DISENTANGLING THE CONCEPT OF INFORMATION SECURITY PROPERTIES - ENABLING EFFECTIVE INFORMATION SECURITY GOVERNANCE

Research Paper

Bitzer, Michael, FIM Research Center, University of Augsburg, Augsburg, Germany, michael.bitzer@fim-rc.de

Brinz, Nicolas, Department of Orthodontics, University Medical Centre of Regensburg, Germany, nicolas.brinz@ukr.de

Ollig, Philipp, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, University of Bayreuth, Bayreuth, Germany, philipp.ollig@fit.fraunhofer.de

Abstract

The hyper-dynamic, global adoption of digital technologies due to the Covid-19 pandemic and the increasing digitalization of business models necessitate a dialogue on fundamental concepts that assist organizations in defining appropriate requirements for their information security measures. The definition of information security properties (ISPs) represents a widely used approach to describe the security needs of business assets in an understandable manner. However, academia and practice lack a consensus on underlying concepts and definitions. Here, we eliminate prevailing inconsistencies in definitions of ISPs by synthesizing the available literature. By extending the most common information security concept – i.e., the Confidentiality, Integrity & Availability (CIA) Triad – we disentangle the interrelations between various ISPs. Our results enhance the understanding of relevant ISPs and their interrelations, support organizations' information security strategies, and deliver valuable impulses to stimulate further research concerning the influence of organizational characteristics on ISP prioritizations.

Keywords: Information Security, Information Security Properties, CIA Triad, Literature Review.

1 Introduction

In 2017, the WannaCry ransomware carried out a hostile encryption of valuable data assets across the world, causing massive damage to various organizations and industries (Mohurle and Patil, 2017; McLaughlin and Gogan, 2018). Overall, the frequency and impact of information security (IS) incidents have grown dramatically in recent decades (Brinz et al., 2018; McLaughlin and Gogan, 2018). The constantly increasing variety of cyber threats, together with the ongoing digitalization of business models, requires more than ever sophisticated IS governance (Hohan et al., 2015). This development has become apparent to chief information officers (CIOs) around the world. According to the Society for Information Management, IS emerged as the most important information management issue (Kappelman et al., 2020), even before the impact of the Covid-19 pandemic led to the hyper-dynamic adoption of digital technologies. As time and budgets are limited, the appropriate allocation of resources is key to minimize the impact that IS incidents have on businesses (Fabian et al., 2010). The case of Yahoo! Inc. in 2014 (United States Securities and Exchange Commission, 2017) shows the devastating effects of a lack of common understanding between management and IS experts. Therefore, determining relevant information security properties (ISPs) represents the first meaningful step toward addressing this issue (Ma and Ratnasingam, 2008).

ISPs are criteria or constraints that describe business assets' security needs in a manner that can be understood by IS experts and on the management level (Dubois et al., 2010; Fabian et al., 2010). One model widely used to conceptualize IS threats is the CIA Triad, which identifies *confidentiality*, *integrity*, and *availability* as ISPs that organizations need to protect (Eckert, 2009). Although the use of ISPs is widespread in the context of IS governance (Brotby, 2007; de Oliveira Alves, Gustavo Alberto et al., 2006; Posthumus and Solms, 2004; Williams, 2001), academia and practice lack uniform and unambiguous definitions of ISPs as well as a common nomenclature and understanding of the concept of ISPs. Due to a lack of standardization in the field of ISPs, designations, definitions, and the resulting relevance of different ISPs diverge (Moghaddasi et al., 2016). As a consequence, organizations struggle to adequately allocate available resources and, therefore, guarantee IS governance, i.e., the identification and satisfaction of their most relevant ISPs (Gao and Zhong, 2015). As IS becomes more important than ever (Brinz et al., 2018), gaining insights about existing ISPs and their interrelations helps organizations to assess the significance of particular ISPs for their business and, consequently, identify countermeasures against cyber threats (Fabian et al., 2010; Moghaddasi et al., 2016; Hedström et al., 2011). Being aware of the interrelations between ISPs also helps organizations to develop IS strategies that focus not on single countermeasures but the development of a portfolio of countermeasures. This means that resources can be allocated both more effectively and efficiently by creating synergies (Huang et al., 2014). Common nomenclature and understanding of ISPs and their interrelations also facilitate further IS research in the information systems discipline (Moghaddasi et al., 2016). Against this backdrop, we address the following research questions:

RQ1: Which Information Security Properties exist?

RQ 2: How do Information Security Properties relate to one another?

To answer our research questions, we follow Webster and Watson (2002) and conduct a comprehensive and structured literature review. To create a clear understanding of existing ISPs, we screen the reviewed papers for different terms in the field of ISPs and, subsequently, merge terms and definitions to create a consistent overview of existing ISPs and their interdependencies. Thereby, we build upon the widespread and well-accepted concept of the CIA Triad (Lundgren and Möller, 2017). Our research emphasizes the importance of ISPs for an organization's IS governance and the design of information systems. The study, thus, extends the general understanding of ISPs in the information system community. Furthermore, our resultant synthesis of definitions and interrelations summarizes existing insights about ISPs. Thereby, our work lays the foundation for interdisciplinary communication across different hierarchical levels in practice (Fabian et al., 2010; Zissis and Lekkas, 2012).

2 Theoretical Background

2.1 Information Security Properties in Information Security Governance

Even though definitions of IS vary, deviations in meaning are marginal. Most scholars agree that ensuring business continuity and minimizing the impact – i.e., damage to business – of security incidents are the central objectives of IS (Solms and van Niekerk, 2013). According to Solms (2001), IS represents an elementary part of corporate governance, which comprises processes and structures that enable those in power to control and direct an organization (Abdullah and Valentine, 2009). Accordingly, IS governance is a system that directs and controls an organization's IS activities (International Organization for Standardization, 2018a). While IS governance was initially seen as a reactive technical activity to fulfil certain (governmental) requirements (Carcary et al., 2016), the ongoing digitalization of business models and processes led to a change in IS threats and, thus, to a shift in IS governance (Carcary et al., 2016; Hedström et al., 2011). Today, IS governance takes a more holistic and proactive view, including the identification, communication, and preservation of ISPs that are relevant for organizations' business environments and objectives (Carcary et al., 2016; Ma and Ratnasingam, 2008).

So far, authors have used different designations when approaching ISPs (Cherdantseva and Hilton, 2013), e.g., IS objectives (Mukundan and Sai, 2014; National Institute of Standards and Technology, 2013; Wang et al., 2010), IS properties (Dubois et al., 2010; Lundgren and Möller, 2017; International Organization for Standardization, 2018b, 2018a; Alvarez et al., 2016), and IS requirement (D'Arcy et al., 2014; Gerber et al., 2001; Gao and Zhong, 2015). These designations are rarely defined (International Organization for Standardization, 2018a; Singh et al., 2018; Kozlovs et al., 2016; Otero et al., 2010), but those definitions that have been provided are rather congruent (Beckers et al., 2012; Dubois et al., 2010; Fabian et al., 2010). We present an overview of the identified designations in Section 4. In line with Dubois et al. (2010), the International Organization for Standardization (2018b), and Lundgren and Möller (2017), in this paper we use the term ISP as this is the term most commonly used in academia.

In general, ISPs define a baseline for effective IS management (International Organization for Standardization, 2018b; Firesmith, 2005) by ensuring "reasonable protection of the organization's assets" (Dubois et al., 2010, p. 5). According to Gao and Zhong (2015), ISPs should help to protect information assets and associated information systems. Since ISPs can be relatively vague, they need to be subdivided into increasingly specific requirements (Fabian et al., 2010), such that they provide every employee with unambiguous instructions for action (D'Arcy et al., 2014; Firesmith, 2005; Elberzhager et al., 2009). In our research, we follow Dubois et al. (2010) and Fabian et al. (2010), who define ISPs as criteria or constraints that describe the security needs of business assets in a comprehensible manner.

2.2 Existing Concepts relating to Information Security Properties

Although the importance of ISPs is indisputable, the scope of relevant ISPs is not commonly defined. For instance, researchers assign different ISPs to IS governance, and even widely used concepts, such as the CIA Triad (Lundgren and Möller, 2017), are approached from markedly different angles in the literature (Moghaddasi et al., 2016; Mosenia and Jha, 2016; Solms and van Niekerk, 2013). For instance, Moghaddasi et al. (2016) include 15 different ISPs in their paper, whereas others only mention the CIA Triad (Agarwal and Agarwal, 2011; Cardenas et al., 2008). Such differences are rooted in divergent definitions of ISPs and different underlying IS concepts.

The CIA Triad consists of the ISPs: *confidentiality*, *integrity*, and *availability* (Moghaddasi et al., 2016). Many research papers criticize the CIA Triad for being insufficiently detailed (Arhin and Wiredu, 2018; Cherdantseva and Hilton, 2013). Hence, alternative IS concepts that seek to expand the CIA Triad have emerged. The Parkerian Hexad expands the CIA Triad by adding *authenticity*, *possession*, and *utility* (Moghaddasi et al., 2016; Sattarova Feruza and Kim, 2007). The Five Pillars of Information Assurance Model expands the CIA Triad by adding *authenticity* and *non-repudiation* (Moghaddasi et al., 2016). The Pentagon of Trust Model expands the CIA Triad by adding *authenticity* (Moghaddasi et al., 2016). A*uthenticity* plays a major role in alternative concepts. However, the violation of *authenticity* only causes financial damage when either *confidentiality*, *integrity*, or *availability* have, subsequently, been tampered with (Agarwal and Agarwal, 2011). In contrast to the alternative concepts, a violation of the CIA Triad (depending on the concrete definition of *confidentiality*, *integrity*, and *availability*) leads directly to financial damage. As the consequences are reflected in at least one of the three ISPs, the CIA Triad covers the majority of all IS incidents. Hence, we use the CIA Triad as a foundation to structure the various ISPs.

3 Research Methodology

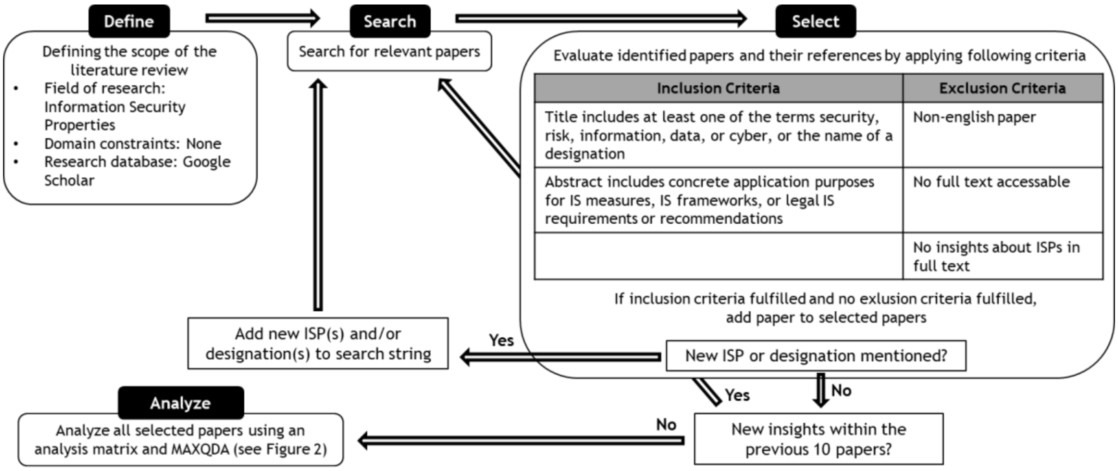
The extensive and diverse literature in the field of information security properties is dispersed across various literature streams, e.g., computer science and information security. The lack of a structured description of the security needs of business assets may discourage information systems researchers from integrating ISPs into their research. To synthesize the existing definitions of and interrelations between ISPs, we conduct a structured literature review following Webster and Watson (2002) and provide a conceptual model to summarize our findings. Our objective is to provide an initial overview of existing ISPs and their interrelations. Since the field of ISPs is very broad, an analysis of all potentially relevant papers is impractical. When searching through Google Scholar, the search term “security properties” leads to more than 93,000 results, and there exist many synonyms for this term, as shown in Figure 3. Hence, our use of the following recursive methodology does not mean that our analysis is complete but that it includes the most common ISPs.

Following Vom Brocke et al. (2009), we use Google Scholar as a search engine as it provides a comprehensive selection of research papers, e.g., journal publications, monographs, and conference proceedings from various disciplines (Vom Brocke et al., 2009). Following the idea of an iteratively expanding search string, proposed by Jia and Liu (2018), we include all ISPs and designations, i.e., synonyms for the term ISP, which we identify during numerous iterations of literature research. In line with Rowe (2014), we choose this rarely-applied approach to develop a clear and comprehensive search string in this highly diverse and broad research area, which helps us to provide a theoretical overview of the existing literature. As a starting point, we build upon insights from Vuorinen and Tetri (2012), who wrote the only research paper dealing with ISPs that features in the esteemed Senior Scholars’ Basket of Journals (College of Senior Scholars, 2011).

Like Vuorinen and Tetri (2012), we include *availability*, *confidentiality*, and *integrity* (which together form the CIA triad) and the designation “security concepts” in our initial search string. Vuorinen and Tetri (2012) also mention secrecy and accessibility, but as they do not explicitly refer to these as ISPs, we refrain from including them in our initial search string:

(Confidentiality OR Integrity OR Availability) AND (“Security Concepts”)

In the following, we screen the papers in the sequence provided by Google Scholar. The whole process of our literature review, as well as underlying inclusion and exclusion criteria, is shown in Figure 1.


Define
Defining the scope of the literature review
• Field of research: Information Security Properties
• Domain constraints: None
• Research database: Google Scholar
Search
Search for relevant papers
Select
Evaluate identified papers and their references by applying following criteria
If inclusion criteria fulfilled and no exlusion criteria fulfilled, add paper to selected papers
New ISP or designation mentioned?
Yes
Add new ISP(s) and/or designation(s) to search string
Yes
No
New insights within the previous 10 papers?
No
Analyze
Analyze all selected papers using an analysis matrix and MAXQDA (see Figure 2)

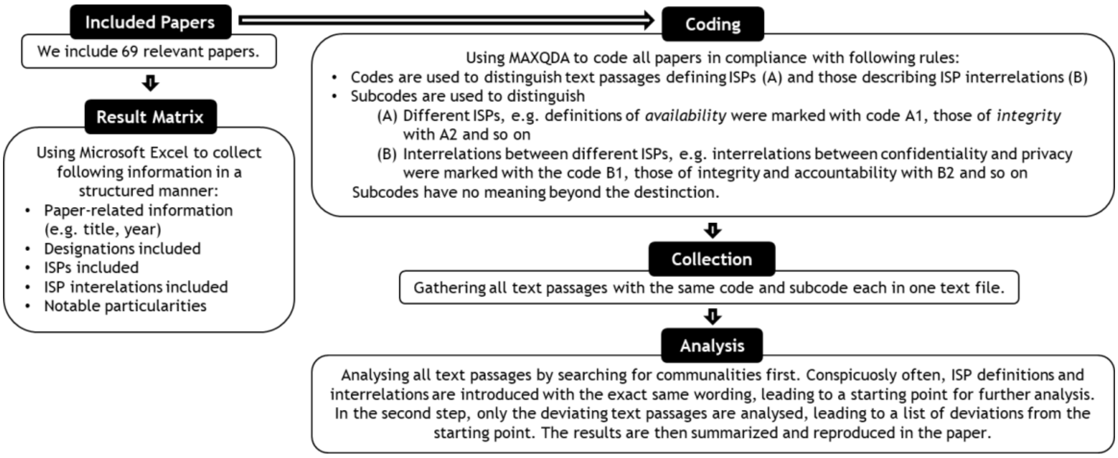
Inclusion Criteria	Exclusion Criteria
Title includes at least one of the terms security, risk, information, data, or cyber, or the name of a designation	Non-english paper
Abstract includes concrete application purposes for IS measures, IS frameworks, or legal IS requirements or recommendations	No full text accessable
	No insights about ISPs in full text

Figure 1. Research Methodology

To ensure our review is sufficiently thorough, we screen the references of relevant papers for additional literature, as proposed by Weaver and Fasel (2018). Thereby, we identify standards and laws, e.g., from the International Organization for Standardization (2018a) and the United States Government (2011), that provide relevant insights for our research but would not have been found within a research database. We proceed through the results until we identify, within the relevant papers, ISPs or designations that we have not already considered within our search string. In this case, we enhance our search string by adding the new ISPs or designations. For all iterations, we combine the ISPs and designations as follows: (ISP 1 OR ISP 2 OR … OR ISP n) AND (designation 1 OR designation 2 OR … OR designation k). We iteratively repeat this procedure until we reach saturation, which means that additional results might not provide new or noteworthy insights (Christiansen, 2011). Following Christiansen (2011) and Wolfswinkel et al. (2013), we define saturation as the threshold whereafter additional results do not provide further designations, ISPs, or interrelations between ISPs. When ten successive papers classified as relevant do not provide additional insights regarding ISPs or their interrelations, we define our review as saturated. Finally, our search string comprises 32 ISPs and 16 designations (for details see Figure 3 in Section 4). Owing to its increasing length, the search string becomes unmanageable for the search engine. Hence, we divide the search string multiple times and run combinatorial searches, i.e., 16 search runs, each consisting of four ISPs and eight designations in all possible combinations, resulting in more than 300,000 results (without the clean-up of duplicates). To avoid a premature termination of the combinatorial search, we extend our saturation rule, so our review is only saturated when ten successive papers per search run, classified as relevant, do not provide additional insights regarding ISPs or their interrelations.

As we aim to incorporate all literature that offers relevant insights into ISPs, we include empirical as well as conceptual papers. We not only consider peer-reviewed papers but papers that fulfil either scientific standards or form part of international security standards and laws. In total, our research strategy led us to 69 relevant papers published between 1994 and 2020, which we consider for further analysis. To provide transparency, we mark these documents with a * within our references.

To structure insights from the relevant documents, we first use an analysis matrix. In addition to document-related information (e.g., title), our matrix encompasses four sections: designations, ISPs, mentioned interrelations, and notable particularities of the analysed papers, e.g., outliers in terms of ISP definitions. For the latter, we follow Castleberry and Nolen (2018), who guide the analysis of qualitative research data, to disassemble and reassemble the definitions of the different ISPs by highlighting similarities using the coding software MAXQDA. We summarize the process in Figure 2.



Included Papers

We include 69 relevant papers.

Result Matrix

Using Microsoft Excel to collect following information in a structured manner:
- Paper-related information (e.g. title, year)
- Designations included
- ISPs included
- ISP interelations included
- Notable particularities

Coding

Using MAXQDA to code all papers in compliance with following rules:
- Codes are used to distinguish text passages defining ISPs (A) and those describing ISP interrelations (B)
- Subcodes are used to distinguish
  - (A) Different ISPs, e.g. definitions of *availability* were marked with code A1, those of *integrity* with A2 and so on
  - (B) Interrelations between different ISPs, e.g. interrelations between confidentiality and privacy were marked with the code B1, those of integrity and accountability with B2 and so on

Subcodes have no meaning beyond the destinction.

Collection

Gathering all text passages with the same code and subcode each in one text file.

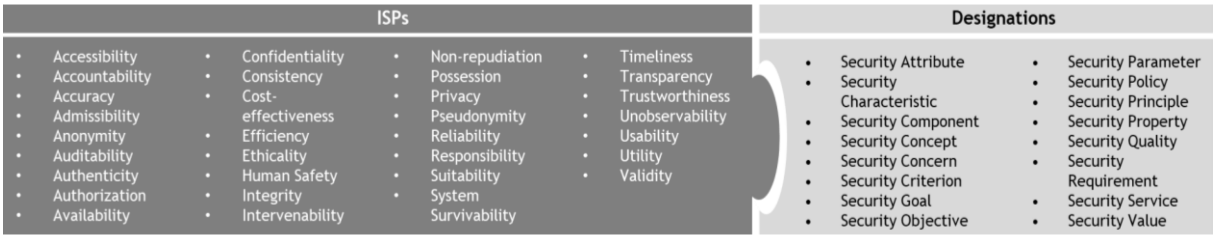
Analysis

Analysing all text passages by searching for communalities first. Conspicuosly often, ISP definitions and interrelations are introduced with the exact same wording, leading to a starting point for further analysis. In the second step, only the deviating text passages are analysed, leading to a list of deviations from the starting point. The results are then summarized and reproduced in the paper.

Figure 2. Analysis Process

4 ISPs and their interrelations

As a first insight, we present the designations and ISPs we identified in our literature review (Figure 3). As the core of our research, we outline both the definitions of all identified ISPs (Table 1) and the identified interrelations between the ISPs (Figure 4). Within the sample of ISPs, we placed a particular focus on the discussion of divergent definitions of confidentiality, integrity, and availability, since we provide the interrelations based upon our understanding of the CIA Triad.



ISPs

- Accessibility
- Accountability
- Accuracy
- Admissibility
- Anonymity
- Auditability
- Authenticity
- Authorization
- Availability
- Confidentiality
- Consistency
- Cost-effectiveness
- Efficiency
- Ethicality
- Human Safety
- Integrity
- Intervenability
- Non-repudiation
- Possession
- Privacy
- Pseudonymity
- Reliability
- Responsibility
- Suitability
- System Survivability
- Timeliness
- Transparency
- Trustworthiness
- Unobservability
- Usability
- Utility
- Validity

Designations

- Security Attribute
- Security Characteristic
- Security Component
- Security Concept
- Security Concern
- Security Criterion
- Security Goal
- Security Objective
- Security Parameter
- Security Policy
- Security Principle
- Security Property
- Security Quality
- Security Requirement
- Security Service
- Security Value

Figure 3. ISPs and Designations

4.1 The CIA Triad

Confidentiality

According to International Organization for Standardization (2018a), *confidentiality* describes the "property that information is not made available or disclosed to unauthorized individuals, entities or processes" (International Organization for Standardization, 2018a), p. 2). Even though this definition is widely accepted in academia (Ma and Ratnasingam, 2008; Eckert, 2009), there are definitions that either disagree with, or provide more specific information about, the kind of asset to be protected (Independent Data Protection Authorities, 2016; Agarwal and Agarwal, 2011; National Institute of Standards and Technology, 2013), the entities from whom the assets must be protected (Mukundan and Sai, 2014; Firesmith, 2005; Sattarova Feruza and Kim, 2007; Whitman and Mattord, 2011), or the way a breach of *confidentiality* is caused (Independent Data Protection Authorities, 2016; National Institute of Standards and Technology, 2013; Sattarova Feruza and Kim, 2007; Agarwal and Agarwal, 2011; United States Government, 2011). The Independent Data Protection Authorities (2016) only consider personal data in their definition, whereas others include all kinds of proprietary information (Agarwal and Agarwal, 2011; National Institute of Standards and Technology, 2013). Since the value of information depends on the context of the application, we refrain from any further delimitation and follow, inter alia, Antoniou (2018), Gerber et al. (2001), Singh et al. (2018), and Williams (2001) who define information in a general way. Concerning the question from whom information must be protected, various researchers only consider people as potential intruders (Arhin and Wiredu, 2018; Cardenas et al., 2008; Yu and Wen, 2010), whereas others also consider processes (Dubois et al., 2010; Fabian et al., 2010), systems (Firesmith, 2005; Zissis and Lekkas, 2012), agents (Vuorinen and Tetri, 2012), or (more general) entities (Lopes and Oliveira, 2014; Dubois et al., 2010; Gerber et al., 2001). To ensure the definition is universally valid, we consider all kinds of entities. Definitions also differ in the way a breach of *confidentiality* is caused. Neumann (1994) emphasizes that information must be protected from unintended disclosure. According to the Independent Data Protection Authorities (2016), the National Institute of Standards and Technology (2013), and Sattarova Feruza and Kim (2007), *confidentiality* demands that no unauthorized entity is allowed to tamper with information. However, access to proprietary information on the part of an unintended entity only causes harm if the entity misuses the information for its own purposes or transfers it to additional entities. Therefore, we incorporate the disclosure and misuse of leaked information into the definition of *confidentiality* (Agarwal and Agarwal, 2011; Yu and Wen, 2010; United States Government, 2011).To keep the definition universally valid and maintain the assumption that a breach of *confidentiality* has a direct negative impact, we define *confidentiality* as the protection of proprietary information from unauthorized disclosure or misuse.

Integrity

In academia, *Integrity* is the least uniformly defined ISP. Firesmith (2005) defines *integrity* as the authorization of identified and authenticated people, applications, and systems to create, modify, and delete assets. The National Institute of Standards and Technology (2006) understands a violation of *integrity* as improper asset modification or destruction. Whitman and Mattord (2011) state that *integrity* is preserved when all assets are whole, complete, and uncorrupted. Some researchers define *integrity* merely by referring to requirements, such as accuracy (Dubois et al., 2010; International Organization for Standardization, 2018a), completeness (Fabian et al., 2010; Lundgren and Möller, 2017), wholeness (Ma and Ratnasingam, 2008), or soundness (Ma and Ratnasingam, 2008). Even though these definitions seem very heterogeneous, most researchers agree that maintaining *integrity* protects assets from unauthorized modification (Arhin and Wiredu, 2018; Firesmith, 2005; Zissis and Lekkas, 2012; Neumann, 1994). However, definitions deviate in terms of the assets considered and how *integrity* is violated. Literature differentiates between system and data *integrity* (Neumann, 1994; Zissis and Lekkas, 2012; Stallings et al., 2012). System *integrity* means that a system and its data are maintained in a correct and consistent condition (Stallings et al., 2012; Neumann, 1994). Thus, data *integrity* is a subcomponent of system *integrity* (Zissis and Lekkas, 2012; Neumann, 1994). To be more holistic, we define *integrity* as system *integrity*. According to Dhingra (2016) and Sattarova Feruza and Kim (2007), the modification of data is enough to cause a violation of *integrity*. However, the unauthorized modification of backup data only causes harm when the *availability* or *integrity* of the primary system is also violated. Hence, other researchers state that *integrity* is preserved when systems comply with the determined specifications and work as intended (Stallings et al., 2012; Independent Data Protection Authorities, 2016). To keep the definition universally valid and maintain the assumption that a breach of *integrity* has a direct negative impact, we define *integrity* as the guarantee that all assets are functioning correctly and as intended.

Availability

According to the International Organization for Standardization (2018a), *availability* is the "property of being accessible and usable on demand by an authorized entity" (International Organization for Standardization, 2018a), p. 2). Even though this definition is widespread in academia (Dubois et al., 2010; Fabian et al., 2010), there are definitions that either deviate from this or provide more specific information concerning the actions covered by a breach of *availability* (Mukundan and Sai, 2014; Firesmith, 2005) and how a breach of *availability* can be caused (Qadir and Quadri, 2016; Agarwal and Agarwal, 2011; Kumar et al., 2018; National Institute of Standards and Technology, 2013; Whitman and Mattord, 2011). Mukundan and Sai (2014) and Sattarova Feruza and Kim (2007) state that systems must be able to access and use resources, whereas Agarwal and Agarwal (2011) and Dhingra (2016) relate the definition of *availability* to users. Singh et al. (2018) extend the definition by including devices. In line with most researchers (Gerber et al., 2001; International Organization for Standardization, 2018b; Moghaddasi et al., 2016; Zissis and Lekkas, 2012), our definition is less precise, referring to authorized entities. Some definitions are merely limited to the *availability* of data (Kozlovs et al., 2016; Brotby, 2007), files (Vuorinen and Tetri, 2012), services (Mosenia and Jha, 2016; Wang et al., 2010), or systems (Casoni and Paganelli, 2011; Antoniou, 2018), but the majority of researchers name either several different resources (Zissis and Lekkas, 2012; Dhillon and Backhouse, 2000; Sattarova Feruza and Kim, 2007) or no concrete resource at all (Lundgren and Möller, 2017; Dubois et al., 2010; International Organization for Standardization, 2018a). Since there is no consistent definition, we follow Neumann (1994) in relating *availability* to all kinds of resources. Nearly all definitions agree that *availability* requires an authorized entity to be able to access and use resources. Furthermore, some definitions also demand access be granted in a timely and prompt manner (Casoni and Paganelli, 2011; Kozlovs et al., 2016; Yu and Wen, 2010). Literature also provides an extensive list of additional, very precise requirements concerning access. The access must be granted in an uninterrupted (Agarwal and Agarwal, 2011) and adequate way (Independent Data Protection Authorities, 2016), the communication channels used for access must be functioning correctly (Sattarova Feruza and Kim, 2007), and accessed data must be formatted correctly (Whitman and Mattord, 2011). According to Brotby (2007) and Williams (2001), systems must also be able to resist attacks and recover from failures. To ensure the definition is universally valid and maintain the assumption that a breach of availability has a direct negative effect, we define *availability* as the property of resources to be accessible and usable for all authorized entities in a timely and reliable manner.

4.2 Overview of ISPs

In the following, we discuss all of the other ISPs that we have identified in the existing literature. We recognized that there is a general difference between properties that contribute to IS – e.g., *anonymity* – and properties that describe the manner in which IS should be fulfilled – e.g., *cost-effectiveness*. In the remainder of this paper, we distinguish between these properties and ISPs and refer to the former as meta-characteristics. ISPs and meta-characteristics are not distinguished in the extant literature, yet, we define meta-characteristics as properties of, or related to, ISPs, which do not address a security need but should be considered in the protection of ISPs.

Table 1 provides an overview of all ISPs and meta-characteristics identified in our literature review. We aim to provide a common and consistent understanding of ISPs, and so propose a definition for each

ISP that we identify. In line with our discussion of the CIA Triad, our goal is to provide a general and universally valid definition that can be used in IS-related contexts. As with our definitions of *confidentiality* and *availability,* we do not restrict an ISP to a specific entity – e.g., users, systems, processes, or devices – unless there is an explicit requirement to do so. Consistent with our definition of *availability,* we do not limit the preservation of an ISP to data but also involve other resources – e.g., services or systems – whenever meaningful. Consistent with our definition of *confidentiality,* we consider the unauthorized use of information as well as unauthorized disclosure. In cases where a definition provided in the literature already meets our requirements, we use this definition. For confidentiality, integrity, and availability – i.e., the CIA Triad – we use the previously discussed definitions from Section 4.1. When we find different definitions in the reviewed papers, we discuss the differences and outline how we merge these definitions to provide one that is consistent with the description above. When there is only one definition, we do not discuss the definition in detail. In these cases, we follow the definition provided but adapt it to meet our goal of providing a general and universally valid definition. When no definition is provided, we discuss how we determine a definition. We outline the discussion in alphabetic order and distinguish between ISPs and meta-characteristics, i.e., we first provide the ISPs and then the meta-characteristics. In Table 1, we provide references for all definitions of ISPs and meta-characteristics except for *accountability, authenticity, availability, confidentiality, integrity,* and *possession* due to their incongruent definitions in the literature, which we discuss in detail before introducing Table 1.

The reviewed literature provides no concrete definition of *accessibility,* but Vuorinen and Tetri (2012) consider the terms to be synonymous with availability. Accordingly, we propose that *accessibility* means that resources can be accessed and used by all authorized entities in a timely and reliable manner.

Definitions of *accountability* are essentially consistent in the literature. They provide two different perspectives yet have the same aim. In some cases, it is defined as the property of a system to hold entities responsible for their actions (Casoni and Paganelli, 2011; Cherdantseva and Hilton, 2013; Mosenia and Jha, 2016). In others, it requires that all actions from an entity can be traced uniquely to that entity (Gerber et al., 2001; Mukundan and Sai, 2014; Stallings et al., 2012). Thus, we define *accountability* as the property of a system to trace the actions of an entity and hold it uniquely responsible for its actions.

The Independent Data Protection Authorities (2016) define *accuracy* as "sufficient congruency between the legal-normative requirement and common practice, both in terms of technical detail as well as in the broad context of the procedure and its overall purpose" (Independent Data Protection Authorities, 2016, p. 12). Elsewhere, Whitman and Mattord (2011) propose that *accuracy* is ensured when "data is free of errors and has the value that the user expects" (Whitman and Mattord, 2011, p.14). We follow Whitman and Mattord (2011) but replace "users" with "affected entities" to provide a more general definition.

The definitions of *authenticity* differ in two key respects. Firstly, they differ as to who or what must be authentic. Some claim that it is only data or information that must be authentic (Independent Data Protection Authorities, 2016; Whitman and Mattord, 2011). Others focus exclusively on transactions (Antoniou, 2018; Williams, 2001) or persons (Kumar et al., 2018). In addition to data and transactions, Wang et al. (2010) include communications in their definition of authenticity. Gerber et al. (2001) and Moghaddasi et al. (2016) consider users, processes, systems, and information in their definition. To provide a universally valid definition, we suggest that entities must be authentic. The question of how *authenticity* is maintained is not answered consistently. One aspect is the ability to verify an entity's identity (Alvarez et al., 2016; Casoni and Paganelli, 2011; International Organization for Standardization, 2018b). Another is whether the entity can be trusted (Brotby, 2007; Williams, 2001) and is genuine or original (Wang et al., 2010; Whitman and Mattord, 2011). Moghaddasi et al. (2016) expand the requirements by demanding truth and correctness on the part of the entity. Some claim that the entity's origin must be unambiguously traceable (Independent Data Protection Authorities, 2016; Antoniou, 2018). Depending on which kind of entity the definition is based on, the requirements must be fulfilled by the entity (data, information, transactions, and persons) itself (Stallings et al., 2012; Wang et al., 2010), or demanded by it (systems) (Cherdantseva and Hilton, 2013; Casoni and Paganelli, 2011).

Having considered the available definitions, we define authenticity as the property of an entity to be correct and genuine, to have the ability to be trusted, to have a verifiable identity, and to demand the same from other entities as well.

For *authorization,* we identify two definitions that are, generally speaking, congruent. Casoni and Paganelli (2011) define *authorization* as the "granting of access rights to the resources of the system (or the network) to only specific users" (Casoni and Paganelli, 2011, p. 2147). As we aim to provide a more general definition, we follow Kumar et al. (2018) who define authorization as the "act of determining whether a user is allowed to perform an activity on data" (Kumar et al., 2018, p. 693), replacing "user" with "entity", and "data" with "resource".

While Mukundan and Sai (2014) claim that *reliability* primarily means consistent results and behaviour, other sources invoke the concept of intention (Gerber et al., 2001; International Organization for Standardization, 2018b; Moghaddasi et al., 2016). As both perspectives extend each other, we define *reliability* as consistency in the intended behaviour and results.

Researchers agree that *non-repudiation* requires a system to be able to prove the occurrence or non-occurrence of some type of event (Cherdantseva and Hilton, 2013). However, the types of events to be included are not consistently defined. Some authors only include transactions (Antoniou, 2018; Sattarova Feruza and Kim, 2007), messages (Casoni and Paganelli, 2011; Ma and Ratnasingam, 2008), or information (Brotby, 2007). Other, more general definitions simply include actions, without any further specification (Mosenia and Jha, 2016; Moghaddasi et al., 2016). To keep the definition as general as possible, we define *non-repudiation* as the property of a system to be able to prove the occurrence or non-occurrence of actions.

We identify two definitions of *possession* (Moghaddasi et al., 2016; Whitman and Mattord, 2011). Both focus on the ownership and control of information and how it is authorized or legitimated. We replace "information" with "resources" and hold *possession* to means that resources are under the control and ownership of authorized entities.

Existing definitions of *privacy* agree that individuals control their information (Stallings et al., 2012; Mosenia and Jha, 2016; Zissis and Lekkas, 2012). Cherdantseva and Hilton (2013) provide a general definition, while Zissis and Lekkas (2012) focus only on disclosure and Stallings et al. (2012) include the collection and storage of information. To provide a general definition that includes all necessary aspects, we define *privacy* as the guarantee that individuals can control the extent to which information related to them may be collected and stored, by whom this may be done and how it may be used or disclosed.

Since Lopes and Oliveira (2014) focus more on the consequences of *trustworthiness*, i.e., higher self-control and responsibility at the expense of external control and supervision, we follow Mosenia and Jha (2016) who define *trustworthiness* as the "ability of a system to verify identity and establish trust in a third party" (Mosenia and Jha, 2016, p. 590). To maintain the consistency of our approach, we replace "system" with the more general term of "entity".

Moghaddasi et al. (2016) and Whitman and Mattord (2011) agree that *utility* refers to the value and usefulness of information. As the definition by Moghaddasi et al. (2016) is more precise, we define *utility* as the usefulness of information.

ISPs	
Accessibility	Resources can be accessed and used by all authorized entities in a timely and reliable manner (Vuorinen and Tetri, 2012)
Accountability	Ability of systems to trace the actions of an entity and hold it uniquely responsible for its actions
Accuracy	Data is free of errors and has the value affected entities expect (Whitman and Mattord, 2011)
Admissibility	State in which the status of the data is acceptable or lawful (Moghaddasi et al., 2016)
Anonymity	Ability of an entity to not be identified or at least undistinguished among another group of entities, if required (Alvarez et al., 2016)
Auditability	Ability to conduct persistent, non-bypassable monitoring of all actions performed by entities within the system (Cherdantseva and Hilton, 2013)
Authenticity	Entities are correct and genuine, have the ability to be trusted, have a verifiable identity and demand the same from other entities as well

Authorization	Act of determining whether an entity is allowed to perform an activity on a resource (Kumar et al., 2018)
Availability	Resources can be accessed and used by all authorized entities in a timely and reliable manner
Confidentiality	Protection of proprietary information from unauthorized disclosure or misuse
Consistency	Entities do what they are expected to do (Whitman and Mattord, 2011)
Human Safety	Safety of anyone dependent on the satisfactory behaviour and proper use of resources (Neumann, 1994)
Integrity	Guarantee that all assets are functioning correctly and as intended
Intervenability	Data subjects are effectively granted their rights to notification, information, rectification, blocking and erasure at any time and the controller is obliged to implement appropriate measures (Independent Data Protection Authorities, 2016)
Non-Repudiation	The ability of a system to prove the occurrence or non-occurrence of actions (Mosenia and Jha, 2016)
Possession	Resources are under the control and ownership of authorized entities
Privacy	Guarantee that individuals can control the extent to which information related to them may be collected and stored, by whom this may be done and how it may be used or disclosed (Stallings et al., 2012)
Pseudonymity	Ability to use a resource without disclosing its entity identity, but can still be accountable for that use (Stallings et al., 2012)
Reliability	Consistency in the intended behaviour and results (Gerber et al., 2001; Moghaddasi et al., 2016)
Responsibility	Handling the development of events in the future in a particular sphere (Dhillon and Backhouse, 2000)
System Survivability	Ability to maintain resource availability despite adverse circumstances (Neumann, 1994)
Timeliness	Ensuring that necessary resources are available quickly enough when needed (Neumann, 1994)
Transparency	The ability of a data subject, system operators, and supervisory authorities to understand how data is collected and processed for which purpose, as well as who is legally responsible (Independent Data Protection Authorities, 2016)
Trustworthiness	The ability of an entity to verify identity and establish trust in a third party (Mosenia and Jha, 2016)
Unobservability	The ability of an entity to use a resource without others being able to observe that the resource is used (Stallings et al., 2012)
Validity	Information is up to date and has not been superseded by another (Alvarez et al., 2016)
Meta Characteristics	
Cost-Effectiveness/ Efficiency/	Optimal use of resources, with minimum losses (Moghaddasi et al., 2016)
Ethicality	Enhancement of responses from co-operators in informal, new, and dynamic situations (Lopes and Oliveira, 2014)
Suitability	The ability of specific resources to fulfil their respective purposes (Livshitz et al., 2016)
Usability	Engaging stakeholders in core business processes (Carcary et al., 2016)
Utility	The usefulness of information (Moghaddasi et al., 2016)

Table 1. Overview of ISPs and meta-characteristics

4.3 Interrelations between ISPs in connection with the CIA Triad

The existence of interrelations becomes apparent when we examine the definitions of *confidentiality*, *integrity*, and *availability* (see Section 4.1). For instance, some authors define *confidentiality* by referring to *privacy* (Kozlovs et al., 2016; Pattanavichai, 2018; Stallings et al., 2012), *integrity* by referring to *accuracy* (Dubois et al., 2010; Fabian et al., 2010; Lundgren and Möller, 2017), and *availability* by referring to *accessibility* (Arhin and Wiredu, 2018; Qadir and Quadri, 2016; Vuorinen and Tetri, 2012). Interrelations can be characterized by one ISP guaranteeing or supporting the preservation of another ISP. Supporting the preservation of an ISP means that neither the preservation of the supportive ISP guarantees the preservation of the supported ISP nor does the preservation of the supported ISP guarantee the preservation of the supportive ISP.

To help create a better understanding of ISPs and overcome the weaknesses of the granular CIA Triad, we highlight the manifold interrelations between relevant ISPs. We summarize our findings in Figure 2. The arrows visualize the relationships between the ISPs which we describe in the previous section. The dashed lines represent the context in which the necessity for the preservation of *confidentiality* and *integrity* depends on *availability* (Qadir and Quadri, 2016). If one ISP guarantees the preservation of another (as in the case of *possession* and *confidentiality*), we highlight this relationship using a light grey arrow. Some ISPs are mutually supportive of one another (*authenticity* and *transparency* (Independent Data Protection Authorities, 2016), and *availability* and *accessibility* (Vuorinen and Tetri, 2012)). The latter pairing are synonyms (Vuorinen and Tetri, 2012), which means that the preservation/violation of one ISP guarantees the preservation/violation of the other. In general, we focus on the interrelations that we identify in the existing literature. Thus, ISPs with no interrelations mentioned in the existing literature have been omitted from this section. There is, however, one exception: We did not find any interrelation for *validity* within the reviewed papers. Yet, by definition, *validity* supports integrity and does not represent a meta-characteristic. Thus, we integrate it into our model. Meta-characteristics are not interrelated with ISPs but describe how the ISPs should be fulfilled.

Accordingly, we do not include them in Figure 4. Below, we structure our insights in terms of the CIA Triad, i.e., *confidentiality*, *integrity*, and *availability*.

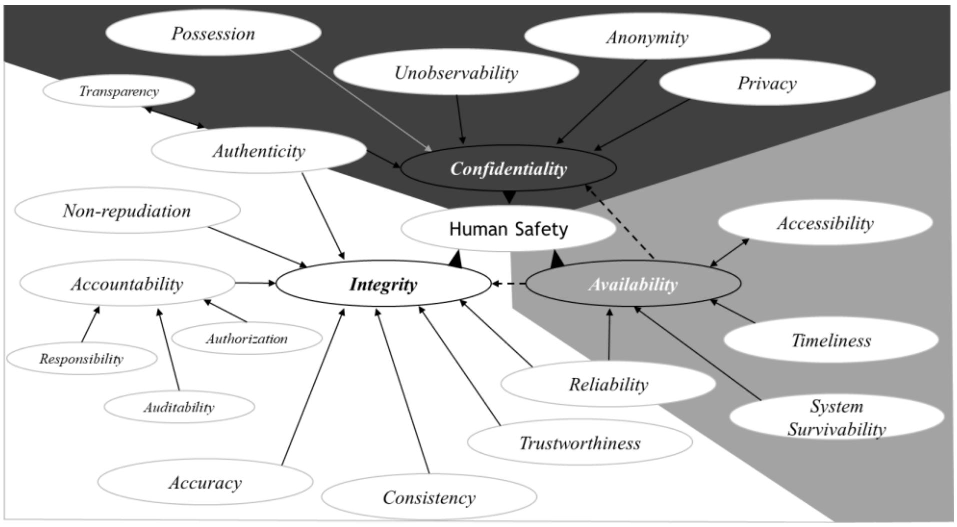


Figure 4. ISPs and their interrelations

Confidentiality

The ISP of *confidentiality* cannot be pursued without considering other, related ISPs, i.e. *possession* (Whitman and Mattord, 2011), *anonymity* (Fabian et al., 2010; Firesmith, 2005), *authenticity* (Fabian et al., 2010), *privacy* (Cherdantseva and Hilton, 2013; Kumar et al., 2018), *transparency* (Independent Data Protection Authorities, 2016), and *unobservability* (Fabian et al., 2010; Stallings et al., 2012). While the preservation of *possession* guarantees the preservation of *confidentiality*, the other ISPs merely support the preservation of *confidentiality*. *Possession* means that data assets are under the control of the respective entity (Moghaddasi et al., 2016). Logically, if entities do not possess data, there is nothing to misuse or disclose. A violation of *possession* does not automatically result in a violation of *confidentiality* (Whitman and Mattord, 2011), e.g., if attackers are not able to decrypt stolen data (Whitman and Mattord, 2011). However, a violation of *confidentiality* automatically includes the loss of *possession* (Whitman and Mattord, 2011). The need to preserve *confidentiality* is dependent on the ISP *availability*. If an asset is not available, there is no need to protect its *confidentiality* (Qadir and Quadri, 2016). *Human safety* is also related to the preservation of *confidentiality* (International Organization for Standardization, 2018a). *Human safety* means that all systems must work satisfactorily to ensure the well-being of individuals and groups of people (Neumann, 1994). Thus, *human safety* also depends on the *confidentiality*, *integrity*, and *availability* of information systems. Accordingly, the preservation of *confidentiality* is necessary, but not sufficient, to ensure *human safety* (Neumann, 1994).

Integrity

The ISP *integrity* cannot be pursued without considering other ISPs. There are eleven ISPs that support the preservation of *integrity*, i.e. *accountability* (Beckers et al., 2012; Fabian et al., 2010), *accuracy* (Kumar et al., 2018; Pattanavichai, 2018), *auditability* (Cherdantseva and Hilton, 2013; Gerber et al., 2001), *authenticity* (Fabian et al., 2010; Solms and van Niekerk, 2013), *authorization* (Casoni and Paganelli, 2011; Fabian et al., 2010), *consistency* (Kumar et al., 2018; Pattanavichai, 2018), *non-repudiation* (Fabian et al., 2010; Moghaddasi et al., 2016), *responsibility* (Dhillon and Backhouse, 2000; Fabian et al., 2010), *reliability* (Lundgren and Möller, 2017), *transparency* (Independent Data Protection Authorities, 2016), and *trustworthiness* (Kumar et al., 2018; Pattanavichai, 2018). The need to preserve *integrity* is also dependent on *availability*. If an asset is not available, there is no need to protect its *integrity* (Qadir and Quadri, 2016). As previously mentioned, *human safety* depends on the preservation of *integrity*, meaning that the preservation of *integrity* is necessary, but not sufficient, to ensure *human safety* (Neumann, 1994; International Organization for Standardization, 2018a).

Availability

Availability cannot be pursued without considering *accessibility* (Vuorinen and Tetri, 2012), *reliability* (Gerber et al., 2001), *system survivability* (Neumann, 1994), and *timeliness* (Kumar et al., 2018; Neumann, 1994). According to Vuorinen and Tetri, (2012), *availability* and *accessibility* are synonyms. Consequently, the preservation of *accessibility* guarantees the preservation of *availability*, and vice versa (Vuorinen and Tetri, 2012). The violation of *availability* also leads to the violation of *accessibility*, and vice versa (Vuorinen and Tetri, 2012). The other three ISPs – i.e., *reliability*, *system survivability*, and *timeliness* – support the preservation of *availability*. Like *confidentiality* and *integrity*, *availability* is necessary, but not sufficient, to ensure *human safety* (International Organization for Standardization, 2018a; Neumann, 1994).

5 Discussion & Future Research

Our results provide a foundation for further research on ISPs. As organizations continue to develop data-driven business models based on inter-organizational connectivity (Rüßmann et al., 2015), opportunities for cyber-attacks increase, as do the potential impacts on business (Brewster et al., 2015; Vaidya et al., 2018). Consequently, organizations need to rethink their IS governance strategies. ISPs may play a major role in defining and effective communication of IS strategies (Dubois et al., 2010). In particular, it is increasingly important that relevant objectives are clear and easy to understand, as digitalization affects not only information technology departments but whole organizations (Berger et al., 2020). To provide an efficient means of communication, future research should examine how organizations can raise awareness of the significance of ISPs and their complex interrelations beyond information technology departments.

To enable a comprehensive understanding of ISPs, we identify existing ISPs, consolidate their definitions, and outline relationships between specific ISPs and the CIA Triad. We recognize that certain proposed properties do not address a security need – e.g., *efficiency* – and, thus, do not represent an ISP. However, such properties have one common characteristic: They describe the manner in which IS should be fulfilled. For instance, ensuring the *efficiency* of IS activities is important for organizations, but does not specify what should be secured. This argument is also valid for *cost-effectiveness*, *ethicality*, *suitability*, *usability*, and *utility*. Thus, we call these meta-characteristics. This distinction between ISPs and meta-characteristics represents a major insight into how to different designations can be understood and used more thoughtfully in the future. Thus, we propose that future research draws on our insights, reworking existing approaches to distinguish between ISPs and meta-characteristics and provide a more consistent and holistic view.

In this study, we provide an initial overview of the interrelations between ISPs. As we consolidate existing literature, we identify existing interrelations, e.g., *confidentiality* is supported by *anonymity*. Most of these interrelations may seem obvious, in that they build logically upon one another. However, there are less obvious cases – e.g., the connection between *authenticity* and *transparency* – and the extent to which cited references examine the proposed relationship varies. In most cases, the interrelationships are mentioned but are not the focus of the research. Moreover, as we see in the case of *validity*, for which we do not find any relationships in the reviewed papers, we cannot be sure that the existing literature captures all interrelations. Therefore, to enhance our understanding of existing interrelations between different ISPs, we call for further research to validate the identified interrelations. While this study is theoretical in its approach, future research might switch perspective and discuss our findings with practitioners to examine potential misunderstandings between academia and practice. Future research should also gain further insights as to how organizations currently leverage ISPs to analyse risk scenarios, develop IS strategies, and how such organizations might use ISPs more effectively in the future.

Even though we help organizations to both identify relevant ISPs and consider their interrelations, our model does not deliver any insights on how to prioritize ISPs. The significance of ISPs depends on the business context, e.g., the affected data, the business model, the significance of the particular information system, and the organization's business environment and goals (Brotby, 2007; Ma and Ratnasingam, 2008; Williams, 2001). Historically, *availability* has been a high priority for operation technology in manufacturing companies (Sadeghi et al., 2015). On the contrary, *confidentiality* and *integrity* were particularly crucial for information technologies (Tom et al., 2008). The ongoing digitalization and connectivity within and beyond organizations – e.g., through cyber-physical systems – merge hitherto separate approaches (Murray et al., 2017). Until now, academia has lacked studies about the influence of organizational characteristics on the prioritization of ISPs. As CIOs need to prioritize ISPs for their business context, further research should address this issue. Case study research might help to analyse the connection between organizational characteristics – e.g., the business model, size, or popularity of organizations – and the prioritization of ISPs. Thereby, academia might gain insights on how to provide valuable directives for practitioners defining an appropriate IS strategy.

6 Theoretical Contribution and Practical Implications

Our conceptual model contributes to the descriptive knowledge of IS and holds several implications for practitioners. Firstly, our systematic review of ISPs eliminates current inconsistencies in definitions of ISPs and offers a structured description of business assets' security needs that may help information systems researchers to integrate ISPs into their research. Our findings build on current knowledge in the fields of IS governance and ISPs and extend existing frameworks as the CIA Triad. Thereby, we provide an overview of and common nomenclature for designations and definitions in the context of ISPs. Furthermore, we address the limitations of existing frameworks by structuring ISPs and identifying interrelations between ISPs. By highlighting interrelations, we find a difference between ISPs and meta-characteristics that has not previously been acknowledged. Overall, we create awareness of the significance of ISPs in the information system community to stimulate future research.

Our research provides relevant managerial implications for practitioners. In particular, these concern the prioritization of ISPs and their interrelations within the IS strategy. This, in turn, enables the evaluation of an organization's current IS strategy and, subsequently, the derivation of an action roadmap and the definition of individual projects that contribute to the IS objectives. Our model supports managers in the selection and prioritization of IS projects and increases the transparency of associated decisions. Thereby, it may help to reduce the cost of establishing an IS strategy as it aligns the various stakeholders.

As with any research project, our conceptual model is subject to limitations that may stimulate future research. Firstly, due to our search string and our saturation threshold, we may have excluded papers that could generate additional insights. As we screened a huge number of papers, a narrower approach that builds on a set of high-quality journals may enhance the reliability of the research results. Thus, in contrast to our explorative approach, an exploitative approach with a more restricted search string in a scientific database or another research methodology – e.g., a Delphi study – represent promising next steps to validify and enhance our insights. Further, even though we had good reasons to build our analysis on the CIA Triad, building on alternative concepts or integrating different perspectives might lead to different insights. Thus, further research should examine ISPs and ongoing digitalization, and evaluate whether the concept of the CIA Triad as core properties is still valid for all areas of application.

7 Conclusion

As finances and time are restricted, organizations need to identify and prioritize relevant security measures for their business contexts. ISPs are a suitable way of communicating security objectives. Even though the use of ISPs as a concept is widespread and their coarse granular character enables interdisciplinary communication across different hierarchical levels, widely diverging definitions limit the effectiveness of ISPs. To resolve this issue, we conduct a comprehensive literature review following Webster and Watson (2002) and synthesize the existing knowledge. Finally, we develop a conceptual model that includes 25 ISPs and 6 meta-characteristics, as well as their interrelations.

8 References

Abdullah, H. and B. Valentine (2009). "Fundamental and Ethics Theories of Corporate Governance." *Middle Eastern Finance and Economics* 4 (4), 88–96.

Agarwal, A. and A. Agarwal (2011). "The Security Risks Associated With Cloud Computing." *International Journal of Computer Applications in Engineering Sciences* 1, 257–259. *

AlKalbani, A., H. Deng and B. Kam (2015). "Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure." In: *PACIS 2015 Proceedings.* Singapore. *

Alvarez, F., M. Hollick and P. Gardner-Stephen (2016). "Maintaining Both Availability and Integrity of Communications: Challenges and Guidelines for Data Security and Privacy During Disasters and Crises." In: Proceedings of the *2016 IEEE Global Humanitarian Technology Conference (GHTC).*Seattle, Washington, USA. *

Antoniou, G. S. (2018). "A Framework for the Governance of Information Security: Can it be Used in an Organization." In: *SoutheastCon 2018*, pp. 1–30. Ketchikan, Alaska, USA. *

Arhin, K. and G. O. Wiredu (2018). "An Organizational Communication Approach to Information Security." *The African Journal of Information Systems* 10 (4), 1. *

Beckers, K., S. Faßbender, M. Heisel and H. Schmidt (2012). "Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation." In: *2012 Seventh International Conference on Availability, Reliability and Security.* Prague, Czech Republic. *

Berger, S., M. Bitzer, B. Häckel and C. Voit (2020). "Approaching Digital Transformation - Development of a Multi-Dimensional Maturity Model." In: *Proceedings of the 28th European Conference on Information Systems (ECIS).* Marrakech, Morocco.

Brewster, B., B. Kemp, S. Galehbakhtiari and B. Akhgar (2015). "Cybercrime: Attack Motivations and Implications for Big Data and National Security.". In *Application of Big Data for National Security*, pp. 108–127: Elsevier.

Brinz, N., C. Regal, M. Schmidt and J. Töppel (2018). "Reducing the Pain of the Inevitable: Assisting IT Project Managers in Performing Risk Management." In: *Proceedings of the 39th International Conference on Information Systems.* San Francisco: California. *

Brotby, W. K. (2007). *Information Security Governance*. *Guidance for Information Security Managers.* Rolling Meadows: Information Systems Audit and Control Association. *

Carcary, M., K. Renaud, S. McLaughlin and C. O'Brien (2016). "A Framework for Information Security Governance and Management." *IT Professional* 18 (2), 22–30. *

Cardenas, A. A., S. Amin and S. Sastry (2008). "Secure Control: Towards Survivable Cyber-Physical Systems." In: *2008 The 28th International Conference on Distributed Computing Systems Workshops*. Beijing, China. *

Casoni, M. and A. Paganelli (2011). "Security Issues in Emergency Networks." In: *2011 7th International Wireless Communications and Mobile Computing Conference*, pp. 2145–2150. *

Castleberry, A. and A. Nolen (2018). "Thematic Analysis of Qualitative Research Data: Is It as Easy as It Sounds?" *Currents in Pharmacy Teaching and Learning* 10 (6), 807–815.

Cherdantseva, Y. and J. Hilton (2013). "A Reference Model of Information Assurance & Security." In: *2013 International Conference on Availability, Reliability and Security*, pp. 546–555. *

Christiansen, Ó. (2011). "The Literature Review in Classic Grounded Theory Studies: A Methodological Note." *The Grounded Theory Review* 10 (3), 21–25.

College of Senior Scholars (2011). *Senior Scholars' Basket of Journals*. URL: https://aisnet.org/page/SeniorScholarBasket (visited on 05/17/2019).

Correia, A., A. Gonçalves and M. F. Teodoro (2017). "A model-driven approach to information security compliance." In: *AIP Conference Proceedings*. Puertollano, Spain. *

D'Arcy, J., T. Herath and M. K. Shoss (2014). "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective." *Journal of Management Information Systems* 31 (2), 285–318. *

de Oliveira Alves, Gustavo Alberto, da Costa Carmo, Luiz Fernando Rust and de Almeida, Ana Cristina Ribeiro Dutra (2006). “Enterprise Security Governance: A Practical Guide to Implement and Control Information Security Governance (ISG).” In: *2006 IEEE/IFIP Business Driven IT Management*, pp. 71–80. *

Dhillon, G. and J. Backhouse (2000). “Information System Security Management in the New Millennium.” *Commun. ACM* 43 (7), 125–128. *

Dhingra, M. (2016). “Review on Information Security Management.” In: *International Conference on Futuristic Trends in Engineering, Science, Humanities, and Technolog*, pp. 1–4. *

Dong, N., J. Zhao, L. Yuan and Y. Kong (2018). “Research on Information Security System of Smart City Based on Information Security Requirements.” *Journal of Physics: Conference Series* 1069, 12040. *

Dubois, É., P. Heymans, N. Mayer and R. Matulevičius (2010). “A Systematic Approach to Define the Domain of Information System Security Risk Management.”. In *Intentional Perspectives on Information Systems Engineering*, pp. 289–306: Springer. *

Eckert, C. (2009). *IT-Security. Concepts - Approaches - Protocoles (in German).* 5., überarb. Aufl. München: Oldenbourg Wissenschaftsverlag.

Elberzhager, F., A. Klaus and M. Jawurek (2009). “Software Inspections Using Guided Checklists to Ensure Security Goals.” In: *Proceedings of the International Conference on Availability, Reliability and Security, 2009*. Fukuoka, Japan. *

Fabian, B., S. Gürses, M. Heisel, T. Santen and H. Schmidt (2010). “A Comparison of Security Requirements Engineering Methods.” *Requirements Engineering* 15 (1), 7–40. *

Firesmith, D. G. (2005). “A Taxonomy of Security-related Requirements.” In: *International Workshop on High Assurance Systems (RHAS’05)*, pp. 29–30. *

Gao, X. and W. Zhong (2015). “Information Security Investment for Competitive Firms with Hacker Behavior and Security Requirements.” *Annals of Operations Research* 235 (1), 277–300. *

Gerber, M., R. von Solms and P. Overbeek (2001). “Formalizing Information Security Requirements.” *Information Management & Computer Security* 9 (1), 32–37. *

Hedström, K., E. Kolkowska, F. Karlsson and J. P. Allen (2011). “Value Conflicts for Information Security Management.” *The Journal of Strategic Information Systems* 20 (4), 373–384. *

Hohan, A. I., M. Olaru and I. C. Pirnea (2015). “Assessment and Continuous Improvement of Information Security based on TQM and Business Excellence Principles.” *Procedia Economics and Finance* 32, 352–359.

Huang, C. D., R. S. Behara and J. Goo (2014). “Optimal information security investment in a Healthcare Information Exchange: An economic analysis” *Decision Support Systems* 61, 1–11.

Independent Data Protection Authorities (2016). *The Standard Data Protection Model. A Concept for Inspection and Consultation on the Basis of Unified Protection Goals*. URL: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf (visited on 12/04/2019). *

International Organization for Standardization (ISO) (2018a). *ISO/IEC 27000: Information Technology - Security Techniques - Information Security Management Systems - Overview and Vocabulary*. *

International Organization for Standardization (ISO) (2018b). *ISO/IEC 27005: Information Technology - Security Techniques - Information Security Risk Management* 35.030 IT Security. *

Ismail, S., E. Sitnikova and J. Slay (2015). “Studying SCADA Organisations Information Security Goals: An Integrated System Theory Approach.” In: *PACIS 2015 Proceedings*, p. 77. Singapore. *

Jia, J. and X. Liu (2018). “Improving Systematic Literature Review Based on Text Similarity Analysis.” In: *Journal of Physics: Conference Series*, pp. 10–1088.

Kagermann, H. (2015). “Change Through Digitization—Value Creation in the Age of Industry 4.0.”. In Albach, H., Meffert, H., Pinkwart, A., Reichwald, R. (ed.) *Management of Permanent Change*, pp. 23–45: Springer.

Kappelman, L., V. Johnson, C. Maurer, K. Guerra, E. McLean, R. Torres, M. Snyder and K. Kim (2020). “The 2019 SIM IT Issues and Trends Study.” *MIS Quarterly Executive* 19 (1).

Khajouei, H., M. Kazemi and S. H. Moosavirad (2017). “Ranking information security controls by using fuzzy analytic hierarchy process.” *Information Systems and e-Business Management* 15 (1), 1–19. *

Khan, A. and M. P. Sebastian (2018). *Understanding the Human, Managerial and Organizational Aspects of Information Security Management: A Literature Review*. URL: https://www.iimk.ac.in/websiteadmin/FacultyPublications/Working%20Papers/2131IIMKWPS225ITS201801sebastian%20mp2.pdf (visited on 11/17/2020). *

Khidzir, N. Z., A. R. Ismail, K. A. M. Daud, M. S. Afendi, A. Ghani and M. A. H. Ibrahim (2016). "Critical Cybersecurity Risk Factors in Digital Social Media: Analysis of Information Security Requirements." *Lecture Notes on Information Theory Vol* 4 (1). *

Kozlovs, D., K. Cjaputa and M. Kirikova (2016). "Towards Continuous Information Security Audit." In: *REFSQ Workshops*. *

Kumar, P. R., P. H. Raj and P. Jelciana (2018). "Exploring Data Security Issues and Solutions in Cloud Computing." *Procedia Computer Science* 125, 691–697. *

Lezzi, M., M. Lazoi and A. Corallo (2018). "Cybersecurity for Industry 4.0 in the Current Literature: A Reference Framework." *Computers in Industry* 103, 97–110.

Livshitz, I. I., K. A. Nikiforova, P. A. Lontsikh and V. A. Karaseva (2016). "The Evaluation of the Electronic Services With Accordance to IT-Security Requirements based on ISO/IEC 27001." In: *2016 IEEE Conference on Quality Management, Transport and Information Security, Information Technologies (IT&MQ&IS)*, pp. 128–131. *

Lopes, I. and P. Oliveira (2014). "Understanding Information Security Culture: A Survey in Small and Medium Sized Enterprises.". In *New Perspectives in Information Systems and Technologies, Volume 1*, pp. 277–286: Springer. *

Lundgren, B. and N. Möller (2017). "Defining Information Security." *Science and Engineering Ethics*, 1–23. *

Ma, Q. and P. Ratnasingam (2008). "Factors Affecting the Objectives of Information Security Management." In: *Proceedings of the CONF-IRM 2008 Proceedings*. Ontario, Canada. *

McLaughlin, M.-D. and J. Gogan (2018). "Challenges and Best Practices in Information Security Management." *MIS Quarterly Executive* 17 (3).

Moghaddasi, H., S. Sajjadi and M. Kamkarhaghighi (2016). "Reasons in Support of Data Security and Data Security Management as Two Independent Concepts: a New Model." *The open medical informatics journal* 10, 4. *

Mohurle, S. and M. Patil (2017). "A Brief Study of Wannacry Threat: Ransomware Attack 2017." *International Journal of Advanced Research in Computer Science* 8 (5).

Mosenia, A. and N. K. Jha (2016). "A Comprehensive Study of Security of Internet-of-Things." *IEEE Transactions on Emerging Topics in Computing* 5 (4), 586–602. *

Mukundan, N. R. and L. P. Sai (2014). "Perceived Information Security of Internal Users in Indian IT Services Industry." *Information Technology and Management* 15 (1), 1–8. *

Murray, G., M. N. Johnstone and C. Valli (2017). "The Convergence of IT and OT in Critical Infrastructure." In: *The Proceedings of 15th Australian Information Security Management Conference*. Perth, Australia.

National Institute of Standards and Technology (2006). *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems*. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf. *

National Institute of Standards and Technology (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (visited on 05/31/2019). *

Neumann, P. G. (1994). *Computer-related Risks:* Addison-Wesley Professional. *

Otero, A. R., C. E. Otero and A. Qureshi (2010). "A multi-criteria evaluation of information security controls using boolean features." *International Journal of Network Security & Its Applications* 2 (4), 1–11. *

Paja, E., F. Dalpiaz and P. Giorgini (2013). "Managing Security Requirements Conflicts in Socio-Technical Systems.". In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar,

M. Y. Vardi, G. Weikum, W. Ng, V. C. Storey and J. C. Trujillo (eds.) *Conceptual Modeling*, pp. 270–283. Berlin, Heidelberg: Springer Berlin Heidelberg. *

Pattanavichai, S. (2018). "Design Network Model for Information Security Management Standard depend on ISO 27001." *GSTF Journal on Computing (JoC)* 5 (4). *

Posthumus, S. and R. von Solms (2004). "A Framework for the Governance of Information Security." *Computers & Security* 23 (8), 638–646. *

Qadir, S. and S. M.K. Quadri (2016). "Information Availability: An insight into the most Important Attribute of Information Security." *Journal of Information Security* 7 (03), 185. *

Riel, A., C. Kreiner, R. Messnarz and A. Much (2018). "An architectural approach to the integration of safety and security requirements in smart products and systems design." *CIRP Annals* 67 (1), 173–176. *

Rowe, F. (2014). "What literature review is not: diversity, boundaries and recommendations." *European journal of information systems* 23 (3), 241–255.

Rüßmann, M., M. Lorenz, P. Gerbert, M. Waldner, J. Justus, P. Engel and M. Harnisch (2015). "Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries." *Boston Consulting Group* 9 (1), 54–89.

Sadeghi, A.-R., C. Wachsmann and M. Waidner (2015). "Security and Privacy Challenges in Industrial Internet of Things." In: *Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC).* San Francisco, California, USA. *

Saleh, M. F. (2011). "Information Security Maturity Model." *International Journal of Computer Science and Security* 5 (3), 316–337. *

Sattarova Feruza, Y. and T.-h. Kim (2007). "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security." *International journal of multimedia and ubiquitous engineering* 2 (2), 17–32. *

Singh, K. P., V. Rishiwal and P. Kumar (2018). "Classification of Data to Enhance Data Security in Cloud Computing." In: *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU).* Nainital, Uttarakhand, India. *

Solms, B. von (2001). "Corporate Governance and Information Security." *Computers & Security* 20 (3), 215–218.

Solms, R. von and J. van Niekerk (2013). "From Information Security to Cyber Security." *Computers & Security* 38, 97–102. *

Stallings, W., L. Brown, M. D. Bauer and A. K. Bhattacharjee (2012). *Computer Security: Principles and Practice:* Pearson Education Upper Saddle River, NJ, USA. *

Timmermanns, J. (2018). *The relation between the organizational information security climate and employees' information security behavior.* Delft University of Technology. URL: https://repository.tudelft.nl/islandora/object/uuid:78a12359-a9a9-4b65-8e8f-83aeae8b8939 (visited on 11/17/2020). *

Tom, S., D. Christiansen and D. Berrett (2008). *Recommended practice for patch management of control systems.* Idaho National Laboratory (INL).

United States Government (2011). *Coordination of Federal Information Policy*. URL: https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/FISMA-final.pdf. *

United States Securities and Exchange Commission (2017). *Annual Report pursuant to Section 13 or 15(d) of the Security Exchange Act of 1934 for Yahoo! Inc.* URL: https://www.sec.gov/Archives/edgar/data/1011006/000119312517065791/d293630d10k.htm#toc.

Vaidya, S., P. Ambad and S. Bhosle (2018). "Industry 4.0 - A Glimpse." *Procedia Manufacturing* 20, 233–238.

van Lamsweerde, A. (2004). "Elaborating security requirements by construction of intentional anti-models." In: *Proceedings. 26th International Conference on Software Engineering*: IEEE Comput. Soc. Edinburgh, UK. *

Vom Brocke, J., A. Simons, B. Niehaves, K. Riemer, R. Plattfaut, A. Cleven and others (2009). "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process." In: *Proceedings of the 17th European Conference on Information Systems (ECIS).* Verona, Italia

Vuorinen, J. and P. Tetri (2012). “The Order Machine-The Ontology of Information Security.” *Journal of the Association for Information Systems* 13 (9), 695. *

Wang, E. K., Y. Ye, X. Xu, S.-M. Yiu, L. C. K. Hui and K.-P. Chow (2010). “Security Issues and Challenges for Cyber Physical System.” In: *Proceedings of the 2010 IEEE/ACM Int’l Conference on Green Computing and Communications & Int’l Conference on Cyber, Physical and Social Computing*. Hangzhou, China. *

Weaver, L. J. and C. B. Fasel (2018). “A Systematic Review of the Literature on the Relationships Between Chronic Diseases and Food Insecurity.” *J Nutr Food Sci* 9 (05), 519.

Webster, J. and R. T. Watson (2002). “Analyzing the Past to Prepare for the Future: Writing a Literature Review.” *MIS Quarterly*, xiii–xxiii.

Weitzner, D. J., H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler and G. J. Sussman (2008). “Information accountability.” *Commun. ACM* 51 (6), 82–87. *

Whitman, M. E. and H. J. Mattord (2011). *Principles of Information Security:* Cengage Learning. *

Williams, P. (2001). “Information Security Governance.” *Information Security Technical Report* 6 (3), 60–70. *

Wolfswinkel, J. F., E. Furtmueller and C. P. M. Wilderom (2013). “Using Grounded Theory as a Method for Rigorously Reviewing Literature.” *European journal of information systems* 22 (1), 45–55.

Yang, T.-H., C.-Y. Ku and M.-N. Liu (2016). “An integrated system for information security management with the unified framework.” *Journal of Risk Research* 19 (1), 21–41. *

Yu, X. and Q. Wen (2010). “A View about Cloud Data Security from Data Life Cycle.” In: *2010 International Conference on Computational Intelligence and Software Engineering*, pp. 1–4. *

Zaini, M. K., M. N. Masrek, Sani, M. K. J. A. and N. Anwar (2018). “Theoretical Modeling of Information Security: Organizational Agility Model based on Integrated System Theory and Resource Based View.” *International Journal of Academic Research in Progressive Education and Development* 7 (3), 390–400. *

Zhou, K., T. Liu and L. Zhou (2015). “Industry 4.0: Towards Future Industrial Opportunities and Challenges.” In: *Proceedings of the 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. Zhangjiajie, China. *

Zissis, D. and D. Lekkas (2012). “Addressing Cloud Computing Security Issues.” *Future Generation Computer Systems* 28 (3), 583–592. *

* means that the paper is part of our literature review