Investigating Accountability in Business-intensive Systems-of-Systems

Felipe Cordeiro
Foundation to Support Technical Education - FAETEC
Rio de Janeiro, RJ, Brazil
felipecordeiro@faetec.rj.br

Aline Vasconcelos
Fluminense Federal Institute - IFF Campos
Campos dos Goytacazes, RJ, Brazil
apires@iff.edu.br

Rodrigo Pereira dos Santos
Federal University of the State of Rio de Janeiro - UNIRIO
Rio de Janeiro, RJ, Brazil
rps@uniriotec.br

Patricia Lago
Vrije Universiteit Amsterdam
Amsterdam, The Netherlands
p.lago@vu.nl

ABSTRACT

CONTEXT: The evolution of business processes has driven the integration of systems-of-systems (SoS) across various domains, leveraging technologies such as cloud computing, e-commerce platforms, and smart environments. In this context, the integration of various heterogeneous and independent constituents systems include information systems that collaborate to achieve business goals. Hence, the accountability of these systems must be a concern, but traditional accountability approaches can obscure the responsibility and ownership of data, processes, and outcomes. PROBLEM: This complexity often results in studies offering specific solutions, then highlighting the ongoing need for a shared understanding of accountability. Furthermore, establishing accountability as a quality requirement poses a significant challenge due to limited research and an undefined agenda for underlying challenges. SOLUTION: This paper presents an overview of accountability from reporting on the current landscape to proposing a research agenda to address existing challenges. METHOD: The study adopts a prescriptive approach based on a systematic mapping study. RESULTS: The study yields insights into accountability, and a research agenda when identifying seven topics for further investigation. CONCLUSION: By consolidating knowledge on accountability, this study facilitates the expansion of the body of knowledge on the field and brings new inquiry to inspire innovative solutions.

CCS CONCEPTS

• **Software and its engineering → Software creation and management**.

KEYWORDS

Accountability, Systems-of-Systems, Business Aspects of Software Engineering, Systems-of-Information Systems, Roadmap.

1 INTRODUCTION

Nowadays, organizations rely more on complex and interconnected systems to manage operations, exchange information, and coordinate activities in a non-linear manner. Among these, system-of-systems (SoS) stands out as complex system [1–4]. These solutions have in common the fact that they integrate independent systems into larger and more complex systems that provide capabilities that can only be achieved through collaboration among systems [5]. SoS complexity differs from traditional systems due to features such as operational and managerial independence, distributed constituent systems, and evolutionary development, often leading to emergent behaviors [6]. In this context, a specific subset of business-intensive SoS emerges: system-of-information systems (SoIS) [7], in which independent systems, including information systems (IS) among their constituents systems, are organized in an interconnected arrangement for supporting business goals [8, 9].

SoIS exhibit a strong business nature, with goals often being expressed as dynamic and inter-organizational business processes [9]. While SoS primarily focus on technical artifacts, such as software components, SoIS take a broader perspective, concentrating on various elements within the system structure. SoIS is formed by exhibit unique properties, such as the flow of information, a business-process-oriented nature, and the creation of earned value from interoperability among constituent systems [8, 10]. Unlike traditional systems, a SoIS involves diverse engineering interconnections, potentially sourced from various entities (e.g., users, developers, organizations), and often operates across different legal and regulatory frameworks. This distinction underscores the importance of considering not only technical but also business aspects.

Despite many benefits, SoIS also pose significant challenges, particularly in terms of accountability as detailed in previous works [11, 12]. *Accountability is a non-functional requirement [13] for holding responsible actions in organizations regarding obligations and sanctions [14] and must encompass evaluation strategies [13, 15, 16].* It refers to the obligation of individuals or organizations to be answerable for their actions, decisions, and consequences arising from their activities [16]. For example, ethics on programming, transparency of services, or a security breaches, pinpointing accountability becomes intricate due to its distribution among multiple systems. Determining the root cause and allocating responsibility for addressing the issue poses a significant challenge, emphasizing the need for strategies to assess accountability within systems.

Understanding the current state-of-the-art on the SoIS accountability is thus essential for addressing constituent systems engineering challenges and developing effective solutions [17]. To the best of our knowledge, there is no characterization in the state-of-the-art of SoIS accountability. Thus, the main contribution of this work are (i) characterization of the state-of-the-art on the SoIS accountability, and (ii) identification of research directions. To do so, we reviewed the existing literature to identify the factors that affect accountability in this context. After discussing the results, we point out some directions to stimulate future research.

The remainder of this paper is organized as follows: Section 2 presents the background; Section 3 covers related work; Section 4 explains the research method; Section 5 presents findings and implications; Section 6 outlines a research agenda on SoIS accountability; Section 7 provides a discussion; Section 8 lists threats to validity; and Section 9 concludes the paper with some final remarks.

2 BACKGROUND

Accountability definitions are quite broad and are adapted to many domains. Gortmaker *et al.* [18] explore a definition of accountability, mentioning that it *"always involves an actor with the duty to render an account and another actor with the power to judge or impose sanctions"*. Furthermore, authors argue that *"duty to render an account"* corresponds with the *"delegation of authority to act"*, and *"held to answer implicitly assumes that one party has the power to judge the other party's performance"*.

Attempting to further elucidate the concept of accountability, Feigenbaum *et al.* [19] performed a literature review in the field of Computer Science, defining accountability as a strategic mechanism that links actions to consequences and dispels misconceptions such as the notion that accountability precludes anonymity or requires centralized authority. Vance *et al.* [20] contribute with an accountability theory, framing it within the context of access policy violations and emphasizing the process whereby individuals are obligated to explain their actions to relevant parties who possess the authority to adjudicate and impose consequences.

Additionally, accountability appears in diverse forms related to service quality: (i) as a proactive measure to improve security and protect online privacy; (ii) as a fundamental aspect of effective governance in public and private sectors; (iii) as a means to align organizational goals with operational functions and enhance oversight; (iv) as a facilitator of democratic processes; and (v) as a defining attribute influencing system dynamics and functionality, based on previous research [11, 12, 21]. Despite these varied definitions, they generally imply the capacity of someone or something (e.g., sensors or systems) to assess and establish a culture of responsibility through evaluation [16, 19].

In the context of complex systems engineering (e.g., SoS and, consequently, SoIS), prioritizing accountability is advocated to tackle challenges and foster innovation throughout the software lifecycle. An accountable approach to software projects can significantly enhance their business relevance by offering clear insights into capability gaps, operational needs, requirements (functional and non-functional), interoperability, and operational procedures. Moreover, accountable behaviors from software engineers ensures alignment with organizational goals and facilitates effective decision-making. Strategies for enhancing software engineers accountability may include implementing checkpoints to monitor performance, providing training and resources to support developers in fulfilling their responsibilities, and establishing a system of rewards and recognition for outstanding performance. Thus, understanding the scope of the project and implementing controls for managing and controlling it are fundamental aspects of accountability.

In addition, by clearly defining the scope and establishing effective controls, the project team can mitigate risks, address potential challenges, and maintain alignment with stakeholder expectations. Regarding all the above findings, this paper claims the following definition: **accountability, as a non-functional requirement, entails holding individuals or entities responsible for their actions within organizations, encompassing obligations, sanctions, and necessitating comprehensive evaluation strategies**, based on previous work [11, 12, 21].

Therefore, as prior research has delved into methods for integrating accountability into systems, there is an urgent call for further investigation into the intricacies of accountability. This is especially important when developing successful strategies for evaluating and improving accountability in complex systems.

3 RELATED WORK

Systematic mapping study (SMS) is a relevant strategy in scientific research by providing a comprehensive understanding of existing knowledge, identifying gaps, and uncovering avenues for further exploration [22]. Based on structured methodologies, SMS enable researchers to systematically gather, assess, and synthesize relevant literature on a particular topic or research question. This process not only helps in identifying prevailing problems and challenges but also sheds light on emerging opportunities and areas for advancement within a given field. Thus, this section presents related work on the investigated topic.

Studies conducted by Inocencio *et al.* [23], Teixeira *et al.* [17], Silva *et al.* [24], Ferreira *et al.* [5] and Fernandes *et al.* [10] demonstrate the importance of SMS in uncovering insights related to SoS and SoIS that are often underexplored (or insufficient) in the literature. For example, Inocencio *et al.* [23] and Silva *et al.* [24] underscore the significance of emergent behavior as a critical characteristic of SoS. Similarly, Teixeira *et al.* [17] highlight the scarcity of studies addressing languages, techniques, and tools for modeling SoIS architectures, indicating a need for more comprehensive research in this area.

Furthermore, Ferreira *et al.* [5] presents the state-of-the-art on the way reliability of SoS has been addressed. After investigating the literature, authors selected 27 studies to perform a detailed analysis regarding factors that affect the reliability of SoS and approaches and metrics to improve it. Fernandes *et al.* [10] purpose a conceptual model to support researchers and practitioners to recognize SoIS, based on a literature review on the topic, aiming to support researchers and practitioners in the SoIS design. In common, authors argue that investigating complex systems arrangements, including concepts, definitions, and relationships, based on literature review can significantly enhance understanding in these domains.

Concerning to investigations in real scenarios, in previous research, we have explored the use of systems thinking to support SoIS accountability. Firstly, we analyzed a Brazilian public school scenario support within SoIS [11]. This study highlighted the importance of understanding the relationships and interactions among the various actors involved in the educational process to build a more accountable and efficient SoIS. In another research, we investigated the application of a modeling technique that incorporates feedbacks from SoIS stakeholders, demonstrating how the proposed approach can be used to suggest and enhance accountability in complex systems [21].

Returning to SoIS accountability, it is clear that this aspect is unexplored despite its significance. Additionally, it is worth noting that this study not only addresses the gap in accountability within SoIS but also contributes to a broader understanding of accountability dynamics in SoS. It highlights the need for additional research to pinpoint gaps and effectively guide future investigations.

4 RESEARCH METHOD

The study's research method followed Kitchenham *et al.* [22] approach, depicted in Figure 1, which presents three main phases: planning, execution, and results synthesis. In the SMS planning, it was apparent that limited studies explored the accountability topic in conjunction with SoIS. As a result, research questions (RQ) were devised to encompass broader systems, including complex systems arrangements, such as SoIS. The initial stage involved defining research scope and formulating the following RQ:

RQ1 – *What does the scientific literature say about accountability in SoIS?* – Concerning to RQ1, a SoIS has supported parts of organizations, entire organizations, or groups of organizations. Thus, accountability tends to be different since it depends on organizational objectives and how it is supposed to be achieved. RQ1 refers to aspects of accountability developed over time (and still unclear) encompassing complex systems.

RQ2 – *What are the research challenges related to accountability in SoIS?* – RQ2 focused on establishing how far researchers have investigated accountability in the literature. Moreover, it considers accountability elements for supporting systems operation and maintenance, aiming to put efforts into accountability evaluation and where the potential for further research challenges lies.

Next, in the SMS execution, a generic search string was defined from four keywords. The keywords were connected by using the logical operator *AND*, while variations and synonyms were connected via the logical operator *OR*. The terms were selected aiming at a broader search, i.e., a large coverage of studies. We tested configurations of the search string in Scopus, which is considered the largest scientific publication database that indexes the most relevant publication venues. After calibration, the search string was:

("Systems-of-Information Systems" ***OR*** *"Systems of Information Systems"* ***OR*** *"Information Systems")* ***AND*** *("Accountability")*

To verify the accuracy of the search string, we used a control group containing a study which is relevant to the topic addressed in this study [25]. We also carried out searches in ACM Digital Library, IEEE Xplore, ScienceDirect, and SpringerLink. We chose no time or area/field restrictions, covering studies until April 2023.

During the study selection stage, we retrieved 905 studies, encompassing the control group study. Duplicated studies were removed, leaving a set of 713 studies for further examination. Next, the publication venue, title, and abstract were scrutinized, and the inclusion and exclusion criteria shown in Table 1 were applied. This process led to the exclusion of 562 studies, resulting in 151 studies that were considered for a thorough analysis.

During the data extraction, relevant information was systematically gathered using a data collection form. Furthermore, to enhance the review's inclusiveness, a snowballing technique was employed

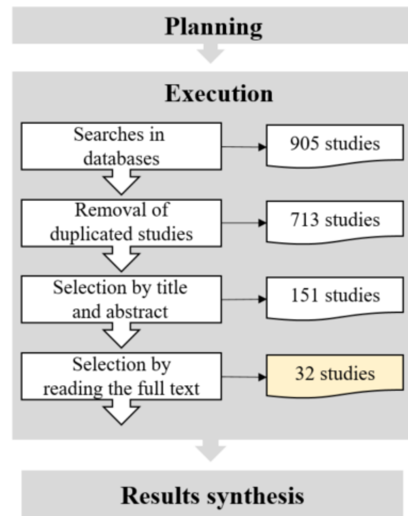

Figure 1: Process of selection of primary studies

Table 1: Inclusion and exclusion criteria

Inclusion Criteria (IC)
IC1: The study is available for download.
IC2: The study reports on accountability.
IC3: The study describes accountability in other disciplines related to complex systems.
Exclusion Criteria (EC)
EC1: The study is not peer-reviewed.
EC2: The study is not available online or was not obtained by contacting the authors.
EC3: The study is written in a language other than English.
EC4: The study is a editorial, summary of keynotes, or tutorial.

to identify additional studies through their references. Finally, after a thorough review of these studies and the application of selection criteria, a final set of 32 studies was chosen for data extraction (Table 2). The study was supervised by three experienced researchers with over 20 years of experience on SoS and empirical software engineering. Their oversight was crucial for ensuring the accuracy and reliability of the study, as well as for mitigating potential biases. Given the page limitations, the Artifact Availability Section presents this study's dataset.

5 WHAT DOES THE SCIENTIFIC LITERATURE SAY ABOUT ACCOUNTABILITY IN SOIS?

Before answering RQ1, we give an overview of the selected studies.

5.1 Overview

The search yielded a limited number of results, categorized by study identification, name, and authors, as depicted in Table 2. Several researchers and research groups have worked independently and shared their findings in multiple venues. More specifically, 14 studies were published across 13 different journals, while 18 studies

Table 2: List of selected studies

ID	Tittle	Ref.
S01	A framework for performance based logistics: a system of systems approach	[26]
S02	A meta-modeling framework to support accountability in business process modeling	[27]
S03	A method for identification of potential interoperability links between information systems towards system-of-information systems	[10]
S04	Accountability in cloud service provision ecosystems	[13]
S05	Accountability in the iot: systems, law, and ways forward	[28]
S06	Accountability issues in multihop message communication	[29]
S07	Accountability of electronic cross-agency service-delivery processes	[18]
S08	Adaptability and accountability of information architectures in interorganizational networks	[30]
S09	An agent-based framework for identity management: the unsuspected relation with iso/iec 15504	[31]
S10	An online transparency for accountability maturity model	[32]
S11	Being ethical in developing information systems: an issue of methodology or maturity in judgment?	[33]
S12	Cross-boundary e-government systems: determinants of performance	[34]
S13	Decision provenance: harnessing data flow for accountable systems	[35]
S14	Descriptions of responsibility for implementation: a content analysis of strategic information systems/technology planning documents	[36]
S15	Designing for accountability	[37]
S16	Designing the accountability of enterprise architectures	[38]
S17	Discriminative effect of user influence and user responsibility on information system development processes and project management	[39]
S18	Discussions about perfecting chinese system of official accountability for mining disasters	[40]
S19	Expanding citizen access and public official accountability through knowledge creation technology: one recent development in e-democracy	[41]
S20	Health information systems, decentralisation and democratic accountability	[42]
S21	Information systems and the open world challenges	
S22	Information technology, responsibility, and anthropology	[43]
S23	Information, not technology, is essential to accountability: electronic records and public-sector financial management	[44]
S24	Privacy by information accountability for e-health systems	[45]
S25	Public sector information management in east and southern africa: implications for foi, democracy and integrity in government	[46]
S26	Sharing with care: an information accountability perspective	[47]
S27	State education agencies, information systems, and the expansion of state power in the era of test-based accountability	[48]
S28	Systems thinking as a resource for supporting accountability in system-of-information-systems: exploring a brazilian school case	[11]
S29	Toward accountability in the cloud	[49]
S30	Towards a formal model of accountability	[19]
S31	Towards accountable enterprise mashup services	[50]
S32	Using accountability to reduce access policy violations in information systems	[20]

were disseminated through 13 different conference or workshop proceedings. It suggests that the research is not concentrated in some groups and may have been conducted without collaboration or coordination towards a common terminology or agenda. Two studies have referenced service-oriented architectures as a potential option for the SoIS engineering, as shown in Figure 2.

Additionally, Grounded Theory was applied in two studies for better understanding the phenomenon, while business process modeling, enterprise architecture, systems thinking, neural network, neural logic and digital signal have each been mentioned in one study, as shown in Figure 3. The identified results were analyzed to assess how the systems typically addresses accountability and its relevance in different approaches. The analysis revealed that the term accountability is used as a buzzword without demonstrating its practical relevance. Few results were found that directly address SoIS accountability. Therefore, the results are organized considering the perspective of accountability in complex systems, which are further discussed in the next sections.

5.1.1 Definition of Accountability. Accountability in SoS, particularly in the SoIS context, lacks a specific definition. Studies often blur the line between accountability and responsibility, creating confusion. In our investigation, we approached accountability from two angles: a direct perspective based on formal definitions found in existing literature, and an indirect perspective illustrated through examples. However, despite this dual approach, establishing a uniform definition remains challenging, resulting in accountability remaining elusive within SoIS (e.g., S02, S08, S28, and S30). It emerges as a multidimensional concept that transcends mere technological aspects. This ambiguity holds significant implications for software development processes, underscoring the necessity for a nuanced understanding and precise delineation to effectively manage accountability as a quality requirement.

5.1.2 Accountability versus Responsibility. The term "responsibility" is often used without explicit mention of accountability, and studies not addressing responsibility from an accountability perspective are excluded from our research. While accountability and responsibility are related terms, they do not mean the same concept. Responsibility refers to performing a specific task or function (S30), while accountability involves accepting the consequences of that task's outcome [51]. In SoIS, defining both is crucial for stakeholders to understand their roles and obligations. In S14, S21 and S22, responsibility is depicted as a moral or legal obligation leading to accountability, concentrating on various elements within the system engineering.

5.1.3 Dependence on People. SoIS nature often depend on human involvement for operation and maintenance, posing challenges. Human errors, illness, or turnover can disrupt the system. Additionally, intentional misuse of constituents systems can compromise security and data integrity. For instance, S11 and S14 highlight the importance of improving ethical conduct, fostering accountable behaviors, and addressing the negative impact of poor decision-making on organizational objectives. The research emphasizes a thorough understanding of accountability toward tasks, relationships, communication, and participation. These findings have important implications for advancing and promoting ethical and responsible behavior in SoIS engineering.

5.1.4 Frameworks and Models. Some studies have proposed frameworks and models (e.g., S07, S09, and S10) to enhance accountability related to management improvement, transparency, technology, and involvement. However, these studies have not been explored in SoIS research to establish a structure for designing, implementing, and managing these systems, especially regarding accountability. Essentially, this area is still emerging, particularly in terms of how these frameworks and models can address accountability strategies by mapping roles, responsibilities, decision-making processes, and escalation procedures to ensure clarity and awareness of responsibilities among all involved constituents systems and stakeholders.

5.1.5 Information and Communication Technology. SoIS heavily rely on information and communication technology (ICT) to function as a system. ICT includes hardware, software, and networking components that are critical to the operation of constituents systems. Ensuring that the constituent systems are reliable, secure, and up-to-date is essential to their success. Results indicate a strong connection between accountability and ICT in different systems (e.g., S04, S06, and S32). Moreover, the ICT factor is relevant, given the constituent systems dynamics. However, there is still much room

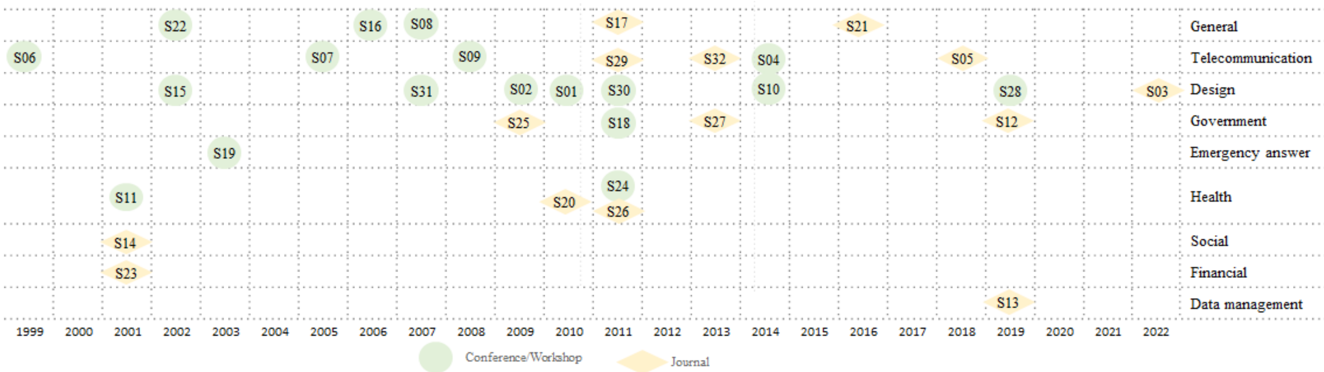

Figure 2: Overview of the selected studies

for research as few results demonstrate the influence of accountability with a focus on ICT. The studies refer to security strategies, transparency, and data access privileges.

5.1.6 Governance and Competitive Advantage. Some studies investigate initiatives in public or private services, focusing on governance and competitive advantage (e.g., S12, S18, S20, and S21). These initiatives involve tracking activities, participating in system decisions, and evaluating service quality. For example, there are studies on neural network-based applications and algorithms for accessing public information as part of e-democracy and participation strategies. SoIS governance is crucial for effective and efficient operation. Good governance can enhance decision-making, agility, and risk reduction, providing a competitive edge.

5.1.7 Data Management. Some studies highlighted concerns raised by medical professionals about patient privacy (e.g., S24 and S26), data sharing (S13), and monitoring student academic progress (S27). SoIS generate and store large amounts of data, requiring effective management to ensure accuracy, security, and availability. Transparency is crucial for SoIS operations, including data collection, storage, use, and sharing. Transparency is vital for establishing trust with users and stakeholders and ensuring ethic.

5.2 The Need of Accountability Evaluation

The comprehensive exploration of accountability, underscores the intricate nature of its evaluation. Building upon this foundation, the research integrates the General Systems Theory (GST) [52] as a way to provide a holistic approach to understanding complex systems and their interrelationships. From this process, we observed that the outcomes of this SMS were inherently aligned with the three fundamental categories of engagement, regulation, and management. For instance, findings related to stakeholder involvement and influence naturally fell under the category of engagement, while aspects concerning rule enforcement and control mechanisms were categorized under regulation. Similarly, results pertaining to organizational oversight and strategic planning were attributed to the management category.

This alignment underscores our categorization process and reinforces the relevance of these categories in assessing SoIS accountability. The categorization process involved a rigorous comparative analysis of the SMS findings, identifying recurring themes and concerns related to accountability. Based on iterative refinement and cross-referencing, these three categories surfaced as categories of evaluation. Therefore, each category is directly linked to specific studies, ensuring a traceable connection. Given the page limitations, the complete list of SMS results and categorization according with the accountability evaluation categories can be observed in the Artifact Availability Section.

In this context, a discussion is designed to enhance and strengthen accountability throughout the entire software lifecycle, encompassing the design, development, and implementation of both SoS and SoIS. Its purpose is to contribute to the expanding body of research in the field by focusing on fundamental accountability questions, including "Who is responsible for", "What are the objectives", "How will they be achieved," and "When will they be accomplished". In essence, the findings indicate the need for a thorough examination of accountability, grounded in the three categories for supporting the accountability evaluation, as discussed next.

The **Engagement** category was chosen due to its direct relevance to studies exploring human influences, highlighting the pivotal role of stakeholder involvement in shaping accountability dynamics within SoIS and software development processes. Engagement serves as the cornerstone for fostering a culture of accountability, necessitating active participation and commitment from stakeholders at all levels. It entails sustaining stakeholders' involvement in identifying strategies to achieve the purpose of constituents system, playing a crucial role in optimizing software development processes within complex systems [12]. Thus, engagement category "involves maintaining and sustaining people's participation in identifying strategies that may help SoIS achieve its purpose".

The **Management** category was selected for its intricate connections to various management controls, underscoring its significance in orchestrating and optimizing accountability initiatives within constituent systems. Effective management facilitates the integration of accountability into processes, ensuring its seamless implementation and continuous improvement. The interplay between management and accountability may enhance operations to optimize the performance of constituent systems. Additionally, the management category encompasses best practices for managerial purposes, emphasizing the need to define structures that support

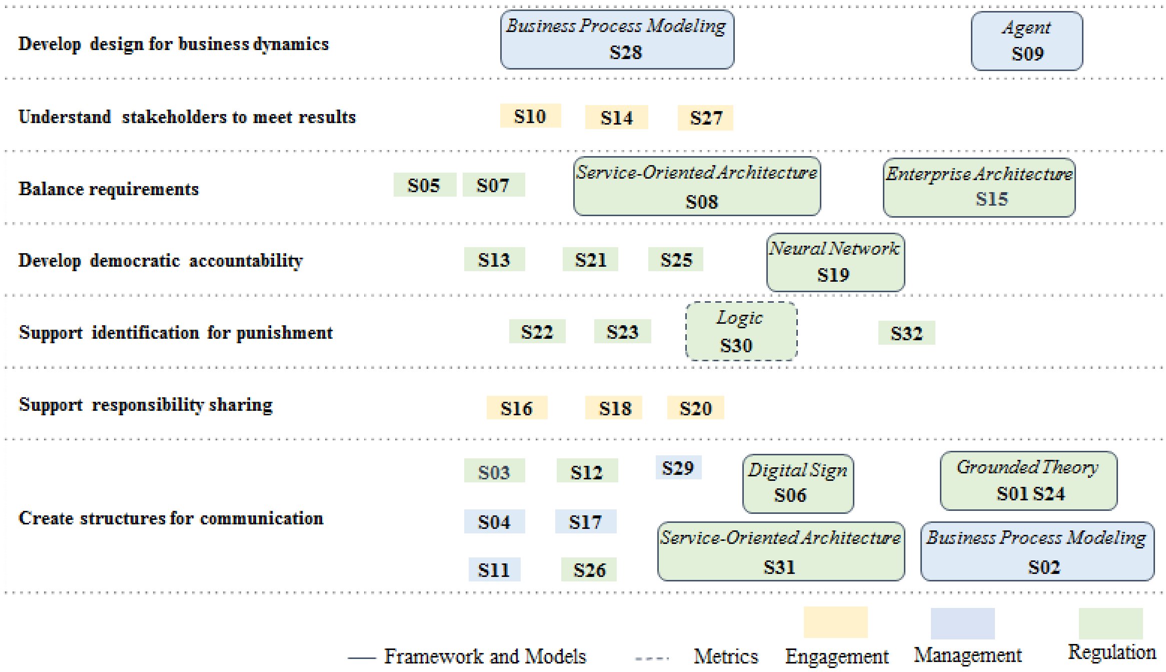

Figure 3: Characteristics of the selected studies

accountability to assess the performance and impact within software development processes [12]. Thus, management as part of the accountability evaluations strategy "seeks to support managerial workforce activities aligned with a process in public or private organizations supported with SoIS".

Lastly, the **Regulation** category was singled out for its direct correlation with technological influences, illustrating the impact of regulatory mechanisms and technological advancements on constituent systems processes. Regulation serves as a guiding mechanism, ensuring adherence to established norms and standards, thereby fostering transparency and trust within complex systems. Furthermore, regulation holds the responsibility of establishing a link between engagement and management, forming a tripartite association for evaluating accountability [12]. Thus, regulation as part of accountability evaluations strategy "refers to meeting an organization's requirements to comply with (and enforce) legal and regulatory standards aligned with technology regarding IS/SoIS".

It is worth mentioning, that through the diagnostic of accountability evaluation, insights can be gained into how to enhance software development lifecycle processes. For instance, leveraging engagement strategies may optimize stakeholder involvement in requirements gathering and validation phases (e.g., user stories and acceptance criteria). Effective management practices could streamline project planning and resource allocation, ensuring accountability throughout development iterations. Regulatory mechanisms, on the other hand, can guide compliance efforts during software testing and deployment phases, promoting transparency and trust among stakeholders. By integrating these categories into the software development lifecycle, organizations can foster a culture of accountability and enhance overall project success.

6 WHAT ARE THE RESEARCH CHALLENGES RELATED TO ACCOUNTABILITY IN SOIS?

In our SMS, we have identified distinct challenges from the primary studies which reveal insights into the complexity of establishing SoIS accountability. These challenges highlight the gaps in current accountability systems when applied to business-intensive environments where diverse and often independent systems interact.

Therefore, in order to answer RQ2, we provide a list of seven opportunities for future research on SoIS aiming to invite researchers and practitioners for further inquiry to inspire innovative solutions. It highlights aspects of engagement, management, and regulation categories, frameworks and models, and metrics, as shown in Figure 3. These findings suggest a urgent need for more research that can cope with the dynamic nature of SoIS and ensure accountability across all levels.

6.1 Develop Design for Business Dynamics

This challenge involves creating models of the business process that can be used to identify potential accountability issues and optimize the constituent systems engineering process. The solution should take into account the distributed nature of systems arrangement by including several stakeholders involved in the process, their roles, responsibilities, and information flow within the process. These stakeholders may have different levels of commitment and varying degrees of control over the process.

Therefore, designing for different dynamics involves taking into account the diversity of stakeholders and their interactions within the process, as well as the potential conflicts that may arise (e.g., S09 and S28). By developing a design that can accommodate such dynamics, organizations can ensure that their systems are adaptable, flexible, and responsive to changing circumstances.

6.2 Understand Stakeholders to Meet Results

In order to effectively integrate technology within SoIS use, this challenge revolves around understanding the demands and relationships of actors with software usability as a valuable resource for analyzing technology acceptance and usage. By understanding these objectives, we can uncover the essential skills, knowledge, and efforts required to effectively implement technology in support of SoIS. These stakeholders may include business analysts, developers, users, regulatory bodies, and others. By understanding the needs and expectations of these stakeholders, organizations can ensure that the system meets the necessary accountability requirements and achieves the desired outcomes (e.g., S10, S14, and S27).

6.3 Balance Requirements

This challenge involves designing for accountability while considering various other quality requirements, including non-functional ones, which are crucial for system success. Our research highlights diverse needs. For example, ensuring accountability might require transparent data governance mechanisms (architecture), robust access controls (control), participatory decision-making processes (democracy), ethical handling of sensitive information (ethics), appropriate development methodologies (methods), and accurate data management practices (data), as shown in S05, S07, S08, and S15. However, aligning these different requirements can be complex. These non-functional requirements play a vital role in shaping how accountability is upheld within the constituent system, emphasizing the necessity for careful engineering and alignment across all aspects of system design and implementation.

6.4 Develop Democratic Accountability

This challenge is an important topic for research on SoIS since complex systems have a significant impact on society and can shape people's lives in many ways. Democratic accountability is founded upon the fundamental principle that individuals who are impacted by a given decision ought to possess the right to participate in the decision-making process and subsequently bear the capacity to hold decision-makers responsible for their conduct. In the context of constituent systems, this means ensuring that the benefits and risks of these systems are fairly distributed across society. Developing democratic accountability across business process helps to promote trust, fairness, and legitimacy in these systems as well as to ensure that they serve the public interest (e.g., S13, S29, S21, and S25). This requires interdisciplinary research that draws on insights from computer science, law, ethics, and social science, among other fields.

6.5 Support Identification for Punishment

This challenge plays a critical role in several domains, including healthcare, finance, and government, among others. However, these systems can also be used to commit fraudulent activities or cause harm to individuals or society. Therefore, it is crucial to ensure that individuals or entities responsible for such actions are held accountable. Identification of the culprits is a critical aspect of accountability, which can be challenging in SoIS due to the complexity of the systems and the anonymity of actors (e.g., S23, S30, and S32). Research on supporting the identification for punishment can help develop methods and technologies to overcome these challenges and improve the SoIS accountability. This includes developing techniques for tracing the origin of malicious activities, identifying individuals involved, and ensuring appropriate punishment.

6.6 Support Responsibility Sharing

Responsibility sharing refers to the distribution of responsibilities among stakeholders in a SoIS to ensure that all parties share the burden of accountability. This approach promotes collaboration, transparency, and trust among stakeholders, which is essential for the effective governance of SoIS (e.g., S16, S18, S20, and S22). The importance of responsibility sharing has been recognized in several fields, including cybersecurity, healthcare, and public administration. Therefore, supporting responsibility sharing is a relevant topic for SoIS research, and it is crucial to develop effective strategies and frameworks to ensure that all stakeholders in the SoIS take responsibility for their actions.

6.7 Create Structures for Communication

This challenge involves a complex network of interconnected constituent systems that can have far-reaching implications. As such, it is important to establish clear lines of communication between all the stakeholders involved in the development, deployment, and maintenance of systems (e.g., S02, S04. S11, S17, and S29). This includes not just the technical teams, but also the end-users, regulatory bodies, and other external parties. Effective communication can help to identify potential risks and vulnerabilities early on, allowing for proactive measures to be taken to mitigate these risks. It can also help to ensure that all stakeholders are kept informed of any changes or updates to the system, and that they understand their responsibilities in maintaining the system's integrity.

7 DISCUSSION

The field of SoS engineering research has experienced significant growth in recent years, with some parallel investigation on SoIS. While the SoIS engineering has presented opportunities, it has also introduced new challenges - and accountability is a significant one. The interdisciplinary nature of accountability requires an effort from researchers and practitioners acting in several areas.

7.1 Implications for Researchers

The introduction of accountability as a quality requirement has opened up new research directions. To effectively embed accountability, researchers must delve deeper into its multifaceted nature. We present some aspects that researchers should consider when exploring the implications of accountability.

Ethical Considerations: Research into accountability in system design, implementation, and use presents significant ethical challenges. Decisions at each stage can profoundly impact individuals, communities, and society. Common concerns, such as data privacy and algorithmic biases, underscore the importance of prioritizing user consent and fairness in system operations. Ethical frameworks and guidelines derived from such research are essential for guiding both researchers and practitioners through these challenges.

The direct application of these ethical considerations in real-world systems demonstrates their practical importance. This alignment also highlights the need for continuous dialogue between ethical theory and practical system development within SoIS, ensuring that ethical standards evolve in step with technological advancements.

Human-Centered Design: Ensuring accountability requires a human-centered approach. For instance, the research revealed that user engagement in accountability processes helps in enhancing system trustworthiness and user satisfaction. By focusing on user-centered design principles, developers can create more effective interfaces and functionalities that facilitate easier monitoring and management of accountability measures. Moreover, the inclusion of user feedback mechanisms is paramount. These mechanisms not only support the adaptation of systems to real-world needs but also foster a sense of ownership and responsibility among users, crucial for the long-term success of SoIS. Researchers must focus on understanding end-users' perspectives, needs, and concerns to develop constituent system that are usable, accessible, and trustworthy. Integrating human factors research and user experience studies into the design and evaluation of accountable software can enhance user acceptance and hence adoption.

Governance and Regulation: The incorporation of accountability may need new governance structures and regulations. As we have identified in this SMS, the need for enhanced governance structures is crucial in managing the interdependencies within SoIS. The governance of these systems must be agile enough to adapt to rapid technological changes while ensuring that accountability is maintained. This requirement for flexibility in governance structures echoes the challenges we have highlighted in Section 6, where the dynamic nature of SoIS often influences accountability measures. Researchers must explore how accountability requirements intersect with legal and regulatory frameworks and assess the potential challenges and opportunities that arise from compliance. Additionally, they may investigate the role of standardization organizations, policymakers, and industry stakeholders in shaping accountable practices in business process.

Long-term Sustainability: The successful integration of accountability requires considering the long-term sustainability [53] when thinking about the constituent systems themselves. Researchers must explore how accountability measures can adapt to evolving technological advances and changing societal needs. Such includes the scalability of accountability mechanisms and the potential trade-offs between accountability, performance, and innovation.

Evaluation and Metrics: The evaluation metrics are crucial for guiding systems engineers in making informed decisions aimed at enhancing service quality. Results emphasize the importance of accountability in reducing access policy violations in system, highlighting that rigorous and clear evaluation metrics are essential for effective implementation. By establishing systematic and precise metrics, researchers can provide a structured approach to evaluating the performance and impact on systems, thereby facilitating continuous improvement in system design and implementation. This systematic evaluation is critical to ensure that accountability measures are not only implemented but also effective in promoting responsible and transparent practices within systems engineering.

Security and Resilience: As accountability measures are integrated into constituent systems, researchers must also address potential security implications. The introduction of accountability mechanisms should not inadvertently introduce new vulnerabilities that could be exploited by malicious actors. Ensuring that accountable constituent systems are robust and resilient to cyber-threats is of paramount importance.

7.2 Implications for Practitioners

For practitioners, the emphasis on accountability implies a shift in the way constituent systems are designed and developed in SoIS. We present some aspects that developers should consider when exploring the implications of accountability.

Auditing and Logging: Developers should design systems with comprehensive auditing and logging capabilities. Keeping a detailed record of SoIS actions, user interactions, and decisions made by the constituent systems can help in post-incident analysis, compliance checks, and identifying areas for improvement. For example, development of logging systems that records all user actions, system state changes, and automated decisions using strategies to store and analyze logs in real-time. This setup enables detailed post-incident analysis and facilitates compliance audits.

User-Centric Design: Creating accountable softwares involves understanding the needs and expectations of end-users. Developers should involve end-users in the design process, gather feedback, and prioritize user-centric design principles to build systems that align with users' values and preferences. For example, use of platforms to create interactive user interface prototypes. Conducting usability tests frequently with focus groups representing the target audience ensures that the system design aligns with the needs and expectations of end-users.

Ethical Considerations: Accountability investigation must go beyond meeting legal requirements; it should also encompass ethical considerations. Software engineers should engage in ethical discussions about the potential consequences of their systems and strive to build technologies that align with ethical principles and societal values. For example, the development of ethical checklists to be used during the design and development phases of the software. This checklist can include questions to ensure that the system does not inadvertently cause harm, promotes inclusion and diversity, and operates fairly and transparently.

Continuous Testing and Monitoring: Accountability requires ongoing scrutiny. Developers should implement continuous testing and monitoring practices to ensure that the software functions as intended and remains accountable throughout its lifecycle. This includes periodic code reviews, security audits, and performance assessments. For example, implementation of a continuous integration pipeline using tools, which includes automated regression and performance tests with each code update.

Documentation and Transparency: Transparent systems facilitate accountability. Developers should document the design, implementation, and decision-making processes thoroughly. Clear and accessible documentation helps stakeholders, including support to users and regulators understand how the system operates and how accountability is ensured. For example, development of tools to automatically document a SoIS, providing a clear view of how constituent systems. This facilitates understanding of system operations for regulators and stakeholders.

Data Privacy and Security: Accountability goes hand in hand with data privacy and security. Software engineers must prioritize implementing robust data protection measures, encryption techniques, and access controls to safeguard sensitive information. Data breaches and leaks can have severe consequences for both the users and the organization responsible for the system. For example, develpment of end-to-end encryption techniques to sensitive data and use multi-factor authentication to access the system. Conducting regular vulnerability assessments helps in the identification and mitigation of potential security threats.

We emphasize that our research thoroughly investigates key aspects of enhancing accountability in software development environments, detailed in previous sections. For example, software engineers must engage in discussions about the ethical implications of their systems, striving to develop technologies that align with ethical principles and societal values. Involving end-users in the design process is crucial. Understanding their needs and expectations ensures that the developed software aligns with user values and preferences, which is important for creating accountable systems. Designing systems with robust auditing and logging capabilities is essential. Such features maintain records that aid in post-incident analysis, compliance checks, and identification of areas for improvement. Lastly, comprehensive documentation of the design, implementation, and decision-making processes is imperative. This transparency helps stakeholders understand the system's operations and reinforces accountability.

Thus, the inclusion of accountability in constituent systems engineering is not just important, but necessary. In this paper, we present challenges for researchers and practitioners based on a prescriptive approach by performing an SMS to discern recurring themes and concerns related to the topic. As the complexity and pervasiveness of SoIS continue to increase, the importance of accountability cannot be overstated. The research yields significant insights and a research agenda into accountability. The following section relates threats to vaility of the research.

8 THREATS TO VALIDITY

This study is susceptible to threats that may influence its validity. This section examines the main potential threats to validity, as suggested by Petersen *et al.* [54]. For consensus, we consulted with three researchers with 20 years of experience in research on SoS and empirical software engineering, including conducting SMS.

Descriptive validity relates to how accurately and objectively the observations are described. The researcher (first author) designed a data collection form to support the execution of the protocol, the recording of decisions made, and the data extraction process. This form played a crucial role in facilitating protocol execution, recording decisions, and guiding the data extraction process. The involvement of three researchers provided oversight, ensuring the reliability and precision of the observational data. This approach mitigated threats associated with the potential introduction of bias during data collection.

Theoretical validity was addressed through the implementation of a snowballing technique during this SMS. This technique complemented the initial search process by incorporating studies identified through full-text reading, enhancing the inclusiveness of the review. To mitigate potential personal biases, the study was conducted under the supervision of three experienced researchers who actively contributed to the final report as part of a PhD Thesis [12]. This approach mitigated threats in cases where selected studies discussed accountability without explicit mention of SoIS, inclusion decisions were based on the relevance of these studies to the investigated topic and their applicability within the SoIS context.

Generalizability validity covers constraints due to the use of search engines in this SMS. To mitigate associated threats, we adhered to the insights provided by Kitchenham *et al.* [22], demonstrating the coverage based on five search engines within the domains of Software Engineering and IS. Additionally, to mitigate generalizability, the first author refrained from implementing any filters related to publication years during the search process. This deliberate choice contributes to a more comprehensive inclusion of relevant literature, bolstering the study's potential applicability across various timeframes

Interpretative validity refers to the trustworthiness and credibility of the interpretations drawn from the collected data and findings. We addressed it by implementing strict study selection criteria and consulting with three researchers for consensus. However, potential bias may have been introduced due to the use of specific keywords related to accountability and responsibility in our search strategy. Identifying suitable alternatives for these terms was challenging, and we acknowledge the potential limitations in our search results. Another threat concerns the potential misclassification of studies that may not explicitly pertain to the SoIS. However, the decision was deemed appropriate as accountability was depicted in decentralized systems with close applicability to SoIS.

Repeatability depends on a comprehensive and transparent report of the research process. To ensure this, the first author, who conducted the study, ran the search string, used deterministic databases, and employed free software to perform this SMS. The approach followed a step-by-step procedure meticulously designed for easy replication. This not only enhances the repeatability of the study but also provides clarity and guidance for future researchers looking to replicate or build upon this work.

9 CONCLUSION

Designing business-oriented complex systems, such as SoIS, requires a dedicated commitment to accountability. Our study delves into the complex interplay between accountability and the engineering challenges of constituent systems within business environments. Based on an SMS, we have surveyed the current state-of-the-art on accountability within these systems and also pinpointed research challenges. These findings lay a foundation for future explorations, aiming to enhance the effectiveness and integrity of SoIS. Concerning to primary contribution, it lies in the detailed characterization of SoIS accountability. By systematically reviewing the literature and synthesizing insights from primary studies, we have developed a categorization that clarifies the distinction between accountability and responsibility. This categorization emphasizes the role of individuals in promoting accountability, explores the integration of accountability measures with ICT, and demonstrates how accountability interacts with governance structures and competitive advantages. Furthermore, it addresses data management in complex systems, enhancing our understanding of these dynamics.

Moreover, the findings from review in RQ1 are organized over the need for accountability evaluation based on three categories: engagement, management, and regulation. This tripartite approach not only clarifies the pathways through which accountability can be embedded the software development processes but also ensures that these processes foster transparency, trust, and ultimately, success. This perspective is relevant for researchers and practitioners to effectively tackle the complexities inherent in SoIS and underscores the importance of accountability in enhancing the robustness and reliability of software systems.

Regarding RQ2, a comprehensive examination of challenges in the topic was provided. By deepening the understanding of accountability within SoIS, our study assists in addressing complex system engineering challenges and fosters innovation throughout the software lifecycle. This overview focuses on key aspects within the accountability evaluation categories, encompassing frameworks, models, and metrics, as well as based on seven challenges. Furthermore, a discourse extends to the interdisciplinary nature of constituent systems, analyzing them from the lenses of both researchers and practitioners. This perspective aims to consolidate knowledge on accountability within SoIS, facilitating the expansion of the body of knowledge on the field and inviting further inquiry to inspire innovative solutions.

Future work will explore new accountability evaluation strategy, develop advanced evaluation tools, and conduct empirical studies to validate and refine a framework to do so. This will not only refine the implementation of SoIS accountability but also enhance the effectiveness and efficiency of these systems in real-world applications. This endeavor aims at optimizing end-user interaction with SoIS, and invites the academic community to explore innovative solutions that can overcome the existing and emerging challenges in SoS within software engineering.

ARTIFACT AVAILABILITY

The SMS dataset is available online [55].

10 ACKNOWLEDGMENTS

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001, CNPq (Proc. 316510/2023-8), FAPERJ (Proc. 211.583/2019), and UNIRIO (PPQ 2022 and 2023).

REFERENCES

[1] Ferreira, F. H. C. et al., A framework for the design of fault-tolerant systems-of-systems. *Journal of Systems and Software* 211 (2024), pp. 112010. ISSN: 0164-1212. doi: 10.1016/j.jss.2024.112010.

[2] Imamura, M. et al., A Catalog of Heuristics to Support the Design of Systems-of-Systems. *iSys - Brazilian Journal of Information Systems* 17.1 (Mar. 2024), pp. 1:1–1:26. doi: 10.5753/isys.2024.3774.

[3] Imamura, M. et al., System-of-Systems Reliability: An Exploratory Study in a Brazilian Public Organization. *Proceedings of the XVII Brazilian Symposium on Information Systems.* SBSI '21. Uberlândia, Brazil: Association for Computing Machinery, 2021. ISBN: 9781450384919. doi: 10.1145/3466933.3466954.

[4] Imamura, M. et al., Towards a Catalog of Heuristics for the Design of Systems-of-Systems. *Proceedings of the XIX Brazilian Symposium on Information Systems.* SBSI '23. Maceió, Brazil: Association for Computing Machinery, 2023, pp. 128–135. ISBN: 9798400707599. doi: 10.1145/3592813.3592897.

[5] Ferreira, F. H. C., Nakagawa, E. Y., and Santos, R. P., Towards an understanding of reliability of software-intensive systems-of-systems. *Information and Software Technology* 158 (2023), pp. 107186. ISSN: 0950-5849. doi: 10.1016/j.infsof.2023.107186.

[6] Maier, Mark W., Architecting principles for systems-of-systems. *Systems Engineering: The Journal of the International Council on Systems Engineering* 1.4 (1998), pp. 267–284.

[7] Fernandes, J. et al., PIS: Interoperability and Decision-Making Process—A Review. *The Evolution of Pervasive Information Systems.* Ed. by Kirsch Pinheiro, Manuele et al. Cham: Springer International Publishing, 2023, pp. 157–190. doi: 10.1007/978-3-031-18176-4_7.

[8] Saleh, M. and Abel, M., System of Information Systems to Support Learners (A Case Study at the University of Technology of Compiègne). *Behaviour & Information Technology* 37.10 (2018). Publisher: Taylor & Francis, pp. 1097–1110. doi: 10.1080/0144929X.2018.1502808.

[9] Graciano Neto, V. V. et al., Expanding Frontiers: Settling an Understanding of Systems-of-Information Systems. *CoRR* abs/2103.14100 (2021). arXiv: 2103.14100. URL: https://arxiv.org/abs/2103.14100.

[10] Fernandes, J. et al., A conceptual model for systems-of-information systems. *2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI).* IEEE. 2019, pp. 364–371. doi: 10.1109/IRI.2019.00063.

[11] Cordeiro, F. P. and Santos, R. P., Systems Thinking as a Resource for Supporting Accountability in System-of-Information-Systems: Exploring a Brazilian School Case. *2019 IEEE/ACM 7th International Workshop on Software Engineering for Systems-of-Systems (SESoS) and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (WDES).* Canada, 2019, pp. 42–49. doi: 10.1109/SESoS/WDES.2019.00014.

[12] Cordeiro, F., "Accountability Evaluation in Systems-of-Information Systems Based on Systems Thinking". PhD thesis. Rio de Janeiro, Brazil: UNIRIO, 2021. doi: 10.13140/RG.2.2.35828.22402.

[13] Pearson, S., Accountability in Cloud Service Provision Ecosystems. *Nordic Conference on Secure IT Systems.* Springer, 2014, pp. 3–24. doi: 10.1007/978-3-319-11599-3_1.

[14] Feltus, Christophe, Petit, Michaël, and Dubois, Eric, Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study. *Proceedings of the first ACM workshop on Information security governance.* 2009, pp. 23–32.

[15] Bissland, James H, Accountability gap: Evaluation practices show improvement. *Public Relations Review* 16.2 (1990), pp. 25–35.

[16] AccountAbility, *AA1000 Stakeholder Engagement Standard*. AccountAbility London, 2015.

[17] Teixeira, P. G. et al., The Status Quo of Systems-of-Information Systems. *2019 IEEE/ACM 7th International Workshop on Software Engineering for Systems-of-Systems (SESoS) and 13th Workshop on Distributed Software Development, Software Ecosystems and Systems-of-Systems (WDES)*. IEEE, 2019, pp. 34–41. doi: 10.1109/SESoS/WDES.2019.00013.

[18] Gortmaker, J., Janssen, M., and Wagenaar, R. W., Accountability of Electronic Cross-agency Service-delivery Processes. *International Conference on Electronic Government*. Springer, 2005, pp. 49–56. doi: 10.1007/11545156_5.

[19] Feigenbaum, J., Jaggard, A. D., and Wright, R. N., Towards a Formal Model of Accountability. *Proceedings of the 2011 New Security Paradigms Workshop*. 2011, pp. 45–56. doi: 10.1145/2073276.2073282.

[20] Vance, A., Lowry, P. B., and Eggett, D., Using Accountability to Reduce Access Policy Violations in Information Systems. *Journal of Management Information Systems* 29.4 (2013), pp. 263–289. doi: 10.2753/MIS0742-1222290410.

[21] Cordeiro, F. et al., Towards an accountability suggestion map for supporting information systems management based on systems thinking. *Proceedings of the 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*. IEEE. 2020, pp. 295–300. doi: 10.1109/IRI49571.2020.00049.

[22] Kitchenham, B. A., Budgen, D., and Brereton, P., *Evidence-based Software Engineering and Systematic Reviews*. Vol. 4. CRC Press, 2015.

[23] Inocencio, T. J. et al., Emergent Behavior in System-of-Systems: A Systematic Mapping Study. *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*. 2019, pp. 140–149. doi: 10.1145/3350768.3350779.

[24] Silva, K. C., Horita, F., and Graciano Neto, V. V., Bring Us MacGyver Predictor: Towards a Deep Learning-Based Mechanism to Design Emergent Behaviors in Systems-of-Systems. *Proceedings of the XXXIII Brazilian Symposium on Software Engineering*. 2022, pp. 299–304. doi: 10.1145/3555228.3555265.

[25] Graciano Neto, V. V. et al., Model-based Engineering & Simulation of Software-intensive Systems-of-Systems: Experience Report and Lessons Learned. *Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings*. 2018, pp. 1–7. doi: 10.1145/3241403.3241432.

[26] Nowicki, D., Randall, W. S., and Gorod, A., A framework for performance based logistics: A system of systems approach. *2010 International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2010*. 2010, pp. 681–692. doi: 10.1109/ICUMT.2010.5676562.

[27] Zou, J., De Vaney, C., and Wang, Y., A Meta-modeling Framework to Support Accountability in Business Process Modeling. *Information Systems: Modeling, Development, and Integration*. 2009, pp. 539–550. doi: 10.1007/978-3-642-01112-2_54.

[28] Singh, J. et al., Accountability in the IoT: Systems, Law, and Ways Forward. *Computer* 51.7 (2018), pp. 54–65. doi: 10.1109/MC.2018.3011052.

[29] Bhattacharya, S. and P., R., Accountability Issues in Multihop Message Communication. *Proceedings 1999 IEEE Symposium on Application-Specific Systems and Software Engineering and Technology*. Mar. 1999, pp. 74–81. doi: 10.1109/ASSET.1999.756754.

[30] Janssen, M., Adaptability and Accountability of Information Architectures in Interorganizational Networks. *Proceedings of the 1st International Conference on Theory and Practice of Electronic Governance*. Macao, China, 2007, pp. 57–64. doi: 10.1145/1328057.1328072.

[31] Gateau, B. et al., An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504. *2008 Second International Conference on Research Challenges in Information Science*. 2008-06-03, pp. 35–44. doi: 10.1109/RCIS.2008.4632091.

[32] Lourenço, R. P. and Serra, L., An Online Transparency for Accountability Maturity Model. *International Conference on Electronic Government*. Springer, 2014, pp. 35–46. doi: 10.1007/978-3-662-44426-9_3.

[33] Rogerson, S., Fairweather, N. B., and Wu, X., Being Ethical in Developing Information Systems: An Issue of Methodology or Maturity in Judgment? (2001). doi: 10.1109/HICSS.2001.927150.

[34] Chen, Y. C. et al., Cross-boundary E-government Systems: Determinants of Performance. *Government Information Quarterly* 36.3 (2019-07-01), pp. 449–459. doi: 10.1016/j.giq.2019.02.001.

[35] Singh, J., Cobbe, J., and Norval, C., Decision Provenance: Harnessing Data Flow for Accountable Systems. *IEEE Access* 7 (2019), pp. 6562–6574. doi: 10.1109/ACCESS.2018.2887201.

[36] Gottschalk, P., Descriptions of Responsibility for Implementation: A Content Analysis of Strategic Information Systems/Technology Planning Documents. *Technological Forecasting and Social Change* 68.2 (2001). Publisher: Elsevier, pp. 207–221. doi: 10.1016/S0040-1625(00)00084-6.

[37] Eriksén, S., Designing for Accountability. *Proceedings of the Second Nordic Conference on Human-Computer Interaction*. 2002, pp. 177–186. doi: 10.1145/572020.572041.

[38] Campagnolo, G. M. and Jacucci, G., Designing the Accountability of Enterprise Architectures. *IFIP International Conference on Human Choice and Computers*. Springer, 2006, pp. 355–366. doi: 10.1145/572020.572041.

[39] Chen, C. C, Liu, J. Y.h, and Chen, H., Discriminative effect of user influence and user responsibility on information system development processes and project management. *Information and Software Technology* 53.2 (2011), pp. 149–158.

[40] Zhang, C. and Hu, B., Discussions about Perfecting Chinese System of Official Accountability for Mining Disasters. *Proceedings of International Conference on Information Systems for Crisis Response and Management (ISCRAM)*. IEEE, 2011, pp. 70–75. doi: 10.1109/ISCRAM.2011.6184081.

[41] Shires, M. A. and Craig, M. S., Expanding Citizen Access and Public Official Accountability Through Knowledge Creation Technology: One Recent Development in E-democracy. *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE, 2003, 10–pp. doi: 10.1109/HICSS.2003.1174321.

[42] Madon, S., Krishna, S., and Michael, E., Health Information Systems, Decentralisation and Democratic Accountability. *Public Administration and Development* 30.4 (2010). Publisher: Wiley Online Library, pp. 247–260. doi: 10.1002/pad.571.

[43] Stahl, B. C., Information Technology, Responsibility, and Anthropology. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. IEEE, 2002, 10–pp. doi: 10.1109/HICSS.2002.994367.

[44] Cain, P., Information, Not Technology, Is Essential to Accountability: Electronic Records and Public-sector Financial Management. *The Information Society* 17.4 (2001). Publisher: Taylor & Francis, pp. 247–258. doi: 10.1080/019722401753330841.

[45] Gajanayake, R., Iannella, R., and Sahama, T., Privacy by Information Accountability for E-health Systems. *2011 6th International Conference on Industrial and Information Systems*. IEEE, 2011, pp. 49–53. doi: 10.1109/ICIINFS.2011.6038039.

[46] Mutula, S. and Wamukoya, J. M., Public Sector Information Management in East and Southern Africa: Implications for FOI, Democracy and Integrity in Government. *International Journal of Information Management* 29.5 (2009). Publisher: Elsevier, pp. 333–341. doi: 10.1016/j.ijinfomgt.2009.04.004.

[47] Gajanayake, R., Iannella, R., and Sahama, T., Sharing with Care: An Information Accountability Perspective. *IEEE Internet Computing* 15.4 (2011). Publisher: IEEE, pp. 31–38. doi: 10.1109/MIC.2011.51.

[48] Anagnostopoulos, D., Rutledge, S., and Bali, V., State Education Agencies, Information Systems, and the Expansion of State Power in the Era of Test-Based Accountability. *Educational Policy* 27.2 (2013). Publisher: Sage Publications Sage CA: Los Angeles, CA, pp. 217–247. doi: 0.1177/0895904813475.

[49] Pearson, S., Toward Accountability in the Cloud. *IEEE Internet Computing* 15.4 (2011). Publisher: IEEE, pp. 64–69. doi: 10.1109/MIC.2011.98.

[50] Zou, J. and Pavlovski, C. J., Towards Accountable Enterprise Mashup Services. *IEEE International Conference on e-Business Engineering (ICEBE'07)*. IEEE, 2007, pp. 205–212. doi: 10.1109/ICEBE.2007.12.

[51] Khadraoui, A. and Feltus, C., Service specification and service compliance: How to consider the responsibility dimension? *Journal of Service Science Research* 4 (2012). Publisher: Springer, pp. 123–142.

[52] Von Bertalanffy, L., The history and status of general systems theory. *Academy of management journal* 15.4 (1972), pp. 407–426.

[53] Lago, P., The Digital Society Is Already Here – Pity It Is 'Unsustainable'. *Connected World - Insights from 100 Academics on How to Build Better Connections*. Ed. by Vermeulen, Ivar. Amsterdam: VU University Press, 2023, pp. 55–58. URL: https://vuuniversitypress.com/product/connected-world.

[54] Petersen, K., Vakkalanka, S., and Kuzniarz, L., Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. *Information and Software Technology* 64 (2015), pp. 1–18. doi: 10.1016/j.infsof.2015.03.007.

[55] Cordeiro, F. et al., *Supplementary Material - Investigating Accountability in Systems-of-Information Systems*. https://doi.org/10.5281/zenodo.10251673. Dec. 2023.