall ist. Diese Entscheidung ist dem Umfang und der damit einhergehenden Komplexität der Systemtheorie nach Luhmann geschuldet. Die Theorie erstreckt sich über mehrere Werke, darunter die Dissertation „Funktionen und Folgen formaler Organisationen“ [Luh99]mit 435 Seiten und spätere Werke wie „Soziale Systeme: Grundriss einer allgemeinen Theorie“ [Luh21] mit 666 Seiten, sowie „Organisation und Entscheidung“ [Luh11] mit 478 Seiten. Stattdessen führt dieses Kapitel die erforderlichen Aspekte der Theorie in einem angemessenen Umfang ein. Angemessen bedeutet hierbei, dass die Einführung der Theorie nur soweit erfolgt, dass die im folgenden besprochenen Aspekte im Sinne der Theorie eingeordnet sind. Für eine umfassende Einführung sei an dieser Stelle auf die genannten Arbeiten verwiesen, sowie die Einführungswerke von Simon [Sim23] und Kühl [Kü11].

6.1 Einführende Überlegungen

Dieses Unterkapitel grenzt den Organisationsbegriff Luhmanns von dem der klassischen Managementtheorie ab. Diese unterscheiden sich fundamental in ihren Grundannahmen. Ausgehend von diesen grundlegenden Unterschieden in der Organisation befasst sich das Kapitel ferner mit der Frage, wie sich der Managementbegriff zwischen den beiden Theorien unterscheidet. Diese Überlegungen bereiten die Grundlage für die Betrachtungen der nächsten Abschnitte, welche demonstrieren, wie ein systemtheoretischer Organisations- und Managementbegriff zu einer gesteigerten Erklärbarkeit im Bezug auf das ISMS führt.

6.1.1 Organisationen in der Systemtheorie nach Luhmann

Die Systemtheorie versteht Organisationen grundlegend anders als die klassische Managementtheorie. Zur Erinnerung: Die klassische Managementtheorie idealisiert die Organisationen als trivial funktionierende Maschinen. Trivial bedeutet vereinfacht zusammengefasst, dass die Organisation die Anweisungen des Managements im weitesten Sinne umsetzt und ausführt. Zusätzlich lassen sich alle Dynamiken außerhalb des Plans hinreichend als eine Abweichung von diesen Vorgaben modellieren (Kapitel 3.3.4).[23]

Dem gegenüber definiert Luhmann Organisationen als autopoietische Systeme, was im folgenden kurz erklärt wird: In „Organisation und Entscheidung“ [Luh11] beschreibt Luhmann auf den Seiten 44 bis 56 den Begriff der Autopoiesis im Sinne seiner Theorie. Dieser Abschnitt erklärt deshalb nur kurz den Ursprung und die Bedeutung des Begriffes Autopoiesis sowie dessen relevante Auswirkungen für die Analysen in diesem Kapitel. [24]

Der Begriff „Autopoiesis“ setzt sich aus dem Griechischen „auto“ (selbst) und „poiesis“ schöpferische Tätigkeit zusammen. Er beschreibt den Prozess der Selbsterschaffung und wurde von dem Biologen Humberto Maturana begründet (S.280 [Mat87]). Mit Selbsterschaffung ist gemeint, dass die Entität sich selbstständig erzeugt und erneuert, wie bei einem Lebewesen der Stoffwechselprozess die Lebensfähigkeit aufrecht erhält.

Luhmann überträgt dieses Konzept auf die Organisation: Organisationen in Luhmanns Theorie sind selbsterzeugende soziale Systeme. Dies ist für diese Thesis besonders wichtig, da mit der Selbsterzeugung auch eine *Selbststeuerung* der Organisation einher geht.

Der Gedankengang zur Verbindung von Selbsterzeugung und Selbststeuerung lässt sich unter Zuhilfenahme der Unterscheidung von trivialen und nicht-trivialen Maschinen nach Heinz von Foerster veranschaulichen. Luhmann beschreibt deren Unterschiede wie folgt:

> Trivial sind Maschinen ohne Selbstbeobachtung, die von außen eingesetzte Funktionen vollziehen und deshalb bei gleichen Eingabe/Inputs immer die gleichen Ausgaben produzieren. Nichttrivial sind dagegen „historische“ Maschinen, die bei all ihren Operationen immer erst den Zustand konsultieren müssen in dem sie sich selbst dank vorheriger Operationen gerade befinden. Und auch von diesen nichttrivialen Maschinen gilt, dass sie unausrechenbar komplex sind, also so behandelt werden müssen (durch sich selbst oder durch

[23] Siehe auch S.379 [Luh11]

[24] Der Abschnitt nimmt hierbei Bezug auf die kürzere und an Beispielen veranschaulichte Einführung zu Organisationen als autopoietische Systeme in [Sim23] Kapitel 2.3

andere Beobachter), als ob sie frei entscheiden könnten.(S.73f [Luh11] bzw im Original Heinz von Foerster S.233-268 [Foe93]).

Die klassische Managementtheorie versteht die Organisation, wie eingangs erwähnt, im Wesentlichen als triviale Maschine, welche auf die Eingaben des Managements aller Voraussicht nach mit den zu erwartenden Ausgaben reagiert.

Für die Argumentation greift die vorliegende Arbeit diesen Aspekt der Selbststeuerung heraus. Die Selbststeuerung ist demnach eine Folge der Eigenkomplexität der Organisation, die ein vollständiges Überblicken unmöglich macht. Die Organisation führt gewissermaßen ein „Eigenleben“, das in jedem Fall erhalten bleibt. Eine direkte Steuerung der Organisation, wie bei einer trivialen Maschine, wird schlichtweg unmöglich.

Die Selbststeuerung bildet damit den fundamentalen Unterschied zur maschinenartigen Organisationsdefinition der klassischen Managementtheorie, welche vom Management gesteuert wird. Wie im Verlaufe der weiteren Kapitel zu sehen sein wird, bildet die Grundannahme der Selbststeuerung eine breitere Erklärungsbasis im Gegensatz zur klassischen Managementtheorie.

6.1.2 Selbststeuernde Organisationen und Management

Vor dem Hintergrund der selbststeuernden Organisation stellt sich die Frage, wie die Systemtheorie nach Luhmann überhaupt als Grundlage für ein Informationssicherheits*management*system dienen kann. Denn bis hierhin wurde Management als eben diese Steuerungsaufgabe im Verständnis einer trivialen Maschine „Organisation“ durch das Management verstanden.[25] Es ist entsprechend nicht offensichtlich, wie sich das Management der Informationssicherheit in der Selbststeuerung von Organisationen einordnen lässt.

Auf diese Problematik machen auch Schreyögg et al. in ihrer Diskussion über „Offene Fragen“ der Systemtheorie im Zusammenhang mit Management aufmerksam (Kapitel 4.2.3 [SK20]). Die Autoren überlegen hierbei, wie sich Management als Steuerungsaufgabe und die Selbststeuerung der Systemtheorie zusammenführen lassen. Sie schlagen vor, die Systemtheorie verständnisorientiert zu verwenden.

Wie eine verständnisorientierte Verwendung aussehen kann, schildern die Autoren von [KE06] in ihrer Diskussion darüber, wie Fremdsteuerung durch Management und Selbststeuerung durch die Organisation zusammenpassen:

Das hindert nicht, seinem Werk inspirierendste Einsichten auch in Sachen

[25] Siehe für die Bedeutung des Begriffs Management in der klassischen Managementtheorie Kapitel 3.3.1

> Steuerung und Management abzugewinnen, besonders: Warnungen vor Illusionen in Sachen Plan- und Steuerbarkeit sozialer Systeme und die Auffassung jedweden Managements als „Kontingenzmanagement“ ([LK19]: 152 ff.).

Die Autoren sehen die Rolle der Systemtheorie für das Management damit als eine Art Schutzmechanismus vor den idealisierenden Annahmen der klassischen Managementtheorie.

Weitere verständnisorientierte Nutzungen der Systemtheorie finden sich in unterschiedlichsten Anwendungsdomänen. Die Systemtheorie wird beispielsweise in der Prüfung von Organisationen [AH22], der Organisationsberatung [KE19] und der Therapie [SRS21] erfolgreich verwendet.

Diese Thesis folgt diesem Beispiel und nutzt die Systemtheorie ebenfalls verständnisorientiert zur Analyse von ausgewählten Dynamiken des ISMS, welche anhand der klassischen Managementtheorie nicht hinreichend differenziert begriffen werden konnten.

6.2 Organisation als autopoietisches System

Nachdem der Kernunterschied mit der Selbststeuerung der Organisation hinreichend beschrieben ist, gilt es nun die Kritikpunkte aus dem vorherigen Kapitel 5 zu adressieren. Dieses Kapitel beschäftigt sich hierbei mit den Kritikpunkten an dem idealisierten Organisationsverständnis (vgl. Kapitel 5.1). Dieses ist nicht in der Lage, informelle Strukturen hinreichend abzubilden und übersieht somit relevante Dynamiken zur Verbesserung der Informationssicherheit. Diese Unfähigkeit gründet in dem Verständnis der inneren Determiniertheit, d.h. die Organisation maschinenartig verstehen und steuern zu können (vgl.Kapitel 4.3).

Die Steuerung der Organisation erfolgt in der klassischen Managementtheorie vornehmlich über formale Maßnahmen, wie beispielsweise im ISO 27000 angeführt: „Informationssicherheitspolitik, -verfahren und -richtlinien“ (4.2.4 [ISO20]). Alles neben dieser Steuerung fasst die klassische Managementtheorie als Implementationsproblem oder Störung der „trivialen Maschine“ Organisation auf.

Die folgenden Abschnitte beschäftigen sich sowohl damit, wie die Systemtheorie nach Luhmann die Steuerung durch das Management abbildet, als auch wie die Theorie formelle und informelle Strukturen auffasst.

6.2.1 Irritation statt Steuerung

Kapitel 6.1.2 spricht bereits an, dass das Managementverständnis der klassischen Managementtheorie nicht mit dem Organisationsverständnis nach Luhmanns Systemtheorie vereinbar ist. Deshalb widmet sich dieser Abschnitt den Fragen, wie Luhmann Steuerung in seiner Systemtheorie versteht und wie sich Management unter diesem Steuerungsverständnis begreifen lässt. Außerdem gilt es, die Vorzüge einer solchen Konzeption von Management in ihrer gesteigerten Erklärbarkeit von Dynamiken des ISMS herauszuarbeiten.

Einleitend lässt sich festhalten, dass Management und damit verbundene Steuerungsversuche in der Systemtheorie nicht der primäre Weg für die Entwicklung der Organisation sind, sondern nur einer von verschiedenen Wegen. Die Autoren von [KE06] schreiben hierzu:

> Denn Steuerung durch ein Management ist nicht Selbststeuerung der Organisation, nicht selbsttragende Entwicklung, sie impliziert Planung und Intentionalität der Manager, und zwar auch in Bezug auf Kommunikationsstrukturen. Das macht Luhmanns Organisationstheorie so sperrig für eine betriebswirtschaftliche Nutzung, zumal, wenn damit eine Führungs- oder Managementlehre gemeint ist. Steuerungsversuche sind für Luhmann einer unter den Wegen der Evolution, ein Weg, der Variation ermöglicht, aber in eine nicht-intendierte, nicht absehbare Selektion hineinläuft. “ (S.440 [KE06]).[26]

Damit bricht die Systemtheorie mit der Annahme der klassischen Managementtheorie, die Planung sei die einzige zielgebende Instanz, welche die Organisation kontrolliert und lenkt. [27] Was die Autoren als „[...] sperrig für eine betriebswirtschaftliche Nutzung“ insbesondere für eine Führungs- oder Managementlehre bezeichnen, ist für die Erklärbarkeit der Theorie als positiv zu bewerten. Durch die Verlagerung der Steuerung vom Management hin zur Steuerung der Organisation durch sich selbst ermöglicht die Theorie, eine Evolution der Organisation auch auf anderen Wegen zu erklären. Kapitel 5.1.4 führte das Beispiel an, dass die Informationssicherheit durch die nicht vorgeschriebene Nutzung von Passwortmanagern verbessert wurde. Diese Verbesserung ließ sich in der klassischen Managementtheorie nicht abbilden, da diese die Planung als einzige zielgebende Instanz der Organisation versteht und alle Abweichungen von dieser als negativ bewertet. Eine Erklärung ist in diesem Fall nur durch das Ausbrechen aus der

[26] siehe hierzu auch kurz S.356 [Luh11]
[27] Siehe hierzu auch Kapitel 4.1

Theorie möglich. In der Systemtheorie nach Luhmann ist besagtes Beispiel hingegen abbildbar, da die Evolution der Organisation nicht auf die Planung beschränkt ist, sondern von der Organisation selbst ausgeht. Es ist genauso gut möglich, dass die Passwortrichtlinien, die vom Management verordnet werden, zu einer Verbesserung der Informationssicherheit führen, da dies ebenfalls ein möglicher Weg für die Evolution der Organisation darstellt. [28]

Anhand des Beispiels lässt sich bereits erkennen, dass sich durch die Auflockerung des strikten Ursache-Wirkungs-Verständnisses hinter der Steuerung weitreichendere Erklärungen ermöglichen.

In der Systemtheorie bezeichnet man einen solchen Auslöser für Evolution als „Irritation". Die Autoren von [KE06] auf Seite 439f. bringen diesen Begriff mit dem der Steuerung zusammen. Luhmann selbst schreibt zur Irritation:

> Irritation heißt nur: Regenerierung von Unsicherheit aus jeweils besonderen Anlässen, also Wiederherstellung einer Mischung aus Orientierung an den strukturbestimmten Erwartungen des Systems und Wahrnehmung neuartiger Anforderungen, einer Mischung also aus Selbstreferenz und Fremdreferenz mit Anhaltspunkten in den jeweiligen Situationen (S.220 [Luh11]).

Vereinfacht ordnet das Zitat die im Beispiel geschilderte Dynamik der Evolution durch Steuerung in die Begrifflichkeiten der Systemtheorie ein. Damit das Zitat nachvollziehbar für den Kontext dieser Arbeit ist, sollen die darin verwendeten Begriffe im Folgenden kurz erklärt und eingeordnet werden. Für das Verständnis kann es hilfreich sein, sich vor Augen zu führen, dass in der Systemtheorie die Organisation als autopoietisches System der „Akteur" ist, von dem die Steuerung ausgeht und nicht die Mitarbeitenden oder das Management.

Die Verarbeitung von Unsicherheit (bzw. Kontingenz) stellt in der Systemtheorie den zentralen Treiber für die Ausbildung von Organisationen und deren Evolution dar.[29] Die Regenerierung dieser Unsicherheit bedeutet, dass sich die Organisation erneut mit deren Verarbeitung beschäftigen muss. Beschäftigen bedeutet genauer, dass sich die Organisation als autopoietisches System selbst erneuert, um (immer wieder) mit der Unsicherheit ihres Umfeldes umzugehen. Die strukturbestimmten Erwartungen lassen sich in diesem Zusammenhang als das verstehen, was die Organisation bis dahin ausgemacht hat, und die neuartigen Anforderungen sind demgegenüber die Inhalte der Irritation.

[28] An dieser Stelle sei auf S.407 in [KE06] verwiesen, welche das Verständnis von So-Oder-Auch-Anders als zentralen Gedanken für Luhmanns Theorie herausstellen.

[29] Für eine Erklärung siehe [KE06] Kapitel 11.1

Vereinfacht auf das ISMS übertragen bedeutet die Einführung eines neuen Sicherheitssystems, dass sich die Organisation mit dessen Gebrauch auseinandersetzen muss. Sie muss unter anderem Abläufe in ihrer Arbeitsweise verändern und potenziell neue Mitarbeiter in die Organisation aufnehmen mit entsprechenden Kompetenzen. Eine strukturbestimmte Erwartung gegenüber diesen neuen Anforderungen könnte beispielsweise das Bewusstsein dafür sein, dass sich Abteilung Y häufig schwerer mit neuen Sicherheitsmaßnahmen tut als Abteilung Z. Die Unsicherheit entsteht, weil die Organisation nicht wie vor der Irritation funktioniert, sondern sich mit dem neuen Sicherheitssystem auseinandersetzen muss.

Die Begriffe der Selbst- und Fremdreferenz sind ebenfalls aus der Perspektive der Organisation formuliert. Die Selbstreferenz bezieht sich demnach auf die Organisation. Die Fremdreferenz bezieht sich auf die zu beachtenden Aspekte der Umwelt und meint damit beispielsweise die neuartigen Anforderungen, welche durch die Irritation[30] an die Organisation herangetragen werden (vgl. S.92 [BCE97]).[31]

Das Beispiel zeigt noch einmal detaillierter, wie sich die Perspektive vom Management und den Mitarbeitenden als Akteure zugunsten einer agierenden Organisation verschiebt. Nicht das Management steuert die Organisation und verbessert deren Informationssicherheit, sondern das Management irritiert die Organisation und regt sie dazu an, sich potenziell so zu verändern, dass sich die Informationssicherheit verbessert. Dieser Begriff lässt übrigens bewusst offen, ob sich hierdurch eine Verbesserung der Informationssicherheit einstellt. Es wäre ebenfalls möglich, dass die Irritation des Managements eine Verschlechterung der Informationssicherheit bewirkt. Kapitel 5.1.4 zeigt erneut am Beispiel der Passwortrichtlinien, wie sich durch deren Erlassen die tatsächliche Informationssicherheit in der Organisation nicht verbessert, sondern verschlechtert hat. [32] Die klassische Managementtheorie ist an dieser Stelle durch die Annahme der Planung als zu erreichendes Optimum in ihrer Erklärbarkeit beschränkt, da sie die Ursache einer Verschlechterung nur in der Umsetzung und Ausführung der erlassenen Maßnahmen sehen kann und nicht in den Maßnahmen selbst (vergleiche auch hierfür Kapitel 5.1.4). Die Systemtheorie unterliegt mit ihrem Verständnis von Steuerung als Irritation nicht dieser Limitation und bietet an dieser Stelle eine breitere Erklärungsbasis als die klassische Managementtheorie.

Bis jetzt wurde ersichtlich, wie die Steuerung als Irritation eine deutlich weitere Er-

[30] Siehe Definition auf der vorherigen Seite.

[31] Zur Selbstreferenz siehe S.47 Punkt drei und vier [Luh11] oder in Kurzform zu beidem in S. 163ff. [BCE97]

[32] Für weitere Beispiele von formalen Maßnahmen, die einen gegenteiligen Effekt als den intendierten ausgelöst haben, siehe [DH97]

klärungsbasis bietet als die klassische Managementtheorie. Es bleibt allerdings die Frage, wie sich die „Steuerung“ des Managements von anderen Irritationen der Organisation, beispielsweise durch die von Mitarbeitenden oder Ereignissen wie Naturkatastrophen, unterscheidet. Damit befassen sich die kommenden Abschnitte

Luhmann selbst betont in „Organisation und Entscheidung“ [Luh11], dass die Steuerung durch das Management einen Zweck erfüllen muss, da sie sonst im Laufe der Evolution eliminiert worden wäre (vgl. S.403 [Luh11]).

Dieser Zweck liegt laut Luhmann in der Abschwächung oder Verstärkung von Differenzen. Die Differenzen beziehen sich dabei nicht auf die eigentliche Organisation[33], sondern lediglich:

> [...] als Kontext spezifischer Differenzen man könnte sagen: als Endloskontext der Unterscheidungen von Unterscheidungen mit der Maßgabe, dass Veränderungen in einer Differenz das tangieren können oder auch nicht, was mit den Differenzen in anderen Unterscheidungen geschieht. (S.403f [Luh11])

Vereinfacht lässt sich das Management demnach als ein Scheinwerfer im Dunkeln veranschaulichen. Das Management lenkt den Fokus der Aufmerksamkeit der Organisation auf die zu betrachtenden Unterscheidungen, mit denen sich diese Organisation beschäftigen soll. Die Unterscheidung kann hierbei, wie im oberen Beispiel, die Einführung eines Sicherheitssystems sein. Mit dem möglichen Tangieren von anderen Unterscheidungen betont Luhmann die Abhängigkeit einer solchen Betrachtung von bereits getroffenen und zukünftig zu treffenden Unterscheidungen. Bezogen auf das Beispiel hängt die Einführung eines neuen Sicherheitssystems beispielsweise mit den vorherigen Entscheidungen zur Verbesserung der Informationssicherheit zusammen. In einem spezifischen Szenario könnte es beispielsweise sein, dass die Beschaffung eines neuen Sicherheitssystems A weniger Sinn ergibt, da dieses nicht im gleichen Maße kompatibel mit dem bereits angeschafften Identity- und Access-Management-System ist wie Sicherheitssystem B. Die Entscheidung der Beschaffung eines Sicherheitssystems hat ebenfalls Implikationen für zukünftige Entscheidungen, beispielsweise weil die Beschaffung Kapital bindet, welches dann an anderer Stelle nicht mehr zur Verfügung steht.

In diesen Punkten scheinen sich die klassische Managementtheorie mit der Formulierung ihres Plans, der diese Aspekte berücksichtigt, und die Systemtheorie ähnlich. Der entscheidende Unterschied ist jedoch, dass Luhmann kategorisch ausschließt, dass es

[33] Warum die eigentliche Organisation nicht betrachtet werden kann, erklärt bereits Kapitel 2.5 unter Zuhilfenahme des Komplexitätsbegriffs von Luhmann.

möglich ist, alle relevanten Faktoren für die Fragestellung zu berücksichtigen. [34] Die klassische Managementtheorie baut hingegen ihre gesamte Theorie um diese Annahme auf. [35]

Luhmann schließt aus der komplexen Verknüpfung von einer unüberschaubaren Anzahl an Entscheidungen, dass die Halbwertszeit der Steuerung relativ gering sein muss und sich dementsprechend eine neue Steuerung an die alte Steuerung anschließen muss (vgl. S.404 [Luh11]). Anschließend an das vorherige Beispiel könnte nach der Wahl des Sicherheitssystems B auffallen, dass einige Aspekte bei der Entscheidung nicht bedacht wurden, wodurch eine neue Entscheidung nötig ist.

Fasst man die Ausführungen zur Steuerung und Irritation bis hierhin zusammen, lässt sich Steuerung in der Systemtheorie als kontinuierlich auftretende Tätigkeit verstehen. Die Steuerung regeneriert Unsicherheit indem sie Unterscheidungen verstärkt oder abschwächt. Hierbei beobachtet sie Aspekte der Organisation in ihrer Umwelt. Die Organisation verarbeitet diese Unsicherheit dann im Rahmen ihrer Autopoiesis. Dadurch, dass die Theorie der Organisation den Umgang mit der Unsicherheit überlässt, kann sie die in Kapitel 5.1.3 benannten komplexeren Wirkungszusammenhänge der Steuerung einfangen, ohne die Theorie verlassen zu müssen.

Das Ganze erinnert in seinem wiederkehrenden Charakter an den PDCA-Zyklus des ISO 27001 (vgl. Kapitel 3.2.2) oder auch den klassischen Managementprozess (vgl. Abb. 5). Dennoch unterscheiden sich die Ansätze in ihrem Verständnis von Steuerung und Organisation fundamental, da der PDCA-Zyklus von einem anderen Steuerungsbegriff ausgeht als Methodiken, die auf der Systemtheorie nach Luhmann fußen. Die „Systemische Schleife“ von [KE19], visualisiert in Abb. 9, ist ein Beispiel dafür.

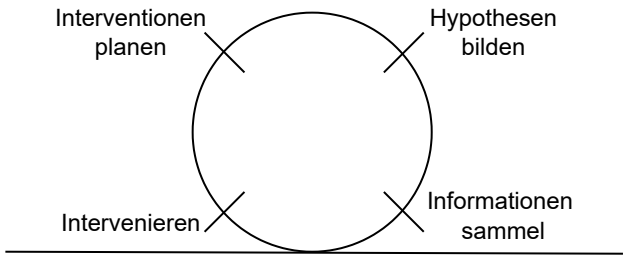

Abbildung 9: Systemische Schleife nach [KE19] S.24

Sie gleicht in ihrem iterativen Aufbau zwar dem PDCA-Zyklus[36], formuliert jedoch

[34] Siehe hierzu auch Kapitel 2.5 und die Ausführungen zum Komplexitätsbegriff in der Systemtheorie nach Luhmann.

[35] Vergleiche hierzu die Ausführungen zur externen und internen Determiniertheit Kapitel 3.3.3

[36] Für den Aufbau des PDCA-Zyklus siehe Kapitel 3.2.2

grundverschiedene Phasen und Ziele, da diese nicht von einer Ursache-Wirkungsbeziehung zwischen Management und Organisation ausgeht.

Mit diesen abschließenden Einblicken lässt sich zusammenfassend festhalten, dass die Erklärbarkeit der Systemtheorie in Sachen Steuerungsdynamik zwischen Organisation und Management umfassender ist als die der klassischen Managementtheorie. Diese begründet sich letztlich in der Verlagerung von Steuerung in die Organisation und der daraus resultierenden Konzeption der Steuerung als Irritation, welche die Organisation lediglich zur Evolution anregt. Die Implikationen dieser grundlegend anderen Perspektive sind mannigfaltig und werden im restlichen Kapitel anhand weiterer Überlegungen ausgeführt. Es sei an dieser Stelle final betont, dass die Selbststeuerung der Organisation und die damit verbundene Unsicherheit darüber, welche Auswirkungen Informationssicherheitsmaßnahmen im Rahmen des ISMS haben, die Basis darstellen, durch die die soziale Systemtheorie nach Luhmann die von der klassischen Managementtheorie unzureichend oder nicht erfassten Dynamiken greifen kann. Letztlich bedeutet dies für die Praxis im besten Fall, dass durch die Perspektive der Systemtheorie nach Luhmann bestehende Probleme im Zusammenhang mit dem ISMS differenzierter und umfassender erklärt und adressiert werden können. Die restlichen Abschnitten demonstrieren diesen Vorzug weiter.

6.2.2 Entscheidungsprämissen

Der vorherige Kapitel 6.2.1 deutet bereits darauf hin, dass die bewusste Beeinflussung der Organisation in eine bestimmte Richtung aus Sicht der Systemtheorie nach Luhmann deutlich schwieriger ist als in der klassischen Managementtheorie. Vor diesem Hintergrund stellt sich die Frage, wie sich Organisationen in der Systemtheorie überhaupt so weit organisieren können, dass sie eine so „geregelte“ Welt wie unsere ermöglichen.

Das Beispiel zum Unterscheiden von Steuerung und anderen Arten der Irritation hat bereits gezeigt, dass die Entscheidungen für ein bestimmtes Sicherheitssystem bereits in ihrer Komplexität unüberblickbar sind. Die Autoren von [KE06] führen in Kapitel 11 verschiedene Konzepte von Luhmanns Systemtheorie ein, die den Umgang mit dieser unüberblickbaren Menge an Optionen ermöglichen.

Eines dieser Konzepte sind die sogenannten Entscheidungsprämissen, welche in den folgenden Abschnitten vertieft betrachtet werden. Die Entscheidungsprämissen lassen sich in entscheidbare und unentscheidbare Entscheidungsprämissen unterteilen. Entscheidbare Entscheidungsprämissen lassen sich dabei in Teilen mit den formalen Strukturen einer Organisation – Aufbauorganisation, Ablauforganisation, Stellen, Prozesse –

vergleichen, wie Kapitel 6.2.2 im Anschluss an diese Einleitung ausführt. Die nicht entscheidbaren Entscheidungsprämissen sind vergleichbar mit den informellen Strukturen, welche beispielsweise in der „Bank-Wiring Observation Room"-Studie als von den Mitarbeitern formulierte und durchgesetzte Regeln beobachtet werden konnten (vgl. Kapitel 5.1.2). Beide Arten von Entscheidungsprämissen steuern auf ihre Art zur Eingrenzung der Handlungsmöglichkeiten bei und ermöglichen somit eine „geregelte" Welt.

Die Kritik aus Kapitel 5.1.4 betont, dass die klassische Managementtheorie insbesondere bei der Abbildung von informellen Strukturen mit der pauschalen Definition als Abweichung nicht hinreichend komplexe Beobachtungen erlaubt und somit relevante Dynamiken des ISMS nicht einfangen kann. Die folgenden Abschnitte zeigen, wie die Systemtheorie in der Lage ist, diese blinden Flecken beleuchtet.

Entscheidbare Entscheidungsprämissen und formale Strukturen Das erste Konzept zur Einschränkung von Kontingenz sind die sogenannten „entscheidbaren Entscheidungsprämissen" (vgl. Kapitel 11.7 in [KE06] oder ausführlich im Original Kapitel sieben, acht, neun und zehn in [Luh11]).

Diese entscheidbaren Entscheidungsprämissen lassen sich noch am ehesten im Rahmen einer klassischen Managementtheorie erklären. Dies liegt vornehmlich daran, dass die entscheidbaren Entscheidungsprämissen in ihren drei Formen – Programme, Kommunikationswege und Personen – scheinbar mit den formalen Strukturen der klassischen Managementtheorie übereinstimmen. So schreiben die Autoren von [KE06]: „Entscheidungsprogramme, Kommunikationswege, Personal(-management): Das sind Strukturen, die in Organisationstheorie und Betriebswirtschaftslehre – unter Namen wie „Aufbau- und Ablauforganisation", „Kommunikation und Information" und „Human Resource Management" – auch sonst geläufig sind." (S.422 [KE06]).

Der Unterschied zwischen der klassischen Managementtheorie und der Systemtheorie in Bezug auf diese formalen Strukturen bzw. Entscheidungsprämissen liegt in der unterschiedlichen Organisationskonzeption. In der klassischen Managementtheorie steuert das Management die Organisation direkt mit formalen Strukturen in Form von Regeln, Richtlinien, Prozessen usw. (vgl. Kapitel 3.3). Die formalen Strukturen sind sozusagen die Teile, aus denen die Organisation als maschinenartige Idealisierung besteht (vgl. Kapitel 3.3.4), sie sind deckungsgleich.

In der Systemtheorie hingegen verhält sich die Beziehung zwischen entscheidbaren Entscheidungsprämissen und Organisation anders, da die Organisation selbststeuernd ist.

Die Autoren von [KE06] zitieren hierzu:

> [Entscheidungsprämissen] legen die künftigen Entscheidungen noch nicht fest, sie können ja nicht jetzt schon in der Zukunft entscheiden. Aber sie fokussieren die Kommunikation auf die in den Prämissen festgelegten Unterscheidungen. (S.224 [Luh11], S.425 [KE06])

Anders gesagt, erhöhen die Entscheidungsprämissen als Erwartungen lediglich die Wahrscheinlichkeit, dass die Organisation sich entsprechend der Entscheidungsprämissen verhält. Es besteht immer die Möglichkeit, dass die Organisation sich auch außerhalb der entscheidbaren Entscheidungsprämissen bewegt. Damit lässt sich die Organisation nicht auf ihre entscheidbaren Entscheidungsprämissen reduzieren.[37].

Zum besseren Verständnis verdeutlicht der Abschnitt die Wirkung von entscheidbaren Entscheidungsprämissen in einer Organisation durch drei kurze Beispiele:

- Ein dokumentierter Prozess erhöht die Wahrscheinlichkeit, dass die Organisationsmitglieder die Aufgaben entsprechend dieses Prozesses durchführen.
- Es sind E-Mail-Adressen für IT-Supportanfragen definiert, über die sich Organisationsmitglieder an die IT-Abteilung wenden können. Damit ist es wahrscheinlicher, dass sich Organisationsmitglieder bei Problemen mit ihrer Technik über diese Wege an die IT-Abteilung wenden.
- In der Organisation ist die Person T. Hauser zuständig für Aufgaben rund um die Automatisierung von Prozessen. Demnach ist es wahrscheinlicher, dass er sich mit Aufgaben aus diesem Themenbereich befasst.

Im Gegensatz zu den formalen Strukturen in der klassischen Managementtheorie ist es durch die Entscheidungsprämissen in der Systemtheorie nicht garantiert, dass die Organisation die Entscheidungen genau so trifft. Der Prozess kann, muss aber nicht so durchgeführt werden. Die Organisation könnte beispielsweise vom Standardprozess abweichen, wenn sie merkt, dass sie damit die Aufgaben zweckdienlicher erfüllen kann. Die Kommunikation mit dem IT-Support könnte auch außerhalb der definierten Kommunikationswege erfolgen, beispielsweise in persönlichen Gesprächen „zwischen Tür und Angel“. Genauso könnte Herr Hauser trotz seiner eigentlichen Rolle auch weitere Aufgaben übernehmen, wie gelegentliches Aushelfen bei Aufgaben aus seiner ehemaligen Rolle als hausinterner Softwareentwickler.

[37] Vgl. hierzu auch [BCE97] S.184ff. zu Struktur bzw. im Original S.73f. und S.377ff. [Luh21]

Andersherum gedacht: Wenn es diese entschiedenen Entscheidungsprämissen nicht gäbe, wüssten die Organisationsmitglieder nicht, in welcher Reihenfolge sie die Aufgaben des Prozesses erledigen sollen. Die Organisationsmitglieder mit Technikproblemen wüssten nicht, an welche E-Mail sie ihre Hilfeersuchen richten sollten. Es wäre unklar, wer in der Organisation für die Automatisierung zuständig ist. Die Organisation könnte die Aufgaben immer noch entsprechend durchführen, insbesondere wenn diese durch die anderen im übernächsten Abschnitt vorgestellten Entscheidungsprämissen abgebildet werden, auch ohne dass sie durch entschiedenen Entscheidungsprämissen gekennzeichnet sind. Dies wäre jedoch deutlich unwahrscheinlicher, da diese gewünschten Handlungsmöglichkeiten ohne die Hervorhebung in Entscheidungsprämissen im Vergleich zu anderen Handlungsoptionen nicht herausstünden.

Damit ermöglicht die Systemtheorie, wie schon beim Steuerungsbegriff in Kapitel 6.2.1, eine umfassendere Erklärung im Hinblick auf von der Erwartung abweichende Beobachtungen als die klassische Managementtheorie und erhöht somit die Anzahl der in der Theorie erklärbaren Phänomene.

Mit den entscheidbaren Entscheidungsprämissen enden hier die Überschneidungen zwischen den Konzepten in der Systemtheorie und der klassischen Managementtheorie. Die klassische Managementtheorie geht davon aus, dass die Organisation relativ sicher im Managementprozess (vgl. Abb. 5) abgebildet ist, und sich Abweichungen von diesem hinreichend als Abweichungen darstellen lassen. Entsprechend benötigt sie darüber hinaus keine weiteren Konzepte für eine differenzierte Erklärung. Hierdurch tut sich die klassische Managementtheorie als pragmatisches und handlungsorientiertes Erklärungsmodell hervor, wie beispielsweise in Kapitel 5.1.4 erklärt. Der Nachteil dieser Konzeption ist allerdings, dass Dynamiken der informellen Strukturen außerhalb dieses Steuerungsverständnisses liegen und demnach nicht erfasst werden können (vgl. Kapitel 5.1).

Die Systemtheorie unterliegt mit dem Verständnis der Selbststeuerung der Organisation nicht diesen Limitationen. Sie kann daher weitere Konzepte zur Erklärung von Dynamiken innerhalb einer Organisation heranziehen, namentlich die nicht entscheidbaren Entscheidungsprämissen.

Informelle Strukturen als Differenz Die bisher beschriebenen entscheidbaren Entscheidungsprämissen spielen eine besonders wichtige Rolle bei der Einschränkung von Handlungsoptionen innerhalb einer Organisation (vgl. Kapitel 11.7 und die Rolle von Entscheidungsprämissen in Bezug auf die Steuerbarkeit von Organisationen, S.439 [KE06]).

Diese sind jedoch nur eine Ausprägung von Luhmanns allgemeinerem Begriff der

„Struktur“. Struktur umfasst alle Bedingungen, die den Anschlussbereich von Operationen eines autopoietischen Systems einschränken (S.184ff. [BCE97], S.418ff. [KE06]). Hierzu gehören nicht nur die entscheidbaren Entscheidungsprämissen, sondern auch die nicht entscheidbaren Entscheidungsprämissen (auch „Unternehmenskultur“, S.239ff. [Luh11]) sowie Erwartungen und Erwartungserwartungen (S.418 [KE06]). Die Erwartungen und Erwartungserwartungen greift das spätere Kapitel 6.3 noch einmal auf.

Der Rest dieses Unterkapitels befasst sich mit den unentscheidbaren Entscheidungsprämissen. Dabei befasst sich dieser Abschnitt mit der Definition der nicht entschiedenen Entscheidungsprämissen als Differenz (vgl. S.242 [Luh11]) der entscheidbaren Entscheidungsprämissen. Luhmann führt hierzu aus:

> So passt der Begriff der Organisationskultur [nichtentschiedene Entscheidungsprämissen] genau zu dem, was die Systemtheorie im Anschluss an Heinz von Foerster als nicht-triviale Maschine beschreiben würde. Man mag sich auf der Ebene der entscheidbaren Enscheidungsprämissen um intentionalrationale Zukunftsvorsorge bemühen. Dass dies geschehen kann und geschieht, bleibt unbestritten und produziert sozusagen das Sinnmaterial, an das die Entwicklung einer Organiastionskultur anschließt. Aber diese modifiziert die Rationalitätsannahme beträchtlich.(S.249 [Luh11]).

Die nichtentschiedenen Entscheidungsprämissen bilden sich demnach an den entschiedenen Entscheidungsprämissen aus. Entsprechend lässt sich die Organisationskultur nicht durch formale Strukturen wie Richtlinien oder Vorgaben kontrollieren, da diese lediglich zu anderen Auswüchsen der Organisationskultur anregen würden.

Kapitel 5.1.4 hat bereits darauf hingewiesen, dass das Management aus einer klassischen managementtheoretischen Sicht dazu neigen könnte, die informellen Strukturen (Organisationskultur) der Organisation „unter Kontrolle zu bringen“, damit sie sich eben doch erwartbar, wie eine triviale Maschine verhält und die Anweisungen des Managements wie von diesen intendiert umsetzt. Dazu müssten nur genügend wohldefinierte und detaillierte Richtlinien, Rollenbeschreibungen und Kommunikationswege festgelegt werden, um solche informellen Strukturen überflüssig zu machen.

Im Bezug auf das ISMS könnten die Verantwortlichen versuchen, die „unsicheren“ Praktiken durch Richtlinien zu verbieten. Ein Beispiel hierfür sind die eingeführten Passwortrichtlinien aus den vorherigen Kapiteln. Die Verantwortlichen führen zur Verbesserung der Informationssicherheits-richtlinien zur Erstellung von Passwörtern. Dies kann als Versuch verstanden werden, die Organisationskultur in entschiedene Entscheidungsprämissen

zu überführen. Der Begriff „regeln“, wie im Regelkreis, deutet bereits darauf hin, dass mit dem Erlassen der Richtlinie die nicht-trivialen Anteile an dieser Tätigkeit „trivialisiert“ sind.

Durch die obige Definition der Organisationskultur als Differenz zu entscheidbaren Entscheidungsprämissen, nimmt Luhmann solchen Vorstellungen mit seiner Systemtheorie jegliche Erfolgsaussichten.

Die Passwortrichtlinien führen beispielsweise zur Verwendung von Post-Its, auf denen die Passwörter notiert werden. Das Verbot dieser Praxis führt dazu, dass einige auf Textdateien ausweichen oder Passwortmanager verwenden. Das Verbot von Zwischengesprächen über Projekte im Pausenraum könnte zu einer Verlagerung der Gespräche in andere private Räumlichkeiten führen.

Somit kann die Organisationskultur und damit der unkontrollierbare Teil der Organisation niemals eliminiert werden. Das Management erlässt neue Sicherheitsrichtlinien in der Hoffnung, dass diese die nicht-geregelten und unsicheren Praktiken in der Organisation regeln. Dabei erzeugen diese Regularien als formale Strukturen neue informelle Strukturen als deren Differenz. Diese sind wiederum nicht reguliert und im klassischen Managementverständnis als Abweichung vom Plan ein Problem.[38] Diese informellen Strukturen müssen als unkontrollierte, mögliche Ursachen von Schwachstellen durch weitere Richtlinien adressiert werden. Somit entsteht ein sich selbst verstärkender Kreislauf: ein Teufelskreis nach dem Verständnis des Buches „Die Fünfte Disziplin“ [Sen06], der die Anzahl der Richtlinien erhöht, die alle einzuhalten sind.[39]

Das Bestreben, die unentscheidbaren Entscheidungsprämissen ebenfalls durch entscheidbare Entscheidungsprämissen abzubilden, nennt sich in der Organisationsforschung „Hyperformalisierung“ (vgl. S.13 ff. [Kü23]). Die „radikalste“ (S.24 [Kü23]) Organisationsform, die eine solche Hyperformalisierung zugrunde legt, ist die „Holokratie“ ([Rob16]). Der Kerngedanke hinter dieser Organisationsform ist die Eliminierung von Hierarchien durch die explizite Transparenz aller formalen und nicht formalen Erwartungen in der Organisation (vgl. insbesondere Teil 1 [Rob16]). Dadurch soll die Notwendigkeit für Hierarchien entfallen, was eine agile Organisation ohne Silobildung und Hierarchien schaffen soll (S.12 [Kü23]). Obwohl diese Organisationsform aufgrund der Negierung der Hierarchien keine zentrale Steuerungsstelle definiert, folgt sie mit dem Anspruch, die Organisation vollständig abbilden zu können, dennoch der Grundannahme der Organisation als Maschine (vgl. S.55 [Kü23]), oder spezifischer als Betriebssystem (vgl. [Kü23] bzw. im Original S.11 [Rob16]).

[38] Siehe Ausführungen in Kapitel 5.1

[39] Die stetige Ausprägung von immer neuen informellen Strukturen wirkt einer vollständigen Modellbildung wie in Kapitel 2.5 mit dem BMIS entgegen.

Kühl widmet den Ausweichmechanismen der Organisation auf den Versuch, deren nicht entscheidbare Entscheidungsprämissen nach dem Verständnis der Holokratie formal vollständig zu erfassen, ein ganzes Buch ([KSNI23]).

Das Ziel der Holokratie unterscheidet sich vom Ziel des ISMS. Die Holokratie ist dennoch relevant, da sie zeigt, dass auch in diesem Fall der Versuch, die Organisation zu „enttrivialisieren“, nicht möglich ist.

Als Fazit für diesen Abschnitt lässt sich festhalten, dass die Fähigkeit der für das ISMS verantwortlichen Personen, die Informationssicherheit in der Organisation vollständig zu überblicken und die Organisation zu kontrollieren, gegen Null geht. Die Autoren von [SK20] kommen in ihrer Kritik zur klassischen Managementtheorie zum selben Ergebnis (vgl. S.120ff. [SK20]). Reflektiert auf die Praxis kann diese Einsicht bedeuten, dass die Verantwortlichen des ISMS trotz größter Anstrengungen und genauer Befolgung von Best Practices, wie dem IT-Grundschutz des BSI [BSI17], an der erfolgreichen Umsetzung des ISMS scheitern. Aus der Perspektive der systemtheoretischen Sichtweise Luhmanns kann die „Schuld“ an diesem Scheitern weder eindeutig den Verantwortlichen noch den Mitarbeitern zugewiesen werden, sondern ist in der Selbststeuerung der Organisation verankert.

Die Systemtheorie nach Luhmann trägt diesem Umstand durch die Definition der Organisationskultur als Differenz zu den entscheidbaren Entscheidungsprämissen Rechnung. Diese macht eine vollständige Eliminierung der Selbststeuerung unmöglich, wodurch die daraus resultierende Unsicherheit dauerhaft bestehen bleibt.

Nicht entschiedene und unentscheidbare Entscheidungsprämissen Der vorherige Abschnitt hat ausgeführt, wie nicht entscheidbare Entscheidungsprämissen entstehen und dass diese aufgrund ihrer Definition ein unumgänglicher Bestandteil der Organisation sind. Dieser Abschnitt befasst sich insbesondere mit den Vorteilen, solche nicht entscheidbaren Entscheidungsprämissen im Kontext des ISMS differenziert betrachten zu können.

In einem ersten Schritt führt dieser Abschnitt dafür die Unterteilung der nicht entscheidbaren Entscheidungsprämissen in zwei Arten nach Kühls Einführungswerk [Kü11] ein:

- Nicht entschiedene Entscheidungsprämissen (S.116f. [Kü11] bzw. im Original [Rod12] S.140f.)
- Unentscheidbare Entscheidungsprämissen (S.118f. [Kü11]).

Zusammen mit den entscheidbaren Entscheidungsprämissen und dem Bewusstsein, dass die nicht entscheidbaren Entscheidungsprämissen die Differenz der entscheidbaren Entscheidungsprämissen bilden, lässt sich das Ganze wie in Abb. 10 visualisieren:

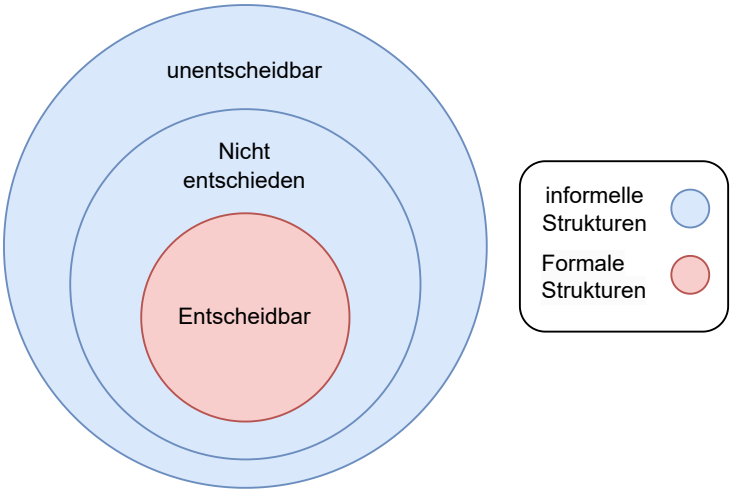

Abbildung 10: Illustration der verschiedenen Entscheidungsprämissen nach [Kü11] basierend auf [Rod12] und [Luh11]

.

Die entscheidbaren Entscheidungsprämissen hat Kapitel 6.2.2 bereits betrachtet. Den verbleibenden nicht entschiedenen und unentscheidbaren Entscheidungsprämissen widmet sich der Rest dieses Kapitels.

Nicht entschiedene Entscheidungsprämissen zeichnen sich dadurch aus, dass sie prinzipiell in entscheidbare Entscheidungsprämissen überführbar sind. Die klassische Managementtheorie bewertet die informellen Strukturen als eindeutig negative Implementationsprobleme und wäre dementsprechend dazu angehalten, alle nicht entschiedenen Entscheidungsprämissen zu entscheiden. Würden die Mitarbeiter beispielsweise auf Passwortmanager zurückgreifen, müsste dies aus einer klassischen managementtheoretischen Sicht durch entsprechende Richtlinien geregelt werden.

Die Systemtheorie nimmt keine Bewertung der nicht entschiedenen Entscheidungsprämissen vor, sondern betrachtet diese lediglich im Hinblick auf deren Funktion für die Organisation[40]. Manchmal kann es im Interesse der Verbesserung der Informationssicherheit sein, nicht entschiedene Entscheidungsprämissen als solche zu belassen. In anderen Fällen kann es sinnvoll sein, sie in entschiedene Entscheidungsprämissen, wie beispielsweise anhand von Richtlinien, zu überführen. Mit der Fokussierung auf die Funk-

[40]Siehe hierfür erneut Kapitel 11.1 [KE06] zur Ausführung von Luhmanns Analyse von Funktionalitäten und Funktionsäquivalenten.

tion eröffnet die Systemtheorie die Möglichkeit von differenzierten und kontextabhängigen Betrachtungen.

Die Veröffentlichung „„Shadow security“ as a tool for the learning organization“ [KPS14] bietet ein Beispiel, wie eine komplexere Auffassung von informellen Strukturen über die simple Sicht als Implementationsproblem hinaus, Vorteile für die Informationssicherheit bieten kann.

Die Autoren appellieren in ihrer Veröffentlichung, Schatten-IT nicht ausschließlich als Quelle von Sicherheitsproblemen zu sehen, sondern als Indikator dafür, dass die aktuellen Sicherheitsmaßnahmen nicht gut genug in die Arbeitsabläufe der Mitarbeiter integriert sind. Anhand dieser gilt es dann die formalen Strukturen weiter nachzubessern, bis die Mitarbeiter keinen Grund mehr sehen, die Maßnahmen zu umgehen.

In die Systemtheorie nach Luhmann übersetzt, ermöglicht die differenziertere Betrachtung der nicht entschiedenen Entscheidungsprämissen die Beobachtung deren Funktion für die Organisation, wodurch diese in entscheidbare Entscheidungsprämissen überführt werden können.

Dennoch bewerten die Autoren die nicht entschiedenen Entscheidungsprämissen in erster Linie als potenzielle Gefahren für die Informationssicherheit, die entsprechend zu formalisieren sind.

Dabei kann selbst so etwas wie Schatten-IT zur Verbesserung der Informationssicherheit beitragen. Das bereits mehrfach angeführte Beispiel des Passwortmanagers fällt unter diesen Fall. Der indirekte Austausch über Tipps zum fachgerechten Umgang mit der Unternehmenssoftware in einer kurzen Pause kann ein anderes Beispiel sein.

Auch Kühl hebt in [Kü11] die positiven Aspekte von nicht entschiedenen Entscheidungsprämissen als „Abkürzungen, Tricks und Schliche, die das Organisationsleben durchziehen“ (S.119 [Kü11]), auf einer allgemeineren Ebene hervor. Er führt ferner aus, dass die nicht entschiedenen Entscheidungsprämissen, insbesondere die gegen formale Richtlinien verstoßen, ein wichtiger Teil der Organisation sind, um ihren Aufgaben gerecht werden zu können. Eine detaillierte Einführung in die Hintergründe dieser Feststellung würde an dieser Stelle zu weit führen. Kurz gesagt, eine Organisation muss verschiedenen Anforderungen gerecht werden, die häufig widersprüchlich oder sogar paradox sind.[41]

Der Verstoß gegen Sicherheitsmaßnahmen lässt sich somit nicht nur aus der individuellen Perspektive der Mitarbeiter erklären, wie in [KPS14], sondern auch auf organisatorischer Ebene.

Die Systemtheorie ermöglicht die Abbildung von beiden Möglichkeiten, indem sie vor-

[41] Kühl vertieft diese Feststellung auf den Seiten 120ff. [Kü11] und in [Kü20].

nehmlich die Funktion von (nicht) entschiedenen Entscheidungsprämissen für die Organisation in den Blick nimmt und dabei keine Wertung vornimmt.

Unentscheidbare Entscheidungsprämissen lassen sich prinzipiell nicht in entscheidbare Entscheidungsprämissen überführen. Damit fangen sie die Differenz der nicht entscheidbaren Entscheidungsprämissen ein, weswegen sie der Abschnitt im Folgenden synonym auch als Organisationskultur bezeichnet.

Kühl fasst unter diesen Begriff die „Einstellungen, Denkstile und Haltungen“ sowie die „gemeinsam geteilten Grundannahmen, Orientierungsmuster und fraglos akzeptierten Kausalattributionen“, die in Organisationen gelten, oder auch das „Rezeptwissen“ (S.118f. [Kü11]) zusammen.

Darüber hinaus betont Kühl auf den Seiten 127ff. [Kü11], dass sich die Organisationskultur nicht im Sinne des Managements formen lässt.

Luhmann beschreibt die Organisationskultur in erster Linie als Trägheitseffekte, die sich insbesondere bei tiefgreifenden organisatorischen Veränderungen äußern (vgl. S.247ff. [Luh11]). Die Autoren in [Smi+10] konstatieren in vergleichbarer Weise Gruppennormen und kulturelle Vorurteile als hinderliche Faktoren bei der Umsetzung eines mandatierten Informationssicherheitssystems. Diese hinderlichen Faktoren können dazu führen, dass Sicherheitsmaßnahmen auf Widerstand stoßen oder nur halbherzig umgesetzt werden.

Obwohl sich die Organisationskultur nicht mit entschiedenen Entscheidungsprämissen im Sinne des Managements formen lässt, kann sie dennoch beeinflusst werden. In seinem kurzen Einführungswerk „Organisationskulturen beeinflussen“ [Kü18] thematisiert Kühl in Kapitel drei verschiedene Möglichkeiten, die Organisationskultur zu beeinflussen. Hierbei beschreibt er insbesondere, wie sich der bereits angesprochene Grad an Formalisierung, gemessen an den entschiedenen Entscheidungsprämissen, auf unentscheidbare Entscheidungsprämissen auswirken kann. Wie bereits gezeigt wurde, können diese relevante Auswirkungen auf die Verbesserung der Informationssicherheit haben, beispielsweise wenn zu viele Richtlinien für einen „Compliance Overload“ sorgen und die Mitarbeiter die Richtlinien umgehen (vgl. Kapitel 5.1.4).

Die Systemtheorie erkennt die Existenz solcher Mechanismen in der Organisation an und macht sie damit explizit zum Teil des organisatorischen Wirkungsgefüges. Diese Integration ermöglicht es, Informationssicherheitsmaßnahmen nicht nur hinsichtlich ihres Zwecks zur Verbesserung der Informationssicherheit in einer maschinenartigen Organisation zu reflektieren. Sie erlaubt es auch, diese Maßnahmen im Hinblick auf ihre Anschlussfähigkeit an die Organisationskultur zu evaluieren, ohne aus der Theorie aus-

zubrechen. Dadurch kann die Theorie differenziertere Erklärungen liefern, warum die Umsetzung von Sicherheitsmaßnahmen in einer bestimmten Organisation A erfolgreich ist, während dies in einer anderen Organisation B nicht gelingt.

6.2.3 Fazit

Zusammenfassend lässt sich festhalten, dass das ISMS auf Basis der Systemtheorie nach Luhmann grundlegend anders zu verstehen ist als auf Basis der klassischen Managementtheorie. Das Kapitel hat gezeigt, dass die Systemtheorie eine umfassendere und differenziertere Grundlage für die Erklärung von Dynamiken in der Organisation bietet als die klassische Managementtheorie. Darüber hinaus wurde kurz umrissen, welche praktischen Folgen eine gesteigerte Fähigkeit, die Dynamiken des ISMS zu erklären, haben kann.

6.3 Aktive Umwelt

Nachdem das vorherige Kapitel 6.2 demonstriert hat, dass die Systemtheorie eine breitere und tiefere Erklärungsgrundlage für die Dynamiken des ISMS in der Organisation bietet, beschäftigt sich dieses Unterkapitel mit der Erklärbarkeit der Theorie für die Umwelt der Organisation.

Auch dieses Kapitel orientiert sich hierbei an der Kritik aus dem vorherigen Kapitel 5. Genauer greift dieses Kapitel die Kritik auf, dass die Umwelt in der klassischen Managementtheorie als passiv dargestellt wird.

Die klassische Managementtheorie erweckt den Eindruck, dass ein Plan die relevanten Aspekte der Umwelt abbilden kann. Sie geht davon aus, dass der aktuelle Zustand und die Veränderungen der Umwelt über die Zeit durch Planung erfasst werden können. Dies führt zu einer falschen Sicherheit, nämlich dass ein ISMS ausreichend vor einem Schadensfall vorbereitet werden kann.

Insbesondere Fälle, in denen der Angreifer nicht mit der Planung des Sicherheitsmanagements „kooperiert“, d.h aus der Planungsschleife (vgl. beispielsweise den PDCA-Zyklus in Kapitel 3.2 oder dem Managementprozess Abb. 5) ausbricht, können somit nicht ausreichend abgebildet werden. Die Erklärung solcher Dynamiken ist auf die Reduktion des „Abweichens“ von der Planung begrenzt. Die Limitation einer solchen Idealisierung für die Erklärbarkeit der Theorie wurde bereits in Kapitel 6.2 für die Organisation erläutert und überträgt sich entsprechend auf die Umwelt.

Auch im Falle der Umwelt adressiert die Systemtheorie diese Limitation über ihre Konzeption von Organisationen als selbststeuernde Systeme. Denn auch die Umwelt besteht

„zum erheblichen Teil aus handelnden Personen und Organisationen“ (S.123 [SK20]), wie in der Kritik an der externen Determiniertheit in Kapitel 5.2.2 bereits ausgeführt. Der Angreifer ist somit ebenfalls ein selbststeuerndes System und lässt sich genauso wenig wie die Organisation anhand eines Plans steuern und seine zukünftigen Handlungen sind nicht kalkulierbar (vgl. Kapitel 6.1.1).

Hierdurch ergibt sich eine deutlich differenzierte Betrachtungsmöglichkeit der Wirkungszusammenhänge zwischen der Organisation als Verteidiger, die das ISMS zum Schutz ihrer Informationssicherheit umsetzt, und einem böswilligen Angreifer.

Zunächst einmal gilt es hierfür allgemein zu klären, was passiert, wenn zwei selbststeuernde Systeme aufeinandertreffen, wie bei dem Aufeinandertreffen von Verteidiger und Angreifer. Im besagten Fall entsteht sogenannte doppelte Kontingenz. Das „doppelt“ bezieht sich darauf, dass beide Systeme das jeweils andere beobachten und wegen der Selbststeuerung des Gegenübers nicht sicher sein können, welche Implikationen die eigene Handlung hat.

Die Autoren von [KE06] führen aus: „Was tun? Man weiß es nicht. Alles ist kontingent. Beide warten vielleicht lieber ab. A macht sein Handeln, Kommunizieren, Entscheiden von dem des B abhängig, B aber das seine von dem des A.“ (S.409 [KE06]). Die Autoren schlussfolgern, dass die Systeme auf die potenzierten Handlungsoptionen durch Überforderung und Lähmung reagieren.

Um eine solche Lähmung zu vermeiden, entwickeln die Systeme sogenannte „Erwartungen und Erwartungserwartungen“, welche Kapitel 6.2.2 bereits kurz bei den Entscheidungsprämissen anspricht. Die Erwartungen wirken der Lähmung dabei entgegen, indem sie die Vielzahl möglicher Handlungen auf ein handhabbares Maß an wahrscheinlichen und akzeptablen Verhaltensweisen reduzieren (S.45ff. „Erwartungen“ [BCE97]). Erwartungserwartungen sind wiederum die Erwartungen der einen Seite, dass die gegenüberliegenden Seite Erwartungen an sie adressiert, und sich entsprechend dieser Erwartungen verhält.(S.418 [KE06]).

Ein mögliche Erwartung des Managements im ISMS-Bereich kann beispielsweise sein, dass das Schulen von Mitarbeitern sich positiv auf deren Verhalten im Bezug auf die Informationssicherheit auswirkt (7.2 [ISO22]).

Eine Erwartungserwartung wäre, dass die Mitarbeiter erwarten, dass das Management von ihnen eine Verbesserung im Verhalten nach der Schulung erwartet. [42]

Die Systeme tauschen dann das mögliche Handlungsspektrum des jeweils anderen Systems durch das zu erwartende Handlungsspektrum aus.

[42] Für ein weiteres Beispiel vergleiche [KE06] S.418

Hält mich beispielsweise ein Polizist in einer Verkehrskontrolle an, gehe ich nicht davon aus, dass dieser mit mir über die Vorlesung zu Thermodynamik einer japanischen Universität reden möchte. Vielmehr erwarte ich, dass er mit mir über mein kaputtes Rücklicht reden möchte.

Damit erlangen die Systeme die Möglichkeit, eine Handlung auf Basis der als Reaktion zu erwartenden Handlungen des gegenüberliegenden Systems durchzuführen. Ich übe im Kopf bereits meine Ausrede, warum das Rücklicht kaputt ist. Der Polizist bereitet schon einmal den Strafzettel vor, da er bereits beschlossen hat, dass ihn meine Ausrede sowieso nicht interessiert.

Die Planung des ISMS muss ebenfalls Erwartungen und Annahmen für die Entwicklung von Maßnahmen formulieren. Angriffe, die die Maßnahmen adressieren sollen, liegen in der Zukunft und gehen von einem selbstgesteuerten Angreifer aus. Die Planung muss also Erwartungen über das wahrscheinliche Verhalten des Angreifers haben, um in der Gegenwart wirksame Maßnahmen zu formulieren.

Der Angreifer stellt seinerseits Erwartungen an die Organisation und deren Sicherheitsmaßnahmen.

Die sich daraus ergebende Dynamik ist im Kreis der Darstellung von Abb. 11 visualisiert:

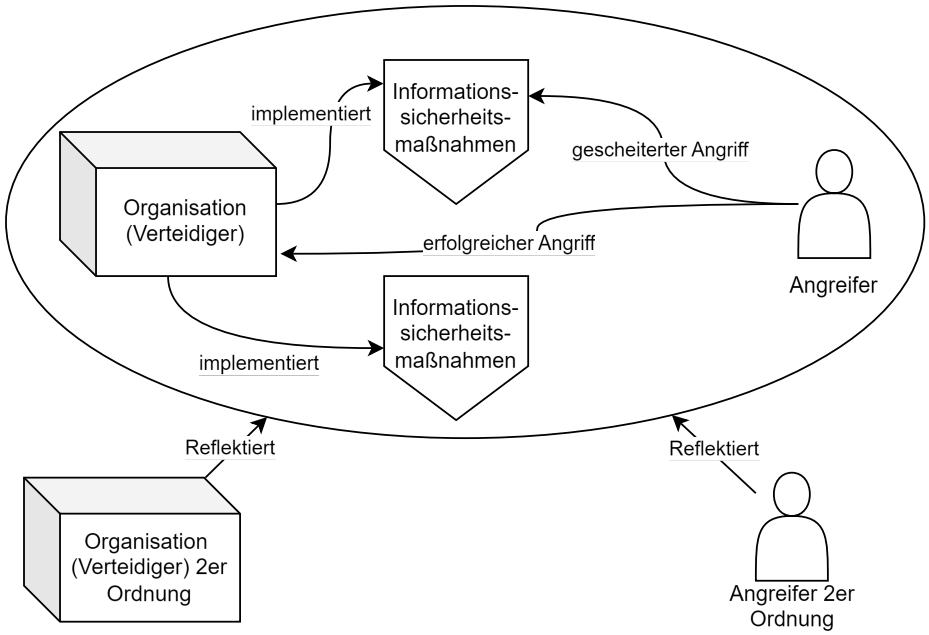

Abbildung 11: Illustration der Dynamik zwischen einer Organisation, die sich mit Maßnahmen schützen möchte, und einem Angreifer, welcher der Organisation schaden möchte. Ergänzt durch Reflektion dieser Dynamik durch Organisation und Angreifer auf zweiter Ordnung. Grafik inspiriert durch Abbildungen 8-1 und 8-2 aus [AH22]

Die Organisation implementiert Maßnahmen in der Hoffnung, die Angriffe des feind-

lichen Akteurs abzufangen. Der Angreifer versucht mit seinen Angriffen, trotz dieser Sicherheitsmaßnahmen erfolgreich zu sein.[43]

Wie bereits die Kritik aus Kapitel 5.2 anmerkt, ist der Angreifer daher gut beraten, die Erwartungen und Maßnahmen zu brechen und Sicherheitsmaßnahmen auf unerwarteten Wegen zu umgehen. Würde er die Erwartungen der verteidigenden Organisation erfüllen, würden seine Angriffe genau auf die Maßnahmen treffen, die seine Angriffe verhindern sollen.

Ein Beispiel für erwartungsbrechendes Angreiferverhalten ist ein Handbuch für Sabotage von Organisationen, welches aus der Zeit des zweiten Weltkriegs stammt. Das „Simple Sabotage Field Manual“ [Off44] (zu deutsch: „Das kleine Sabotage-Handbuch“ [Sch18]) enthält entgegen der Erwartungen keine Anleitungen zum Bauen von Bomben, sondern Hinweise wie „Insist on doing everything through „channels“. Never permit shortcuts to be taken in order to expedite decisions“ oder „Hold up mail until the next collection“(vgl. S.28ff [Off44]).

Die Planung des ISMS muss sich wiederum bewusst sein, dass ihre Maßnahmen stets nur ihre Erwartungen eines Angreifers adressieren. Tatsächliche Bedrohungen können potentiell beliebig davon abweichen. In diesem Zusammenhang sei angemerkt, dass Luhmann darauf hinweist, dass die Beobachtung der Umwelt entsprechend eine wichtige Quelle vieler Unsicherheiten in der Organisation ist (S.209f. [Luh11]), da hierbei die Beobachtung der Umwelt und die darauf getroffenen Entscheidungen fehlerhaft sein können.

Eine Sicherheit vor Angriffen ist somit nie garantiert. Hierauf macht auch der ISO 27000 aufmerksam: „Es sollte beachtet werden, dass kein Satz von Maßnahmen vollständige Informationssicherheit erreichen kann.“ (S.26 [ISO20]).

Sowohl Angreifer als auch Verteidiger müssen für die Beobachtung, was der jeweils andere erwartet, Abstand von ihren Erwartungen nehmen und diese von „außen“ reflektieren.

Dieses Reflektieren lässt sich mit der Unterscheidung von Kybernetik erster und zweiter Ordnung nach Heinz von Foerster erklären (vgl. [VFF02]).

Die Beobachtung erster Ordnung erfolgt aus dem kybernetischen System heraus (in dem Kreis von Abb. 11). Man betrachtet die Welt sozusagen durch die getroffenen Erwartungen. Die Planung des ISMS bezieht beispielsweise aus historischen Daten und Expertenmeinungen (vgl. 3.68 Anmerkung 2 [ISO20]), was die aktuell häufigsten Angriffe sind und reflektiert diese auf ihre Organisation.

Die Beobachtung zweiter Ordnung tritt aus dem System heraus und betrachtet es von

[43] Für eine mögliche Taxonomie von Angriffsmotivationen siehe [LN22] S.19ff.

außen. Die Planung des ISMS betrachtet nicht, welche Angriffe häufig sind, sondern das aktuelle Verständnis, was sie als Angriffe verstehen.

Diese analytische Ebene ermöglicht die Entwicklung von Methodiken, wie es die Autoren von [AH22] beispielsweise in ihrem Lernprozess für die agile Prüfung von Organisationen in zwei Phasen tun, angelehnt an [BHB17].

In der Phase des umsetzungsorientierten Lernens gilt: „Der Lernende verändert innerhalb eines bestimmten Kontextes sein Verhalten, indem er dieses durch Versuch und Irrtum optimiert und sich dadurch neues Wissen erwirbt.“ (S.379 [BHB17]). Auf das ISMS bezogen bedeutet dies, dass der Verteidigende bei seiner Konzeption des Angreifers bleibt. Ausgehend von diesem Bild überlegt sich der Verteidigende Maßnahmen, um erwartete Angriffe zu adressieren.

In der Phase des reflektierenden Lernens sind die Annahmen des Verteidigenden über den Angreifer das Ziel der Beobachtung: „Bei dieser Form des Lernens wird versucht, durch Reflexion etwas Abstand von der Situation zu bekommen. Aus der damit gewonnenen Distanz zum umsetzungsorientierten Handlungskontext wird dann die Gesamtsituation reflektiert und hinterfragt.“ (S.38 [AH22]).

Für ein besseres Verständnis des Unterschieds zwischen Reflexionen erster und zweiter Ordnung führt der Abschnitt einige Beispiele an:

Am Beispiel des „Simple Sabotage Field Manual“ wäre eine Beobachtung zweiter Ordnung beispielsweise, den Begriff der Sabotage zu hinterfragen. So könnte man den Begriff der Sabotage anders erfassen und neben Sprengstoffangriffen auch das gelegentliche Vergessen wichtiger Unterlagen für ein Meeting einschließen. Eine Beobachtung erster Ordnung hingegen wäre die Ausarbeitung von Sabotagemaßnahmen anhand der Vorstellungen des Handbuchs.

Ein weiteres Beispiel für Beobachtung zweiter Ordnung stellt der Bericht [Gau+22] des European Union Institute for Security Studies (EUISS) dar. Der Bericht hinterfragt, was passieren würde, wenn aktuelle Annahmen nicht korrekt wären. Beispielsweise wird untersucht, was es für die Sicherheitslage Europas bedeuten würde, wenn nicht jede Militärintervention wie Afghanistan enden würde (vgl. S.18-22 [Gau+22]) oder wenn das Vereinigte Königreich der Europäischen Union wieder beitreten würde (vgl. S.48-52 [Gau+22]).

Die Beobachtung zweiter Ordnung äußert sich durch das Hinterfragen aktueller Annahmen. Zum Beispiel könnte man hinterfragen, ob das „Nation Building“ (zu deutsch „Nationenbildung“) wie in Afghanistan zum Scheitern verurteilt ist. Ein weiteres Beispiel wäre das Hinterfragen, ob das Vereinigte Königreich der Europäischen Union wirklich endgültig den Rücken gekehrt hat.

Beobachtungen zweiter Ordnung im Bezug auf das ISMS könnten beispielsweise das Hinterfragen der Rolle von Maßnahmen umfassen. Sind Maßnahmen tatsächlich nur als Abwehr gegen Angreifer zu verstehen, oder bringen sie ebenfalls Gefahren mit sich, die Angreifer ausnutzen können? Ein mögliches Beispiel wäre die Einführung einer Network-Security-Monitoring-Software zur Überwachung des Datenverkehrs in der Organisation. Was wäre, wenn diese von Angreifern korrumpiert würde und von diesen zur Spionage des Datenverkehrs in der Organisation genutzt würde?

Ein weiteres Beispiel für eine Beobachtung zweiter Ordnung im Kontext des ISMS wäre die Reflexion der Rolle von Mitarbeitern. Grundsätzlich versteht die Planung diese als Organisationsmitglieder und nicht gleichzeitig als potenzielle Angreifer. Diese Annahme lässt die Möglichkeit außer Acht, dass ein Mitglied als Innentäter agieren und bewusst der Organisation schaden könnte. Ein Ansatz, der dieser Annahme entgegenwirkt, ist eine sogenannte „Zero Trust"-Architektur, die versucht, die Berechtigungen von Organisationsmitgliedern auf technischem Weg zu minimieren [Bun23].

Anhand der verschiedenen Beispiele zu Beobachtungen erster und zweiter Ordnung wird deutlich, dass die möglichen Szenarien, die sich bei solchen Reflexionen auftun, schnell den Rahmen des Handhabbaren übersteigen.

Zusätzlich sei betont, dass auch mit einer Methodik, die Reflexionen auf der zweiten Ebene einbezieht, keine Sicherheit einhergeht. Die Reflexionen beziehen sich immer auf das zukünftige Verhalten von Angreifern und versuchen somit, das Verhalten selbststeuernder Systeme vorherzusehen, was per Definition nicht vorhersehbar ist.

Erschwerend kommt hinzu, dass die Umwelt als Differenz zur Organisation einem Komplexitätsgefälle unterliegt und im Verhältnis zum System komplexer ist (S.197 [BCE97]). Wegen der vergleichsweise höheren Komplexität sind die Erfolgschancen einer dauerhaften Prognostizierung aller Angriffe entsprechend gering.[44]

Anhand der ausführlichen Beispiele lässt sich erkennen, dass die Systemtheorie auch im Falle der Bedeutung der Umwelt für das ISMS eine umfassendere Basis für Erklärungen bietet als die klassische Managementtheorie. Alleine am Beispiel der Dynamik zwischen Angreifer und Verteidiger zeigt sich, dass die Systemtheorie mit ihrer Annahme von selbststeuernden Organisationen in der Lage ist, deutlich weitreichendere Aussagen zu treffen als die passive Darstellung der klassischen Managementtheorie.

Diese Fähigkeit, weitreichendere Aussagen zu treffen, können Verantwortliche in der Praxis nutzen, um „über den Tellerrand" von Standardsicherheitsmaßnahmen wie denen des ISO 27002 hinauszudenken und sich auch gegen Angriffe außerhalb dieser Konzep-

[44] Siehe hierzu auch die Notwendigkeit von Steuerung in Kapitel 6.2.1

tion zu wappnen.

6.4 Zusammenfassung

Dieses Kapitel beschäftigte sich mit der Erarbeitung einer systemtheoretischen Betrachtung des ISMS. Dafür bildeten die Kritikpunkte aus dem vorherigen Kapitel einen Ausgangspunkt anhand dessen die Erklärbarkeit der Systemtheorie nach Luhmann für das ISMS demonstriert wurde. Dabei beleuchteten die verschiedenen Abschnitte das Management, die Organisation und die Umwelt des ISMS. Das Kapitel konnte in allen drei Bereichen belegen, dass die Systemtheorie nach Luhmann im Vergleich zur klassischen Managementtheorie deutlich differenziertere und umfassendere Betrachtungen relevanter Dynamiken des ISMS ermöglicht. Diese gesteigerte Erklärbarkeit öffnet Praktikern das Blickfeld auf die Komplexität von Sicherheitsmaßnahmen.

7 Resümee

Dieses Kapitel schließt die Arbeit zur systemtheoretischen Betrachtung des ISMS ab. Es weist auf die Limitationen der vorliegenden Arbeit hin, zeigt mögliche Entwicklungsrichtungen auf und endet mit einer Zusammenfassung der wichtigsten Ergebnisse.

7.1 Limitationen

Dieser Abschnitt bespricht zwei Limitationen, welche die Ergebnisse dieser Arbeit in ihrer allgemeinen Aussagekraft einschränken. Beide Grenzen gehen dabei auf die Konzeption der Systemtheorie nach Luhmann zurück.

Die erste Limitation der Ergebnisse ergibt sich daraus, dass die Systemtheorie eigentlich keine direkte Betrachtung des Managements zulässt. Dies liegt darin begründet, dass die Organisation an sich selbststeuernd ist und somit eine zielgerichtete Beeinflussung durch das Management nicht vorsieht. Dies erschwert eine Konzeption des ISMS auf Basis der Systemtheorie. Kapitel 6.1.2 thematisierte diese Problematik bereits. Das Kapitel folgt dabei der Argumentation von [SK20] und [KE06], dass die Nutzung der Systemtheorie auf einer verständnisorientierten Ebene geschehen muss. Mit einer verständnisorientierten Nutzung besteht allerdings die Gefahr, die Theorie in einer nicht konsistenten Art und Weise zu interpretieren. Dem wird in der vorliegenden Thesis durch die Herstellung von klaren Bezügen auf die Systemtheorie an den entsprechenden Stellen vorgebeugt.

Die zweite Limitation bezieht sich auf die Überprüfbarkeit der Ausführungen in dieser Arbeit. Die Systemtheorie ist nach dem Verständnis von [PP73] keine wissenschaftliche Theorie, genauso wie beispielsweise der Marxismus oder die Mathematik in diesem Sinne keine sind. Dies begründet sich darin, dass sich die Systemtheorie von Luhmann nicht falsifizieren lässt. Denn mit dem Anspruch, alle sozialen Phänomene erfassen zu können, entzieht sich diese jedweder empirischen Widerlegung. Würde eine solche empirische Validierung angestrebt, könnten sowohl ein positives Resultat als auch ein negatives Resultat wieder im Rahmen der Theorie beschrieben werden. Aus der fehlenden empirischen Widerlegbarkeit der Theorie folgt, dass ein anderes Qualitätsmaß zur Bewertung der Theorie als Basis für das ISMS und der Erkenntnisse in dieser Arbeit nötig ist.

Die Arbeit hat versucht, die Qualität der Theorie als Basis für das ISMS über den Vergleich mit einer konkurrierenden Theorie, der klassischen Managementtheorie, zu belegen. Zudem wurden von anderen Forschern aufgeworfene Fragen und damit wis-

senschaftlich gut belegte Phänomene aus dem Arbeitsalltag des ISMS herangezogen, die von der Theorie gut erklärt werden konnten. Deren „Korrektheit“ in Form von empirischen Untersuchungen zu belegen, bietet sich darüber hinaus als eine von mehreren Entwicklungsrichtungen für weiterführende wissenschaftliche Arbeiten an. Diese Entwicklungsrichtungen bespricht der nächste Abschnitt detaillierter.

7.2 Weitere Entwicklungsrichtungen

Die Arbeit hat gezeigt, dass die Systemtheorie eine differenzierte Betrachtung der Dynamiken eines ISMS innerhalb und außerhalb einer Organisation ermöglicht und eine umfassendere theoretische Basis als die klassische Managementtheorie bietet. Daraus ergeben sich mehrere potenzielle Entwicklungsrichtungen:

1. Die Analyse von Zielkonflikten und Paradoxien ist ein zentraler Aspekt der Systemtheorie nach Luhmann, welcher im Rahmen dieser Arbeit nicht angeschnitten werden konnte. Es wäre interessant, die in der Praxis wichtigen Spannungsfelder des ISMS auf Basis der Systemtheorie zu erarbeiten. Mögliche Einstiegspunkte hierfür wären beispielsweise die verschiedenen Schutzziele (z.B. Vertraulichkeit vs. Verfügbarkeit in bestimmten Kontexten).

2. Es besteht die Möglichkeit, weitere Elemente der Systemtheorie in Bezug auf das ISMS zu reflektieren z.B. die drei Formen der entschiedenen Entscheidungsprämissen: Programme, Kommunikationswege und Personen.

3. Die Ausdehnung der Betrachtung von anlehnenden Bereichen, beispielsweise auf den Bereich des Safety-Managements und dessen Integration mit IT-Sicherheitsmaßnahmen.

4. Die Untersuchung des ISMS anhand von Fallstudien in verschiedenen Organisationen, welche sich in ihren Beobachtungen auf die Systemtheorie nach Luhmann stützen.

7.3 Zusammenfassung

Diese Masterarbeit widmete sich der systemtheoretischen Betrachtung von Informationssicherheitsmanagementsystemen auf Basis der Systemtheorie nach Niklas Luhmann. Die zentrale Fragestellung bestand darin, zu erforschen, inwiefern die Systemtheorie eine geeignete theoretische Grundlage für eine umfassende und differenzierte Erklärung des ISMS bietet.

Hierzu führte die Arbeit die klassische Managementtheorie als alternative theoretische Basis ein und demonstrierte, inwieweit damit Phänomene des ISMS sowie die Anforderungen entsprechender Industriestandards erklärt werden konnten. Dabei wurde deutlich, dass diese Theorie bestimmte Limitationen aufweist, wie die differenzierte Betrachtung von Dynamiken außerhalb der Maschinenmetapher der Organisation oder die Darstellung der Umwelt über passive zu berücksichtigende Faktoren hinaus.

Diese Kritikpunkte nahm das darauf folgende Kapitel als Ausgangspunkt, um die Systemtheorie nach Luhmann als umfassendere und differenziertere Erklärungsbasis für das ISMS zu demonstrieren. Dabei wurde am Ende der Kapitel auch auf mögliche Vorteile der gesteigerten Erklärbarkeit für die Praxis verwiesen. Dank der Konzeption von Organisationen als selbststeuernd lassen sich mit der Theorie bisher unzureichende oder nicht erfasste Herausforderungen bei der Umsetzung eines ISMS erklären. Die erfassten Herausforderungen lassen sich dann zweckdienlicher für in einem konkreten Kontext adressieren. Diese Arbeit hat diesen Effekt insbesondere an drei Aspekten herausgearbeitet:

Die Beziehung des Managements und der Organisation: Diese lässt sich nicht hinreichend komplex durch eine einfache Ursache-Wirkungsbeziehung von Maßnahmen und der Verbesserung der Informationssicherheit, wie in der klassischen Managementtheorie, abbilden. Es wurde gezeigt, dass die Selbststeuerung der Organisation eine praxisnähere Abbildung der Gegebenheiten in einer Organisation ermöglicht, in dem sie dem Umstand Rechnung trägt, dass Abweichungen von geplanten Maßnahmen nicht eine Ausnahme sondern die Regel darstellen. Diese praxisnähere Darstellung entlastet sowohl das Management als auch die Mitarbeiter von der „Schuldfrage“, wenn Informationssicherheitsmaßnahmen nicht zur gewünschten Verbesserung führen. Die systemtheoretische Betrachtung des ISMS abstrahiert von diesen personenbezogenen Debatte und fokussiert sich dafür auf die Organisation und warum die Organisation nicht wie gewünscht auf die Anpassung des ISMS reagiert.

Informelle Strukturen der Organisation: Aufbauend auf der Selbststeuerung von Organisationen konnte die Arbeit zeigen, dass die Systemtheorie in der Lage ist, die informellen Strukturen einer Organisation differenzierter darzustellen als die klassische Managementtheorie. Neben den Teilen, die sich direkt durch das Management formen lassen, bleibt in der Systemtheorie nach Luhmann immer ein Rest, die sogenannte Organisationskultur. Diese entzieht sich per Definition einer direkten Beeinflussung durch die

Verantwortlichen des ISMS, hat jedoch Implikationen auf die Verbesserung der Informationssicherheit. Durch die Anerkennung dieser Organisationskultur kann die Systemtheorie nach Luhmann „weiche Faktoren“ bei der Umsetzung eines ISMS berücksichtigen. Praktiker sind auf dieser Basis eher in der Lage, die Informationssicherheitsmaßnahmen im Hinblick auf deren soziale Anschlussfähigkeit an die Organisation zu reflektieren und so potentiell zweckdienlichere Maßnahmen zur Verbesserung der Informationssicherheit zu ersinnen.

Dynamik zwischen Angreifern und Verteidigern: Zuletzt war es auf Basis dieser Unsicherheit möglich, die Dynamiken zwischen Angreifern und Verteidigern sowohl in einem gegebenen Kontext zu interpretieren als auch aus diesem Kontext herauszutreten und diesen aus einer Vogelperspektive zu betrachten. Damit eröffnete die Theorie die Möglichkeit, die eigenen Erwartungen in Bezug auf Informationssicherheitsangriffe zu reflektieren und den Raum möglicher Angriffsszenarien gedanklich zu erweitern. Praktiker können dies für die Entwicklung von Sicherheitsmaßnahmen nutzen, indem sie sowohl auf erwartete Angriffe mit Standardsicherheitsmaßnahmen wie denen des ISO 27002 reagieren, als auch abwegigere Szenarien außerhalb des aktuellen Konsenses als mögliche Quellen für Informationssicherheitsvorfälle durchdenken und bei Bedarf adressieren können.

Zusammenfassend lässt sich festhalten, dass anhand dieser drei Aspekte gezeigt werden konnte, dass die Systemtheorie in der Lage ist, die Limitationen der klassischen Managementtheorie zu überwinden. Sie adressiert die angebrachten Kritikpunkte durch eine umfassendere und differenziertere Erklärungsbasis. Die Systemtheorie nach Luhmann stellt somit aufgrund ihrer Komplexität eine vielversprechende Grundlage für die theoretische und praktische Weiterentwicklung des ISMS dar.

Quellenverzeichnis

[U.S49] U.S. Department of Defense. *Procedure for Performing a Failure Mode, Effects, and Criticality Analysis*. Military Standard. 1949.

[Bun15] Bundesrepublik Deutschland. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 1.0)*. Juli 2015. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1713555101460.

[Bun16] Bundesrepublik Deutschland. *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung)*. Published: Bundesgesetzblatt Teil I Nr. 14. 2016. URL: https://www.gesetze-im-internet.de/bsi-kritisv/.

[BSI17] BSI. *BSI-Standard 200-1*. de. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.html?nn=128578 (besucht am 07. 12. 2023).

[ISO20] ISO. *DIN EN ISO/IEC 27000:2020-06, Informationstechnik- Sicherheitsverfahren-Informationssicherheitsmanagementsysteme- Überblick und Terminologie (ISO/IEC_27000:2018); Deutsche Fassung EN_ISO/IEC_27000:2020*. 2020. DOI: 10.31030/3144079.

[Bun21] Bundesrepublik Deutschland. *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)*. Published: Bundesgesetzblatt Teil I Nr. 31. Mai 2021. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s1122.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1122.pdf%27%5D__1713555081825.

[ISO22] ISO ISO. *DIN EN ISO/IEC 27002 Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022); Deutsche Fassung EN ISO/IEC 27002:2022*. 2022. (Besucht am 14. 03. 2024).

[ISO23] ISO ISO. *DIN EN ISO/IEC 27001, Informationssicherheit, Cybersicherheit und Datenschutz –Informationssicherheitsmanagementsysteme –Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023*. de. 2023.

Literatur

[Off44] Office of Strategic Services. *Simple Sabotage Field Manual*. Washington, D.C.: United States Government Printing Office, 1944.

[KO55] H. Koontz und C. O'Donnell. *Principles of Management: An Analysis of Managerial Functions*. International student ed. McGraw-Hill, 1955.

[Mac69] Mackenzie, Alec R. „The management process 3-D". In: *Harvard Business Review* 47 (1969), S. 81–86.

[WW72] Max Weber und Johannes Winckelmann. *Wirtschaft und Gesellschaft: Grundriß der verstehenden Soziologie*. ger. Studienausg., 5., rev. Aufl. Tübingen: Mohr, 1972. ISBN: 978-3-16-533631-3.

[PP73] Karl R. Popper und Karl R. Popper. *Logik der Forschung*. ger. 5. Aufl., Nachdr. der 4., verb. Aufl. Die Einheit der Gesellschaftswissenschaften Bd. 4. Tübingen: Mohr, 1973. ISBN: 978-3-16-532711-3.

[Mat87] Humberto Maturana. „Repräsentation und Kommunikation". In: *Erkennen: Die Organisation und Verkörperung von Wirklichkeit*. Hrsg. von Humberto Maturana. Braunschweig: Vieweg, 1987, S. 272–296.

[Dav89] Fred D. Davis. „Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". In: *MIS Quarterly* 13.3 (Sep. 1989), S. 319. ISSN: 02767783. DOI: 10.2307/249008.

[SG89] Susan Leigh Star und James R. Griesemer. „Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907-39". In: *Social Studies of Science* 19.3 (1989). Publisher: Sage Publications, Ltd., S. 387–420. URL: http://www.jstor.org/stable/285080.

[TF90] Louis G. Tornatzky und Mitchell Fleischer. *The processes of technological innovation*. eng. 4. print. Issues in organization and management series. Lexington, Mass.: Lexington Books, 1990. ISBN: 978-0-669-20348-6.

[Bar91] Jay Barney. „Firm Resources and Sustained Competitive Advantage". en. In: *Journal of Management* 17.1 (März 1991), S. 99–120. ISSN: 0149-2063, 1557-1211. DOI: 10.1177/014920639101700108.

[Foe93] Heinz von Foerster. „Prinzipien der Selbstorganisation im sozialen und betriebswirtschaftlichen Bereich“. In: Hrsg. von Siegfried J. Schmidt. 1. Aufl. Num Pages: 396. Frankfurt: Suhrkamp, 1993, S. 233–268. ISBN: 3-518-28476-2.

[BCE97] Claudio Baraldi, Giancarlo Corsi und Elena Esposito. *GLU: Glossar zu Niklas Luhmanns Theorie sozialer Systeme*. 1. Aufl. Suhrkamp Taschenbuch Wissenschaft 1226. Frankfurt am Main: Suhrkamp, 1997. ISBN: 978-3-518-28826-9.

[DH97] Arthur M. (Art) Dowell und Dennis C. Hendershot. „No good deed goes unpunished: Case studies of incidents and potential incidents caused by protective systems“. In: *Process Safety Progress* 16 (1997). URL: https://api.semanticscholar.org/CorpusID:110177499.

[PC98] Christine M. Pearson und Judith A. Clair. „Reframing Crisis Management“. In: *The Academy of Management Review* 23.1 (Jan. 1998), S. 59. ISSN: 03637425. DOI: 10.2307/259099.

[AS99] Anne Adams und Martina Angela Sasse. „Users are not the enemy“. en. In: *Communications of the ACM* 42.12 (Dez. 1999), S. 40–46. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/322796.322806.

[Luh99] Niklas Luhmann. *Funktionen und Folgen formaler Organisation: mit einem Epilog 1994*. ger. 5. Auflage. Schriftenreihe der Hochschule Speyer 20. Berlin: Duncker & Humblot, 1999. ISBN: 978-3-428-08341-1.

[BA02] Chester Irving Barnard und Kenneth R. Andrews. *The functions of the executive*. eng. 30. anniversary ed. with an introd. by Kenneth R. Andrews, 39. print. Cambridge, Mass.: Harvard Univ. Press, 2002. ISBN: 978-0-674-32803-7.

[Cle02] Stewart Clegg. *Frameworks of power*. eng. Reprint. London: Sage, 2002. ISBN: 978-0-8039-8160-7 978-0-8039-8161-4.

[VFF02] Heinz Von Foerster und Heinz von Foerster. *Short Cuts*. ger. Orig.-Ausg., 2. Aufl. Short cuts 5. Frankfurt am Main: Zweitausendeins, 2002. ISBN: 978-3-86150-305-7.

[Han03] Michael J. Handel, Hrsg. *The sociology of organizations: classic, contemporary, and critical readings*. Thousand Oaks: Sage Publications, 2003. ISBN: 978-0-7619-8766-6.

[Tay04] Frederick Winslow Taylor. *Scientific Management*. en. 0. Aufl. Routledge, Juni 2004. ISBN: 978-1-134-46624-5. DOI: 10.4324/9780203498569.

[LBL05] Niklas Luhmann, John Bednarz und Niklas Luhmann. *Social systems*. eng. Reprinted. Writing science. Stanford, Calif: Stanford Univ. Press, 2005. ISBN: 978-0-8047-2625-2.

[Min05] Henry Mintzberg. *Managers not MBAs: a hard look at the soft practice of managing and management development*. eng. OCLC: 567912043. San Francisco, CA: Berrett-Koehler Pub., 2005. ISBN: 978-1-57675-511-2.

[Tag05] Nancy R. Tague. *The quality toolbox*. 2nd ed. Milwaukee, Wis: ASQ Quality Press, 2005. ISBN: 978-0-87389-639-9.

[KB06] Laree Kiely und Terry Benzel. „Systemic Security Management“. In: *IEEE Security and Privacy Magazine* 4.6 (Nov. 2006), S. 74–77. ISSN: 1540-7993. DOI: 10.1109/MSP.2006.167.

[KE06] Alfred Kieser und Mark Ebers, Hrsg. *Organisationstheorien*. ger. 6., erw. Aufl. W: Stuttgart: Kohlhammer, 2006. ISBN: 978-3-17-019281-2.

[Sen06] Peter M. Senge. *The fifth discipline: the art and practice of the learning organization*. eng. Rev. and updated ed. A Currency book. New York, NY: Currency Doubleday, 2006. ISBN: 978-0-385-51725-6 978-0-385-51782-9.

[BSW08] Adam Beautement, M. Angela Sasse und Mike Wonham. „The compliance budget: managing security behaviour in organisations“. en. In: *Proceedings of the 2008 New Security Paradigms Workshop*. Lake Tahoe California USA: ACM, Sep. 2008, S. 47–58. ISBN: 978-1-60558-341-9. DOI: 10.1145/1595676.1595684.

[Ber09] Ludwig von Bertalanffy. *General system theory: foundations, development, applications*. eng. Rev. ed., 17. paperback print. New York, NY: Braziller, 2009. ISBN: 978-0-8076-0453-3.

[ISA09] ISACA. „An Introduction to the Business Model for Information Security“. In: ISACA, 2009.

[KCY09] Cheng-Yuan Ku, Yi-Wen Chang und David C. Yen. „National information security policy and its implementation: A case study in Taiwan“. en. In: *Telecommunications Policy* 33.7 (Aug. 2009), S. 371–384. ISSN: 03085961. DOI: 10.1016/j.telpol.2009.03.002.

[NP09] Anand Nair und Daniel Prajogo. „Internalisation of ISO 9000 standards: the antecedent role of functionalist and institutionalist drivers and performance implications“. en. In: *International Journal of Production Research* 47.16 (Aug. 2009), S. 4545–4568. ISSN: 0020-7543, 1366-588X. DOI: 10.1080/00207540701871069.

[Win09] Robert Winter. „Was ist eigentlich Grundlagenforschung in der Wirtschaftsinformatik?“ de. In: *WIRTSCHAFTSINFORMATIK* 51.2 (Apr. 2009), S. 223–231. ISSN: 0937-6429, 1861-8936. DOI: 10.1007/s11576-008-0130-1.

[AH10] T. Asai und A.U. Hakizabera. „Human-related problems of information security in East African cross-cultural environments“. en. In: *Information Management & Computer Security* 18.5 (Nov. 2010). Hrsg. von Steven M. Furnell, S. 328–338. ISSN: 0968-5227. DOI: 10.1108/09685221011095245.

[IS10] Philip G. Inglesant und M. Angela Sasse. „The true cost of unusable password policies: password use in the wild“. en. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Atlanta Georgia USA: ACM, Apr. 2010, S. 383–392. ISBN: 978-1-60558-929-9. DOI: 10.1145/1753326.1753384.

[Pow10] Michael Power. *Organized uncertainty: designing a world of risk management*. eng. Reprinted. Oxford: Oxford Univ. Press, 2010. ISBN: 978-0-19-954880-4 978-0-19-925394-4.

[Smi+10] Smith u. a. „Circuits of Power: A Study of Mandated Compliance to an Information Systems Security ”De Jure” Standard in a Government Organization“. In: *MIS Quarterly* 34.3 (2010), S. 463. ISSN: 02767783. DOI: 10.2307/25750687.

[VR10] Rolf Von Roessing. „The ISACA Business Model for Information Security: An Integrative and Innovative Approach“. en. In: *ISSE 2009 Securing Electronic Business Processes*. Hrsg. von Norbert Pohlmann, Helmut Reimer und Wolfgang Schneider. Wiesbaden: Vieweg+Teubner, 2010, S. 37–47. ISBN: 978-3-8348-0958-2 978-3-8348-9363-5. DOI: 10.1007/978-3-8348-9363-5_4.

[Kü11] Stefan Kühl. *Organisationen*. de. Wiesbaden: VS Verlag für Sozialwissenschaften, 2011. ISBN: 978-3-531-17978-0 978-3-531-93185-2. DOI: 10.1007/978-3-531-93185-2.

[Luh11] Niklas Luhmann. *Organisation und Entscheidung*. ger. 3. Auflage. Wiesbaden: VS Verlag, 2011. ISBN: 978-3-531-17817-2.

[VWYDV11] Robert Van Wessel, Xu Yang und Henk J. De Vries. „Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study“. en. In: *Technology Analysis & Strategic Management* 23.8 (Sep. 2011), S. 865–879. ISSN: 0953-7325, 1465-3990. DOI: 10.1080/09537325.2011.604155.

[Rod12] Darío. Rodróguez. *Gestión Organizacional*. spa. OCLC: 1374010371. S.l.: Ediciones UC, 2012. ISBN: 978-956-14-1212-5.

[FS13] Otto K. Ferstl und Elmar J. Sinz. *Grundlagen der Wirtschaftsinformatik*. ger. 7., aktualisierte Aufl. München: Oldenbourg, 2013. ISBN: 978-3-486-71353-4.

[BS14] M Bada und A Sasse. „Cyber Security Awareness Campaigns: Why do they fail to change behaviour?“ In: Place: Oxford, UK. Global Cyber Security Capacity Centre, University of Oxford, 2014.

[KPS14] Iacovos Kirlappos, Simon Parkin und M. Angela Sasse. „Learning from “Shadow Security:” Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security“. en. In: *Proceedings 2014 Workshop on Usable Security*. San Diego, CA: Internet Society, 2014. ISBN: 978-1-891562-37-2. DOI: 10.14722/usec.2014.23007.

[PSF14] Shari Lawrence Pfleeger, M. Angela Sasse und Adrian Furnham. „From Weakest Link to Security Hero: Transforming Staff Security Behavior“. en. In: *Journal of Homeland Security and Emergency Management* 11.4 (Dez. 2014), S. 489–510. ISSN: 1547-7355, 2194-6361. DOI: 10.1515/jhsem-2014-0035.

[BYU15] Zahari Bakar, Noorulsadiqin Yaacob und Zulkifli Udin. „The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework“. In: *International Journal of Economics and Financial Issues* 5.1S (Juli 2015), S. 128–134. ISSN: 2146-4138.

[BBS15] Odette Beris, Adam Beautement und M. Angela Sasse. „Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors“. en. In: *Proceedings of the 2015 New Security Paradigms Workshop*. Twente Netherlands: ACM,

Sep. 2015, S. 73–84. ISBN: 978-1-4503-3754-0. DOI: 10.1145/2841113.2841119.

[HKR15] Masoud Hayeri Khyavi und Mina Rahimi. „The Missing Circle of ISMS (LL-ISMS)“. en. In: *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. Newport Beach California USA: ACM, Juni 2015, S. 73–77. ISBN: 978-1-4503-3557-7. DOI: 10.1145/2751957.2751972.

[Nil15] Per Nilsen. „Making sense of implementation theories, models and frameworks“. en. In: *Implementation Science* 10.1 (Dez. 2015), S. 53. ISSN: 1748-5908. DOI: 10.1186/s13012-015-0242-0.

[Sas15] Angela Sasse. „Scaring and Bullying People into Security Won't Work“. In: *IEEE Security & Privacy* 13.3 (Mai 2015), S. 80–83. ISSN: 1540-7993. DOI: 10.1109/MSP.2015.65.

[Rob16] Brian J. Robertson. *Holacracy: ein revolutionäres Management-System für eine volatile Welt*. ger. Übers. von Mike Kauschke. München: Verlag Franz Vahlen, 2016. ISBN: 978-3-8006-5087-3.

[BHB17] Gregory Bateson, Hans Günter Holl und Gregory Bateson. *Ökologie des Geistes: anthropologische, psychologische, biologische und epistemologische Perspektiven*. ger. 12. Aufl. Suhrkamp-Taschenbuch Wissenschaft 571. Frankfurt am Main: Suhrkamp, 2017. ISBN: 978-3-518-28171-0.

[LSK17] Niklas Luhmann, Johannes F. K. Schmidt und André Kieserling. *Systemtheorie der Gesellschaft*. ger. Erste Auflage. Berlin: Suhrkamp, 2017. ISBN: 978-3-518-58705-8.

[PJF17] Hans-Rüdiger Pfister, Helmut Jungermann und Katrin Fischer. *Die Psychologie der Entscheidung: Eine Einführung*. de. Berlin, Heidelberg: Springer Berlin Heidelberg, 2017. ISBN: 978-3-662-53037-5 978-3-662-53038-2. DOI: 10.1007/978-3-662-53038-2.

[SWM17] Anselm Schneider, Christopher Wickert und Emilio Marti. „Reducing Complexity by Creating Complexity: A Systems Theory Perspective on How Organizations Respond to Their Environments“. en. In: *Journal of Management Studies* 54.2 (März 2017), S. 182–208. ISSN: 0022-2380, 1467-6486. DOI: 10.1111/joms.12206.

[SCC17] Arbia Riahi Sfar, Zied Chtourou und Yacine Challal. „A systemic and cognitive vision for IoT security: A case study of military live simulation and security challenges“. In: *2017 International Conference on Smart, Monitored and Controlled Cities (SM2C)*. Sfax, Tunisia: IEEE, Feb. 2017, S. 101–105. ISBN: 978-1-5090-6323-9. DOI: 10.1109/SM2C.2017.8071828.

[Bur18] Manfred Burghardt. *Projektmanagement: Leitfaden für die Planung, Überwachung und Steuerung von Projekten*. ger. 10., überarbeitete und erweiterte Auflage. Erlangen: Publicis Publishing, 2018. ISBN: 978-3-89578-472-9.

[Fer+18] Rogério Dos Santos Ferreira u. a. „Information security management practices: study of the influencing factors in a Brazilian Air Force institution“. In: *Journal of Information Systems and Technology Management* 15 (Nov. 2018). ISSN: 18071775. DOI: 10.4301/S1807-1775201815005.

[Kü18] Stefan Kühl. *Organisationskulturen beeinflussen: eine sehr kurze Einführung*. ger. 1. Auflage. Management kompakt. Wiesbaden [Heidelberg]: Springer VS, 2018. ISBN: 978-3-658-20197-5 978-3-658-20196-8. DOI: 10.1007/978-3-658-20197-5.

[RS+18] Arbia Riahi Sfar u. a. „A roadmap for security challenges in the Internet of Things“. en. In: *Digital Communications and Networks* 4.2 (Apr. 2018), S. 118–137. ISSN: 23528648. DOI: 10.1016/j.dcan.2017.04.003.

[Sch18] Jan Schönherr. *Das kleine Sabotage-Handbuch von 1944: die besten Tricks des amerikanischen Geheimdienstes im Kampf gegen Hitler*. ger. Rororo 63416. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag, 2018. ISBN: 978-3-499-63416-1.

[Axe19] Axelos. *ITIL® Foundation: ITIL 4 edition*. eng. First edition. OCLC: 1088317356. Norwich: TSO (The Stationery Office), 2019. ISBN: 978-0-11-331606-9.

[KE19] Roswita Königswieser und Alexander Exner. *Systemische Intervention: Architekturen und Designs für Berater und Veränderungsmanager*. Schäffer-Poeschel, 2019. ISBN: 978-3-7910-4323-4. DOI: 10.34156/9783791043234.

[LK19] Niklas Luhmann und André Kieserling. *Die Politik der Gesellschaft*. ger. 5. Auflage. Suhrkamp-Taschenbuch Wissenschaft 1582. Frankfurt am Main: Suhrkamp, 2019. ISBN: 978-3-518-29182-5.

[MB19] Zaydi Mounia und Nassereddine Bouchaib. „A new comprehensive solution to handle information security Governance in organizations“. en. In: *Proceedings of the 2nd International Conference on Networking, Information Systems & Security*. Rabat Morocco: ACM, März 2019, S. 1–5. ISBN: 978-1-4503-6645-8. DOI: 10.1145/3320326.3320382.

[TGG19] Segundo Moisés T. Toapanta, Alexander Jimenez Gurumendi und Luis Enrique Mafla Gallegos. „An Approach of National and International Cybersecurity Laws and Standards to Mitigate Information Risks in Public Organizations of Ecuador“. en. In: *Proceedings of the 2019 2nd International Conference on Education Technology Management*. Barcelona Spain: ACM, Dez. 2019, S. 61–66. ISBN: 978-1-4503-7629-7. DOI: 10.1145/3375900.3375909.

[Kü20] Stefan Kühl. *Brauchbare Illegalität: vom Nutzen des Regelbruchs in Organisationen*. ger. Frankfurt: Campus Verlag, 2020. ISBN: 978-3-593-51301-0.

[Pic+20] Arnold Picot u. a. *Organisation: Theorie und Praxis aus ökonomischer Sicht*. ger. 8., aktualisierte und überarbeitete Auflage. Stuttgart [Freiburg]: Schäffer-Poeschel Verlag, 2020. ISBN: 978-3-7910-4708-9.

[Saf+20] Olga M. Safonova u. a. „Methodology for Creating, Implementing and System Effectiveness Evaluation of the Business Processes' Information Security System“. In: *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*. Yaroslavl, Russia: IEEE, Sep. 2020, S. 127–131. ISBN: 978-1-72818-179-0. DOI: 10.1109/ITQMIS51053.2020.9322855.

[SK20] Georg Schreyögg und Jochen Koch. *Management: Grundlagen der Unternehmensführung*. de. Wiesbaden: Springer Fachmedien Wiesbaden, 2020. ISBN: 978-3-658-26513-7 978-3-658-26514-4. DOI: 10.1007/978-3-658-26514-4.

[Sun+20] Zhe Sun u. a. „Research on the Effectiveness Analysis of Information Security Controls“. In: *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*. Chongqing, China: IEEE, Juni 2020, S. 894–897. ISBN: 978-1-72814-390-3. DOI: 10.1109/ITNEC48623.2020.9084809.

[TPG20] Segundo Moisés T. Toapanta, Gary Xavier Rázuri Peralta und Luis Enrique Mafla Gallegos. „Security Model for the Integration of the Ministry of Telecommunications and the Information Society with a Public Organization of Ecuador“. en. In: *Proceedings of the 2020 the 4th International Conference on Information System and Data Mining*. Hawaii HI USA: ACM, Mai 2020, S. 43–50. ISBN: 978-1-4503-7765-2. DOI: 10.1145/3404663.3404670.

[Yas+20] Muhammad Yasin u. a. „Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)“. In: *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*. Bandung, Indonesia: IEEE, Nov. 2020, S. 1–5. ISBN: 978-1-72817-598-0. DOI: 10.1109/TSSA51342.2020.9310875.

[AQ21] Hamzeh AlKilani und Abdallah Qusef. „OSINT Techniques Integration with Risk Assessment ISO/IEC 27001“. en. In: *International Conference on Data Science, E-learning and Information Systems 2021*. Ma'an Jordan: ACM, Apr. 2021, S. 82–86. ISBN: 978-1-4503-8838-2. DOI: 10.1145/3460620.3460736.

[Cul+21] Giovanna Culot u. a. „The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda“. In: *The TQM Journal* 33.7 (Jan. 2021), S. 76–105. ISSN: 1754-2731. DOI: 10.1108/TQM-09-2020-0202.

[Luh21] Niklas Luhmann. *Soziale Systeme: Grundriß einer allgemeinen Theorie*. ger. 18. Auflage. Suhrkamp-Taschenbuch Wissenschaft 666. Frankfurt am Main: Suhrkamp, 2021. ISBN: 978-3-518-28266-3.

[MKB21] Mona Mirtsch, Jan Kinne und Knut Blind. „Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis“. In: *IEEE Transactions on Engineering Management* 68.1 (Feb. 2021), S. 87–100. ISSN: 0018-9391, 1558-0040. DOI: 10.1109/TEM.2020.2977815.

[SRS21] Fritz B. Simon und Christel Rech-Simon. *Zirkuläres Fragen: systemische Therapie in Fallbeispielen: ein Lernbuch*. ger. Vierzehnte Auflage. Systemische Therapie. Heidelberg: Carl-Auer Verlag, 2021. ISBN: 978-3-8497-0166-6.

[AH22] Urs Andelfinger und Petra Haferkorn. *Agilität für IT-Governance, Prüfung & Revision: Grundlagen und Umsetzung in die Praxis*. ger. 1. Auflage. Edition ISACA Germany Chapter. Heidelberg: dpunkt.verlag, 2022. ISBN: 978-3-96910-563-4 978-3-86490-861-3.

[Eur22] European Union Agency for Cybersecurity (ENISA). „ENISA Threat Landscape 2022“. In: ISBN: 978-92-9204-633-0. European Union Agency for Cybersecurity, Okt. 2022. DOI: 10.2824/196582.

[Gau+22] Florence Gaub u. a. „What If ... Not? The Cost of Assumptions“. In: *European Union Institute for Security Studies (EUISS)* (Jan. 2022), S. 172. DOI: 10.2815/380497. URL: https://www.iss.europa.eu/content/what-ifnot-cost-assumptions.

[Hie+22] Jonas Hielscher u. a. „“Taking out the Trash”: Why Security Behavior Change Requires Intentional Forgetting“. In: *Proceedings of the 2021 New Security Paradigms Workshop*. NSPW '21. event-place: Virtual Event, USA. New York, NY, USA: Association for Computing Machinery, 2022, S. 108–122. ISBN: 978-1-4503-8573-2. DOI: 10.1145/3498891.3498902.

[ISO22] ISO. „ISO - The ISO Survey“. en. In: *International Organization for Standardization* (2022). Publication Title: ISO. URL: https://www.iso.org/the-iso-survey.html (besucht am 28. 09. 2023).

[LN22] Martti Lehto und P. Neittaanmäki, Hrsg. *Cyber security: critical infrastructure protection*. eng. OCLC: 1308976278. Cham, Switzerland: Springer, 2022. ISBN: 978-3-030-91293-2.

[Men+22] Uta Menges u. a. „Why IT Security Needs Therapy“. en. In: *Computer Security. ESORICS 2021 International Workshops*. Hrsg. von Sokratis Katsikas u. a. Bd. 13106. Series Title: Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022, S. 335–356. ISBN: 978-3-030-95483-3 978-3-030-95484-0. DOI: 10.1007/978-3-030-95484-0_20.

[SSD22] Varbinka Stefanova-Stoyanova und Petko Danov. „Comparative Analysis of Specialized Standards and Methods on Increasing the Effectiveness and Role of PDCA for Risk Control in Management Systems“. In: *2022 10th International Scientific Conference on Computer Science (COMSCI)*. Sofia, Bulgaria: IEEE, Mai 2022, S. 1–4. ISBN: 978-1-66549-777-0. DOI: 10.1109/COMSCI55378.2022.9912583.

[WPO22] Alfan Cahyo Wicaksono, Sidik Prabowo und Dita Oktaria. „Risk and Security Measurement Based on ISO 27001 Using FMEA Methodology Case Study: National Government Agency“. In: *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)*. Bandung, Indonesia: IEEE, Nov. 2022, S. 6–11. ISBN: 978-1-66547-303-3. DOI: 10.1109/ICoSEIT55604.2022.10029988.

[Bun23] Bundesamt für Sicherheit in der Informationstechnik. „Positionspapier Zero Trust 2023“. In: Bonn, Deutschland: Bundesamt für Sicherheit in der Informationstechnik, 2023. URL: https://www.bsi.bund.de.

[Eck23] Claudia Eckert. *IT-Sicherheit: Konzepte – Verfahren – Protokolle*. De Gruyter, Feb. 2023. ISBN: 978-3-11-098511-5.

[Eur23] European Union Agency for Cybersecurity (ENISA). „ENISA Threat Landscape 2023“. In: ISBN: 978-92-9204-645-3. European Union Agency for Cybersecurity, Okt. 2023. DOI: 10.2824/782573.

[Hul23] John Hull. *Risk management and financial institutions*. eng. Sixth edition. Wiley finance series. Hoboken, New Jersey: Wiley, 2023. ISBN: 978-1-119-93249-9 978-1-119-93248-2.

[Kü23] Stefan Kühl. *Schattenorganisation: agiles Management und ungewollte Bürokratisierung*. ger. Frankfurt New York: Campus Verlag, 2023. ISBN: 978-3-593-51732-2.

[KSNI23] Stefan Kühl und Phanmika Sua-Ngam-Iam, Hrsg. *Holacracy: Funktionen und Folgen eines Managementmodells*. de. Wiesbaden: Springer Fachmedien Wiesbaden, 2023. ISBN: 978-3-658-40110-8 978-3-658-40111-5. DOI: 10.1007/978-3-658-40111-5.

[Pai23] Darren Pain. „Cyber Risk Accumulation: Fully tackling the insurability challenge“. In: *The Geneva Association* (Nov. 2023). URL: www.genevaassociation.org.

[Sim23] Fritz B. Simon. *Einführung in Systemtheorie und Konstruktivismus*. ger. Zehnte Auflage. Carl-Auer Compact. Heidelberg: Carl-Auer-Systeme Verlag und Verlagsbuchhandlung GmbH, 2023. ISBN: 978-3-89670-547-1.

[The23] Jonathan Theis. „Herausforderungen von Informationssicherheitsmanagementsystemen“. Deutsch. In: *Masterprojekt Hochschule Bonn-Rhein-Sieg* (Dez. 2023), S. 53.

[TH23] Romel Tintin und Monica Hidalgo. „Could an ISMS Model (ISO/IEC 27001:2013 Standard) Implementation Really Protect Public Data?“ In: *2023 Ninth International Conference on eDemocracy & eGovernment (ICEDEG)*. Quito, Ecuador: IEEE, Apr. 2023, S. 1–5. ISBN: 9798350324501. DOI: 10.1109/ICEDEG58167.2023.10122109.

[WDB23] Günter Wöhe, Ulrich Döring und Gerrit Brösel. *Einführung in die allgemeine Betriebswirtschaftslehre*. ger. 28., überarbeitete und aktualisierte Auflage. Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften. München: Verlag Franz Vahlen, 2023. ISBN: 978-3-8006-7200-4.

[Kri24] Joana Krizanits. *Leadership, Management, Führung: die essenziellen Konzepte vom Industriezeitalter zur klimaneutralen Gesellschaft*. ger. Erste Auflage. Management, Organisationsberatung. Heidelberg: Carl-Auer-Systeme Verlag, 2024. ISBN: 978-3-8497-0522-0.