UNIVERSITY FOR CONTINUING EDUCATION KREMS

Department of E-Governance in Business and Administration

Dr.-Karl-Dorrek-Str

. 30

A - 3500 Krems

The extension of the IT-Grundschutz approach with Enterprise Security Architecture capabilities

Master's thesis

as part of the university continuing education programme

Professional MSc Management and IT

Specialisation - Information Security Management

submitted by:

Nicolas Kritharas

28. August 2024

Carer:

FH-Prof. Dipl.-Ing. Peter Kieseberg

AFFIDAVIT

I, Nicolas Kritharas, hereby declare on oath,

1. that I have written my Master's thesis independently, have not used any sources and aids other than those specified and have not made use of any other unauthorised aids,

2. that I have not yet submitted my Master's thesis or significant parts of it as an examination paper in any form either in Germany or abroad,

3. that, if the Master's thesis concerns my company or an external co-operation partner, I have informed my employer about the title, form and content of the Master's thesis and have obtained his/her consent.

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AAL3	Authenticator Assurance Level 3
AM	Architecture Manager
BAA	Business Area Arechitect
BASA	Business Area Security Architect
BCM	Business Continuity Management
BISO	Business Information Security Officer
BSI	Federal Office for Information Security
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	Data protection officer
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 / Information Security
ISCC	IS Coordination Committee
ISMS	Information security management system

ISO	International Organization for Standardisation
ITSO	IT Security Officer
KCI	Key Control Indicator
KPI	Key Performance Indicator
KRI	Key Risk Indicator
CIP	Continuous improvement process
MFA	Multifactor authentication
NDA	Non Disclousre Agreement
NIS	Network and Information Security
OTSO	OT-Security Officer
PA	Programme Architect
PCI DSS	Payment Card Industry Data Security Standard
PSO	Project Security Officer
RCE	Resilience of Critical Entities
RM	Risk management
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 Privilige
TLS	Transport Layer Security
TOGAF	The Open Group Architecture Framework

GLOSSARY

Antifragile

Adjective of the term 'antifragility'. It describes the ability of a system to increase its capabilities under the influence of negative events (cf. Taleb 2012).

Business Attributes

Conceptual abstraction of a requirement that also enables the achievement of this requirement to be measured.

Business Attribute Profile

Conceptual representation of the organisation, mapped via the business attributes to measure performance for compliance with requirements (cf. Sherwood et al. 2009: 218).

Business Capability Model

Graphic representation for visualising all the business capabilities of an organisation and their relationships to each other.

Business Driver

Significant internal or external factors and forces that influence the success of an organisation. They can exist in various forms, e.g. market conditions, technological developments, regulatory frameworks and internal processes.

Business Driver for Security

Represents a derived abstraction of a security requirement of the business driver.

Control Library

Library for the reuse of defined security services and security mechanisms.

Control Objective

A statement of a desired outcome or purpose to be achieved by implementing controls within a particular business activity (cf. Sherwood et al. 2009: 219).

Defence-in-depth strategy

Procedure in which several security measures are used to protect one or more assets.

EA-Artifact

Separate documents that form the enterprise architecture (cf. Winter/Fischer 2006: 1-2).

Enterprise Architecture

Formalises the requirements of various stakeholders and presents them in the context of the company. The interdependencies are visualised with the help of business and technical architectures.

Enterprise Security Architecture

Sub-area of enterprise architecture in which the enterprise architecture is supplemented with an enterprise security architecture. It is the practice of designing, creating and maintaining security in an organisation.

Information security management system

Takes a holistic and coordinated view of the organisation's information security risks in order to identify and implement comprehensive information security controls within the overall framework of a coherent management system (cf. ISO 2022b).

IT-Grundschutz methodology

A methodology that shows "how an efficient management system for information security can be set up and how the IT-Grundschutz compendium can be used as part of this task" (BSI 2017a: 11).

Operating Model

Describes a standardised framework of how an organisation is set up.

RAS(C)I matrix

Model for representing the roles and responsibilities in an organisation.

Risk assessment

Describes the summary of the information security risk management processes 'risk identification', 'risk analysis' and 'risk evaluation' (cf. ISO 2022c).

Sherwood Applied Business Security Architecture

Represents a methodology for developing risk-based enterprise architectures for information security and information assurance and for providing security infrastructure solutions that support critical business initiatives (cf. Sherwood et al. 2009: 1).

Security Mechanism

Physical service that operationalises and implements the specifications of the security services.

Security Service

Logical service that implements the specifications of the business attribute profile, the control objectives and the security strategy (cf. Sherwood et al. 2009: 294).

1. INTRODUCTION

The growing interest in information security (cf. McKinsey 2019: 8-17) is leading to increased pressure on organisations to focus on the protection of information and assets. Due to the large number of systems and their inherent complexity, a movement emerged at the end of the 20th century (cf. Sherwood 1996; Lowman/Mosier 1997) to design information security using architecture. The aim is to achieve a holistic and appropriate protective effect for the organisation. The background to this new way of working is explained below.

This chapter describes the current establishment of information security in organisations as of 2024 and the associated problems. Furthermore, a brief overview of the architecture of information security is provided. The research design and the structure of this thesis are also discussed.

1.1. CLASSIC IMPLEMENTATION OF INFORMATION SECURITY

The subject area of information security is complex and encompasses numerous organisational and technical aspects. There are individual best practices and recommendations for each of these specific topics, the application of which ensures an appropriate level of security depending on the context. In order to establish and maintain the latter in an organisation, organisations can develop an information security management system (ISMS) in accordance with the international standard ISO/IEC 27001, which defines holistic standards and best practices for securing information (cf. ISO 2022a). ISO/IEC 27001 defines a framework for dealing with risks in order to ensure the confidentiality, integrity and availability of information in an organisation. Organisations have the option of certification in accordance with this standard.

In Germany, the Federal Office for Information Security (BSI) developed IT-Grundschutz as an instrument for introducing and maintaining an ISMS. The procedure is set out in the IT-Grundschutz methodology, which is implemented using a bottom-up approach and focuses on the technical aspects of establishing security (cf. BSI 2017a). Organisations that have implemented an ISMS in accordance with IT-Grundschutz can have this certified by external service providers in accordance with ISO/IEC 27001 on the basis of IT-Grundschutz (cf. BSI n.d.).

1.2. ESTABLISHMENT OF INFORMATION SECURITY IN ACCORDANCE WITH BSI 200-2

Information security is designed and established in accordance with the *BSI standard 200-2 IT-Grundschutz methodology* (cf. BSI 2017a) through a security process that comprises several phases and is processed sequentially. The process is illustrated in Figure 1 illustrated.

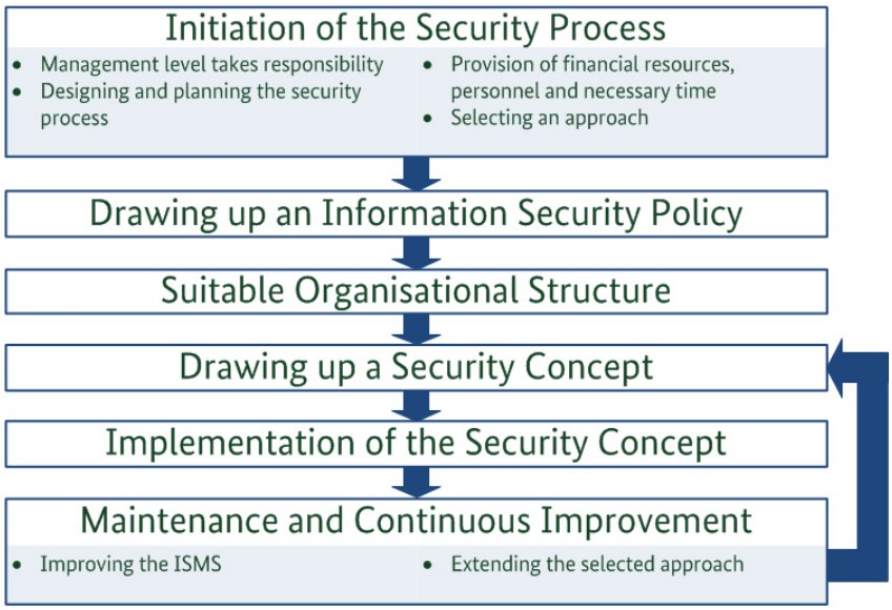

Figure 1: Phases of the security process according to BSI 200-2
Source: (BSI 2017a: 15)

The initiative for implementation comes from upper management, which also monitors and regulates the security process. The first step is to define responsibilities and develop a concept or strategy for information security. The latter includes the framework conditions and information security objectives. The existing business processes and assets are then recorded. Upper management then decides on the establishment of information security, as there are three different approaches in IT-Grundschutz.

Basic protection relates to the relevant business processes and forms the initial introduction to information security. The core protection largely corresponds to the basic protection, but goes beyond this and takes into account additional requirements to ensure an increased need for protection of the relevant business processes. The final approach, also referred to as standard protection, establishes a fully-fledged ISMS and includes consideration of further aspects beyond the relevant processes (cf. ibid.: 20-32).

In the second phase, the specific security guideline for the organisation is designed. The roles and responsibilities for various security topics are defined and the scope of their content is determined. The developed security guideline is communicated to the affected interest groups (cf. ibid.: 32-35).

During the security process, the organisational structure is specified and the information classifications within the organisation are established. Furthermore, the information flow is defined in the context of information security (cf. ibid.: 36-60).

The creation of the safety concept depends on the chosen procedure for safeguarding. The process is identical. Based on the identified processes and their assets, the defined building blocks of the IT-Grundschutz compendium are selected and evaluated to determine whether the requirements defined in the building block are fulfilled. Depending on the respective need for protection, the non-fulfilment of requirements or the lack of security coverage despite the previously selected building blocks, a risk analysis must be carried out in order to determine a possible need for further implementation (cf. ibid.: 76-152).

The identified gaps are closed. The entire process must be monitored through the continuous improvement process in order to exploit optimisation potential (cf. ibid.: 158-170).

1.3. Lack of context in information security

ISO/IEC 27001 and IT-Grundschutz postulate that the design of information security must be aligned with the objectives of the respective organisation (cf. ISO 2022a: v; BSI 2017a: 21). According to both approaches, information security must be established in line with the organisation's objectives. However, the respective standards do not provide a systematic methodology for this (cf. ISO 2017; BSI 2023b), which is why the requirements are perceived as too formal and far-reaching (cf. Bounagui et al. 2019; Diesch et al. 2020).

As a result, organisations focus on establishing information security at the process and technology level (cf. Dhillon et al. 2021: 8; Van Wessel et al. 2011: 869-874). According to Sherwood (cf. 2005: 28), however, this orientation proves to be suboptimal, as the organisation-specific requirements are not fully taken into account and therefore do not bring the desired success. The process-orientation of security requires strategically aligned business process management, which, according to Schmelzer and Sesselmann (2020), is not widespread in practice (cf. 170-171). The exclusive focus on technology does not offer an organisation com-

prehensive protection, which is why organisational measures should be supplemented. This creates a socio-technical perspective that enables holistic information security (cf. Iivari/Hirschheim 1996).

The lack of consideration of the organisational context when establishing information security is due to various factors. In addition to the inadequate application of a systematic methodology, the methods used themselves are also decisive. According to Baskerville (1993), these can be divided into three generations.

The first generation (checklist method) consists of three parts:

1. Checklist consisting of a list of security measures that could be implemented,
2. Risk management, which is used to determine the necessity of implementing the respective measures from the checklist, and
3. cost-effective implementation (cf. ibid.: 380-389).

The second generation (mechanistic design method) consists of five parts:

1. Inventory of assets and threats,
2. Viewing the safety measures list - an activity that has been adopted from the first generation, but can be expanded independently,
3. Risk management,
4. Prioritisation of security measures according to risk management and
5. regular reviews to maintain the design of the implemented information security (cf. ibid.: 390-400).

IT-Grundschutz and ISO/IEC 27001 can be assigned to the second generation. The ISMS is audited on the basis of the first generation. The action steps of the two generations show that the context of the organisation is not included in the working and auditing methods. In addition, the scientific literature shows that the traditional approach of the first and second generation according to Baskerville dominates (cf. Dhillon et al. 2021: 2-3).

The third generation (logical-transformative method) consists of three parts:

1. Requirements analysis to identify the problem and understand the context,
2. Abstraction of the organisation to different meta-levels and
3. Design of the solution based on the abstractions and requirements (cf. Baskerville 1993: 401-408).

According to Siponen (2005), one possible reason why the third generation is not considered or is unknown is that the various methods for establishing information security in organisations are developed by research groups that work according to different paradigms and do not include other research results (cf. 340). The main

difference between the logical-transformative method and the other two methods is that the focus is on the requirements analysis and the organisations are abstracted into meta-levels in order to view security from multiple perspectives. As a result, the peculiarities of an organisation can be taken into account when designing information security. This requires that the person responsible for the architecture has experience in developing the architecture so that the security measures are effective and no subsequent modifications are necessary, as potential planning errors are only recognised when the measures are implemented later.

Therefore, the design of an architecture that meets the information security requirements of an organisation is done by modelling according to various abstracted meta-levels. This is based on the previous generation. An information security architecture is conceptualised in accordance with the requirement to integrate information security into the enterprise architecture in accordance with SP 800-53 (cf. NIST 2020: 198). The former is also referred to as Enterprise Security Architecture (ESA). It allows a holistic conception of information security and can also be integrated into the enterprise architecture in order to expand the overall architecture of the organisation.

1.4. Definition of the enterprise security architecture

ISO/IEC/IEEE 15704:2019 defines the term 'architecture' as the conceptualisation of the form, function and purpose of an enterprise in its environment. This conceptualisation is embodied in the elements of the enterprise, the relationships between these elements, the relationships of the enterprise to its environment and the principles for the design and development of the enterprise (cf. ISO 2019a). The real world is abstracted and visualised in a defined modelling language. Reducing the complexity of an entity allows various analyses to be carried out in order to address the requirements of different stakeholders in the architecture. Architectures are developed using methodical process models to (1) create transformation plans that implement an organisation's strategy, (2) perform various types of analyses and (3) support decision-making.

The aim of enterprise architecture is to formalise the requirements of various stakeholders and present them in the context of the company. To this end, the dependencies between business and technical architectures are shown. The term 'enterprise architecture' was introduced in 1987 in the article *A framework for information systems architecture*. At the same time, the Zachman framework was presented

for the first time (cf. Zachman 1987). The framework represents an enterprise ontology and a fundamental structure for enterprise architecture.

The expansion of enterprise architecture to include a holistic security architecture has been driven by the development of various ESA frameworks such as 'Sherwood Applied Business Security Architecture' (SABSA) (cf. Sherwood 2005) and 'The Open Group Architecture Framework' (TOGAF) (cf. The Open Group 2022b). The latter is an enterprise architecture framework that does not explicitly focus on security. The methodical approach to implementing security supports the strategy and the organisations in dealing with complex business processes (cf. Goudalo/Seret 2009; Wang et al. 2009).

In TOGAF, security requirements are implicitly taken into account when recording and analysing stakeholder requirements. The implicit working method harbours the risk that not all security aspects are taken into account. To counter this, an integration model was developed in which SABSA is incorporated into TOGAF in order to explicitly consider security (cf. The Open Group 2011). In practice, SABSA is therefore taken into account in the development of the ESA (cf. Sherwood et al. 2009: 4).

1.5. SABSA

The SABSA framework has a similar structure to the Zachman framework and abstracts the organisation into five levels. The abstraction and the ways of looking at the organisation can be seen in Figure 2. The architecture matrix comprises the results of the respective level. The last row serves as a reference to the management matrix, which shows the measures required to achieve the respective results of the architecture matrix.

The context of the organisation is determined as part of the contextual architecture. Firstly, the business requirements are collected in order to determine the respective security requirements on this basis. Furthermore, entity and relationship models are created in order to record the affected organisations in the area under investigation. This is followed by a risk analysis to identify potential risks and opportunities (cf. Sherwood 2005: 169-215; Sherwood et al. 2018).

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

Figure 2: Architecture matrix
Source: (Sherwood et al. 2018: 7)

The key performance indicators, the key risk indicators, the key control indicators and the performance targets for each security requirement determined are defined in the conceptual architecture, as is the target state (control objectives) of security. Within these control objectives, the security measures of the various security standards such as IT-Grundschutz (cf. BSI 2017a), ISO/IEC 27001 (cf. ISO 2022a), PCI DSS (cf. PCI Security Standards Council 2024) and NIST SP 800-53 (cf. NIST 2020) can be compiled and formalised in order to establish uniform security that complies with the security standards (cf. Sherwood 2005: 217-283; Sherwood et al. 2018).

The Logical to Component Architecture models the architecture according to the specifications of the previous level by concretising the modelling (cf. Sherwood 2005: 289-405; Sherwood et al. 2018). This can be illustrated using an example:

- Logical: When entering the domain, authentication according to AAL3 is required.
- Physical: Digital certificates are used for authentication.
- Component: The X.509 standard is used.

1.6. RESEARCH DESIGN AND STRUCTURE OF THE THESIS

In this thesis, the methodology 'Design Science Research' (DSR) is applied as it focuses on the design and evaluation of innovative artefacts so that organisations can overcome key information-related challenges (cf. Hevner et al. 2004). Furthermore, this methodology has already been successfully applied in previous work on ESA (cf. Loft et al. 2022; Graham et al. 2021; McClintock et al. 2020). This thesis follows the DRP guidelines and implements them through the 'Design Science Research Process' (DSRP) methodology (cf. Peffers et al. 2007), which is also embedded as the document structure of this master's thesis, see Figure 3. The DSRP according to Peffers was chosen as the research process because it operationalises the specifications of the DSR according to Hevner and specifies the course of implementation in accordance with the methodology.

In Figure 3 visualises the linking of the various DSRPs. The demonstration process is outside the scope of this work, as the aim is to create a conceptual model, which is why the demonstration process is not considered.

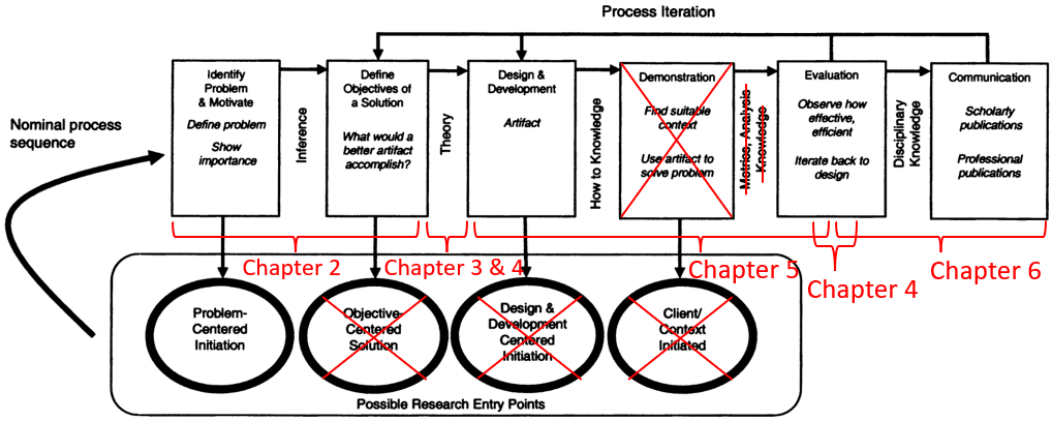

Figure 3: Research design
Source: Based on (Peffers et al. 2007: 54)

In chapter 2 identifies the problem that relates to the first step of the DSRP. For this reason, this thesis follows a problem-orientated approach.

In chapter 3 describes the research methods used in this study. The method used to evaluate the artefact developed is also discussed.

In chapter 4 presents the results of the inputs received for the "Design & Development" phase and describes the results of the evaluation.

In chapter 5 describes the development and evaluation process of the artefact. It also outlines ways in which the artefact could be implemented in practice.

In the discussion (cf. chapter 6), the artefact developed is examined with regard to the fulfilment of the previously defined requirements. This work and the results are also evaluated on the basis of Hevner's seven guidelines (cf. 2004: 83).

In chapter 7 'Conclusio' outlines the relevant research contributions of this thesis and identifies possible aspects for future research.

2. OBJECTIVES OF THE THESIS

This chapter deals with the problem of establishing information security in organisations. Firstly, the requirements for the organisation of information security are discussed, on the basis of which the research question of this thesis is developed.

2.1. PROBLEM IDENTIFICATION

As described in chapter 1.3 the security standards stipulate that information security must be aligned with the organisation's strategy. In the absence of references or descriptions in the implementation guidelines of these standards (cf. ISO 2017; BSI 2023b), those responsible are confronted with difficulties in achieving the objectives. The low likelihood of integrating security officers into management committees (cf. Stewart 2018: 47), the prevailing emphasis on cybersecurity in the public debate (cf. BSI 2016: 3-5) and the increasing number of regulatory requirements in cybersecurity such as PCI DSS (cf. PCI Security Standards Council 2024), EU NIS2 and EU RCE/CER Directive result in a focus of security measures on technical and procedural aspects (cf. Dhillon et al. 2021: 8; Van Wessel et al. 2011: 869-874).

In order to align information security with an organisation's strategy, an architecture is required. This supports organisations in designing and establishing the information security strategy, the organisational strategy and in dealing with complex business processes (cf. Goudalo/Seret 2009; Wang et al. 2009).

The focus of this thesis is on the establishment of information security in accordance with IT-Grundschutz. This raises the question of how the methodology can be expanded in order to create a framework in which information security is designed and established in the organisation in a context-specific manner on the one hand and the different regulatory requirements in the organisation are standardised on the other.

2.2. DESIGN REQUIREMENTS

The aim of this thesis is to extend the IT-Grundschutz methodology to enable the design and establishment of information security according to the organisational strategy. In order to generate an artefact that can be used in research and business, the following requirements are placed on the result:

Requirement 1: The extended IT-Grundschutz methodology must include ESA capabilities.

Requirement 2: Compliance with IT-Grundschutz should continue to be guaranteed in order to be able to have the ISMS certified in accordance with BSI Standard 200-2.

Requirement 3: The result should generally be clear enough to be applicable in practice.

2.3. RESEARCH QUESTION

The following research question will be answered so that information security can be designed and established according to the organisational strategy in the IT-Grundschutz methodology:

How can the IT-Grundschutz methodology be combined with SABSA to develop a holistic security architecture?

The research question is limited to the question of the methodology for developing information security according to the strategy and objectives of an organisation. The Duden editorial team (n.d.) defines methodology as a "defined way of proceeding". In this work, the consideration of security measures is excluded. When answering the research question, it must be taken into account that the methods described in chapter 2.2 must be complied with and answered.

3. RESEARCH METHODS USED

This chapter provides an overview of the methods used to answer the research question. Firstly, a general overview of the methods is given, followed by the main reasons for their use and the methods are compared with the research question and the requirements from chapter 2.2 are linked. This is followed by a detailed explanation of each individual method.

3.1. INVESTIGATION APPROACH

Qualitative research methods were used to answer the research question. In Figure 4 visualises the research approach used for this master's thesis.

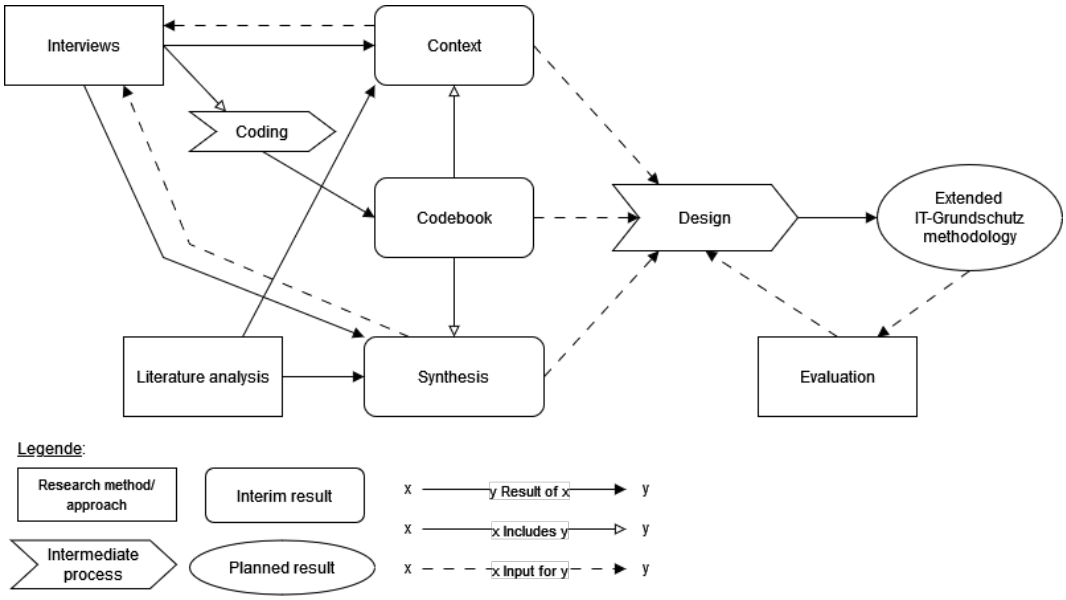

Figure 4: Research approach of this thesis
Source: Own figure

The evaluation approach consists of two steps: Interim evaluation and final evaluation. The interim evaluation is based on the expert interviews conducted. The final evaluation is carried out by the author of this thesis, whereby the results are evaluated against the requirements. In the DSR approach, the interim results of the evaluation method provide continuous feedback for the design. Therefore, the design cycle is run through several times.

The aim of the literature analysis is to formulate the problem to be analysed, identify relevant concepts and methods and position the study (cf. Ghauri et al. 2020: 57). In this work, a literature analysis was first carried out in order to identify the connections within the topic and existing concepts on the one hand and to model an initial interim result as a basis for the expert interviews on the other.

As part of the expert interviews, the interim product was presented and feedback on it was obtained. In addition, an interim evaluation was carried out by the experts. This procedure served the purpose of gaining an understanding of the experts' views on the presented approach and further context for the establishment of information security. In addition, possible practical tips for use could be collected.

The results of the surveys were integrated into the model in order to be able to evaluate the extent to which the artefact would promote the solution of the problem in the final evaluation (cf. Peffers et al. 2007). The evaluation was intended to determine the extent to which:

1. experts agree with the extended IT-Grundschutz methodology and believe that the approach helps them to set up an architecture in line with organisational objectives,
2. the extended IT-Grundschutz methodology is accepted and
3. something is still missing.

3.2. LITERATURE ANALYSIS

In order to identify relevant backgrounds and procedures for ESA, a systematic literature analysis was carried out. In addition to scientific literature, grey literature was also included, as methodologies and procedures are described in the field of 'enterprise architecture' that are sometimes considered impractical in practice (cf. Wagter et al. 2005; Ross et al. 2006: vii). For this reason, variations of enterprise architecture methods have been developed (cf. Carr/Else 2018; Ivas 2023; Namagembe et al. 2023). In order to prevent this discrepancy in the modelling of the extended methodology, an attempt was made to incorporate information on implementation options into the methodology and thus close the gap between research and practice. This could ensure the success of the application beyond this thesis and would fulfil the third requirement for the result from chapter 2.2.

A structured approach was chosen for the search for scientific literature via the platforms ACM Digital Library, IEEE Xplore, ScienceDirect, dblp, Österreichischer Bibliothekenverbund, Bayerische Staatsbibliothek and the university libraries of RWTH Aachen University, Karlsruhe Institute of Technology, Ludwig-Maximilians-Universität, Technological University of Munich and University for Continuing Education Krems. The platforms are scientific online databases. The search terms can be found in the appendices B.1 'Structured literature research on IT-Grundschutz' and B.2 'Structured literature search on ESA and SABSA' can be taken from these.

The following steps were taken:

1. Search in selected scientific online databases for defined search terms;
2. Export of the results as a list using scripts that remove duplicates;
3. Check the title and abstract of each article to see if it is an ESA;
4. Assess whether the text was freely available digitally via Google Scholar, University Library of the University for Continuing Education Krems and own access through memberships (IEEE-Membership, Science Direct, Bavarian State Library);
5. Evaluate the articles by skimming the text and checking the introduction and conclusion to see whether the focus was on technology;
6. read other articles carefully and assess whether ESA has been discussed at a meta-level, and
7. Check whether information enriched the extended methodology.

Furthermore, unstructured searches were carried out using the search engines 'Google Scholar' and 'Google'. Due to the high number of results, filtering was necessary (cf. Giustini/Boulos 2013: 4). Although the content was constantly changing, unknown updating practices were used and a lack of reliability was noted, these were to be used in a complementary manner in the literature analysis (cf. Mastrangelo et al. 2010). In addition, the Google search engine supported the search for grey literature using various keywords.

3.3. EXPERT INTERVIEW

As part of this study, interviews were conducted with specialists and managers in the field of information security. The term 'professional' refers to a person who deals with information security or ESA in practice, in counselling or in research. Researchers are familiar with the current state of research in the field of information security and ESA, while practitioners have practical experience in the application of methods for implementing information security and are aware of the various limitations and long-term effects in an organisation. The consultants can contribute their experience from different organisations to the discussion. The perspective of those responsible for information security in an organisation is relevant, as they establish the ISMS and create an information security strategy. The perspectives gained through the interviews provided a holistic picture of the topic. The aim of the interviews was to deductively test the extended methodology and to generate a theory on the use of the extended methodology using an inductive approach.

The extended methodology was presented at the beginning of the interviews. Based on this, a semi-structured survey took place. The use of predefined questions made it possible to guide the interviews in a targeted manner. In addition, a topic was defined in advance for each question in order to simplify coding. A list of these predefined questions can be found in Appendix C.1 'Interview questions and itheir topics'. The open structure gave the interviewer a more precise and clearer perspective of the interviewees, as they were able to answer according to their own ideas (cf. Ghauri et al. 2020: 114). Follow-up questions about the answers led to additional information that would not have been possible in a structured interview (cf. ibid.: 115).

3.4. DATA ANALYSIS OF THE EXPERT INTERVIEWS

The interviews were conducted using video telephony. The recordings were then subjected to automated transcription. The former serve to check the correct transcription, which is essential for analysing the data.

The transcribed responses were coded using a generic form of open coding based on grounded theory (cf. Corbin/Strauss 2015). The grounded theory methodology was used for the study, although the entire approach was not taken into account, as theoretical saturation could not be achieved. The reasons for this were the inconsistent definition and the divergent views on the systematic approach and how to deal with it in the ESA. This can be attributed to the low information power of the interviewees (cf. Malterud et al. 2016), due to the low prevalence of ESA. Furthermore, according to Hennink et al. (cf. 2016: 15), there are no generally applicable criteria for measuring saturation. Instead, different interpretations of the concept of saturation can be found in the literature (cf. Morse et al. 2014; Hancock et al. 2016; Fusch/Ness 2015; Hennink et al. 2019). According to Fusch and Ness (cf. 2015), this means that theoretical satiation is subjective and satiation is assessed differently by different people. The *QDA Miner Lite* application was used for the open coding. The transcripts were imported and coded using a generic form of open coding. In addition, the codes were grouped according to the questions asked in the interview. The coded transcripts were then analysed. An attempt was made to find relationships between the answers given. Codes with a frequency of more than 50 % were analysed in detail, as they were considered to be recurring themes.

3.5. EVALUATION

The evaluation phase comprises two stages, each based on the results of the expert interviews and the overall results. In accordance with the feedback, the extended methodology was evaluated and tested to determine the extent to which the impulses could be integrated.

4. RESULTS OF THE RESEARCH METHODS

This chapter contains the results of the literature analysis and the expert interviews.

4.1. LITERATURE ON ENTERPRISE SECURITY ARCHITECTURE

The literature identified on the topics of ' IT-Grundschutz ', 'SABSA' and 'ESA' is discussed below.

4.1.1. SEARCH RESULTS

Peer reviews, journal articles, books and book chapters in German and English up to 10 August 2024 were included in a structured search. Two separate searches were carried out to obtain a comprehensive overview of IT-Grundschutz and the ESA. The results were exported using scripts, whereby duplicates were automatically sorted out according to the Digital Object Identifier (DOI) or title with the inclusion of author names.

During the literature search on IT-Grundschutz, a total of 167 unique texts were identified and grouped according to their content. They can be found in Appendix B.1 'Structured literature research on IT-Grundschutz' and Figure 5 and Figure 5.

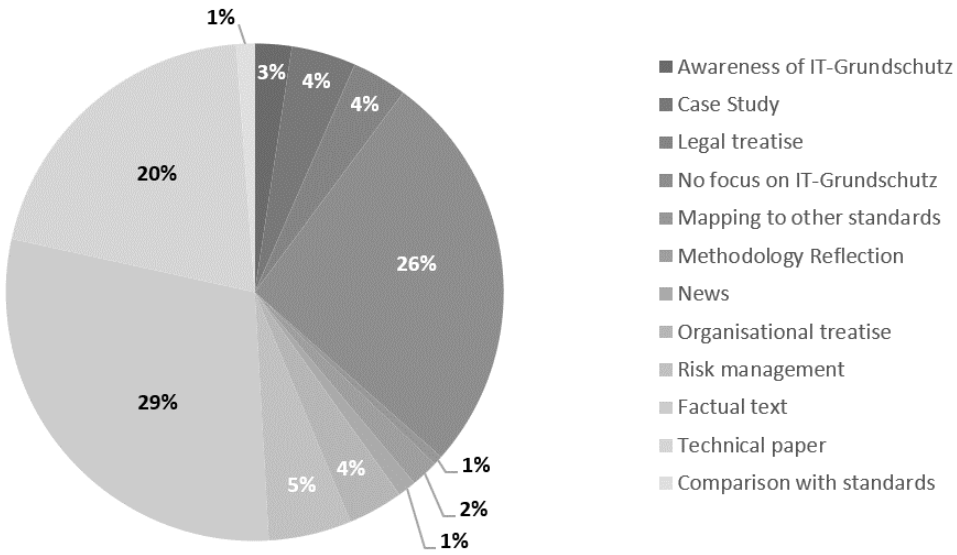

Figure 5: Breakdown of text types for IT-Grundschutz
Source: Own figure

In the second step, the abstracts and texts were checked for compliance with the objectives of the study. The exclusion criteria were:

1. Factual texts with an explanation of the IT-Grundschutz methodology,
2. Texts that make little or no reference to IT-Grundschutz,

3. Articles that demonstrate awareness of IT-Grundschutz,
4. technical papers or texts focussing on technical aspects,
5. Case studies in which only the application is written about, without reflecting on the methodology, and
6. News.

Inclusive features were:

1. Texts focussing on the analysis of IT-Grundschutz,
2. Comparisons of IT-Grundschutz with other security standards and
3. Case studies on IT-Grundschutz with a critical analysis of the methodology or lessons learnt on the methodology.

The procedure described resulted in a reduction of the results to six texts. Three of the texts are legal treatises, two of which deal with the issue of data protection in the context of IT-Grundschutz (cf. Meints 2006; Claus 2007) and the third addresses compliance with the KRITIS-DachG through ISO/IEC 27001 and IT-Grundschutz (cf. Maseberg 2023). Another text is based on a legal background. This compares various security standards with one another in order to cover the missing aspect of legal requirements for IT and security (cf. Simić-Draws et al. 2013). The fifth text reflects on IT-Grundschutz and presents a proposal for a top-down approach as well as some organisational controls (cf. Neitzel/Witt 2012). The last text discusses a mapping of TOGAF to IT-Grundschutz (cf. Mathew et al. 2018).

The literature research carried out revealed that there are no disputes with ESA in the area of IT-Grundschutz. Furthermore, it can be stated that there is little theoretical foundation for IT-Grundschutz. This finding is not limited to IT-Grundschutz, but was also demonstrated in a literature analysis of scientific articles on ISO/IEC 27001 (cf. Culot et al. 2021).

The second search for ESA resulted in a total of 95 unique texts. The list can be found in Appendix B.2 'Structured literature search on ESA and SABSA'.

The exclusion criteria were:

1. Failure to consider safety,
2. Focus on technical safety,
3. Focussing on special topics such as risk management,
4. lack of focus on architecture and
5. Texts for previous versions that have been revised (e.g. SALSA).

Inclusive features were:

1. Focus on ESA,
2. In-house developments of frameworks and
3. Critical observations of the ESA.

This filtering reduced the number of unique texts to eleven. Of these, six texts consist of in-house developments of ESA frameworks (cf. Loft et al. 2022; Larno et al. 2019; Ahmed et al. 2017; Lowman/Mosier 1997), two of which are similar to SABSA (cf. Graham et al. 2021; McClintock et al. 2020). Another text covers risk modelling and the possibility of automated decision making in ESA to accelerate architecture creation and improve quality (cf. Grov et al. 2019). This proposed automation process based on checking using ontologies could be extended by the possibility of mapping security requirements to the STRIDE model (cf. Peterson 2010) in order to simplify architecture work with SABSA. A total of two texts on SABSA were found, the only edition on SABSA (cf. Sherwood 2005), in which the processes and methods described are partly outdated, and the description of the conceptual architecture using metamodels (cf. Pleinevaux 2016). The last text deals with the quantified evaluation of ESA (cf. Alshammari 2017).

The unstructured searches were carried out with similar and other keywords such as ESA in various combinations in Google and Google Scholar. Twenty articles on SABSA and ESA were recorded. Revisions of the outdated edition on SABSA (cf. Sherwood 2005) are distributed in white papers and conference proceedings (cf. The SABSA Institute 2023). A literature analysis of the current trends and core areas from 1996 to 2021 showed a focus on the operational aspects of information security (cf. Shiau et al. 2023).

4.1.2. Adaptive knowledge transfer

Despite the small number of treatises on ESA, aspects of enterprise architecture can be adapted. The methods and processes that are relevant for the architecture work and the environment in ESA are described below.

From a historical perspective, the establishment of a holistic enterprise architecture is the result of an evolution of the architecture, which is driven by the need to be able to deal with increasing complexity in an organisation. The evolution can be divided into the four maturity levels 'Business Silo', 'Standardised Technology', 'Optimised Core' and 'Business Modulatiry' (cf. Ross et al. 2006: 97-120). This development also reflects the transformation of enterprise architecture in organisations

(cf. Barrera et al. 2011). The visualisation of the maturity levels in Figure 6 also shows the distribution of IT investment costs.

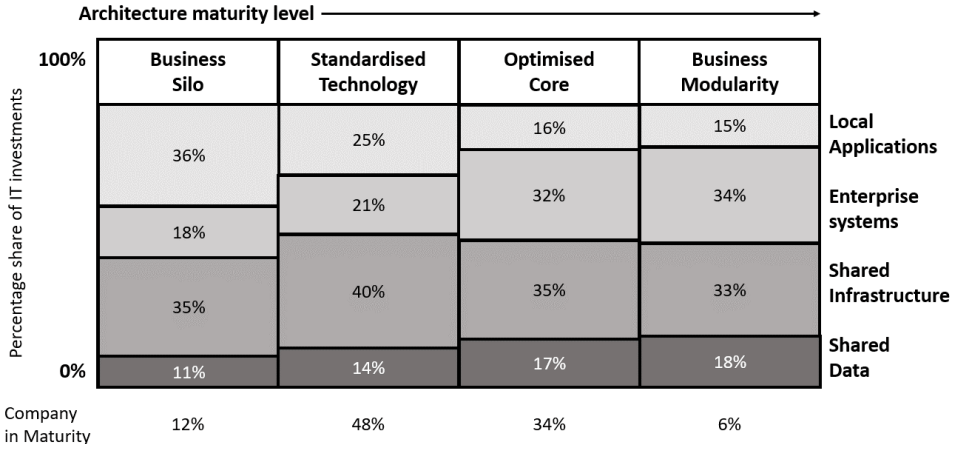

Figure 6: Maturity levels of the enterprise architecture
Source: Based on (Ross et al. 2006: 100)

ISO/IEC/IEEE 42020:2019 (cf. ISO 2019b) contains process descriptions for the creation, control and management of architectures. Six processes are highlighted and their relationship to each other is shown. The latter can be Figure 7 can be taken from it.

The architecture governance process defines the guidelines and provides instructions for dealing with architectures. Architecture governance describes the direction and objectives of the architecture in order to keep the different architectures uniform and ensures that organisational needs are addressed (cf. ISO 2019b: 15-20). To ensure that the guidelines and specifications of the architecture are adhered to, the architecture management process is used as a review and control body. This ensures the timely, effective and efficient achievement of objectives (cf. ibid.: 20-27).

Overall, the ISO/IEC/IEEE 42020 standard defines three core processes. The first is architecture conceptualisation (cf. ibid.: 27-38). It characterises the problem space and determines a suitable solution that addresses the requirements of the stakeholders and the architecture.

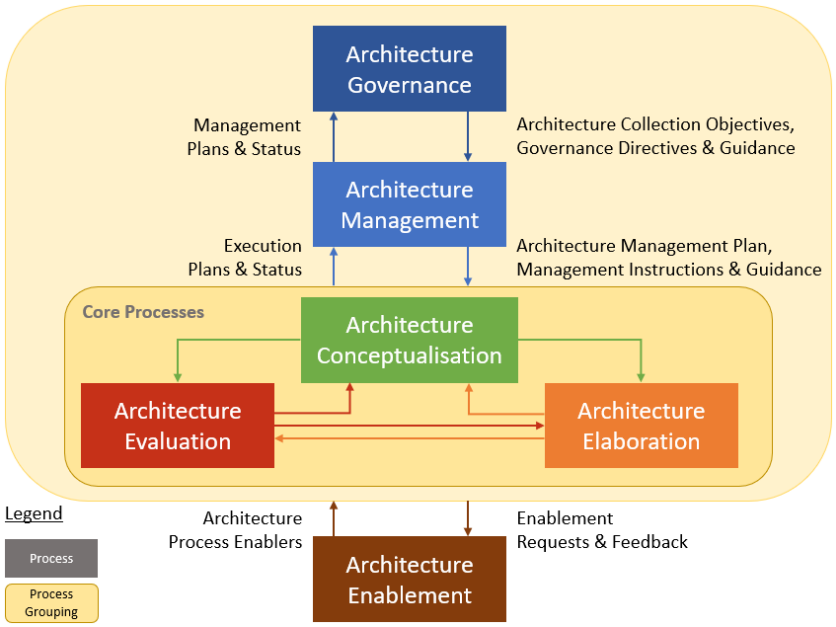

Figure 7: Architecture processes
Source: Based on (ISO 2019b: 9)

The second process is the architecture evaluation, i.e. the extent to which the objectives and requirements are fulfilled (cf. ISO 2019b: 38-47). The evaluation is structured in three tiers: Architectural Analysis, Value Assessment and Evaluation Synthesis. The architectural analysis examines the key characteristics of an architecture, for example its properties in relation to specific dimensions such as security, costs, performance and others. In addition, the relevant characteristics of the architectural unit and the actual or potential impact on stakeholders or the environment are analysed. In addition, the architectural vision, principles and concepts relevant to achieving the objectives are examined (cf. ISO 2019c: 11). The value assessment determines the scope and type of value of an architecture that stakeholders can expect. This value can be described quantitatively or qualitatively (cf. ibid.: 9). The highest tier is the evaluation synthesis. Here, the results of several value assessments are combined to determine the extent to which the evaluation objectives are achieved. Stakeholders' concerns about the evaluation can be addressed through the evaluation synthesis (cf. ibid.: 7). An overview of the evaluation tiers and their relationships to each other can be found in Figure 8 can be seen in Figure 8.

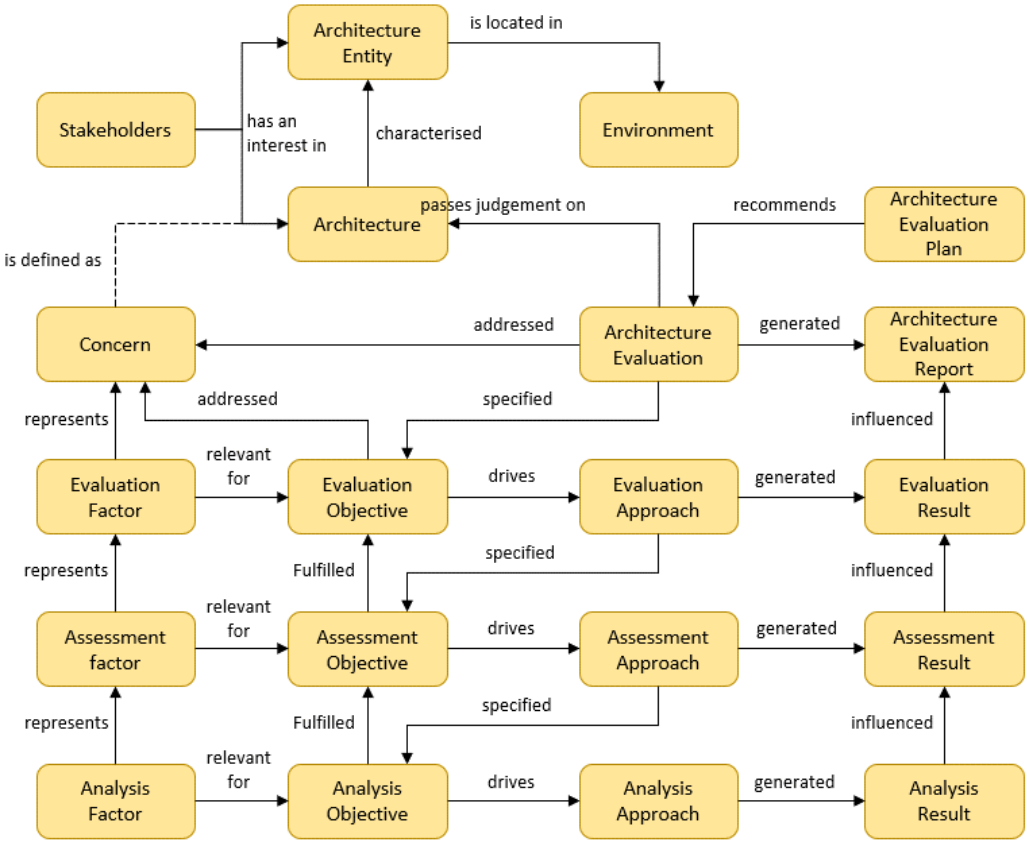

Figure 8: Evaluation of the architecture
Source: Based on (ISO 2019c: 13)

The third core process is Architecture Elaboration. This process is the actual architectural work, as the architecture is documented in a complete and correct manner that is sufficient for the intended use (cf. ISO 2019b: 47-53).

The final process is architecture enablement. The aim is to enable the departments to carry out the architecture processes by providing the necessary resources, deploying qualified staff and providing staff with further training.

Enterprise architecture works with six EA artifacts that influence each other (cf. Kotusev 2021: 129-142). Figure 9 is used to visualise the EA artifacts and describe their relationships to each other.

The 'Considerations' document the decisions made with regard to the collaboration between the organisation and IT. The 'Vision' describes the long-term support of the organisation through IT. The 'Outlines' define the specific implementations of an organisation's IT initiatives. The 'Standards' define technical rules that form the basis for the implementation of IT systems. The 'Landscapes' present the current status of the IT landscape and describe the decisions regarding its future development. The decisions on the exact specifications are documented under the last EA artifact 'Designs' (cf. ibid.: 129-142).

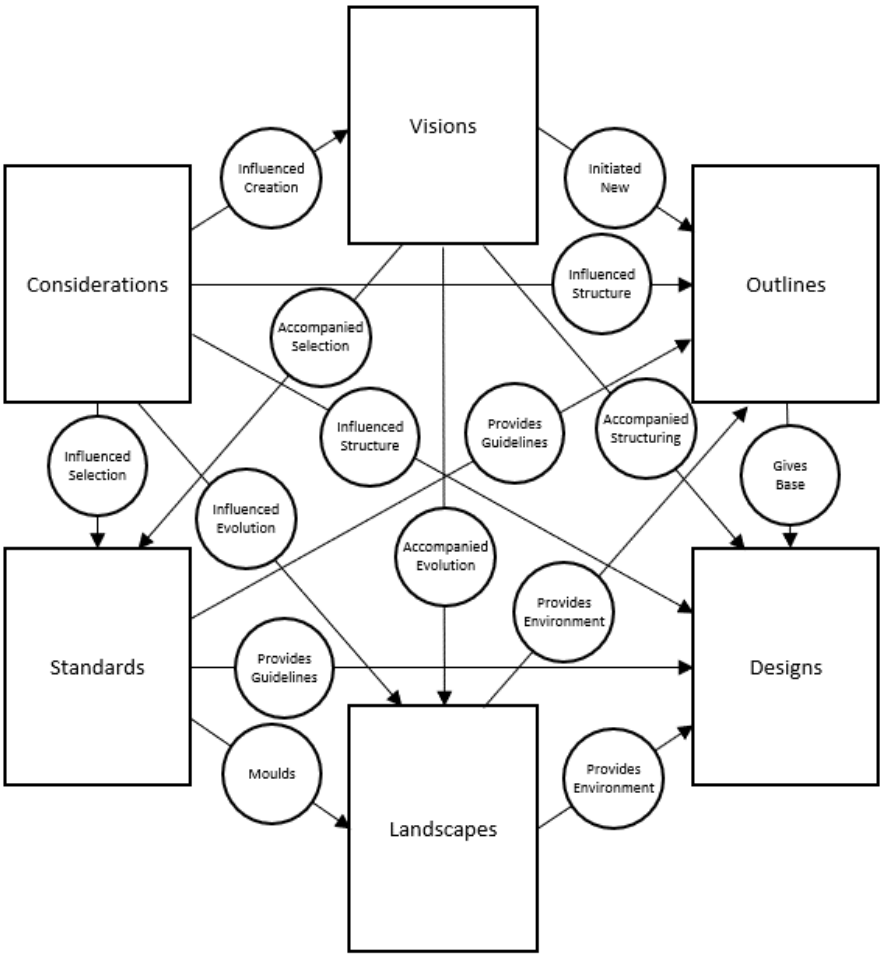

Figure 9: CSVLOD model
Source: Based on (Kotusev 2021: 66)

Traditional enterprise architecture frameworks such as TOGAF (cf. The Open Group 2022b) have their origins in IBM Business Systems Planning (cf. IBM 1984), as the frameworks were influenced by their respective predecessors (cf. Kotusev 2016: 396-407). Organisations are viewed as systems and their requirements are derived from the organisational strategy.

However, there are two alternative approaches as to how an enterprise architecture can be set up in an organisation. The first approach is Enterprise Architecture as Strategy, according to which organisations should align their strategy with the enterprise architecture. The architecture should be structured according to the organisation's operation model (cf. Ross et al. 2006). Due to the reversal of the relationship between enterprise architecture and strategy, this approach is particularly suitable for larger organisations that do not work in a volatile environment. The second alternative is the Dynamic Architecture (DYA) approach (cf. Wagter et al. 2005). This propagates the principle of "just enough, just in time" (ibid.: 44). This means that architecture activities should only be carried out when they are needed.

In addition, the circle of participants should be kept as small as possible. Another special feature is that only the respective business case is considered and no strategy is included. This makes DYA suitable for smaller organisations that operate in an unpredictable environment.

Although enterprise architecture sustainably improves the performance of an organisation (cf. Gerow et al. 2014; Byrd et al. 2006) and communication between IT and the business (cf. Wagner et al. 2014; Luftman/Brier 1999), there is a lack of concrete implementation descriptions for its establishment (cf. Karpovsky/Galliers 2015; Coltman et al. 2015; Chan/Reich 2007). This makes it difficult to develop competences and establish an effective architecture.

4.2. Perspectives of the experts

In the appendix C.2 'Background information on the expert interview' is presented in Table 15 shows the distribution of interviewees. Representatives of all relevant Chief Information Security Officer (CISO) interest groups, practitioners, consultants and researchers were included in the expert interviews. It can also be seen that more than half of the people invited cancelled (at short notice). A total of ten expert interviews were conducted via *Microsoft Teams*. These were recorded and automatically transcribed using Microsoft Teams. The smoothed transcripts can be Appendix D can be found in Appendix D. In order to contextualise the perspectives of the individuals, Appendix C.2 'Background information on the expert interview' in Table 16 the level of security maturity of an organisation in which the person is employed or advises. For data protection reasons, the interviewees are treated anonymously.

As described in chapter 3.5 each transcript was coded. Appendix C.3 'Codes and their frequency' contains an overview of the codes created with their respective frequency in the expert interviews. The answers to the open questions and the follow-up questions led to further information, which was then assigned a code from another topic. In order to clarify the relationships between the codes and the content, the codes were visualised using *Microsoft PowerPoint* and grouped into categories according to their content. The illustration can be found in the appendix C.4 'Summarised coding'. Synthesising the information content into categories simplifies the analysis and enables a holistic view of the extended IT-Grundschutz methodology. Categories with a frequency of >= 50 % were analysed in more detail, as they are considered recurring categories. The recurring categories interpreted by the author of this paper from the expert interviews are described below.

The relevance of the various interviewees for the categories is shown by placing markers in brackets in the category descriptions. These consist of the initial letter of the role (F for researcher, P for practitioner, B for consultant, C for CISO) and the number of the person.

Integrated solution approach

The extended IT-Grundschutz methodology discussed in the expert interviews was perceived as an integrated solution that enables end-to-end development and the establishment of information security in an organisation (P1, B2, F2). This end-to-end approach creates transparency regarding the use of the security measures to be implemented and makes work easier thanks to the predefined manner in which they are to be used and where (P3). In addition, in contrast to the existing security standards, this can avoid interpretations of how certain security measures should be applied (P3). Deriving the information security requirements from the organisational objectives, structuring them according to a target vision, modelling the architecture using SABSA and the operational description for implementing security with IT-Grundschutz represent a complementary addition. The extended methodology would provide guidance on establishing information security from the strategy to the operational measures (P1, F2). At the same time, the procedure ensures the traceability of security (P3). The description of the procedure also enables the target-orientated implementation of work activities, which ensures the structured processing of tasks (P1, P3). In addition, the extended methodology supplements measurability in order to improve safety on the basis of measured values (B1). The structure allows a holistic view of information security (C2, F1), which stands out from other standards as the focus is on flows rather than hierarchies (B3).

The integration of this solution approach into existing organisational structures and processes is influenced by the organisational culture, security culture and adaptation (cf. Figure 25).

Safety culture

As part of the expert interviews, follow-up questions were asked about the interviewees' answers in order to understand the underlying context. This revealed the working methods for safety.

One aspect is that organisations would align their security with compliance in order to meet regulatory requirements (F1, C2, B2, B3, P2). Building on this, organisations would work with checklists to design and establish information security (F1). Depending on the professional background of the people in a security team, the focus would be on a technical or a process-based approach (B1). For this reason, the extended methodology is viewed with scepticism, especially in regulated industries, as there are no publicly known applications (B3).

Although IT-Grundschutz enables the creation of profiles to adapt the methodology to the respective industry, the organisational context is not considered at the higher level (P2). It was also noted that - despite the aim of certifying the ISMS - information security was cited as an unstructured way of working in various organisations (C1).

The sum of the statements in this category leads to the conclusion that information security is driven by an extrinsic motivation that can be traced back to the organisational culture. The possible backgrounds are shown in the 'Organisational culture' category.

Organisational culture

The identified codes on the challenges and risks in the application of the extended methodology were primarily found in this topic area.

The application of the extended methodology requires the commitment of management (P1), which may not be present (C1). According to a field report, although the enterprise architects support the application of the extended methodology, the specialist departments are against the architecture approach due to its intensity - a category that is highlighted in the course of this chapter (F2, P3). To counteract this, the added value of the new way of working should be emphasised (P3). In addition, the structure and organisation of the extended methodology could be misunderstood by stakeholders, which could lead to false expectations regarding the possibilities (C2).

In addition to the lack of support from the departments, cooperation between the departments could also be problematic (B1). The introduction could also lead to conflicts of interest, as the integrated approach raises the question of the extent to which the organisational structure and processes need to be adapted (F2).

According to the results of a survey, the organisational culture has no intrinsic motivation to establish information security holistically. According to one study, the

extrinsic motivation is due to the desire of customers. Information security or certification according to ISO/IEC 27001 improves the image of the organisation (cf. Liao/Chueh 2012: 7867) and increases the chance of closing more deals, as potential and existing customers demand information security certifications (cf. Barafort et al. 2018: 57-58). One way to convince groups of people with economic interests in the organisation would be to demonstrate the impact of cyberattacks on the organisation's share value. Since cyberattacks are negative for the share value, this can serve as a basis for argumentation (cf. Spanos/Angelis 2016; Corbet/Gurdgiev 2019).

Due to the influence of organisational culture on the various topics, stakeholder management is essential for the use of the extended methodology. As this aspect is also relevant for the enterprise architecture, there are approaches to implement this effectively (cf. Kurnia et al. 2021). The TOGAF framework offers a template for stakeholder management and shows a possible way of dealing with the various groups of people (cf. The Open Group 2022: 296-318).

Dealing with complexity

With regard to the future relevance of the extended methodology, the interviewees emphasised the improvement in dealing with complexity (F1, C1, C2, B1, B2, P3). Increasing regulatory requirements for information security and the increasing networking of technical systems would lead to complexity that is more difficult to manage.

Due to the technological complexity in corporate networks, there is an increasing switch to zero-trust architectures. These could be implemented with the help of the extended methodology (P3).

Adaptation

This category summarises the aspects that make it necessary to adapt the extended methodology for use in the organisation.

When applying the extended methodology, a detailed description of the activities to be carried out in the respective phases and the results to be achieved is necessary (P1). It is also recommended that the organisation examines how the extended methodology can be integrated into the organisational structure and into existing topics and systems (F2). IT-Grundschutz profiles would exist that could be created for specific use cases and adopted by other organisations (P2). These

could also be developed for the extended methodology by the various sectors. However, the application would probably be carried out primarily by larger organisations (P1). Organisations in regulated sectors would not apply the extended methodology immediately as they would doubt whether they could comply with it. The reason is that they lack experience, expertise and experts (B3). This uncertainty could be dispelled by pioneering projects that would demonstrate the possibilities and conformity with regulatory requirements (B3).

The inconsistent application of IT-Grundschutz in Germany and the resulting problems in the implementation of security measures could be cited as potential difficulties in adaptation (F1). There is also the possibility that, despite the widespread use of IT-Grundschutz in Germany, various organisations do not apply it correctly, which could lead to problems in the operational implementation of security measures (F1).

The following aspects were mentioned in less than half of the interviews. Nevertheless, they are listed as they are relevant for the critical consideration of the extended methodology.

Strategic uncertainty

Due to the complexity of an organisation's environment, the organisation's strategy (F1) and therefore the corporate objectives (C2) may be missing and unclear. This has a negative impact on the derivation of security requirements, as these are derived from the strategy and the organisational objectives.

One way of dealing with this strategic uncertainty would be to adapt the procedure according to DYA (cf. Wagter et al. 2005). However, the disadvantages should not be ignored, as the results only adapt to the circumstances and cannot be reused in the future.

Enterprise architecture issues

ESA is based on the same methods and principles as Enterprise Architecture. Therefore, similar or the same problems occur in ESA as in EA. The overly academic view within the EA was criticised (P1). In addition, security is not taken into account in the EA (P1, P2).

The overly academic approach has been criticised by various people. However, there is currently no solution for a practicable approach (cf. Buckl et al. 2009: 15; Kotusev 2019: 104; Saint-Louis et al. 2017: 46-47). The second aspect of the lack of treatment of security could be solved with SABSA and this thesis by using the structure of SABSA or the extended methodology with the article on integration into TOGAF (cf. The Open Group 2011).

Intensity

A field report shows that the implementation of SABSA is associated with a high expenditure of time and complex requirements (F2). The intensity of the SABSA implementation is due to the adaptation of the methodology and the lack of expertise in the design of security architectures in an agile environment.

Due to the intensity, various groups of people could lose confidence in the project. One countermeasure would be an incremental approach in which a small area of application is initially selected and the area is expanded after each increment. This would allow early results to be delivered in order to maintain the commitment of the groups of people.

One approach would also be to use agile methods in the architecture. The definitions and structures for an agile architecture are described in TOGAF (cf. The Open Group 2022c; The Open Group 2022a).

Uncertainty as to whether ESA is necessary

In one of the expert interviews, the uncertainty was described as to what extent the extension of IT-Grundschutz with SABSA would be necessary (P2). In this context, it was also pointed out that the postulated need to expand the security concept would only be unnecessary if the security standards were applied with a focus on the organisation.

As security standards such as ISO/IEC 27001 (cf. ISO 2022a), NIST SP 800-53 (cf. NIST 2020) and IT-Grundschutz (cf. BSI 2017a) do not provide guidance on how to align security with the organisation, organisations must develop their own methods. The extended IT-Grundschutz methodology is based on the extension with the SABSA framework, which enables a business-oriented architecture.

Auditing

The extended approach moves away from an audit-centric methodology and becomes architecture-centric by deriving security from the context of the organisation. This changes the establishment of information security and differs from the typical procedure for certifying the ISMS (F2). However, this is not the problem, but the lack of experience in successfully certifying the ISMS modelled according to SABSA or the extended methodology (B3).

For certification according to ISO/IEC 27001 on the basis of IT-Grundschutz, the ISMS is audited according to the modules in the IT-Grundschutz compendium. For this purpose, a mapping of the R1 modules to SABSA was carried out as part of this work and a Security Service Catalogue and Security Mechanism Catalogue were created. This would enable certification of the architecture in accordance with ISO/IEC 27001 on the basis of IT-Grundschutz. The mapping can be found in Appendix A.2 'Mapping of the R1 building blocks to SABSA meta levels'.

The results of the analysis carried out show that the extended IT-Grundschutz methodology has the potential to improve the quality of work in information security. Nevertheless, adaptation and acceptance are difficult. The predominantly extrinsic motivation for establishing information security calls into question the use of the extended methodology, as the changeover would be from an audit-centred to an architecture-centred approach. This change could result in uncertainties and initial additional costs, which could act as negative influencing factors and prevent the introduction or stop it due to a lack of support from departments and management during implementation. Therefore, the adaptation of the extended IT-Grundschutz methodology is an essential aspect of achieving successful application. This is illustrated by the relationships between adaptation and the other categories in Figure 25 illustrates this.

Adaptation involves the comprehensive and targeted adjustment of the extended methodology to the existing needs of the organisation. The informal, formal and value-adding structures as well as the culture of an organisation should be taken into account. The adaptation requires an analysis of the internal dynamics and an alignment of the extended methodology with the specific internal and regulatory requirements of the organisation. Adaptation is outside the scope of the research question, but would be of interest for future research.

5. DESIGN AND DEVELOPMENT

This chapter describes the extended IT-Grundschutz methodology and discusses the associated adjustments.

5.1. ADVANCED IT-GRUNDSCHUTZ METHODOLOGY

The extended IT-Grundschutz methodology is based on the IT-Grundschutz methodology in accordance with BSI Standard 200-2 (cf. BSI 2017a) and the changes to SABSA from 2018 (cf. Sherwood et al. 2018). The mapping of the building blocks to the SABSA layer and the first draft of the Security Service Catalogue and Security Mechanism Catalogue are based on the IT-Grundschutz Compendium 2023 (cf. BSI 2023b). The following subsections describe the structure of the methodology through the extension, as well as highlighting practical implementation options and discussing the problems.

5.1.1. STRUCTURE OF THE EXTENDED METHODOLOGY

Existing processes and wording have largely been retained to improve comprehensibility. In Figure 10 visualises the extended methodology with its various processes.

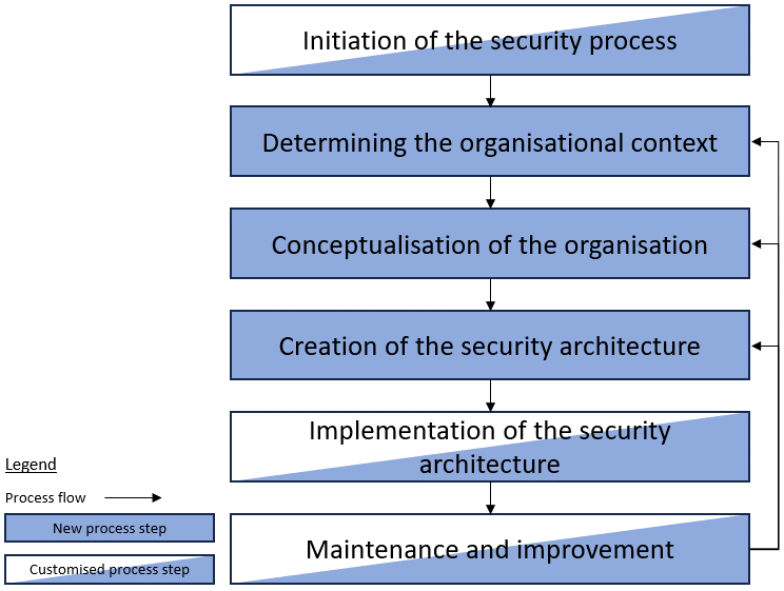

Figure 10: Phases of the security process of the extended methodology
Source: Own figure

Compared to the security process according to BSI Standard 200-2, see Figure 1 the processes 'Creation of the information security guideline', 'Organisation of the security process' and 'Creation of a security concept' have been incorporated into

the new ones or can be found in the various layers due to the way SABSA works. The initiation of the security process corresponds to the original, but the architecture governance and the structure and responsibility of the architecture are also defined. In chapter 5.1.2 this is discussed in more detail.

When determining the organisational context, the organisation as such is included, as well as its company, environment and risk landscape. This can be Chapter 5.3 can be found in chapter 5.3.

For a closer look at the organisation, the organisation is conceptualised on the basis of the identified organisational context. This provides a holistic representation of the organisational structure and processes. In addition, a framework is defined within which the organisation should operate, see chapter 5.4.

The conceptualisation is used to create the security architecture, which is described in chapter 5.5 is discussed. The security architecture described in chapter 5.6 is similar to the original phase. For the continuous improvement and maintenance of the architecture, chapter 5.7 shows a possible procedure.

The combination of SABSA and IT-Grundschutz enables the design and establishment of information security from end to end. While SABSA determines the security-specific requirements of the organisation and establishes the architecture, IT-Grundschutz provides information on the operational security measures, which is why the two complement each other. This symbiosis is illustrated in Figure 11 visualised. The specific work products of the individual processes can be found in Appendix A.3 'Work products'.

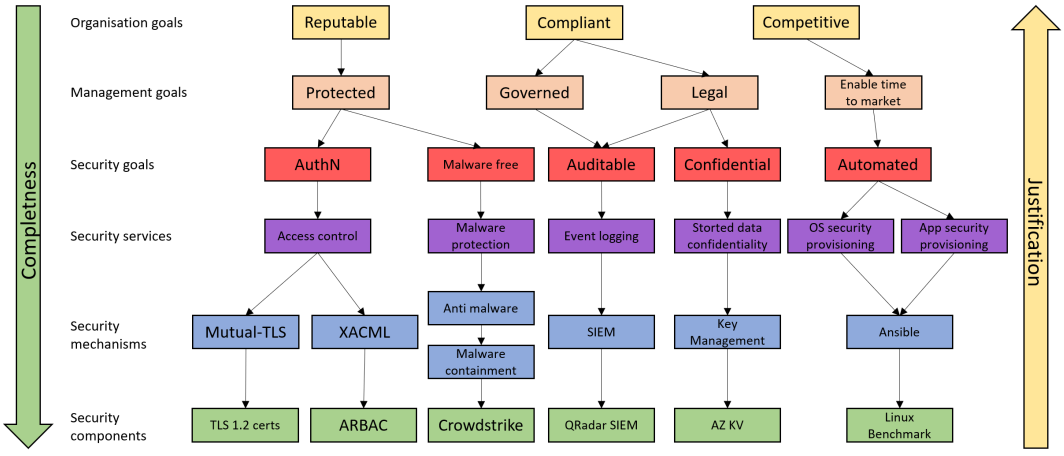

Figure 11: Abstraction levels in SABSA
Source: Based on (Platt 2021)

5.1.2. LIFE CYCLE

The design of the lifecycle of the extended IT-Grundschutz methodology is based on the SABSA lifecycle (cf. Sherwood 2005: 113), which is a proprietary development of the SABSA framework and is based on the PDCA cycle and the ITIL 3 lifecycle (cf. Sherwood et al. 2009: 5). The cycle comprises four phases. A continuous feedback loop ensures that potential for improvement is identified and integrated in each phase. The life cycle is summarised in Figure 12 graphically illustrated.

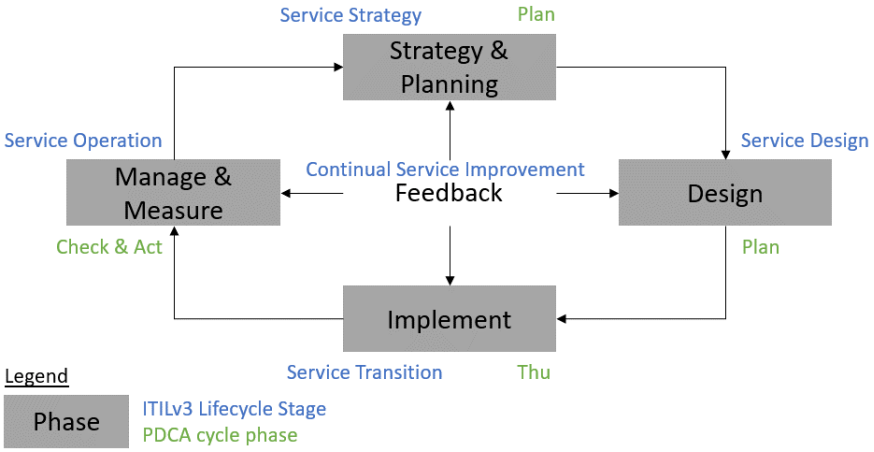

Figure 12: Life cycle of the extended IT-Grundschutz
Source: Based on (Sherwood 2005: 113)

The individual phases serve to define the sequence of the security processes to be carried out within the extended methodology:

- Strategy and planning: Determining the organisational context (cf. chapter 5.3) and conceptualisation of the organisation (cf. chapter 5.4),
- Design: Creation of the security architecture from the logical level to the component level (cf. chapter 5.5),
- Implement: Implementation of the security measures (cf. chapter 5.6) and
- Manage and Measure: The management of security measures and the performance of measurements to determine business attribute values.

As part of the feedback process, continuous improvement measures are developed and implemented on the basis of key figures, risk indicators, action indicators and feedback in accordance with section 5.7. Due to this structuring, the life cycle is process-orientated and does not use the agile elements that could be implemented by using the lean approach and agile practices, as would be possible according to ITIL 4 (cf. Axelos 2020: 227).

5.1.3. LIMITATIONS OF THE EXTENDED METHODOLOGY

Due to the low prevalence of ESA, two software solutions were identified by 10 August 2024 that are suitable for modelling the security architecture. The first solution is the *SABSA Security Architecture Extension* (cf. Cephas Consulting 2018), which is available as an add-on for *Enterprise Architect* (cf. Sparx Systems 2023). The second solution is *Qnous* and implements SABSA natively (cf. Qiomos Nous 2024). It has the disadvantage that the ESA set up cannot be natively integrated into the EA, which is why intermediate solutions would be necessary. An alternative approach to modelling the architecture is *ArchiMate 3.1* (cf. The SABSA Institute 2021). However, this is based on overloads and custom notations, as the security aspect is not natively considered in *ArchiMate 3.1* (cf. The Open Group 2019). This also reinforces the statement that security is not taken into account by EA, as described in chapters 1.4 and 4.2 was explained.

Another limitation is the small size of the SABSA community and its low level of activity. An analysis of the official forum of the SABSA Institute revealed (cf. The SABSA Institute n.d.) a total of 167 posts up to 10 August 2024 - one of which was written by the author of this paper in 2024. The distribution of all messages in the forum over the entire period is shown in Figure 13 visualised.

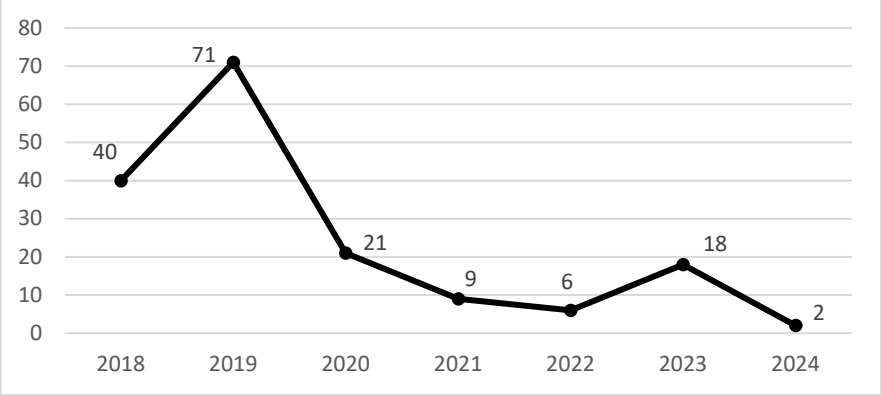

Figure 13: Posts in the forum in the period
Source: Own figure

Furthermore, there are no published SABSA case studies, which makes it difficult to get started and understand the topic. One reason for this could be the professional position of the members, which requires the handling of sensitive information and prevents its publication. It could also be due to the members' limited time resources.

5.2. INITIATION OF THE SECURITY PROCESS

The security process is initiated by the organisation's management. The latter defines responsibility for information security - if it has not already done so - by appointing a CISO (cf. BSI 2017a: 20). If no scope has been defined, the organisational management can define this in cooperation with the CISO for information security in the organisation. Furthermore, the impact on groups that are most affected, that will benefit the most and whose capabilities will change even though they are not directly affected can be determined. The governance structures should also be identified, as these should be taken into account within the architecture and may need to be adapted. The identified impacts should be coordinated and agreed with the organisation's management.

Before further preparation and design, the CISO could decide with the organisational management on the two options for establishing the ESA in the organisation. The first is the complete implementation of the architecture in the entire defined scope. One disadvantage of this approach is that initial work results are finalised later, while stakeholder acceptance decreases. This leads to conflicts within the organisation, so that compromises are made at the expense of the effectiveness of the ESA or the entire ESA project is cancelled (cf. chapter 4.2). An alternative to prevent this is the second option, i.e. piloting with a focus on a specific area of the organisation. The aim of piloting is to demonstrate the possibilities of ESA in the organisation, to highlight the specific advantages for the organisation and to increase the acceptance and commitment of stakeholders to the new way of working.

In this context, the SABSA framework presents the concept of the 'Fast Track Workshop'. In this five-day workshop, SABSA is to be established for a sub-area of the organisation in cooperation with key stakeholders (cf. Sherwood 2005: 152-155). Based on the available results, the organisation could extend the ESA approach to other areas of the scope, provided that the necessary acceptance and commitment of the organisational management are guaranteed.

Depending on the scope and approach, the organisation's existing options are identified. Gaps and the interests of the stakeholders are determined in an assessment. The results are used as a basis to determine the need for change, the limitations of the ESA and the required budget and personnel. Based on the framework conditions, the information security organisation is formed or adapted if information security structures exist. The CISO defines the positioning of the ESA topic with

the organisation's management and other executives, taking existing structures into account.

The two options for integration are shown in Figure 14 visualised. In a pilot project, the team with responsibility for ESA could be formed temporarily and then transformed into a permanent team. In the first option, a separate ESA team could be set up under the responsibility of the CISO, which would work with the ISMS and EA teams, if available. Depending on the existing structures, the ESA team acts according to the specifications of the ISMS team or develops them itself.

The second option is to integrate the ESA into the EA team under the responsibility of the CIO in cooperation with the CISO, who works with the ISMS team if available. The structure of the information security organisation is described in BSI Standard 200-2 (cf. BSI 2017a: 36-50). A description of the harmonisation of positions and responsibilities can be found in Appendix A.1 'Possible structure of the organisational structure' can be taken from it.

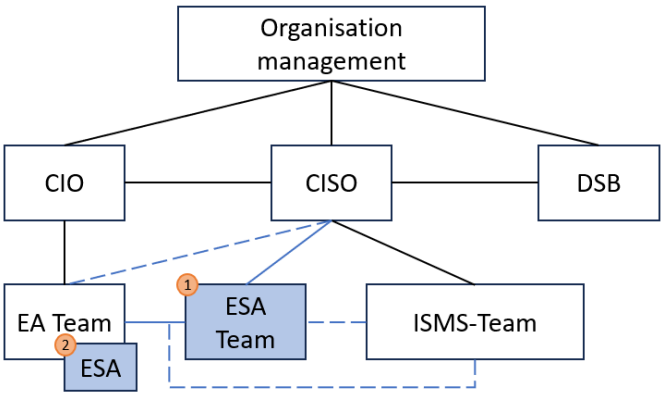

Figure 14: Possible organisational design
Source: Own figure

The documented results are coordinated with the organisational management and summarised in the organisational model for ESA. In addition, a stakeholder analysis could be carried out and a communication plan drawn up in order to establish the ESA in a targeted manner. The process step could be finalised by defining the architecture governance.

5.3. Determining the context of the organisation

Once the initiation has been completed, the organisational context is determined by collecting information about the organisation, e.g. strategies, drivers, goals, success factors, organisational structure and processes, budgets, existing management systems, structures, technical problems and specific limitations. Sources of

information can include existing strategy documents, business plans, corporate principles, process documents and relevant stakeholders. In addition, the financial aspects of the organisation are identified and business relationships with internal and external entities are recorded. A contextual description of the organisation is created based on the information collected. The information collected could be recorded as follows:

- The motivations behind business plans and decisions can be documented using the business motivation model (cf. OMG 2015a).
- The structure of the process organisation could be represented using the business process model (cf. OMG 2014).
- The relationships between the organisation and internal and external organisations could be represented by the entity-relationship model (cf. Chen 1976).
- The internal organisational structure could be recorded in the form of an organisational chart.

The choice of information to be used and the existing strategic and tactical plans have an impact on the future viability of the architecture due to the level of detail of the planning scope. This information can be divided into six categories: 'business requirements', 'business processes', 'specific business needs', 'business capabilities', 'business strategy' and 'operating model', see Figure 15. As the planning period increases, the level of detail decreases, meaning that the requirements become increasingly blurred. Information with a short planning period and a high level of detail has little fuzziness, but is not meaningful for future planning.

An architecture that is modelled on the basis of business requirements can become too rigid over time, so that a regular, complete renewal of the architecture becomes necessary. In contrast, an architecture based on a strategy would be too imprecise and could not fully fulfil all the requirements of the present.

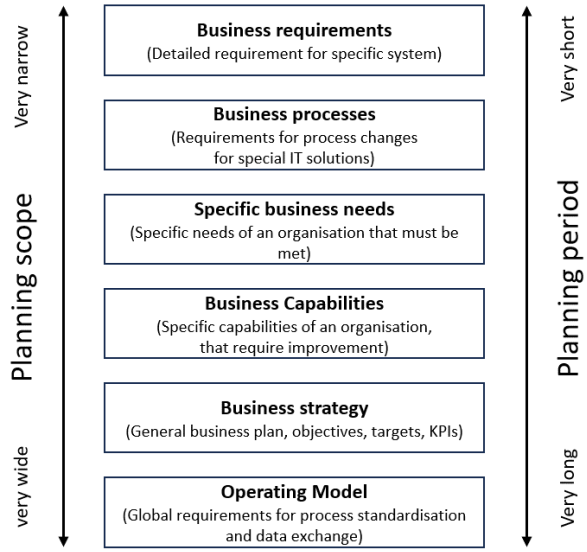

Figure 15: Categories of requirements
Source: Based on (Kotusev 2021: 89)

According to experience reports in EA, architectures modelled on the basis of organisational strategies are not reusable (cf. Weill/Ross 2009: 1-20; Ross et al. 2006: 17-24). The reason for this is that the life cycle of organisational and technical systems is taken into account in these strategies and therefore specific, non-reusable solutions are required. In addition, information security could have a similar problem to IT in that it becomes a bottleneck in the strategy due to the focus on the current strategy instead of supporting it (cf. Ross 2005: 1).

This focus also leads to an alignment trap. This means that different initiatives deal with specific needs of the organisation independently of each other, but do not generate any added value for the organisation as a whole due to the lack of a holistic view (cf. Shpilberg et al. 2007). Furthermore, the systems from the initiatives become a burden. IT systems have an average useful life of 15 years, strategies of around four years, which means that systems outlast several strategies, meaning that aligning systems with strategies would not make sense (cf. Wierda 2017: 140-141). The operating model can provide an alternative information basis.

An operating model comprises the dimensions of standardisation of business processes and integration, which ensure the provision of goods and services for customers. It describes how a company wants to grow. As the operating model provides a more stable and realisable vision of the company than the strategy, it drives the development of the basis for implementation. The decision for an operating model affects how a company implements its business processes and IT infrastructures. An organisation without a clear operating model cannot bring automated,

existing and cost-effective capabilities to a new strategic project, but must identify its core competencies for each new strategic initiative.

Standardising business processes and the associated systems means defining how a process is to be executed. It ensures efficiency and predictability throughout the entire organisation. Integration links the efforts of organisational units through shared data. This data sharing can occur between processes to enable end-to-end transaction processing, or across processes to enable the organisation to present a consistent face to customers. The benefits of integration include increased efficiency, coordination, transparency and flexibility. An integrated approach to business processes can improve service to customers, provide management with information for decision making and allow changes in one part of the organisation to highlight necessary actions in other parts. Integration can also speed up the overall flow of information and transactions within the organisation (cf. Ross et al. 2006: 45-48).

Depending on the scope and type of implementation, a distinction can be made between different categories of information when using information. A decision basis for this can be found in Figure 16 can be seen in Figure 16.

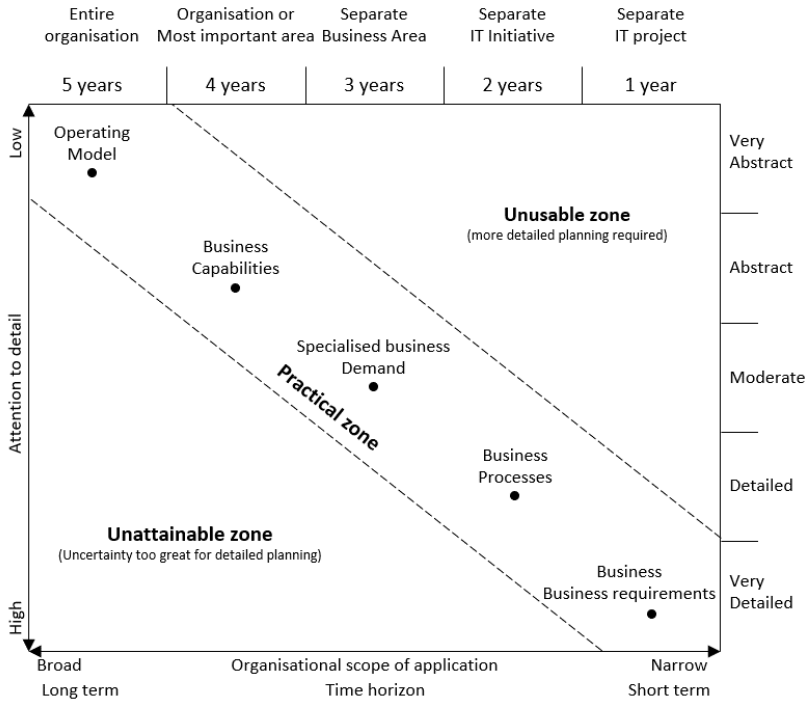

Figure 16: Choice of information category
Source: Based on (Kotusev 2021: 91)

The information collected is needed to record the organisation's business drivers. Due to possible contradictory requirements, conflicts could be identified within the

information, which are smoothed out in consultation with the organisation's management. This can be done by resolving the conflicts or prioritising them using risk analysis. The business drivers for security are derived for each business driver.

The latter represent a derived abstraction of a security requirement of a business driver. The business driver for security is formulated in business language so that the organisation management and other executives understand the security requirement. Business drivers can have several business drivers for security, which is why it is a 1:n relationship. They contain a name and a description.

Once the business drivers for security have been recorded, an organisation and relationship diagram is created. It contains all the organisations affected in the scope and their respective relationship model. The business drivers for security and the organisational and relationship model are agreed with and approved by the organisational management.

Finally, a business risk model is used to analyse the risks and opportunities based on the assets, impacts and existing threats. SABSA uses the proprietary 'SABSA Risk Assessment' method. The risks are identified and qualitatively assessed using an impact-oriented approach (cf. Sherwood 2005: 205-209). The approach presented differs from BSI Standard 200-3 on risk management, in which risks are identified using a threat-oriented approach (cf. BSI 2017b). The advantage of the impact-oriented approach is that risks can be identified not only for assets, but also for business objectives. This simplifies prioritisation for dealing with risks.

A further distinction in risk management between SABSA and IT-Grundschutz is that in SABSA it is carried out without preconditions, whereas in the IT-Grundschutz methodology a risk analysis must be carried out explicitly if: (1) a high or very high protection requirement is identified in at least one of the protection objectives, (2) a target object cannot be adequately modelled with the existing building blocks or (3) a target object is operated in a deployment scenario that is not provided for in IT-Grundschutz (cf. BSI 2017a: 153). This is possible because the assessment of the threats in the building blocks has already been carried out (cf. BSI 2017a: 152-153).

SABSA and IT-Grundschutz also differ in terms of when a risk analysis is carried out. In SABSA, the latter is carried out at the beginning of the context determination process in order to supplement the information on the organisational design and the requirements of the risk environment. They are used as a basis for prioritising the criticality of the respective aspects of the organisation (cf. Sherwood 2005:

453). In the IT-Grundschutz methodology, a risk analysis is carried out after a policy or guideline has been drawn up, the ISMS organisation has been established and an analysis of the current situation has been carried out. This means that the organisation's risk environment is not taken into account at the strategic level (cf. BSI 2017a: 76).

In order to create the business risk model and comply with the requirements of IT-Grundschutz, a business impact analysis could be carried out in accordance with BSI standard 200-4 (cf. BSI 2023a: 158-193). This can be combined with the BCM risk analysis (cf. BSI 2023a: 199-214), which uses BSI standard 200-3 (cf. BSI 2017b). The business impact analysis identifies the criticality of the processes and determines the organisation's performance targets, which is why the effects of a process failure are recorded. These are supplemented by the risk analysis in accordance with BSI Standard 200-3, which can be used to determine the possible causes. Despite the threat-orientated approach according to the BSI procedure, the impact is determined. This combination is in line with SABSA and the requirement for the artefact to comply with the specifications for an audit. During an audit, the result of the risk analysis could be shown in accordance with the BSI standard.

5.4. Conceptualisation of the organisation

The results for determining the context of the organisation are created by the organisational management from their perspective. The former are used by architects to create a conceptualisation and model the organisation. The work products can be classified according to the EA artefacts 'Vision' and 'Consideration' using the CSVLOD model. At the beginning, the business drivers for security are used and the business attributes are defined. A business driver for security can contain several business attributes and a business attribute can be assigned to several business drivers, resulting in an n:m relationship (cf. Sherwood et al. 2009: 89).

Business attributes are a conceptual abstraction of a requirement and allow it to be measured. In addition, communication with the organisation's management is simplified, as the business attributes provide a data-based factual situation in a language suitable for the target group, depending on the meta-level (cf. ibid.: 89). The metric for the measurability of a requirement is defined within a business attribute. Qualitative or quantitative methods can be used to collect the metrics, but there are specific requirements: The data used must be available, the collection as well as the possible calculation must be carried out independently of interests and

the measurement must be repeatable. In addition to setting up the metric and collecting it, the performance targets are determined taking into account the organisation's performance targets. The performance targets define the expected minimum and maximum values. Predefined business attributes exist within the SABSA framework (cf. ibid.: 20-21), which can be expanded as required or with your own attributes.

The sum of all defined business attributes in the conceptualisation is summarised in a Business Attribute Profile. The latter is a conceptual representation of the organisation, mapped via the business attributes to measure the performance for compliance with the requirements (cf. ibid.: 218). This enables data-driven work by allowing decisions to be made on the basis of collected information.

Once the method of measuring compliance with the organisation's requirements has been defined, the control objectives are determined. A control objective is a statement of a desired result or purpose to be achieved through the implementation of controls within a specific business activity (cf. ibid.: 219). They are implemented through the framework defined in the ISMS documents. Their use could stem from a specific requirement for the organisation or be a good practice (cf. ibid.: 219). Within the control objectives, security topics and specifications from various standards such as ISO/IEC 27001:2022 (cf. ISO 2022a), NIST SP 800-53 (cf. NIST 2020), COBIT 2019 (cf. Isaca 2018) and IT-Grundschutz-Kompendium (cf. BSI 2023b) can be normalised and translated into a uniform terminology for the organisation.

As part of this master's thesis, a first draft approach of the building blocks of the IT-Grundschutz Compendium 2023 (cf. BSI 2023b) for the Control Objectives and the Control Library was carried out, which is presented in Appendix A.2 'Mapping the R1to -SABSA' can be taken from it. The Control Library is explained in this chapter.

Only building blocks with the implementation sequence R1 were used, as the entire building blocks and their security requirements will be revised for the next version of the compendium (cf. Schmidt 2023). Building blocks with an assignment of implementation sequence R1 should be realised as a priority (cf. BSI 2017a: 137). They are universal and essential for every organisation and can be used as an example of possible compliance with the BSI requirements. The design approach consists of mapping the objectives and security requirements of R1 building blocks between SABSA and the compendium. The mapping is based on a content analysis in which the sentences are interpreted according to their content and assigned

to the respective SABSA meta-level. In addition, the specific safety measures for each requirement were extracted and listed in order to simplify the creation of the safety catalogues. The use and explanation of the security catalogues are explained in chapter 5.5 .

Modelling the architecture could be simplified by mapping the security measures to the business attributes, which would also make it possible to automate the selection of security measures. Furthermore, such mapping can lead to an approximation of comparable results, as the same security measures are used when selecting attributes. Similar to the mapping of security measures to STRIDE in Peterson (cf. 2010), the normalised control objectives could be placed in a relationship to the elementary threats in the IT-Grundschutz compendium. The BSI has created a cross-reference table for this purpose (cf. BSI 2023c) in order to relate the security requirements of the building blocks to the elementary threats and simplify risk management. The control objectives conceptualise the business risk model and serve as an interface between the contextual and conceptual meta-level (cf. Sherwood et al. 2009: 219). This means that the organisation's risks can be considered and dealt with across all meta-levels.

In order to determine the responsibilities for dealing with the defined organisational risks, the trust relationships and their requirements in the organisational environment must first be determined (cf. ibid.: 255). Trust modelling helps to determine which entities require which trust, which values need to be protected, what level of trust is necessary and under what conditions trust is granted or withdrawn. Within this framework, the interactions between the entities are established and analysed. Three categories of relationships can be distinguished:

- Unilateral: One entity distributes information, other entities can receive it.
- Bilateral: Two entities act and exchange information within the framework of their contract.
- Multilateral: Several entities act and exchange information within the framework of their contract and/or common rules (cf. ibid.: 255).

In order to determine trust and the associated requirements for bilateral and multilateral relationships, these are first decomposed into unilateral relationships and their requirements are set out. A visualisation of the composition can be Figure 17.

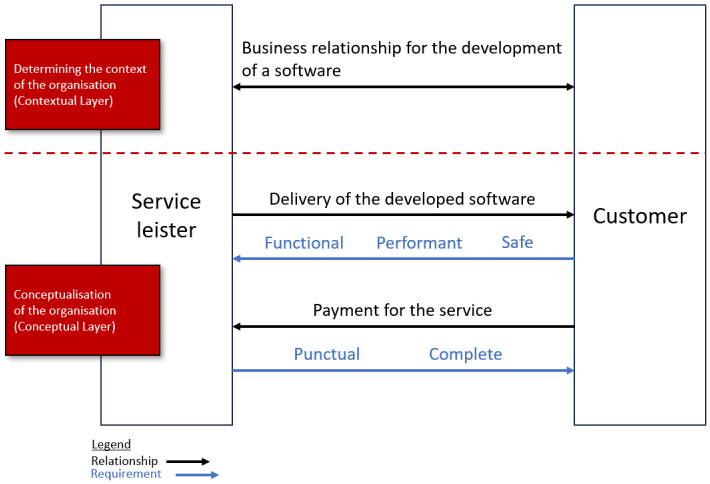

Figure 17: Decomposition of a bilateral trust relationship
Source: Own figure

Modelling the trust relationships between internal entities, including the organisation and its further structure such as department, team, etc., and external entities that are external to the organisation allows the creation of a RASCI matrix. This comprises the responsibilities of the various entities. However, the classic RASCI matrix cannot adequately map the complex relationship landscape and the distribution of different responsibilities. The SABSA Institute therefore developed the SABSA Responsibility Assignment Model, which is an extension of the RACI matrix (cf. Sherwood et al. 2023).

Once the responsibilities and relationships between the entities have been determined, the internal entities can be structured using a management system. The topic-specific guidelines and directives are created by the respective responsible entities as part of a policy architecture, which apply throughout the organisation. The guidelines and directives contain general specifications for the management of an area of activity, e.g. HR, marketing or security.

The procedure differs from the IT-Grundschutz methodology in that the organisation's risk landscape is taken into account when designing the guidelines and policies. The processes for dealing with guidelines and policies are similar to the procedure according to Ward and Smith (cf. 2002). After the initiation of the safety process or project, the guideline is developed, approved and its existence is publicised through awareness campaigns and the dissemination of the document. This is in contrast to the handling of the extended methodology, which corresponds to a combined approach according to Rees et al. (cf. 2003) and Flowerday and Tuyikeze (cf. 2016). Before the guidelines and directives are formulated, a risk and policy assessment is carried out to identify the necessary requirements. The risk assessment is not necessary in the conceptualisation, as the business risk model

can be used (cf. section 5.3). The policy assessment consists of an evaluation of the regulatory landscape, an identification of gaps and contradictions and a derivation of procedures (cf. Rees et al. 2003: 102-103).

The results of the risk and policy assessment are used to formulate, implement and monitor the guidelines and directives, and compliance with their requirements is also monitored. The advantage of this approach lies in the needs-based structuring and formulation of the guidelines. As a result, information security can be tailored to the organisation so that not only general, unspecific risks are covered.

The policy architecture could be supplemented by a business capability model that describes the organisation's business capabilities, shows their relationships to each other and structures them hierarchically. The highly aggregated presentation facilitates communication with the organisation's management and forms the basis for strategic planning of capability development and investment strategies. The term business capability refers to the ability or skill of an organisation to fulfil its core function. The latter encompasses and describes all applications, roles and skills required to provide a business function (cf. Pouya et al. 2018: 4603).

The topic-specific motivations of information security are formed by the policy architecture and the business capability model and form the basis for the further development of the business motivation model. They complement the business view and provide further technical insights into the decisions made.

In order to integrate the requirements of the guidelines and directives into the technical and organisational structures and processes, a control library must be created in which the potentially usable treatment measures in the organisation are listed. The specific security measures can be harmonised in the same way as the control objectives. The mapping enables the assignment of safety standards to the respective measures, which simplifies the verifiability of compliance with standards.

The results of the activities carried out and the determination of the context for the development of a security strategy serve to systematically realise the target state. The approval and representation of the security strategy by the organisational management are essential to ensure the success of the project and the implementation of the strategy.

This process step is completed by carrying out a gap analysis. The technical and organisational current status is determined and compared with the defined target status from the control objectives. Based on the data obtained, further steps can be derived in order to achieve the defined target image.

5.5. CREATION OF THE SECURITY ARCHITECTURE

The 'logical', 'physical' and 'component' meta levels specify and operationalise the security requirements for the security architecture of the previous level. The security measures are taken from the Control Library for this purpose. The elaborations of the architectures can be modelled using the Unified Modeling Language (cf. OMG 2015b) and ArchiMate (cf. The Open Group 2023). The results affect all artefacts according to the CSVLOD model.

5.5.1. LOGICAL LEVEL

Once the organisation has been conceptualised, the required security functionality is considered at the logical level. It defines the requirements for the functions that are implemented at the physical level. The organisation's information and value flows form the basis of the logical level, at which the measures are defined in accordance with the Security Service Catalogue.

Following the results of the policy architecture and taking into account the organisation's information architecture, the various topics relating to specific areas or functions of the organisation are discussed in the guidelines. These guidelines concretise an area or function and are aimed at a defined target group. The security services can be adapted and supplemented based on the internal specifications of the guidelines.

The trust model forms the basis for dividing the entities or departments within the organisation into security domains. The latter are logical groupings of entities and resources that have similar security requirements and controls. They are independent and manage their risks through their own policies. It is possible for a security domain (superdomain) to comprise one or more security domains (subdomains). The superdomain passes on its requirements to the subdomain, which either adopts them unchanged or tightens or adapts them through local customisation. A visualisation is shown in Figure A in Figure 18.

The exchange between domains, regardless of whether they are related or not, takes place via controlled transitions in a secure exchange. The controlled transition ensures that the entry, exit and transfer of information takes place in accordance with its own security guidelines. The security policies shown in Figure 18 illustrates a communication between two unrelated domains. Accordingly, it is up to each domain to manage its specific risks independently by enforcing its policy once the controlled transition has taken place. However, there is an exception

within the extended domain concept: one domain is able to extend its authority into the domain of another unrelated domain to manage its own risks.

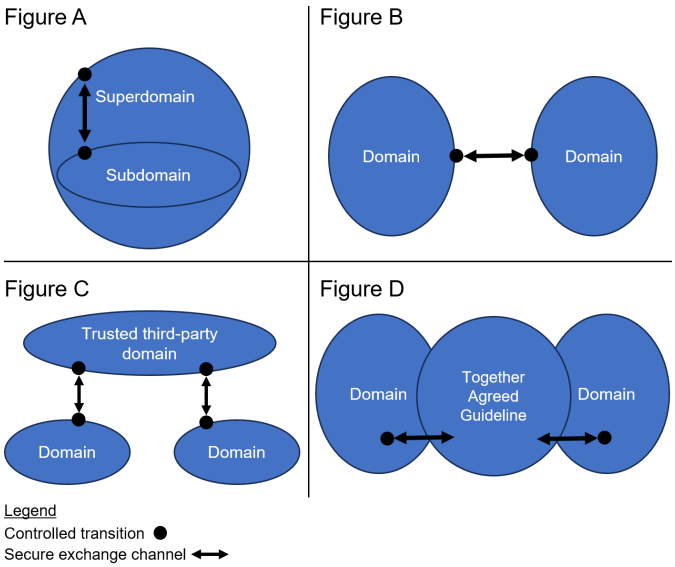

Figure 18: Logical relationships of domains
Source: Own figure

In addition to the standard option for an exchange between two domains, there are two other options. The first is an exchange via a trusted third-party domain. As both domains trust the third-party domain, a transitive relationship is created. This is shown in Figure 18 with figure C. The exchange can take place exclusively via the third-party domain or in combination with a direct exchange, whereby the third-party domain authenticates the respective domains.

The second option is to agree a common policy. This means that the domains remain autonomous and manage their own risks independently. However, the policy is shared, creating a relationship of trust and ensuring that information is handled in accordance with the policy at all times. This is illustrated in Figure D in Figure 18 is visualised.

The logical security measures are defined on the basis of the modelled security domains with their relationships and the underlying processes as well as information and value flows, taking into account their risk assessment, so that the treatment of measures is proportional and appropriate to the risk. For this purpose, the security measures predefined in the security service are selected or treated with new measures depending on the context. The following sequence must be observed: Deterrence, Prevention, Detection, Containment and Corrective. Each type of treatment affects the various parameters of a risk, as shown in Figure 19 is visualised.

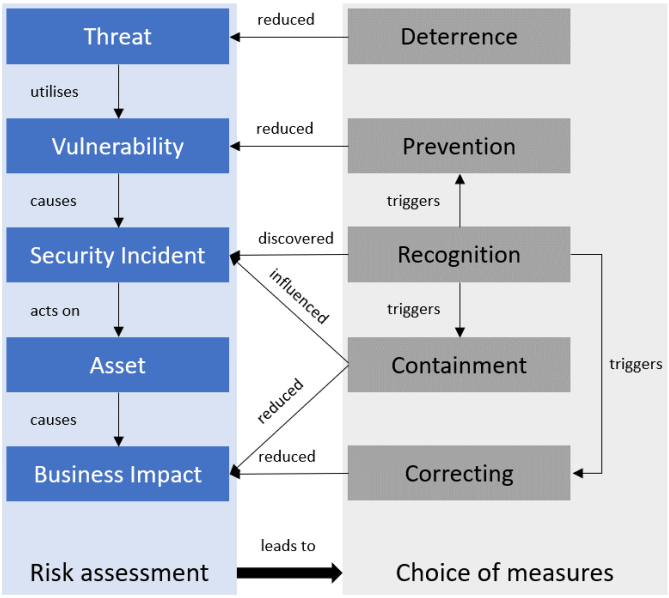

Figure 19: Effect of the types of treatment
Source: Own figure

5.5.2. PHYSICAL LEVEL

At this level, the logical requirements are operationalised by implementing the logic in the physical world. In addition, the selected security measures of the Security Service Catalogue are developed with the help of the Security Mechanism Catalogue.

Before operationalising the logical security architecture, the specific security guidelines for the logical level should be drawn up in the form of instructions and regulations for the physical level. This can take the form of work instructions that describe the security processes and contain step-by-step instructions. Further elaboration could be supplemented by guidelines that represent best practices. As part of the concretisation process, security mechanisms can be developed that comply with the requirements of the internal guidelines and the defined work instructions and guidelines. The possibility of linking these to the security services would create a connection between the logical security measures and the physical measures.

This is followed by a breakdown of the organisation's logical architecture into physical architectures. Information and value streams are represented in various architectures, including network architectures and data structures, for example. These are used to model the security mechanism in the physical architectures, taking into account the logical architecture.

5.5.3. COMPONENT LEVEL

To realise the security mechanism, a detailed description of the security components used is provided at component level. The defined measures not only include specialised software and hardware solutions, but can also include organisational aspects.

When selecting specific safety measures, the factors 'economic efficiency', 'existing competences' and 'coexistence with other safety measures' should be taken into account. The ROSI model (cf. ENISA 2012), which is based on estimates, can be used to calculate cost-effectiveness. It therefore does not exactly reflect reality, but approximates it. As part of the development of a defence-in-depth strategy (cf. NSA n.d.), it must be taken into account that the use of an increasing number of security measures is neither effective nor economical (cf. Gordon/Loeb 2002: 446-450). Furthermore, the planned security measures may be negatively influenced, opening up new security gaps. In addition to the cost and impact considerations, it should be noted that the skills and knowledge to implement, use and maintain the measure may be lacking within the organisation. In this context, further training measures may be necessary.

The choice of measures is only one aspect of standardisation. Operational standardisation, which aims to increase the effectiveness and efficiency of the measures, also takes place at this level. To this end, templates for documents can be created and hardened standard configurations of CIS can be used (cf. CIS n.d.).

5.6. IMPLEMENTATION OF THE ENTERPRISE SECURITY ARCHITECTURE

Once the enterprise security architecture has been modelled, it is implemented as part of this process step. As the extended methodology is based on IT-Grundschutz and the IT-Grundschutz Compendium, the respective implementation notes can be used for the design and implementation (cf. BSI 2019). However, a large part of the implementation notes refer to the outdated 2022 edition, which is why they may no longer correspond to the state of the art or current requirements.

Before implementation, an implementation strategy should be defined according to which the security measures are to be implemented. You can choose between the 'big bang', the incremental or the iterative variant. The big bang approach is characterised by the fact that the planned measures are implemented simultaneously and without delay. In contrast to the incremental approach, in which a new, fully functional measure is introduced at each step, the iterative approach involves adaptation through repeated cycles. When making decisions, the internal governance

structures of the organisation should be taken into account and supplemented if necessary. Based on the IT engagement model by Ross et al. (cf. 2006: 152-154), an information security engagement model could be established that consists of control mechanisms. The latter ensure that business and information security projects achieve both local and organisation-wide goals. The model consists of three levels, which are shown in Figure 20 visualised with their relationships:

- Organisation-wide IS governance: responsible for the decision and handling of organisation-wide information security,
- Project management: formalised methodology for handling projects with clear objectives and deliverables, and
- Connection mechanism: Alignment of operational activities in the projects with organisation-wide IS governance.

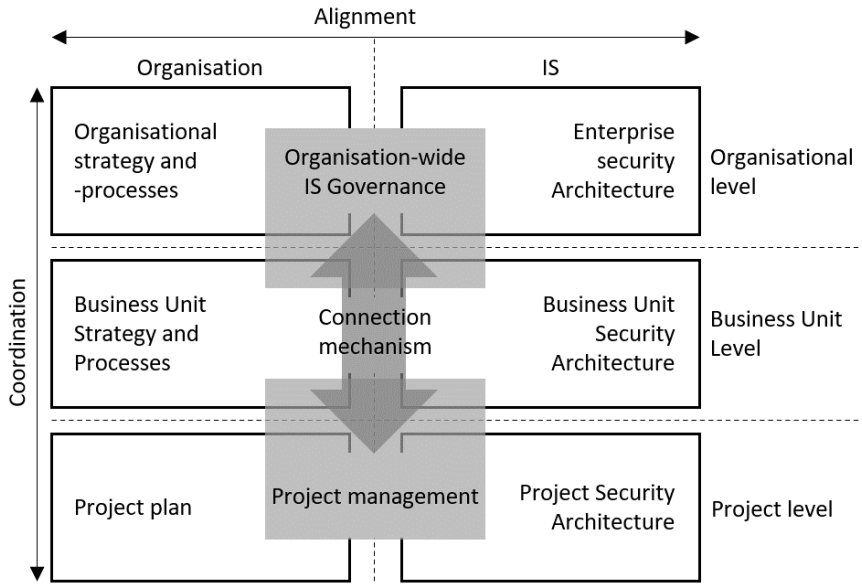

Figure 20: IS engagement model
Source: Based on (Ross et al. 2006: 154)

Organisation-wide IS governance reflects the principles of organisational governance and is focused on aligning information security with the organisational objectives. It consists of the CISO, the ISMS team (cf. Appendix A.1.1) and - depending on the organisation - the ESA team. To standardise project management, organisations use either existing standards or their own designs. The Project Security Architecture is managed by the respective Project Security Officer (cf. Appendix A.1.1) and architects. Ensuring the alignment of activities and results according to the organisation is achieved through the early and regular monitoring, prioritisation, adjustment and correction of project implementation via the liaison mechanism. This can be carried out by the IS Coordination Committee (cf. Appendix A.1.1) in cooperation with the ISMS team, the specialist managers and the security officers

concerned in order to ensure that information security is aligned with the organisational objectives (cf. BSI 2017a: 46).

When choosing the implementation options and structuring the organisation, it is necessary to determine the information requirements and define the necessary information exchange, taking into account the formal and informal hierarchies within the organisation. This would ensure that the relevant stakeholders remain positive even after the implementation of the information security architecture and do not demand a change to the traditional way of working.

In addition to the information requirements, the existing knowledge in the organisation should be compared with the knowledge requirements of the target state of the architecture in order to evaluate the necessary measures. This includes the examination of further education, training or sensitisation measures.

As organisations do not carry out their activities exclusively with their own staff, but also through outsourcing, it is relevant to consider entities external to the organisation and their impact on the processes and the organisation. The alignment of the outsourcing relationship could be compared and adapted according to the architecture maturity levels (cf. chapter 4.1.2).

5.7. MAINTENANCE AND IMPROVEMENT

Systems are adapted to meet external and internal requirements as part of the continuous improvement process. This opens up new possibilities on the one hand and increases their complexity on the other. The term 'system' does not exclusively cover technical systems, but generally the interaction of several components to fulfil a purpose. These can be, for example, companies, business functions, task areas, products, IT systems and software (cf. ISO 2019b: iv). To manage the complexity of systems, concepts, principles, processes and tools are used to design effective architectures and optimise architecture-related decisions.

Architecture Evaluations are carried out for various reasons (cf. ISO 2019c: vi):

- Determining whether something has been or will be designed to fulfil its intended purpose (or can be modified to serve a new purpose),
- Evaluation of the effectiveness and suitability of an architecture with regard to the needs and expectations of those involved,
- Identification of risks that need to be minimised,
- Identification of opportunities for improvement,
- Clarification of the problem area and the needs of those involved and

- Evaluation of progress in achieving the architectural goals.

The evaluation process in accordance with ISO/IEC/IEEE 42030:2019 (cf. ISO 2019c), which can be supported by the business attributes for a data-driven approach, is suitable for evaluating the ESA. This allows feedback to be introduced at all meta levels, which serves both to maintain the architecture and to improve it. While the Architectural Analysis centrally covers the ESA set up, its effects are analysed by the Value Assessment and the Evaluation Synthesis. These reviews allow the potential for improvement to be identified and the effectiveness of the implemented measures to be monitored. Further potential can be identified by evaluating the maturity level of the architecture based on the CMMI (cf. Isaca n.d.) and the maturity level according to Ross et al. (cf. 2006: 97-120), which could be used by the organisation.

6. DISCUSSION

In this chapter, the proposed solution is evaluated on the basis of the previously defined design requirements, the guidelines of the research approach and the underlying process. The weaknesses of this thesis are subsequently analysed.

6.1. FULFILMENT OF THE DESIGN REQUIREMENTS

In the following, the extended IT-Grundschutz methodology is described according to the principles described in chapter 2.2 defined in chapter 2.2.

Requirement 1: The extended IT-Grundschutz methodology must include ESA capabilities.

This requirement is met, as the model presented in chapter 5 extends the IT-Grundschutz methodology with the ESA framework SABSA. Practical options for implementing the capabilities and embedding them in the enterprise architecture were also demonstrated.

Requirement 2: Compliance with IT-Grundschutz should continue to be guaranteed in order to be able to have the ISMS certified according to the BSI.

For certification in accordance with ISO/IEC 27001 based on IT-Grundschutz, two aspects of the extended IT-Grundschutz methodology must be considered in order to verify compliance with the regulatory requirements. The first aspect concerns the implementation of the security process. As part of the extended methodology, the processes have been supplemented by linking security with the organisational objectives. The second aspect covers compliance with the security requirements in accordance with the IT-Grundschutz compendium and the modelling of the organisation. The link between the IT-Grundschutz compendium and SABSA enables the design and implementation of a security architecture that complies with the BSI specifications. As a consequence, the security process is carried out according to the extended methodology in compliance with the requirements for the certification of the organisation according to the BSI standard.

Requirement 3: The result should generally be clear enough to be applicable in practice.

The modelling of the various meta-levels of the extended IT-Grundschutz methodology can be carried out by the Object Management Group on the basis of various modelling languages. In addition, linking options with the enterprise architecture were identified. However, due to the current limitations of SABSA, the application and implementation of the architecture in practice involves a great deal of effort.

6.2. ASSESSMENT ACCORDING TO DESIGN SCIENCE GUIDELINES

In this subchapter, the implementation of this research is evaluated on the basis of Hevner's seven guidelines (cf. 2004: 82-90).

Guideline 1: Design as an Artifact - DSR must produce a usable artefact in the form of a construct, a model, a method or an instantiation (cf. ibid.: 83).

The aim of this research work was to extend the IT-Grundschutz methodology to include ESA capabilities. The solution is the extended IT-Grundschutz methodology with SABSA.

Guideline 2: Problem Relevance - The aim of DSR is to develop technological solutions for significant and relevant economic problems (cf. ibid.: 83).

The extended IT-Grundschutz methodology enables security to be aligned with organisational objectives. As described in chapter 2 this is difficult because the BSI and other security standards do not describe how this could be done. With the help of the extended methodology, ESA can be aligned with the organisation.

Guideline 3: Design evaluation - the benefit, quality and effectiveness of a design artefact must be demonstrated by suitable evaluation methods (cf. ibid.: 83).

A descriptive approach was chosen, as the design can currently only be evaluated on the basis of well-founded arguments (cf. ibid.: 86) - based on literature and expert interviews.

Guideline 4: Research Contributions - effective DSR must include clear and verifiable contributions in the areas of 'design artefact', 'design principles' and/or 'design methods' (cf. ibid.: 83).

After analysing the literature, it can be concluded that no studies have yet been carried out on the extension of the IT-Grundschutz methodology with SABSA or on an ESA framework in general. The result of this work is based on a conceptual analysis and has not yet been tested under real conditions. As a result, the knowledge base can only be supplemented on a theoretical level.

Guideline 5: Research Rigour - DSR is based on the application of rigorous methods in both the construction and evaluation of the design artefact (cf. ibid.: 83).

The accuracy and limitations of this research are reviewed, taking into account the limitations of the chosen research methods. At the beginning of the research, a literature analysis was carried out in order to obtain a theoretical basis for the ESA topic as well as possible designs with ESA and critical considerations of IT-Grundschutz. The literature analysis took the form of a structured and unstructured literature search. Digitally available texts were identified in several databases and sorted according to filter criteria. The aim of the literature analysis was to gain an overview of existing methods and theories. Both peer reviews and specialised articles were taken into account. This goal was achieved by including a wide range of both academic and grey literature in this research. In this context, only a few conceptual papers for ESA and IT-Grundschutz were found. However, the use of Google and Google Scholar for the unstructured literature search may lead to criticism, especially with regard to the scope and reproducibility of the research. In order to place the extended methodology on a higher theoretical basis, general aspects of enterprise architecture were used to incorporate them into the model. The former was developed on the basis of theory and was to be evaluated by means of expert interviews.

In this study, ten expert interviews were conducted with selected individuals. Guiding questions were prepared in order to reduce the influence and own bias in the individual interviews. Furthermore, the bias was reduced by using the coding technique.

The objective of the expert interviews was to evaluate the extended methodology and to generate information about the potential environment. A deductive approach was chosen to evaluate the methodology and an inductive approach to determine the environment. The interviewees were researchers, chief information security officers, consultants and practitioners. Interviewing these people, who work or research on the respective meta-levels as part of their job, made it possible to consider all levels and analyse the process holistically. According to the evaluation of

the expert interviews, although the extended methodology has potential, it could lead to complications in the environment or organisation. Another option for evaluating the results would be a group discussion. However, it can be assumed that this would not provide any new insights due to the potentially low information power of the individuals. Therefore, the theoretically extended methodology could be tested in an experiment.

The extended IT-Grundschutz methodology has not yet been applied in practice. Evaluations have only been carried out on a theoretical basis, which is why the 'demonstration' process step of the DSRP was omitted in this research. This limitation can be found in all identified ESA methodologies. However, practical implementation options were identified in the description of the extended methodology.

Guideline 6: Design as a Search Process - the search for an efficient artefact requires the use of available means to achieve the desired goals and also the laws of the problem environment (cf. ibid.: 83).

As this research was conceived as a search process, it became apparent that each step of the process led to new findings. The iterative process of design and evaluation resulted in a solution that fulfils the requirements described in chapter 2.2 outlined in chapter 2.2.

Guideline 7: Communication of Research - Design and scientific research must be presented to both technology- and business-orientated target groups (cf. ibid.: 83).

The results were presented to a working group consisting of enterprise architects, security experts and managers from Nortal AG.

7. CONCLUSIO

This chapter summarises the most important results of this work. Recommendations for future research are also given, based in part on the previous discussion.

7.1. RELEVANT CONTRIBUTIONS TO THE THESIS

The focus of this work is on adapting the IT-Grundschutz methodology to a business-driven model. In doing so, information security is aligned with the organisational objectives, as the methodology does not show how this is possible. As part of the investigation into how the IT-Grundschutz methodology can be combined with SABSA to develop a holistic security architecture, the following results were obtained:

- A broad overview of enterprise architecture and ESA was provided, describing the possibilities, background and limitations.
- Above all, the extrinsic motivation of organisations for information security was uncovered by the expert interviews. Stakeholder management is therefore critical for establishing new procedures in an organisation.
- The extended IT-Grundschutz methodology with the SABSA methodology was presented. This was done in order to design the architecture according to the organisational objectives and integrate it into the enterprise architecture when establishing information security according to the IT-Grundschutz methodology.
- A mapping was created to enable organisational certification in accordance with ISO/IEC 27001 on the basis of IT-Grundschutz when using the extended IT-Grundschutz methodology. The latter can support the implementation of compliance with the regulatory requirements of the BSI.

The extended IT-Grundschutz methodology was modelled on the basis of the literature and evaluated through expert interviews. This result enables people to align their information security with the organisational goals and thus achieve business-driven information security. This enables target group-oriented communication, which leads to a better understanding of information security in the organisation and can support decision-making.

7.2. Recommendation for future research

As described in chapter 4.2 adaptation is an essential aspect for the application of the extended methodology. Therefore, a detailed consideration of this aspect is necessary in order to simplify the application and gain additional insights. For future research, an investigation of adaptation is suitable in the following three areas:

Structuring the extended IT-Grundschutz methodology according to a classic approach requires a process-orientated approach. This can lead to problems when implementing the methodology in adaptive, antifragile organisations that rely on agile approaches. It would therefore be necessary to determine which modifications to the extended IT-Grundschutz methodology are required in order to design an ESA in an agile environment. One approach would be to restructure the lifecycle of SABSA according to ITIL 4 and introduce agile principles.

Furthermore, it could be investigated to what extent a blurring of the architecture would be conceivable so that outdated information does not impair the architecture and a reduction in labour intensity could be recorded. This topic was addressed by interviewee F2, who experienced the use of SABSA in a corporate group. Maintaining the architecture was associated with a high use of resources (cf. chapter 4.2category 'Intensity').

Another potential consideration would be the collection of practical experience in the use of the extended IT-Grundschutz methodology. The findings could support the future adaptation of the methodology in order to make work processes more effective and efficient and to identify opportunities to adapt the methodology for organisations of different sizes and challenges.

8. BIBLIOGRAPHY

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.

Alshammari, 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 [accessd on 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.

Bounagui, 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 [accessd on 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 [accessd on 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-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html [accessd on 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 [accessd on 10.08.2024].

BSI (o. D.): IT-Grundschutz, Bundesamt für Sicherheit in der Informationstechnik, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html [accessd on 10.08.2024].

BSI (2023b): IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit, BSI, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html [accessd on 10.08.2024].

BSI (2023c): Kreuzreferenztabellen zum IT-Grundschutz-Kompendium (Edition 2023), BSI, [online] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/krt2023_Excel.html [accessd on 10.08.2024].

BSI (2019): Umsetzungshinweise: zum IT-Grundschutz-Kompendium, BSI, [online] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Umsetzungshinweise/umsetzungshinweise_node.html [accessd on 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-Vaw1c2S8nVry3jjniQsfdIBMN [accessd on 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 [accessd on 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.cisecurity.org/cis-benchmarks [accessd on 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 [accessd on 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 [accessd on 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-architecturea-top-down-approach [accessd on 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/smr.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/businesssystemsp00inte [accessd on 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/ [accessd on 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 [accessd on 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 [accessd on 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 [accessd on 10.08.2024].

ISO (2017): ISO/IEC 27003:2017, ISO, [online] https://www.iso.org/standard/63417.html [accessd on 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 [accessd on 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 [accessd on 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 [accessd on 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 [accessd on 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 Zamprogno/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 [accessd on 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.

Namagembe, 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 [accessd on 10.08.2024].

OMG (2014): *Business Process Model and Notation*, OMG, 2.0.2, Object Management Group, [online] https://www.omg.org/spec/BPMN/ [accessd on 10.08.2024].

OMG (2015b): *Unified Modeling Language*, OMG, 2.5, Object Management Group, [online] https://www.omg.org/spec/UML/2.5 [accessd on 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 [accessd on 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 [accessd on 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, Aleatrati 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.

Qiomos Nous (2024): Qnous, Qnous, [online] https://www.qnous.io/ [accessd on 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://cisr.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/Marcklyvens 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/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/4GS_Tag_2023/Aktuelles_und_Ausblick_zum_IT_Grundschutz.pdf?__blob=publicationFile&v=2 [accessd on 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 [accessd on 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/ [accessd on 10.08.2024].

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

The SABSA Institute (o. D.): Forums Archive - The SABSA Institute, SABSA, [online] https://sabsa.org/forums/ [accessd on 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 [accessd on 10.08.2024].

The SABSA Institute (2023): White Paper requests - the SABSA Institute, The SABSA Institute, [online] https://sabsa.org/white-paper-requests/ [accessd on 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.

APPENDIX A

Additional information on the extended IT-Grundschutz methodology

A.1 POSSIBLE ORGANISATIONAL STRUCTURE

As described in chapter 5.2 it is possible to locate the Enterprise Security Architects in the organisational structure in different ways. The following sub-chapters serve to specify and describe the previously outlined options for locating the Enterprise Security Architects within an organisation.

A.1.1 NORMALISATION OF ROLES AND RESPONSIBILITIES

In Table 1 harmonises the roles named in the IT-Grundschutz methodology. In addition, customised designations are provided in order to serve as a possible interface to other frameworks and to simplify communication.

Table 1: Normalisation and description of the IT-Grundschutz roles
Source: Own figure

IT-Grundschutz Role	New name	Description of the
Top management level	Organisation management	The highest management level for managing an organisation.
Information Security Officer (ISB)	Chief Information Security Officer (CISO)	Main contact person for all aspects of information security. It includes the coordination and promotion of security measures within the organisation.

IT-Grundschutz Role	New name	Description of the
		The position reports directly to the organisation's management.
Specialist responsible	Business Owner	Leading position within an organisation or department responsible for the implementation of professionally relevant decisions.
(Company) data protection officer (bDSB)	Chief Privacy Officer (CPO)	Supports the organisation in complying with data protection legislation to protect personal information.
Divisional Information Security Officer	Business Information Security Officer (BISO)	Implements the information security guidelines within a sub-area or department and manages security within the area.
Project Information Security Officer	Project Security Officer (PSO)	Implements information security requirements within a project and manages security within the project.
ICS Information Security Officer (ICS-ISB)	OT Security Officer (OTSO)	With an extended scope, the position translates information security requirements into OT and implements them technically and organisationally.

IT-Grundschutz Role	New name	Description of the
IS Management Team	ISMS team	Includes the coordination of overarching measures in the overall organisation, the consolidation of information and the implementation of control tasks. It consists of at least the position of CISO and deputy CISO.
Representative for IT security	IT Security Officer (ITSO)	Implements information security requirements technically in IT systems.
Safety officer	Safety Expert (SE) (Specialist for occupational safety)	Supports the organisation in complying with legal requirements for occupational safety in order to protect people and the environment.
	Security Service Expert (SSE) (Specialist for protection and security)	Ensures physical protection through preventive measures and hazard defence.
IS Coordination Committee	IS Coordination Committee (ISCC)	Not intended as a permanent institution in the organisation, but is convened when necessary, for example in the context of planning a large-scale project. Its function is to coordinate the interaction between the IS

IT-Grundschutz Role	New name	Description of the
		management team, specialist managers and security officers.

The following Table 2 presents an overview of the potential subdivisions of roles within the Enterprise Architecture and Enterprise Security Architecture. The subdivision of specialist areas in the EA areas is based on the following categories: 'Business', 'Application', 'Data', 'Integration', 'Infrastructure' and 'Security'.

Table 2: Description of the EA roles
Source: Own figure

Roles in Enterprise Architecture	Description of the
Chief Information Officer (CIO)	Responsible for information management in an organisation.
Architecture Manager (AM)	Manage the architecture teams and usually report to the CIO (cf. Kotusev: 291 - 292). The expansion could extend reporting to the CISO.
Enterprise Architect (EA)	Plan the overarching organisation-wide of all EA areas. They are generalists and are familiar with the various EA areas (cf. ibid.: 291).
Enterprise Security Architect (ESA)	Similar to an EA, but with a focus on overarching security. Due to the complexity of information security and the cross-thematic effects (processes, applications, systems, networks, etc.), a security architect should be established at EA level.

Roles in Enterprise Architecture	Description of the
Business Area Architect (BAA)	Plan IT end-to-end for a sub-area or business area / department (cf. ibid.: 291).
Business Area Security Architect (BASA)	Similar to a BAA, but focussing on end-to-end security for a sub-area or business area / department. It is unclear whether the security topics could be taken over by a BAA. This role is therefore proposed for the time being. There is a possibility that the BAAs could also model security through further training, so that a BASA would not be necessary.
Programme Architect (PA)	Plan major initiatives with an impact on various EA areas and several organisational units within an organisation (cf. ibid.: 293).
Domain Architect (DA)	Plan an EA area across the organisation. They are divided into business-supporting and business-enabling domains and are specialised in a specific EA area (cf. ibid.: 288 - 289).
Solution Architect (SA)	Plan the architecture of IT initiatives with a limited scope. They specialise in certain technologies, which is why they inherently specialise in a certain EA area (cf. ibid.: 287).

A.1.2 INCLUSION OF RESPONSIBILITIES FROM IT-GRUNDSCHUTZ

The following Table 3 summarises the distributed responsibilities described for the roles within BSI Standard 200-2 (cf. BSI 2017a).

Table 3: Synthesis of responsibilities from IT-Grundschutz methodology
Source: Own figure

Normalised roll	Responsibility
Organisation management	Responsible for the targeted and proper functioning of all business areas (cf. ibid.: 20)
Organisation management	Obligation to inform oneself about the risks and consequences of a lack of information security (cf. ibid.: 20)
Organisation management	Responsible for information security and achieving security objectives (cf. ibid.:20)
Organisation management	Defines basic safety objectives (cf. ibid.: 21)
Organisation management	Determines sufficient safety level (cf. ibid.: 21)
CISO	Coordinates information security and drives it forward (cf. ibid.: 40)
CISO	Advises the organisation's management on information security issues (cf. ibid.: 41)
CISO	Supports the implementation of information security (cf. ibid.: 41)
CISO	Controls the information security process and the associated tasks (cf. ibid.: 41)
CISO	Supports organisational management in drawing up the guideline on information security (cf. ibid.: 41)
CISO	Creates security concept, emergency supply concept and other sub-concepts and system security guideline as well as other guidelines and regulations on information security (cf. ibid.: 41)

Normalised roll	Responsibility
CISO	Initiates the realisation of measures and reviews their implementation (cf. ibid.: 41)
CISO	Reports to the organisation management and ISMS team on the status quo of information security (cf. ibid.: 41)
CISO	Coordinates security-related projects (cf. ibid.: 41)
CISO	Investigates security incidents (cf. ibid.: 41)
CISO	Initiates and monitors awareness-raising and training measures on information security (cf. ibid.: 41)
CPO	Monitors compliance with regulatory requirements for data protection (cf. ibid.: 48)
CPO	Contact person for all persons in an organisation for data protection and advises them (cf. ibid.: 48)
BISO, PSO, ITSO	Implement the CISO's information security require-ments (cf. ibid.: 44)
BISO, PSO, ITSO	Implement security measures in accordance with the security policy (cf. ibid.: 44)
BISO, PSO, ITSO	Summarise project or IT/OT system-specific information and forward it to the CISO (cf. ibid.: 44)
BISO, PSO, ITSO	Contact person for operational employees and manage-ment (cf. ibid.: 44)
BISO, PSO, ITSO	Participate in the selection of safety measures to imple-ment the specific safety guidelines (cf. ibid.: 44)
BISO, PSO, ITSO	Determining the training and sensitisation needs of em-ployees (cf. ibid.: 44)
BISO, PSO, ITSO	Check and analyse log files (cf. ibid.: 45)
BISO, PSO, ITSO	Report security-related incidents to the CISO (cf. ibid.: 45)

Normalised roll	Responsibility
OTSO	Implementation of security requirements from the guideline for information security and other guidelines in the area of OT (cf. ibid.: 46)
OTSO	Harmonisation of OT security and overall ISMS (cf. ibid.: 46)
OTSO	Carrying out risk assessments in the OT area that meet the requirements of risk management (cf. ibid.: 46)
OTSO	Creating security guidelines and concepts for OT areas (cf. ibid.: 46)
OTSO	Schools on the guidelines and concepts for the OT sector (cf. ibid.: 46)
OTSO	Contact for operational employees and management on OT security (cf. ibid.: 46)
OTSO	Developing security measures for OT security (cf. ibid.: 46)
OTSO	Participate in the implementation of OT safety measures (cf. ibid.: 46)
OTSO	Determining the training and sensitisation needs of employees (cf. ibid.: 46)
OTSO	Handle security incidents in the OT area with CISO (cf. ibid.: 46)
ISMS team	Developing information security goals and strategy (cf. ibid.: 43)
ISMS team	Developing the guideline for information security (cf. ibid.: 43)
ISMS team	Checking the implementation of the security guidelines (cf. ibid.: 43)
ISMS team	Initiating the security process (cf. ibid.: 43)
ISMS team	Controlling and monitoring the security process (cf. ibid.: 43)

Normalised roll	Responsibility
ISMS team	Support in the creation of the safety concept (cf. ibid.: 43)
ISMS team	Checking the effectiveness and appropriateness of security measures in the security concept (cf. ibid.: 43)
ISMS team	Designing training and awareness-raising programmes for information security (cf. ibid.: 43)
ISMS team	Advising business owners, IT operations, BSIO, OTSO and organisational management on information security issues (cf. ibid.: 43)
ISCC	Coordination of cooperation between the ISMS team, business owner, SE & SSE (cf. ibid.: 46)

A.1.3 STRUCTURING THE ARCHITECTURE ROLES

In order to strengthen the understanding of the structuring of architecture roles, the Figure 21 is used to explain the responsibilities.

The EAs and ESAs are responsible for cross-divisional planning within the entire organisation. BAAs and BASAs design a sub-area (e.g. a business unit) of an organisation with an end-to-end perspective. The planning of extensive initiatives that have an impact on several EA areas and sub-areas of an organisation is carried out by PAs. DAs have the task of harmonising the models in the EA areas across the organisation so that an effective architecture can be guaranteed. SAs create the architecture in which the technologies and measures to be used are specifically planned. As AMs do not carry out any architecture work, there is no overlap with the architects' areas of work.

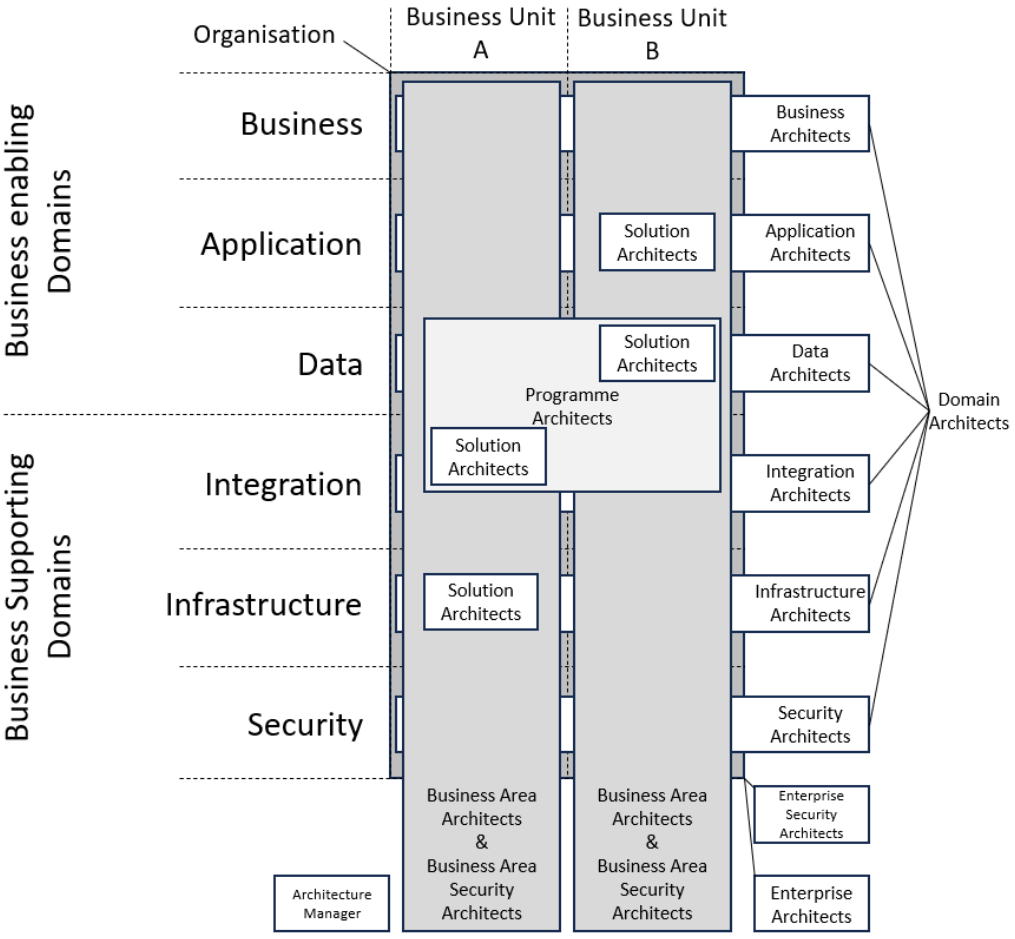

Figure 21: Localisation of the architectural roles
Source: Based on (Kotusev 2021: 294)

A.2 Mapping the R1 building blocks to SABSA Meta levels

The following subchapters contain an elaborated mapping between SABSA and all building blocks of the IT-Grundschutz Compendium 2023 (cf. BSI 2023b), whose prioritised implementation (R1) is recommended, as they form the basis for an effective security process (BSI 2017a: 137).

In A.2.1 Determined control objectives from the compendium the described target states of the building block are elaborated as control objectives. The control objectives form an essential basis for the systematic planning, implementation and management of security measures in an organisation.

To model and implement the necessary security measures, an initial control library was developed in A.2.2 Elaborated control library from IT-Grundschutz was created.

Furthermore, specific documentation is required in the modules. The required documentation is listed under A.2.3 Required documentation from R1 modules and are created in the course of the security process. They supplement the work products of A.3 Work products.

A mapping of all requirements of the selected modules can be found in A.2.4 Mapping the R1 building blocks of the compendium with SABSA levels to understand their impact on the meta levels.

A.2.1 DETERMINED CONTROL OBJECTIVES OF R1 MODULES

The Table 4 describes the identified control objectives of the R1 modules.

Table 4: Control objectives of the R1 modules
Source: Own figure

Building block	Control Objectives
ISMS.1	• Establishment of a functioning ISMS • Continuous improvement of the ISMS in operation
ORP.1	• Regulation of information flows • Regulation of the organisational structure • Regulation of the process organisation • Regulation of the distribution of roles
ORP.2	• Regulation of the employee lifecycle
ORP.3	• Strengthen employees' understanding of security risks by raising awareness • Strengthen employees' understanding of security risks through training
ORP.4	• Allow access to IT resources only for authorised entities • Allow access to information only for authorised entities • Allow access to IT resources only when required to perform an activity • Allow access to information only when required to perform an activity
CON.3	• Protection against data loss
CON.6	• Secure deletion and destruction of information
OPS.1.1.1	• Establishing information security in all aspects of IT operations • Ensuring functional, proper and systematic IT operations
OPS.1.1.2	• Establishing information security in all aspects of IT administration

Building block	Control Objectives
	• Ensuring that IT administration is carried out properly and systematically
OPS.1.1.3	• Regulation of patch management • Regulation of change management
OPS.1.1.4	• Protection of technical systems against malware
OPS.1.1.5	• Logging of all security-relevant events
OPS.1.1.6	• Evaluation and testing of software to be used • Systematic and methodical review of existing weaknesses in the software to be used
DER.1	• Collection, correlation and evaluation of security-relevant events • Detection of security incidents
DER.2.1	• Handling of security incidents

A.2.2 Elaborated control library from IT-Grundschutz

In the present Figure 22 shows a breakdown of the security requirements into logical and physical meta-levels, enabling visualisation. The creation in English serves to simplify cooperation and communication with the SABSA Institute.

Specific requirements of BSI Standard 200-2 (cf. BSI 2017a) were incorporated in individual points, as these are relevant for a secure and effective security process and are subject to a review during the audit.

With the aim of improving the overview and optimising the integration of security mechanisms, the author of this paper has developed additional security services. These can be recognised by a missing source reference.

Figure 22: R1 Building blocks for SABSA mapping
Source: Own figure

A.2.3 REQUIRED DOCUMENTATION FROM R1 MODULES

The data shown in the following Table 5 are relevant for the certification of an ISMS according to ISO/IEC 27001 on the basis of IT-Grundschutz. Furthermore, the requirements for the respective documents are set out, which define the creation of the documents and their content. Depending on the information security structure in an organisation, further documentation may also be required to demonstrate compliance with requirements or sub-requirements. The list is therefore not exhaustive, but merely shows the documentation that is explicitly required.

Table 5: Mandatory documentation according to R1 modules
Source: Own figure

Document	Requirement
Guideline on information security	• ISMS.1.A2 • ISMS.1.A3
Security concept	• ISMS.1.A6 • ISMS.1.A7 • ISMS.1.A10 • ISMS.1.A11 • ISMS.1.A13 • ISMS.1.A16
Management report	• ISMS.1.A12
Asset register	• ORP.1.A8 • OPS.1.1.1.A6
Information security user manual	• 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

Document	Requirement
Declaration of commitment and confirmation of awareness of and compliance with the information security requirements	• ORP.1.A2 • ORP.1.A16 • ORP.2.A14
Declaration of commitment for external personnel	• ORP.2.A4 • ORP.2.A5
Training and sensitisation concept for information security	• ORP.3.A4 • ORP.3.A8 • ORP.4.A5 • ORP.4.A6 • ORP.4.A7
Identity and authorisation management concept	• ORP.4.A1 • ORP.4.A3 • ORP.4.A8 • ORP.4.A11 • ORP.4.A12 • ORP.4.A16
Logging means of access	• ORP.4.A2 • ORP.4.A5
Logging means of access	• ORP.4.A2 • ORP.4.A6
Logging access means	• ORP.4.A2 • ORP.4.A7
Data backup concept	• CON.3.A1 • CON.3.A2 • CON.3.A4 • CON.3.A6 • CON.3.A7
Concept for deleting and destroying data	• CON.6.A1 • CON.6.A4
IT operating concept	• 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

Document	Requirement
	• 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
Documentation on the implementation of proper IT operations	• 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
Patch and change management concept	• OPS.1.1.3.A1 • OPS.1.1.3.A3 • OPS.1.1.3.A8
Documentation on the implementation of patch and change management	• 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
Concept for protection against malware	• OPS.1.1.4.A1 • OPS.1.1.4.A5 • OPS.1.1.4.A9
Logging concept	• OPS.1.1.5.A1
Protocol data	• OPS.1.1.5.A3 • OPS.1.1.5.A11

Document	Requirement
Concept for software testing and software releases	• 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
Security guideline for the detection of security-relevant events	• DER.1.A1 • DER.1.A3 • DER.1.A6 • DER.1.A7 • DER.1.A10
Documentation of detected security events	• DER.1.A5 • DER.1.A11 • DER.1.A12
Documented results of the audit of systems for the detection of safety-relevant events	• DER.1.A13
Guideline for handling security incidents	• 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
IT forensics concept	• DER.2.1.A3 • DER.2.1.A18

A.2.4 MAPPING THE R1 BUILDING BLOCKS OF THE COMPENDIUM WITH SABSA

The security requirements in the building blocks define the necessary establishment of technical and organisational security measures within an organisation to ensure effective information security. In order to address and incorporate these requirements into the extended methodology to meet the specifications, a mapping of each requirement was carried out.

The Table 6 serves as a first possible point of reference for the creation of further checklists. The R1 building blocks comprise a total of 221 requirements, whereby the omitted requirements were not taken into account. A consideration of all modules of the compendium results in a total number of 7,358 requirements, again excluding the omitted requirements. As each requirement is considered at the various levels, the creation of checklists that enable the complete consideration of all requirements could be advantageous.

Table 6: Building blocks for SABSA Layer Mapping
Source: Own figure

Requirement	Request type	SABSA meta level
ISMS.1.A1	Base	Contextual, Logical, Physical
ISMS.1.A2	Base	Conceptual, Logical, Physical
ISMS.1.A3	Base	Conceptual, Logical, Physical
ISMS.1.A4	Base	Contextual
ISMS.1.A5	Base	Contextual, Logical, Physical
ISMS.1.A6	Base	Conceptual, Logical, Component
ISMS.1.A7	Base	Conceptual, Logical, Component
ISMS.1.A8	Base	Logical
ISMS.1.A9	Base	Conceptual

Requirement	Request type	SABSA meta level
ISMS.1.A10	Standard	Conceptual
ISMS.1.A11	Standard	Logical
ISMS.1.A12	Standard	Logical
ISMS.1.A13	Standard	-/- (mapping not possible, affects all process steps of the extended methodology)
ISMS.1.A15	Standard	Conceptual
ISMS.1.A16	Increased protection requirements	Logical
ISMS.1.A17	Increased protection requirements	Logical
ORP.1.A1	Base	Conceptual
ORP.1.A2	Base	Conceptual, Logical
ORP.1.A3	Base	Physical
ORP.1.A4	Base	Logical
ORP.1.A8	Standard	Physical
ORP.1.A13	Standard	Logical
ORP.1.A15	Base	Conceptual, Logical
ORP.1.A16	Standard	Logical
ORP.1.A17	Increased protection requirements	Physical
ORP.2.A1	Base	Logical
ORP.2.A2	Base	Logical
ORP.2.A3	Base	Physical
ORP.2.A4	Base	Physical
ORP.2.A5	Base	Physical
ORP.2.A7	Standard	Logical

Requirement	Request type	SABSA meta level
ORP.2.A13	Increased protection requirements	Logical
ORP.2.A14	Base	Phyiscal
ORP.2.A15	Base	Logical
ORP.3.A1	Base	Physical
ORP.3.A3	Base	Physical
ORP.3.A4	Standard	Physical
ORP.3.A6	Standard	Logical
ORP.3.A7	Standard	Physical
ORP.3.A8	Standard	Logical
ORP.3.A9	Increased protection requirements	Physical
ORP.4.A1	Base	Logical, Physical, Component
ORP.4.A2	Base	Logical, Physical, Component
ORP.4.A3	Base	Physical
ORP.4.A4	Base	Logical
ORP.4.A5	Base	Logical, Physical
ORP.4.A6	Base	Logical, Physical
ORP.4.A7	Base	Logical, Physical
ORP.4.A8	Base	Logical, Physical
ORP.4.A9	Base	Logical
ORP.4.A10	Standard	Logical
ORP.4.A11	Standard	Logical
ORP.4.A12	Standard	Physical
ORP.4.A13	Standard	Logical, Physical

Requirement	Request type	SABSA meta level
ORP.4.A14	Standard	Physical
ORP.4.A15	Standard	Logical, Physical
ORP.4.A16	Standard	Logical
ORP.4.A17	Standard	Component
ORP.4.A18	Standard	Component
ORP.4.A19	Standard	Logical
ORP.4.A20	Increased protection requirements	Physical
ORP.4.A21	Increased protection requirements	Physical
ORP.4.A22	Base	Logical
ORP.4.A23	Base	Logical
ORP.4.A24	Increased protection requirements	Logical
CON.3.A1	Base	Contextual, Component
CON.3.A2	Base	Physical
CON.3.A4	Base	Component
CON.3.A5	Base	Logical
CON.3.A6	Standard	Component
CON.3.A7	Standard	Component
CON.3.A9	Standard	Physical
CON.3.A12	Base	Physical
CON.3.A13	Increased protection requirements	Logical
CON.3.A14	Base	Logical
CON.3.A15	Base	Physical
CON.6.A1	Base	Logical

Requirement	Request type	SABSA meta level
CON.6.A2	Base	Logical
CON.6.A4	Standard	Component
CON.6.A8	Standard	Logical
CON.6.A11	Base	Physical
CON.6.A12	Base	Component
CON.6.A13	Standard	Component
CON.6.A14	Increased protection requirements	Component
OPS.1.1.1.A1	Base	Conceptual, Component
OPS.1.1.1.A2	Base	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

Requirement	Request type	SABSA meta level
OPS.1.1.1.A19	Standard	Logical
OPS.1.1.1.A20	Standard	Logical
OPS.1.1.1.A21	Increased protection requirements	Logical
OPS.1.1.1.A22	Increased protection requirements	Physical
OPS.1.1.1.A23	Increased protection requirements	Logical
OPS.1.1.1.A24	Increased protection requirements	Logical
OPS.1.1.1.A25	Increased protection requirements	Logical
OPS.1.1.1.A26	Increased protection requirements	Logical
OPS.1.1.2.A2	Base	Physical
OPS.1.1.2.A4	Base	Logical, Physical
OPS.1.1.2.A5	Base	Logical
OPS.1.1.2.A6	Base	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	Increased protection requirements	Physical
OPS.1.1.2.A18	Increased protection requirements	Logical
OPS.1.1.2.A19	Increased protection requirements	Component

Requirement	Request type	SABSA meta level
OPS.1.1.2.A21	Base	Logical
OPS.1.1.2.A22	Base	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	Increased protection requirements	Logical
OPS.1.1.2.A30	Increased protection requirements	Logical
OPS.1.1.3.A1	Base	Logical
OPS.1.1.3.A2	Base	Contextual, Component
OPS.1.1.3.A3	Base	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	Increased protection requirements	Component
OPS.1.1.3.A13	Increased protection requirements	Logical

Requirement	Request type	SABSA meta level
OPS.1.1.3.A14	Increased protection requirements	Physical
OPS.1.1.3.A15	Base	Phyiscal
OPS.1.1.4.A1	Base	Logical
OPS.1.1.4.A2	Base	Component
OPS.1.1.4.A3	Base	Component
OPS.1.1.4.A5	Base	Component
OPS.1.1.4.A6	Base	Logical
OPS.1.1.4.A7	Base	Logical, Component
OPS.1.1.4.A9	Standard	Physical
OPS.1.1.4.A10	Increased protection requirements	Logical, Physical
OPS.1.1.4.A11	Increased protection requirements	Logical
OPS.1.1.4.A12	Increased protection requirements	Physical
OPS.1.1.4.A13	Increased protection requirements	Logical
OPS.1.1.4.A14	Increased protection requirements	Component
OPS.1.1.5.A1	Base	Logical
OPS.1.1.5.A3	Base	Physical
OPS.1.1.5.A4	Base	Logical
OPS.1.1.5.A5	Base	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

Requirement	Request type	SABSA meta level
OPS.1.1.5.A11	Increased protection requirements	Logical, Physical
OPS.1.1.5.A12	Increased protection requirements	Logical, Physical
OPS.1.1.5.A13	Increased protection requirements	Logical
OPS.1.1.6.A1	Base	Physical, Component
OPS.1.1.6.A2	Base	Logical, Physical
OPS.1.1.6.A3	Base	Logical, Physical
OPS.1.1.6.A4	Base	Logical, Physical
OPS.1.1.6.A5	Base	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	Base	Physical
OPS.1.1.6.A12	Standard	Physical
OPS.1.1.6.A13	Standard	Logical
OPS.1.1.6.A14	Increased protection requirements	Logical
OPS.1.1.6.A15	Standard	Logical
OPS.1.1.6.A16	Increased protection requirements	Physical
DER.1.A1	Base	Logical
DER.1.A2	Base	Contextual
DER.1.A3	Base	Physical
DER.1.A4	Base	Component
DER.1.A5	Base	Physical, Component

Requirement	Request type	SABSA meta level
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	Increased protection requirements	Physical, Component
DER.1.A15	Increased protection requirements	Physical
DER.1.A16	Increased protection requirements	Physical
DER.1.A17	Increased protection requirements	Physical
DER.1.A18	Increased protection requirements	Physical
DER.2.1.A1	Base	Logical
DER.2.1.A2	Base	Logical
DER.2.1.A3	Base	Logical, Physical
DER.2.1.A4	Base	Logical
DER.2.1.A5	Base	Physical
DER.2.1.A6	Base	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

Requirement	Request type	SABSA meta level
DER.2.1.A11	Standard	Physical
DER.2.1.A12	Standard	Logical
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	Increased protection requirements	Physical
DER.2.1.A20	Increased protection requirements	Conceptual, Physical, Component
DER.2.1.A21	Increased protection requirements	Conceptual, Physical, Component
DER.2.1.A22	Increased protection requirements	Logical, Physical

A.3 WORK PRODUCTS

The following tables describe the work products of the respective process steps of the extended IT-Grundschutz methodology in accordance with Chapter 5. They only contain the general work products. The specific products according to the R1 building blocks of the IT-Grundschutz Compendium 2023 (cf. BSI 2023b) can be found in Appendix A.2 Mapping of the R1 building blocks to SABSA meta levels can be taken from this.

Table 7: Work products from the initiation phase
Source: Own figure

Work product	Source
Certificate of appointment as CISO	-/-
Organisational model for ESA	-/-
Architecture Governance Plan	(ISO 2019b: 20)
Architecture Governance Policy & 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)
Catalogue of Enabling Capabilities	(ISO 2019b: 58)
Catalogue of Enabling Services	(ISO 2019b: 58)
Catalogue of Enabling Resources	(ISO 2019b: 58)
Architecture Work Product Templates	(ISO 2019b: 58)

Work product	Source
Recording of management decisions	(BSI 2017a: 56)

Table 8: Work products from the determination of the context
Source: Own figure

Work product	Source
Context description of the organisation	(cf. Sherwood et al. 2018: 7)
Business Driver	(cf. Sherwood et al. 2018: 7)
Business Driver for Security	(cf. Sherwood et al. 2018: 7)
Organisational and relationship model	(cf. Sherwood et al. 2018: 7)
Geography model	(cf. Sherwood et al. 2018: 7)
Time dependency model	(cf. Sherwood et al. 2018: 7)
Business risk model	(cf. Sherwood et al. 2018: 7)
Recording of management decisions	(BSI 2017a: 56)

Table 9: Work products from the conceptualisation
Source: Own figure

Work product	Source
Architecture Conceptualisation 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)
Architecture Models	(ISO 2019b: 53)

Work product	Source
Architecture Descriptions	(ISO 2019b: 53)
Business Attributes	(cf. Sherwood et al. 2018: 7)
Business Attributes Profile	(cf. Sherwood et al. 2018: 7)
Control Objectives	(cf. Sherwood et al. 2018: 7)
Control objectives integrated into business risk model	(cf. Sherwood et al. 2018: 7)
Determined actual state	(cf. Sherwood et al. 2018: 7)
Security Domain Model	(cf. Sherwood et al. 2018: 7)
Lifetimes & Deadlines	(cf. Sherwood et al. 2018: 7)
Security strategy	(cf. Sherwood et al. 2018: 7)
Responsibility Assignment Model	(cf. Sherwood et al. 2023)
Recording of management decisions	(BSI 2017a: 56)

Table 10: Work products from the security architecture
Source: Own figure

Work product	Source
Business Attribute Profile	(cf. Sherwood et al. 2018: 7)
Control Objectives	(cf. Sherwood et al. 2018: 7)
Control Library	(cf. Sherwood et al. 2018: 7)
Organisational structure IS	(cf. Sherwood et al. 2018: 7)
Policy architecture	(cf. Sherwood et al. 2018: 7)
Architecture Conceptualisation 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)

Work product	Source
Models Kinds	(ISO 2019b: 53)
Architecture Views	(ISO 2019b: 53)
Architecture Models	(ISO 2019b: 53)
Architecture Descriptions	(ISO 2019b: 53)
Security Policy Architecture	(cf. Sherwood et al. 2018: 7)
Security Policies	(cf. Sherwood et al. 2018: 7)
Security Services	(cf. Sherwood et al. 2018: 7)
Security Domains & Associations	(cf. Sherwood et al. 2018: 7)
Security Processing Cycle	(cf. Sherwood et al. 2018: 7)
CIP	(cf. Sherwood et al. 2018: 7)
Business Data Model	(cf. Sherwood et al. 2018: 7)
Security Rules & Procedures	(cf. Sherwood et al. 2018: 7)
Security Mechanism	(cf. Sherwood et al. 2018: 7)
IT landscape map	(cf. Sherwood et al. 2018: 7)
Capacity Plan	(cf. Sherwood et al. 2018: 7)
Resilience model	(cf. Sherwood et al. 2018: 7)
Control Structure Execution	(cf. Sherwood et al. 2018: 7)
IT & security concepts	(cf. Sherwood et al. 2018: 7)
IT & security fine concepts	(cf. Sherwood et al. 2018: 7)
Recording of management decisions	(BSI 2017a: 56)

Table 11: Work products from the implementation
Source: Own figure

Work product	Source
Cost and effort estimates	(BSI 2017a: 66)
Sequence of implementation of the measures	(BSI 2017a: 66)

Work product	Source
Project plan	(Sherwood 2005: 132)
Specification of the implementation	(Sherwood 2005: 132)
Procurement plan	(Sherwood 2005: 132)
Quality assurance plan	(Sherwood 2005: 132)
Test plan	(Sherwood 2005: 132)
Status and degree of implementation of the security concept or architecture	(BSI 2017a: 55)
Reports on successes to date in the security process	(BSI 2017a: 55)
Reports on the reduction of existing implementation deficits and the associated risks	(BSI 2017a: 55)
Installation and configuration instructions	(BSI 2017a: 56)
Instructions for restarting after a safety incident	(BSI 2017a: 56)
Documentation of test and release procedures	(BSI 2017a: 56)
Instructions for behaviour in the event of malfunctions and security incidents	(BSI 2017a: 56)
Instructions on work processes and organisational requirements	(BSI 2017a: 56)
Policy on the use of the Internet	(BSI 2017a: 56)
Instructions on behaviour in the event of security incidents	(BSI 2017a: 56)
Recording of management decisions	(BSI 2017a: 56)

Table 12: Work products from the CIP
Source: Own figure

Work product	Source
Architecture Governance Compliance Status Report	(ISO 2019b: 20)
Architecture Management Status Report	(ISO 2019b: 26)
Execution Status Report	(ISO 2019b: 27)
Architecture Conceptualisation 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)
Catalogue of Enabling Capabilities	(ISO 2019b: 58)
Catalogue of Enabling Services	(ISO 2019b: 58)
Catalogue of Enabling Resources	(ISO 2019b: 58)
Architecture Work Product Templates	(ISO 2019b: 58)
Gap analysis	(Sherwood 2005: 134)
Event Report	(Sherwood 2005: 134)
Incident Report	(Sherwood 2005: 134)

Work product	Source
Penetration Test Report	(Sherwood 2005: 134)
Operational Reports	(Sherwood 2005: 134)
Improvement Plan	(Sherwood 2005: 134)
Results of audits and data protection checks	(BSI 2017a: 55)
Recording of management decisions	(BSI 2017a: 56)

APPENDIX B

Search queries of the systematic Literature research

B.1 STRUCTURED LITERATURE RESEARCH ON IT-GRUNDSCHUTZ

The following search query was used for the searches described in Chapter 3.2 defined in chapter 3.2:

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

The following pages contain the results of the structured literature search. To simplify the grouping, the categories in Table 13 in abbreviated form. The column 'Included' indicates the possible inclusion of the text in this thesis.

Table 13: Literature on IT-Grundschutz
Source: Own figure

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

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

No.	Literature	In-cluded	Grouping
56	Einfallspforten für IT-Angreifer in der Medizin: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis	n	Factual text
57	Qualifizierung nach IT-Grundschutz - Maßstab für IT-Sicherheit.	n	Factual text
58	Hybride Testumgebungen in der Informationssicherheit - Effiziente Sicherheitsanalysen für Industrieanlagen	n	Tech treatise
59	Modellierung und Implementierung hybrider Testumgebungen für cyber-physische Sicherheitsanalysen	n	Tech treatise
60	Cyber-Sicherheits-Check: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden	n	Factual text
61	Normen, Standards, Practices: Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices	n	Factual text
62	Hybride Testumgebungen für Kritische Infrastrukturen: Effiziente Implementierung für IT-Sicherheitsanalysen von KRITIS-Betreibern	n	Tech treatise
63	Anforderungen an eine IT-Lösung für den ISO27-Sicherheitsprozess	n	No basic protection Focus
64	ISO 27001-Zertifikat auf der Basis von IT-Grundschutz	n	Factual text
65	Arbeiten zum Datenschutz im IT-Grundschutz vorläufig abgeschlossen	n	Message
66	Zweiter Akt – Erste Szene: Überwindung der Hürden	n	Factual text
67	Anwendung und Untersuchung einer Methode zur Analyse von IT-Sicherheitsrisiken anhand eines hochwertigen Erdfernerkundungssystems	n	No basic protection Focus
68	Datenschutzaudit nach IT-Grundschutz–Konvergenz zweier Welten	n	No basic protection Focus
69	Informantenschutz	n	No basic protection Focus
70	Compliance-Anforderungen und deren Einhaltung	n	No basic protection Focus
71	Die Zertifizierung in der Informationssicherheit	n	No basic protection Focus
72	The CAST Method for Comparing Security Standards	n	No basic protection Focus
73	Informationssicherheits-Management	n	No basic protection Focus
74	Herausforderungen der IT-Sicherheit bei kleinen und mittleren Betreibern kritischer Infrastrukturen	n	Tech treatise
75	A Structured Comparison of Security Standards	n	No basic protection Focus
76	DNS-Sicherheit im Rahmen eines IT-Grundschutz-Bausteins	n	Tech treatise
77	Sicherheitsprobleme für IT-Outsourcing durch Cloud Computing	n	Tech treatise
78	Methoden zur Umsetzung von Datensicherheit und Datenschutz im vernetzten Steuergerät	n	Tech treatise
79	Web Service Security für die IT-Grundschutz-Kataloge	n	Tech treatise
80	IT security issues in factories	n	Tech treatise

No.	Literature	In-cluded	Grouping
81	IT-Sicherheit 3.0: Der neue IT-Grundschutz: Grundlagen und Neuerungen unter Berücksichtigung des Internets der Dinge und Künstlicher Intelligenz	n	Tech treatise
82	IT-Grundschutz-basierendes Sicherheitskonzept für die Virtuelle Poststelle des Bundes.	n	No basic protection Focus
83	Holistic and Law Compatible IT Security Evaluation:	j	Comparison
84	Grundzüge eines Sicherheitskonzepts für Arztpraxen unter Berücksichtigung der Gesundheitstelematik	n	Tech treatise
85	IT security Issues in factories	n	Tech treatise
86	Ontology-based security standards mapping optimization by the means of Graph theory	n	No basic protection Focus
87	Audits und Zertifizierungen	n	Factual text
88	IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz: Der Weg zur Zertifizierung	n	Factual text
89	Vergleich von ISO/IEC 27033-1 und IT- Grundschutz	n	Tech treatise
90	Towards Process Centered Information Security Management - A Common View for Federated Business Processes and Personal Data Usage Processes	j	Methodology Customisation
91	Formalizing information security knowledge	n	No basic protection Focus
92	Specification of a Voting Service Provider	n	Tech treatise
93	Evaluation of Advanced Security Concepts to Improve the Trustworthiness of x86-Based Systems	n	Tech treatise
94	Notfallorganisation	n	No basic protection Focus
95	The Current State of "Information Security Awarenes" in German SMEs	n	Awarness
96	Internet security resources	n	No basic protection Focus
97	Ontological Mapping of Information Security Best-Practice Guidelines	n	No basic protection Focus
98	IT-Security Governance	n	No basic protection Focus
99	Towards the impact of the operational environment on the security of e-voting	n	Tech treatise
100	Sicherheitsaspekte von Instant Messaging	n	Tech treatise
101	Protokollierung in Sicherheitsstandards	n	Tech treatise
102	Messbare IT-Sicherheit	n	Tech treatise
103	Einführung in Informationsmanagementsysteme (II): BSI-Standards und Vergleich	n	Factual text
104	Sicherheitsaspekte von Instant Messaging	n	Tech treatise
105	Specification of a Voting Service Provider	n	Tech treatise
106	IT-Grundschutz-Kompendium	n	Factual text
107	IT-Grundschutz-Kataloge : Standardwerk zur IT-Sicherheit	n	Factual text

No.	Literature	In-cluded	Grouping
108	IT-Grundschutz und Datenschutz : Analyse des Informationsverbundes mittels IT-Grundschutz sowie rechtliche Aspekte einer Datenschutzrichtlinie anhand BSI	n	Risk management
109	Implementation of the IT-Grundschutz in Small and Medium Enterprises	n	Case Study
110	Checklisten Handbuch IT-Grundschutz : Prüfaspekte des IT-Grundschutz-Kompendiums	n	Factual text
111	Checklisten Handbuch IT-Grundschutz : Prüffragen zum IT-Grundschutz-Kompendium	n	Factual text
112	Systemsicherheits-Optimierungen in Web-basierten Systemen am Beispielprojekt DigiFit4All	n	No basic protection Focus
113	Exemplarische Sicherheitsanalyse und Sicherheitsanforderungen an eine Arztpraxis in Deutschland	n	No basic protection Focus
114	Ontology- and Bayesian-based information security risk management	n	No basic protection Focus
115	Managing security policies	n	Case Study
116	Sicheres verteiltes Rechnen unter dem Aspekt der Wirtschaftlichkeit	n	Tech treatise
117	Die Anforderungen von EUROSOX an IT-Prozesse : ein Umsetzungsleitfaden für Führungskräfte zur Implementierung von IT-Governance	n	Org treatise
118	Einführung von IT Policies und ITIL-konformen IT Service Management Prozessen in Kleinunternehmen	n	Org treatise
119	IT-Datenschutz und IT-Datensicherheit innerhalb von Unternehmen - moderne IT Infrastrukturen und deren Risiken im Fokus	n	Risk management
120	Entwicklung und Implementierung einer Methode für die Selektion von Sicherheitsmaßnahmen gemäß ISO/IEC 27001	n	Tech treatise
121	Smart Metering : Architektur und Vertragskonstellationen	n	No basic protection Focus
122	IT-Security und Geschäftsprozesse: Gelungenes Schnittstellenmanagement : Untersuchung von Potenzial und Problemen beim Zusammenspiel von IT-Security-Maßnahmen und Geschäftsprozessen	n	Tech treatise
123	Implementation model for the digital transformation of small and medium-sized enterprises	n	No basic protection Focus
124	Der IT Security Manager : aktuelles Praxiswissen für IT Security Manager und IT-Sicherheitsbeauftragte in Unternehmen und Behörden	n	No basic protection Focus
125	IT-Sicherheitsmanagement : Praxiswissen für IT Security Manager	n	No basic protection Focus
126	Managed IT Services : Leitfaden für die Transformation vom einfachen IT-Dienstleister zum Managed Service Provider	n	Org treatise
127	Sicherheitskonzept für Maritime Informations- und Kommunikationsservices	n	Tech treatise
128	IT-Sicherheitsmanagement und IT-Grundschutz : BSI-Standards zur IT-Sicherheit	n	Factual text
129	Checklisten Handbuch IT-Grundschutz : Prüfaspekte des IT-Grundschutz-Kompendiums	n	Factual text

No.	Literature	In-cluded	Grouping
130	IT-Grundschutz - Sicherheit in KMU	n	Case Study
131	Mapping security frameworks into SecOnt	n	Risk management
132	IT-Grundschutz Arbeitshandbuch : DIN ISO/IEC 27001, DIN ISO/IEC 27002; BSI-Standards 200-1/2/3	n	Factual text
133	Informationssicherheit und IT-Grundschutz : BSI-Standards 100-1, 100-2 und 100-3 ; mit CD-ROM	n	Factual text
134	Vermittlung von Informations-Sicherheit mittels E-Learning	n	No basic protection Focus
135	Implementierung von Sicherheitskennzahlen in den IT-Grundschutz	n	Org treatise
136	Entwurf eines BSI-IT-Grundschutz-Frameworks für Leitsysteme	n	Methodology Customisation
137	Durchführbarkeit und Nutzen von IT-Sicherheitsanalysen nach IT-Grundschutz in KMUs	n	Risk management
138	Einführung von Informationssicherheit basierend auf den IT-Grundschutz-Katalogen	n	Org treatise
139	Erstellung eines IT-Grundschutz-Profils für eine oberste Landesbehörde in der Bundesrepublik Deutschland	n	Org treatise
140	ISO/IEC 27001 ISO/IEC 27002 und IT-Grundschutz : Schnelleinstieg Informationssicherheit 2022	n	Factual text
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	Factual text
143	IT-Grundschutz für "Kleine und Mittlere Unternehmen" (KMU´s) : Schwachstellen in DV-Landschaften erkennen und beseitigen	n	Tech treatise
144	Praxisbuch Netzwerk-Sicherheit : Risikoanalyse, Methoden und Umsetzung	n	Factual text
145	BSI und DSGVO für österreichische KMUs	n	Methodology Customisation
146	Ein KMU-orientiertes Disaster Preparedness Konzept für IT-Infrastrukturen zur Vorbereitung auf natürliche und, daraus resultierende, technologische Katastrophen	n	No basic protection Focus
147	Ein Security Testverfahren zur Unterstützung von KMUs in der Softwareentwicklung	n	Tech treatise
148	Konzeptualisierung und Implementierung eines Security Layers für ArchiMate	n	No basic protection Focus
149	An approach to continuous information security risk assessment focused on security measurements	n	Risk management
150	IT-Compliance an der Pädagogischen Hochschule Steiermark : Initiierungsplan eines Sicherheitskonzeptes und Erarbeitung der datenschutzrechtlichen Bestimmungen für die Verarbeitung von Studierendendaten im Hochschulbereich	n	No basic protection Focus
151	Einführung des Oracle Identity Managements in das Unternehmen Austrian Energy & Environment mittels Workflows und die Analyse des IT Grundschutzes	n	Case Study

No.	Literature	In-cluded	Grouping
152	IT-Risikomanagement mit System : praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken	n	Risk management
153	Handbuch Datenschutz und IT-Sicherheit	n	No basic protection Focus
154	Checklisten Handbuch IT-Grundschutz : sämtliche Prüffragen des BSI / Bundesamt für Sicherheit in der Informationstechnik	n	Factual text
155	Informationssicherheit und Datenschutz : Handbuch für Praktiker und Begleitbuch zum T.I.S.P.	n	No basic protection Focus
156	IT-Grundschutz umsetzen mit GSTOOL : Anleitungen und Praxistipps für den erfolgreichen Einsatz des BSI-Standards / Frederik Humpert	n	Factual text
157	Quick-Check Security Audit	n	Factual text
158	Quick-Check Security Audit	n	Factual text
159	ISO 17799 und BSI-Grundschutz	n	Factual text
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 treatise
162	Datenschutz nach BSI-Grundschutz? Das Verhaltnis zwischen Datenschutz und Datensicherheit	n	Jur treatise
163	Datenschutz im IT-Grundschutz	n	Jur treatise
164	BSI IT-Grundschutz – Arbeitswerkzeug für ganzheitliche Informationssicherheit	n	Factual text
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	No basic protection Focus
166	VS-Zulassung: Einführung und Grundlagen	n	No basic protection Focus
167	Sicherheit nach BSI-Grundschutz und ISO 27001 : Grundlagen der Sicherheitsstandards ; Audits ; Unterstützung des Sicherheitsprozesses mit verinice	n	Factual text

B.2 STRUCTURED LITERATURE RESEARCH ON ESA AND SABSA

The following search query was used for the searches described in Chapter 3.2 defined in chapter 3.2:

(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")

The following pages contain the results of the structured literature search. Column 'Included' means the possible inclusion of the text in this thesis.

Table 14: Literature on ESA and SABSA
Source: Own figure

No.	Literature	In-cluded	Description of the
1	Chapter 3 - Cyber Risk Management: A New Era of Enterprise Risk Management	n	Focus on RM
2	Chapter 13 - A Blueprint for Security	n	Focus on RM
3	Towards augmented proactive cyberthreat intelligence	n	Focus on threat intelligence
4	Chapter 2 - Risk Assessment and Monitoring in Intelligent Data-Centric Systems	n	Focus on RM
5	Integrated identity and access management metamodel and pattern system for secure enterprise architecture	n	Focus on integrating IAM into EA
6	SALSA: A method for developing the enterprise security architecture and strategy	n	Predecessor of SABSA
7	Enterprise security pattern: A model-driven architecture instance	n	Focus on software architecture
8	CAESAR8: An agile enterprise architecture approach to managing information security risks	j	Agile working methods for ESA
9	A new month, a new data breach	n	Describes why encryption is important
10	What does 'secure by design' actually mean?	n	Describes the general shift-left approach
11	Enterprise information security, a review of architectures and frameworks from interoperability perspective	n	Compares ESA Frameworks
12	AT&T strengthen security of Network Notes	n	Focus on network security
13	Top to tail router security	n	Focus on network security
14	The changing face of IT security	n	Focus is also on tech. Security
15	The importance of context in keeping end users secure	n	Focus on IT architecture
16	Do you have the right security?	n	Describes the threat situation in 2011
17	The cybersecurity workforce and skills	n	Describes qualifications in cyber security
18	Investigating digital fingerprints: advanced log analysis	n	Focus on analysing logs
19	Securing the building blocks of system architecture	n	Describes in an abstract way how security could be organised in companies
20	Two-factor authentication – a look behind the headlines	n	Focus on authentication
21	From auditor-centric to architecture-centric: SDLC for PCI DSS	j	Mapping the architecture via thread modelling to PCI DSS security requirements
22	A roadmap to develop enterprise security architecture	n	Article describes a separate immature ESA that resembles SABSA
23	Virtual enterprises and the enterprise security architecture	n	Focus on technical architecture
24	An enterprise security architecture for accessing SaaS cloud services with BYOD	n	Focus on technical architecture
25	Enterprise Security Architecture For Cloud Computing: A Review	n	Focus on cloud architecture
26	Securing the mobile enterprise with network-based security and cloud computing	n	Focus on network security
27	Towards a Metamodel for SABSA Conceptual Architecture Descriptions	j	Description of the conceptual architecture using metamodels
28	Rethinking Security Operations Centre Onboarding	n	Focus on SOC
29	An Organization-Driven Approach for Enterprise Security Development and Management	n	Own ESA development with focus on tech, similar to SABSA
30	A Distributed Approach to Delegation of Access Rights for Electronic Health Records	n	Focus on integrating IAM into EA

No.	Literature	In-cluded	Description of the
31	Protection of enterprise resources: A novel security framework	n	Focus is also on tech. Security
32	Towards a Holistic Information Security Governance Framework for SOA	n	Shows how SABSA can be used for SOAs
33	Integrating Trusted Computing Mechanisms with Trust Models to Achieve Zero Trust Principles	n	Focus on Zero Trust
34	Enterprise Security Architecture	n	Focus on network security & IAM
35	Fujitsu Enterprise Security Architecture	n	Focus on technical architecture
36	Enterprise security architecture in business convergence environments	n	Describes convergence of security and EA, result is similar to SABSA
37	Ranking Criteria of Enterprise Information Security Architecture Using Fuzzy Topsis	n	Describes fuzzers for identifying popular IS topics in the EISA area
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	Focus on technical safety
40	Zero Trust Security : An Enterprise Guide	n	Focus on Zero Trust
41	The handbook of technology management. 3 Management support systems, electronic commerce, legal and security considerations	n	Describes the technical safety
42	Cyber Security on Azure : An IT Professional's Guide to Microsoft Azure Security Center	n	Focus on technical safety
43	Cloud Attack Vectors : Building Effective Cyber-Defense Strategies to Protect Cloud Resources	n	Focus on the cloud
44	IoT – Best Practices : Internet der Dinge, Geschäftsmodellinnovationen, IoT-Plattformen, IoT in Fertigung und Logistik	n	Focus on IoT
45	A Comprehensive Guide for Web3 Security : From Technology, Economic and Legal Aspects	n	Focus on technology
46	A UML-based methodology for model-driven B2B integration: from business values, over business processes to deployment artifacts	n	Focus on IT architecture
47	Web services enterprise security architecture: a case study	n	Focus on tech. Security
48	WebUpdated Standard for Secure Satellite Communications: Analysis of Satellites, Attack Vectors, Existing Standards, and Enterprise and Security Architectures	n	Focus also on satellite security
49	Mitigating IoT Enterprise Vulnerabilities Using Radio Frequency Security Architecture	n	Focus on IoT
50	Security Architecture Framework for Enterprises	j	Own ESA development, similar to SABSA
51	Enterprise Security Architecture: Mythology or Methodology?	j	Own ESA development, similar to SABSA
52	Method Framework for Developing Enterprise Architecture Security Principles	j	Own ESA development
53	A novel architecture for an integrated enterprise network security system	n	Focus on network security
54	An integrated conceptual model for information system security risk management supported by enterprise architecture management	n	Focus on RM with integration in EA
55	Towards an Integration of Information Security Management, Risk Management and Enterprise Architecture Management – A Literature Review	n	Focus on RM with integration in EA

No.	Literature	In-cluded	Description of the
56	Challenges for Risk and Security Modelling in Enterprise Architecture	j	Risk modelling and automated decision-making for ESA
57	Research on Enterprise Security Early Warning System Architecture Based on Internet of Things	n	Focus on IoT
58	Adaptive security architecture for protecting RESTful web services in enterprise computing environment	n	Focus on REST
59	Enterprise Architecture for International Agreements in Social Security Institutions	n	Focus on EA
60	An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement	n	Focus on network security
61	Enterprise Architecture Security Assessment Framework (EASAF)	j	Quantified measurement of security in EA
62	Unikernels for Cloud Architectures: How Single Responsibility can Reduce Complexity, Thus Improving Enterprise Cloud Security	n	Focus on the cloud
63	Exploring the Role of Enterprise Architecture Models in the Modularization of an Ontology Network: A Case in the Public Security Domain	n	Creation of ontology for the description of information exchange
64	A secure enterprise architecture focused on security and technology-transformation (SEAST)	j	Own ESA development
65	Where Enterprise Architecture and Early Ontology Engineering Meet: A Case Study in the Public Security Domain	n	Focus on ontology
66	Security analysis model, system architecture and relational model of enterprise cloud services	n	Focus on the cloud
67	Enterprise Architecture-Based Risk and Security Modelling and Analysis	n	Focus on risk assessment in TOGAF
68	An Integrated Conceptual Model for Information System Security Risk Management and Enterprise Architecture Management Based on TOGAF	n	Focus on RM in TOGAF
69	Knowledge Elicitation and Conceptual Modeling to Foster Security and Trust in SOA System Evolution	n	Focus on SOA
70	Towards the ENTRI Framework: Security Risk Management Enhanced by the Use of Enterprise Architectures	n	Focus on RM in TOGAF
71	Robust Enterprise Application Security with eTRON Architecture	n	Focus on technical safety
72	The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures	n	Focus on technical safety
73	Conceptual Integration of Enterprise Architecture Management and Security Risk Management	n	Focus on RM with integration in EA
74	Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®	n	Explains SABSA
75	Long-term security of digital information: Assessment through risk management and Enterprise Architecture	n	Focus on RM with integration in EA
76	On an Integration of an Information Security Management System into an Enterprise Architecture	n	Mapping of ISO/IEC 27001 in EA with a focus on tech
77	A Novel Architecture for Enterprise Network Security	n	Focus on network security
78	Governance of Information Security Elements in Service-Oriented Enterprise Architecture	n	Focus on SOA

No.	Literature	In-cluded	Description of the
79	Combining Defense Graphs and Enterprise Architecture Models for Security Analysis	n	Focus on technical safety
80	Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool	n	Focus on integrating IAM into EA
81	Using FDAF to bridge the gap between enterprise and software architectures for security	n	Combines ontology with IAM
82	A Security Architecture for Enterprise Rights Management	n	IAM in security architecture
83	A distributable security management architecture for enterprise systems spanning multiple security domains	n	Focus on technical safety
84	Mobile-driven architecture for managing enterprise security policies	n	Focus on mobile security
85	Security in enterprise resource planning systems and service-oriented architectures	n	Focus on technical safety
86	Securing Service-Oriented and Event-Driven Architectures Results of an Evaluation of Enterprise Security Frameworks	n	Focus on technical safety
87	SANE: A Protection Architecture for Enterprise Networks	n	Focus on network security
88	Enterprise knowledge security architecture for military experimentation	n	Combination of the ontology of information and access to it
89	SPECSA: a scalable, policy-driven, extensible, and customizable security architecture for wireless enterprise applications	n	Focus on technical safety
90	Enterprise Engineering And Security: Enterprise Frameworks and Architectures, and IA Patterns	n	Focus on EA
91	Security management system functional architecture for enterprise network	n	Focus on network security
92	Security aspects of an enterprise-wide network architecture	n	Focus on network security
93	Applying the DoD goal security architecture as a methodology for the development of system and enterprise security architectures	j	Own ESA framework created
94	Inter-enterprise contract architecture for open distributed systems: security requirements	n	Focus on technical safety
95	Obtaining secure business process models from an enterprise architecture considering security requirements	n	Focus on technical safety

APPENDIX C

Interview structure and results

C.1 INTERVIEW QUESTIONS AND YOUR TOPICS

1. How do you rate the general approach in the context of information security? (Topic: Perspective)
2. Are there any aspects of the methodology that you find particularly relevant or innovative? (Topic: Relevance)
3. What challenges or risks can arise when applying this methodology? (Topic: Challenge)
4. How do you see the relevance of this methodology and the main challenges in the light of future developments in the field of information security? (Topic: Future)

In addition, the category 'Other' was created in order to be able to code information that goes beyond the question but would be relevant or interesting for the extended methodology.

C.2 BACKGROUND INFORMATION ON THE EXPERT INTERVIEW

The following Table 15 provides information on the distribution of enquiries and feedback.

Table 15: Distribution of respondents
Source: Own figure

Role	Enquiries	Feedback	% of total responses
CISO	6	2	20%
Practitioner	8	3	30%
Consultant	8	3	30%
Researcher	5	2	20%
Total	27	10	100%

In Table 16 shows the maturity levels indicated by the respondents for their respective organisations and customers.

Table 16: Maturity level of the respondents' organisations
Source: Own figure

Person	Maturity level of information security
CISO 1	Medium
CISO 2	Medium
Practitioner 1	Medium
Practitioner 2	Medium
Practitioner 3	High
Consultant 1	Medium
Consultant 2	Medium
Consultant 3	High
Researcher 1	Low
Researcher 2	Medium

C.3 CODES AND THEIR FREQUENCY

The following pages list the excerpt of the raw coding of the expert interviews as a result of the open coding. These codes were not edited.

Table 17: Codes and their frequency in interviews
Source: Own figure

Category	Code	Cases	% Cases
Perspective	End-to-end	3	30,0%
Perspective	Focussing	2	20,0%
Perspective	Seamless working	1	10,0%
Perspective	CIP	3	30,0%
Perspective	Holistic view	2	20,0%
Perspective	Uncertainty as to whether ESA is required	1	10,0%
Perspective	Integration into existing structures	1	10,0%
Perspective	Supplement	1	10,0%
Perspective	Data-driven	1	10,0%
Perspective	Transparency	1	10,0%
Perspective	Traceability	1	10,0%
Perspective	Scepticism	1	10,0%
Perspective	Not for regulated areas	1	10,0%
Further information	Commitment	1	10,0%
Further information	Design	1	10,0%
Further information	Uncertainty	1	10,0%
Further information	Tailoring	2	20,0%
Further information	Practical example	1	10,0%
Further information	No security in EA consideration	2	20,0%
Further information	EA too academic	1	10,0%
Further information	Agility is becoming more important	1	10,0%
Further information	Working without the right tools	2	20,0%
Further information	EA Tool	1	10,0%
Further information	Security according to compliance	5	50,0%
Further information	Expectation to align InfoSec with business objectives	1	10,0%
Further information	Lack of organisational context in security standards	1	10,0%
Further information	Unstructured way of working	1	10,0%
Further information	Enterprise Architects for ESA	1	10,0%
Further information	Structural design	1	10,0%
Further information	Promoter	1	10,0%
Further information	Unclear corporate goals	1	10,0%

Category	Code	Cases	% Cases
Further information	Alignment Security Different	1	10,0%
Further information	Work according to checklist	1	10,0%
Further information	Lack of strategy	1	10,0%
Further information	Application of safety measures	1	10,0%
Relevance	Link	1	10,0%
Relevance	Organisation size	2	20,0%
Relevance	Alignment Sec according to organisational goals	3	30,0%
Relevance	Support for	1	10,0%
Relevance	No interpretation	1	10,0%
Relevance	Connection with Zero Trust	1	10,0%
Relevance	data streams	1	10,0%
Challenge	Complexity	3	30,0%
Challenge	Acceptance	1	10,0%
Challenge	Elaborate	1	10,0%
Challenge	No support for departments	1	10,0%
Challenge	Time consuming	1	10,0%
Challenge	Conflict of interest	1	10,0%
Challenge	Lack of agility	1	10,0%
Challenge	Expectations	1	10,0%
Challenge	KPI Election	1	10,0%
Challenge	Cooperation between departments	1	10,0%
Challenge	Methodology Application	1	10,0%
Challenge	Internal resistor	1	10,0%
Challenge	Showing the added value of architecture	1	10,0%
Challenge	Uncertainty in compliance	1	10,0%
Challenge	Lack of experience	1	10,0%
Challenge	New topic	1	10,0%
Challenge	Lack of knowledge	1	10,0%
Challenge	Lack of experts	1	10,0%
Challenge	Auditing not problematic	1	10,0%
Future	Dealing with complexity	7	70,0%
Future	Connecting with other topics	1	10,0%
Future	Auditing	1	10,0%
Future	Increasing regulations	1	10,0%
Future	Difficult market establishment	1	10,0%
Future	Pioneer company	1	10,0%

C.4 SUMMARISED CODING

To synthesise the information content of the ten expert interviews, the codes were grouped according to their content using axial coding. The result and the percentage of mentions in relation to the total number of interviews can be seen in Table 18.

Table 18: Content consolidation
Source: Own figure

Category	% Cases
Integrated solution approach	80,0%
Safety culture	70,0%
Organisational culture	60,0%
Dealing with complexity	60,0%
Adaptation	60,0%
CIP	40,0%
Security alignment	40,0%
Complexity	30,0%
Strategic uncertainty	20,0%
EA problems	20,0%
Auditing	20,0%
Intensity	10,0%
EA tools	10,0%
Uncertainty as to whether ESA is necessary	10,0%

To improve the comprehensibility of the topics and the interpretability of the synthesis, the result was visualised, see Figure 24and the respective categories were placed in context, see Figure 25. The legend for the visualisation can be found in Figure 23 can be taken from Figure 23.

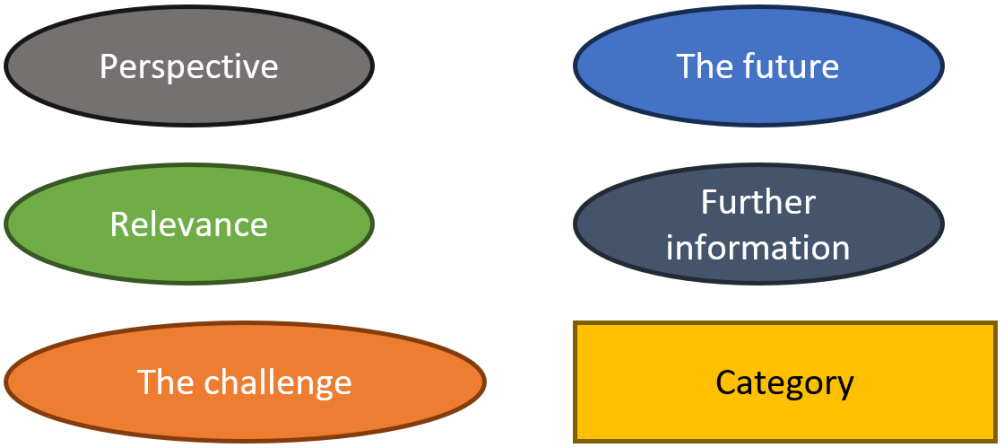

Figure 23: Legend for Figures 24 and 25
Source: Own figure

Two codes could not be summarised with other codes due to their content representation, which is why they are presented as a separate summary.

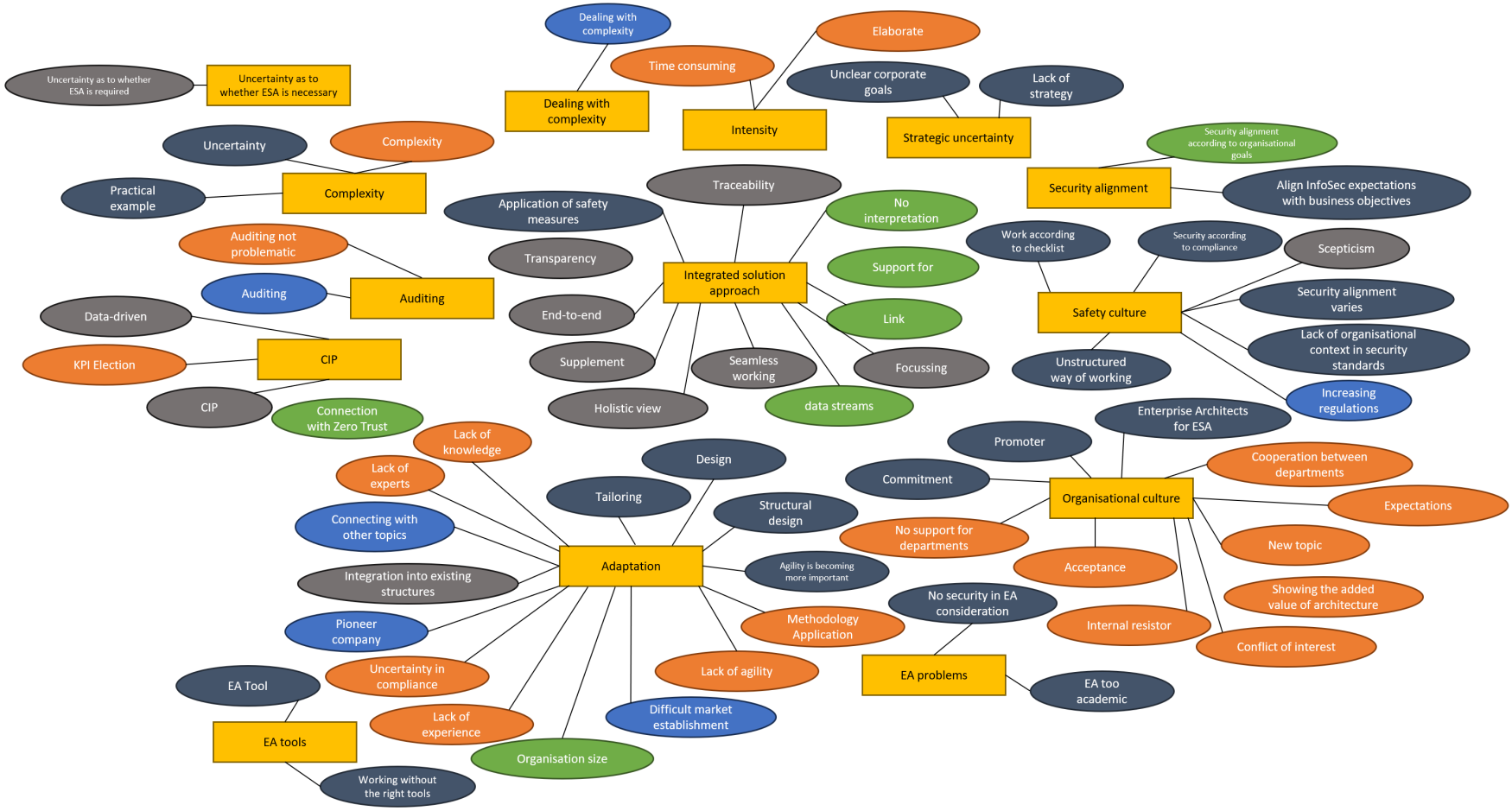

Figure 24: Visualisation of the content merging
Source: Own figure

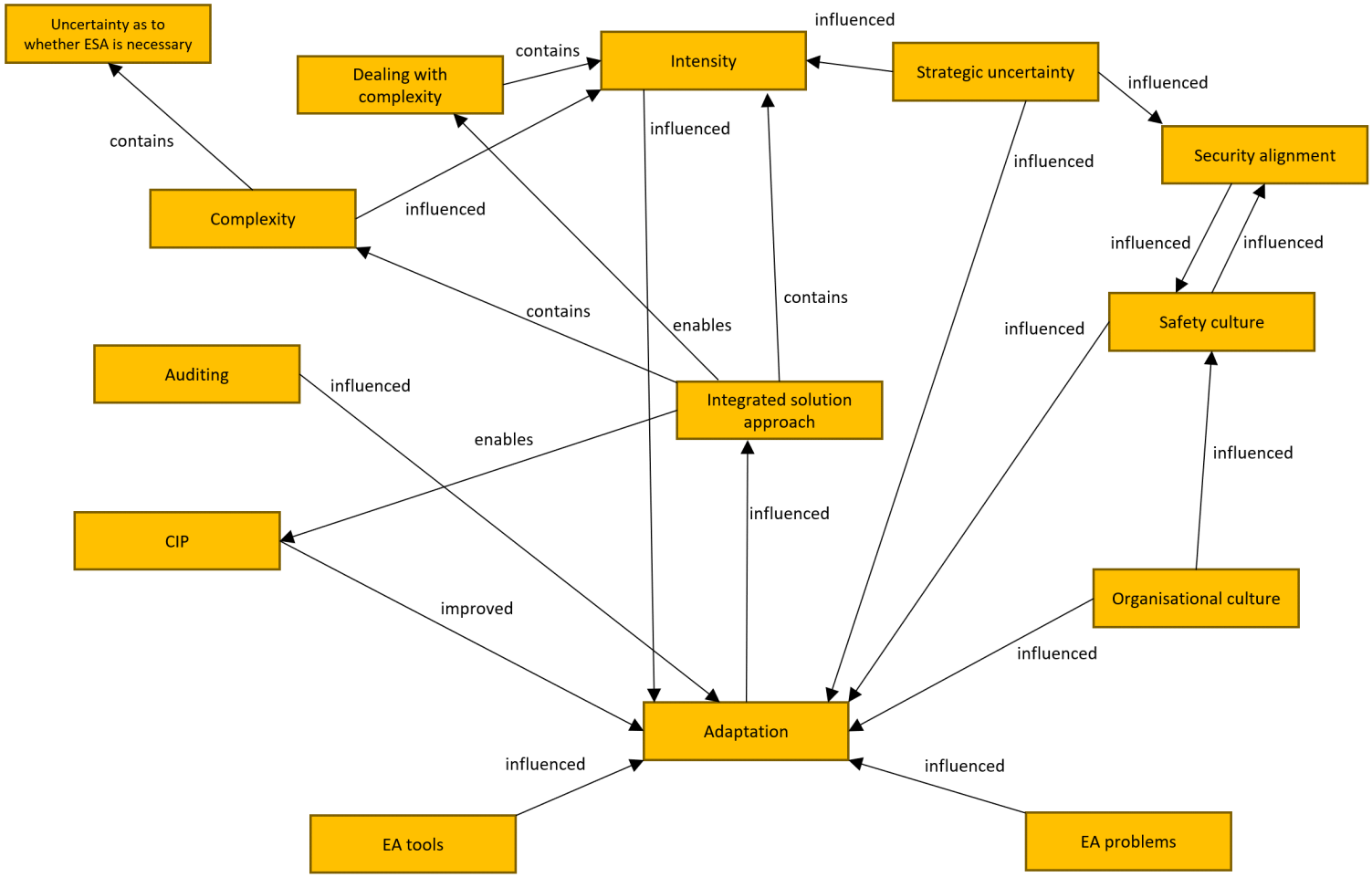

Figure 25: Relationships between the categories
Source: Own figure

APPENDIX D

Raw expert interview transcriptions

This appendix is supplied separately.