

UNIVERSITÄT FÜR WEITERBILDUNG KREMS
Department für E-Governance in Wirtschaft und Verwaltung
Dr.-Karl-Dorrek-Str. 30
A - 3500 Krems



**Die Erweiterung des IT-Grundschutz Vorgehens mit
Enterprise Security Architecture Fähigkeiten**

Master-Thesis
im Rahmen des universitären Weiterbildungsprogramms
Professional MSc Management und IT
Spezialisierung – Information Security Management

eingereicht von:

Nicolas Kritharas
22. September 2024

Betreuer:

FH-Prof. Dipl.-Ing. Peter Kieseberg

EIDESSTATTLICHE ERKLÄRUNG

Ich, Nicolas Kritharas, erkläre hiermit an Eides statt,

1. dass ich meine Master-Thesis selbstständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe,
2. dass ich meine Master-Thesis oder wesentliche Teile daraus bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,
3. dass ich, falls die Master-Thesis mein Unternehmen oder einen externen Kooperationspartner betrifft, meinen Arbeitgeber über Titel, Form und Inhalt der Master-Thesis unterrichtet und sein Einverständnis eingeholt habe.

KURZBESCHREIBUNG

Im Rahmen der Informationssicherheit setzen Organisationen technische und organisatorische Maßnahmen auf Basis von Sicherheitsstandards um, sodass sie ihre Assets schützen. In diesen Sicherheitsstandards ist jedoch nicht dargelegt, wie die Sicherheit nach der Strategie und den Zielen der Organisation realisiert werden kann.

Das Ziel in der vorliegenden Thesis ist es, ein solches Vorgehen durch die Erweiterung der IT-Grundschatz-Methodik mit SABSA zu beschreiben. Dazu wurde folgende Forschungsfrage gestellt: Wie kann die IT-Grundschatz-Methodik zur Entwicklung einer ganzheitlichen Sicherheitsarchitektur mit SABSA kombiniert werden?

Um die Forschungsfrage zu beantworten, wurde auf Basis der Theorie ein Modell entwickelt, das anhand von Interviews mit Expert:innen evaluiert wurde. Dabei wurden sowohl Einsatzpotenziale als auch Einsatzrisiken identifiziert. Es konnte festgestellt werden, dass das theoretische Modell von den Expert:innen akzeptiert wurde. Die praktische Anwendung und die damit einhergehende Adaption werden von verschiedenen Faktoren beeinflusst, die sich auf den Anwendungserfolg negativ auswirken. Die Ergebnisse dieser Arbeit zeigen auf konzeptioneller Ebene, wie die Informationssicherheit businessgetrieben modelliert und etabliert werden kann. Zudem werden mögliche Umsetzungs- und Gestaltungshinweise gegeben.

Weiterführende Forschung mit der erweiterten IT-Grundschatz-Methodik könnte auf die Adaption und Anwendung ausgerichtet sein.

Schlagworte: Enterprise Information Security Architecture, Enterprise Architecture, Security Architecture, Information Security Architecture, SABSA, Sherwood Applied Business Security Architecture

ABSTRACT

In the context of information security, organisations implement technical and organisational measures based on security standards to protect their assets. However, these security standards do not explain how security can be implemented according to the organisation's strategy and objectives.

The aim of this thesis is to describe such an approach by extending the IT-Grundschutz methodology with SABSA. To this end, the following research question was posed: How can the IT-Grundschutz methodology be combined with SABSA to develop a holistic security architecture?

To answer the research question, a theory-based model was developed and evaluated through interviews with experts. Both potential benefits and risks were identified. It was found that the experts accepted the theoretical model. The practical application and adaptation is influenced by several factors that have a negative impact on the success of the application. The results of this work show on a conceptual level how information security can be modelled and established in a business-driven manner. In addition, this work provides potential implementation and design guidelines.

Further research with the extended IT-Grundschutz methodology could be directed towards adaptation and application.

Keywords: enterprise information security architecture, enterprise architecture, security architecture, information security architecture, sabsa, sherwood applied business security architecture

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS	VII
TABELLENVERZEICHNIS	VIII
ABKÜRZUNGSVERZEICHNIS	IX
GLOSSAR	XI
1. EINFÜHRUNG.....	1
1.1. KLASISCHE IMPLEMENTIERUNG DER INFORMATIONSSICHERHEIT	1
1.2. ETABLIERUNG DER INFORMATIONSSICHERHEIT NACH BSI 200-2	2
1.3. FEHLENDER ORGANISATIONSKONTEXT BEI ETABLIERUNG.....	3
1.4. DEFINITION DER ENTERPRISE SECURITY ARCHITECTURE	6
1.5. SABSA.....	7
1.6. UNTERSUCHUNGSDESIGN UND GLIEDERUNG DER THESIS.....	8
2. ZIELSETZUNG DER THESIS.....	10
2.1. PROBLEMIDENTIFIZIERUNG	10
2.2. DESIGNANFORDERUNGEN	10
2.3. FORSCHUNGSFRAGE.....	11
3. EINGESETZTE FORSCHUNGSMETHODEN	12
3.1. UNTERSUCHUNGSANSATZ	12
3.2. LITERATURANALYSE.....	13
3.3. EXPERT:INNENINTERVIEW.....	14
3.4. DATENANALYSE DER EXPERT:INNENINTERVIEWS	15
3.5. EVALUATION.....	16
4. ERGEBNISSE DER FORSCHUNGSMETHODEN.....	17
4.1. LITERATUR ZU ENTERPRISE SECURITY ARCHITECTURE	17
4.1.1. Suchergebnisse der Literaturanalyse	17
4.1.2. Adaptiver Wissenstransfer von EA zu ESA	20
4.2. PERSPEKTIVEN DER EXPERT:INNEN	24
5. DESIGN UND ENTWICKLUNG	32
5.1. ERWEITERTE IT-GRUND SCHUTZ-METHODIK	32
5.1.1. Aufbau der erweiterten Methodik	32
5.1.2. Lebenszyklus	34
5.1.3. Limitationen der erweiterten Methodik.....	35
5.2. INITIIERUNG DES SICHERHEITSPROZESSES.....	36
5.3. ERMITTlung DES KONTEXTES DER ORGANISATION.....	38
5.4. KONZEPTUALISIERUNG DER ORGANISATION.....	43
5.5. ERSTELLUNG DER SICHERHEITSARCHITEKTUR.....	48
5.5.1. Logische Ebene	48

	VI
5.5.2. Physische Ebene	50
5.5.3. Komponentenebene.....	51
5.6. UMSETZUNG DER UNTERNEHMENSSICHERHEITSARCHITEKTUR	51
5.7. AUFRECHTERHALTUNG UND VERBESSERUNG	54
6. DISKUSSION DER THESIS.....	56
6.1. ERFÜLLUNG DER DESIGNANFORDERUNGEN	56
6.2. BEURTEILUNG NACH DESIGN-SCIENCE-GUIDELINES.....	57
7. CONCLUSIO.....	60
7.1. RELEVANTE BEITRÄGE DER THESIS.....	60
7.2. EMPFEHLUNG FÜR ZUKÜNTIGE FORSCHUNG	61
8. LITERATURVERZEICHNIS.....	61
ANHANG A	72
A.1 MÖGLICHER AUFBAU DER ORGANISATIONSSTRUKTUR	72
A.1.1 Normalisierung von Rollen und Verantwortlichkeiten	72
A.1.2 Aufnahme der Verantwortlichkeiten aus dem IT-Grundschutz	78
A.1.3 Strukturierung der Architekturrollen	82
A.2 MAPPING DER R1 BAUSTEINE ZU SABSA METAEBENEN	83
A.2.1 Ermittelte Control Objectives von R1 Bausteinen.....	84
A.2.2 Ausgearbeitete Control Library aus dem IT-Grundschutz	86
A.2.3 Benötigte Dokumentationen aus R1-Bausteinen	88
A.2.4 Mapping der R1-Bausteine des Kompendiums mit SABSA Ebenen	92
A.3 ARBEITSPRODUKTE	102
ANHANG B	109
B.1 STRUKTURIERTE LITERATURRECHERCHE ZUM IT-GRUND SCHUTZ	109
B.2 STRUKTURIERTE LITERATURRECHERCHE ZU ESA UND SABSA.....	117
ANHANG C	122
C.1 INTERVIEW FRAGEN UND IHRE THEMEN	122
C.2 HINTERGRUNDINFORMATION ZUM EXPERTENINTERVIEW	123
C.3 CODES UND IHRE HÄUFIGKEIT	124
C.4 ZUSAMMENGEFASSTE KODIERUNG	126
ANHANG D	130

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1: PHASEN DES SICHERHEITSPROZESSES NACH BSI 200-2	2
ABBILDUNG 2: ARCHITEKTURMATRIX.....	7
ABBILDUNG 3: FORSCHUNGSDESIGN.....	9
ABBILDUNG 4: FORSCHUNGSANSATZ DIESER ARBEIT	12
ABBILDUNG 5: AUFTEILUNG TEXTARTEN ZUM IT-GRUNDSCHUTZ.....	17
ABBILDUNG 6: REIFEGRADE DER ENTERPRISE ARCHITECTURE	20
ABBILDUNG 7: ARCHITEKTURPROZESSE	21
ABBILDUNG 8: EVALUIERUNG DER ARCHITEKTUR.....	22
ABBILDUNG 9: CSVLOD-MODELL	23
ABBILDUNG 10: PHASEN DES SICHERHEITSPROZESSES DER ERWEITERTEN METHODIK	32
ABBILDUNG 11: ABSTRAKTIONSEBENEN IN SABSA.....	33
ABBILDUNG 12: LEBENSZYKLUS DES ERWEITERTEN IT-GRUNDSCHUTZES	34
ABBILDUNG 13: BEITRÄGE IM FORUM IM ZEITRAUM.....	35
ABBILDUNG 14: MÖGLICHE ORGANISATORISCHE AUSGESTALTUNG	37
ABBILDUNG 15: KATEGORIEN DER ANFORDERUNGEN.....	39
ABBILDUNG 16: WAHL DER INFORMATIONSKATEGORIE	41
ABBILDUNG 17: DEKOMPOSITION EINER BILATERALEN VERTRAUENSBEZIEHUNG	45
ABBILDUNG 18: LOGISCHE BEZIEHUNGEN VON DOMÄENEN	49
ABBILDUNG 19: AUSWIRKUNG DER BEHANDLUNGSSARTEN	50
ABBILDUNG 20: IS-ENGAGEMENT-MODELL.....	53
ABBILDUNG 21: VERORTUNG DER ARCHITEKTURROLLEN.....	82
ABBILDUNG 22: R1 BAUSTEINE ZU SABSA MAPPING.....	87
ABBILDUNG 23: LEGENDE FÜR ABBILDUNG 24 UND 25	127
ABBILDUNG 24: VISUALISIERUNG DER INHALTLICHEN ZUSAMMENFÜHRUNG	128
ABBILDUNG 25: BEZIEHUNGEN ZWISCHEN DEN KATEGORIEN	129

TABELLENVERZEICHNIS

TABELLE 1: NORMALISIERUNG UND BESCHREIBUNG DER IT-GRUNDSCHUTZ ROLLEN	72
TABELLE 2: BESCHREIBUNG DER EA-ROLLEN	75
TABELLE 3: SYNTHESE VERANTWORTLICHKEITEN AUS IT-GRUNDSCHUTZ-METHODIK	78
TABELLE 4: CONTROL OBJECTIVES DER R1 BAUSTEINE	84
TABELLE 5: VERPFlichtende Dokumentation nach R1 Bausteine.....	88
TABELLE 6: BAUSTEINE ZU SABSA LAYER MAPPING	92
TABELLE 7: ARBEITSPRODUKTE AUS DER INITIIERUNGSPHASE	102
TABELLE 8: ARBEITSPRODUKTE AUS DER ERMITTlung DES KONTEXTES	103
TABELLE 9: ARBEITSPRODUKTE AUS DER KONZEPTUALISIERUNG.....	103
TABELLE 10: ARBEITSPRODUKTE AUS DER SICHERHEITSARCHITEKTUR	104
TABELLE 11: ARBEITSPRODUKTE AUS DER UMSETZUNG.....	106
TABELLE 12: ARBEITSPRODUKTE AUS DEM KVP	107
TABELLE 13: LITERATUR ZUM IT-GRUNDSCHUTZ	110
TABELLE 14: LITERATUR ZU ESA UND SABSA	118
TABELLE 15: VERTEILUNG DER BEFRAGTEN	123
TABELLE 16: REIFEGRAD DER ORGANISATIONEN VON BEFRAGTEN	123
TABELLE 17: CODES UND IHRE HÄufigkeit IN INTERVIEWS	124
TABELLE 18: INHALTliche ZUSAMMENFÜHRUNG.....	126

ABKÜRZUNGSVERZEICHNIS

AAL3	Authenticator Assurance Level 3
AM	Architecture Manager
BAA	Business Area Architect
BASA	Business Area Security Architect
BCM	Business Continuity Management
BISO	Business Information Security Officer
BSI	Bundesamt für Sicherheit in der Informationstechnik
CER	Critical Entities Resilience
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMMI	Capability Maturity Model
CPO	Chief Privacy Officer
DA	Domain Architect
DOI	Digital Object Identifier
DSB	Datenschutzbeauftragte
DSR	Design Science Research
DSRP	Design Science Research Process
DYA	Dynamic Enterprise Architecture
EA	Enterprise Architecture
EISA	Enterprise Information Security Architecture
ESA	Enterprise Security Architecture
HR	Human Resources
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
IS	Information Security / Informationssicherheit
ISCC	IS Coordination Committee
ISMS	Informationssicherheitsmanagementsystem

ISO	International Organization for Standardization
ITSO	IT Security Officer
KCI	Key Control Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
KVP	Kontinuierlicher Verbesserungsprozess
MA	Mitarbeitende(r)
MFA	Multifaktor Authentifizierung
NDA	Non Disclosure Agreement
NIS	Network and Information Security
OTSO	OT-Security Officer
PA	Program Architect
PCI DSS	Payment Card Industry Data Security Standard
PSO	Project Security Officer
RCE	Resilience of Critical Entities
RM	Risikomanagement
SA	Solution Architect
SABSA	Sherwood Applied Business Security Architecture
SE	Safety Expert
SOAR	Security Orchestration, Automation and Response
SSE	Security Service Expert
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework

GLOSSAR

Antifragil

Adjektiv des Begriffs ‚Antifragilität‘. Es beschreibt die Eigenschaft eines Systems, seine Fähigkeiten unter dem Einfluss von negativen Ereignissen zu steigern (vgl. Taleb 2012).

Business Attribute

Konzeptionelle Abstraktion einer Anforderung, die zudem eine Messbarkeit der Erreichung dieser Anforderung ermöglicht.

Business Attribute Profile

Konzeptionelle Repräsentation der Organisation, gemappt über die Business Attributes zur Messung der Performance für die Einhaltung der Anforderungen (vgl. Sherwood et al. 2009: 218).

Business Capability Model

Grafische Darstellung zur Visualisierung sämtlicher Geschäftsfähigkeiten einer Organisation sowie ihrer Beziehungen zueinander.

Business Driver

Wesentliche interne oder externe Faktoren und Kräfte, die den Erfolg einer Organisation beeinflussen. Sie können in verschiedenen Formen existieren, z. B. Marktbedingungen, technologischen Entwicklungen, regulatorischen Rahmenbedingungen und internen Prozessen.

Business Driver for Security

Repräsentiert eine abgeleitete Abstraktion einer Sicherheitsanforderung des Business Drivers.

Control Library

Bibliothek zur Wiederverwendung definierter Security Services und Security Mechanisms.

Control Objective

Aussage über ein gewünschtes Ergebnis oder einen Zweck, der durch die Implementierung von Kontrollen innerhalb einer bestimmten Geschäftstätigkeit erreicht werden soll (vgl. Sherwood et al. 2009: 219).

Defense-in-Depth-Strategie

Vorgehen, bei dem mehrere Sicherheitsmaßnahmen eingesetzt werden, um ein oder mehrere Assets zu schützen.

EA-Artifact

Separate Dokumente, die die Enterprise Architecture bilden (vgl. Winter/Fischer 2006: 1–2).

Enterprise Architecture

Formalisiert die Anforderungen verschiedener Stakeholder:innen und stellt diese im Kontext des Unternehmens dar. Dabei werden mit Hilfe geschäftlicher und technischer Architekturen die Abhängigkeiten zueinander dargestellt.

Enterprise Security Architecture

Teilbereich der Enterprise Architecture, in dem die Unternehmensarchitektur mit einer Unternehmenssicherheitsarchitektur ergänzt wird. Sie ist die Praxis der Gestaltung, Erstellung und Pflege der Sicherheit in einer Organisation.

Informationssicherheitsmanagementsystem

Betrachtet die Informationssicherheitsrisiken der Organisation ganzheitlich und koordiniert, um umfassende Informationssicherheitskontrollen innerhalb des Gesamtrahmens eines kohärenten Managementsystems zu ermitteln und umzusetzen (vgl. ISO 2022b).

IT-Grundschutz-Methodik

Eine Methodik, die aufzeigt „wie ein effizientes Managementsystem für die Informationssicherheit aufgebaut und wie das IT-Grundschutz-Kompendium im Rahmen dieser Aufgabe verwendet werden kann“ (BSI 2017a: 11).

Operating Model

Beschreibt ein standardisiertes Rahmenwerk, wie eine Organisation aufgestellt ist.

RAS(C)I-Matrix

Modell zur Darstellung der Rollen und Verantwortlichkeiten in einer Organisation.

Risiko-Assessment

Beschreibt die Zusammenfassung der Informationssicherheitsrisikomanagementprozesse ‚Risiko Identifikation‘, ‚Risiko Analyse‘ und ‚Risiko Evaluation‘ (vgl. ISO 2022c).

Sherwood Applied Business Security Architecture

Stellt eine Methodik zur Entwicklung risikobasierter Unternehmensarchitekturen für Informationssicherheit und Informationssicherung sowie zur Bereitstellung von Sicherheitsinfrastrukturlösungen dar, die die Unterstützung kritischer Geschäftsinitiativen haben (vgl. Sherwood et al. 2009: 1).

Security Mechanism

Physischer Dienst, der die Vorgaben der Security Services operationalisiert und umsetzt.

Security Service

Logischer Dienst, der die Vorgaben des Business Attribute Profiles, der Control Objectives und der Sicherheitsstrategie umsetzt (vgl. Sherwood et al. 2009: 294).

1. EINFÜHRUNG

Das zunehmende Interesse an der Informationssicherheit (vgl. McKinsey 2019: 8–17) führt zu einer Intensivierung des Drucks auf Organisationen, den Schutz von Informationen und Assets in den Fokus zu stellen. Wegen der hohen Anzahl von Systemen und ihrer inhärenten Komplexität hat sich eine Bewegung Ende des 20. Jahrhunderts (vgl. Sherwood 1996; Lowman/Mosier 1997) formiert, die die Informationssicherheit mittels Architektur gestaltet. Das Ziel besteht darin, eine ganzheitliche und angemessene Schutzwirkung für die Organisation zu erreichen. Im Folgenden werden die Hintergründe der neuen Arbeitsweise erläutert.

In diesem Kapitel wird die aktuelle Etablierung der Informationssicherheit, Stand 2024, in Organisationen beschrieben und die damit einhergehenden Problematiken werden dargestellt. Des Weiteren wird ein kurzer Überblick über die Architektur der Informationssicherheit gegeben. Zudem werden das Forschungsdesign sowie die Gliederung der vorliegenden Thesis erörtert.

1.1. KЛАSSISCHE IMPLEMENTIERUNG DER INFORMATIONSSICHERHEIT

Das Themengebiet der Informationssicherheit ist vielschichtig und umfasst zahlreiche organisatorische und technische Aspekte. Für jedes dieser spezifischen Themen existieren individuelle Best Practices und Empfehlungen, deren Anwendung in Abhängigkeit des Kontextes ein angemessenes Sicherheitsniveau gewährleistet. Um letzteres in einer Organisation zu etablieren und aufrechtzuerhalten, können Organisationen ein Informationssicherheitsmanagementsystem (ISMS) gemäß der internationalen Norm ISO/IEC 27001 entwickeln, in der ganzheitliche Standards und Best Practices für die Sicherung von Informationen festgelegt sind (vgl. ISO 2022a).

Die ISO/IEC 27001 definiert einen Rahmen für den Umgang mit Risiken, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in einer Organisation zu gewährleisten. Für Organisationen besteht die Möglichkeit einer Zertifizierung nach diesem Standard.

In Deutschland wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) der IT-Grundschutz als Instrument zur Einführung und Aufrechterhaltung eines ISMS entwickelt. Die Vorgehensweise ist in der IT-Grundschutz-Methodik festgelegt, welche nach einem Bottom-up-Ansatz durchgeführt wird und einen

technischen Fokus bei der Etablierung der Sicherheit setzt (vgl. BSI 2017a). Organisationen, die ein ISMS nach IT-Grundschutz implementiert haben, können dieses nach der ISO/IEC 27001 auf Basis von IT-Grundschutz durch externe Dienstleister:innen zertifizieren lassen (vgl. BSI o. D.).

1.2. ETABLIERUNG DER INFORMATIONSSICHERHEIT NACH BSI 200-2

Die Gestaltung und Etablierung der Informationssicherheit erfolgt gemäß dem *BSI-Standard 200-2 IT-Grundschutz-Methodik* (vgl. BSI 2017a) durch einen Sicherheitsprozess, der mehrere Phasen umfasst und sequenziell bearbeitet wird. Der Prozess ist in Abbildung 1 dargestellt.

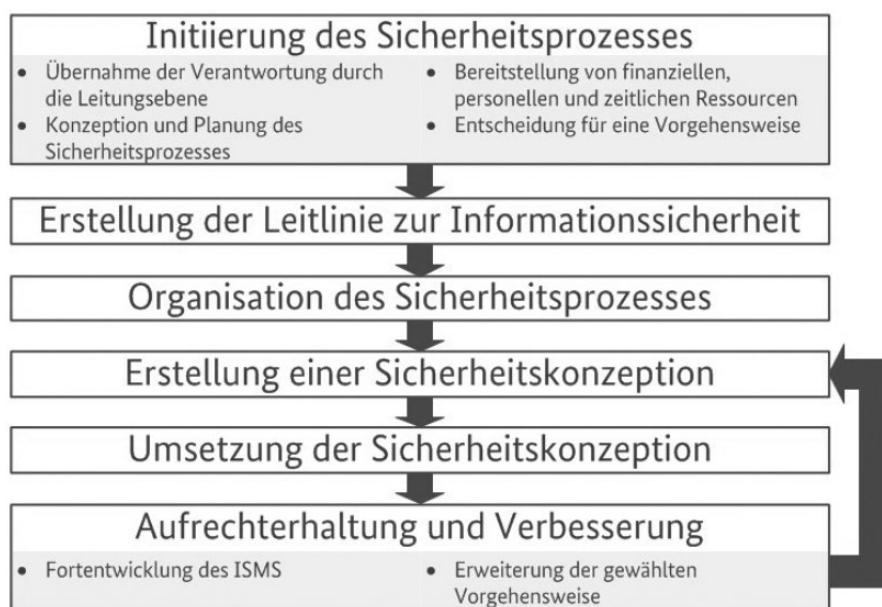


Abbildung 1: Phasen des Sicherheitsprozesses nach BSI 200-2
Quelle: (BSI 2017a: 15)

Die Initiative zur Implementierung geht vom oberen Management aus, das den Sicherheitsprozess auch überwacht und reguliert. Hierbei wird zunächst die Verantwortlichkeit festgelegt sowie ein Konzept bzw. eine Strategie für die Informationssicherheit entwickelt. Letztere beinhaltet die Rahmenbedingungen sowie die Informationssicherheitsziele. In der Folge werden die bereits vorhandenen Geschäftsprozesse und Assets erfasst. Danach entscheidet das obere Management über die Etablierung der Informationssicherheit, da im IT-Grundschutz drei Vorgehensweisen differenziert sind.

Die Basisabsicherung bezieht sich auf die relevanten Geschäftsprozesse und bildet den initialen Einstieg in die Informationssicherheit. Die Kernabsicherung entspricht in weiten Teilen der Basisabsicherung, geht jedoch über diese hinaus und berücksichtigt zusätzliche Anforderungen zur Gewährleistung eines erhöhten

Schutzbedarfs der relevanten Geschäftsprozesse. Die letzte Absicherung, auch als Standardabsicherung bezeichnet, stellt ein vollwertiges ISMS auf und umfasst die Betrachtung weiterer Aspekte über die relevanten Prozesse hinaus (vgl. ebd.: 20–32).

In der zweiten Phase erfolgt die Konzeption der spezifischen Sicherheitsleitlinie für die Organisation. Die Rollen sowie die Verantwortlichkeiten für verschiedene Sicherheitsthemen werden definiert und der Geltungsbereich ihres Inhalts wird festgelegt. Die erarbeitete Sicherheitsleitlinie wird an die betroffenen Interessengruppen kommuniziert (vgl. ebd.: 32–35).

Während des Sicherheitsprozesses wird die Aufbauorganisation konkretisiert und die Informationsklassifizierungen innerhalb der Organisation werden aufgestellt. Des Weiteren wird der Informationsfluss im Kontext der Informationssicherheit definiert (vgl. ebd.: 36–60).

Die Schaffung der Sicherheitskonzeption hängt von der gewählten Vorgehensweise zur Absicherung ab. Der Ablauf ist identisch. Basierend auf den identifizierten Prozessen und ihren Assets werden die definierten Bausteine des IT-Grundschutz-Kompendiums ausgewählt und evaluiert, ob die im Baustein definierten Anforderungen erfüllt werden. In Abhängigkeit des jeweils vorliegenden Schutzbedarfs, der Nicterfüllung von Anforderungen oder der fehlenden Sicherheitsabdeckung trotz der zuvor gewählten Bausteine ist eine Risikoanalyse durchzuführen, um auf diese Weise einen möglichen weiteren Umsetzungsbedarf zu ermitteln (vgl. ebd.: 76–152).

Die identifizierten Lücken werden geschlossen. Dabei ist der gesamte Ablauf durch den kontinuierlichen Verbesserungsprozess zu überwachen, um Optimierungspotenziale auszuschöpfen (vgl. ebd.: 158–170).

1.3. FEHLENDER ORGANISATIONSKONTEXT BEI ETABLIERUNG

Die ISO/IEC 27001 sowie der IT-Grundschutz postulieren, dass die Ausgestaltung der Informationssicherheit an den Zielen der jeweiligen Organisation auszurichten ist (vgl. ISO 2022a: v; BSI 2017a: 21). Demnach müsste nach beiden Vorgehensweisen eine an den Unternehmenszielen ausgerichtete Informationssicherheit etabliert werden. In den jeweiligen Standards wird dafür aber keine systematische Methodik aufgezeigt (vgl. ISO 2017; BSI 2023b), weshalb die Anforderungen als zu formal und weitreichend empfunden werden (vgl. Bounagui et al. 2019; Diesch et al. 2020).

In der Konsequenz fokussieren Organisationen die Etablierung der Informationssicherheit auf Basis der prozessualen Ebene sowie der Technologie (vgl. Dhillon et al. 2021: 8; Van Wessel et al. 2011: 869–874).

Laut Sherwood (vgl. 2005: 28) erweist sich diese Ausrichtung jedoch als suboptimal, da die organisationsspezifischen Anforderungen nicht vollständig berücksichtigt werden und somit nicht den gewünschten Erfolg bringen. Die prozessorientierte Ausrichtung der Sicherheit erfordert ein strategisch ausgerichtetes Geschäftsprozessmanagement, das laut Schmelzer und Sesselmann (2020) in der Praxis aber nicht verbreitet ist (vgl. 170–171). Der ausschließliche Fokus auf die Technologie bietet einer Organisation keinen umfassenden Schutz, weshalb organisatorische Maßnahmen ergänzt werden sollten. Dadurch entsteht eine soziotechnische Sichtweise, die eine ganzheitliche Informationssicherheit ermöglicht (vgl. Iivari/Hirschheim 1996).

Die fehlende Berücksichtigung des Organisationskontextes bei der Etablierung der Informationssicherheit ist auf verschiedene Faktoren zurückzuführen. Neben der unzureichenden Anwendung einer systematischen Methodik sind auch die genutzten Methoden selbst entscheidend. Diese lassen sich gemäß Baskerville (1993) in drei Generationen unterteilen.

Die erste Generation (Checklisten-Methode) besteht aus drei Teilen:

1. Checkliste bestehend aus einer Liste von Sicherheitsmaßnahmen, die implementiert werden könnten,
2. Risikomanagement, anhand dessen die Notwendigkeit der Implementierung der jeweiligen Maßnahmen aus der Checkliste ermittelt wird und
3. kosteneffektive Implementierung (vgl. ebd.: 380–389).

Die zweite Generation (Mechanistic-Design-Methode) besteht aus fünf Teilen:

1. Inventarisierung von Assets und Bedrohungen,
2. Sichtung der Sicherheitsmaßnahmenliste – eine Aktivität, die aus der ersten Generation übernommen wurde, aber eigenständig erweitert werden kann,
3. Risikomanagement,
4. Priorisierung der Sicherheitsmaßnahmen nach dem Risikomanagement und
5. regelmäßige Überprüfung zur Aufrechterhaltung des Designs der implementierten Informationssicherheit (vgl. ebd.: 390–400).

Der IT-Grundschutz und die ISO/IEC 27001 können der zweiten Generation zugeordnet werden. Die Auditierung des ISMS erfolgt auf Basis der ersten Generation.

Über die Aktionsschritte der beiden Generationen wird ersichtlich, dass der Kontext der Organisation in den Arbeits- und Prüfweisen nicht aufgegriffen ist. Zudem zeigt sich, dass in der wissenschaftlichen Literatur die traditionelle Vorgehensweise der ersten und zweiten Generation nach Baskerville dominiert (vgl. Dhillon et al. 2021: 2–3).

Die dritte Generation (logisch-transformative Methode) besteht aus drei Teilen:

1. Anforderungsanalyse zur Problemidentifikation und zum Verständnis des Kontextes,
2. Abstraktion der Organisation auf verschiedene Metaebenen und
3. Design der Lösung auf Basis der Abstraktionen sowie Anforderungen (vgl. Baskerville 1993: 401–408).

Nach Siponen (2005) ist ein möglicher Grund, weshalb die dritte Generation nicht berücksichtigt oder unbekannt ist, ist, dass die diversen Methoden zur Etablierung der Informationssicherheit in Organisationen von Forschungsgruppen entwickelt werden, die nach unterschiedlichen Paradigmen arbeiten und andere Forschungsergebnisse nicht einbeziehen (vgl. 340). Der wesentliche Unterschied der logisch-transformativen Methode zu den beiden anderen Methoden besteht darin, dass der Fokus auf die Anforderungsanalyse gerichtet ist und die Organisationen in Metaebenen abstrahiert werden, um die Sicherheit aus mehreren Perspektiven zu betrachten. Infolge können die Eigenheiten einer Organisation bei der Konzeption der Informationssicherheit beachtet werden. Dies bedingt, dass die für die Architektur verantwortliche Person über Erfahrung in der Entwicklung der Architektur verfügt, damit die Sicherheitsmaßnahmen effektiv greifen und keine nachträglichen Modifikationen erforderlich sind, da potenzielle Fehlplanungen erst bei der späteren Implementierung der Maßnahmen erkannt werden.

Daher geschieht die Konzeption einer Architektur, die die Anforderungen an die Informationssicherheit einer Organisation erfüllt, durch die Modellierung nach verschiedenen abstrahierten Metaebenen. Dabei wird auf die vorherige Generation zurückgegriffen. Eine Architektur der Informationssicherheit wird in Übereinstimmung mit der Vorgabe zur Integration der Informationssicherheit in die Enterprise Architecture gemäß SP 800-53 konzeptioniert (vgl. NIST 2020: 198). Erstere wird auch als Enterprise Security Architecture (ESA) bezeichnet. Sie erlaubt eine ganzheitliche Konzeption der Informationssicherheit und kann zudem in die Enterprise Architecture integriert werden, um die Gesamtarchitektur des Unternehmens zu erweitern.

1.4. DEFINITION DER ENTERPRISE SECURITY ARCHITECTURE

Die ISO/IEC/IEEE 15704:2019 definiert den Begriff ‚Architektur‘ als Konzeptualisierung der Form, Funktion und Zweckmäßigkeit eines Unternehmens in seiner Umwelt. Diese Konzeptualisierung ist in den Elementen des Unternehmens, den Beziehungen zwischen diesen Elementen, den Beziehungen des Unternehmens zu seiner Umwelt sowie den Grundsätzen für die Gestaltung und Entwicklung des Unternehmens verkörpert (vgl. ISO 2019a). Dabei wird die reale Welt abstrahiert, die in einer definierten Modellierungssprache visualisiert wird. Die Reduktion der Komplexität einer Einheit erlaubt die Durchführung diverser Analysen, um die Anforderungen verschiedener Stakeholder:innen in der Architektur zu adressieren. Architekturen werden unter Zuhilfenahme von methodischen Vorgehensmodellen entwickelt, um (1) Transformationspläne aufzustellen, die die Strategie einer Organisation implementieren, (2) diverse Arten von Analysen durchzuführen und (3) in der Entscheidungsfindung zu unterstützen.

Eine Unternehmensarchitektur (Enterprise Architecture) hat zum Ziel, die Anforderungen verschiedener Stakeholder:innen zu formalisieren und diese im Kontext des Unternehmens darzustellen. Dazu werden anhand geschäftlicher sowie technischer Architekturen die Abhängigkeiten zueinander aufgezeigt. Der Begriff ‚Enterprise Architecture‘ wurde im Jahr 1987 im Artikel *A framework for information systems architecture* eingeführt. Gleichzeitig wurde das Zachman-Framework erstmalig präsentiert (vgl. Zachman 1987). Das Framework stellt eine Enterprise Ontologie sowie eine fundamentale Struktur für die Enterprise Architecture dar.

Die Erweiterung der Enterprise Architecture um eine ganzheitliche Sicherheitsarchitektur wurde durch die Entwicklung verschiedener ESA-Frameworks wie ‚Sherwood Applied Business Security Architecture‘ (SABSA) (vgl. Sherwood 2005) und ‚The Open Group Architecture Framework‘ (TOGAF) (vgl. The Open Group 2022b) vorangetrieben. Letzteres ist ein Enterprise-Architecture-Framework, dessen Fokus nicht explizit auf Sicherheit liegt. Das methodische Vorgehen zur Implementierung der Sicherheit unterstützt die Strategie sowie die Organisationen im Umgang mit komplexen Geschäftsprozessen (vgl. Goudalo/Seret 2009; Wang et al. 2009).

Die Berücksichtigung der Sicherheitsanforderungen erfolgt in TOGAF implizit im Rahmen der Aufnahme und der Analyse der Stakeholder:innen-Anforderungen. Die implizite Arbeitsweise birgt das Risiko, dass nicht alle Sicherheitsaspekte berücksichtigt werden. Um diesem Umstand zu begegnen, wurde ein Integrationsmodell entwickelt, in dem SABSA in TOGAF eingebunden ist, um die Sicherheit

explizit mit zu betrachten (vgl. The Open Group 2011). In der Praxis findet SABSA daher bei der Entwicklung der ESA Beachtung (vgl. Sherwood et al. 2009: 4).

1.5. SABSA

Das SABSA-Framework weist eine ähnliche Struktur wie das Zachman-Framework auf und abstrahiert die Organisation in fünf Ebenen. Die Abstrahierung sowie die Betrachtungsweisen lassen sich Abbildung 2 entnehmen. Die Architekturmatrixt umfasst die Resultate der jeweiligen Ebene. Die letzte Reihe dient als Referenz zur Managementmatrix, die die erforderlichen Maßnahmen zur Erzielung der jeweiligen Resultate der Architekturmatrixt darstellt.

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECTURE	Business Goals & Decisions Business Value; Taxonomy of Business Assets, including Goals & Objectives, Success Factors, Targets	Business Risk Opportunities & Threats Inventory	Business Meta-Processes Business Value Chain; Business Capabilities	Business Governance Organisational Structure & the Extended Enterprise	Business Geography Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Business Time Dependence Time dependencies of Business Goals and Value Creation
CONCEPTUAL ARCHITECTURE	Business Value & Knowledge Strategy Business Attributes Taxonomy & Profile (with integrated performance targets)	Risk Management Strategy & Objectives Enablement & Control Objectives; Policy Architecture; Risk Categories; Risk Management Strategies; Risk Architecture; Risk Modelling Framework; Assurance Framework.	Strategies for Process Assurance Inventory of all Operational Processes (IT, Industrial, & manual); Process Mapping Framework; Architectural Strategies for IT used in process support.	Security & Risk Governance; Trust Framework Owners, Custodians and Users; Service Providers & Customers; Trust Modelling Framework	Domain Framework Security Domain Concepts & Framework	Time Management Framework Through-Life Risk Management Framework; Attribute Performance Targets
LOGICAL ARCHITECTURE	Information Assets Inventory of Information Assets; Information Model of the Business	Risk Management Policies Risk Models; Domain Policies; Assurance Criteria (populated Assurance Framework).	Process Maps & Services Information Flows; Functional Transformations; Service Oriented Architecture; Services Catalogue; Application Functionality and Services	Trust Relationships Domain Authorities; Entity Schema; Privilege Profiles; Trust Relationship Models	Domain Maps Domain Definitions; Inter-domain Associations & Interactions	Calendar & Timetable Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets Data Dictionary & Data Storage Devices Inventory	Risk Management Practices Risk Management Rules & Procedures; Risk Metadata	Process Mechanisms Working Procedures; Application Software; Middleware; Systems; Security Mechanisms; Process Control Points	Human Interface User Interface to Business Systems; Identity & Access Control Systems	Infrastructure Workspaces; Host Platforms, Layout of Devices & Networks	Processing Schedule Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	Component Assets Products and Tools, including Data Repositories and Processors	Risk Management Components & Standards Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Process Components & Standards Tools and Protocols for Process Delivery; Application Products	Human Entities: Components & Standards Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Locator Components & Standards Nodes, Addresses and other Locators; Component Configuration	Step Timing & Sequencing Components and Standards Time Schedules; Clocks, Timers & Interrupts
MANAGEMENT ARCHITECTURE	Delivery and Continuity Management Assurance of Operational Excellence & Continuity	Operational Risk Management Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Process Delivery Management Management & Support of Systems, Applications & Services	Governance, Relationship & Personnel Management Management & Support of Enterprise-wide and Extended Enterprise Relationships	Environment Management Management of Buildings, Sites, Platforms & Networks	Time & Performance Management Management of Calendar and Timetable

Abbildung 2: Architekturmatrixt

Quelle: (Sherwood et al. 2018: 7)

Im Rahmen der Contextual Architecture wird der Kontext der Organisation ermittelt. Zunächst werden die Businessanforderungen gesammelt, um auf dieser Grundlage die jeweiligen Sicherheitsanforderungen zu erheben. Des Weiteren werden Entitäts- und Beziehungsmodelle erstellt, um die betroffenen Organisationen des Untersuchungsbereiches zu erfassen. Im Anschluss erfolgt eine Risikoanalyse, um potenzielle Risiken und Chancen zu identifizieren (vgl. Sherwood 2005: 169–215; Sherwood et al. 2018).

In der Conceptual Architecture werden die Key-Performance-Indicators, die Key-Risk-Indicators, die Key-Control-Indicators und die Performanceziele für jede ermittelte Sicherheitsanforderung definiert, zudem der SOLL-Zustand (Control Ob-

jectives) der Sicherheit. Innerhalb dieser Control Objectives können die Sicherheitsmaßnahmen der verschiedenen Sicherheitsstandards wie der IT-Grundschutz (vgl. BSI 2017a), die ISO/IEC 27001 (vgl. ISO 2022a), PCI DSS (vgl. PCI Security Standards Council 2024) und NIST SP 800-53 (vgl. NIST 2020) zusammengetragen sowie formalisiert werden, um eine einheitliche und den Sicherheitsstandards entsprechende Sicherheit zu etablieren (vgl. Sherwood 2005: 217–283; Sherwood et al. 2018).

Die Logical bis Component Architecture modellieren die Architektur nach den Vorgaben der vorherigen Ebene, indem die Modellierungen konkretisiert werden (vgl. Sherwood 2005: 289–405; Sherwood et al. 2018). Dies lässt sich anhand eines Beispiels verdeutlichen:

- Logical: Beim Betreten der Domäne muss nach AAL3 authentifiziert werden.
- Physical: Für die Authentifizierung werden digitale Zertifikate eingesetzt.
- Component: Es wird der X.509-Standard verwendet.

1.6. UNTERSUCHUNGSDESIGN UND GLIEDERUNG DER THESIS

In dieser Arbeit wird die Methodologie ‚Design Science Research‘ (DSR) angewendet, da diese auf die Konzeption und die Evaluierung innovativer Artefakte fokussiert ist, sodass die Organisationen wesentliche informationsbezogene Herausforderungen bewältigen können (vgl. Hevner et al. 2004). Des Weiteren wurde diese Methodologie bereits in früheren Arbeiten zu ESA erfolgreich angewendet (vgl. Loft et al. 2022; Graham et al. 2021; McClintock et al. 2020). Diese Thesis folgt den Guidelines der DRP und setzt diese durch die Methodologie ‚Design Science Research Process‘ (DSRP) um (vgl. Peffers et al. 2007), die zudem als Dokumentenstruktur dieser Master-Thesis eingebettet ist, siehe Abbildung 3. Der DSRP nach Peffers wurde als Forschungsprozess gewählt, da er die Vorgaben des DSR nach Hevner operationalisiert und den Ablauf der Durchführung entsprechend der Methodologie vorgibt.

In Abbildung 3 ist die Verknüpfung der verschiedenen DSRP visualisiert. Der Demonstrationsprozess liegt außerhalb des Scopes dieser Arbeit, da das Ziel die Erstellung eines konzeptionelles Modell ist, weshalb der Demonstrationsprozess nicht betrachtet wird.

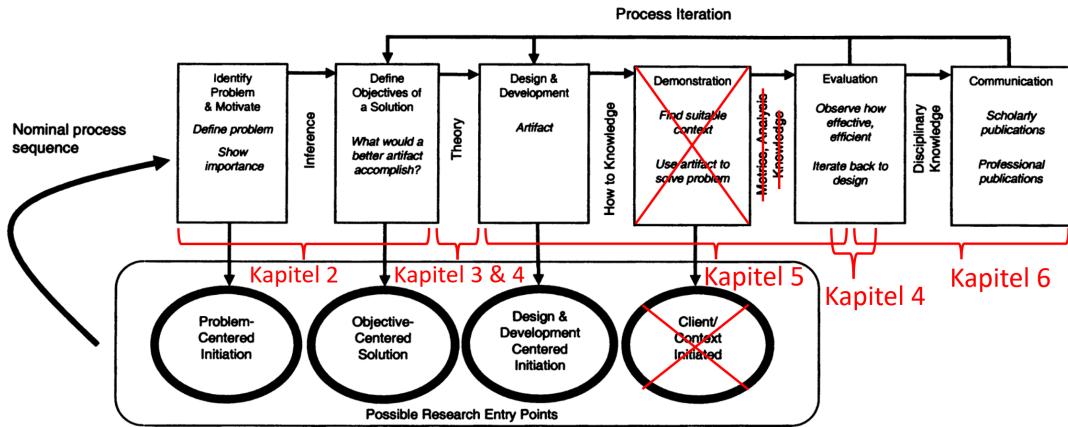


Abbildung 3: Forschungsdesign
Quelle: In Anlehnung an (Peffers et al. 2007: 54)

In Kapitel 2 wird das Problem aufgezeigt, das sich auf den ersten Schritt des DSRP bezieht. Aus diesem Grund wird in dieser Arbeit ein problemorientierter Ansatz verfolgt.

In Kapitel 3 werden die in der vorliegenden Untersuchung eingesetzten Forschungsmethoden beschrieben. Zudem wird die Methode zur Evaluierung des entwickelten Artefakts erörtert.

In Kapitel 4 werden die Resultate der für die Phase "Design & Development" einfließenden Inputs dargelegt sowie die Resultate der Evaluation beschrieben.

In Kapitel 5 erfolgt eine Darstellung des Entwicklungs- und Evaluationsprozesses des Artefakts. Des Weiteren werden Möglichkeiten dargelegt, wie das Artefakt in der Praxis implementiert werden könnte.

In der Diskussion (vgl. Kapitel 6) wird das entwickelte Artefakt in Bezug auf die Erfüllung der zuvor definierten Anforderungen geprüft. Ebenfalls werden diese Arbeit und die Ergebnisse anhand der sieben Guidelines von Hevner bewertet (vgl. 2004: 83).

In Kapitel 7 'Conclusio' sind relevante Forschungsbeiträge dieser Arbeit skizziert und mögliche Aspekte für zukünftige Forschungen aufgezeigt.

2. ZIELSETZUNG DER THESIS

Dieses Kapitel beinhaltet die Problematik, die Informationssicherheit in Organisationen zu etablieren. Zunächst werden die Anforderungen an die Gestaltung der Informationssicherheit erörtert, auf deren Basis die Forschungsfrage dieser Arbeit entwickelt wird.

2.1. PROBLEMIDENTIFIZIERUNG

Wie in Kapitel 1.3 dargelegt, ist in den Sicherheitsstandards festgelegt, dass die Informationssicherheit nach der Strategie der Organisation auszurichten ist. In Ermangelung von Hinweisen oder Beschreibungen in den Umsetzungsleitlinien dieser Standards (vgl. ISO 2017; BSI 2023b) sind die Verantwortlichen mit Schwierigkeiten bei der Zielerreichung konfrontiert. Die geringe Wahrscheinlichkeit einer Integration von Sicherheitsverantwortlichen in Verwaltungsausschüssen (vgl. Stewart 2018: 47), die vorherrschende Betonung der Cybersicherheit in der öffentlichen Diskussion (vgl. BSI 2016: 3–5) und die steigende Anzahl regulatorischer Vorgaben bei der Cybersicherheit wie PCI DSS (vgl. PCI Security Standards Council 2024), EU NIS2- und EU RCE/CER-Richtlinie resultieren in einer Ausrichtung der Sicherheitsmaßnahmen nach technischen und prozessualen Aspekten (vgl. Dhillon et al. 2021: 8; Van Wessel et al. 2011: 869–874).

Um die Informationssicherheit nach der Strategie einer Organisation auszurichten, ist eine Architektur erforderlich. Diese unterstützt Organisationen bei der Gestaltung und Etablierung der Informationssicherheitsstrategie, der Organisationsstrategie sowie beim Umgang mit komplexen Geschäftsprozessen (vgl. Goudalo/Seret 2009; Wang et al. 2009).

Der Fokus dieser Arbeit liegt auf der Etablierung der Informationssicherheit nach dem IT-Grundschutz. Somit stellt sich die Frage, wie die Methodik erweitert werden kann, um einen Rahmen zu schaffen, in dem Informationssicherheit einerseits kontextspezifisch in der Organisation gestaltet sowie etabliert wird und andererseits die unterschiedlichen regulatorischen Anforderungen in der Organisation vereinheitlicht werden.

2.2. DESIGNANFORDERUNGEN

Das Ziel dieser Thesis ist die Erweiterung der IT-Grundschutz-Methodik, um die Gestaltung und die Etablierung der Informationssicherheit nach der Organisationsstrategie zu ermöglichen. Um ein Artefakt zu generieren, das in der Forschung und

der Wirtschaft genutzt werden kann, werden folgende Anforderungen an das Ergebnis gestellt:

Anforderung 1: Die erweiterte IT-Grundschutz-Methodik muss ESA-Fähigkeiten enthalten.

Anforderung 2: Es sollte weiterhin die Einhaltung des IT-Grundschutzes gewährleistet sein, um das ISMS nach dem BSI-Standard 200-2 zertifizieren lassen zu können.

Anforderung 3: Das Ergebnis sollte generell so klar sein, dass es in der Praxis anwendbar ist.

2.3. FORSCHUNGSFRAGE

Damit in der IT-Grundschutz-Methodik die Informationssicherheit nach der Organisationsstrategie gestaltet und etabliert werden kann, wird folgende Forschungsfrage beantwortet werden:

Wie kann die IT-Grundschutz-Methodik zur Entwicklung einer ganzheitlichen Sicherheitsarchitektur mit SABSA kombiniert werden?

Die Forschungsfrage beschränkt sich auf die Frage der Methodik zur Entwicklung der Informationssicherheit nach der Strategie und den Zielen einer Organisation. Die Dudenredaktion (o. D.) definiert Methodik als „festgelegte Art des Vorgehens“. In dieser Arbeit wird die Betrachtung von Sicherheitsmaßnahmen ausgeschlossen. Im Rahmen der Beantwortung der Forschungsfrage ist dabei zu berücksichtigen, dass die in Kapitel 2.2 beschriebenen Anforderungen eingehalten und beantwortet werden müssen.

3. EINGESETZTE FORSCHUNGSMETHODEN

Dieses Kapitel gibt einen Überblick über die Methoden, die zur Beantwortung der Forschungsfrage zum Einsatz gekommen sind. Zunächst wird ein allgemeiner Überblick über die Methoden gegeben, anschließend werden die Hauptgründe für deren Anwendung dargelegt und die Methoden mit der Forschungsfrage sowie den Anforderungen aus Kapitel 2.2 verknüpft. Im Anschluss erfolgt eine ausführliche Erläuterung jeder einzelnen Methode.

3.1. UNTERSUCHUNGSANSATZ

Zur Beantwortung der Forschungsfrage wurden qualitative Forschungsmethoden genutzt. In Abbildung 4 ist der eingesetzte Forschungsansatz für diese Master-Thesis visualisiert.

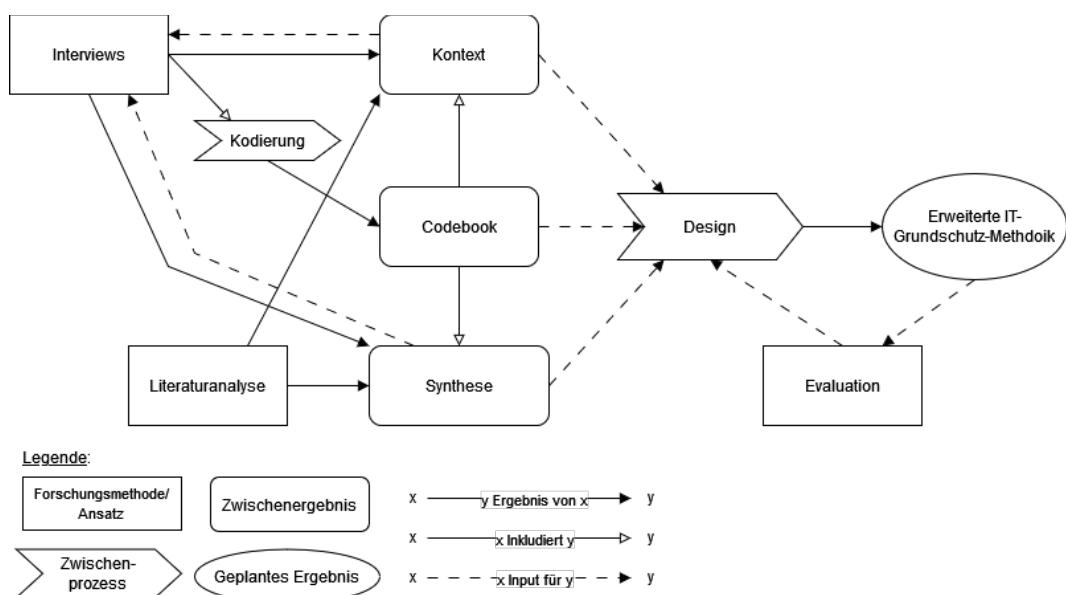


Abbildung 4: Forschungsansatz dieser Arbeit

Quelle: Eigene Darstellung

Der Evaluationsansatz besteht aus zwei Schritten: Zwischenbewertung und Endbewertung. Die Zwischenbewertung erfolgt auf Basis der durchgeföhrten Expert:inneninterviews. Die Endbewertung wird durch den Autor dieser Arbeit vorgenommen, wobei die Ergebnisse gegen die Anforderungen evaluiert werden. Beim DSR-Ansatz liefern die Zwischenergebnisse der Evaluierungsmethode ein kontinuierliches Feedback für das Design. Deshalb wird der Designzyklus mehrfach durchlaufen.

Die Zielsetzung der Literaturanalyse besteht in der Formulierung des zu untersuchenden Problems, der Identifikation relevanter Konzepte und Methoden sowie der

Positionierung der Studie (vgl. Ghauri et al. 2020: 57). In dieser Arbeit wurde zunächst eine Literaturanalyse durchgeführt, um einerseits die Zusammenhänge innerhalb der Thematik sowie bereits vorhandene Konzepte zu identifizieren und andererseits ein erstes Zwischenergebnis als Basis für die Expert:inneninterviews zu modellieren.

Im Rahmen der Expert:inneninterviews erfolgte die Präsentation des Zwischenprodukts sowie die Einholung von Feedback zu diesem. Darüber hinaus wurde eine Zwischenbewertung durch die Expert:innen durchgeführt. Dieses Vorgehen diente dem Zweck, ein Verständnis für die Ansichten der Expert:innen über die vorgestellte Herangehensweise sowie weiteren Kontext für die Etablierung der Informationssicherheit zu erhalten. Zudem konnten mögliche praktische Hinweise zur Nutzung gesammelt werden.

Die Resultate der Befragungen wurden in das Modell integriert, um abschließend in der Endbewertung evaluieren zu können, in welchem Umfang das Artefakt die Lösung des Problems fördern würde (vgl. Peffers et al. 2007). Anhand der Evaluation sollte festgestellt werden, inwiefern:

1. Expert:innen mit der erweiterten IT-Grundschutz-Methodik einverstanden und der Meinung sind, dass der Ansatz ihnen hilft, eine Architektur nach den Organisationszielen aufzustellen,
2. die erweiterte IT-Grundschutz-Methodik akzeptiert wird und
3. noch etwas fehlt.

3.2. LITERATURANALYSE

Um relevante Hintergründe und Vorgehensweisen zur ESA zu identifizieren, wurde eine systematische Literaturanalyse durchgeführt. Neben wissenschaftlicher wurde auch graue Literatur einbezogen, da im Bereich ‚Enterprise Architecture‘ Methodiken und Vorgehensweisen beschrieben werden, die in der Praxis teilweise als nicht praktikabel angesehen werden (vgl. Wagter et al. 2005; Ross et al. 2006: vii). Deshalb wurden eigene Variationen von Enterprise-Architecture-Methoden entwickelt (vgl. Carr/Else 2018; Ivas 2023; Namagembe et al. 2023). Um diese Diskrepanz in der Modellierung der erweiterten Methodik zu verhindern, wurde versucht, Hinweise zur Umsetzungsmöglichkeit in die Methodik einfließen zu lassen und somit die Lücke zwischen Forschung und Praxis zu schließen. Dies könnte über diese Thesis hinaus den Erfolg der Anwendung sichern und entspräche der dritten Anforderung an das Ergebnis aus Kapitel 2.2.

Für die Recherche nach wissenschaftlicher Literatur über die Plattformen ACM Digital Library, IEEE Xplore, ScienceDirect, dblp, Österreichischer Bibliothekenverbund, Bayerische Staatsbibliothek sowie die Universitätsbibliotheken von RWTH Aachen Universität, Karlsruher Institut für Technologie, Ludwig-Maximilians-Universität, Technologische Universität München und Universität für Weiterbildung Krems wurde ein strukturierter Ansatz gewählt. Es handelt sich bei den Plattformen um wissenschaftliche Online-Datenbanken. Die Suchbegriffe können den Anhängen B.1 ‚Strukturierte Literaturrecherche zum IT-Grundschutz‘ sowie B.2 ‚Strukturierte Literaturrecherche zu ESA und SABSA‘ entnommen werden.

Folgende Schritte wurden vorgenommen:

1. Suche in ausgewählten wissenschaftlichen Online-Datenbanken nach definierten Suchbegriffen;
2. Export der Ergebnisse mittels Skripts als Liste, das Duplikate entfernte;
3. Prüfen des Titels sowie des Abstracts jedes Artikels, ob es sich um ESA handelt;
4. Beurteilen, ob der Text über Google Scholar, Universitätsbibliothek der Universität für Weiterbildung Krems und eigene Zugänge durch Mitgliedschaften (IEEE-Membership, Science Direct, Bayerische Staatsbibliothek) digital frei verfügbar war;
5. Beurteilen der Artikel durch Überfliegen des Textes sowie Prüfen der Einleitung und der Schlussfolgerung, ob der Fokus auf Technik lag;
6. übrige Artikel genau lesen und beurteilen, ob über ESA auf Metaebene diskutiert wurde, sowie
7. Prüfen, ob Informationen die erweiterte Methodik bereicherten.

Des Weiteren wurden unstrukturierte Recherchen über die Suchmaschinen ‚Google Scholar‘ sowie ‚Google‘ durchgeführt. Aufgrund der hohen Anzahl von Ergebnissen war eine Filterung erforderlich (vgl. Giustini/Boulos 2013: 4). Obgleich der Inhalt sich laufend wandelte, unbekannte Aktualisierungspraktiken zum Einsatz kamen und eine mangelnde Zuverlässigkeit zu konstatieren war, sollten diese in der Literaturanalyse komplementär eingesetzt werden (vgl. Mastrangelo et al. 2010). Zudem unterstützte die Google-Suchmaschine bei der Recherche nach grauer Literatur, wobei verschiedene Keywords verwendet wurden.

3.3. EXPERT:INNENINTERVIEW

Im Rahmen der vorliegenden Untersuchung wurden Interviews mit Fachkräften und Verantwortlichen aus dem Bereich der Informationssicherheit durchgeführt.

Der Begriff ‚Fachkraft‘ bezeichnet eine Person, die sich in der Praxis, in der Beratung oder in der Forschung mit Informationssicherheit oder ESA befasst. Die forschenden Personen sind mit dem aktuellen Stand der Forschung im Bereich ‚Informationssicherheit und ESA‘ vertraut, während die Praktiker:innen über praktische Erfahrung in der Anwendung von Methoden zur Umsetzung der Informationssicherheit verfügen und die diversen Grenzen sowie langfristigen Auswirkungen in einer Organisation kennen. Die beratenden Personen können ihre Erfahrungen aus unterschiedlichen Organisationen in die Diskussion einbringen. Die Sichtweise der Verantwortlichen der Informationssicherheit einer Organisation ist relevant, da sie das ISMS etablieren und eine Informationssicherheitsstrategie erstellen. Die Perspektiven, die durch die Interviews gewonnen wurden, ergaben ein ganzheitliches Bild des Themas. Ziele der Interviews waren die deduktive Prüfung der erweiterten Methodik und die Generierung einer Theorie zum Einsatz der erweiterten Methodik mittels induktiven Vorgehens.

In den Interviews wurde zu Beginn die erweiterte Methodik präsentiert. Darauf aufbauend fand eine semistrukturierte Befragung statt. Die Verwendung festgelegter Fragen ermöglichte eine zielorientierte Lenkung der Interviews. Zudem wurde vorab ein Thema für jede Fragestellung definiert, um die Kodierung zu vereinfachen. Eine Auflistung dieser vordefinierten Fragen findet sich in Anhang C.1 ‚Interview Fragen und ihre Themen‘. Durch die offene Strukturierung erhielt der Interviewer eine genauere und klarere Perspektive der befragten Personen, da diese nach den eigenen Vorstellungen antworten konnten (vgl. Ghauri et al. 2020: 114). Nachfragen zu den Antworten führten zu zusätzlichen Informationen, die bei einem strukturierten Interview nicht möglich gewesen wären (vgl. ebd.: 115).

3.4. DATENANALYSE DER EXPERT:INNENINTERVIEWS

Die Durchführung der Interviews erfolgte mittels Videotelefonie. Die Aufzeichnungen wurden im Anschluss einer automatisierten Transkription unterzogen. Erstere dienen der Überprüfung der korrekten Transkription, die für die Datenanalyse unabdingbar ist.

Die transkribierten Antworten wurden mit einer generischen Form des offenen Kodierens kodiert, die an der Grounded Theory orientiert ist (vgl. Corbin/Strauss 2015). Für die Untersuchung wurde die Methodologie Grounded Theory angewandt, wobei nicht der gesamte Ansatz berücksichtigt wurde, da die theoretische Sättigung nicht erreicht werden kann. Gründe hierfür sind die uneinheitliche Definition sowie die divergierenden Ansichten zur systematischen Vorgehensweise

und zum Umgang in der ESA. Dies lässt sich auf die geringe Informationsmacht der befragten Personen zurückführen (vgl. Malterud et al. 2016), aufgrund der geringen Verbreitung von ESA. Des Weiteren existieren nach Hennink et al. (vgl. 2016: 15) keine allgemeingültigen Kriterien zur Messung der Sättigung. Stattdessen finden sich in der Literatur unterschiedliche Ausprägungen der Auslegung der Begrifflichkeit von Sättigung (vgl. Morse et al. 2014; Hancock et al. 2016; Fusch/Ness 2015; Hennink et al. 2019). Dies hat laut Fusch und Ness (vgl. 2015) zur Folge, dass die theoretische Sättigung subjektiv ist und die Sättigung von verschiedenen Personen unterschiedlich bewertet wird. Für die offene Kodierung wurde die Anwendung *QDA Miner Lite* verwendet. Dabei wurden die Transkripte importiert und mit einer generischen Form des offenen Kodierens kodiert. Zudem wurden die Kodierungen nach den im Interview gestellten Fragen gruppiert. Im Anschluss wurden die kodierten Transkripte analysiert. Es wurde versucht, Beziehungen zwischen den gegebenen Antworten zu finden. Kodierungen mit einer Häufigkeit von mehr als 50 % wurden einer detaillierten Betrachtung unterzogen, da sie als wiederkehrende Themen betrachtet wurden.

3.5. EVALUATION

Die Evaluierungsphase umfasst zwei Stufen, die jeweils auf den Resultaten des Expert:inneninterviews und den Gesamtergebnissen basieren. Gemäß dem Feedback erfolgten eine Evaluierung und Prüfung der erweiterten Methodik, um zu eruieren, inwiefern die Impulse integrierbar waren.

4. ERGEBNISSE DER FORSCHUNGSMETHODEN

Dieses Kapitel beinhaltet die Ergebnisse der Literaturanalyse und der Expert:inneninterviews.

4.1. LITERATUR ZU ENTERPRISE SECURITY ARCHITECTURE

Im Folgenden wird die identifizierte Literatur zu den Themen ‚IT-Grundschutz‘, ‚SABSA‘ und ‚ESA‘ erörtert.

4.1.1. SUCHERGEBNISSE DER LITERATURANALYSE

In einer strukturierten Suche wurden Peer-Reviews, Zeitschriftenartikel, Bücher sowie Bücherkapitel in deutscher und englischer Sprache bis zum 10. August 2024 berücksichtigt. Um einen umfassenden Überblick über den IT-Grundschutz sowie die ESA zu erlangen, wurden zwei separate Suchen durchgeführt. Die Ergebnisse wurden jeweils mittels Skripten exportiert, wobei Duplikate automatisiert nach dem Digital Object Identifier (DOI) oder Titel mit Einbezug der Autor:innennamen aussortiert wurden.

Bei der Literatursuche zum IT-Grundschutz wurden insgesamt 167 einzigartige Texte identifiziert und nach ihrem Inhalt gruppiert. Sie können dem Anhang B.1 ‚Strukturierte Literaturrecherche zum IT-Grundschutz‘ und Abbildung 5 entnommen werden.

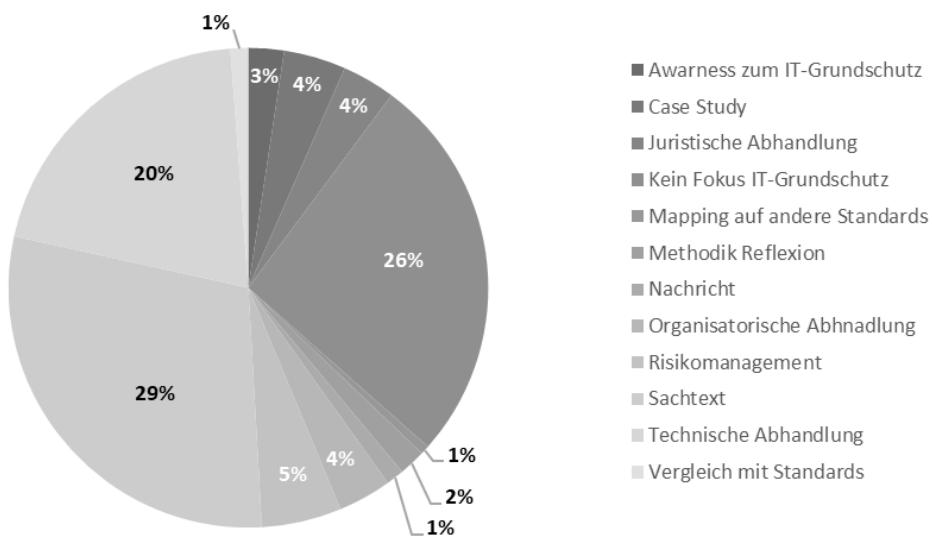


Abbildung 5: Aufteilung Textarten zum IT-Grundschutz
Quelle: Eigene Darstellung

Im zweiten Schritt wurden die Abstracts und die Texte auf ihre Übereinstimmung mit den Zielen der Studie geprüft. Die Ausschlusskriterien waren:

1. Sachtexte mit Erklärung der IT-Grundschutz-Methodik,
2. Texte, in denen kaum oder gar nicht auf den IT-Grundschutz eingegangen wird,
3. Artikel, die die Awareness zum IT-Grundschutz aufzeigen,
4. technische Abhandlungen oder Texte mit Fokus auf technische Aspekte,
5. Case Studies, in denen ausschließlich über die Anwendung geschrieben wird, ohne über die Methodik zu reflektieren, und
6. Nachrichten.

Inkludierende Merkmale waren:

1. Texte mit Fokus auf die Analyse des IT-Grundschutzes,
2. Vergleiche des IT-Grundschutzes mit anderen Sicherheitsstandards und
3. Case Studies zum IT-Grundschutz mit einer kritischen Betrachtung der Methodik oder Lessons Learned zur Methodik.

Das beschriebene Verfahren ergab eine Reduktion der Ergebnisse auf sechs Texte. Drei der Texte sind juristische Abhandlungen, wobei zwei die Frage des Datenschutzes im Kontext des IT-Grundschutzes beinhalten (vgl. Meints 2006; Claus 2007) und im dritten die Einhaltung des KRITIS-DachG durch die ISO/IEC 27001 und den IT-Grundschutz thematisiert ist (vgl. Maseberg 2023). Ein weiterer Text basiert auf einem juristischen Hintergrund. In diesem werden verschiedene Sicherheitsstandards miteinander verglichen, um den fehlenden Aspekt der rechtlichen Anforderungen an die IT und die Sicherheit abzudecken (vgl. Simić-Draws et al. 2013). Im fünften Text wird über den IT-Grundschutz reflektiert und es werden ein Vorschlag für einen Top-down-Ansatz sowie einige organisatorische Kontrollen präsentiert (vgl. Neitzel/Witt 2012). Im letzten Text ist ein Mapping von TO-GAF zum IT-Grundschutz thematisiert (vgl. Mathew et al. 2018).

Die durchgeführte Literaturrecherche hat ergeben, dass im Bereich des IT-Grundschutzes mit ESA keine Auseinandersetzungen bestehen. Des Weiteren lässt sich konstatieren, dass nur eine geringe theoretische Fundierung zum IT-Grundschutz existiert. Dieser Befund ist nicht auf den IT-Grundschutz beschränkt, sondern konnte auch in einer Literaturanalyse wissenschaftlicher Artikel zur ISO/IEC 27001 nachgewiesen werden (vgl. Culot et al. 2021).

Die zweite Suche zur ESA ergab eine Gesamtanzahl von 95 einzigartigen Texten. Die Liste kann dem Anhang B.2 „Strukturierte Literaturrecherche zu ESA und SABSA“ entnommen werden.

Die Ausschlusskriterien waren:

1. Nichtbetrachtung von Sicherheit,
2. Fokussierung auf technische Sicherheit,
3. Fokussierung auf spezielle Themen wie Risikomanagement,
4. fehlender Fokus auf Architektur und
5. Texte zu Vorgängerversionen, die überarbeitet wurden (z. B. SALSA).

Inkludierende Merkmale waren:

1. Fokussierung auf ESA,
2. Eigenentwicklungen von Frameworks und
3. kritische Betrachtungen der ESA.

Diese Filterung reduzierte die Anzahl der einzigartigen Texte auf elf. Davon bestehen sechs Texte aus Eigenentwicklungen von ESA-Frameworks (vgl. Loft et al. 2022; Larno et al. 2019; Ahmed et al. 2017; Lowman/Mosier 1997), von denen zwei SABSA ähneln (vgl. Graham et al. 2021; McClintock et al. 2020). Ein weiterer Text umfasst die Risikomodellierung und die Möglichkeit der automatisierten Entscheidungsfindung in ESA zur Beschleunigung der Architekturerstellung und zur Verbesserung der Qualität (vgl. Grov et al. 2019). Dieser vorgeschlagene Automatisierungsprozess auf Basis der Prüfung mittels Ontologien könnte durch eine Möglichkeit des Mappings von Sicherheitsanforderungen am STRIDE-Modell erweitert werden (vgl. Peterson 2010), um die Architekturarbeit mit SABSA zu vereinfachen. Insgesamt wurden zwei Texte zu SABSA gefunden, die einzige Auflage zu SABSA (vgl. Sherwood 2005), in der die aufgezeigten Prozesse und Methoden teils veraltet sind, sowie die Beschreibung der Conceptual Architektur mittels Metamodellen (vgl. Pleinevaux 2016). Der letzte Text handelt von der quantifizierten Bewertung der ESA (vgl. Alshammari 2017).

Die unstrukturierten Suchen wurden mit ähnlichen und anderen Keywords wie ESA in verschiedenen Kombinationen in Google und Google Scholar durchgeführt. Dabei wurden zwanzig Artikel zu SABSA und ESA verzeichnet. Überarbeitungen der veralteten Auflage zu SABSA (vgl. Sherwood 2005) sind in Whitepaper und Konferenztexte verteilt (vgl. The SABSA Institute 2023). Eine Literaturanalyse über die aktuellen Trends und die Kerngebiete von 1996 bis 2021 zeigte einen Fokus auf die operativen Aspekte der Informationssicherheit (vgl. Shiau et al. 2023).

4.1.2. ADAPTIVER WISSENSTRANSFER VON EA zu ESA

Trotz der geringen Anzahl von Abhandlungen zu ESA können Aspekte der Enterprise Architecture adaptiert übernommen werden. Nachfolgend werden die Methoden und Prozesse beschrieben, die für die Architekturarbeiten sowie das Umfeld in ESA relevant sind.

Die Etablierung einer ganzheitlichen Enterprise Architecture entsteht historisch betrachtet über eine Evolution der Architektur, die durch das Bedürfnis gegeben ist, in einer Organisation mit einer steigenden Komplexität umgehen zu können. Die Evolution kann in die vier Reifegrade ‚Business Silo‘, ‚Standardized Technology‘, ‚Optimized Core‘ und ‚Business Modularity‘ eingeteilt werden (vgl. Ross et al. 2006: 97–120). Diese Entwicklung spiegelt auch die Transformation der Enterprise Architecture in Organisationen wider (vgl. Barrera et al. 2011). Die Visualisierung der Reifegrade in Abbildung 6 zeigt zudem die Investitionskostenverteilung der IT.

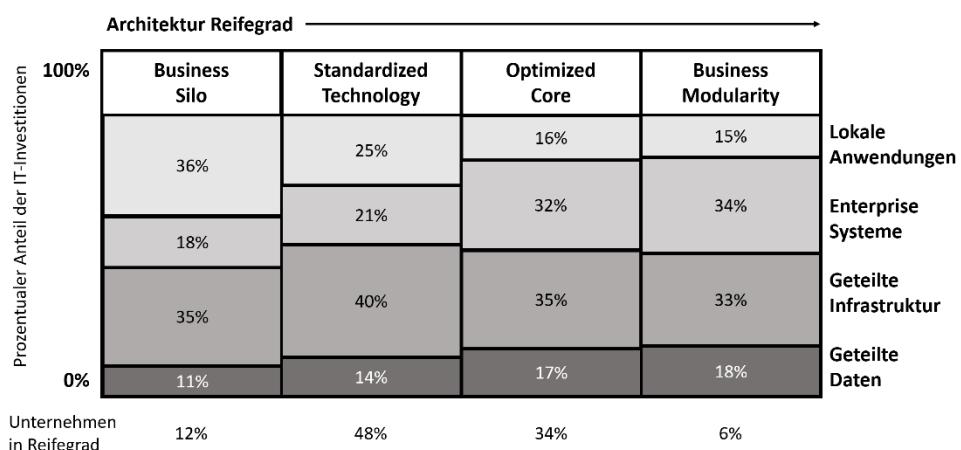


Abbildung 6: Reifegrade der Enterprise Architecture

Quelle: In Anlehnung an (Ross et al. 2006: 100)

Die ISO/IEC/IEEE 42020:2019 (vgl. ISO 2019b) enthält Prozessbeschreibungen für die Erstellung, Steuerung und Verwaltung von Architekturen. Dabei sind sechs Prozesse hervorgehoben und ihre Beziehung zueinander ist dargestellt. Letztere kann Abbildung 7 entnommen werden.

Der Architecture-Governance-Prozess definiert die Richtlinien und gibt Anleitungen für den Umgang mit Architekturen. Die Architecture Governance beschreibt die Ausrichtung und die Ziele der Architektur, um die unterschiedlichen Architekturen einheitlich zu halten und gewährleistet die Adressierung der Organisationsbedürfnisse (vgl. ISO 2019b: 15–20). Damit die Richtlinien und Vorgaben der Architektur eingehalten werden, wird der Architecture-Management-Prozess als Prüf- und Kontrollinstanz eingesetzt. Dieser gewährleistet die zeitliche, effektive und effiziente Erreichung der Ziele (vgl. ebd.: 20–27).

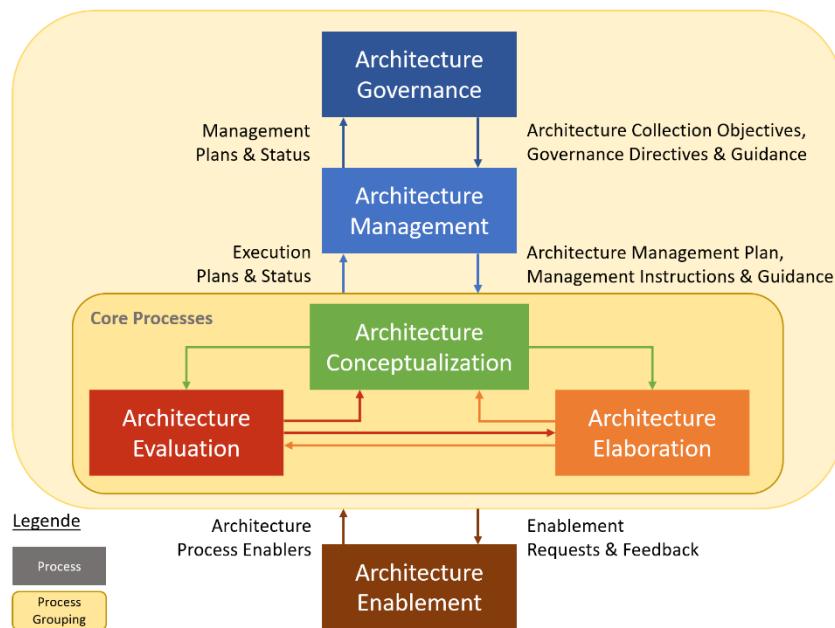


Abbildung 7: Architekturprozesse
Quelle: In Anlehnung an (ISO 2019b: 9)

Insgesamt definiert der Standard ISO/IEC/IEEE 42020 drei Kernprozesse. Der erste ist die Architecture Conceptualization (vgl. ebd.: 27–38). Sie charakterisiert den Problemraum und ermittelt eine passende Lösung, die die Anforderungen der Stakeholder:innen und der Architektur adressiert.

Der zweite Prozess ist die Architecture Evaluation, d. h., inwieweit die Ziele und Anforderungen erfüllt werden (vgl. ISO 2019b: 38–47). Die Evaluierung ist in drei Tiers aufgebaut: Architectural Analysis, Value Assessment und Evaluation Synthesis. Die Architectural Analysis untersucht die wesentlichen Charakteristika einer Architektur, beispielsweise ihre Eigenschaften in Bezug auf spezifische Dimensionen wie Sicherheit, Kosten, Leistung und andere. Darüber hinaus werden die relevanten Merkmale der Architektureinheit sowie die tatsächlichen oder potenziellen Auswirkungen auf Stakeholder:innen oder die Umwelt analysiert. Zudem werden die Architekturvision, die Prinzipien und die Konzepte geprüft, die für die Zielerreichung relevant sind (vgl. ISO 2019c: 11). Das Value Assessment ermittelt den Umfang und die Art des Wertes einer Architektur, den Stakeholder:innen erwarten können. Dieser Wert kann quantitativ oder qualitativ beschrieben werden (vgl. ebd.: 9). Das höchste Tier ist die Evaluation Synthesis. Hierbei wird das Ergebnis mehrerer Value Assessments kombiniert, um festzustellen, inwieweit die Bewertungsziele erreicht werden. Die Bedenken der Stakeholder:innen zur Evaluierung

können durch die Evaluation Synthesis adressiert werden (vgl. ebd.: 7). Eine Übersicht der Evaluierungs-Tiers und ihre Beziehungen zueinander können Abbildung 8 entnommen werden.

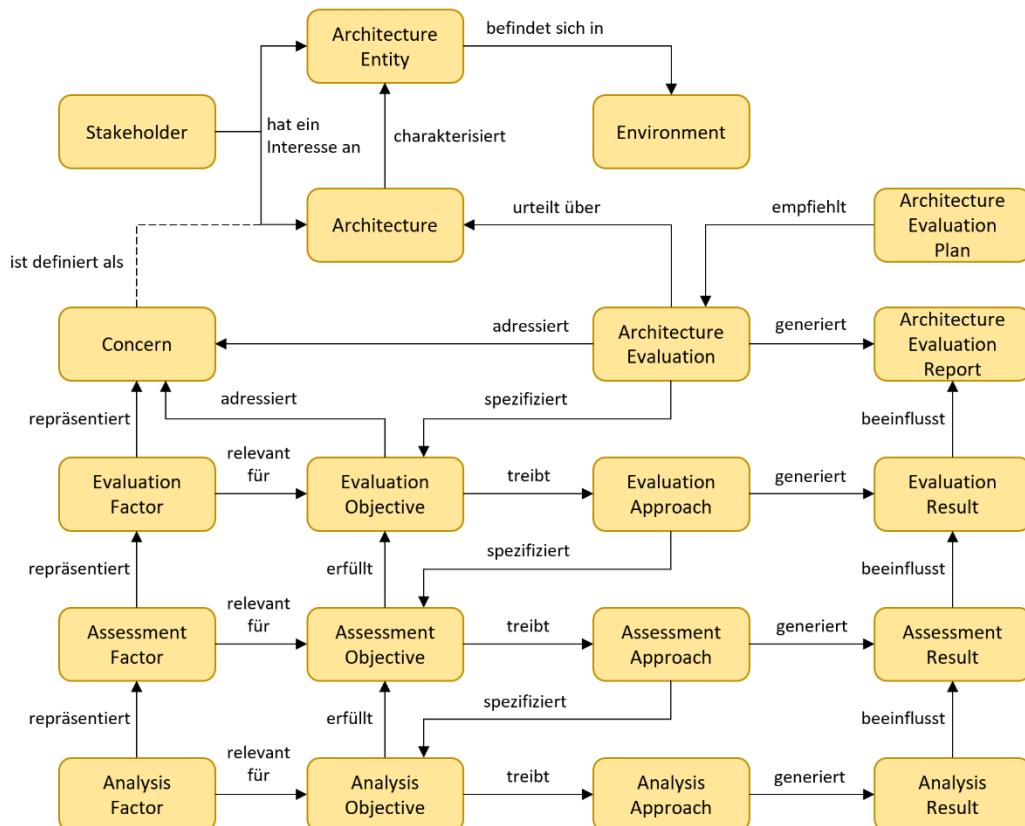


Abbildung 8: Evaluierung der Architektur
Quelle: In Anlehnung an (ISO 2019c: 13)

Der dritte Kernprozess ist die Architecture Elaboration. Dieser Prozess ist die eigentliche architektonische Arbeit, da die Architektur in einer für die beabsichtigte Nutzung ausreichenden, vollständigen und korrekten Weise dokumentiert wird (vgl. ISO 2019b: 47–53).

Der letzte Prozess ist das Architecture Enablement. Ziel ist die Befähigung der Abteilungen, die Architekturprozesse durchzuführen, indem die benötigten Ressourcen bereitgestellt werden, qualifiziertes Personal eingesetzt und das Personal weitergebildet wird.

In der Enterprise Architecture wird mit sechs EA-Artifacts gearbeitet, die sich gegenseitig beeinflussen (vgl. Kotusev 2021: 129–142). Abbildung 9 dient der Visualisierung der EA-Artifacts sowie der Beschreibung ihrer Beziehungen zueinander.

Im Rahmen der ‚Considerations‘ werden die getroffenen Entscheidungen in Bezug auf die Zusammenarbeit zwischen Organisation und IT dokumentiert. Die ‚Vision‘

beschreibt die langfristige Unterstützung der Organisation durch die IT. Die ‚Outlines‘ definieren die spezifischen Implementierungen der IT-Initiativen einer Organisation. In ‚Standards‘ werden technische Regeln festgelegt, die die Grundlage für die Implementierung der IT-Systeme bilden. Die ‚Landscapes‘ legen den aktuellen Ist-Stand der IT-Landschaft dar und beschreiben die Entscheidungen zu ihrer zukünftigen Entwicklung. Unter dem letzten EA-Artifact ‚Designs‘ werden die Entscheidungen zu den genauen Spezifikationen dokumentiert (vgl. ebd.: 129–142).

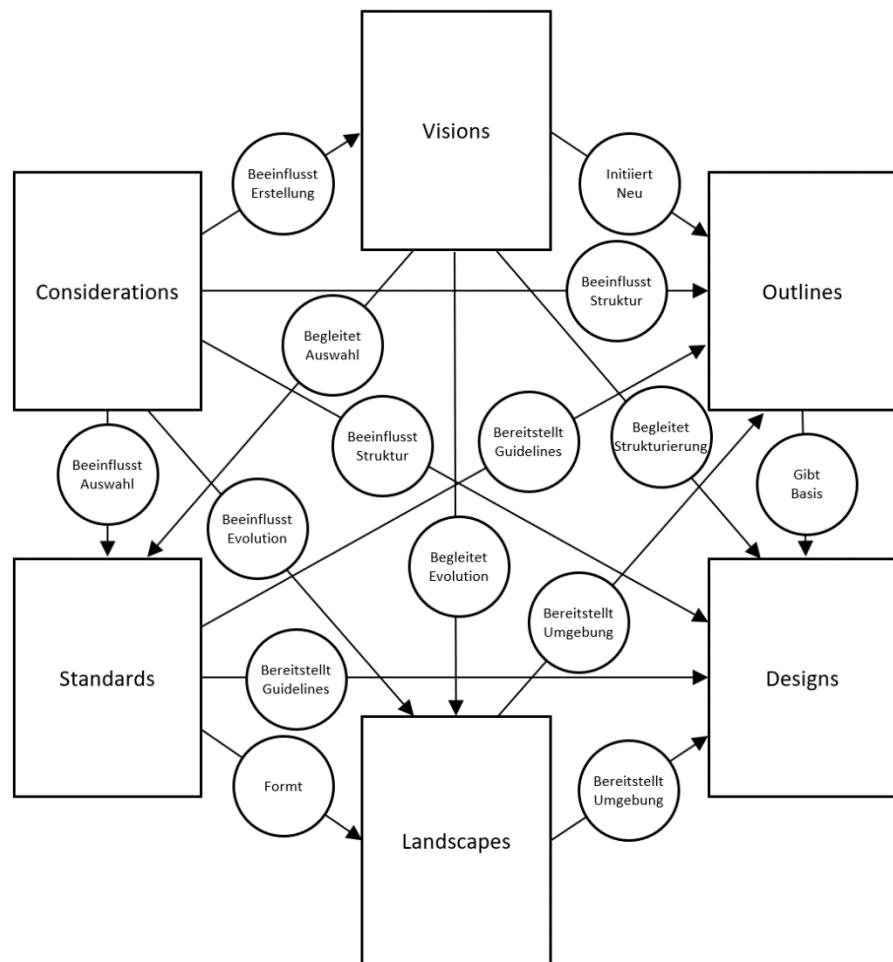


Abbildung 9: CSVLOD-Modell
Quelle: In Anlehnung an (Kotusev 2021: 66)

Traditionelle Enterprise Architecture Frameworks wie TOGAF (vgl. The Open Group 2022b) haben ihren Ursprung im IBM Business Systems Planning (vgl. IBM 1984), da die Frameworks vom jeweiligen Vorgänger beeinflusst wurden (vgl. Kotusev 2016: 396–407). Organisationen werden als Systeme betrachtet und ihre Anforderungen aus der Organisationsstrategie abgeleitet.

Es existieren jedoch zwei alternative Ansätze, wie eine Enterprise Architecture in einer Organisation aufgestellt werden kann. Der erste Ansatz ist die Enterprise

Architecture as Strategy, nach der Organisationen ihre Strategie nach der Enterprise Architecture ausrichten sollten. Die Architektur soll nach dem Operation Model der Organisation strukturiert werden (vgl. Ross et al. 2006). Aufgrund der Umkehrung der Beziehung zwischen Enterprise Architecture und Strategie eignet sich dieses Vorgehen vor allem für größere Organisationen, die nicht in einem volatilen Umfeld arbeiten. Die zweite Alternative ist der Dynamic-Architecture(DYA)-Ansatz (vgl. Wagter et al. 2005). Bei diesem wird das Prinzip „just enough, just in time“ (ebd.: 44) propagiert. Das heißt, Architekturaktivitäten sollen erst durchgeführt werden, wenn sie benötigt werden. Zudem soll der Beteiligtenkreis so klein wie möglich gehalten werden. Eine weitere Besonderheit ist, dass ausschließlich der jeweilige Business Case betrachtet und keine Strategie einbezogen wird. Dadurch eignet sich DYA für kleinere Organisationen, die in einem unvorhersagbaren Umfeld agieren.

Obwohl die Enterprise Architecture die Performance einer Organisation (vgl. Ge- row et al. 2014; Byrd et al. 2006) sowie die Kommunikation zwischen der IT und dem Business nachhaltig verbessert (vgl. Wagner et al. 2014; Luftman/Brier 1999), fehlen konkrete Umsetzungsbeschreibungen zu ihrer Etablierung (vgl. Kar- povsky/Galliers 2015; Coltman et al. 2015; Chan/Reich 2007). Dies erschwert den Aufbau von Kompetenzen und die Etablierung einer effektiven Architektur.

4.2. PERSPEKTIVEN DER EXPERT:INNEN

Im Anhang C.2 ‚Hintergrundinformation zum Expert:inneninterview‘ wird in Tabelle 15 die Verteilung der Befragten dargestellt. Es wurden Vertreter:innen aller relevanten Interessensgruppen von Chief Information Security Officer (CISO), praxisbezogene, beratende und forschende Personen in den Expert:inneninterviews berücksichtigt. Zudem ist erkennbar, dass mehr als die Hälfte der eingeladenen Personen (kurzfristig) abgesagt haben. Insgesamt wurden zehn Expert:inneninterviews über *Microsoft Teams* geführt. Diese wurden aufgezeichnet und mittels Microsoft Teams automatisiert transkribiert. Die geglätteten Transkripte können Anhang D entnommen werden. Um die Perspektiven der Personen in einen Kontext zu setzen, ist unter Anhang C.2 ‚Hintergrundinformation zum Expert:inneninterview‘ in Tabelle 16 der Reifegrad der Sicherheit einer Organisation aufgezeigt, in der die Person angestellt ist oder berät. Aus datenschutzrechtlichen Gründen werden die befragten Personen anonym behandelt.

Wie in Kapitel 3.5 dargelegt, wurde jedes Transkript kodiert. Anhang C.3 ‚Codes und ihre Häufigkeit‘ beinhaltet eine Übersicht der erstellten Codes mit ihrer jeweiligen Häufigkeit in den Expert:inneninterviews. Die Antworten auf die offenen Fragestellungen und die Folgefragen führten zu weiteren Informationen, die dann mit einem Code eines anderen Themas versehen wurden. Um die Beziehungen zwischen den Codes und dem Inhalt zu verdeutlichen, wurden die Codes mittels *Microsoft PowerPoint* visualisiert und nach ihrem Inhalt in Kategorien gruppiert. Die Abbildung ist im Anhang C.4 ‚Zusammengefasste Kodierung‘ dargestellt. Die Synthese des Informationsgehaltes in Kategorien vereinfacht die Analyse und ermöglicht eine ganzheitliche Betrachtung der erweiterten IT-Grundschutz-Methodik. Dabei wurden Kategorien mit einer Häufigkeit von $\geq 50\%$ genauer analysiert, da sie als wiederkehrende Kategorien gelten. Infolge werden die wiederkehrenden Kategorien beschrieben, die der Autor dieser Arbeit aus den Expert:inneninterviews interpretiert hat.

Die Relevanz der verschiedenen befragten Personen für die Kategorien wird durch das Setzen von Markern in Klammern in den Kategoriebeschreibungen dargestellt. Diese bestehen aus dem Anfangsbuchstaben der Rolle (F für Forscher:in, P für Praktiker:in, B für Berater:in, C für CISO) und der Nummer der Person.

Integrierter Lösungsansatz

Die in den Expert:inneninterviews thematisierte erweiterte IT-Grundschutz-Methodik wurde als integrierte Lösung wahrgenommen, die eine Ende-zu-Ende-Entwicklung und eine Etablierung der Informationssicherheit in einer Organisation ermöglicht (P1, B2, F2). Diese Ende-zu-Ende-Betrachtung schaffe eine Transparenz über den Einsatz der zu implementierten Sicherheitsmaßnahmen und biete durch die vordefinierte Art, wann diese an welcher Stelle einzusetzen seien (P3), eine Arbeitserleichterung. Zudem könne dies im Gegensatz zu den bestehenden Sicherheitsstandards Interpretationen vermeiden, wie gewisse Sicherheitsmaßnahmen anzuwenden seien (P3). Die Ableitung der Informationssicherheitsanforderungen aus den Organisationszielen, ihre Strukturierung nach einer Zielvision sowie die Modellierung der Architektur mittels SABSA und die operative Beschreibung zur Implementierung der Sicherheit mit dem IT-Grundschutz stellten eine komplementäre Ergänzung dar. Die erweiterte Methodik gäbe eine Anleitung zur Etablierung der Informationssicherheit von der Strategie bis zu den operativen Maßnahmen (P1, F2). Gleichzeitig gewährleiste das Vorgehen die Nachvollziehbarkeit der Sicherheit (P3). Ebenfalls ermögliche die Beschreibung des Vorgehens

die zielorientierte Durchführung der Arbeitstätigkeiten, wodurch eine strukturierte Bearbeitung der Aufgaben sichergestellt werde (P1, P3). Zudem ergänze die erweiterte Methodik die Messbarkeit, um die Sicherheit auf Basis von gemessenen Werten zu verbessern (B1). Der Aufbau lasse eine ganzheitliche Betrachtung der Informationssicherheit zu (C2, F1), die sich von anderen Standards abhebe, da der Fokus auf Strömen statt Hierarchien liege (B3).

Die Integration dieses Lösungsansatzes in bestehende Aufbau- und Ablauforganisationen werde durch die Organisationskultur, die Sicherheitskultur und die Adaptation beeinflusst (vgl. Abbildung 25).

Sicherheitskultur

Im Rahmen der Expert:inneninterviews wurden Nachfragen zu den Antworten der Befragten gestellt, um den dahinterstehenden Kontext zu verstehen. Dabei wurden die Arbeitsweisen zur Sicherheit aufgedeckt.

Ein Aspekt sei, dass Organisationen ihre Sicherheit nach der Compliance ausrichten würden, um regulatorische Anforderungen einzuhalten (F1, C2, B2, B3, P2). Aufbauend darauf würden Organisationen mit Checklisten zur Konzeption und Etablierung der Informationssicherheit arbeiten (F1). Je nach fachlichem Hintergrund der Personen eines Sicherheitsteams liege der Fokus auf einer technischen oder einer prozessbasierten Herangehensweise (B1). Deshalb werde die erweiterte Methodik vor allem in regulierten Branchen mit Skepsis betrachtet, da keine öffentlich bekannten Anwendungen existieren würden (B3).

Obgleich der IT-Grundschutz die Erstellung von Profilen zur Anpassung der Methodik an die jeweilige Branche ermögliche, werde der organisatorische Kontext auf der höheren Ebene nicht betrachtet (P2). Zudem wurde angemerkt, dass – trotz des Ziels der Zertifizierung des ISMS – die Informationssicherheit in verschiedenen Organisationen als unstrukturierte Arbeitsweise angeführt würde (C1).

Die Summe der Aussagen dieser Kategorie lässt den Schluss zu, dass die Informationssicherheit durch eine extrinsische Motivation angetrieben wird, die auf die Organisationskultur zurückzuführen ist. Die möglichen Hintergründe werden in der Kategorie ‚Organisationskultur‘ aufgezeigt.

Organisationkultur

Die identifizierten Kodierungen zu den Herausforderungen und Risiken bei der Anwendung der erweiterten Methodik wurden vor allem in diesem Themenbereich gefunden.

Für die Anwendung der erweiterten Methodik sei das Engagement des Managements erforderlich (P1), das nicht vorhanden sein könne (C1). Laut einem Erfahrungsbericht unterstützen zwar die Enterprise Architects die Anwendung der erweiterten Methodik, aber die Fachbereiche seien aufgrund der Intensität – eine Kategorie, die im Verlauf dieses Kapitels aufgezeigt wird – gegen den Architekturansatz (F2, P3). Um dem entgegenzuwirken, sollte der Mehrwert der neuen Arbeitsweise verdeutlicht werden (P3). Zudem könnten die Struktur und der Aufbau der erweiterten Methodik von den Stakeholder:innen missverstanden werden, was zu falschen Erwartungen in Bezug auf die Möglichkeiten führen könne (C2).

Neben der mangelnden Unterstützung durch die Abteilungen könne auch die Zusammenarbeit zwischen den Abteilungen problematisch sein (B1). Zudem könne die Einführung zu Interessenskonflikten führen, da der integrierte Ansatz die Frage aufwerfe, inwieweit die Aufbau- und Ablauforganisation angepasst werden müsse (F2).

Gemäß den Ergebnissen einer Befragung weist die Organisationskultur keine intrinsische Motivation auf, die Informationssicherheit ganzheitlich zu etablieren. Nach einer Untersuchung ist die extrinsische Motivation auf den Wunsch der Kund:innen zurückzuführen. Die Informationssicherheit bzw. die Zertifizierung nach ISO/IEC 27001 verbessert das Image der Organisation (vgl. Liao/Chueh 2012: 7867) und erhöht die Chance, mehr Geschäfte abzuschließen, da potenzielle und bestehende Kund:innen Zertifizierungen zur Informationssicherheit fordern (vgl. Barafot et al. 2018: 57–58). Eine Möglichkeit, Personengruppen mit Wirtschaftsinteressen von der Organisation zu überzeugen, wäre die Darlegung der Auswirkung von Cyberangriffen auf den Aktienwert der Organisation. Da Cyberangriffe für den Aktienwert negativ sind, kann dies als Argumentationsgrundlage dienen (vgl. Spanos/Angelis 2016; Corbet/Gurdiev 2019).

Aufgrund des Einflusses der Organisationskultur auf die verschiedenen Themen ist das Stakeholder:innenmanagement für den Einsatz der erweiterten Methodik essenziell. Da dieser Aspekt auch für die Unternehmensarchitektur relevant ist, gibt es Ansätze, dies effektiv umzusetzen (vgl. Kurnia et al. 2021). Das TOGAF-Framework bietet hierzu eine Vorlage für das Stakeholder:innenmanagement und

zeigt einen möglichen Umgang mit den verschiedenen Personengruppen auf (vgl. The Open Group 2022: 296–318).

Umgang mit Komplexität

Im Hinblick auf die zukünftige Relevanz der erweiterten Methodik wurde von den Befragten die Verbesserung des Umgangs mit Komplexität hervorgehoben (F1, C1, C2, B1, B2, P3). Steigende regulatorische Anforderungen an die Informations-sicherheit sowie die zunehmende Vernetzung technischer Systeme würden zu ei-ner Komplexität führen, die schwieriger zu beherrschen sei.

Wegen der technologischen Komplexität in Unternehmensnetzwerken werde zu-nehmend auf Zero-Trust-Architekturen umgestellt. Diese könnten mit Hilfe der er-weiterten Methodik umgesetzt werden (P3).

Adaption

In dieser Kategorie erfolgt eine Zusammenfassung der Aspekte, die eine Anpas-sung der erweiterten Methodik für eine Anwendung in der Organisation erforderlich machen.

Bei der Anwendung der erweiterten Methodik sei eine detaillierte Beschreibung der durchzuführenden Aktivitäten in den jeweiligen Phasen sowie der zu erzielende Ergebnisse notwendig (P1). Zudem sei empfehlenswert, dass die Organisation prüfe, wie die erweiterte Methodik in die Organisationsstruktur sowie in bereits be-stehende Themen und Systeme integriert werden könne (F2). Es würden IT-Grundschutz-Profile existieren, die für spezifische Anwendungsfälle erstellt und von anderen Organisationen übernommen werden könnten (P2). Diese könnten ebenfalls für die erweiterte Methodik von den verschiedenen Branchen entwickelt werden. Die Anwendung würde jedoch voraussichtlich primär von größeren Orga-nisationen durchgeführt (P1). Organisationen in regulierten Sektoren würden die erweiterte Methodik nicht sofort anwenden, da sie zweifeln würden, ob sie sie ein-halten könnten. Grund sei, dass ihnen Erfahrung, Fachwissen und Expert:innen fehlen würden (B3). Diese Unsicherheit könne durch Pionierprojekte ausgeräumt werden, die die Möglichkeiten und die Konformität mit den regulativen Anforderun-gen aufzeigen würden (B3).

Als potenzielle Schwierigkeiten bei der Adaption könnten die uneinheitliche An-wendung des IT-Grundschutzes in Deutschland sowie die daraus resultierenden Probleme bei der Umsetzung von Sicherheitsmaßnahmen genannt werden (F1).

Des Weiteren bestehe die Möglichkeit, dass trotz der weiten Verbreitung des IT-Grundschutzes im deutschen Raum diverse Organisationen diesen nicht korrekt anwenden, was zu Problemen bei der operativen Umsetzung von Sicherheitsmaßnahmen führen könnte (F1).

Die folgenden Aspekte wurden in weniger als der Hälfte der Interviews erwähnt. Dennoch werden sie aufgeführt, da sie für die kritische Betrachtung der erweiterten Methodik relevant sind.

Strategische Unsicherheit

Aufgrund der Komplexität des Umfeldes einer Organisation könnten die Strategie der Organisation (F1) und damit die Unternehmensziele (C2) fehlen und unklar sein. Dies wirke sich negativ auf die Ableitung der Sicherheitsanforderungen aus, da diese aus der Strategie und den Unternehmenszielen abgeleitet würden.

Eine Möglichkeit, mit dieser strategischen Unsicherheit umzugehen, wäre die Anpassung des Vorgehens nach DYA (vgl. Wagter et al. 2005). Jedoch sollten die Nachteile nicht außer Acht gelassen werden, da die Ergebnisse sich ausschließlich an die Gegebenheiten anpassen und in Zukunft nicht wiederverwendet werden könnten.

Enterprise Architecture-Probleme

Die ESA basiert auf denselben Methoden und Prinzipien wie die Enterprise Architecture. Daher treten in der ESA ähnliche oder gleiche Probleme wie in der EA auf. Kritisiert wurde die zu akademische Sichtweise innerhalb der EA (P1). Zudem werde in der EA die Sicherheit nicht berücksichtigt (P1, P2).

Der Aspekt der zu akademischen Betrachtung wurde von verschiedenen Personen kritisiert. Aktuell existiert jedoch keine Lösung für einen praktikablen Umgang (vgl. Buckl et al. 2009: 15; Kotusev 2019: 104; Saint-Louis et al. 2017: 46–47). Der zweite Aspekt der fehlenden Behandlung der Sicherheit könnte mit SABSA und dieser Thesis gelöst werden, indem die Struktur von SABSA oder die erweiterte Methodik mit dem Artikel zur Integration in TOGAF verwendet würde (vgl. The Open Group 2011).

Intensität

Ein Erfahrungsbericht belegt, dass die Umsetzung von SABSA mit einem hohen Zeitaufwand und komplexen Anforderungen verbunden ist (F2). Die Intensität der SABSA-Durchführung sei auf die Adaption der Methodik sowie die fehlende Expertise in der Konzeption von Sicherheitsarchitekturen in einem agilen Umfeld zurückzuführen.

Aufgrund der Intensität könnten verschiedene Personengruppen das Vertrauen in das Vorhaben verlieren. Eine Gegenmaßnahme wäre der Ansatz eines inkrementellen Vorgehens, bei dem anfangs ein kleiner Anwendungsbereich gewählt und nach jedem Inkrement der Bereich erweitert wird. Dadurch könnten vorzeitige Ergebnisse geliefert werden, um das Commitment der Personengruppen zu halten.

Eine Herangehensweise wäre zudem die Verwendung agiler Methoden in der Architektur. In TOGAF werden die Definitionen und Strukturierungen für eine agile Architektur beschrieben (vgl. The Open Group 2022c; The Open Group 2022a).

Unsicherheit, ob ESA nötig

In einem der Expert:inneninterviews wurde die Unsicherheit beschrieben, inwiefern die Erweiterung des IT-Grundschutzes mit SABSA erforderlich wäre (P2). In diesem Kontext wurde ergänzend darauf hingewiesen, dass die postulierte Notwendigkeit einer Erweiterung des Sicherheitskonzeptes nur dann gegeben wäre, wenn bei der Anwendung der Sicherheitsstandards die Sicherheit auf die Organisation ausgerichtet würde.

Da Sicherheitsstandards wie ISO/IEC 27001 (vgl. ISO 2022a), NIST SP 800-53 (vgl. NIST 2020) und IT-Grundschutz (vgl. BSI 2017a) keine Anleitung zur Ausrichtung der Sicherheit auf die Organisation bieten, müssen Organisationen eigene Methoden entwickeln. Die erweiterte IT-Grundschutz-Methodik basiert auf die Erweiterung mit dem SABSA-Framework, das eine geschäftsorientierte Architektur ermöglicht.

Auditierung

Das erweiterte Vorgehen entferne sich von einer auditzentrierten Methodik und werde architekturzentriert, indem die Sicherheit aus dem Kontext der Organisation abgeleitet werde. Das verändere die Etablierung der Informationssicherheit und unterscheide sich vom typischen Vorgehen zur Zertifizierung des ISMS (F2). Dies

stelle jedoch nicht das Problem dar, sondern die fehlende Erfahrung, das nach SABSA bzw. der erweiterten Methodik modellierte ISMS erfolgreich zertifizieren zu lassen (B3).

Für eine Zertifizierung nach ISO/IEC 27001 auf Basis von IT-Grundschutz wird das ISMS nach den Bausteinen im IT-Grundschutz Kompendium auditiert. Hierzu wurde im Rahmen dieser Arbeit ein Mapping der R1-Bausteine zu SABSA durchgeführt und die ein Security Service Catalogue als auch Security Mechanism Catalogue aufgestellt. Somit wäre eine Zertifizierung der Architektur nach ISO/IEC 27001 auf Basis des IT-Grundschutzes möglich. Das Mapping kann dem Anhang A.2 ‚Mapping der R1 Bausteine zu SABSA Metaebenen‘ entnommen werden.

Die Ergebnisse der durchgeführten Analyse zeigen, dass die erweiterte IT-Grundschutz-Methodik das Potenzial birgt, die Qualität der Arbeit in der Informationssicherheit zu verbessern. Dennoch sind die Adaption und die Akzeptanz schwierig. Die vorwiegend extrinsische Motivation zur Etablierung der Informationssicherheit stellt den Einsatz der erweiterten Methodik infrage, da die Umstellung von einem auditzentrierten zu einem architekturzentrierten Vorgehen erfolgen würde. Diese Veränderung könnte Unsicherheiten und anfängliche Mehraufwände nach sich ziehen, die als negative Einflussfaktoren wirken und die Einführung verhindern oder aufgrund mangelnder Unterstützung der Abteilungen sowie des Managements während der Umsetzung stoppen könnten. Daher ist die Adaption der erweiterten IT-Grundschutz-Methodik ein wesentlicher Aspekt, um einen Anwendungserfolg zu erzielen. Dies wird durch die Beziehungen zwischen der Adaption und den anderen Kategorien in Abbildung 25 verdeutlicht.

Die Adaption beinhaltet die umfassende und gezielte Anpassung der erweiterten Methodik an den bestehenden Bedarf der Organisation. Dabei sollten die informellen, die formellen und die wertschöpfenden Strukturen sowie die Kultur einer Organisation berücksichtigt werden. Die Anpassung erfordert eine Analyse der internen Dynamiken sowie eine Abstimmung der erweiterten Methodik mit den spezifischen internen und regulatorischen Anforderungen der Organisation. Eine Adaption liegt außerhalb der Forschungsfrage, wäre jedoch für zukünftige Forschungen von Interesse.

5. DESIGN UND ENTWICKLUNG

In diesem Kapitel erfolgt eine Beschreibung der erweiterten IT-Grundschutz-Methodik sowie eine Erörterung der damit einhergehenden Anpassungen.

5.1. ERWEITERTE IT-GRUNDSCHUTZ-METHODIK

Die erweiterte IT-Grundschutz-Methodik basiert auf der IT-Grundschutz-Methodik gemäß dem BSI-Standard 200-2 (vgl. BSI 2017a) sowie den Änderungen an SABSA von 2018 (vgl. Sherwood et al. 2018). Das Mapping der Bausteine auf den SABSA-Layer sowie der erste Entwurf des Security Service Catalogue und Security Mechanism Catalogue beruhen auf dem IT-Grundschutz-Kompendium 2023 (vgl. BSI 2023b). In den folgenden Unterkapiteln wird der Aufbau der Methodik durch die Erweiterung beschrieben, zudem werden praktische Umsetzungsmöglichkeiten aufgezeigt und die Probleme erörtert.

5.1.1. AUFBAU DER ERWEITERTEN METHODIK

Zur besseren Verständlichkeit wurden bestehende Prozesse und Formulierungen weitgehend beibehalten. In Abbildung 10 ist die erweiterte Methodik mit ihren verschiedenen Abläufen visualisiert.

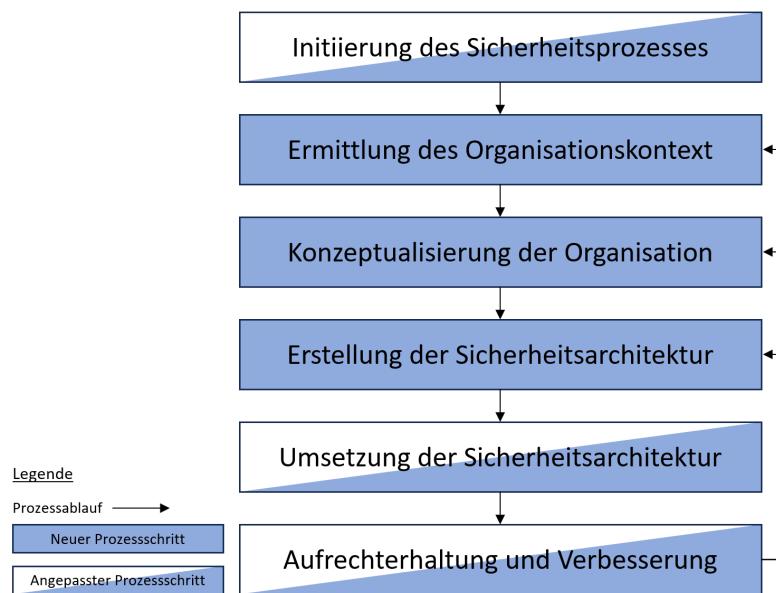


Abbildung 10: Phasen des Sicherheitsprozesses der erweiterten Methodik
Quelle: Eigene Darstellung

Im Vergleich zum Sicherheitsprozess gemäß BSI-Standard 200-2, siehe Abbildung 1, wurden die Prozesse ‚Erstellung der Leitlinie zur Informationssicherheit‘, ‚Organisation des Sicherheitsprozesses‘ und ‚Erstellung einer Sicherheitskonzeption‘ in

die neuen eingearbeitet bzw. finden sie sich durch die Arbeitsweise in SABSA in den verschiedenen Layern wieder. Die Initiierung des Sicherheitsprozesses entspricht der ursprünglichen, jedoch werden zusätzlich die Architecture Governance sowie der Aufbau und die Verantwortlichkeit der Architektur definiert. In Kapitel 5.1.2 wird darauf näher eingegangen.

In der Ermittlung des Organisationskontextes wird die Organisation als solche aufgenommen, zudem ihre Unternehmung, Umwelt und Risikolandschaft. Dies kann Kapitel 5.3 entnommen werden.

Für die genauere Betrachtung der Organisation findet auf Basis des ermittelten Organisationskontextes die Konzeptualisierung der Organisation statt. In dieser ist die Aufbau- sowie Ablauforganisation ganzheitlich dargestellt. Zudem wird ein Rahmenwerk definiert, in dem die Organisation agieren soll, siehe Kapitel 5.4.

Anhand der Konzeptualisierung wird die Sicherheitsarchitektur erstellt, die in Kapitel 5.5 behandelt wird. Die in Kapitel 5.6 beschriebene Umsetzung der Sicherheitsarchitektur gleicht der ursprünglichen Phase. Zur kontinuierlichen Verbesserung und Aufrechterhaltung der Architektur wird in Kapitel 5.7 ein mögliches Vorgehen aufgezeigt.

Durch die Kombination von SABSA und IT-Grundschutz werden die Konzeption und die Etablierung der Informationssicherheit von Ende zu Ende ermöglicht. Während in SABSA die sicherheitsspezifischen Anforderungen der Organisation ermittelt werden und die Architektur aufgestellt wird, bietet der IT-Grundschutz Angaben zu den operativen Sicherheitsmaßnahmen, weshalb sich beide ergänzen. Diese Symbiose wird in Abbildung 11 visualisiert. Die spezifischen Arbeitsprodukte der einzelnen Prozesse können Anhang A.3 ‚Arbeitsprodukte‘ entnommen werden.

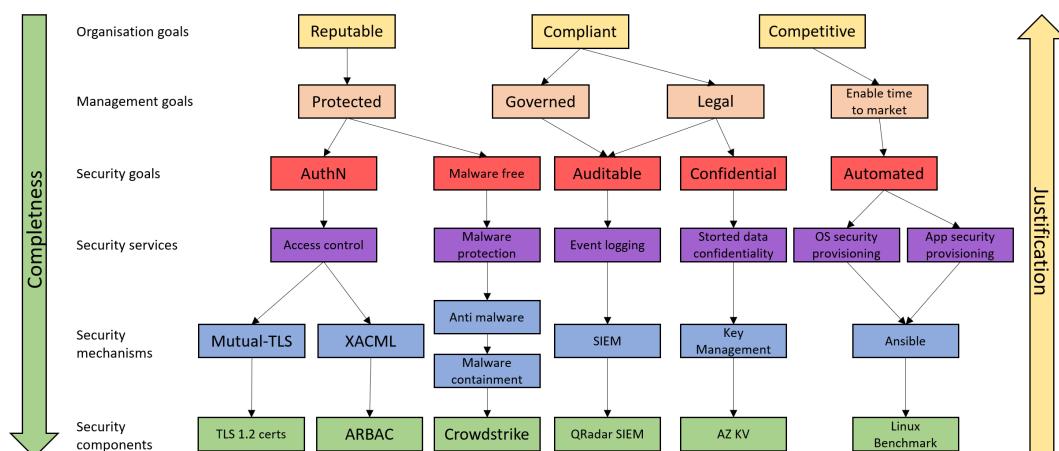


Abbildung 11: Abstraktionsebenen in SABSA

Quelle: In Anlehnung an (Platt 2021)

5.1.2. LEBENSZYKLUS

Die Ausgestaltung des Lebenszyklus der erweiterten IT-Grundschutz-Methodik basiert auf dem SABSA-Lifecycle (vgl. Sherwood 2005: 113), der eine Eigenentwicklung des SABSA-Frameworks ist und auf dem PDCA-Zyklus sowie dem ITIL-3-Lebenszyklus gründet (vgl. Sherwood et al. 2009: 5). Der Zyklus umfasst vier Phasen. Eine kontinuierliche Feedbackschleife gewährleistet, dass in jeder Phase Verbesserungspotenziale identifiziert und integriert werden. Der Lebenszyklus ist in Abbildung 12 grafisch dargestellt.

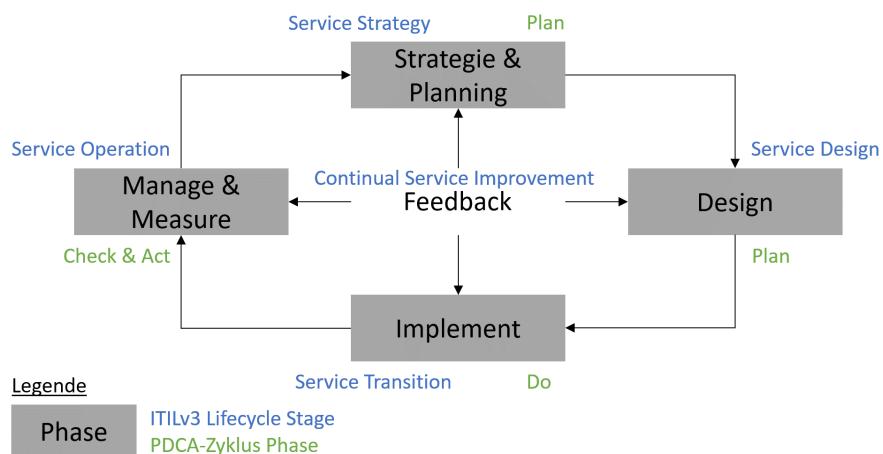


Abbildung 12: Lebenszyklus des erweiterten IT-Grundschutzes
Quelle: In Anlehnung an (Sherwood 2005: 113)

Die einzelnen Phasen dienen der Definition des Ablaufs der durchzuführenden Sicherheitsprozesse innerhalb der erweiterten Methodik:

- Strategie und Planning: Ermittlung des Organisationskontextes (siehe Kapitel 5.3) und Konzeptualisierung der Organisation (siehe Kapitel 5.4),
- Design: Erstellung der Sicherheitsarchitektur von der logischen Ebene bis zur Komponentenebene (siehe Kapitel 5.5),
- Implement: Implementierung der Sicherheitsmaßnahmen (siehe Kapitel 5.6) und
- Manage and Measure: Die Verwaltung der Sicherheitsmaßnahmen und Durchführung von Messungen zur Ermittlung der Business Attribute Werten.

Im Rahmen des Feedbacks erfolgen die Ausarbeitung und die Implementierung kontinuierlicher Verbesserungsmaßnahmen auf Basis von Kennzahlen, Risikoidikatoren, Maßnahmenindikatoren sowie Rückmeldungen gemäß Kapitel 5.7. Der Lebenszyklus ist aufgrund dieser Strukturierung prozessorientiert und bedient sich

nicht der agilen Elemente, die durch die Nutzung des Lean-Ansatzes und die agilen Praktiken implementiert werden könnten, wie es nach ITIL 4 möglich wäre (vgl. Axelos 2020: 227).

5.1.3. LIMITATIONEN DER ERWEITERTEN METHODIK

Infolge der geringen Verbreitung der ESA wurden bis zum 10. August 2024 zwei Softwarelösungen identifiziert, die sich für die Modellierung der Sicherheitsarchitektur eignen. Die erste Lösung ist die Erweiterung *SABSA Security Architecture Extension* (vgl. Cephas Consulting 2018), die als Add-on für *Enterprise Architect* verfügbar ist (vgl. Sparx Systems 2023). Die zweite Lösung ist *Qnous* und implementiert SABSA nativ (vgl. Qiomas Nous 2024). Sie hat den Nachteil, dass die aufgestellte ESA nicht nativ in die EA integriert werden kann, weshalb Zwischenlösungen nötig wären. Ein alternativer Ansatz zur Modellierung der Architektur ist *ArchiMate 3.1* (vgl. The SABSA Institute 2021). Dieser basiert allerdings auf Überladungen und eigenen Notationen, da in *ArchiMate 3.1* der Sicherheitsaspekt nicht nativ betrachtet wird (vgl. The Open Group 2019). Dies bestärkt zudem die Aussage, dass die Sicherheit durch EA unberücksichtigt bleibt, wie in den Kapiteln 1.4 und 4.2 dargelegt wurde.

Eine weitere Einschränkung stellt die geringe Größe der SABSA-Community sowie deren geringe Aktivität dar. Eine Analyse des offiziellen Forums des SABSA Instituts ergab (vgl. The SABSA Institute o. D.) bis zum 10. August 2024 insgesamt 167 Beiträge – einer davon wurde im Jahr 2024 vom Autor dieser Arbeit verfasst. Die Verteilung aller Nachrichten im Forum über den gesamten Zeitraum ist in Abbildung 13 visualisiert.

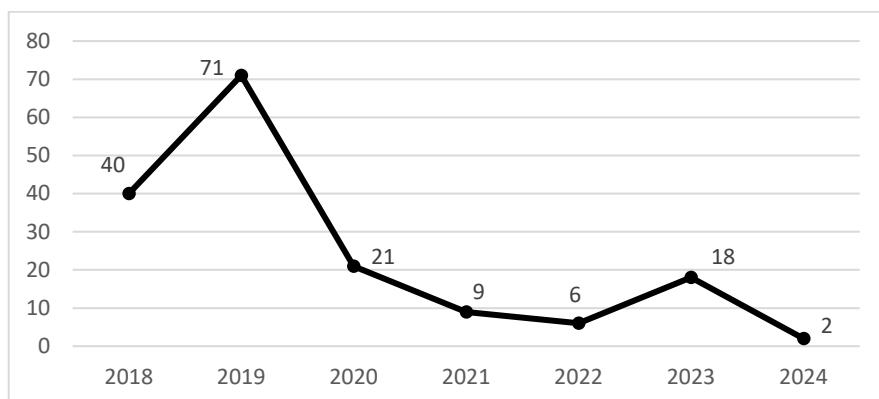


Abbildung 13: Beiträge im Forum im Zeitraum
Quelle: Eigene Darstellung

Des Weiteren liegen keine publizierten SABSA-Case-Studies vor, was den Einstieg und das Verständnis der Thematik erschwert. Eine Ursache hierfür könnte

die berufliche Position der Mitglieder sein, die den Umgang mit sensiblen Informationen erfordert und deren Veröffentlichung verhindert. Darüber hinaus könnte es auch auf die knappen zeitlichen Ressourcen der Mitglieder zurückzuführen sein.

5.2. INITIIERUNG DES SICHERHEITSPROZESSES

Der Sicherheitsprozess wird durch die Organisationsleitung initiiert. Letztere definiert – sofern noch nicht geschehen – die Verantwortlichkeit für die Informations-sicherheit, indem sie einen CISO einsetzt (vgl. BSI 2017a: 20). Wurde kein Geltungsbereich bestimmt, kann die Organisationsleitung diesen in Zusammenarbeit mit dem CISO für die Informationssicherheit in der Organisation festlegen. Des Weiteren kann die Auswirkung auf Gruppen eruiert werden, die am meisten betroffen sind, die den größten Nutzen ziehen und deren Fähigkeiten sich ändern werden, obwohl sie nicht direkt tangiert sind. Zudem sind die Governance-Strukturen zu identifizieren, da diese innerhalb der Architektur berücksichtigt werden sollten und ggf. angepasst werden müssten. Die ermittelten Auswirkungen sollten mit der Organisationsleitung abgestimmt und vereinbart werden.

Vor der weiteren Vorbereitung und Ausgestaltung könnte der CISO mit der Organisationsleitung über die zwei Etablierungsmöglichkeiten der ESA in der Organisation entscheiden. Die erste ist die vollständige Implementierung der Architektur in den gesamten definierten Geltungsbereich. Ein Nachteil dieses Vorgehens ist, dass erste Arbeitsergebnisse später fertiggestellt werden, während die Akzeptanz der Stakeholder:innen sinkt. Dadurch entstehen Konflikte innerhalb der Organisation, sodass Kompromisse auf Kosten der Effektivität der ESA eingegangen werden oder das gesamte ESA-Vorhaben abgebrochen wird (vgl. Kapitel 4.2). Eine Alternative, um dies zu verhindern, ist die zweite Möglichkeit, d. h. eine Pilotierung mit dem Fokus, einen spezifischen Teilbereich der Organisation zu bearbeiten. Ziel der Pilotierung ist, die Möglichkeiten der ESA in der Organisation aufzuzeigen, die spezifischen Vorteile für die Organisation hervorzuheben und die Akzeptanz sowie das Commitment der Stakeholder:innen für die neue Arbeitsweise zu steigern.

Das SABSA-Framework präsentiert in diesem Kontext das Konzept des ‚Fast Track Workshops‘. In diesem fünftägigen Workshop soll SABSA in Zusammenarbeit mit Schlüsselstakeholder:innen für einen Teilbereich der Organisation etabliert werden (vgl. Sherwood 2005: 152–155). Auf Basis der vorliegenden Ergebnisse könnte die Organisation das ESA-Vorgehen auf weitere Bereiche des Geltungsbereichs ausdehnen, sofern die notwendige Akzeptanz und das Commitment der Organisationsleitung gewährleistet sind.

Je nach Geltungsbereich und Vorgehen werden die bestehenden Möglichkeiten der Organisation identifiziert. Dabei werden in einem Assessment Gaps und die Interessen der Stakeholder:innen ermittelt. Die Ergebnisse werden als Basis genutzt, um den Änderungsbedarf, die Limitationen der ESA sowie das benötigte Budget und Personal zu bestimmen. Aufbauend auf den Rahmenbedingungen wird die Informationssicherheitsorganisation gebildet oder angepasst, falls Strukturen zur Informationssicherheit existieren. Der CISO definiert mit der Organisationsleitung und anderen leitenden Personen die Platzierung des ESA-Themas unter Berücksichtigung vorhandener Strukturen.

Die zwei Möglichkeiten der Eingliederung sind in Abbildung 14 visualisiert. Bei einer Pilotierung könnte das Team mit der Verantwortung für ESA temporär gebildet werden und im Verlauf in ein permanentes umgewandelt werden. In der ersten Möglichkeit könnte ein eigenes ESA-Team unter der Verantwortung des CISO gegründet werden, das, falls vorhanden, mit dem ISMS- und dem EA-Team arbeitet. In Abhängigkeit der existierenden Strukturen agiert das ESA-Team nach den Vorgaben des ISMS-Teams oder entwickelt diese selbst.

Die zweite Möglichkeit ist die Eingliederung der ESA ins EA-Team unter der Verantwortung des CIO in Kooperation mit dem CISO, das, falls vorhanden, mit dem ISMS-Team arbeitet. Ausgestaltungen der Informationssicherheitsorganisation werden im BSI-Standard 200-2 beschrieben (vgl. BSI 2017a: 36–50). Eine Ausformung der Harmonisierung der Positionen und Verantwortlichkeiten kann Anhang A.1 „Möglicher Aufbau der Organisationsstruktur“ entnommen werden.

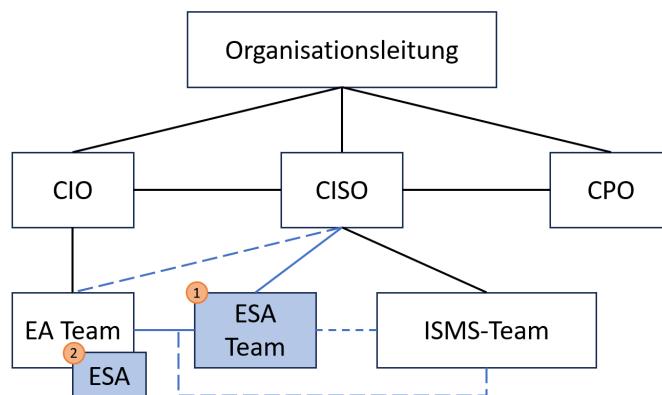


Abbildung 14: Mögliche organisatorische Ausgestaltung
Quelle: Eigene Darstellung

Die dokumentierten Ergebnisse werden mit der Organisationsleitung abgestimmt und im organisatorischen Modell für ESA zusammengefasst. Zudem könnte eine

Stakeholder:innen-Analyse durchgeführt und ein Kommunikationsplan erstellt werden, um die Etablierung der ESA zielgerichtet durchzuführen. Der Prozessschritt könnte durch die Definition der Architecture Governance abgeschlossen werden.

5.3. ERMITTlung DES KONTEXTES DER ORGANISATION

Nach Abschluss der Initiierung wird der organisatorische Kontext ermittelt, indem Informationen über die Organisation gesammelt werden, z. B. Strategien, Treiber, Ziele, Erfolgsfaktoren, Aufbau- und Ablauforganisation, Budgets, vorhandene Managementsysteme, Strukturen, technische Probleme und spezifische Limitationen. Informationsquellen können bestehende Strategiedokumente, Businesspläne, unternehmerische Prinzipien, Prozessdokumente und relevante Stakeholder:innen sein. Zudem werden die finanziellen Aspekte der Organisation identifiziert sowie die Geschäftsbeziehungen zu internen und externen Entitäten erfasst. Auf Basis der gesammelten Informationen entsteht eine Kontextbeschreibung der Organisation. Die gesammelten Informationen könnten wie folgt festgehalten werden:

- Die Motivationen hinter Geschäftsplänen und Entscheidungen können anhand des Business-Motivation-Modells dokumentiert werden (vgl. OMG 2015a).
- Die Struktur der Ablauforganisation könnte mittels des Business Process Model dargestellt werden (vgl. OMG 2014).
- Die Beziehungen zwischen der Organisation und internen sowie externen Organisationen könnten durch das Entity-Relationship-Modell abgebildet werden (vgl. Chen 1976).
- Die interne Aufbauorganisation könnte in Form eines Organigramms festhalten werden.

Die Wahl der zu nutzenden Informationen sowie die bestehenden strategischen und taktischen Pläne haben Auswirkungen auf die Zukunftsfähigkeit der Architektur, aufgrund ihres Detailierungsgrades des Planungsumfangs. Diese Informationen lassen sich in die sechs Kategorien ‚Business Anforderungen‘, ‚Business Prozesse‘, ‚spezifischer Business Bedarf‘, ‚Business Capabilities‘, ‚Business Strategie‘ und ‚Operating Model‘ einteilen, siehe Abbildung 15. Während der Planungszeitraum steigt, sinkt die Detailgenauigkeit, sodass die Anforderungen eine zunehmende Unschärfe aufweisen. Informationen mit einem geringen Planungszeitraum und hoher Detailgenauigkeit haben wenig Unschärfe, jedoch keine Aussagekraft zu zukünftigen Planungen.

Eine Architektur die auf Grundlage der Businessanforderungen modelliert wird, kann über den Zeitverlauf zu starr werden, sodass eine regelmäßige, vollständige Erneuerung der Architektur erforderlich wird. Im Gegensatz dazu wäre eine Architektur, die auf einer Strategie basiert, zu ungenau und könnte nicht alle Anforderungen der Gegenwart vollständig erfüllen.

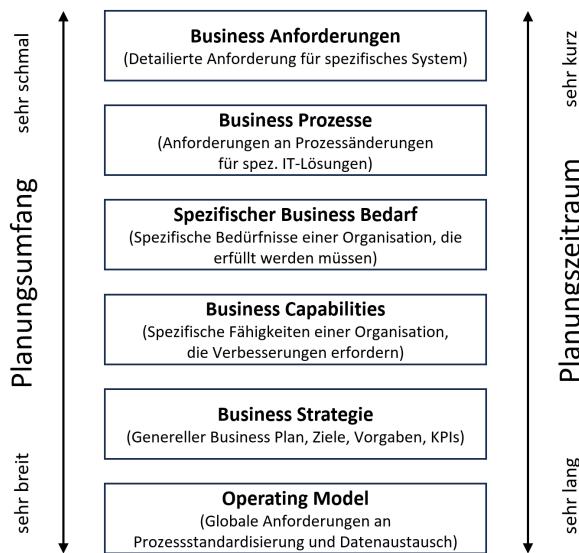


Abbildung 15: Kategorien der Anforderungen
Quelle: In Anlehnung an (Kotusev 2021: 89)

Laut Erfahrungsberichten in der EA sind auf Basis von Organisationsstrategien modellierte Architekturen nicht wiederverwendbar (vgl. Weill/Ross 2009: 1–20; Ross et al. 2006: 17–24). Grund ist, dass in diesen Strategien der Lebenszyklus von organisatorischen und technischen Systemen mitbedacht ist und somit spezifische, nicht wiederverwendbare Lösungen benötigt werden. Zudem könnte die Informationssicherheit ein ähnliches Problem wie die IT aufweisen, indem sie aufgrund der Fokussierung auf die aktuelle Strategie zu einem Flaschenhals der Strategie wird, statt diese zu unterstützen (vgl. Ross 2005: 1).

Diese Fokussierung führt zudem in eine Ausrichtungsfalle. Das heißt, verschiedene Initiativen behandeln unabhängig voneinander spezifische Bedürfnisse der Organisation, generieren jedoch aufgrund der fehlenden holistischen Sicht keinen Mehrwert für die gesamte Organisation (vgl. Shpilberg et al. 2007). Des Weiteren werden die Systeme aus den Initiativen zu einer Belastung. Die IT-Systeme haben eine durchschnittliche Nutzungszeit von 15 Jahren, Strategien von etwa vier Jahren, dadurch überdauern Systeme mehrere Strategien, sodass die Ausrichtung der Systeme an Strategien nicht sinnvoll wäre (vgl. Wierda 2017: 140–141). Eine Alternative als Informationsbasis kann das Operating Model darstellen.

Ein Operating Model umfasst die Dimensionen Standardisierung von Geschäftsprozessen und Integration, welche die Bereitstellung von Gütern und Dienstleistungen für Kund:innen gewährleisten. Es beschreibt, wie ein Unternehmen wachsen will. Da das Operating Model eine stabilere und umsetzbarere Vision des Unternehmens bietet als die Strategie, treibt es die Entwicklung der Grundlage für die Umsetzung voran. Die Entscheidung für ein Operating Model wirkt sich darauf aus, wie ein Unternehmen seine Geschäftsprozesse und IT-Infrastrukturen implementiert. Ein Unternehmen ohne klares Operating Model kann keine automatisierten, bereits vorhandenen und kostengünstigen Fähigkeiten in ein neues strategisches Projekt einbringen, sondern muss bei jeder neuen strategischen Initiative seine Kernkompetenzen identifizieren.

Die Standardisierung der Geschäftsprozesse und der zugehörigen Systeme bedeutet, dass festgelegt wird, wie ein Prozess auszuführen ist. Sie sorgt für Effizienz und Berechenbarkeit im gesamten Unternehmen. Integration verbindet die Anstrengungen der Organisationseinheiten durch geteilte Daten. Diese gemeinsame Datennutzung kann zwischen Prozessen erfolgen, um eine durchgängige Transaktionsverarbeitung zu ermöglichen, oder prozessübergreifend, um dem Unternehmen ein einheitliches Auftreten gegenüber Kund:innen zu ermöglichen. Zu den Vorteilen der Integration gehören erhöhte Effizienz, Koordination, Transparenz und Flexibilität. Ein integrierter Ansatz von Geschäftsprozessen kann den Service für Kund:innen verbessern, dem Management Informationen für die Entscheidungsfindung liefern und es ermöglichen, dass Änderungen in einem Teil des Unternehmens notwendige Maßnahmen in anderen Teilen aufzeigen. Integration kann auch den gesamten Informations- und Transaktionsfluss im Unternehmen beschleunigen (vgl. Ross et al. 2006: 45–48).

Abhängig vom Geltungsbereich und von der Implementierungsart kann bei der Nutzung von Informationen zwischen verschiedenen Informationskategorien unterschieden werden. Eine Entscheidungsgrundlage hierfür kann in Abbildung 16 entnommen werden.

Die gesammelten Informationen werden benötigt, um die Business Driver der Organisation aufzunehmen. Aufgrund möglicher widersprüchlicher Anforderungen könnten Konflikte innerhalb der Informationen identifiziert werden, die in Absprache mit der Organisationsleitung geglättet werden. Dies kann durch die Behebung der Konflikte oder die Priorisierung mittels Risikoanalyse geschehen. Für jeden Business Driver werden die Business Driver for Security abgeleitet.

Letztere repräsentieren eine abgeleitete Abstraktion einer Sicherheitsanforderung eines Business Drivers. Die Business Driver for Security wird in Businesssprache formuliert, damit die Organisationsleitung und andere leitende Personen die Sicherheitsanforderung verstehen. Business Driver können mehrere Business Driver for Security haben, weshalb es sich um eine 1:n-Beziehung handelt. Sie enthalten einen Namen und eine Beschreibung.

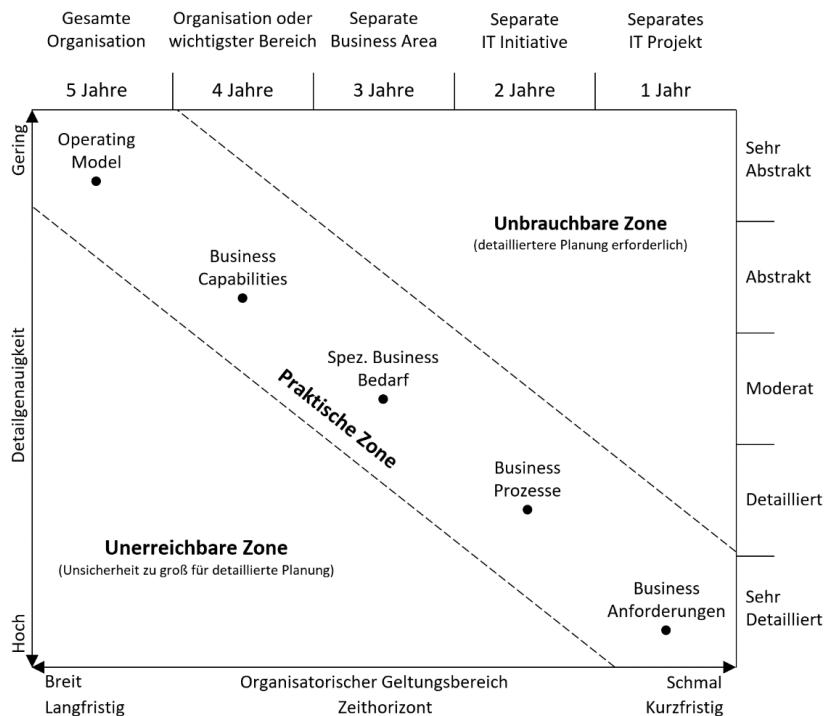


Abbildung 16: Wahl der Informationskategorie
Quelle: In Anlehnung an (Kotusev 2021: 91)

Nachdem die Business Driver for Security aufgenommen wurden, wird ein Organisations- und Beziehungsdiagramm erstellt. Es enthält alle im Geltungsbereich betroffenen Organisationen und ihr jeweiliges Beziehungsmodell. Die Business Driver for Security sowie das Organisations- und Beziehungsmodell werden mit der Organisationsleitung abgestimmt und von ihr abgenommen.

Abschließend werden anhand eines Businessrisikomodells die Risiken und die Chancen basierend auf den Assets, Auswirkungen und bestehenden Bedrohungen analysiert. In SABSA wird die eigenentwickelte Methode ‚SABSA Risk Assessment‘ genutzt. Dabei werden die Risiken mit einem auswirkungsorientierten Ansatz identifiziert und qualitativ bewertet (vgl. Sherwood 2005: 205–209). Der vorgestellte Ansatz unterscheidet sich vom BSI-Standard 200-3 zum Risikomanagement, bei dem Risiken nach einem bedrohungsorientierten Ansatz ermittelt werden.

(vgl. BSI 2017b). Der Vorteil des auswirkungsorientierten Ansatzes ist, dass Risiken nicht nur für Assets, sondern auch für die Businessziele erhoben werden können. Somit wird die Priorisierung für den Umgang mit Risiken vereinfacht.

Eine weitere Unterscheidung im Risikomanagement zwischen SABSA und dem IT-Grundschutz ist, dass es in SABSA ohne Vorbedingungen durchgeführt wird, während in der IT-Grundschutz-Methodik eine Risikoanalyse explizit erfolgen muss, wenn: (1) ein hoher oder sehr hoher Schutzbedarf in mindestens einem der Schutzziele ermittelt wird, (2) ein Zielobjekt nicht mit den vorhandenen Bausteinen hinreichend modelliert werden kann oder (3) ein Zielobjekt in einem Einsatzszenario betrieben wird, das im Rahmen des IT-Grundschutzes nicht vorgesehen ist (vgl. BSI 2017a: 153). Dies ist möglich, da die Bewertung der Gefährdungen in den Bausteinen bereits vorgenommen wurde (vgl. BSI 2017a: 152–153).

Zudem differenzieren sich SABSA und der IT-Grundschutz beim Zeitpunkt der Durchführung einer Risikoanalyse. Letztere wird in SABSA zu Beginn in der Kontextermittlung durchgeführt, um die Informationen zur organisatorischen Gestaltung und die Anforderungen durch das Risikoumfeld zu ergänzen. Sie werden als Grundlage genutzt, um die Kritikalität der jeweiligen Aspekte der Organisation zu priorisieren (vgl. Sherwood 2005: 453). Bei der IT-Grundschutz-Methodik erfolgt eine Risikoanalyse, nachdem eine Richtlinie bzw. Leitlinie verfasst, die ISMS-Organisation aufgestellt und eine IST-Analyse durchgeführt wurde. Dadurch wird das Risikoumfeld der Organisation auf der strategischen Ebene nicht berücksichtigt (vgl. BSI 2017a: 76).

Um das Businessrisikomodell zu erstellen und die Vorgaben des IT-Grundschutzes einzuhalten, könnte eine Business-Impact-Analyse gemäß des BSI-Standards 200-4 durchgeführt werden (vgl. BSI 2023a: 158–193). Diese kann mit der BCM-Risikoanalyse kombiniert werden (vgl. BSI 2023a: 199–214), die den BSI-Standard 200-3 nutzt (vgl. BSI 2017b). Durch die Business-Impact-Analyse wird die Kritikalität der Prozesse identifiziert und die Performancevorgaben der Organisation werden ermittelt, weshalb die Auswirkungen eines Prozessausfalls aufgenommen werden. Diese werden durch die Risikoanalyse nach dem BSI Standard 200-3 ergänzt, mit der die möglichen Ursachen ermittelt werden können. Trotz des bedrohungsoorientierten Ansatzes nach dem BSI-Vorgehen wird die Auswirkung ermittelt. Diese Kombination steht im Einklang mit SABSA und der Anforderung ans Artefakt, die Vorgaben für ein Audit einzuhalten. Bei einem Audit könnte das Ergebnis der Risikoanalyse gemäß dem BSI-Standard aufgezeigt werden.

5.4. KONZEPTUALISIERUNG DER ORGANISATION

Die Ergebnisse zur Ermittlung des Kontextes der Organisation werden durch die Organisationsleitung aus deren Perspektive erstellt. Erstere werden durch Architekt:innen genutzt, um eine Konzeptualisierung zu erstellen und die Organisation zu modellieren. Die Arbeitsprodukte lassen sich gemäß den EA-Artefakten ‚Vision‘ und ‚Consideration‘ nach dem CSVLOD-Modell klassifizieren. Zu Beginn werden die Business Driver for Security herangezogen sowie die Business Attributes definiert. Ein Business Driver for Security kann mehrere Business Attributes enthalten und ein Business Attribute mehreren Business Drivern zugewiesen werden, so dass es sich um eine n:m-Beziehung handelt (vgl. Sherwood et al. 2009: 89).

Business Attributes sind eine konzeptionelle Abstraktion einer Anforderung und erlauben ihre Messbarkeit. Zudem wird die Kommunikation mit der Organisationsleitung vereinfacht, da die Business Attribute je nach Metaebene in einer zielgruppengerechten Sprache eine datenbasierte Faktenlage bietet (vgl. ebd.: 89). Innerhalb eines Business Attributes wird die Metrik zur Messbarkeit einer Anforderung definiert. Für die Erhebung der Metriken können qualitative oder quantitative Methoden herangezogen werden, jedoch gibt es spezifische Anforderungen: Die verwendeten Daten müssen zur Verfügung stehen, die Erhebung sowie die mögliche Berechnung müssen unabhängig von Interessen durchgeführt werden und die Messung muss wiederholbar sein. Neben der Aufstellung der Metrik und ihrer Erhebung werden die Performanceziele unter Berücksichtigung der Performancevorgaben der Organisation bestimmt. Die Performancevorgaben definieren, die erwarteten Mindest- und Maximalwerte. Innerhalb des SABSA-Frameworks existieren vordefinierte Business Attributes (vgl. ebd.: 20–21), die nach eigenem Bedarf oder mit eigenen Attributen erweitert werden können.

Die Summe aller definierten Business Attributes in der Konzeptualisierung wird in einem Business Attribute Profile zusammengefasst. Letzteres ist eine konzeptionelle Repräsentation der Organisation, gemappt über die Business Attributes zur Messung der Performance für die Einhaltung der Anforderungen (vgl. ebd.: 218). Dadurch wird ein datengetriebenes Arbeiten ermöglicht, indem Entscheidungen auf Basis gesammelter Informationen getroffen werden können.

Nachdem die Methode der Messung für die Einhaltung der Anforderungen an die Organisation definiert wurde, werden die Control Objectives bestimmt. Ein Control Objective ist eine Aussage über ein gewünschtes Ergebnis oder einen Zweck, der durch die Implementierung von Kontrollen innerhalb einer bestimmten Geschäftstätigkeit erreicht werden soll (vgl. ebd.: 219). Sie werden durch die in den ISMS-

Dokumenten festgelegten Rahmenbedingungen implementiert. Ihr Einsatz könnte aus einer bestimmten Anforderung an die Organisation stammen oder eine Good Practice sein (vgl. ebd.: 219). Innerhalb der Control Objectives können Sicherheitsthemen und -vorgaben von verschiedenen Standards wie ISO/IEC 27001:2022 (vgl. ISO 2022a), NIST SP 800-53 (vgl. NIST 2020), COBIT 2019 (vgl. Isaca 2018) und IT-Grundschutz-Kompendium (vgl. BSI 2023b) normalisiert und in eine einheitliche Terminologie der Organisation übersetzt werden.

Im Rahmen dieser Master-Thesis wurde ein erster Entwurfsansatz der Bausteine des IT-Grundschutz-Kompendiums 2023 (vgl. BSI 2023b) für die Control Objectives und die Control Library durchgeführt, der in Anhang A.2 „Mapping der R1-Bausteine zu SABSA-Metaebenen“ entnommen werden kann. Die Control Library wird in diesem Kapitel erklärt.

Es wurden ausschließlich Bausteine mit der Umsetzungsreihenfolge R1 herangezogen, da für die nächste Version des Kompendiums die gesamten Bausteine und ihre Sicherheitsanforderungen überarbeitet werden (vgl. Schmidt 2023). Bausteine mit einer Zuordnung der Umsetzungsreihenfolge R1 sollten vorrangig realisiert werden (vgl. BSI 2017a: 137). Sie sind universell und essenziell für jede Organisation und können als Beispiel für die mögliche Einhaltung der BSI-Vorgaben genutzt werden. Der Entwurfsansatz besteht aus einem Mapping der Ziele und der Sicherheitsanforderungen von R1-Bausteinen zwischen SABSA und dem Kompendium. Das Mapping basiert auf einer inhaltlichen Analyse, in der die Sätze nach ihrem Inhalt interpretiert und der jeweiligen SABSA-Metaebene zugewiesen werden. Zudem wurden die spezifischen Sicherheitsmaßnahmen der jeweiligen Anforderung extrahiert und mitgelistet, um die Erstellung der Sicherheitskataloge zu vereinfachen. Die Nutzung und die Erklärung der Sicherheitskataloge werden in Kapitel 5.5 behandelt.

Die Modellierung der Architektur könnte durch ein Mapping der Sicherheitsmaßnahmen an die Business Attributes vereinfacht werden, wodurch zudem eine Automatisierung der Auswahl von Sicherheitsmaßnahmen möglich wäre. Des Weiteren kann ein solches Mapping zu einer Annäherung der vergleichbaren Ergebnisse führen, da bei der Wahl von Attributen dieselben Sicherheitsmaßnahmen genutzt werden. Ähnlich wie das Mapping der Sicherheitsmaßnahmen an STRIDE bei Peterson (vgl. 2010) könnten die normalisierten Control Objectives an die elementaren Gefährdungen im IT-Grundschutz-Kompendium in eine Beziehung gestellt werden. Das BSI hat hierfür eine Kreuzreferenztabelle geschaffen (vgl. BSI 2023c), um die Sicherheitsanforderungen der Bausteine in Beziehung zu den elementaren Gefährdungen zu stellen und das Risikomanagement zu vereinfachen.

Die Control Objectives konzeptualisieren das Businessrisikomodell und dienen als Schnittstelle zwischen der Contextual und der Conceptual Metaebene (vgl. Sherwood et al. 2009: 219). Somit können die Risiken der Organisation über alle Metaebenen hinweg betrachtet und behandelt werden.

Zur Bestimmung der Verantwortlichkeiten für den Umgang mit den definierten Organisationsrisiken müssen zunächst die Vertrauensbeziehungen und ihre Anforderungen im Organisationsumfeld ermittelt werden (vgl. ebd.: 255). Die Vertrauensmodellierung unterstützt bei der Bestimmung, welche Entitäten welches Vertrauen bedingen, welche Werte geschützt werden müssen, welches Maß an Vertrauen notwendig ist und unter welchen Bedingungen Vertrauen gewährt oder entzogen wird. In diesem Rahmen werden die Interaktionen zwischen den Entitäten aufgestellt und analysiert. Es lassen sich drei Beziehungskategorien unterscheiden:

- Unilateral: Eine Entität verteilt Information, andere Entitäten können diese empfangen.
- Bilateral: Zwei Entitäten agieren und tauschen Informationen im Rahmen ihres Vertrages aus.
- Multilateral: Mehrere Entitäten agieren und tauschen Informationen im Rahmen ihres Vertrages und/oder gemeinsamer Regeln aus (vgl. ebd.: 255).

Um das Vertrauen und die damit verbundenen Anforderungen für die bilateralen und multilateralen Beziehungen zu ermitteln, werden diese zunächst in unilaterale Beziehungen dekomponiert und ihre Anforderungen aufgestellt. Eine Visualisierung der Komposition kann Abbildung 17 entnommen werden.

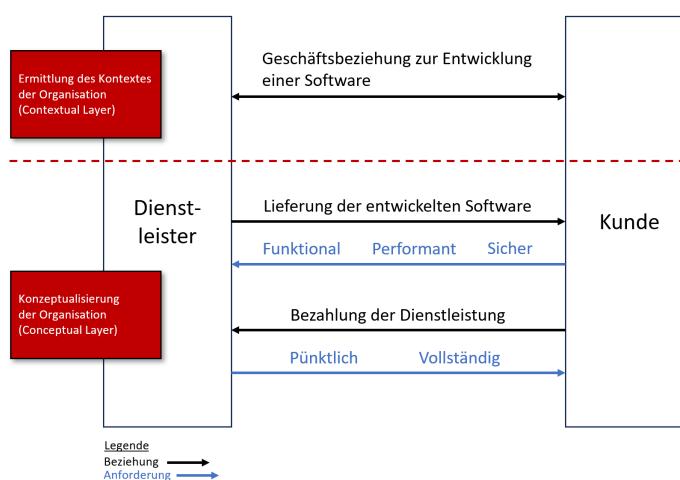


Abbildung 17: Dekomposition einer bilateralen Vertrauensbeziehung
Quelle: Eigene Darstellung

Die Modellierung der Vertrauensbeziehungen zwischen internen Entitäten, darunter fallen die Organisation und ihre weitere Strukturierung wie Abteilung, Team etc., und externen Entitäten, die organisationsfremd sind, erlaubt die Erstellung einer RASCI-Matrix. Diese umfasst die Verantwortlichkeiten der verschiedenen Entitäten. Mittels der klassischen RASCI-Matrix können jedoch nicht die komplexe Beziehungslandschaft und die Verteilung unterschiedlicher Verantwortlichkeiten adäquat abgebildet werden. Das SABSA-Institut entwickelte daher das SABSA Responsibility Assignment Model, das eine Erweiterung der RACI-Matrix darstellt (vgl. Sherwood et al. 2023).

Wenn die Verantwortlichkeiten und Beziehungen zwischen den Entitäten festgestellt sind, können die internen Entitäten mittels eines Managementsystems strukturiert werden. Dabei werden die themenspezifischen Leit- und Richtlinien im Rahmen einer Policyarchitektur durch die jeweils verantwortlichen Entitäten erstellt, die organisationsweit gelten. Die Leit- und Richtlinien enthalten allgemeine Vorgaben für die Verwaltung eines Tätigkeitsbereichs, z. B. HR, Marketing oder Sicherheit.

Das Vorgehen unterscheidet sich im Vergleich zur IT-Grundschutz-Methodik, indem die Risikolandschaft der Organisation in der Konzeption der Leit- und Richtlinien berücksichtigt wird. Die Prozesse im Umgang mit Leit- und Richtlinien ähneln dem Vorgehen nach Ward und Smith (vgl. 2002). Dabei wird nach der Initiierung des Sicherheitsprozesses bzw. des Projekts die Leitlinie entwickelt, genehmigt und über ihre Existenz durch Sensibilisierungskampagnen und die Verbreitung des Dokuments aufgeklärt. Dies steht dem Umgang der erweiterten Methodik entgegen, die einer kombinierten Vorgehensweise nach Rees et al. (vgl. 2003) sowie Flowerday und Tuyikeze (vgl. 2016) entspricht.

Bevor die Leit- und Richtlinien formuliert werden, werden ein Risiko- und ein Policyassessment durchgeführt, um den benötigten Bedarf zu identifizieren. Das Risikoassessment ist in der Konzeptualisierung nicht notwendig, da das Businessrisikomodell genutzt werden kann (vgl. Kapitel 5.3). Das Policyassessment besteht aus einer Evaluierung der Regelungslandschaft, einer Identifizierung von Lücken sowie Widersprüchen und einer Ableitung der Vorgehensweisen (vgl. Rees et al. 2003: 102–103).

Mit den Ergebnissen des Risiko- und Policyassessments werden die Leit- und Richtlinien formuliert, implementiert und überwacht, zudem wird die Einhaltung ihrer Vorgaben verfolgt. Der Vorteil dieses Vorgehens liegt in der bedarfsgerechten

Strukturierung und Formulierung der Vorgaben. Dadurch kann die Informationssicherheit für die Organisation maßgeschneidert werden, sodass nicht nur generelle, unspezifische Risiken abgedeckt werden.

Die Policyarchitektur könnte durch ein Business-Capability-Modell ergänzt werden, das die Business Capabilities der Organisation beschreibt sowie ihre Beziehungen zueinander aufzeigt und hierarchisch strukturiert. Die hochaggregierte Darstellung erleichtert die Kommunikation mit der Organisationsleitung und bildet die Grundlage für die strategische Planung des Capability-Ausbaus sowie für Investitionsstrategien. Der Begriff der Business Capability bezeichnet die Fähigkeit oder Fertigkeit einer Organisation, ihre Kernfunktion zu erfüllen. Letztere umfasst und beschreibt alle Anwendungen, Rollen und Fähigkeiten, die zur Bereitstellung einer Geschäftsfunktion erforderlich sind (vgl. Pouya et al. 2018: 4603).

Die themenspezifischen Motivationen der Informationssicherheit werden durch die Policyarchitektur sowie das Business-Capability-Modell gebildet und stellen die Grundlage für die weitere Ausarbeitung des Business Motivation Models dar. Sie ergänzen die Businesssicht und geben weitere fachliche Einblicke zu den getroffenen Entscheidungen.

Um die Vorgaben der Leit- und Richtlinien in die technischen und organisatorischen Strukturen sowie Abläufe zu integrieren, ist eine Control Library zu erstellen, in der die potenziell nutzbaren Behandlungsmaßnahmen in der Organisation aufgelistet sind. Analog zu den Control Objectives kann eine Harmonisierung der spezifischen Sicherheitsmaßnahmen erfolgen. Das Mapping ermöglicht die Zuordnung der Sicherheitsstandards zu den jeweiligen Maßnahmen, wodurch die Nachweisbarkeit der Einhaltung von Standards vereinfacht wird.

Die Resultate der durchgeführten Tätigkeiten sowie die Ermittlung des Kontextes für die Entwicklung einer Sicherheitsstrategie dienen der systematischen Realisierung des Soll-Zustandes. Die Genehmigung sowie die Vertretung der Sicherheitsstrategie durch die Organisationsleitung sind unabdingbar, um den Projekterfolg sowie die Implementierung der Strategie zu gewährleisten.

Dieser Prozessschritt wird mit der Durchführung einer Gap-Analyse abgeschlossen. Dabei werden der technische und der organisatorische Ist-Zustand ermittelt und mit den definierten Soll-Zuständen aus den Control Objectives verglichen. Auf Basis der ermittelten Daten können weitere Schritte abgeleitet werden, um das definierte Zielbild zu erreichen.

5.5. ERSTELLUNG DER SICHERHEITSARCHITEKTUR

Die Metaebenen ‚logisch‘, ‚physisch‘ und ‚Komponente‘ spezifizieren und operationalisieren die Sicherheitsvorgaben für die Sicherheitsarchitektur der vorherigen Ebene. Dazu werden die Sicherheitsmaßnahmen der Control Library entnommen. Die Ausarbeitungen der Architekturen können mit der Unified Modeling Language (vgl. OMG 2015b) und ArchiMate (vgl. The Open Group 2023) modelliert werden. Die Ergebnisse wirken auf alle Artefakte nach dem CSVLOD-Modell.

5.5.1. LOGISCHE EBENE

Nach der Konzeptualisierung der Organisation wird die erforderliche Sicherheitsfunktionalität auf der logischen Ebene betrachtet. Sie definiert die Anforderungen an die Funktionen, die auf der physischen Ebene umgesetzt werden. Die Informations- und Werteflüsse der Organisation bilden die Grundlage der logischen Ebene, auf der die Maßnahmen gemäß dem Security Service Catalogue definiert werden.

Im Anschluss an die Ergebnisse der Policyarchitektur und unter Berücksichtigung der Informationsarchitektur der Organisation werden im Rahmen der Richtlinien die verschiedenen Themenfelder erörtert, die sich auf spezifische Bereiche oder Funktionen der Organisation beziehen. Diese Richtlinien konkretisieren einen Bereich oder eine Funktion und sind auf eine definierte Zielgruppe ausgerichtet. Basierend auf den internen Vorgaben der Richtlinien können die Security Services angepasst und ergänzt werden.

Das Vertrauensmodell bildet die Basis für die Unterteilung der Entitäten bzw. der Abteilungen innerhalb der Organisation in Sicherheitsdomänen. Letztere sind logische Gruppierungen von Entitäten und Ressourcen, die ähnliche Sicherheitsanforderungen und -kontrollen aufweisen. Sie sind unabhängig und verwalten ihre Risiken durch eigene Richtlinien. Es besteht die Möglichkeit, dass eine Sicherheitsdomäne (Superdomäne) eine oder mehrere Sicherheitsdomänen (Subdomänen) umfasst. Dabei gibt die Superdomäne ihre Anforderungen an die Subdomäne weiter, die diese entweder unverändert übernimmt oder durch eine lokale Anpassung verschärft oder anpasst. Eine Visualisierung erfolgt in Figur A in Abbildung 18.

Der Austausch zwischen Domänen, unabhängig, ob sie verwandt sind oder nicht, erfolgt über kontrollierte Übergänge in einem sicheren Austausch. Der kontrollierte Übergang gewährleistet, dass der Eintritt, der Austritt sowie die Übertragung von Informationen im Einklang mit den eigenen Sicherheitsrichtlinien erfolgen. Die in Abbildung 18 dargestellte Figur B veranschaulicht eine Kommunikation zwischen

zwei nicht verwandten Domänen. Demnach obliegt es jeder Domäne, ihre spezifischen Risiken eigenständig zu verwalten, indem sie ihre Richtlinie durchsetzt, sobald der kontrollierte Übergang erfolgt ist. Im Rahmen des erweiterten Domänenkonzepts ist jedoch eine Ausnahme zu verorten: Einer Domäne ist es möglich, ihre Autorität in den Bereich einer anderen, nicht verwandten Domäne auszudehnen, um die eigenen Risiken zu verwalten.

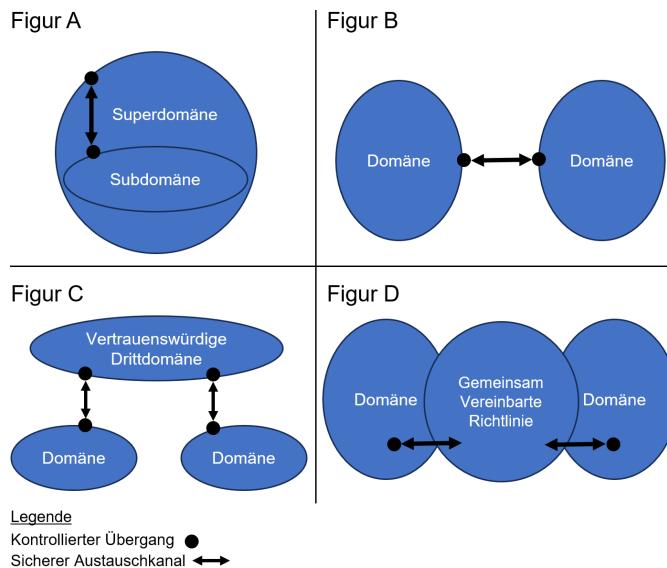


Abbildung 18: Logische Beziehungen von Domänen
Quelle: Eigene Darstellung

Neben der Standardmöglichkeit für einen Austausch zwischen zwei Domänen existieren zwei weitere Möglichkeiten. Die erste ist ein Austausch über eine vertrauenswürdige Drittdomäne. Da beide Domänen der Drittdomäne vertrauen, entsteht eine transitive Beziehung. Dies wird in Abbildung 18 mit Figur C dargestellt. Der Austausch kann ausschließlich über die Drittdomäne oder in Kombination mit einem direkten Austausch erfolgen, wobei die Drittdomäne die jeweiligen Domänen authentifiziert.

Die zweite Möglichkeit besteht in der Vereinbarung einer gemeinsamen Richtlinie. Dadurch bleiben die Domänen autonom und verwalten ihre eigenen Risiken selbstständig. Die Richtlinie wird jedoch geteilt, wodurch eine Vertrauensbeziehung entsteht und zu jeder Zeit der Umgang mit Informationen im Einklang mit der Richtlinie ist. Dies ist in Figur D in Abbildung 18 visualisiert.

Auf Basis der modellierten Sicherheitsdomänen mit ihren Beziehungen und der dahinterstehenden Prozesse sowie Informations- und Wertflüsse werden die logischen Sicherheitsmaßnahmen unter Berücksichtigung ihrer Risikobewertung definiert, damit die Maßnahmenbehandlung proportional und angemessen zum Risiko ist. Dazu werden die im Security Service vordefinierten Sicherheitsmaßnahmen

ausgewählt oder in Abhängigkeit des Kontextes durch neue Maßnahmen behandelt. Dabei ist folgende Reihenfolge zu beachten: Abschreckung, Prävention, Erkennung, Eindämmung und korrigierend. Jede Behandlungsart wirkt sich auf die verschiedenen Parameter eines Risikos aus, wie in Abbildung 19 visualisiert ist.

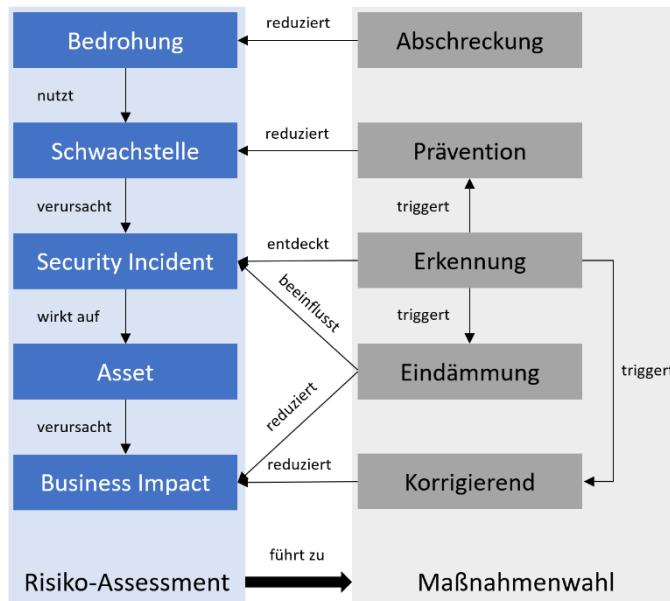


Abbildung 19: Auswirkung der Behandlungsarten
Quelle: Eigene Darstellung

5.5.2. PHYSISCHE EBENE

Auf dieser Ebene werden die logischen Anforderungen operationalisiert, indem die Logik in der physischen Welt realisiert wird. Zudem werden die gewählten Sicherheitsmaßnahmen des Security Service Catalogue mit Hilfe des Security Mechanism Catalogue ausgearbeitet.

Vor der Operationalisierung der logischen Sicherheitsarchitektur sollten die spezifischen Sicherheitsrichtlinien der logischen Ebene in Form von Anweisungen und Regelungen für die physische Ebene erstellt werden. Die Ausgestaltung kann in Form von Arbeitsanweisungen erfolgen, die die Sicherheitsprozesse beschreiben und eine Schritt-für-Schritt-Anleitung enthalten. Weitere Ausarbeitungen könnten durch Guidelines ergänzt werden, die Best Practices darstellen. Im Rahmen der Konkretisierung können die Security Mechanism ausgearbeitet werden, die mit den Vorgaben der internen Richtlinien und der definierten Arbeitsanweisungen sowie Guidelines übereinstimmen. Die Möglichkeit, diese mit den Sicherheitsdiensten zu verknüpfen, würde eine Verbindung zwischen den logischen Sicherheitsmaßnahmen und den physischen Maßnahmen herstellen.

Im Anschluss erfolgt eine Aufteilung der logischen Architektur der Organisation in physische Architekturen. Dabei werden Informations- und Werteströme in verschiedenen Architekturen dargestellt, zu denen beispielsweise Netzwerkarchitekturen und Datenstrukturen zählen. Diese werden genutzt, um die Security Mechanism in den physischen Architekturen unter Berücksichtigung der logischen Architektur zu modellieren.

5.5.3. KOMPONENTENEBENE

Zur Realisierung des Security Mechanism erfolgt auf der Komponentenebene eine detaillierte Beschreibung der eingesetzten Sicherheitskomponenten. Die definierten Maßnahmen umfassen nicht nur spezialisierte Software- und Hardwarelösungen, sondern können auch Organisatorisches beinhalten.

Bei der Auswahl spezifischer Sicherheitsmaßnahmen sollten die Faktoren ‚Wirtschaftlichkeit‘, ‚vorhandene Kompetenzen‘ sowie ‚Koexistenz mit anderen Sicherheitsmaßnahmen‘ berücksichtigt werden. Für die Berechnung der Wirtschaftlichkeit kann das ROSI-Modell herangezogen werden (vgl. ENISA 2012), das auf Schätzungen basiert. Somit bildet es die Realität nicht exakt ab, sondern nähert sich dieser an. Im Rahmen des Aufbaus einer Defense-in-Depth-Strategie (vgl. NSA o. D.) ist zu berücksichtigen, dass der Einsatz einer steigenden Anzahl von Sicherheitsmaßnahmen weder effektiv noch wirtschaftlich ist (vgl. Gordon/Loeb 2002: 446–450). Des Weiteren kann es zu einer negativen Beeinflussung der geplanten Sicherheitsmaßnahmen kommen, wodurch sich neue Sicherheitslücken eröffnen. Neben der Kosten- und Auswirkungsbetrachtung ist anzumerken, dass innerhalb der Organisation die Kompetenzen und das Wissen fehlen können, um die Maßnahme zu implementieren, zu nutzen und zu warten. In diesem Zusammenhang können Weiterbildungsmaßnahmen erforderlich sein.

Die Wahl der Maßnahmen stellt lediglich einen Aspekt der Standardisierung dar. Auf dieser Ebene findet zudem die operative Standardisierung statt, die darauf abzielt, die Effektivität und die Effizienz der Maßnahmen zu steigern. Dazu können Templates für Dokumente erstellt und gehärtete Standardkonfigurationen von CIS genutzt werden (vgl. CIS o. D.).

5.6. UMSETZUNG DER UNTERNEHMENSSICHERHEITSARCHITEKTUR

Nach der Modellierung der Unternehmenssicherheitsarchitektur erfolgt innerhalb dieses Prozessschrittes deren Umsetzung. Da die erweiterte Methodik auf den IT-

Grundschutz und das IT-Grundschutz-Kompendium aufbaut, können die jeweiligen Umsetzungshinweise für die Ausgestaltung und Implementation herangezogen werden (vgl. BSI 2019). Ein Großteil der Umsetzungshinweise referenziert jedoch auf die veraltete Edition 2022, weshalb sie nicht mehr dem Stand der Technik oder den aktuellen Anforderungen entsprechen könnten.

Vor der Umsetzung sollte eine Umsetzungsstrategie definiert werden, nach der die Sicherheitsmaßnahmen implementiert werden sollen. Dabei kann zwischen der ‚Big Bang‘, der inkrementellen oder der iterativen Variante gewählt werden. Der ‚Big Bang‘-Ansatz zeichnet sich dadurch aus, dass die geplanten Maßnahmen gleichzeitig und ohne zeitliche Verzögerung implementiert werden. Im Gegensatz zum inkrementellen Ansatz, bei dem bei jedem Schritt eine neue, vollfunktionsfähige Maßnahme eingeführt wird, erfolgt im iterativen Ansatz eine Anpassung durch wiederholte Zyklen. Bei der Entscheidungsfindung sollten die internen Governance-Strukturen der Organisation berücksichtigt und gegebenenfalls ergänzt werden. In Anlehnung ans IT-Engagement-Modell von Ross et al. (vgl. 2006: 152–154) könnte ein Information-Security-Engagement-Modell etabliert werden, das aus Steuerungsmechanismen besteht. Letztere stellen sicher, dass Geschäfts- und Informationssicherheitsprojekte sowohl lokale als auch organisationsweite Ziele erreichen. Das Modell besteht aus drei Ebenen, die in Abbildung 20 mit ihren Beziehungen visualisiert sind:

- Organisationsweite IS-Governance: verantwortlich für die Entscheidung und den Umgang mit organisationsweiter Informationssicherheit,
- Projektmanagement: formalisierte Methodologie zum Umgang mit Projekten mit klaren Zielen und Lieferobjekten sowie
- Verbindungsmechanismus: Ausrichtung der operativen Aktivitäten in den Projekten an die organisationsweite IS-Governance.

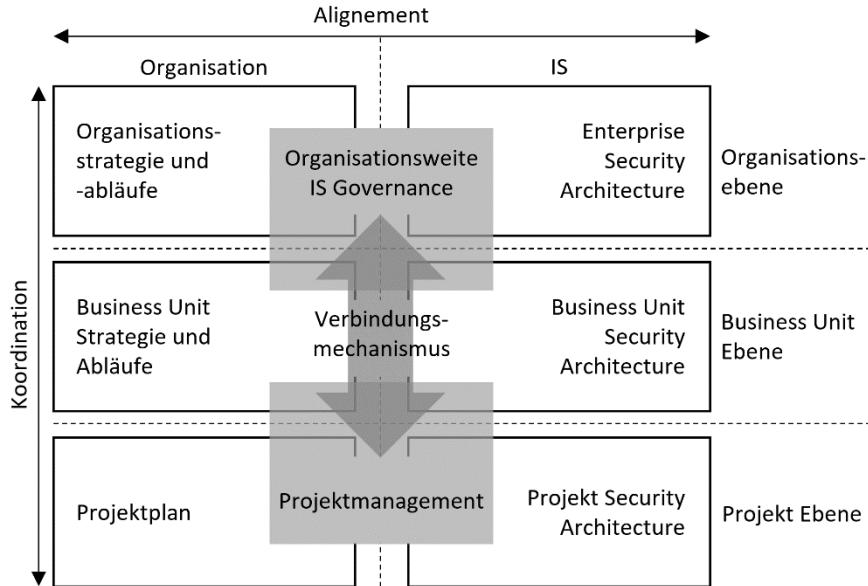


Abbildung 20: IS-Engagement-Modell
Quelle: In Anlehnung an (Ross et al. 2006: 154)

Die organisationsweite IS-Governance reflektiert die Prinzipien der Organisations-Governance und ist auf die Ausrichtung der Informationssicherheit nach den Organisationszielen fokussiert. Sie besteht aus dem CISO, dem ISMS-Team (vgl. Anhang A.1.1) und – je nach Ausgestaltung – dem ESA-Team. Zur Standardisierung des Projektmanagements verwenden Organisationen entweder bestehende Standards oder eigene Ausgestaltungen. Die Steuerung der Project Security Architecture erfolgt durch den jeweiligen Project Security Officer (vgl. Anhang A.1.1) und Architekt:innen. Die Sicherstellung der Ausrichtung von Aktivitäten und Ergebnissen nach der Organisation geschieht durch die frühzeitige und regelmäßige Überwachung, Priorisierung, Anpassung und Korrektur der Projektdurchführung über den Verbindungsmechanismus. Dies kann durch den IS Coordination Committee (vgl. Anhang A.1.1) in Zusammenarbeit mit dem ISMS-Team, den Fachverantwortlichen und den betroffenen Sicherheitsbeauftragten erfolgen, um die Ausrichtung der Informationssicherheit nach den Organisationszielen zu gewährleisten (vgl. BSI 2017a: 46).

Bei der Wahl der Umsetzungsmöglichkeiten und der Strukturierungen der Organisation ist es erforderlich, den Informationsbedarf zu ermitteln und den nötigen Informationsaustausch unter Berücksichtigung der formellen und informellen Hierarchien innerhalb der Organisation zu definieren. Dies würde gewährleisten, dass die relevanten Stakeholder:innen auch nach der Implementierung der Informationssicherheitsarchitektur positiv gestimmt sind und keine Umstellung zur klassischen Arbeitsweise fordern.

Zusätzlich zum Informationsbedarf sollte das vorhandene Wissen in der Organisation mit dem benötigten Wissensbedarf des Soll-Zustands der Architektur verglichen werden, um nötige Maßnahmen zu evaluieren. Dies beinhaltet die Prüfung von Weiterbildungs-, Trainings- oder Sensibilisierungsmaßnahmen.

Da Organisationen ihre Aktivitäten nicht ausschließlich mit eigenem Personal durchführen, sondern auch durch Outsourcing, ist die Betrachtung der organisationsfremden Entitäten sowie ihr Wirken auf die Prozesse und die Organisation relevant. Die Ausrichtung der Outsourcing-Beziehung könnte nach den Architekturreifegraden verglichen und angepasst werden (vgl. Kapitel 4.1.2).

5.7. AUFRECHTERHALTUNG UND VERBESSERUNG

Zur Deckung externer und interner Bedarfe werden Systeme im Rahmen des kontinuierlichen Verbesserungsprozesses angepasst. Dadurch eröffnen sich einerseits neue Möglichkeiten und andererseits ist eine Steigerung ihrer Komplexität zu verzeichnen. Der Begriff ‚System‘ umfasst nicht ausschließlich technische Systeme, sondern allgemein die Interaktion mehrerer Komponenten zur Erfüllung eines Zwecks. Dies können beispielsweise Unternehmen, Geschäftsfunktionen, Aufgabenbereiche, Produkte, IT-Systeme und Software sein (vgl. ISO 2019b: iv). Zur Bewältigung der Komplexität von Systemen werden Konzepte, Prinzipien, Verfahren und Werkzeuge eingesetzt, um effektive Architekturen zu konzipieren und architekturbezogene Entscheidungen zu optimieren.

Architecture Evaluations werden aus verschiedenen Gründen durchgeführt (vgl. ISO 2019c: vi):

- Feststellung, ob etwas so konzipiert wurde oder wird, dass der beabsichtigte Zweck erfüllt wird (oder so geändert werden kann, dass es einem neuen Zweck dient),
- Bewertung der Wirksamkeit und Eignung einer Architektur im Hinblick auf die Bedürfnisse und Erwartungen der Beteiligten,
- Ermittlung von Risiken, die es zu mindern gilt,
- Ermittlung von Möglichkeiten zur Verbesserung,
- Klärung des Problemraums und der Bedürfnisse der Beteiligten sowie
- Bewertung des Fortschritts bei der Erreichung der Architekturziele.

Für die Evaluierung der ESA eignet sich der Evaluierungsprozess nach ISO/IEC/IEEE 42030:2019 (vgl. ISO 2019c), der durch die Business Attributes für

ein datengetriebenes Vorgehen unterstützt werden kann. Dadurch kann ein Feedback auf allen Metaebenen eingeführt werden, das sowohl der Aufrechterhaltung der Architektur als auch ihrer Verbesserung dient. Während die Architectual Analysis zentral die aufgestellte ESA umfassen, werden deren Auswirkungen durch das Value Assessment und die Evaluation Synthesis betrachtet. Diese Überprüfungen erlauben die Ermittlung von Verbesserungspotenzialen sowie die Kontrolle der Wirksamkeit der implementierten Maßnahmen. Weitere Potenziale können durch eine Evaluierung des Reifegrads der Architektur auf Basis des CMMI (vgl. Isaca o. D.) sowie des Reifegrads nach Ross et al. (vgl. 2006: 97–120) erhoben werden, die durch die Organisation genutzt werden könnten.

6. DISKUSSION DER THESIS

In diesem Kapitel wird die vorgeschlagene Lösung anhand der zuvor definierten Designanforderungen, den Guidelines des Forschungsansatzes und des zugrundeliegenden Prozesses evaluiert. Dabei erfolgt eine nachgelagerte Betrachtung der Schwächen dieser These.

6.1. ERFÜLLUNG DER DESIGNANFORDERUNGEN

Im Folgenden wird die erweiterte IT-Grundschutz-Methodik nach den in Kapitel 2.2 definierten Anforderungen bewertet.

Anforderung 1: Die erweiterte IT-Grundschutz-Methodik muss ESA-Fähigkeiten enthalten.

Diese Anforderung ist erfüllt, da das vorgestellte Modell in Kapitel 5 die IT-Grundschutz-Methodik mit dem ESA-Framework SABSA erweitert. Zudem wurden praktische Möglichkeiten zur Ausführung der Fähigkeiten sowie zur Einbettung in die Enterprise Architecture aufgezeigt.

Anforderung 2: Es sollte weiterhin die Einhaltung des IT-Grundschutzes gewährleistet sein, um das ISMS nach dem BSI zertifizieren lassen zu können.

Bei der Zertifizierung nach der ISO/IEC 27001 auf Basis von IT-Grundschutz sind zwei Aspekte der erweiterten IT-Grundschutz-Methodik zu betrachten, um die Einhaltung der regulatorischen Vorgaben zu überprüfen. Der erste Aspekt betrifft die Durchführung des Sicherheitsprozesses. Im Rahmen der erweiterten Methodik wurden die Prozesse um eine Verlinkung der Sicherheit mit den Organisationszielen ergänzt. Der zweite Aspekt umfasst die Einhaltung der Sicherheitsanforderungen gemäß dem IT-Grundschutz-Kompendium sowie die Modellierung der Organisation. Die Verlinkung zwischen dem IT-Grundschutz-Kompendium und SABSA ermöglicht die Konzeption und Implementierung einer Sicherheitsarchitektur, die den Vorgaben des BSI entspricht. In Konsequenz erfolgt die Durchführung des Sicherheitsprozesses gemäß der erweiterten Methodik in Übereinstimmung mit den Vorgaben für die Zertifizierung der Organisation nach dem BSI-Standard.

Anforderung 3: Das Ergebnis sollte generell so klar sein, dass es in der Praxis anwendbar ist.

Die Modellierung der verschiedenen Metaebenen der erweiterten IT-Grundschutz-Methodik kann auf Basis diverser Modellierungssprachen von der Object Management Group durchgeführt werden. Zudem wurden Verknüpfungsmöglichkeiten mit der Enterprise Architecture aufgezeigt. Wegen der aktuellen Limitation von SABSA ist die Anwendung bzw. die Durchführung der Architektur in der Praxis jedoch mit hohen Aufwänden verbunden.

6.2. BEURTEILUNG NACH DESIGN-SCIENCE-GUIDELINES

In diesem Unterkapitel wird die Durchführung dieser Forschung anhand der sieben Guidelines von Hevner (vgl. 2004: 82–90) bewertet.

Guideline 1: Design as an Artifact – DSR muss ein nutzbares Artefakt in Form eines Konstrukts, eines Modells, einer Methode oder einer Instanziierung produzieren (vgl. ebd.: 83).

Ziel dieser Forschungsarbeit war es, die IT-Grundschutz-Methodik um ESA-Fähigkeiten zu erweitern. Die Lösung ist die erweiterte IT-Grundschutz-Methodik mit SABSA.

Guideline 2: Problem Relevance – Ziel der DSR ist die Entwicklung technologischer Lösungen für wesentliche und relevante wirtschaftliche Probleme (vgl. ebd.: 83).

Die erweiterte IT-Grundschutz-Methodik ermöglicht die Ausrichtung der Sicherheit nach den Organisationszielen. Wie in Kapitel 2 beschrieben, ist dies schwierig, da das BSI und andere Sicherheitsstandards nicht beschreiben, wie dies durchgeführt werden könnte. Mit Hilfe der erweiterten Methodik kann die ESA nach der Organisation ausgerichtet werden.

Guideline 3: Design Evaluation – Nutzen, Qualität und Wirksamkeit eines Designartefakts müssen durch geeignete Evaluationsmethoden nachgewiesen werden (vgl. ebd.: 83).

Es wurde ein deskriptiver Ansatz gewählt, da das Design aktuell nur anhand fundierter Argumente (vgl. ebd.: 86) – basierend auf Literatur und Expert:inneninterviews – bewertet werden kann.

Guideline 4: Research Contributions – effektive DSR muss klare und überprüfbare Beiträge in den Bereichen ‚Designartefakt‘, ‚Designgrundlagen‘ und/oder ‚Designmethoden‘ beinhalten (vgl. ebd.: 83).

Nach Auswertung der Literaturanalyse lässt sich feststellen, dass bislang keine Untersuchungen zur Erweiterung der IT-Grundschutz-Methodik mit SABSA oder allgemein zu einem ESA-Framework durchgeführt wurden. Das Ergebnis dieser Arbeit basiert auf einer konzeptionellen Analyse und wurde noch nicht unter realen Bedingungen getestet. Infolgedessen kann eine Ergänzung der Wissensbasis lediglich auf theoretischer Ebene erfolgen.

Guideline 5: Research Rigor – DSR basiert sowohl bei der Konstruktion als auch bei der Bewertung des Designartefakts auf der Anwendung rigoroser Methoden (vgl. ebd.: 83).

Die Genauigkeit und die Limitationen dieser Forschung werden unter Berücksichtigung der Grenzen der gewählten Untersuchungsmethoden überprüft. Zu Beginn der Forschung wurde eine Literaturanalyse durchgeführt, um eine theoretische Grundlage für die ESA-Thematik sowie mögliche Ausgestaltungen mit ESA und kritische Betrachtungen des IT-Grundschatzes zu erlangen. Die Literaturanalyse erfolgte in Form einer strukturierten und unstrukturierten Literaturrecherche. Dabei wurden in mehreren Datenbanken digital verfügbare Texte identifiziert und nach Filterkriterien sortiert. Die Literaturanalyse hatte zum Ziel, einen Überblick über bestehende Methoden und Theorien zu gewinnen. Dazu wurden sowohl Peer-Reviews als auch Fachartikel berücksichtigt. Das genannte Ziel wird durch die Einbeziehung einer breiten Palette sowohl akademischer als auch grauer Literatur in diese Forschung erreicht. In diesem Kontext wurden nur wenige konzeptionelle Arbeiten für die ESA und den IT-Grundschutz gefunden. Die Verwendung von Google und Google Scholar für die unstrukturierte Literaturrecherche kann jedoch zu Kritik führen, insbesondere hinsichtlich des Umfangs und der Reproduzierbarkeit der Recherche. Um die erweiterte Methodik auf eine höhere theoretische Grundlage zu stellen, wurden generelle Aspekte der Enterprise Architecture herangezogen, um sie ins Modell einzuarbeiten. Erstere wurde auf Basis der Theorie entwickelt und sollte mittels Expert:inneninterviews evaluiert werden.

In der vorliegenden Untersuchung wurden zehn Expert:inneninterviews mit ausgewählten Personen durchgeführt. Um die Beeinflussung und den eigenen Bias in den Einzelinterviews zu reduzieren, wurden Leitfragen vorbereitet. Des Weiteren wurde durch den Einsatz der Kodierungstechnik der Bias verringert.

Die Zielsetzung der Expert:inneninterviews bestand in der Evaluierung der erweiterten Methodik sowie der Generierung von Informationen über die potenzielle Umwelt. Für die Evaluierung der Methodik wurde ein deduktives Vorgehen gewählt, für die Ermittlung der Umwelt ein induktives. Die Interviewten waren Forschende, Chief Information Security Officer, Berater:innen sowie Praktiker:innen. Die Befragung dieser Personen, die im Rahmen ihrer Tätigkeit auf den jeweiligen Metaebenen arbeiten oder forschen, ermöglichte die Betrachtung aller Ebenen und eine ganzheitliche Analyse des Prozesses. Laut der Auswertung der Expert:inneninterviews weist die erweiterte Methodik zwar Potenzial auf, sie könnte jedoch in der Umwelt bzw. der Organisation zu Komplikationen führen. Eine weitere Möglichkeit zur Evaluierung der Ergebnisse wäre eine Gruppendiskussion. Allerdings ist aufgrund der möglichen geringen Informationsmacht der Personen davon auszugehen, dass diese keine neuen Erkenntnisse bringen würde. Daher könnte die theoretisch erweiterte Methodik im Rahmen eines Experiments eruiert werden.

Die erweiterte IT-Grundschutz-Methodik wurde bislang nicht in der Praxis angewendet. Evaluierungen wurden ausschließlich auf theoretischer Basis durchgeführt, weshalb der Prozessschritt ‚Demonstration‘ des DSRP in dieser Forschung ausgelassen wurde. Diese Limitation findet sich in allen identifizierten ESA-Methodiken wieder. In der Beschreibung der erweiterten Methodik wurden jedoch praktische Umsetzungsmöglichkeiten aufgezeigt.

Guideline 6: Design as a Search Process – die Suche nach einem effizienten Artefakt erfordert den Einsatz der verfügbaren Mittel, um die gewünschten Ziele und zudem die Gesetze der Problemumgebung zu erreichen (vgl. ebd.: 83).

Da diese Forschung als Suchprozess konzipiert war, manifestierte sich, dass jeder Prozessschritt zu neuen Erkenntnissen führte. Der iterative Prozess aus Design und Evaluierung resultierte in einer Lösung, die die in Kapitel 2.2 dargelegten Designanforderungen erfüllt.

Guideline 7: Communication of Research – Design und naturwissenschaftliche Forschung müssen sowohl technik- als auch wirtschaftsorientierten Zielgruppen präsentiert werden (vgl. ebd.: 83).

Die Ergebnisse wurden einer Arbeitsgruppe bestehend aus Enterprise Architects, Security Expert:innen und Manager:innen der Nortal AG präsentiert.

7. CONCLUSIO

In diesem Kapitel werden die bedeutendsten Ergebnisse dieser Arbeit zusammengefasst. Zudem werden Empfehlungen für zukünftige Forschungsarbeiten gegeben, die zum Teil auf der vorhergehenden Diskussion basieren.

7.1. RELEVANTE BEITRÄGE DER THESIS

Der Fokus dieser Arbeit liegt auf der Anpassung der IT-Grundschutz-Methodik zu einem businessgetriebenen Modell. Dabei wird die Informationssicherheit nach den Organisationszielen ausgerichtet, da in der Methodik nicht aufgezeigt wird, wie das möglich ist. Im Rahmen der Untersuchung, wie die IT-Grundschutz-Methodik zur Entwicklung einer ganzheitlichen Sicherheitsarchitektur mit SABSA kombiniert werden kann, entstanden folgende Ergebnisse:

- Es wurde eine breite Übersicht zur Enterprise Architecture und zur ESA gegeben, in der die Möglichkeiten, Hintergründe und Limitationen beschrieben sind.
- Vor allem die extrinsische Motivation von Organisationen zur Informationssicherheit wurde durch die Expert:inneninterviews aufgedeckt. Deshalb ist das Stakeholder:innenmanagement kritisch, um neue Vorgehen in einer Organisation zu etablieren.
- Die erweiterte IT-Grundschutz-Methodik um die SABSA-Methodologie wurde vorgestellt. Dies erfolgte, um bei der Etablierung der Informationssicherheit nach der IT-Grundschutz-Methodik die Architektur nach den Organisationszielen zu konzipieren und in die Enterprise Architecture zu integrieren.
- Zur Ermöglichung der Organisationszertifizierung nach ISO/IEC 27001 auf Basis des IT-Grundschutzes bei Einsatz der erweiterten IT-Grundschutz-Methodik wurde ein Mapping erstellt. Letzteres kann in der Umsetzung unterstützen, die regulatorischen Vorgaben des BSI einzuhalten.

Die erweiterte IT-Grundschutz-Methodik wurde auf Basis der Literatur modelliert und durch Expert:inneninterviews evaluiert. Dieses Ergebnis ermöglicht Personen eine Ausrichtung ihrer Informationssicherheit nach den Organisationszielen und somit einer businessgetriebenen Informationssicherheit. Dadurch wird eine zielgruppenorientierte Kommunikation ermöglicht, die zu einem besseren Verständnis der Informationssicherheit in der Organisation führt und in der Entscheidungsfindung unterstützen kann.

7.2. EMPFEHLUNG FÜR ZUKÜNFTIGE FORSCHUNG

Wie in Kapitel 4.2 dargelegt, stellt die Adaption einen wesentlichen Aspekt für die Anwendung der erweiterten Methodik dar. Daher ist eine detaillierte Betrachtung dieses Aspekts erforderlich, um die Anwendung zu vereinfachen und zusätzliche Erkenntnisse zu gewinnen. Für die zukünftige Forschung eignet sich eine Untersuchung der Adaption in folgenden drei Bereichen:

Die Strukturierung der erweiterten IT-Grundschatz-Methodik nach einem klassischen Vorgehen bedingt eine prozessorientierte Vorgehensweise. Dies kann bei adaptiven, antifragilen Organisationen, die auf agile Ansätze bauen, zu Problemen bei der Umsetzung der Methodik führen. Deshalb wäre zu eruieren, welche Modifikationen der erweiterten IT-Grundschatz-Methodik erforderlich sind, um eine ESA in einer agilen Umgebung zu konzipieren. Eine Herangehensweise bestünde in der Umstrukturierung des Lebenszyklus von SABSA nach ITIL 4 und der Einführung von agilen Prinzipien.

Des Weiteren könnte untersucht werden, inwiefern eine Unschärfe in der Architektur denkbar wäre, sodass veraltete Informationen die Architektur nicht beeinträchtigen und eine Reduktion der Arbeitsintensität zu verzeichnen wäre. Diese Thematik wurde von der interviewten Person F2 angesprochen, die den Einsatz von SABSA in einem Konzern miterlebt hat. Dabei war die Aufrechterhaltung der Architektur mit einem hohen Ressourceneinsatz verbunden (vgl. Kapitel 4.2, Kategorie ‚Intensität‘).

Eine potentielle Betrachtung wäre zudem die Sammlung praktischer Erfahrungen im Einsatz der erweiterten IT-Grundschatz-Methodik. Die Erkenntnisse könnten bei der zukünftigen Anpassung der Methodik unterstützend wirken, um die Arbeitsabläufe effektiver und effizienter zu gestalten sowie Möglichkeiten zu identifizieren, die eine Anpassung der Methodik für Organisationen mit unterschiedlichen Größen und Herausforderungen ermöglichen.

8. LITERATURVERZEICHNIS

- Ahmed, Md. Tomig Uddin/Nazrul Islam Bhuiya/Md. Mahbubur Rahman (2017): A secure enterprise architecture focused on security and technology-transformation (SEAST), in: *2017 12th International Conference For Internet Technology And Secured Transactions (ICITST)*, [online] doi:10.23919/icitst.2017.8356386.
- Alshammary, Bandar (2017): Enterprise Architecture Security Assessment Framework (EASAF), in: *Journal Of Computer Science*, Bd. 13, Nr. 10, S. 558–571, [online] doi:10.3844/jcssp.2017.558.571.
- Axelos (2020): *ITIL 4 Strategic Leader: Digital and IT Strategy (PDF)*, Tso, the Stationery Office.
- Barafort, Béatrix/Antoni-Lluís Mesquida/Antònia Mas (2018): Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context, in: *Computer Standards & Interfaces*, Bd. 60, S. 57–66, [online] doi:10.1016/j.csi.2018.04.010.
- Barrera, Ariel/Jim Kenneally/Gloria Killen/Wanda McKenzie (2011): *Developing a Standard Enterprise Architecture Practice*, IT@Intel White Paper, IT@Intel White Paper, [online] <https://www.intel.ua/content/dam/doc/white-paper/intel-it-it-leadership-developing-a-standard-enterprise-architecture-practice-paper.pdf> [abgerufen am 10.08.2024].
- Baskerville, Richard (1993): Information Systems Security Design Methods, in: *ACM Computing Surveys*, Association for Computing Machinery, Bd. 25, Nr. 4, S. 375–414, [online] doi:10.1145/162124.162127.
- Baur, Nina/Jörg Blasius (2022): *Handbuch Methoden der empirischen Sozialforschung*, Springer VS.
- Bounogui, Yassine/Abdellatif Mezrioui/Hatim Hafiddi (2019): Toward a unified Framework for cloud Computing governance: an approach for evaluating and integrating IT management and governance models, in: *Computer Standards & Interfaces*, Elsevier BV, Bd. 62, S. 98–118, [online] doi:10.1016/j.csi.2018.09.001.
- BSI (2017a): *BSI-Standard 200-2 IT-Grundschutz-Methodik*, BSI, Bundesamt für Sicherheit in der Informationstechnik, [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html [abgerufen am 10.08.2024].
- BSI (2017b): *BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz*, BSI, Bundesamt für Sicherheit in der Informationstechnik, [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html [abgerufen am 10.08.2024].

- BSI (2023a): *BSI-Standard 200-4 Business Continuity Management*, BSI, Bundesamt für Sicherheit in der Informationstechnik, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html [abgerufen am 10.08.2024].
- BSI (2016): Cyber-Sicherheit als Wettbewerbsvorteil in der Digitalisierung, BSI, [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Cyber-Sicherheit_als_Wettbewerbsvorteil.html [abgerufen am 10.08.2024].
- BSI (o. D.): IT-Grundschatz, Bundesamt für Sicherheit in der Informationstechnik, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/it-grundschatz_node.html [abgerufen am 10.08.2024].
- BSI (2023b): IT-Grundschatz-Kompendium – Werkzeug für Informationssicherheit, BSI, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/IT-Grundschatz-Kompendium/it-grundschatz-kompendium_node.html [abgerufen am 10.08.2024].
- BSI (2023c): Kreuzreferenztabellen zum IT-Grundschatz-Kompendium (Edition 2023), BSI, [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschatz/Kompendium/krt2023_Excel.html [abgerufen am 10.08.2024].
- BSI (2019): Umsetzungshinweise: zum IT-Grundschatz-Kompendium, BSI, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/IT-Grundschatz-Kompendium/Umsetzungshinweise/umsetzungshinweise_node.html [abgerufen am 10.08.2024].
- Buckl, Sabine/Alexander Ernst/Josef Lankes/Florian Matthes/Christian Schweda (2009): *State of the Art in Enterprise Architecture Management*, TUM, Software Engineering for Business Information Systems (sebis), [online] <https://wwwmatthes.in.tum.de/file/1wbr6a65ggqkx/Sebis-Public-Website/Publications/Bu09h.pdf&ved=2ahUKEwiu2uWez-CGAXVjRvEDHXE0Ds4QFnoECBMQAQ&usg=AOv-Vaw1c2S8nVry3jniQsfIBMN> [abgerufen am 10.08.2024].
- Byrd, Terry Anthony/Bruce R. Lewis/Robert W. Bryan (2006): The leveraging influence of strategic alignment on IT investment: An empirical examination, in: *Information & Management*, Bd. 43, Nr. 3, S. 308–321, [online] doi:10.1016/j.im.2005.07.002.
- Carr, Darryl/Steven Else (2018): *State of Enterprise Architecture Survey: Results and Findings*, Enterprise Architecture Professional Journal, Enterprise Architecture Professional Journal, [online] <https://eapj.org/wp-content/uploads/2018/05/EAPJ-Special-Edition-State-of-EA-Survey.pdf> [abgerufen am 10.08.2024].
- Cephas Consulting (2018): SABSA® Security Architecture Extension, [online] <https://enterprisemodelingsolutions.com/ext-sabsa/>.

- Chan, Yolande E./Blaize Horner Reich (2007): IT alignment: What have we learned?, in: *Journal Of Information Technology*, Bd. 22, Nr. 4, S. 297–315, [online] doi:10.1057/palgrave.jit.2000109.
- Chen, Peter Pin-Shan (1976): The entity-relationship model—toward a unified view of data, in: *ACM Transactions On Database Systems*, Bd. 1, Nr. 1, S. 9–36, [online] doi:10.1145/320434.320440.
- CIS (o. D.): CIS Benchmarks List, CIS Security, [online] <https://www.cise-curity.org/cis-benchmarks> [abgerufen am 10.08.2024].
- Claus, Simon (2007): Datenschutz im IT-Grundschutz, in: *Datenschutz und Datensicherheit - Dud*, Springer Nature, Bd. 31, Nr. 2, S. 87–90, [online] doi:10.1007/s11623-007-0045-9.
- Coltman, Tim/Paul P. Tallon/Rajeev Sharma/Magno Queiroz (2015): Strategic IT Alignment: Twenty-Five Years on, in: *Journal Of Information Technology*, Bd. 30, Nr. 2, S. 91–100, [online] doi:10.1057/jit.2014.35.
- Corbet, Shaen/Constantin Gurdgiev (2019): What the hack: Systematic risk contagion from cyber events, in: *International Review Of Financial Analysis (Online)/International Review Of Financial Analysis*, Bd. 65, S. 101386, [online] doi:10.1016/j.irfa.2019.101386.
- Corbin, Juliet/Anselm Strauss (2015): *Basics of Qualitative Research*, SAGE.
- Culot, Giovanna/Guido Nassimbeni/Matteo Podrecca/Marco Sartor (2021): The ISO/IEC 27001 Information Security Management Standard: Literature review and Theory-based Research agenda, in: *The Tqm Journal*, Emerald Publishing Limited, Bd. 33, Nr. 7, S. 76–105, [online] doi:10.1108/tqm-09-2020-0202.
- Dedić, Nedim (2020): FEAMI: A methodology to include and to integrate enterprise architecture processes into existing organizational processes, in: *IEEE Engineering Management Review*, Institute of Electrical and Electronics Engineers, Bd. 48, Nr. 4, S. 160–166, [online] doi:10.1109/emr.2020.3031968.
- Dhillon, Gurpreet/Kane Smith/Indika Dissanayaka (2021): Information Systems Security Research Agenda: Exploring the Gap between research and Practice, in: *Journal Of Strategic Information Systems*, Elsevier BV, Bd. 30, Nr. 4, S. 101693, [online] doi:10.1016/j.jsis.2021.101693.
- Diesch, Rainer/Matthias Pfaff/Helmut Krcmar (2020): A comprehensive model of information security factors for decision-makers, in: *Computers & Security*, Bd. 92, S. 101747, [online] doi:10.1016/j.cose.2020.101747.
- Dudenredaktion (o. D.): Methode, Duden Online, [online] <https://www.duden.de/node/96411/revision/1327949> [abgerufen am 10.08.2024].
- ENISA (2012): *Introduction to Return on Security Investment*, ENISA, European Network and Information Security Agency, [online] <https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment> [abgerufen am 10.08.2024].

- Flowerday, Stephen V./Tite Tuyikeze (2016): Information security policy development and implementation: The what, how and who, in: *Computers & Security*, Bd. 61, S. 169–183, [online] doi:10.1016/j.cose.2016.06.002.
- Fusch, Patricia/Lawrence Ness (2015): Are we there yet? Data saturation in qualitative research, in: *The Qualitative Report*, [online] doi:10.46743/2160-3715/2015.2281.
- Gerow, Jennifer E./Varun Grover/Jason Bennett Thatcher/Philip L. Roth (2014): Looking Toward the Future of IT-Business Strategic Alignment through the Past: A Meta-Analysis, in: *Management Information Systems Quarterly*, Bd. 38, Nr. 4, S. 1059–1085, [online] doi:10.25300/misq/2014/38.4.10.
- Ghauri, Pervez/Kjell Grønhaug/Roger Strange (2020): *Research methods in business studies*, Cambridge University Press.
- Ghaznavi-Zadeh, Rassoul (2017): Enterprise Security Architecture—A top-down approach, ISACA, [online] <https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/enterprise-security-architecture-a-top-down-approach> [abgerufen am 10.08.2024].
- Giustini, Dean/Maged N. Kamel Boulos (2013): Google Scholar is not enough to be used alone for systematic reviews, in: *Online Journal Of Public Health Informatics*, Bd. 5, Nr. 2, [online] doi:10.5210/ojphi.v5i2.4623.
- Gordon, Lawrence A./Martin P. Loeb (2002): The economics of information security investment, in: *ACM Transactions On Information And System Security*, Bd. 5, Nr. 4, S. 438–457, [online] doi:10.1145/581271.581274.
- Goudalo, Wilson/Dominique Seret (2009): The Process of Engineering of Security of Information Systems (ESIS): The Formalism of Business Processes, in: *2009 Third International Conference On Emerging Security Information, Systems And Technologies*, S. 105–113, [online] doi:10.1109/securware.2009.24.
- Graham, Michelle T./Katrina Falkner/Claudia Szabo/Yuval Yarom (2021): Security Architecture Framework for Enterprises, in: *Lecture notes in business information processing*, S. 883–904, [online] doi:10.1007/978-3-030-75418-1_40.
- Grassi, Paul A/James L Fenton/Elaine M Newton/Ray A Perlner/Andrew R Regenscheid/William E Burr/Justin P Richer/Naomi B Lefkovitz/Jamie M Danker/Yee-Yin Choong/Kristen K Greene/Mary F Theofanos (2017): *Digital identity guidelines: authentication and lifecycle management*, [online] doi:10.6028/nist.sp.800-63b.
- Grov, Gudmund/Federico Mancini/Elsie Margrethe Staff Mestl (2019): Challenges for Risk and Security Modelling in Enterprise Architecture, in: *Lecture notes in business information processing*, S. 215–225, [online] doi:10.1007/978-3-030-35151-9_14.
- Hancock, Mary/Linda Amankwaa/Maria Revell/Dale Mueller (2016): Focus Group Data Saturation: A New Approach to Data Analysis, in: *The Qualitative Report*, [online] doi:10.46743/2160-3715/2016.2330.

- Hennink, Monique M./Bonnie N. Kaiser/Vincent C. Marconi (2016): Code saturation versus meaning saturation, in: *Qualitative Health Research*, Bd. 27, Nr. 4, S. 591–608, [online] doi:10.1177/1049732316665344.
- Hennink, Monique M./Bonnie N. Kaiser/Mary Beth Weber (2019): What influences saturation? Estimating sample sizes in focus group research, in: *Qualitative Health Research*, Bd. 29, Nr. 10, S. 1483–1496, [online] doi:10.1177/1049732318821692.
- Heston, Keith M./William Phifer (2011): The multiple quality models paradox: How much ‘best practice’ is just enough?, in: *Journal Of Software Maintenance And Evolution: Research And Practice*, Wiley, Bd. 23, Nr. 8, S. 517–531, [online] doi:10.1002/smrv.481.
- Hevner/March/Hae-Sim Park/Ram (2004): Design science in Information Systems Research, in: *Management Information Systems Quarterly*, MIS Quarterly, Bd. 28, Nr. 1, S. 75, [online] doi:10.2307/25148625.
- IBM (1984): Business Systems Planning: Information Systems Planning Guide, Internet Archive, 4. Aufl., White Plains, [online] <https://archive.org/details/businesssystemsplanningguide> [abgerufen am 10.08.2024].
- Iivari, Juhani/Rudy Hirschheim (1996): Analyzing Information Systems Development: A comparison and analysis of eight IS development approaches, in: *Information Systems*, Elsevier BV, Bd. 21, Nr. 7, S. 551–575, [online] doi:10.1016/s0306-4379(96)00028-2.
- Isaca (o. D.): CMMI, CMMI Institute, [online] <https://cmmiinstitute.com/> [abgerufen am 10.08.2024].
- Isaca (2018): *COBIT 2019 Framework: Governance and Management Objectives*.
- ISO (2019a): ISO 15704:2019 Enterprise modelling and architecture — Requirements for enterprise-referencing architectures and methodologies, ISO, [online] <https://www.iso.org/standard/71890.html> [abgerufen am 10.08.2024].
- ISO (2022a): ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO, [online] <https://www.iso.org/standard/27001.html> [abgerufen am 10.08.2024].
- ISO (2022b): ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, ISO, [online] <https://www.iso.org/standard/75652.html> [abgerufen am 10.08.2024].
- ISO (2017): ISO/IEC 27003:2017, ISO, [online] <https://www.iso.org/standard/63417.html> [abgerufen am 10.08.2024].
- ISO (2022c): ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks, ISO, [online] <https://www.iso.org/standard/80585.html> [abgerufen am 10.08.2024].

- ISO (2023): ISO/IEC/IEEE 15288:2023 Systems and software engineering — System life cycle processes, ISO, [online] <https://www.iso.org/standard/81702.html> [abgerufen am 10.08.2024].
- ISO (2019b): ISO/IEC/IEEE 42020:2019 Software, systems and enterprise — Architecture processes, ISO, [online] <https://www.iso.org/standard/68982.html> [abgerufen am 10.08.2024].
- ISO (2019c): ISO/IEC/IEEE 42030:2019 Software, systems and enterprise — Architecture evaluation framework, ISO, [online] <https://www.iso.org/standard/73436.html> [abgerufen am 10.08.2024].
- Ivas, Ivka (2023): Introduction to BASE Enterprise Architecture Framework for Holistic Strategic Alignment of the Complex Enterprise, in: *Scitepress*, [online] doi:10.5220/0011853200003467.
- Karpovsky, Anna/Robert D. Galliers (2015): Aligning in Practice: From Current Cases to a New Agenda, in: *Journal Of Information Technology*, Bd. 30, Nr. 2, S. 136–160, [online] doi:10.1057/jit.2014.34.
- Konnon, Miton Abel/Nathalie Lodonou/Renaud Horacio Gaffan/Eugène C. Ezin (2023): An Extended Layered Information Security Architecture (ELISA) for e-Government in developing countries, in: *International Journal Of Engineering Trends And Technology*, Bd. 71, Nr. 1, S. 109–123, [online] doi:10.14445/22315381/ijett-v71i1p210.
- Kotusev, Svyatoslav (2019): Enterprise architecture and enterprise architecture artifacts: Questioning the old concept in light of new findings, in: *JIT. Journal Of Information Technology/Journal Of Information Technology*, Bd. 34, Nr. 2, S. 102–128, [online] doi:10.1177/0268396218816273.
- Kotusev, Svyatoslav (2016): The History of Enterprise Architecture: An Evidence-Based Review, in: *Journal Of Enterprise Architecture*, Nr. 12, S. 29–37.
- Kotusev, Svyatoslav (2021): *The Practice of Enterprise Architecture: A Modern Approach to Business and IT Alignment*, Second Edition, SK Publishing, [Kindle] <https://www.amazon.com/dp/064508252X>.
- Kurnia, Sherah/Svyatoslav Kotusev/Graeme Shanks/Rod Dilnutt/Simon K. Milton (2021): Stakeholder engagement in enterprise architecture practice: What inhibitors are there?, in: *Information & Software Technology*, Bd. 134, S. 106536, [online] doi:10.1016/j.infsof.2021.106536.
- Larno, Sara/Ville Seppänen/Jarkko Nurmi (2019): Method Framework for Developing Enterprise Architecture Security Principles, in: *Complex Systems Informatics And Modeling Quarterly*, Nr. 20, S. 57–71, [online] doi:10.7250/csimq.2019-20.03.
- Liao, Kuo-Hsiung/Hao-En Chueh (2012): An evaluation model of information security management of medical staff, in: *International Journal Of Innovative Computing, Information And Control*, Bd. 8, Nr. 11, S. 7865–7873.
- Loft, Paul/Ying He/Iryna Yevseyeva/Isabel Wagner (2022): CAESAR8: An Agile enterprise architecture approach to managing information security risks, in: *Computers & Security*, Bd. 122, S. 102877, [online] doi:10.1016/j.cose.2022.102877.

- Lowman, T./D. Mosier (1997): Applying the DoD goal security architecture as a methodology for the development of system and enterprise security architectures, in: *Proceedings 13th Annual Computer Security Applications Conference*, [online] doi:10.1109/csac.1997.646189.
- Luftman, Jerry N./Tom Brier (1999): Achieving and Sustaining Business-IT Alignment, in: *California Management Review*, Bd. 42, Nr. 1, S. 109–122, [online] doi:10.2307/41166021.
- Malterud, Kirsti/Volkert Dirk Siersma/Ann Dorrit Guassora (2016): Sample size in qualitative interview studies, in: *Qualitative Health Research*, Bd. 26, Nr. 13, S. 1753–1760, [online] doi:10.1177/1049732315617444.
- Maseberg, Sönke (2023): KRITIS-Regularien, in: *Datenschutz und Datensicherheit - Dud*, Springer Nature, Bd. 47, Nr. 9, S. 541–544, [online] doi:10.1007/s11623-023-1814-9.
- Mastrangelo, Giuseppe/Emanuela Fadda/Carlo Róssi/Emanuele Zampogna/Alessandra Buja/Luca Cegolon (2010): Literature search on risk factors for sarcoma: PubMed and Google Scholar may be complementary sources, in: *BMC Research Notes*, Bd. 3, Nr. 1, [online] doi:10.1186/1756-0500-3-131.
- Mathew, Delin/Simon Hacks/Horst Lichter (2018): Developing a semantic mapping between TOGAF and BSI-IT-Grundschutz, in: *ResearchGate*, [online] https://www.researchgate.net/publication/322203229_Developing_a_Semantic_Mapping_between_TOGAF_and_BSI-IT-Grundschutz.
- McClintock, Michelle/Katrina Falkner/Claudia Szabo/Yuval Yarom (2020): Enterprise Security Architecture: Mythology or Methodology?, in: *In Proceedings Of The 22nd International Conference On Enterprise*, Nr. Volume 2, S. 679–689, [online] doi:10.5220/0009404406790689.
- McKinsey (2019): Perspectives on transforming cybersecurity, McKinsey, [online] https://www.mckinsey.com/~/media/mckinsey/mckinsey%20solutions/cyber%20solutions/perspectives%20on%20transforming%20cybersecurity/transforming%20cybersecurity_march2019.pdf [abgerufen am 10.08.2024].
- Meints, Martin (2006): Datenschutz nach BSI-Grundschutz?, in: *Datenschutz und Datensicherheit - Dud*, Springer Nature, Bd. 30, Nr. 1, S. 13–16, [online] doi:10.1007/s02045-006-0005-x.
- Morse, Wayde C./Damon R. Lowery/Todd Steury (2014): Exploring Saturation of Themes and Spatial Locations in Qualitative Public Participation Geographic Information Systems Research, in: *Society & Natural Resources*, Bd. 27, Nr. 5, S. 557–571, [online] doi:10.1080/08941920.2014.888791.
- Namagemebe, Flavia/Agnes Nakakawa/F.P. Tulinayo/Henderik A. Proper/Sietse Overbeek (2023): Towards an E-Government Enterprise Architecture framework for developing economies, in: *Complex Systems Informatics And Modeling Quarterly*, Nr. 35, S. 30–66, [online] doi:10.7250/csimq.2023-35.02.

- Neitzel, Erik/Andreas Witt (2012): Towards Process Centered Information Security Management - A Common View for Federated Business Processes and Personal Data Usage Processes, in: *Proceedings Of The International Conference On Data Technologies And Applications*, S. 189–192, [online] doi:10.5220/0004050301890192.
- NIST (2020): *Security and privacy controls for information systems and organizations*, NIST CSRC, National Institute of Standards and Technology, [online] doi:10.6028/nist.sp.800-53r5.
- NSA (o. D.): Defense in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments, Wayback Machine, [online] https://web.archive.org/web/20121002051613/https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
- OMG (2015a): *Business Motivation Model*, OMG, 1.3, Object Management Group, [online] <https://www.omg.org/spec/BMM/1.3/About-BMM> [abgerufen am 10.08.2024].
- OMG (2014): *Business Process Model and Notation*, OMG, 2.0.2, Object Management Group, [online] <https://www.omg.org/spec/BPMN/> [abgerufen am 10.08.2024].
- OMG (2015b): *Unified Modeling Language*, OMG, 2.5, Object Management Group, [online] <https://www.omg.org/spec/UML/2.5> [abgerufen am 10.08.2024].
- PCI Security Standards Council (2024): *PCI DSS v4.0.1*, PCI Security Standards Council, PCI Security Standards Council, [online] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf [abgerufen am 10.08.2024].
- Peffers, Ken/Tuure Tuunanen/Marcus A. Rothenberger/Samir Chatterjee (2007): A Design Science research Methodology for Information Systems research, in: *Journal Of Management Information Systems*, Taylor & Francis, Bd. 24, Nr. 3, S. 45–77, [online] doi:10.2753/mis0742-1222240302.
- Peterson, Gunnar (2010): From auditor-centric to architecture-centric: SDLC for PCI DSS, in: *Information Security Technical Report*, Bd. 15, Nr. 4, S. 150–153, [online] doi:10.1016/j.istr.2011.02.003.
- Platt, Mario (2021): *What is SABSA Enterprise Security Architecture and why should you care ?*, Medium, Medium, [online] <https://medium.com/@marioplatt/what-is-sabsa-enterprise-security-architecture-and-why-should-you-care-a649418b2742> [abgerufen am 10.08.2024].
- Pleinevaux, Patrick (2016): Towards a Metamodel for SABSA Conceptual Architecture Descriptions, in: *2016 11th International Conference On Availability, Reliability And Security (ARES)*, [online] doi:10.1109/ares.2016.87.
- Pouya, Aleatratı Khosroshahi/Matheus Hauder/Stefan Volkert/Florian Matthes/Martin Gernegroß (2018): Business Capability Maps: Current Practices and Use Cases for Enterprise Architecture Management, [online] <http://hdl.handle.net/10125/50470>.

Qiomas Nous (2024): Qnous, Qnous, [online] <https://www.qnous.io/> [abgerufen am 10.08.2024].

Rees, Jackie/Subhajyoti Bandyopadhyay/Eugene H. Spafford (2003): PFires, in: *Communications Of The ACM*, Bd. 46, Nr. 7, S. 101–106, [online] doi:10.1145/792704.792706.

Ross, Jeanne (2005): Forget Strategy: Focus IT on Your Operating Model, in: *MIT Sloan School Of Management*, Center for Information Systems Research (CISR), Nr. V-3C, [online] https://c isr.mit.edu/publication/2005_12_3C_OperatingModels.

Ross, Jeanne W./Peter Weill/David Robertson (2006): *Enterprise Architecture as strategy: Creating a Foundation for Business Execution*, Harvard Business Press.

Saint-Louis, Patrick/Marclyvens C. Morency/James Lapalme (2017): Defining Enterprise Architecture: A Systematic Literature Review, in: *IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW)*, S. 41–49, [online] doi:10.1109/edocw.2017.16.

Schmelzer, Hermann J./Wolfgang Sesselmann (2020): *Geschäftsprozessmanagement in der Praxis: Kunden zufrieden stellen - Produktivität steigern - Wert erhöhen*.

Schmelzer, Hermann J./Wolfgang Sesselmann (2013): *Geschäftsprozessmanagement in der Praxis : Kunden zufriedenstellen, Produktivität steigern, Wert erhöhen ; [Das Standardwerk]*.

Schmidt, Holger (2023): *Aktuelles und Diskussion zum IT-Grundschutz*, Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik, [online] https://www.bsi.bund.de/Shared-Docs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/4GS_Tag_2023/Aktuelles_und_Ausblick_zum_IT_Grundschutz.pdf?__blob=publicationFile&v=2 [abgerufen am 10.08.2024].

Sherwood, John (1996): SALSA: A method for developing the enterprise security architecture and strategy, in: *Computers & Security*, Bd. 15, Nr. 6, S. 501–506, [online] doi:10.1016/s0167-4048(97)83124-0.

Sherwood, John/Andrew Clark/David Lynas (2009): *TSI W100 The SABSA Whitepaper*, SABSA, SABSA Limited, [online] <https://sabsa.org/download/the-sabsa-whitepaper> [abgerufen am 10.08.2024].

Sherwood, John/David Lynas/John Czaplewski/Maurice Smit (2018): *SABSA Matrices 2018*, SABSA, SABSA Press, [online] <https://sabsa.org/white-paper-requests/> [abgerufen am 10.08.2024].

Sherwood, John/Marouice Smit/David Lynas (2023): *W103 SABSA Responsibility Assignment Modelling*, SABSA, The SABSA Press, [online] <https://sabsa.org/download/tsi-w103-sabsa-responsibility-assignment-model> [abgerufen am 10.08.2024].

Sherwood, Nicholas A (2005): *Enterprise Security Architecture: A Business-Driven Approach*, CRC Press.

- Shiau, Wen-Lung/Xiaoqun Wang/Fei Zheng (2023): What are the trend and core knowledge of information security? A citation and co-citation analysis, in: *Information & Management*, Bd. 60, Nr. 3, S. 103774, [online] doi:10.1016/j.im.2023.103774.
- Shpilberg, David/Steve Berez/Rudy Puryear/Sachin Shah (2007): Avoiding the Alignment Trap in IT, in: *MIT Sloan Management Review*, Nr. 49, [online] <https://sloanreview.mit.edu/article/avoiding-the-alignment-trap-in-it/>.
- Simić-Draws, Daniela/Stephan Neumann/Anna Kahlert/Philipp Richter/Rüdiger Grimm/Melanie Volkamer/Alexander Roßnagel (2013): Holistic and law compatible IT security evaluation, in: *International Journal Of Information Security And Privacy*, Taylor & Francis, Bd. 7, Nr. 3, S. 16–35, [online] doi:10.4018/jisp.2013070102.
- Siponen, Mikko T. (2005): Analysis of Modern IS Security Development Approaches: Towards the next Generation of Social and Adaptable ISS Methods, in: *Information And Organization*, Elsevier BV, Bd. 15, Nr. 4, S. 339–375, [online] doi:10.1016/j.infoandorg.2004.11.001.
- Spanos, Georgios/Lefteris Angelis (2016): The impact of information security events to the stock market: A systematic literature review, in: *Computers & Security*, Bd. 58, S. 216–229, [online] doi:10.1016/j.cose.2015.12.006.
- Sparx Systems (2023): Enterprise Architect, [online] <https://www.sparxsystems.de/>.
- Stewart, Andrew J. (2018): A utilitarian re-examination of enterprise-scale information security management, in: *Information & Computer Security*, Emerald Publishing Limited, Bd. 26, Nr. 1, S. 39–57, [online] doi:10.1108/ics-03-2017-0012.
- Taleb, Nassim Nicholas (2012): *Antifragile: Things That Gain from Disorder*, Random House.
- The Open Group (2019): ArchiMate® 3.1 Specification, Open Group, [online] <https://pubs.opengroup.org/architecture/archimate31-doc/> [abgerufen am 10.08.2024].
- The Open Group (2023): *ArchiMate 3.2 Specification*, Van Haren Publishing.
- The Open Group (2022a): Open Agile Architecture, The Open Group, [online] <https://pubs.opengroup.org/architecture/o-aa-standard-single/> [abgerufen am 10.08.2024].
- The Open Group (2022b): *The TOGAF® Standard, 10th Edition – Architecture Development Method*, Van Haren Publishing.
- The Open Group (2011): *TOGAF® and SABSA® Integration: How SABSA and TOGAF complement each other to create better architectures*, [online] <https://sabsa.org/download/sabsa-togaf-integration-white-paper>.
- The Open Group (2022c): TOGAF Series Guide: Agile Sprint, [online] <https://pubs.opengroup.org/togaf-standard/guides/agile-sprints.html> [abgerufen am 10.08.2024].

- The SABSA Institute (o. D.): Forums Archive - The SABSA Institute, SABSA, [online] <https://sabsa.org/forums/> [abgerufen am 10.08.2024].
- The SABSA Institute (2021): *Modelling SABSA® with ArchiMate®*, SABSA, SABSA Press, [online] <https://sabsa.org/download/tsi-t100-modelling-sabsa-with-archimate/?tmstv=1711969663> [abgerufen am 10.08.2024].
- The SABSA Institute (2023): White Paper requests - the SABSA Institute, The SABSA Institute, [online] <https://sabsa.org/white-paper-requests/> [abgerufen am 10.08.2024].
- Van Wessel, Robert/Xu Yang/Henk J. De Vries (2011): Implementing international standards for information security management in China and Europe: A comparative multi-case study, in: *Technology Analysis & Strategic Management*, Taylor & Francis, Bd. 23, Nr. 8, S. 865–879, [online] doi:10.1080/09537325.2011.604155.
- Wagner, Heinz-Theo/Daniel Beimborn/Tim Weitzel (2014): How Social Capital Among Information Technology and Business Units Drives Operational Alignment and IT Business Value, in: *Journal Of Management Information Systems*, Bd. 31, Nr. 1, S. 241–272, [online] doi:10.2753/mis0742-1222310110.
- Wagter, Roel/Martin Van den Berg/Joost Luijpers/Marlies Van Steenbergen (2005): *Dynamic Enterprise Architecture: How to Make It Work*, Wiley.
- Wang, Hui/Hui Xu/Bao-Liang Lu/Zihao Shen (2009): Research on Security Architecture for Defending Insider Threat, in: *2009 Fifth International Conference On Information Assurance And Security*, S. 30–33, [online] doi:10.1109/ias.2009.53.
- Ward, Peter/Clifton L Smith (2002): The Development of Access Control Policies for Information Technology Systems, in: *Computers & Security*, Bd. 21, Nr. 4, S. 356–371, [online] doi:10.1016/s0167-4048(02)00414-5.
- Weill, Peter/Jeanne W. Ross (2009): *IT savvy: What Top Executives Must Know to Go from Pain to Gain*, Harvard Business Press.
- Wierda, Gerben (2017): *Mastering Archimate Edition III: A Serious Introduction to the Archimate(r) Enterprise Architecture Modeling Language*, R&a.
- Winter, Robert/Ronny Fischer (2006): Essential Layers, Artifacts, and Dependencies of Enterprise Architecture, in: *2006 10th IEEE International Enterprise Distributed Object Computing Conference Workshops (EDOCW'06)*, [online] doi:10.1109/edocw.2006.33.
- Zachman, John A. (1987): A framework for information systems architecture, in: *Ibm Systems Journal*, Institute of Electrical and Electronics Engineers, Bd. 26, Nr. 3, S. 276–292, [online] doi:10.1147/sj.263.0276.

ANHANG A

Zusätzliche Informationen zur erweiterten IT-Grundschutz-Methodik

A.1 MÖGLICHER AUFBAU DER ORGANISATIONSSTRUKTUR

Wie in Kapitel 5.2 dargelegt, besteht die Möglichkeit, die Enterprise Security Architects in der Organisationsstruktur auf unterschiedliche Art und Weise zu verorten. Die nachfolgenden Unterkapitel dienen der Konkretisierung und Beschreibung der zuvor dargelegten Möglichkeiten zur Verortung der Enterprise Security Architects innerhalb einer Organisation.

A.1.1 NORMALISIERUNG VON ROLLEN UND VERANTWORTLICHKEITEN

In Tabelle 1 erfolgt eine Harmonisierung der in der IT-Grundschutz-Methodik genannten Rollen. Darüber hinaus werden angepasste Bezeichnungen mitgegeben, um als mögliche Schnittstelle zu anderen Frameworks zu dienen und die Kommunikation zu vereinfachen.

Tabelle 1: Normalisierung und Beschreibung der IT-Grundschutz Rollen
Quelle: Eigene Darstellung

IT-Grundschutz Rolle	Neuer Name	Beschreibung
Oberste Leitungsebene	Organisationsleitung	Höchste Managementebene zur Verwaltung einer Organisation.
Informationssicherheitsbeauftragten (ISB)	Chief Information Security Officer (CISO)	Hauptansprechperson für alle Aspekte der Informationssicherheit. Sie umfasst die Koordination

IT-Grundschutz Rolle	Neuer Name	Beschreibung
		und Förderung von Sicherheitsmaßnahmen innerhalb der Organisation. Die Position ist direkt der Organisationsleitung unterstellt.
Fachverantwortliche	Business Owner	Leitende Position innerhalb einer Organisation oder Abteilung, die für die Umsetzung fachlich relevanter Entscheidungen verantwortlich ist.
(Betrieblicher) Datenschutzbeauftragten (bDSB)	Chief Privacy Officer (CPO)	Unterstützt die Organisation in der Einhaltung gesetzlicher Vorgaben zum Datenschutz, um personenbezogene Informationen zu schützen.
Bereichs-Informationssicherheitsbeauftragten	Business Information Security Officer (BISO)	Setzt die Vorgaben zur Informationssicherheit innerhalb eines Subbereichs bzw. einer Abteilung um und verwaltet die Sicherheit innerhalb des Bereichs.
Projekt-Informationssicherheitsbeauftragten	Project Security Officer (PSO)	Setzt die Vorgaben zur Informationssicherheit innerhalb eines Projekts um und verwaltet die Sicherheit innerhalb des Projekts.

IT-Grundschutz Rolle	Neuer Name	Beschreibung
ICS-Informationssicherheitsbeauftragte (ICS-ISB)	OT-Security Officer (OTSO)	Mit einem erweiterten Scope, übersetzt die Position die Vorgaben der Informationssicherheit in OT und setzt diese technisch sowie organisatorisch um.
IS-Management-Team	ISMS-Team	Umfasst die Koordination übergreifender Maßnahmen in der Gesamtorganisation, die Zusammenführung von Informationen sowie die Durchführung von Kontrollaufgaben. Es besteht mindestens aus der Position des CISO sowie der des stellvertretenden CISO.
Beauftragter für IT-Sicherheit	IT-Security Officer (ITSO)	Setzt die Vorgaben der Informationssicherheit technisch in IT-Systeme um.
Sicherheitsbeauftragten	Safety Expert (SE) (Fachkraft für Arbeitssicherheit)	Unterstützt die Organisation in der Einhaltung gesetzlicher Vorgaben zur Arbeitssicherheit, um Menschen und Umwelt zu schützen.
	Security Service Expert (SSE) (Fachkraft für Schutz und Sicherheit)	Stellt den physischen Schutz durch präventive Maßnahmen und Gefahrenabwehr sicher.

IT-Grundschutz Rolle	Neuer Name	Beschreibung
IS-Koordinierungsausschuss	IS Coordination Committee (ISCC)	Nicht als Dauereinrichtung in der Organisation vorgesehen, sondern wird bei Bedarf, beispielsweise im Kontext der Planung eines groß angelegten Projekts, einberufen. Ihre Funktion besteht in der Koordination des Zusammenspiels von IS-Management-Team, Fachverantwortlichen und Sicherheitsbeauftragten.

Die nachfolgende Tabelle 2 präsentiert eine Übersicht über die potenziellen Unterteilungen von Rollen innerhalb der Enterprise Architecture und Enterprise Security Architecture. Die Unterteilung von Fachgebieten in den EA-Bereichen erfolgt gemäß den folgenden Kategorien: ‚Business‘, ‚Application‘, ‚Data‘, ‚Integration‘, ‚Infrastructure‘ und ‚Security‘.

Tabelle 2: Beschreibung der EA-Rollen
Quelle: Eigene Darstellung

Rollen in Enterprise Architecture	Beschreibung
Chief Information Officer (CIO)	Verantwortlich für das Informationsmanagement in einer Organisation.
Architecture Manager (AM)	Verwalten die Architektur-Teams und berichten für gewöhnlich an den CIO (vgl. Kotusev: 291 – 292). Durch die Erweiterung könnte die Berichterstattung auf den CISO ausgeweitet werden.

Rollen in Enterprise Architecture	Beschreibung
Enterprise Architect (EA)	Planen die übergreifende organisationsweite aller EA-Bereiche. Sie sind Generalisten und kennen die verschiedenen EA-Bereiche (vgl. ebd.: 291).
Enterprise Security Architect (ESA)	Ähnlich wie ein EA, jedoch mit dem Fokus auf die übergreifende Sicherheit. Aufgrund der Komplexität der Informationssicherheit und der themenübergreifenden Auswirkungen (Prozesse, Anwendungen, Systeme, Netze etc.) sollte ein Security Architekt auf EA-Ebene etabliert werden.
Business Area Architect (BAA)	Planen die IT Ende-zu-Ende für einen Subbereich bzw. Business Area / Abteilung (vgl. ebd.: 291).
Business Area Security Architect (BASA)	Ähnlich wie ein BAA, aber mit Fokus auf die Ende-zu-Ende Sicherheit für einen Subbereich bzw. Business Area / Abteilung. Es besteht Unklarheit darüber, ob die Security-Themen von einem BAA übernommen werden könnten. Daher wird diese Rolle vorerst vorgeschlagen. Es besteht die Möglichkeit, dass die BAAs durch Weiterbildung auch Security modellieren, sodass ein BASA nicht notwendig wäre.
Program Architect (PA)	Planen große Initiativen mit Auswirkungen auf verschiedene EA-Bereiche und mehreren Organisationseinheiten innerhalb einer Organisation (vgl. ebd.: 293).

Rollen in Enterprise Architecture	Beschreibung
Domain Architect (DA)	Planen organisationsweit einen EA-Bereich. Sie werden in business-supporting und business-enabling Domänen unterteilt und sind in einem bestimmten EA-Bereich spezialisiert (vgl. ebd.: 288 – 289).
Solution Architect (SA)	Planen mit limitierten Scope die Architektur von IT-Initiativen. Sie spezialisieren sich in bestimmten Technologien, weshalb sie sich inhärent in einen bestimmten EA-Bereich spezialisieren (vgl. ebd.: 287).

A.1.2 AUFNAHME DER VERANTWORTLICHKEITEN AUS DEM IT-GRUNDVERSCHUTZ

Die folgende Tabelle 3 stellt eine Synthese der verteilt beschriebenen Verantwortlichkeiten an die Rollen innerhalb des BSI-Standards 200-2 dar (vgl. BSI 2017a).

Tabelle 3: Synthese Verantwortlichkeiten aus IT-Grundschutz-Methodik
Quelle: Eigene Darstellung

Normalisierte Rolle	Verantwortlichkeit
Organisationsleitung	Verantwortlich für die zielgerichtete und ordnungsgemäße Funktionsweise aller Geschäftsbereiche (vgl. ebd.: 20)
Organisationsleitung	Holschuld sich über die Risiken und Konsequenzen zu informieren bei fehlender Informationssicherheit (vgl. ebd.: 20)
Organisationsleitung	Verantwortlich für Informationssicherheit und Erreichung der Sicherheitsziele (vgl. ebd.:20)
Organisationsleitung	Definiert grundlegende Sicherheitsziele (vgl. ebd.: 21)
Organisationsleitung	Bestimmt ausreichendes Sicherheitsniveau (vgl. ebd.: 21)
CISO	Koordiniert die Informationssicherheit und treibt diese voran (vgl. ebd.: 40)
CISO	Berät die Organisationsleitung zu Fragen der Informationssicherheit (vgl. ebd.: 41)
CISO	Unterstützt bei Umsetzung der Informationssicherheit (vgl. ebd.: 41)
CISO	Steuert den Informationssicherheitsprozess und die damit zusammenhängenden Aufgaben (vgl. ebd.: 41)
CISO	Unterstützt Organisationsleitung bei der Erstellung der Leitlinie zur Informationssicherheit (vgl. ebd.: 41)

Normalisierte Rolle	Verantwortlichkeit
CISO	Erstellt Sicherheitskonzept, Notfallversorgungskonzept und andere Teilkonzepte und System-Sicherheitsrichtlinie sowie weitere Richtlinien und Regelungen zur Informationssicherheit (vgl. ebd.: 41)
CISO	Initiiert die Realisierung von Maßnahmen und überprüft ihre Umsetzung (vgl. ebd.: 41)
CISO	Berichtet der Organisationsleitung und ISMS-Team über den Status quo der Informationssicherheit (vgl. ebd.: 41)
CISO	Koordiniert sicherheitsrelevante Projekte (vgl. ebd.: 41)
CISO	Untersucht Sicherheitsvorfälle (vgl. ebd.: 41)
CISO	Initiiert und kontrolliert Sensibilisierungs- sowie Schulsungsmaßnahme zur Informationssicherheit (vgl. ebd.: 41)
CPO	Überwacht Einhaltung der regulatorischen Vorgaben zum Datenschutz (vgl. ebd.: 48)
CPO	Ansprechpartner für alle Personen einer Organisation zum Datenschutz und berät diese (vgl. ebd.: 48)
BISO, PSO, ITSO	Setzen Vorgaben an die Informationssicherheit des CISO um (vgl. ebd.: 44)
BISO, PSO, ITSO	Setzen Sicherheitsmaßnahmen gemäß der Sicherheitsrichtlinie um (vgl. ebd.: 44)
BISO, PSO, ITSO	Fassen Projekt- oder IT-/OT-systemspezifischen Informationen zusammenfassen leiten diese an den CISO weiter (vgl. ebd.: 44)
BISO, PSO, ITSO	Ansprechpartner für operative Mitarbeitende und Management (vgl. ebd.: 44)
BISO, PSO, ITSO	Wirken bei der Auswahl der Sicherheitsmaßnahmen zur Umsetzung der spezifischen Sicherheitsleitlinien mit (vgl. ebd.: 44)

Normalisierte Rolle	Verantwortlichkeit
BISO, PSO, ITSO	Ermitteln des Schulungs- und Sensibilisierungsbedarfs von Beschäftigten (vgl. ebd.: 44)
BISO, PSO, ITSO	Kontrollieren und werten Protokolldateien aus (vgl. ebd.: 45)
BISO, PSO, ITSO	Melden sicherheitsrelevante Zwischenfälle an CISO (vgl. ebd.: 45)
OTSO	Umsetzen von Sicherheitsvorgaben aus Leitlinie für Informationssicherheit und weiteren Richtlinien im Bereich OT (vgl. ebd.: 46)
OTSO	Harmonisieren der OT-Sicherheit und Gesamt-ISMS (vgl. ebd.: 46)
OTSO	Durchführen von Risiko-Assessments im OT-Bereich, die den Vorgaben des Risikomanagements entsprechen (vgl. ebd.: 46)
OTSO	Erstellen Sicherheitsrichtlinien und Konzepte für OT-Bereich (vgl. ebd.: 46)
OTSO	Schulen zu den Richtlinien und Konzepten für den OT-Bereich (vgl. ebd.: 46)
OTSO	Ansprechpartner für operative Mitarbeitende und Management zu OT-Sicherheit (vgl. ebd.: 46)
OTSO	Entwickeln von Sicherheitsmaßnahmen für OT-Sicherheit (vgl. ebd.: 46)
OTSO	Mitwirken bei der Umsetzung der OT-Sicherheitsmaßnahmen (vgl. ebd.: 46)
OTSO	Ermitteln des Schulungs- und Sensibilisierungsbedarfs von Beschäftigten (vgl. ebd.: 46)
OTSO	Sicherheitsvorfälle im OT-Bereich mit CISO bearbeiten (vgl. ebd.: 46)
ISMS-Team	Entwickeln der Informationssicherheitsziele und -strategie (vgl. ebd.: 43)

Normalisierte Rolle	Verantwortlichkeit
ISMS-Team	Entwickeln der Leitlinie für Informationssicherheit (vgl. ebd.: 43)
ISMS-Team	Überprüfen der Umsetzung der Sicherheitsrichtlinien (vgl. ebd.: 43)
ISMS-Team	Initiiieren des Sicherheitsprozesses (vgl. ebd.: 43)
ISMS-Team	Steuern und kontrollieren des Sicherheitsprozesses (vgl. ebd.: 43)
ISMS-Team	Unterstützen bei der Erstellung des Sicherheitskonzepts (vgl. ebd.: 43)
ISMS-Team	Überprüfen der Wirksamkeit und Angemessenheit von Sicherheitsmaßnahmen im Sicherheitskonzept (vgl. ebd.: 43)
ISMS-Team	Konzipieren des Schulungs- und Sensibilisierungsprogramme für Informationssicherheit (vgl. ebd.: 43)
ISMS-Team	Beraten der Business Owner, des IT-Betrieb, BSIO, OTSO und Organisationsleitung zu Fragen der Informationssicherheit (vgl. ebd.: 43)
ISCC	Koordinierung der Zusammenarbeit zwischen dem ISMS-Team, Business Owner, SE & SSE (vgl. ebd.: 46)

A.1.3 STRUKTURIERUNG DER ARCHITEKTURROLLEN

Um das Verständnis der Strukturierung von Architekturrollen zu stärken, wird anhand der Abbildung 21 eine Erklärung der Verantwortlichkeiten mitgegeben.

Die EAs sowie ESAs tragen die Verantwortung für die EA-bereichsübergreifende Planung innerhalb der gesamten Organisation. Die BAAs und BASAs konzipieren mit einer Ende-zu-Ende-Perspektive einen Teilbereich (z. B. eine Business Unit) einer Organisation. Die Planung von umfangreichen Initiativen, die Auswirkungen auf mehrere EA-Bereiche und Teilbereiche einer Organisation haben, erfolgt durch PAs. DAs haben die Aufgabe, die Modelle in den EA-Bereichen organisationsweit zu harmonisieren, damit eine effektive Architektur gewährleistet werden kann. Die SAs erstellen die Architektur, in der die einzusetzenden Technologien und Maßnahmen spezifisch geplant werden. Da AMs keine Architekturarbeiten durchführen, ergeben sich keine Überschneidungen mit den Arbeitsgebieten der Architekten.

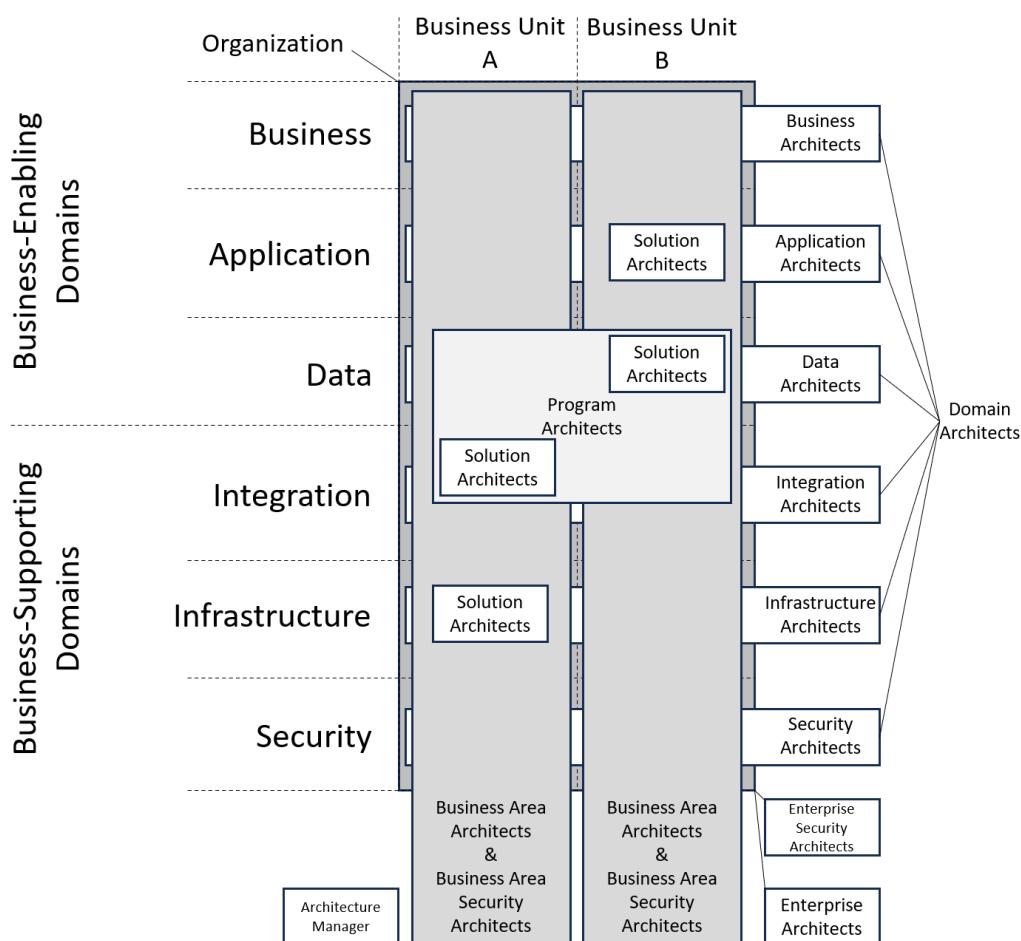


Abbildung 21: Verortung der Architekturrollen

Quelle: In Anlehnung an (Kotusev 2021: 294)

A.2 MAPPING DER R1 BAUSTEINE ZU SABSA METAEBENEN

Die nachfolgenden Unterkapitel beinhalten ein ausgearbeitetes Mapping zwischen SABSA und sämtlichen Bausteinen des IT-Grundschutz-Kompendiums 2023 (vgl. BSI 2023b), deren vorrangige Umsetzung (R1) empfohlen wird, da sie die Basis für einen effektiven Sicherheitsprozess bilden (BSI 2017a: 137).

In A.2.1 Ermittelte Control Objectives aus dem Kompendium erfolgt die Ausarbeitung der beschriebenen Soll-Zustände des Bausteins als Control Objectives. Die Control Objectives stellen eine wesentliche Grundlage für die systematische Planung, Implementierung und Verwaltung von Sicherheitsmaßnahmen in einer Organisation dar.

Zur Modellierung und Implementierung der notwendigen Sicherheitsmaßnahmen, wurde eine erste Control Library in A.2.2 Ausgearbeitete Control Library aus dem IT-Grundschatz erstellt.

Des Weiteren werden in den Bausteinen spezifische Dokumentationen gefordert. Die benötigten Dokumentationen sind unter A.2.3 Benötigte Dokumentationen aus R1-Bausteinen aufgeführt und werden im Verlauf des Sicherheitsprozesses erstellt. Sie ergänzen die Arbeitsprodukte von A.3 Arbeitsprodukte.

Ein Mapping aller Anforderungen der gewählten Bausteine kann in A.2.4 Mapping der R1-Bausteine des Kompendiums mit SABSA Ebenen gesichtet werden, um ihre Auswirkungen auf den Metaebenen zu verstehen.

A.2.1 ERMITTELTE CONTROL OBJECTIVES VON R1 BAUSTEINEN

Die Tabelle 4 beschreibt die identifizierten Control Objectives der R1-Bausteine.

Tabelle 4: Control Objectives der R1 Bausteine

Quelle: Eigene Darstellung

Baustein	Control Objectives
ISMS.1	<ul style="list-style-type: none"> • Einrichtung eines funktionierenden ISMS • Kontinuierliche Verbesserung des ISMS im Betrieb
ORP.1	<ul style="list-style-type: none"> • Regulierung der Informationsflüsse • Regulierung der Aufbauorganisation • Regulierung der Ablauforganisation • Regulierung der Rollenverteilung
ORP.2	<ul style="list-style-type: none"> • Regulierung des Employee-Lifecycles
ORP.3	<ul style="list-style-type: none"> • Verständnis von Sicherheitsrisiken der Mitarbeitenden durch Sensibilisierung stärken • Verständnis von Sicherheitsrisiken der Mitarbeitenden durch Schulung stärken
ORP.4	<ul style="list-style-type: none"> • Zugriff auf IT-Ressourcen ausschließlich für autorisierte Entitäten erlauben • Zugriff auf Informationen ausschließlich für autorisierte Entitäten erlauben • Zugriff auf IT-Ressourcen ausschließlich bei Bedarf zur Durchführung einer Aktivität erlauben • Zugriff auf Informationen ausschließlich bei Bedarf zur Durchführung einer Aktivität erlauben
CON.3	<ul style="list-style-type: none"> • Absicherung gegen Datenverlust
CON.6	<ul style="list-style-type: none"> • Sichere Löschung und Vernichtung von Informationen
OPS.1.1.1	<ul style="list-style-type: none"> • Etablierung der Informationssicherheit in allen Aspekten des IT-Betriebs • Sicherstellung eines funktionsfähigen, ordnungsgemäß und systematisch durchgeführten IT-Betriebs

Baustein	Control Objectives
OPS.1.1.2	<ul style="list-style-type: none"> • Etablierung der Informationssicherheit in allen Aspekten der IT-Administration • Sicherstellung einer ordnungsgemäßen und systematisch durchgeführten IT-Administration
OPS.1.1.3	<ul style="list-style-type: none"> • Regulierung des Patchmanagements • Regulierung des Änderungsmanagements
OPS.1.1.4	<ul style="list-style-type: none"> • Schutz der technischen Systeme vor Schadprogrammen
OPS.1.1.5	<ul style="list-style-type: none"> • Protokollierung aller sicherheitsrelevanten Ereignisse
OPS.1.1.6	<ul style="list-style-type: none"> • Evaluierung und testen von einzusetzender Software • Systematische und methodische Überprüfung auf bestehende Schwachstellen bei einzusetzender Software
DER.1	<ul style="list-style-type: none"> • Sammlung, Korrelation und Auswertung von sicherheitsrelevanten Ereignissen • Detektion von Sicherheitsvorfällen
DER.2.1	<ul style="list-style-type: none"> • Behandlung von Sicherheitsvorfällen

A.2.2 AUSGEARBEITETE CONTROL LIBRARY AUS DEM IT-GRUNDVERSCHUTZ

In der vorliegenden Abbildung 22 erfolgt eine Aufteilung der Sicherheitsanforderungen in die logischen und physischen Metaebenen, wodurch eine Visualisierung ermöglicht wird. Die Erstellung in englischer Sprache dient der Vereinfachung der Zusammenarbeit und Kommunikation mit dem SABSA-Institut.

In einzelnen Punkten wurden spezifische Anforderungen des BSI Standards 200-2 (vgl. BSI 2017a) eingearbeitet, da diese für einen sicheren sowie effektiven Sicherheitsprozess relevant sind und in der Auditierung einer Prüfung unterzogen werden.

Mit dem Ziel einer verbesserten Übersicht sowie einer optimierten Eingliederung von Security Mechanisms wurden seitens des Autors dieser Arbeit darüber liegende Security Services entwickelt. Diese sind anhand einer fehlenden Quellenangabe erkennbar.

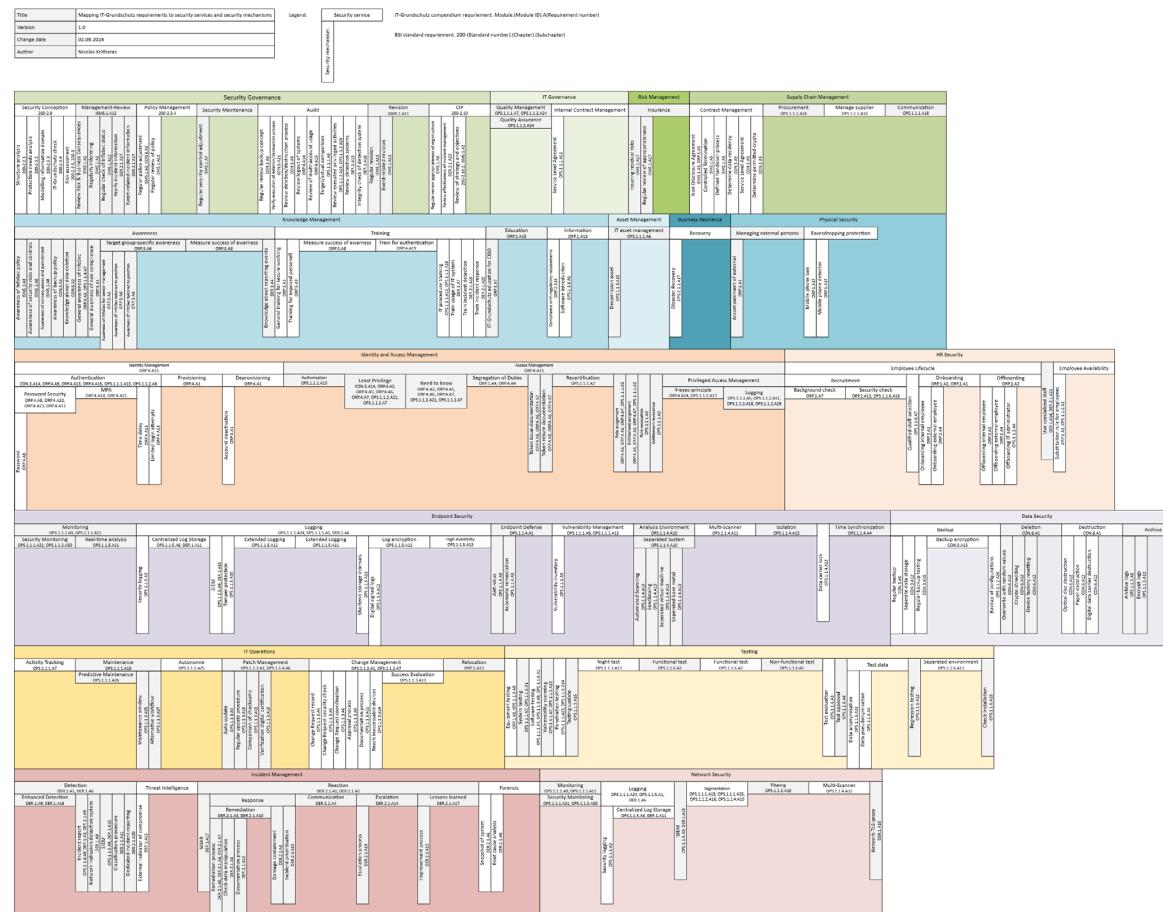


Abbildung 22: R1 Bausteine zu SABSA Mapping
Quelle: Eigene Darstellung

A.2.3 BENÖTIGTE DOKUMENTATIONEN AUS R1-BAUSTEINEN

Die in der nachfolgenden Tabelle 5 aufgelisteten Dokumente sind relevant für die Zertifizierung eines ISMS nach ISO/IEC 27001 auf Basis von IT-Grundschutz. Des Weiteren werden die Anforderungen an die jeweiligen Dokumente dargelegt, welche die Erstellung der Dokumente sowie deren inhaltliche Ausgestaltung definieren. In Abhängigkeit der ausgestalteten Informationssicherheit in einer Organisation können darüber hinaus weitere Dokumentationen erforderlich sein, um die Einhaltung von Anforderungen oder Teilanforderungen nachzuweisen. Die Aufstellung ist folglich nicht vollständig, sondern zeigt lediglich die explizit erforderlichen Dokumentationen auf.

Tabelle 5: Verpflichtende Dokumentation nach R1 Bausteine

Quelle: Eigene Darstellung

Dokument	Anforderung
Leitlinie zur Informationssicherheit	<ul style="list-style-type: none"> • ISMS.1.A2 • ISMS.1.A3
Sicherheitskonzept	<ul style="list-style-type: none"> • ISMS.1.A6 • ISMS.1.A7 • ISMS.1.A10 • ISMS.1.A11 • ISMS.1.A13 • ISMS.1.A16
Management-Bericht	<ul style="list-style-type: none"> • ISMS.1.A12
Asset-Register	<ul style="list-style-type: none"> • ORP.1.A8 • OPS.1.1.1.A6
Benutzendenhandbuch Informations-sicherheit	<ul style="list-style-type: none"> • ISMS.1.A16 • ORP.1.A1 • ORP.1.A4 • ORP.1.A13 • ORP.1.A16 • ORP.3.A3 • OPS.1.1.2.A21 • OPS.1.1.4.A9 • DER.2.1.A1 • DER.2.1.A2 • DER.2.1.A3 • DER.2.1.A9

Dokument	Anforderung
Verpflichtungserklärung und Bestätigung zu Kenntnisnahme und Beachtung der Vorgaben zur Informationssicherheit	<ul style="list-style-type: none"> • ORP.1.A2 • ORP.1.A16 • ORP.2.A14
Verpflichtungserklärung für extern eingesetztes Personal	<ul style="list-style-type: none"> • ORP.2.A4 • ORP.2.A5
Schulungs- und Sensibilisierungskonzept zur Informationssicherheit	<ul style="list-style-type: none"> • ORP.3.A4 • ORP.3.A8 • ORP.4.A5 • ORP.4.A6 • ORP.4.A7
Konzept zum Identitäts- und Berechtigungsmanagement	<ul style="list-style-type: none"> • ORP.4.A1 • ORP.4.A3 • ORP.4.A8 • ORP.4.A11 • ORP.4.A12 • ORP.4.A16
Protokollierung Zutrittsmittel	<ul style="list-style-type: none"> • ORP.4.A2 • ORP.4.A5
Protokollierung Zugangsmittel	<ul style="list-style-type: none"> • ORP.4.A2 • ORP.4.A6
Protokollierung Zugriffsmittel	<ul style="list-style-type: none"> • ORP.4.A2 • ORP.4.A7
Datensicherungskonzept	<ul style="list-style-type: none"> • CON.3.A1 • CON.3.A2 • CON.3.A4 • CON.3.A6 • CON.3.A7
Konzept zum Löschen und Vernichten von Daten	<ul style="list-style-type: none"> • CON.6.A1 • CON.6.A4
IT-Betriebskonzept	<ul style="list-style-type: none"> • OPS.1.1.1.A1 • OPS.1.1.1.A2 • OPS.1.1.1.A3 • OPS.1.1.1.A5 • OPS.1.1.1.A7 • OPS.1.1.1.A10 • OPS.1.1.1.A11 • OPS.1.1.1.A12

Dokument	Anforderung
	<ul style="list-style-type: none"> • OPS.1.1.1.A14 • OPS.1.1.1.A15 • OPS.1.1.1.A16 • OPS.1.1.1.A17 • OPS.1.1.1.A18 • OPS.1.1.1.A19 • OPS.1.1.1.A20 • OPS.1.1.2.A7 • OPS.1.1.2.A8 • OPS.1.1.2.A23 • OPS.1.1.4.A2
Dokumentation über die Durchführung des ordnungsgemäßen IT-Betriebs	<ul style="list-style-type: none"> • OPS.1.1.1.A7 • OPS.1.1.1.A9 • OPS.1.1.1.A10 • OPS.1.1.1.A12 • OPS.1.1.1.A19 • OPS.1.1.1.A22 • OPS.1.1.1.A24 • OPS.1.1.2.A5 • OPS.1.1.2.A11 • OPS.1.1.2.A18 • OPS.1.1.2.A28 • OPS.1.1.2.A30
Konzept zum Patch- und Änderungsmanagement	<ul style="list-style-type: none"> • OPS.1.1.3.A1 • OPS.1.1.3.A3 • OPS.1.1.3.A8
Dokumentation über die Durchführung des Patch- und Änderungsmanagements	<ul style="list-style-type: none"> • OPS.1.1.3.A1 • OPS.1.1.3.A5 • OPS.1.1.3.A6 • OPS.1.1.3.A9 • OPS.1.1.3.A11 • OPS.1.1.3.A13 • OPS.1.1.3.A15
Konzept für den Schutz vor Schadprogrammen	<ul style="list-style-type: none"> • OPS.1.1.4.A1 • OPS.1.1.4.A5 • OPS.1.1.4.A9
Konzept zur Protokollierung	<ul style="list-style-type: none"> • OPS.1.1.5.A1
Protokolldaten	<ul style="list-style-type: none"> • OPS.1.1.5.A3 • OPS.1.1.5.A11

Dokument	Anforderung
Konzept für Software-Test und Software-Freigaben	<ul style="list-style-type: none"> • OPS.1.1.6.A1 • OPS.1.1.6.A3 • OPS.1.1.6.A4 • OPS.1.1.6.A5 • OPS.1.1.6.A12 • OPS.1.1.6.A14 • OPS.1.1.6.A16
Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen	<ul style="list-style-type: none"> • DER.1.A1 • DER.1.A3 • DER.1.A6 • DER.1.A7 • DER.1.A10
Dokumentation detekter Sicherheitsereignisse	<ul style="list-style-type: none"> • DER.1.A5 • DER.1.A11 • DER.1.A12
Dokumentierte Ergebnisse der Auditierung zu Systemen für die Detektion von sicherheitsrelevanten Ereignissen	<ul style="list-style-type: none"> • DER.1.A13
Richtlinie zur Behandlung von Sicherheitsvorfällen	<ul style="list-style-type: none"> • DER.2.1.A1 • DER.2.1.A4 • DER.2.1.A5 • DER.2.1.A7 • DER.2.1.A11 • DER.2.1.A14 • DER.2.1.A16 • DER.2.1.A17 • DER.2.1.A19
Konzept zur IT-Forensik	<ul style="list-style-type: none"> • DER.2.1.A3 • DER.2.1.A18

A.2.4 MAPPING DER R1-BAUSTEINE DES KOMPENDIUMS MIT SABSA EBENEN

Die Sicherheitsanforderungen in den Bausteinen definieren die nötige Etablierung von technischen und organisatorischen Sicherheitsmaßnahmen innerhalb einer Organisation für eine effektive Informationssicherheit zu gewährleisten. Um diese Anforderungen zu in der erweiterten Methodik zu behandeln und einzuarbeiten, um den Vorgaben zu entsprechen, wurde ein Mapping jeder Anforderung durchgeführt.

Die Tabelle 6 fungiert als erster möglicher Anhaltspunkt für die Erstellung weiterer Checklisten. Die R1 Bausteine umfassen insgesamt 221 Anforderungen, wobei die entfallenen Anforderungen nicht berücksichtigt wurden. Bei einer Betrachtung aller Bausteine des Kompendiums ergibt sich eine Gesamtzahl von 7.358 Anforderungen, wiederum exkludiert die entfallenen Anforderungen. Da jede Anforderung auf den verschiedenen Ebenen betrachtet wird, könnte die Erstellung von Checklisten, welche die vollständige Betrachtung aller Anforderungen ermöglichen, von Vorteil sein.

Tabelle 6: Bausteine zu SABSA Layer Mapping

Quelle: Eigene Darstellung

Anforderung	Anforderungstyp	SABSA-Metaebene
ISMS.1.A1	Basis	Contextual, Logical, Physical
ISMS.1.A2	Basis	Conceptual, Logical, Physical
ISMS.1.A3	Basis	Conceptual, Logical, Physical
ISMS.1.A4	Basis	Contextual
ISMS.1.A5	Basis	Contextual, Logical, Physical
ISMS.1.A6	Basis	Conceptual, Logical, Component
ISMS.1.A7	Basis	Conceptual, Logical, Component

Anforderung	Anforderungstyp	SABSA-Metaebene
ISMS.1.A8	Basis	Logical
ISMS.1.A9	Basis	Conceptual
ISMS.1.A10	Standard	Conceptual
ISMS.1.A11	Standard	Logical
ISMS.1.A12	Standard	Logical
ISMS.1.A13	Standard	-/- (Mapping nicht möglich, betrifft alle Prozessschritte der erweiterten Methodik)
ISMS.1.A15	Standard	Conceptual
ISMS.1.A16	Erhöhter Schutzbedarf	Logical
ISMS.1.A17	Erhöhter Schutzbedarf	Logical
ORP.1.A1	Basis	Conceptual
ORP.1.A2	Basis	Conceptual, Logical
ORP.1.A3	Basis	Physical
ORP.1.A4	Basis	Logical
ORP.1.A8	Standard	Physical
ORP.1.A13	Standard	Logical
ORP.1.A15	Basis	Conceptual, Logical
ORP.1.A16	Standard	Logical
ORP.1.A17	Erhöhter Schutzbedarf	Physical
ORP.2.A1	Basis	Logical
ORP.2.A2	Basis	Logical
ORP.2.A3	Basis	Physical
ORP.2.A4	Basis	Physical
ORP.2.A5	Basis	Physical
ORP.2.A7	Standard	Logical

Anforderung	Anforderungstyp	SABSA-Metaebene
ORP.2.A13	Erhöhter Schutzbedarf	Logical
ORP.2.A14	Basis	Physical
ORP.2.A15	Basis	Logical
ORP.3.A1	Basis	Physical
ORP.3.A3	Basis	Physical
ORP.3.A4	Standard	Physical
ORP.3.A6	Standard	Logical
ORP.3.A7	Standard	Physical
ORP.3.A8	Standard	Logical
ORP.3.A9	Erhöhter Schutzbedarf	Physical
ORP.4.A1	Basis	Logical, Physical, Component
ORP.4.A2	Basis	Logical, Physical, Component
ORP.4.A3	Basis	Physical
ORP.4.A4	Basis	Logical
ORP.4.A5	Basis	Logical, Physical
ORP.4.A6	Basis	Logical, Physical
ORP.4.A7	Basis	Logical, Physical
ORP.4.A8	Basis	Logical, Physical
ORP.4.A9	Basis	Logical
ORP.4.A10	Standard	Logical
ORP.4.A11	Standard	Logical
ORP.4.A12	Standard	Physical
ORP.4.A13	Standard	Logical, Physical
ORP.4.A14	Standard	Physical
ORP.4.A15	Standard	Logical, Physical

Anforderung	Anforderungstyp	SABSA-Metaebene
ORP.4.A16	Standard	Logical
ORP.4.A17	Standard	Component
ORP.4.A18	Standard	Component
ORP.4.A19	Standard	Logical
ORP.4.A20	Erhöhter Schutzbedarf	Physical
ORP.4.A21	Erhöhter Schutzbedarf	Physical
ORP.4.A22	Basis	Logical
ORP.4.A23	Basis	Logical
ORP.4.A24	Erhöhter Schutzbedarf	Logical
CON.3.A1	Basis	Contextual, Component
CON.3.A2	Basis	Physical
CON.3.A4	Basis	Component
CON.3.A5	Basis	Logical
CON.3.A6	Standard	Component
CON.3.A7	Standard	Component
CON.3.A9	Standard	Physical
CON.3.A12	Basis	Physical
CON.3.A13	Erhöhter Schutzbedarf	Logical
CON.3.A14	Basis	Logical
CON.3.A15	Basis	Physical
CON.6.A1	Basis	Logical
CON.6.A2	Basis	Logical
CON.6.A4	Standard	Component
CON.6.A8	Standard	Logical
CON.6.A11	Basis	Physical
CON.6.A12	Basis	Component

Anforderung	Anforderungstyp	SABSA-Metaebene
CON.6.A13	Standard	Component
CON.6.A14	Erhöhter Schutzbedarf	Component
OPS.1.1.1.A1	Basis	Conceptual, Component
OPS.1.1.1.A2	Basis	Logical, Component
OPS.1.1.1.A3	Standard	Component
OPS.1.1.1.A4	Standard	Conceptual
OPS.1.1.1.A5	Standard	Component
OPS.1.1.1.A6	Standard	Logical
OPS.1.1.1.A7	Standard	Logical, Physical, Component
OPS.1.1.1.A8	Standard	Physical
OPS.1.1.1.A9	Standard	Logical, Physical
OPS.1.1.1.A10	Standard	Logical, Physical
OPS.1.1.1.A11	Standard	Conceptual
OPS.1.1.1.A12	Standard	Logical, Physical
OPS.1.1.1.A13	Standard	Logical
OPS.1.1.1.A14	Standard	Logical, Conceptual
OPS.1.1.1.A15	Standard	Logical, Component
OPS.1.1.1.A16	Standard	Logical
OPS.1.1.1.A17	Standard	Physical
OPS.1.1.1.A18	Standard	Logical
OPS.1.1.1.A19	Standard	Logical
OPS.1.1.1.A20	Standard	Logical
OPS.1.1.1.A21	Erhöhter Schutzbedarf	Logical
OPS.1.1.1.A22	Erhöhter Schutzbedarf	Physical
OPS.1.1.1.A23	Erhöhter Schutzbedarf	Logical

Anforderung	Anforderungstyp	SABSA-Metaebene
OPS.1.1.1.A24	Erhöhter Schutzbedarf	Logical
OPS.1.1.1.A25	Erhöhter Schutzbedarf	Logical
OPS.1.1.1.A26	Erhöhter Schutzbedarf	Logical
OPS.1.1.2.A2	Basis	Physical
OPS.1.1.2.A4	Basis	Logical, Physical
OPS.1.1.2.A5	Basis	Logical
OPS.1.1.2.A6	Basis	Logical
OPS.1.1.2.A7	Standard	Physical
OPS.1.1.2.A8	Standard	Component
OPS.1.1.2.A11	Standard	Logical
OPS.1.1.2.A16	Standard	Logical
OPS.1.1.2.A17	Erhöhter Schutzbedarf	Physical
OPS.1.1.2.A18	Erhöhter Schutzbedarf	Logical
OPS.1.1.2.A19	Erhöhter Schutzbedarf	Component
OPS.1.1.2.A21	Basis	Logical
OPS.1.1.2.A22	Basis	Physical
OPS.1.1.2.A23	Standard	Conceptual
OPS.1.1.2.A24	Standard	Logical
OPS.1.1.2.A25	Standard	Physical
OPS.1.1.2.A26	Standard	Physical
OPS.1.1.2.A27	Standard	Physical
OPS.1.1.2.A28	Standard	Logical
OPS.1.1.2.A29	Erhöhter Schutzbedarf	Logical
OPS.1.1.2.A30	Erhöhter Schutzbedarf	Logical
OPS.1.1.3.A1	Basis	Logical
OPS.1.1.3.A2	Basis	Contextual, Component

Anforderung	Anforderungstyp	SABSA-Metaebene
OPS.1.1.3.A3	Basis	Physical
OPS.1.1.3.A5	Standard	Physical
OPS.1.1.3.A6	Standard	Physical
OPS.1.1.3.A7	Standard	Logical
OPS.1.1.3.A8	Standard	Component
OPS.1.1.3.A9	Standard	Physical
OPS.1.1.3.A10	Standard	Logical
OPS.1.1.3.A11	Standard	Logical
OPS.1.1.3.A12	Erhöhter Schutzbedarf	Component
OPS.1.1.3.A13	Erhöhter Schutzbedarf	Logical
OPS.1.1.3.A14	Erhöhter Schutzbedarf	Physical
OPS.1.1.3.A15	Basis	Physical
OPS.1.1.4.A1	Basis	Logical
OPS.1.1.4.A2	Basis	Component
OPS.1.1.4.A3	Basis	Component
OPS.1.1.4.A5	Basis	Component
OPS.1.1.4.A6	Basis	Logical
OPS.1.1.4.A7	Basis	Logical, Component
OPS.1.1.4.A9	Standard	Physical
OPS.1.1.4.A10	Erhöhter Schutzbedarf	Logical, Physical
OPS.1.1.4.A11	Erhöhter Schutzbedarf	Logical
OPS.1.1.4.A12	Erhöhter Schutzbedarf	Physical
OPS.1.1.4.A13	Erhöhter Schutzbedarf	Logical
OPS.1.1.4.A14	Erhöhter Schutzbedarf	Component
OPS.1.1.5.A1	Basis	Logical
OPS.1.1.5.A3	Basis	Physical

Anforderung	Anforderungstyp	SABSA-Metaebene
OPS.1.1.5.A4	Basis	Logical
OPS.1.1.5.A5	Basis	Contextual
OPS.1.1.5.A6	Standard	Logical
OPS.1.1.5.A8	Standard	Logical
OPS.1.1.5.A9	Standard	Physical
OPS.1.1.5.A10	Standard	Physical
OPS.1.1.5.A11	Erhöhter Schutzbedarf	Logical, Physical
OPS.1.1.5.A12	Erhöhter Schutzbedarf	Logical, Physical
OPS.1.1.5.A13	Erhöhter Schutzbedarf	Logical
OPS.1.1.6.A1	Basis	Physical, Component
OPS.1.1.6.A2	Basis	Logical, Physical
OPS.1.1.6.A3	Basis	Logical, Physical
OPS.1.1.6.A4	Basis	Logical, Physical
OPS.1.1.6.A5	Basis	Logical, Physical
OPS.1.1.6.A6	Standard	Physical
OPS.1.1.6.A7	Standard	Physical
OPS.1.1.6.A10	Standard	Physical
OPS.1.1.6.A11	Basis	Physical
OPS.1.1.6.A12	Standard	Physical
OPS.1.1.6.A13	Standard	Logical
OPS.1.1.6.A14	Erhöhter Schutzbedarf	Logical
OPS.1.1.6.A15	Standard	Logical
OPS.1.1.6.A16	Erhöhter Schutzbedarf	Physical
DER.1.A1	Basis	Logical
DER.1.A2	Basis	Contextual
DER.1.A3	Basis	Physical

Anforderung	Anforderungstyp	SABSA-Metaebene
DER.1.A4	Basis	Component
DER.1.A5	Basis	Physical, Component
DER.1.A6	Standard	Logical
DER.1.A7	Standard	Physical, Component
DER.1.A9	Standard	Logical, Physical
DER.1.A10	Standard	Physical
DER.1.A11	Standard	Physical
DER.1.A12	Standard	Physical
DER.1.A13	Standard	Logical
DER.1.A14	Erhöhter Schutzbedarf	Physical, Component
DER.1.A15	Erhöhter Schutzbedarf	Physical
DER.1.A16	Erhöhter Schutzbedarf	Physical
DER.1.A17	Erhöhter Schutzbedarf	Physical
DER.1.A18	Erhöhter Schutzbedarf	Physical
DER.2.1.A1	Basis	Logical
DER.2.1.A2	Basis	Logical
DER.2.1.A3	Basis	Logical, Physical
DER.2.1.A4	Basis	Logical
DER.2.1.A5	Basis	Physical
DER.2.1.A6	Basis	Physical
DER.2.1.A7	Standard	Physical
DER.2.1.A8	Standard	Conceptual
DER.2.1.A9	Standard	Physical
DER.2.1.A10	Standard	Logical
DER.2.1.A11	Standard	Physical
DER.2.1.A12	Standard	Logical

Anforderung	Anforderungstyp	SABSA-Metaebene
DER.2.1.A13	Standard	Physical
DER.2.1.A14	Standard	Logical, Physical
DER.2.1.A15	Standard	Physical
DER.2.1.A16	Standard	Physical
DER.2.1.A17	Standard	Logical, Physical
DER.2.1.A18	Standard	Physical
DER.2.1.A19	Erhöhter Schutzbedarf	Physical
DER.2.1.A20	Erhöhter Schutzbedarf	Conceptual, Physical, Component
DER.2.1.A21	Erhöhter Schutzbedarf	Conceptual, Physical, Component
DER.2.1.A22	Erhöhter Schutzbedarf	Logical, Physical

A.3 ARBEITSPRODUKTE

Die folgenden Tabellen beschreiben die Arbeitsprodukte der jeweiligen Prozessschritten der erweiterten IT-Grundschutz-Methodik gemäß Kapitel 5. Sie beinhalten ausschließlich die generellen Arbeitsprodukte. Die spezifischen Produkte nach den R1 Bausteinen des IT-Grundschutz Kompendiums 2023 (vgl. BSI 2023b) können dem Anhang A.2 Mapping der R1 Bausteine zu SABSA Metaebenen entnommen werden.

Tabelle 7: Arbeitsprodukte aus der Initiierungsphase
Quelle: Eigene Darstellung

Arbeitsprodukt	Quelle
Ernennungsurkunde zum CISO	-/-
Organisatorisches Modell für ESA	-/-
Architecture Governance Plan	(ISO 2019b: 20)
Architecture Governance Richtlinie & Guideline	(ISO 2019b: 20)
Architecture Collection Objectives	(ISO 2019b: 20)
Architecture Management Plan	(ISO 2019b: 26)
Architecture Management Work Instructions & Guidance	(ISO 2019b: 26)
Architecture Management Charter	(ISO 2019b: 27)
Execution Plan	(ISO 2019b: 27)
Architecture Enablement Plan	(ISO 2019b: 58)
Architecture Framework	(ISO 2019b: 58)
Architecture Viewpoint	(ISO 2019b: 58)
Catalog of Enabling Capabilities	(ISO 2019b: 58)
Catalog of Enabling Services	(ISO 2019b: 58)
Catalog of Enabling Resources	(ISO 2019b: 58)
Architecture Work Product Templates	(ISO 2019b: 58)

Arbeitsprodukt	Quelle
Aufzeichnung von Managemententscheidungen	(BSI 2017a: 56)

Tabelle 8: Arbeitsprodukte aus der Ermittlung des Kontextes
Quelle: Eigene Darstellung

Arbeitsprodukt	Quelle
Kontextbeschreibung der Organisation	(vgl. Sherwood et al. 2018: 7)
Business Driver	(vgl. Sherwood et al. 2018: 7)
Business Driver for Security	(vgl. Sherwood et al. 2018: 7)
Organisations- und Beziehungsmodell	(vgl. Sherwood et al. 2018: 7)
Geographiemodell	(vgl. Sherwood et al. 2018: 7)
Zeitabhängigkeitsmodell	(vgl. Sherwood et al. 2018: 7)
Business Risikomodell	(vgl. Sherwood et al. 2018: 7)
Aufzeichnung von Managemententscheidungen	(BSI 2017a: 56)

Tabelle 9: Arbeitsprodukte aus der Konzeptualisierung
Quelle: Eigene Darstellung

Arbeitsprodukt	Quelle
Architecture Conceptualization Plan	(ISO 2019b: 38)
Architecture Objectives	(ISO 2019b: 38)
Quality Model	(ISO 2019b: 38)
Architecture Views & Models	(ISO 2019b: 38)
Architecture Elaboration Plan	(ISO 2019b: 53)
Architecture Viewpoints	(ISO 2019b: 53)
Models Kinds	(ISO 2019b: 53)
Architecture Views	(ISO 2019b: 53)

Arbeitsprodukt	Quelle
Architecture Models	(ISO 2019b: 53)
Architecture Descriptions	(ISO 2019b: 53)
Business Attributes	(vgl. Sherwood et al. 2018: 7)
Business Attributes Profile	(vgl. Sherwood et al. 2018: 7)
Control Objectives	(vgl. Sherwood et al. 2018: 7)
Control Objectives integriert in Business Risikomodell	(vgl. Sherwood et al. 2018: 7)
Ermittelter Ist-Zustand	(vgl. Sherwood et al. 2018: 7)
Security Domain Model	(vgl. Sherwood et al. 2018: 7)
Lifetimes & Deadlines	(vgl. Sherwood et al. 2018: 7)
Sicherheitsstrategie	(vgl. Sherwood et al. 2018: 7)
Responsibility Assignment Model	(vgl. Sherwood et al. 2023)
Aufzeichnung von Managemententscheidungen	(BSI 2017a: 56)

Tabelle 10: Arbeitsprodukte aus der Sicherheitsarchitektur
Quelle: Eigene Darstellung

Arbeitsprodukt	Quelle
Business Attribute Profile	(vgl. Sherwood et al. 2018: 7)
Control Objectives	(vgl. Sherwood et al. 2018: 7)
Control Library	(vgl. Sherwood et al. 2018: 7)
Organisatorische Struktur IS	(vgl. Sherwood et al. 2018: 7)
Richtlinien-Architektur	(vgl. Sherwood et al. 2018: 7)
Architecture Conceptualization Plan	(ISO 2019b: 38)
Architecture Objectives	(ISO 2019b: 38)
Quality Model	(ISO 2019b: 38)
Architecture Views & Models	(ISO 2019b: 38)

Arbeitsprodukt	Quelle
Architecture Elaboration Plan	(ISO 2019b: 53)
Architecture Viewpoints	(ISO 2019b: 53)
Models Kinds	(ISO 2019b: 53)
Architecture Views	(ISO 2019b: 53)
Architecture Models	(ISO 2019b: 53)
Architecture Descriptions	(ISO 2019b: 53)
Security Policy Architektur	(vgl. Sherwood et al. 2018: 7)
Security Policies	(vgl. Sherwood et al. 2018: 7)
Security Services	(vgl. Sherwood et al. 2018: 7)
Security Domains & Associations	(vgl. Sherwood et al. 2018: 7)
Security Processing Cycle	(vgl. Sherwood et al. 2018: 7)
CIP	(vgl. Sherwood et al. 2018: 7)
Business Data Model	(vgl. Sherwood et al. 2018: 7)
Security Rules & Procedures	(vgl. Sherwood et al. 2018: 7)
Security Mechanism	(vgl. Sherwood et al. 2018: 7)
IT-Landschaft-Karte	(vgl. Sherwood et al. 2018: 7)
Capacity Plan	(vgl. Sherwood et al. 2018: 7)
Resilience Modell	(vgl. Sherwood et al. 2018: 7)
Control Structure Execution	(vgl. Sherwood et al. 2018: 7)
IT- & Security-Grobkonzepte	(vgl. Sherwood et al. 2018: 7)
IT- & Security-Feinkonzepte	(vgl. Sherwood et al. 2018: 7)
Aufzeichnung von Managemententscheidungen	(BSI 2017a: 56)

Tabelle 11: Arbeitsprodukte aus der Umsetzung
Quelle: Eigene Darstellung

Arbeitsprodukt	Quelle
Kosten- und Aufwandschätzungen	(BSI 2017a: 66)
Umsetzungsreihenfolge der Maßnahmen	(BSI 2017a: 66)
Projektplan	(Sherwood 2005: 132)
Spezifikation der Implementation	(Sherwood 2005: 132)
Beschaffungsplan	(Sherwood 2005: 132)
Qualitätssicherungsplan	(Sherwood 2005: 132)
Testplan	(Sherwood 2005: 132)
Status und Umsetzungsgrad des Sicherheitskonzepts bzw. Architektur	(BSI 2017a: 55)
Berichte über bisherige Erfolge beim Sicherheitsprozess	(BSI 2017a: 55)
Berichte über die Reduzierung bestehender Umsetzungsdefizite und der damit verbundenen Risiken	(BSI 2017a: 55)
Installations- und Konfigurationsanleitungen	(BSI 2017a: 56)
Anleitung für den Wiederanlauf nach einem Sicherheitsvorfall	(BSI 2017a: 56)
Dokumentation von Test- und Freigabeverfahren	(BSI 2017a: 56)
Anweisungen für das Verhalten bei Störungen und Sicherheitsvorfällen	(BSI 2017a: 56)
Anleitungen zu Arbeitsabläufen und organisatorischen Vorgaben	(BSI 2017a: 56)
Richtlinie zur Nutzung des Internets	(BSI 2017a: 56)

Arbeitsprodukt	Quelle
Anleitung zum Verhalten bei Sicherheitsvorfällen	(BSI 2017a: 56)
Aufzeichnung von Managemententscheidungen	(BSI 2017a: 56)

Tabelle 12: Arbeitsprodukte aus dem KVP
Quelle: Eigene Darstellung

Arbeitsprodukt	Quelle
Architecture Governance Compliance Status Report	(ISO 2019b: 20)
Architecture Management Status Report	(ISO 2019b: 26)
Execution Status Report	(ISO 2019b: 27)
Architecture Conceptualization Status Report	(ISO 2019b: 38)
Problem Space Report	(ISO 2019b: 38)
Architecture Evaluation Plan	(ISO 2019b: 47)
Architecture Evaluation Report	(ISO 2019b: 47)
Architecture Value Assessment Result	(ISO 2019b: 47)
Architecture Analysis Result	(ISO 2019b: 47)
Architecture Elaboration Status Report	(ISO 2019b: 53)
Architecture Enablement Plan	(ISO 2019b: 58)
Architecture Enablement Status Report	(ISO 2019b: 58)
Architecture Framework	(ISO 2019b: 58)
Architecture Viewpoint	(ISO 2019b: 58)
Catalog of Enabling Capabilities	(ISO 2019b: 58)

Arbeitsprodukt	Quelle
Catalog of Enabling Services	(ISO 2019b: 58)
Catalog of Enabling Resources	(ISO 2019b: 58)
Architecture Work Product Templates	(ISO 2019b: 58)
Gap-Analyse	(Sherwood 2005: 134)
Event Report	(Sherwood 2005: 134)
Incident Report	(Sherwood 2005: 134)
Penetration Test Report	(Sherwood 2005: 134)
Operational Reports	(Sherwood 2005: 134)
Improvement Plan	(Sherwood 2005: 134)
Ergebnisse von Audits und Datenschutzkontrollen	(BSI 2017a: 55)
Aufzeichnung von Managemententscheidungen	(BSI 2017a: 56)

ANHANG B

Suchanfragen der systematischen Literaturrecherche

B.1 STRUKTURIERTE LITERATURRECHERCHE ZUM IT-GRUNDSCHUTZ

Folgende Suchanfrage wurde für die in Kapitel 3.2 definierten digitalen Bibliotheken verwendet:

(Title :it-grundschutz* OR
Title :it grundschutz*) OR
(Abstract :it-grundschutz* OR
Abstract :it grundschutz*) OR
(Keyword :it-grundschutz* OR
Keyword :it grundschutz*)

Die folgenden Seiten enthalten das Ergebnis der strukturierten Literaturrecherche. Zur Vereinfachung der Gruppierung, wurden die Kategorien in der Tabelle 13 in verkürzter Form dokumentiert. Die Spalte ‚Inkludiert‘ bedeutet die mögliche Einbindung des Textes in diese Thesis.

Tabelle 13: Literatur zum IT-Grundschutz
Quelle: Eigene Darstellung

No.	Literatur	In-kludiert	Gruppierung
1	Developing a Semantic Mapping between TOGAF and BSI-IT-Grundschutz	j	Mapping
2	Praxisbausteine zum IT-Grundschutz	n	Sachtext
3	IT-Grundschutz bei einem Telekommunikationsdienstleister	n	Kein Grundschutz Fokus
4	ISO/IEC 27001 and IT baseline protection (IT-Grundschutz)	n	Vergleich
5	Informationssicherheitskonzept nach IT-Grundschutz für Containervirtualisierung in der Cloud	n	Tech Abhandlung
6	IT-Grundschutz ist Informantenschutz	n	Kein Grundschutz Fokus
7	IT-Grundschutz für die Container-Virtualisierung mit dem neuen BSI-Baustein SYS. 1.6	n	Tech Abhandlung
8	Vorgehensweise nach BSI IT-Grundschutz	n	Sachtext
9	10. BSI-Grundschutz und ISO/IEC 27001	n	Sachtext
10	Informationssicherheit – Grundlagen für Bibliotheken: Praxis-Überblick über den IT-Grundschutz-Standard	n	Sachtext
11	Informationssicherheitsbeauftragte: Aufgaben, notwendige Qualifizierung und Sensibilisierung praxisnah erklärt Basis: ISO/IEC 2700x, BSI-Standards 200-x und IT-Grundschutz-Kompendium	n	Sachtext
12	IT-Grundschutz-Kataloge 2007	n	Sachtext
13	IT-Grundschutz-Kataloge 2006 erschienen	n	Sachtext
14	Datenschutz nach BSI-Grundschutz?	j	Jur Abhandlung
15	BSI IT-Grundschutz – Arbeitswerkzeug für ganzheitliche Informationssicherheit	n	Sachtext
16	KRITIS-Regularien	j	Jur Abhandlung
17	IT-Security Compliance for Home Offices	n	Tech Abhandlung
18	IT-Grundschutz: Two-Tier Risk Assessment for a Higher Efficiency in IT Security Management	n	Risikomanagement
19	Modellgetriebener IT-Grundschutz: Erstellung und Analyse von IT-Sicherheitskonzeptionen in offenen Werkzeugketten	n	Sachtext
20	Holistic and Law compatible IT Security Evaluation: Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA	n	Tech Abhandlung
21	Informationssicherheit für Krankenhäuser und Kliniken IT-Sicherheit ist Patientensicherheit dank ISMS	n	Case Study
22	IT-Grundschutz in der Arztpraxis nicht vernachlässigen	n	Nachricht
23	The Current State of -Information Security Awareness in German SMEs	n	Awareness
24	Zur Abgrenzung eines Informationsverbundes	n	Sachtext
25	Security Awareness für den Mittelstand	n	Awareness
26	Cyber-Risikomanagement	n	Risikomanagement
27	Datenschutz im IT-Grundschutz	j	Jur Abhandlung
28	Systematic Comparison of Methodology in Threat and Risk Analysis of ICT Security in Industry 4.0	n	Risikomanagement

No.		Inkludiert	Gruppierung
29	Zusammenfassung	n	Sachtext
30	Fazit	n	Sachtext
31	Readiness Exercises: Are Risk Assessment Methodologies Ready for the Cloud?	n	Tech Abhandlung
32	Internationalisierung der IT-Grundschutz-Zertifizierung.	n	Sachtext
33	Bekämpfung von Cybercrime durch die Polizei	n	Sachtext
34	Information Security Officer: Job profile, necessary qualifications, and awareness raising in a practical way	n	Sachtext
35	IT-Notfallmanagement mit System	n	Sachtext
36	Compliance-Portfolio-Management	n	Sachtext
37	11. Technische Sicherheitsmaßnahmen	n	Sachtext
38	Ganzheitliche IT-Security Reifegradbestimmung	n	Awarness
39	Einführung: Cybersecurity für die öffentliche Verwaltung	n	Kein Grundschutz Fokus
40	9. Grundzüge des Informationssicherheits- und Datenschutzrechts für Kommunen	n	Kein Grundschutz Fokus
41	8. Vorgehensvorschlag zur Entwicklung von kommunalen Funktionalstrategien am Beispiel der Rolle einer Cybersicherheitsstrategie	n	Kein Grundschutz Fokus
42	5. Bedeutung der Digitalisierung für die kommunale Verwaltung. Bisherige Ansätze, zentrale Entwicklungen und Anforderungen an die Verwaltung	n	Kein Grundschutz Fokus
43	IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz	n	Sachtext
44	1. Formen der Bedrohung von Cyberkriminalität	n	Sachtext
45	14. Cyber-Versicherungen	n	Kein Grundschutz Fokus
46	7. Wege zur breiten IT-Kompetenz in Kommunen	n	Kein Grundschutz Fokus
47	15. Blockchain	n	Kein Grundschutz Fokus
48	13. Einführung eines Informationssicherheitsmanagements in der kommunalen Praxis	n	Sachtext
49	12. Mitarbeitersempfehlungen in der öffentlichen Kommunalverwaltung	n	Kein Grundschutz Fokus
50	6. Die Organisation und Struktur der Digitalisierung der Kommunen	n	Kein Grundschutz Fokus
51	3. Verbreitung von Cyberkriminalität gegen Unternehmen in Deutschland	n	Kein Grundschutz Fokus
52	2. Cybercrime – Die Täter im Netz	n	Kein Grundschutz Fokus
53	IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz	n	Sachtext
54	Seite 1 Informationssicherheit und Datenschutz an Hochschulen: Ohne Moos nichts los? (Draft)	n	Tech Abhandlung
55	Ende-zu-Ende-Sicherheit für die multimodale Mobilität in einer Smart City	n	Tech Abhandlung
56	Einfallsporten für IT-Angrifer in der Medizin: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis	n	Sachtext
57	Qualifizierung nach IT-Grundschutz - Maßstab für IT-Sicherheit.	n	Sachtext

No.	Literatur	Inkludiert	Gruppierung
58	Hybride Testumgebungen in der Informationssicherheit - Effiziente Sicherheitsanalysen für Industrieanlagen	n	Tech Abhandlung
59	Modellierung und Implementierung hybrider Testumgebungen für cyber-physische Sicherheitsanalysen	n	Tech Abhandlung
60	Cyber-Sicherheits-Check: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden	n	Sachtext
61	Normen, Standards, Practices: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices	n	Sachtext
62	Hybride Testumgebungen für Kritische Infrastrukturen: Effiziente Implementierung für IT-Sicherheitsanalysen von KRITIS-Betreibern	n	Tech Abhandlung
63	Anforderungen an eine IT-Lösung für den ISO27-Sicherheitsprozess	n	Kein Grundschutz Fokus
64	ISO 27001-Zertifikat auf der Basis von IT-Grundschutz	n	Sachtext
65	Arbeiten zum Datenschutz im IT-Grundschutz vorläufig abgeschlossen	n	Nachricht
66	Zweiter Akt – Erste Szene: Überwindung der Hürden	n	Sachtext
67	Anwendung und Untersuchung einer Methode zur Analyse von IT-Sicherheitsrisiken anhand eines hochwertigen Erdfernerkundungssystems	n	Kein Grundschutz Fokus
68	Datenschutzaudit nach IT-Grundschutz-Konvergenz zweier Welten	n	Kein Grundschutz Fokus
69	Informantenschutz	n	Kein Grundschutz Fokus
70	Compliance-Anforderungen und deren Einhaltung	n	Kein Grundschutz Fokus
71	Die Zertifizierung in der Informationssicherheit	n	Kein Grundschutz Fokus
72	The CAST Method for Comparing Security Standards	n	Kein Grundschutz Fokus
73	Informationssicherheits-Management	n	Kein Grundschutz Fokus
74	Herausforderungen der IT-Sicherheit bei kleinen und mittleren Betriebem kritischer Infrastrukturen	n	Tech Abhandlung
75	A Structured Comparison of Security Standards	n	Kein Grundschutz Fokus
76	DNS-Sicherheit im Rahmen eines IT-Grundschutz-Bausteins	n	Tech Abhandlung
77	Sicherheitsprobleme für IT-Outsourcing durch Cloud Computing	n	Tech Abhandlung
78	Methoden zur Umsetzung von Datensicherheit und Datenschutz im vernetzten Steuergerät	n	Tech Abhandlung
79	Web Service Security für die IT-Grundschutz-Kataloge	n	Tech Abhandlung
80	IT security issues in factories	n	Tech Abhandlung
81	IT-Sicherheit 3.0: Der neue IT-Grundschutz: Grundlagen und Neuerungen unter Berücksichtigung des Internets der Dinge und Künstlicher Intelligenz	n	Tech Abhandlung
82	IT-Grundschutz-basierendes Sicherheitskonzept für die Virtuelle Poststelle des Bundes.	n	Kein Grundschutz Fokus
83	Holistic and Law Compatible IT Security Evaluation:	j	Vergleich
84	Grundzüge eines Sicherheitskonzepts für Arztpraxen unter Berücksichtigung der Gesundheitstelematik	n	Tech Abhandlung

No.	Literatur	Inkludiert	Gruppierung
85	IT security Issues in factories	n	Tech Abhandlung
86	Ontology-based security standards mapping optimization by the means of Graph theory	n	Kein Grundschutz Fokus
87	Audits und Zertifizierungen	n	Sachtext
88	IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung	n	Sachtext
89	Vergleich von ISO/IEC 27033-1 und IT- Grundschutz	n	Tech Abhandlung
90	Towards Process Centered Information Security Management - A Common View for Federated Business Processes and Personal Data Usage Processes	j	Methodik Anpassung
91	Formalizing information security knowledge	n	Kein Grundschutz Fokus
92	Specification of a Voting Service Provider	n	Tech Abhandlung
93	Evaluation of Advanced Security Concepts to Improve the Trustworthiness of x86-Based Systems	n	Tech Abhandlung
94	Notfallorganisation	n	Kein Grundschutz Fokus
95	The Current State of "Information Security Awareness" in German SMEs	n	Awarness
96	Internet security resources	n	Kein Grundschutz Fokus
97	Ontological Mapping of Information Security Best-Practice Guidelines	n	Kein Grundschutz Fokus
98	IT-Security Governance	n	Kein Grundschutz Fokus
99	Towards the impact of the operational environment on the security of e-voting	n	Tech Abhandlung
100	Sicherheitsaspekte von Instant Messaging	n	Tech Abhandlung
101	Protokollierung in Sicherheitsstandards	n	Tech Abhandlung
102	Messbare IT-Sicherheit	n	Tech Abhandlung
103	Einführung in Informationsmanagementsysteme (II): BSI-Standards und Vergleich	n	Sachtext
104	Sicherheitsaspekte von Instant Messaging	n	Tech Abhandlung
105	Specification of a Voting Service Provider	n	Tech Abhandlung
106	IT-Grundschutz-Kompendium	n	Sachtext
107	IT-Grundschutz-Kataloge : Standardwerk zur IT-Sicherheit	n	Sachtext
108	IT-Grundschutz und Datenschutz : Analyse des Informationsverbundes mittels IT-Grundschutz sowie rechtliche Aspekte einer Datenschutzrichtlinie anhand BSI	n	Risikomanagement
109	Implementation of the IT-Grundschutz in Small and Medium Enterprises	n	Case Study
110	Checklisten Handbuch IT-Grundschutz : Prüfaspakte des IT-Grundschutz-Kompendiums	n	Sachtext
111	Checklisten Handbuch IT-Grundschutz : Prüffragen zum IT-Grundschutz-Kompendium	n	Sachtext
112	Systemsicherheits-Optimierungen in Web-basierten Systemen am Beispielprojekt DigiFit4All	n	Kein Grundschutz Fokus

No.	Literatur	Inkludiert	Gruppierung
113	Exemplarische Sicherheitsanalyse und Sicherheitsanforderungen an eine Arztpraxis in Deutschland	n	Kein Grundschutz Fokus
114	Ontology- and Bayesian-based information security risk management	n	Kein Grundschutz Fokus
115	Managing security policies	n	Case Study
116	Sicheres verteiltes Rechnen unter dem Aspekt der Wirtschaftlichkeit	n	Tech Abhandlung
117	Die Anforderungen von EUROSOX an IT-Prozesse : ein Umsetzungsleitfaden für Führungskräfte zur Implementierung von IT-Governance	n	Org Abhandlung
118	Einführung von IT Policies und ITIL-konformen IT Service Management Prozessen in Kleinunternehmen	n	Org Abhandlung
119	IT-Datenschutz und IT-Datensicherheit innerhalb von Unternehmen - moderne IT Infrastrukturen und deren Risiken im Fokus	n	Risikomanagement
120	Entwicklung und Implementierung einer Methode für die Selektion von Sicherheitsmaßnahmen gemäß ISO/IEC 27001	n	Tech Abhandlung
121	Smart Metering : Architektur und Vertragskonstellationen	n	Kein Grundschutz Fokus
122	IT-Security und Geschäftsprozesse: Gelungenes Schnittstellenmanagement : Untersuchung von Potenzial und Problemen beim Zusammenspiel von IT-Security-Maßnahmen und Geschäftsprozessen	n	Tech Abhandlung
123	Implementation model for the digital transformation of small and medium-sized enterprises	n	Kein Grundschutz Fokus
124	Der IT Security Manager : aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden	n	Kein Grundschutz Fokus
125	IT-Sicherheitsmanagement : Praxiswissen für IT Security Manager	n	Kein Grundschutz Fokus
126	Managed IT Services : Leitfaden für die Transformation vom einfachen IT-Dienstleister zum Managed Service Provider	n	Org Abhandlung
127	Sicherheitskonzept für Maritime Informations- und Kommunikationsservices	n	Tech Abhandlung
128	IT-Sicherheitsmanagement und IT-Grundschutz : BSI-Standards zur IT-Sicherheit	n	Sachtext
129	Checklisten Handbuch IT-Grundschutz : Prüfaspekte des IT-Grundschutz-Kompendiums	n	Sachtext
130	IT-Grundschutz - Sicherheit in KMU	n	Case Study
131	Mapping security frameworks into SecOnt	n	Risikomanagement
132	IT-Grundschutz Arbeitshandbuch : DIN ISO/IEC 27001, DIN ISO/IEC 27002; BSI-Standards 200-1/2/3	n	Sachtext
133	Informationssicherheit und IT-Grundschutz : BSI-Standards 100-1, 100-2 und 100-3 ; mit CD-ROM	n	Sachtext
134	Vermittlung von Informations-Sicherheit mittels E-Learning	n	Kein Grundschutz Fokus
135	Implementierung von Sicherheitskennzahlen in den IT-Grundschutz	n	Org Abhandlung
136	Entwurf eines BSI-IT-Grundschutz-Frameworks für Leitsysteme	n	Methodik Anpassung

No.	Literatur	Inkludiert	Gruppierung
137	Durchführbarkeit und Nutzen von IT-Sicherheitsanalysen nach IT-Grundschutz in KMUs	n	Risikomanagement
138	Einführung von Informationssicherheit basierend auf den IT-Grundschutz-Katalogen	n	Org Abhandlung
139	Erstellung eines IT-Grundschutz-Profil für eine oberste Landesbehörde in der Bundesrepublik Deutschland	n	Org Abhandlung
140	ISO/IEC 27001 ISO/IEC 27002 und IT-Grundschutz : Schnelleinstieg Informationssicherheit 2022	n	Sachtext
141	Einsatz von ISO 17799 und IT-Grundschutz in kleinen und mittleren Unternehmen	n	Case Study
142	IT-Grundschutz Arbeitshandbuch : DIN ISO/IEC 27001 ; DIN ISO/IEC 27002 ; BSI-Standards 200-1/2/3	n	Sachtext
143	IT-Grundschutz für "Kleine und Mittlere Unternehmen" (KMU's) : Schwachstellen in DV-Landschaften erkennen und beseitigen	n	Tech Abhandlung
144	Praxisbuch Netzwerk-Sicherheit : Risikoanalyse, Methoden und Umsetzung	n	Sachtext
145	BSI und DSGVO für österreichische KMUs	n	Methodik Anpassung
146	Ein KMU-orientiertes Disaster Preparedness Konzept für IT-Infrastrukturen zur Vorbereitung auf natürliche und, daraus resultierende, technologische Katastrophen	n	Kein Grundschutz Fokus
147	Ein Security Testverfahren zur Unterstützung von KMUs in der Softwareentwicklung	n	Tech Abhandlung
148	Konzeptualisierung und Implementierung eines Security Layers für ArchiMate	n	Kein Grundschutz Fokus
149	An approach to continuous information security risk assessment focused on security measurements	n	Risikomanagement
150	IT-Compliance an der Pädagogischen Hochschule Steiermark : Initiierungsplan eines Sicherheitskonzeptes und Erarbeitung der datenschutzrechtlichen Bestimmungen für die Verarbeitung von Studierendendaten im Hochschulbereich	n	Kein Grundschutz Fokus
151	Einführung des Oracle Identity Managements in das Unternehmen Austrian Energy & Environment mittels Workflows und die Analyse des IT Grundschatzes	n	Case Study
152	IT-Risikomanagement mit System : praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken	n	Risikomanagement
153	Handbuch Datenschutz und IT-Sicherheit	n	Kein Grundschutz Fokus
154	Checklisten Handbuch IT-Grundschutz : sämtliche Prüffragen des BSI / Bundesamt für Sicherheit in der Informationstechnik	n	Sachtext
155	Informationssicherheit und Datenschutz : Handbuch für Praktiker und Begleitbuch zum T.I.S.P.	n	Kein Grundschutz Fokus
156	IT-Grundschutz umsetzen mit GSTOOL : Anleitungen und Praxistipps für den erfolgreichen Einsatz des BSI-Standards / Frederik Humpert	n	Sachtext
157	Quick-Check Security Audit	n	Sachtext

No.	Literatur	Inkludiert	Gruppierung
158	Quick-Check Security Audit	n	Sachtext
159	ISO 17799 und BSI-Grundschutz	n	Sachtext
160	IT-Grundschutz bei einem Telekommunikationsdienstleister. Besonderheiten bei der Anwendung der Methodik	n	Case Study
161	Arbeiten zum Datenschutz im IT-Grundschutz vorläufig abgeschlossen	n	Jur Abhandlung
162	Datenschutz nach BSI-Grundschutz? Das Verhältnis zwischen Datenschutz und Datensicherheit	n	Jur Abhandlung
163	Datenschutz im IT-Grundschutz	n	Jur Abhandlung
164	BSI IT-Grundschutz – Arbeitswerkzeug für ganzheitliche Informationssicherheit	n	Sachtext
165	JOINED-VIV: Umsetzung der DSGVO mittels SDM und unter Einbindung des BSI IT-Grundschutzes: Gewährleistung von Verfügbarkeit, Integrität und Vertraulichkeit im Datenschutz mittels der technischen und organisatorischen Maßnahmen des BSI IT-Grundschutzes	n	Kein Grundschutz Fokus
166	VS-Zulassung: Einführung und Grundlagen	n	Kein Grundschutz Fokus
167	Sicherheit nach BSI-Grundschutz und ISO 27001 : Grundlagen der Sicherheitsstandards ; Audits ; Unterstützung des Sicherheitsprozesses mit verinice	n	Sachtext

B.2 STRUKTURIERTE LITERATURRECHERCHE ZU ESA UND SABSA

Folgende Suchanfrage wurde für die in Kapitel 3.2 definierten digitalen Bibliotheken verwendet:

(Title :"enterprise security architecture" OR
Title :"enterprise security architectures" OR
Title :"enterprise information security architecture" OR
Title :"enterprise information security architectures" OR
Title :"sabsa" OR
Title :"sherwood applied business security architecture") OR
(Abstract :"enterprise security architecture" OR
Abstract :"enterprise security architectures" OR
Abstract :"enterprise information security architecture" OR
Abstract :"enterprise information security architectures" OR
Abstract :"sabsa" OR
Abstract :"sherwood applied business security architecture") OR
(Keyword :"enterprise security architecture" OR
Keyword :"enterprise security architectures" OR
Keyword :"enterprise information security architecture" OR
Keyword :"enterprise information security architectures" OR
Keyword :"sabsa" OR
Keyword :"sherwood applied business security architecture")

Die folgenden Seiten enthalten das Ergebnis der strukturierten Literaturrecherche.
Spalte „Inkludiert“ bedeutet die mögliche Einbindung des Textes in diese Thesis.

Tabelle 14: Literatur zu ESA und SABSA
Quelle: Eigene Darstellung

No.	Literatur	Inkludiert	Beschreibung
1	Chapter 3 - Cyber Risk Management: A New Era of Enterprise Risk Management	n	Fokus auf RM
2	Chapter 13 - A Blueprint for Security	n	Fokus auf RM
3	Towards augmented proactive cyberthreat intelligence	n	Fokus auf Threat Intelligence
4	Chapter 2 - Risk Assessment and Monitoring in Intelligent Data-Centric Systems	n	Fokus auf RM
5	Integrated identity and access management metamodel and pattern system for secure enterprise architecture	n	Fokus auf IAM in EA integrieren
6	SALSA: A method for developing the enterprise security architecture and strategy	n	Vorgänger von SABSA
7	Enterprise security pattern: A model-driven architecture instance	n	Fokus liegt auf Softwarearchitektur
8	CAESAR8: An agile enterprise architecture approach to managing information security risks	j	Agile Arbeitsweise zu ESA
9	A new month, a new data breach	n	Beschreibt weshalb Verschlüsselung wichtig ist
10	What does 'secure by design' actually mean?	n	Beschreibt den allgemeinen Shift-Left Ansatz
11	Enterprise information security, a review of architectures and frameworks from interoperability perspective	n	Vergleicht ESA Frameworks
12	AT&T strengthen security of Network Notes	n	Fokus auf Netzwerksicherheit
13	Top to tail router security	n	Fokus auf Netzwerksicherheit
14	The changing face of IT security	n	Fokus liegt auch tech. Sicherheit
15	The importance of context in keeping end users secure	n	Fokus auf IT-Architektur
16	Do you have the right security?	n	Beschreibt Bedrohungslage von 2011
17	The cybersecurity workforce and skills	n	Beschreibt Qualifikationen in Cybersicherheit
18	Investigating digital fingerprints: advanced log analysis	n	Fokus auf Analyse von Logs
19	Securing the building blocks of system architecture	n	Beschreibt auf abstrakte Weise wie Sicherheit in Unternehmen aufgebaut werden könnte
20	Two-factor authentication – a look behind the headlines	n	Fokus auf Authentisierung
21	From auditor-centric to architecture-centric: SDLC for PCI DSS	j	Mapping der Architektur über Thread Modelling zu PCI DSS Sicherheitsanforderungen
22	A roadmap to develop enterprise security architecture	n	Artikel beschreibt eine eigene unausgereifte ESA, die SABSA gleicht
23	Virtual enterprises and the enterprise security architecture	n	Fokus auf technische Architektur
24	An enterprise security architecture for accessing SaaS cloud services with BYOD	n	Fokus auf technische Architektur
25	Enterprise Security Architecture For Cloud Computing: A Review	n	Fokus auf Cloud Architektur
26	Securing the mobile enterprise with network-based security and cloud computing	n	Fokus auf Netzwerksicherheit
27	Towards a Metamodel for SABSA Conceptual Architecture Descriptions	j	Beschreibung der Conceptual Architecture mittels Metamodels
28	Rethinking Security Operations Centre Onboarding	n	Fokus auf SOC
29	An Organization-Driven Approach for Enterprise Security Development and Management	n	Eigene ESA Entwicklung mit Fokus auf Tech, ähnelt SABSA

No.	Literatur	Inkludiert	Beschreibung
30	A Distributed Approach to Delegation of Access Rights for Electronic Health Records	n	Fokus auf IAM in EA integrieren
31	Protection of enterprise resources: A novel security framework	n	Fokus liegt auch tech. Sicherheit
32	Towards a Holistic Information Security Governance Framework for SOA	n	Zeigt auf wie SABSA bei SOAs eingesetzt werden kann
33	Integrating Trusted Computing Mechanisms with Trust Models to Achieve Zero Trust Principles	n	Fokus auf Zero Trust
34	Enterprise Security Architecture	n	Fokus auf Netzwerksicherheit & IAM
35	Fujitsu Enterprise Security Architecture	n	Fokus auf technische Architektur
36	Enterprise security architecture in business convergence environments	n	Beschreibt Konvergenz von Sicherheit und EA, Ergebnis ähnelt SABSA
37	Ranking Criteria of Enterprise Information Security Architecture Using Fuzzy Topsis	n	Beschreibt Fuzzier zur Identifizierung beliebter IS Themen im Bereich der EISA
38	Enterprise security architecture : a business-driven approach	j	SABSA
39	Proceedings of the 2005 ACM Workshop on Secure Web Services : November 11, 2005, Fairfax, Virginia, USA, (co-located with CCS 2005) ; SWS'05	n	Fokus auf technische Sicherheit
40	Zero Trust Security : An Enterprise Guide	n	Fokus auf Zero Trust
41	The handbook of technology management. 3 Management support systems, electronic commerce, legal and security considerations	n	Beschreibt die technische Sicherheit
42	Cyber Security on Azure : An IT Professional's Guide to Microsoft Azure Security Center	n	Fokus auf technische Sicherheit
43	Cloud Attack Vectors : Building Effective Cyber-Defense Strategies to Protect Cloud Resources	n	Fokus auf Cloud
44	IoT – Best Practices : Internet der Dinge, Geschäftsmodellinnovationen, IoT-Plattformen, IoT in Fertigung und Logistik	n	Fokus auf IoT
45	A Comprehensive Guide for Web3 Security : From Technology, Economic and Legal Aspects	n	Fokus auf Technologie
46	A UML-based methodology for model-driven B2B integration: from business values, over business processes to deployment artifacts	n	Fokus auf IT-Architektur
47	Web services enterprise security architecture: a case study	n	Fokus auf tech. Sicherheit
48	WebUpdated Standard for Secure Satellite Communications: Analysis of Satellites, Attack Vectors, Existing Standards, and Enterprise and Security Architectures	n	Fokus auch Sicherheit von Satelliten
49	Mitigating IoT Enterprise Vulnerabilities Using Radio Frequency Security Architecture	n	Fokus auf IoT
50	Security Architecture Framework for Enterprises	j	Eigene ESA Entwicklung, ähnelt SABSA
51	Enterprise Security Architecture: Mythology or Methodology?	j	Eigene ESA Entwicklung, ähnelt SABSA
52	Method Framework for Developing Enterprise Architecture Security Principles	j	Eigene ESA Entwicklung
53	A novel architecture for an integrated enterprise network security system	n	Fokus auf Netzwerksicherheit
54	An integrated conceptual model for information system security risk management supported by enterprise architecture management	n	Fokus auf RM mit Integration in EA
55	Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – A Literature Review	n	Fokus auf RM mit Integration in EA

No.	Literatur	Inkludiert	Beschreibung
56	Challenges for Risk and Security Modelling in Enterprise Architecture	j	Risikomodellierung und automatisierte Entscheidungsfindung für ESA
57	Research on Enterprise Security Early Warning System Architecture Based on Internet of Things	n	Fokus auf IoT
58	Adaptive security architecture for protecting RESTful web services in enterprise computing environment	n	Fokus auf REST
59	Enterprise Architecture for International Agreements in Social Security Institutions	n	Fokus auf EA
60	An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement	n	Fokus auf Netzwerksicherheit
61	Enterprise Architecture Security Assessment Framework (EASAF)	j	Quantifizierte Messung der Security in EA
62	Unikernels for Cloud Architectures: How Single Responsibility can Reduce Complexity, Thus Improving Enterprise Cloud Security	n	Fokus auf Cloud
63	Exploring the Role of Enterprise Architecture Models in the Modularization of an Ontology Network: A Case in the Public Security Domain	n	Erstellung von Ontologie zur Beschreibung von Informationsaustausch
64	A secure enterprise architecture focused on security and technology-transformation (SEAST)	j	Eigene ESA Entwicklung
65	Where Enterprise Architecture and Early Ontology Engineering Meet: A Case Study in the Public Security Domain	n	Fokus auf Ontologie
66	Security analysis model, system architecture and relational model of enterprise cloud services	n	Fokus auf Cloud
67	Enterprise Architecture-Based Risk and Security Modelling and Analysis	n	Fokus auf Risiko Assessment in TOGAF
68	An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management Based on TOGAF	n	Fokus auf RM in TOGAF
69	Knowledge Elicitation and Conceptual Modeling to Foster Security and Trust in SOA System Evolution	n	Fokus auf SOA
70	Towards the ENTRI Framework: Security Risk Management Enhanced by the Use of Enterprise Architectures	n	Fokus auf RM in TOGAF
71	Robust Enterprise Application Security with eTRON Architecture	n	Fokus auf technische Sicherheit
72	The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures	n	Fokus auf technische Sicherheit
73	Conceptual Integration of Enterprise Architecture Management and Security Risk Management	n	Fokus auf RM mit Integration in EA
74	Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®	n	Erklärt SABSA
75	Long-term security of digital information: Assessment through risk management and Enterprise Architecture	n	Fokus auf RM mit Integration in EA
76	On an Integration of an Information Security Management System into an Enterprise Architecture	n	Mapping von ISO/IEC 27001 in EA mit Fokus auf Tech
77	A Novel Architecture for Enterprise Network Security	n	Fokus auf Netzwerksicherheit
78	Governance of Information Security Elements in Service-Oriented Enterprise Architecture	n	Fokus auf SOA

No.	Literatur	Inkludiert	Beschreibung
79	Combining Defense Graphs and Enterprise Architecture Models for Security Analysis	n	Fokus auf technische Sicherheit
80	Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool	n	Fokus auf IAM in EA integrieren
81	Using FDAF to bridge the gap between enterprise and software architectures for security	n	Kombiniert Ontologie mit IAM
82	A Security Architecture for Enterprise Rights Management	n	IAM in Sicherheitsarchitektur
83	A distributable security management architecture for enterprise systems spanning multiple security domains	n	Fokus auf technische Sicherheit
84	Mobile-driven architecture for managing enterprise security policies	n	Fokus liegt auf mobile Security
85	Security in enterprise resource planning systems and service-oriented architectures	n	Fokus auf technische Sicherheit
86	Securing Service-Oriented and Event-Driven Architectures Results of an Evaluation of Enterprise Security Frameworks	n	Fokus auf technische Sicherheit
87	SANE: A Protection Architecture for Enterprise Networks	n	Fokus auf Netzwerksicherheit
88	Enterprise knowledge security architecture for military experimentation	n	Kombination der Ontologie von Informationen und der Zugriff auf diese
89	SPECSA: a scalable, policy-driven, extensible, and customizable security architecture for wireless enterprise applications	n	Fokus auf technischer Sicherheit
90	Enterprise Engineering And Security: Enterprise Frameworks and Architectures, and IA Patterns	n	Fokus auf EA
91	Security management system functional architecture for enterprise network	n	Fokus auf Netzwerksicherheit
92	Security aspects of an enterprise-wide network architecture	n	Fokus auf Netzwerksicherheit
93	Applying the DoD goal security architecture as a methodology for the development of system and enterprise security architectures	j	Eigenes ESA Framework erstellt
94	Inter-enterprise contract architecture for open distributed systems: security requirements	n	Fokus auf technische Sicherheit
95	Obtaining secure business process models from an enterprise architecture considering security requirements	n	Fokus auf technische Sicherheit

ANHANG C

Interviewaufbau und Ergebnisse

C.1 INTERVIEW FRAGEN UND IHRE THEMEN

1. Wie bewerten Sie die allgemeine Herangehensweise im Kontext der Informationssicherheit? (Thema: Perspektive)
2. Gibt es Aspekte der Methodik, die Ihnen besonders relevant oder innovativ erscheinen? (Thema: Relevanz)
3. Welche Herausforderungen oder Risiken können bei der Anwendung dieser Methodik auftreten? (Thema: Herausforderungen)
4. Wie sehen Sie die Relevanz dieser Methodik und die wesentlichen Herausforderungen im Licht zukünftiger Entwicklungen im Bereich der Informationssicherheit? (Thema: Zukunft)

Darüber hinaus wurde die Kategorie ‚Weiteres‘ angelegt, um Informationen kodieren zu können, die über die Frage hinaus gehen, jedoch relevant bzw. interessant für die erweiterte Methodik wären.

C.2 HINTERGRUNDINFORMATION ZUM EXPERTENINTERVIEW

Die nachfolgende Tabelle 15 gibt Aufschluss über die Verteilung der gestellten Anfragen und Rückmeldungen.

Tabelle 15: Verteilung der Befragten
Quelle: Eigene Darstellung

Rolle	Anfragen	Rückmeldungen	% der Gesamtantworten
CISO	6	2	20%
Praktiker:in	8	3	30%
Berater:in	8	3	30%
Forscher:in	5	2	20%
Gesamt	27	10	100%

In Tabelle 16 werden die von den Befragten angegebenen Reifegrade für ihre jeweilige Organisation bzw. für ihre Kunden dargestellt.

Tabelle 16: Reifegrad der Organisationen von Befragten
Quelle: Eigene Darstellung

Person	Reifegrad der Informationssicherheit
CISO 1	Mittel
CISO 2	Mittel
Praktiker:in 1	Mittel
Praktiker:in 2	Mittel
Praktiker:in 3	Hoch
Berater:in 1	Mittel
Berater:in 2	Mittel
Berater:in 3	Hoch
Forscher:in 1	Gering
Forscher:in 2	Mittel

C.3 CODES UND IHRE HÄUFIGKEIT

Die folgenden Seiten listen den Auszug der rohen Kodierung der Experteninterviews als Ergebnis der offenen Kodierung. Diese Kodierungen wurden nicht bearbeitet.

Tabelle 17: Codes und ihre Häufigkeit in Interviews
Quelle: Eigene Darstellung

Kategorie	Code	Cases	% Cases
Perspektive	End-to-End	3	30,0%
Perspektive	Fokussierung	2	20,0%
Perspektive	Lückenloses arbeiten	1	10,0%
Perspektive	KVP	3	30,0%
Perspektive	Ganzheitliche Betrachtung	2	20,0%
Perspektive	Unsicherheit ob ESA benötigt wird	1	10,0%
Perspektive	Integration in bestehende Strukturen	1	10,0%
Perspektive	Ergänzung	1	10,0%
Perspektive	Datengetrieben	1	10,0%
Perspektive	Transparenz	1	10,0%
Perspektive	Nachvollziehbarkeit	1	10,0%
Perspektive	Skepsis	1	10,0%
Perspektive	Nicht für regulierte Bereiche	1	10,0%
Weiteres	Commitment	1	10,0%
Weiteres	Ausgestaltung	1	10,0%
Weiteres	Unsicherheit	1	10,0%
Weiteres	Tailoring	2	20,0%
Weiteres	Praxisbeispiel	1	10,0%
Weiteres	Keine Security in EA Betrachtung	2	20,0%
Weiteres	EA zu akademisch	1	10,0%
Weiteres	Agilität Wird Wichtiger	1	10,0%
Weiteres	Arbeit ohne passende Tools	2	20,0%
Weiteres	EA Tool	1	10,0%
Weiteres	Security nach Compliance	5	50,0%
Weiteres	Erwartung InfoSec nach geschäftlichen Zielen auszurichten	1	10,0%
Weiteres	Fehlender Organisationskontext in Security Standards	1	10,0%
Weiteres	Unstrukturierte Arbeitsweise	1	10,0%
Weiteres	Enterprise Architekten für ESA	1	10,0%
Weiteres	Strukturelle Ausgestaltung	1	10,0%
Weiteres	Promotor	1	10,0%
Weiteres	Unklare Unternehmensziele	1	10,0%
Weiteres	Ausrichtung Security Unterschiedlich	1	10,0%
Weiteres	Arbeit nach Checkliste	1	10,0%

Kategorie	Code	Cases	% Cases
Weiteres	Fehlende Strategie	1	10,0%
Weiteres	Anwendung von Sicherheitsmaßnahmen	1	10,0%
Relevanz	Verknüpfung	1	10,0%
Relevanz	Organisationsgröße	2	20,0%
Relevanz	Ausrichtung Sec nach Orgzielen	3	30,0%
Relevanz	Unterstützung	1	10,0%
Relevanz	Keine Interpretation	1	10,0%
Relevanz	Verbindung mit Zero Trust	1	10,0%
Relevanz	Datenströmen	1	10,0%
Herausforderung	Komplexität	3	30,0%
Herausforderung	Akzeptanz	1	10,0%
Herausforderung	Aufwändig	1	10,0%
Herausforderung	Keine Unterstützung bei Abteilungen	1	10,0%
Herausforderung	Zeitintensiv	1	10,0%
Herausforderung	Interessenskonflikt	1	10,0%
Herausforderung	Fehlende Agilität	1	10,0%
Herausforderung	Erwartungshaltung	1	10,0%
Herausforderung	KPI Wahl	1	10,0%
Herausforderung	Zusammenarbeit zwischen Abteilungen	1	10,0%
Herausforderung	Methodik Anwendung	1	10,0%
Herausforderung	Interner Widerstand	1	10,0%
Herausforderung	Mehrwert der Architektur zeigen	1	10,0%
Herausforderung	Unsicherheit in Compliance	1	10,0%
Herausforderung	Fehlende Erfahrungswerte	1	10,0%
Herausforderung	Neue Thematik	1	10,0%
Herausforderung	Fehlendes Wissen	1	10,0%
Herausforderung	Fehlende Fachleute	1	10,0%
Herausforderung	Auditierung nicht problematisch	1	10,0%
Zukunft	Umgang mit Komplexität	7	70,0%
Zukunft	Verbinden mit anderen Themen	1	10,0%
Zukunft	Auditierung	1	10,0%
Zukunft	Steigende Regularien	1	10,0%
Zukunft	Schwierige Marktabstabilierung	1	10,0%
Zukunft	Pionier Unternehmen	1	10,0%

C.4 ZUSAMMENGEFASSTE KODIERUNG

Zur Synthesierung des Informationsgehalts der zehn Experteninterviews, wurden die Codes nach ihrem Inhalt gruppiert durch das axiale Kodieren. Das Ergebnis und die prozentualen Erwähnungen in Relation zur Gesamtanzahl der Interviews kann der Tabelle 12 entnommen werden.

Tabelle 18: Inhaltliche Zusammenföhrung

Quelle: Eigene Darstellung

Kategorie	% Cases
Integrierter Lösungsansatz	80,0%
Sicherheitskultur	70,0%
Organisationskultur	60,0%
Umgang mit Komplexität	60,0%
Adaption	60,0%
KVP	40,0%
Security-Ausrichtung	40,0%
Komplexität	30,0%
Strategische Unsicherheit	20,0%
EA-Probleme	20,0%
Auditierung	20,0%
Intensität	10,0%
EA-Tools	10,0%
Unsicherheit ob ESA nötig	10,0%

Zur Verbesserung der Verständlichkeit der Themen und besseren Interpretierbarkeit der Synthese, wurde das Ergebnis visualisiert, siehe Abbildung 24, und die jeweiligen Kategorien in Kontext gesetzt, siehe Abbildung 25. Die Legende zur Darstellung kann der Abbildung 23 entnommen werden.

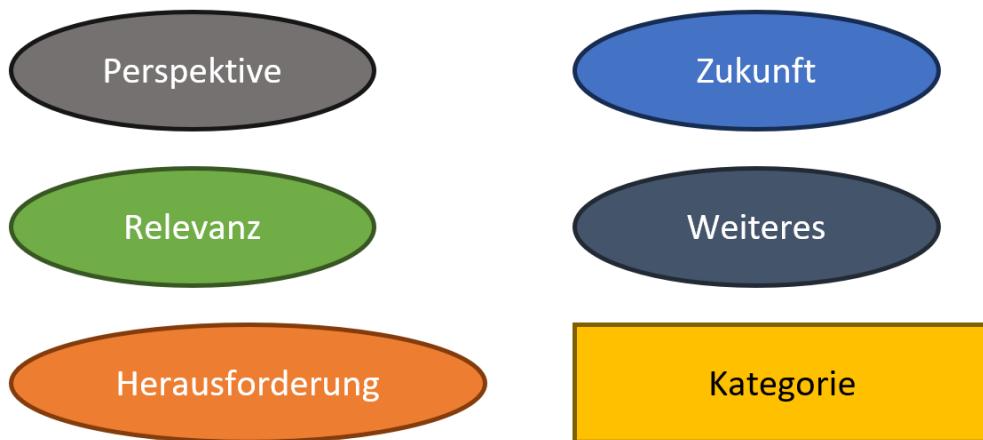


Abbildung 23: Legende für Abbildung 24 und 25
Quelle: Eigene Darstellung

Zwei Codes konnten aufgrund ihrer inhaltlichen Repräsentation nicht mit anderen Codes zusammengefasst werden, weshalb sie als eigene Zusammenfassung dargestellt werden.

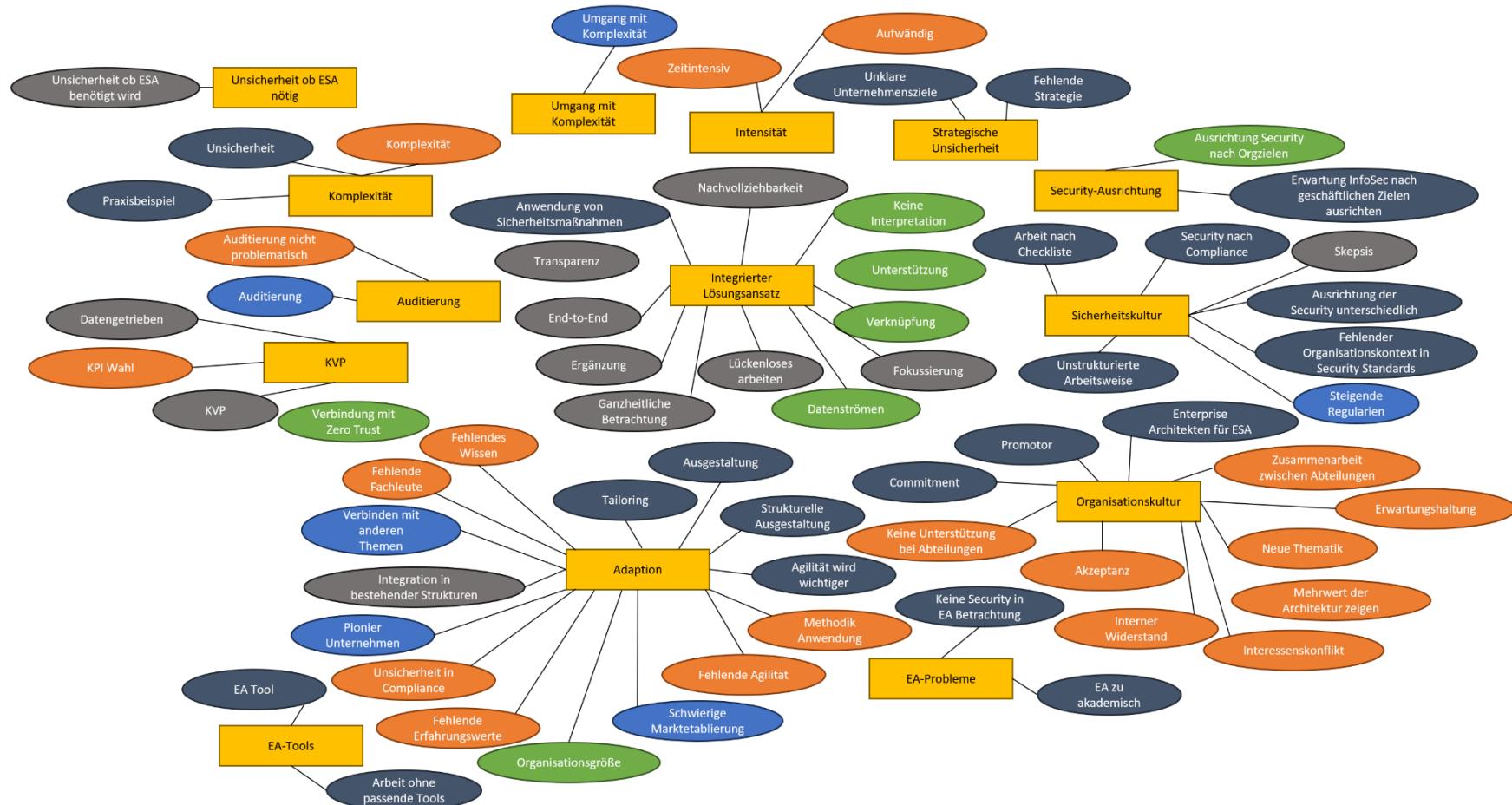


Abbildung 24: Visualisierung der inhaltlichen Zusammenführung
Quelle: Eigene Darstellung

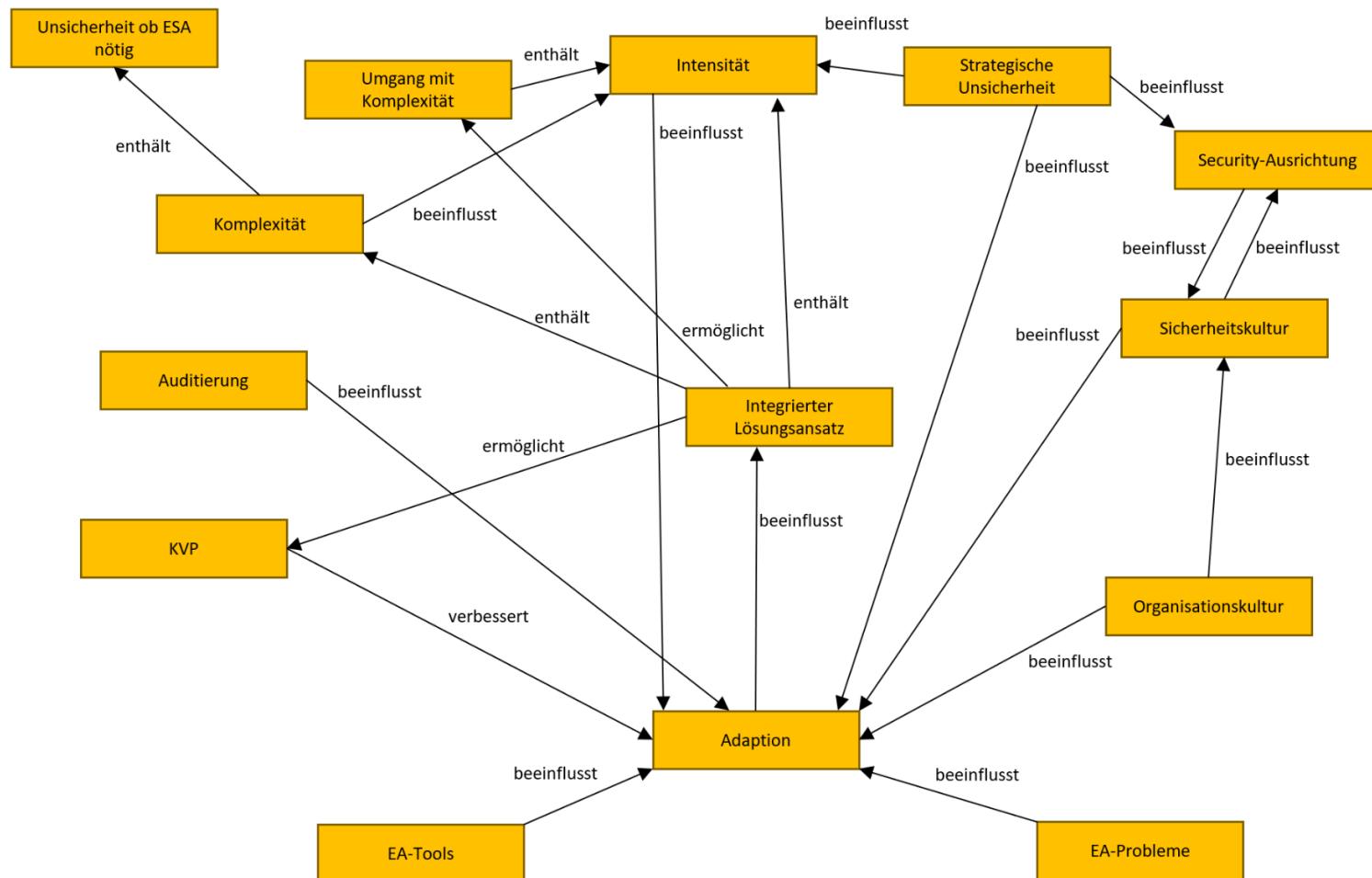


Abbildung 25: Beziehungen zwischen den Kategorien
Quelle: Eigene Darstellung

ANHANG D

Rohe Experteninterview-Transkriptionen

Dieser Anhang wird separat mitgeliefert.