IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 January 2024, accepted 28 January 2024, date of publication 1 February 2024, date of current version 8 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3360864

SURVEY

On the Evaluation of Privacy Impact Assessment and Privacy Risk Assessment Methodologies: A Systematic Literature Review

SAMUEL WAIRIMU[1], LEONARDO HORN IWAYA[1], (Member, IEEE), LOTHAR FRITSCH[1,2], AND STEFAN LINDSKOG[1]

[1]Privacy and Security (PriSec) Research Group, Department of Mathematics and Computer Science, Karlstad University, 651 88 Karlstad, Sweden
[2]Department of Computer Science, Faculty of Technology, Art and Design, Oslo Metropolitan University, 0130 Oslo, Norway

Corresponding author: Samuel Wairimu (samuel.wairimu@kau.se)

This work was supported in part by Region Värmland, Sweden, through the Digital Health Innovation (DHINO) Project under Grant RUN/220266; and in part by the Vinnova via the DigitalWell Arena Project under Grant 2018-03025.

ABSTRACT Assessing privacy risks and incorporating privacy measures from the onset requires a comprehensive understanding of potential impacts on data subjects. Privacy Impact Assessments (PIAs) offer a systematic methodology for such purposes, which are closely related to Data Protection Impact Assessments (DPIAs), particularly outlined in Article 35 of the General Data Protection Regulation (GDPR). The core of a PIA is a Privacy Risk Assessment (PRA). PRAs can be integrated as part of full-fledged PIAs or independently developed to support PIA processes. Although these methodologies have been identified as essential enablers of privacy by design, their effectiveness has been criticized because of the lack of evidence of their rigorous and systematic evaluation. Hence, we conducted a Systematic Literature Review (SLR) to identify published PIA and PRA methodologies and assess how and to what extent they have been scientifically validated or evaluated. We found that these methodologies are rarely evaluated for their performance in practice, and most of them have only been validated in limited studies. Most validation evidence is found with PRA methodologies. Of the evaluated methodologies, PIAs were the most evaluated, where case studies were the predominant evaluation method. These evaluated methodologies can be easily transferred to an industrial setting or used by practitioners, as they provide evidence of their use in practice. In addition, the findings in this study can be used to inform researchers of the current state-of-the-art, and practitioners can understand the benefits and current limitations of the methodologies and adopt evidence-based practices.

INDEX TERMS Privacy impact assessment, data protection impact assessment, general data protection regulation, privacy by design, privacy, review, threat modeling, privacy risks, validity, maturity.

I. INTRODUCTION

As our digital society advances, with a myriad of highly ubiquitous and personalized systems, technology offers great promise for businesses and consumers. However, these benefits are often accompanied by significant threats to people's privacy rights. For this reason, researchers and policymakers have stressed the need for "privacy by design" approaches for many years [1], taking privacy into account throughout the entire engineering process. This concern for privacy in the face of new technology development has also been enshrined in several legal frameworks. As of 2023, 162 countries have enacted national privacy laws [2].

Today, the EU General Data Protection Regulation (GDPR) is regarded as the most influential privacy regulation. Among its provisions, the EU GDPR has not only integrated the notion of privacy by design and by default (Art. 25 GDPR [3]) but also mandated the performance of Privacy Impact Assessments (PIAs) for high-risk systems, which in the GDPR are particularly called Data Protection Impact

The associate editor coordinating the review of this manuscript and approving it for publication was Sedat Akleylek.

Assessments (DPIAs) (Art. 35 GDPR [3]). PIAs come from a long history of legal practice and research [4], having been defined by Wright as, *"a methodology for assessing the impacts on the privacy of a project, policy, program, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impact"* [5]. Full-fledged PIA methodologies often adopt a risk-based approach, incorporating methods for Privacy Risk Assessments (PRA) or Privacy Threat Modeling (PTM) as core components of the complete assessment, documentation, and reporting processes [6]. For this reason, PIAs have also been heralded as robust solutions for privacy by design [7].

However, the effectiveness of such methodologies has been criticized due to the lack of evidence on the rigorous and systematic evaluation of existing PIAs [8], [9]. Common issues reported by practitioners are that PIAs are overly complicated and time-consuming [10], steps are generic and abstract [11], and determining privacy risks is seen as vague and dependent on the skills and experience of the person performing the assessment [12], often in shortage of historic data [13]. Such drawbacks can also be extended to PRA and PTM methods since they can act as sub-components of PIAs as well as for other privacy engineering techniques [14].

To better understand the state-of-the-art, we conduct a Systematic Literature Review (SLR) focusing on scientific evidence from studies that propose and validate or evaluate PIA and PRA methodologies. To do so, this SLR follows well-established guidelines [15], [16], enabling the systematic and exhaustive gathering of studies and synthesis of the body of knowledge on the topic. The systematic nature of SLRs also allows this study to be reproduced or extended by other researchers in the future.

As a result, this SLR offers the following contributions:

i. an in-depth synthesis of the existing methodologies for PIAs and PRAs that are supported by empirical evidence regarding their validation or evaluation;
ii. a detailed discussion of the methods used for the validation and evaluation of PIA and PRA methodologies; and,
iii. a critical appraisal of empirical studies that have evaluated PIA and PRA methodologies.

These contributions, in turn, benefit many stakeholders involved in the development and performance of PIAs and PRAs. Researchers can better understand the state-of-the-art methodologies and pathways for future work on the topic. Practitioners responsible for carrying out PIAs, PRAs, and PTMs in practice can further understand the benefits and limitations of the methodologies and select better approaches. Policymakers can also acquire further insights, helping them to define guidelines better, consult with organizations, and recommend evidence-based practices.

The remainder of this article is structured as follows: Section II establishes the context of this research. Section III presents the related work. Section IV discusses the research methodology employed in the systematic literature review. Section V presents the main findings of this study by providing the analyses and classification of the identified methodologies. Section VI provides the discussion - here, we outline the summary of results and research directions. Section VII discusses the limitations of the study. Section VIII concludes the paper.

II. BACKGROUND

A. TERMINOLOGIES

As previously mentioned, a PIA is mandated under Art.35 of the GDPR as a Data Protection Impact Assessment (DPIA) for assessing high-risk systems concerning the rights and freedoms of natural persons when processing personal data. While the GDPR uses the term DPIA, the term PIA can be utilized to signify the same concept [17], [18]. However, despite their interchangeable use, it is important to recognize the differences between the two terminologies.

The development of the term PIA and its processes, including usage, is predominantly attributed to anglophone countries, specifically the US, New Zealand, Australia, and Canada [4]. Fundamentally, a PIA is prioritized as a process and focuses on multiple aspects of privacy rather than data protection [19]. We refer the reader to Clarke's work on other privacy aspects [20]. With the proposal and implementation of the EU GDPR, the term DPIA emerged under Art.35. A DPIA is a legal requirement for data protection under GDPR. Albeit the introduction of the DPIA concept, researchers in the EU had already established the concept of PIAs,[1] for instance, in [21] and [22]. In addition, in the guidelines for conducting a DPIA, Working Party 29 [18] points to published PIAs, such as CNIL PIA [17], PIA for Radio Frequency Identification [23], and the UK PIA [24] as examples of existing EU Data Protection Impact Assessments. In this study, we use the term PIA with the acknowledgment that the term could be used in other contexts to refer to the DPIA concept as well as to cover jurisdictions outside the EU.

PIAs play a fundamental role in assessing and addressing privacy risks in the development of new projects or systems that process personal data [14], [25]. As mentioned in the Introduction, a full-fledged PIA can incorporate a Privacy Risk Assessment (PRA) or Privacy Threat Modeling as core components of the PIA process. During the PIA process, a PRA aids in the analysis and evaluation of privacy risks identified early in a system under scrutiny [26]. Technically, the impact of privacy risks is estimated using a privacy risk assessment. A Privacy Threat Model (PTM) can also supplement a PIA process, as identified in [27]. A PTM aids in the identification and enumeration of potential privacy threats [28]. The identified threats are then treated based on appropriate controls. Example of a Privacy Threat Model and Privacy Risk Assessment that can supplement a PIA process is LINDDUN [29] and PRIAM [22], respectively.

[1] Note that the use of PIA predates the concept of a DPIA.

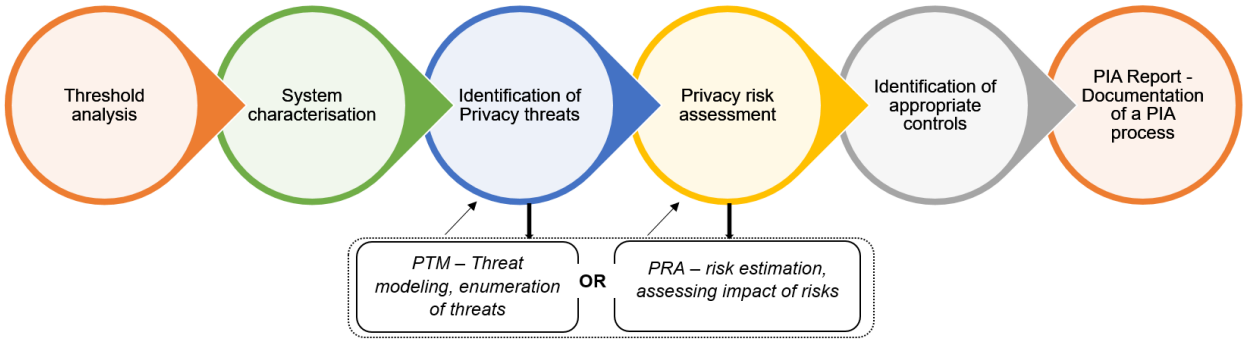

FIGURE 1. Overview of a generalized PIA process, highlighting the core components of a PIA, i.e., PTM or a PRA.

B. PIA PROCESS

To facilitate an understanding of the PIA process, as well as the core components that are essential for establishing a risk-based approach, we illustrate a generalized PIA process inspired by works from [21] and [30] in Fig. 1. Given the context and purpose of processing personal data, a data controller can assess whether the processing will result in high risk; hence, a threshold analysis should be performed [31].

The threshold analysis provides an overview of whether a full-blown PIA process is necessary [30], [31]. If a PIA process is necessary, the system is comprehensively described to model its behavior and characteristics. System description is usually done in the form of Data Flow Diagrams (DFDs), enabling the visualization of how personal data flows within a system and sub-systems, which is suitable for identifying potential privacy threats. At the core of a rigorous PIA process is a Privacy Risk Assessment (PRA), which is crucial in assessing and addressing privacy risks as well as privacy harms [21], [22], [26], [27], [32]. That is, to assess the impact of privacy on the rights and freedoms of natural persons, a privacy risk assessment component is fundamental, as this is the main goal. In addition to Privacy Risk Assessment, a Privacy Threat Model (PTM) can also be integrated into a PIA process [27] to complete the process, supporting the exhaustive enumeration of privacy threats and, optionally, the selection of appropriate controls to address the threats (see Fig. 1).

Considering that a full-fledged PIA can incorporate a Privacy Risk Assessment or a Privacy Threat Modeling method as part of the assessment [22], scholars have proposed independent Privacy Risk Assessments that can complement PIAs. Privacy Risk Assessments, including Privacy Threat Models, can seamlessly complement a PIA process, however, there is a risk of introducing an overhead [27]. Following this process, the identified risks are prioritized and mitigated by selecting appropriate controls. The PIA process must be documented, and the PIA report is generated and maintained as a living document during system or project development [26].

It is worth noting that several studies have proposed other hybrid methodologies, i.e., PIA methodologies that have a security assessment component [33] and Privacy Threat Models that consider security threat modeling as [34], [35]. Technically, these approaches combine two different methodologies or components of a methodology to develop a more comprehensive solution for assessing security and privacy risks.

III. RELATED WORK

We did not find a survey on the validity or maturity of PIA and PRA methods. To the best of our knowledge, this is the only SLR on the evaluation of privacy impact and privacy risk assessment methodologies (further details are provided in Section IV-A1). Nevertheless, in our search for related work, some studies have provided useful insights into PIA and threat modeling methodologies. However, no known studies have conducted systematic reviews of privacy risk assessment.

Recently, Georgiadis and Poels [36] reviewed existing PIA methodologies that could be used in the assessment of privacy risks in the context of big data analytics. They identified 13 methodologies, but most were from data protection authority pages, and they assessed them in terms of Privacy Touch Points, i.e., privacy and data protection risks. Xiong and Lagerström [37] performed an SLR to provide an overview of threat modeling approaches. While they did not focus on PTMs alone (but also on methods that assess security threats), they analyzed whether the threat models had been assessed theoretically or empirically also considering the used methods. The authors mainly concluded that the methods used vary.

Similarly, Tuma, Calikli, and Scandariato [38] conducted a review of the existing threat modeling approaches, and, as in the work of [37], the identified methodologies focused not only on PTMs but also on disparate threat analysis techniques. The authors further investigated how the methodologies were validated, where they provided an approach, domain, and tool, and how the method was empirically tested. The authors pointed out "the immaturity of empirical

TABLE 1. Phases and activities adopted in this SLR [15].

Phase	Activities
Plan	(i.) Determining the need for the SLR and (ii.) Designing the review protocol
Conduct	(i.) Identification of research, (ii.) Selection of primary studies, (iii.) Quality assessment, (iv.) Data extraction and (v.) Data Synthesis
Report	(i.) Communicating the results of the SLR

research in the software engineering community'' given the methods of validation used, for instance, experiments.

Given that research has been conducted in areas concerning PIA and threat analysis, existing studies focus on identifying non-scientific sources and disparate threat modeling methods. However, unlike in this SLR, they did not survey and analyze existing PIA (in scientific publications), PRAs, or PTMs. In addition, they do not provide a taxonomy of methodologies that have not been tested through limited experiments (validated) or that have been put into practice in real-world settings (evaluated). Furthermore, the related work does not provide an account of the studies' methodological quality in terms of their qualitative or quantitative research designs and conduction.

IV. METHODOLOGY

This study employed an SLR methodology to compile and assess research evidence concerning the evaluation and validation methods of reported PIA and PRA methodologies. Essentially, the SLR methodology complies with a clearly defined and rigorous sequence of methodological steps based on a pre-established protocol [39]. Therefore, the approach adopted in this study adheres to the well-known guidelines outlined in the Procedures for Performing Systematic Reviews by Kitchenham [15]. According to the guidelines, the review process consists of three main phases, each encompassing several activities. These phases are detailed in Table 1, along with their constituent activities.

A. PLANNING THE REVIEW

1) DETERMINING THE NEED FOR THE SLR

This study aims to review the reported PIA and PRA approaches available in the scientific literature and synthesize the available evidence by classifying these methods in terms of whether they have been evaluated or validated and the methods used for either validating or evaluating the approaches. Although many PIAs have been proposed in recent years, most come without strong scientific evidence of their reliability other than in terms of limited validation and comparative analysis. For example, the works of [30], [40], and [41] compare approaches regarding the associated legal frameworks, scope, and depth of existing PIAs. In addition, from a preliminary search, there have been no systematic studies reporting approaches that have been validated or evaluated and the methods used. Hence, this topic remains largely unexplored, as comprehensive research and analysis are yet to be undertaken that could report state-of-the-art concerning the validation and evaluation of PIAs and PRAs.

2) DESIGNING THE REVIEW PROTOCOL

Considering that the methodology follows the procedure for performing systematic reviews [15], we ensured that the preparation and writing of the protocol adhered to the same established guidelines. Furthermore, we incorporated the preferred reporting items for systematic reviews and meta-analyses for protocols 2015 (PRISMA-P 2015) proposed in [16] to enhance the planning and development of our review protocol. We archived the review protocol in a Git repository.[2] The components of the review protocol agreed upon function as a guide for conducting this SLR. Technically, these components encompass all essential elements crucial for conducting a successful SLR, which we discuss in the subsequent steps.

3) RESEARCH QUESTIONS (RQS)

The formulation of the RQs is the most crucial step in a review protocol. The remaining steps will systematically guide researchers to address the RQs and generate a literature synthesis. Therefore, we formulated the following research questions:

RQ1: What are the existing validated or evaluated PIA and PRA techniques published in the scientific literature?

RQ2: How and to what extent are PIA and PRA techniques scientifically validated or evaluated?

Following the development of the RQs, the next subsections describe the sequence of methodological steps (constituting the review components) we followed to provide answers to the RQs.

B. CONDUCTING THE REVIEW

As highlighted in Table 1, this phase involves three main steps for generating answers to the formulated RQs. We discuss each activity below, which necessitates the identification of relevant research for this study.

1) SEARCH STRATEGY

Considering the RQs, it was essential to establish an unbiased search strategy that would result in the discovery of potential primary studies directly related to this study. To do so, we decomposed RQ1 into relevant search terms, that were used to design a primary search string. The search terms for this SLR are as follows: (i.) `data protection risk assess*`; (ii.) `privacy risk assess*`; (iii.) `privacy risk analys*`; (iv.) `privacy impact assess*`; (v.) `data protection impact assess*`; (vi.) `privacy threat model*`; and, (vii.) `privacy threat assess*`.

[2]Replication package for the SLR (https://git.cs.kau.se/samuwair/SLR)

TABLE 2. Primary search string.

("privacy impact assess" OR "privacy impact analys*" OR "privacy impact model*" OR "privacy risk assess*" OR "privacy risk analys*" OR "privacy risk model*" OR "privacy threat assess*" OR "privacy threat analys*" OR "privacy threat model*" OR "data protection impact assess*" OR "data protection impact analys*" OR "data protection impact model*" OR "data protection risk assess*" OR "data protection risk analys*" OR "data protection risk model*" OR "data protection threat assess*" OR "data protection threat analys*" OR "data protection threat model*")*

TABLE 3. Primary search string split to comply with IEEE Xplore search restriction.

Search	Search string
Search 1	*("privacy impact assess*" OR "privacy impact analys*" OR "privacy impact model*" OR "privacy risk assess*" OR "privacy risk analys*" OR "privacy risk model*" OR "privacy threat assess*" OR "privacy threat analys*")*
Search 2	*("privacy threat model*" OR "data protection impact assess*" OR "data protection impact analys*" OR "data protection impact model*" OR "data protection risk assess*" OR "data protection risk analys*" OR "data protection risk model*" OR "data protection threat assess*")*
Search 3	*("data protection threat analys*" OR "data protection threat model*")*

These search terms were incorporated and tested with various combinations in all target databases until we agreed upon a primary search string (outlined in Table 2), which was concluded with the Boolean operator **OR**.

However, owing to the restrictions that might come with specific databases, the search string can be adapted to comply with these restrictions. In this instance, while the primary search string was applied to other databases, i.e., Scopus, Web of Science, and ACM Digital Library as it is, the search restrictions in *IEEE Xplore* imposed a limit of only eight wildcards. Hence, the primary search string had to be split to comply with this limitation. Thus, the adapted search strings outlined in Table 3 were used.

2) DATA SOURCES

Fig. 2 illustrates an overview of the SLR. To identify potential research for our study, four separate databases were queried: Scopus, Web of Science, IEEE Xplore, and ACM Digital Library, to retrieve potential studies for the research. However, we did not query Google Scholar as it does not provide the necessary elements for systematic scientific literature retrieval, such as tools for incremental query optimization, export of a large number of references [42], lack of Boolean search operations, and the queries have been found to be irreproducible over time [43].

Our search from the databases yielded 991 primary studies. To manage the screening, we exported the results from each database and imported them into Rayyan software,[3] which we agreed upon as our logging system. A total of 309 duplicate studies were removed using the duplicate detection feature

[3]Rayyan - AI-powered tool for SLRs (https://www.rayyan.ai/)

TABLE 4. Inclusion criteria.

Inclusion	Rationale
(i.) Studies that propose a PIA/DPIA or PRA methodology.	(i.) Identified studies that propose a novel or improved PIA / DPIA or PRA methodology.
(ii.) Studies that describe validation or evaluation of a PIA/DPIA or PRA methodology.	(ii.) Studies need to describe or document a specific validation or evaluation method.
(iii.) Peer-reviewed studies	(iii.) Studies that have undergone a peer-review process. We did not include grey literature.

of Rayyan leaving 682 studies. Using Rayyan, two reviewers also used a double-blind approach to read all the studies' titles and abstracts, allowing them to independently choose to ''include'', ''exclude'', or mark the study as a ''maybe''. Essentially, this step helps determine the relevance of the studies to the RQs following predetermined inclusion criteria, as outlined in Table 4. Articles that did not meet these criteria were excluded.

After independent screening, the blind mode was turned off in Rayyan, revealing any conflicts between the two reviewers. Hence, to solve these conflicts, we discussed until we reached a consensus on which disagreed studies needed to progress to the next phase. In case of disagreement, a third reviewer was consulted to decide on the study's inclusion or exclusion. For the remaining 98 studies that passed this first screening phase after the exclusion of 584 studies, full-text PDFs were downloaded for further analysis. We thoroughly assessed these studies to determine whether they met the predefined inclusion criteria. This involved reading and analyzing the entire article to comprehensively understand its content. However, an article was excluded from further analysis if it did not fit the study based on the exclusion criteria outlined below:

i. Papers not written in English - This criterion is based on our common language of understanding.
ii. Studies/publications on PIA that do not analyze the method, specifically PRA - This study focuses on the core component of the PIA, the privacy risk assessment. Hence, studies that did not analyze a PIA, especially the PRA component, were excluded.
iii. Studies/publications that enumerate or identify privacy risks - Similar to the previous criteria, studies that do not analyze how privacy threats are identified or analyzed are excluded.
iv. Studies that focus on security analysis - This SLR focuses on methods that incorporate privacy requirements, for instance, PIAs.
v. Studies of low quality. i.e., no research question or clear methodology - Studies with a poor research methodology or that do not provide a rationale for the study are excluded.
vi. Studies that do not perform a priori risk analysis - Studies that do not perform privacy risk analysis during the development stage.

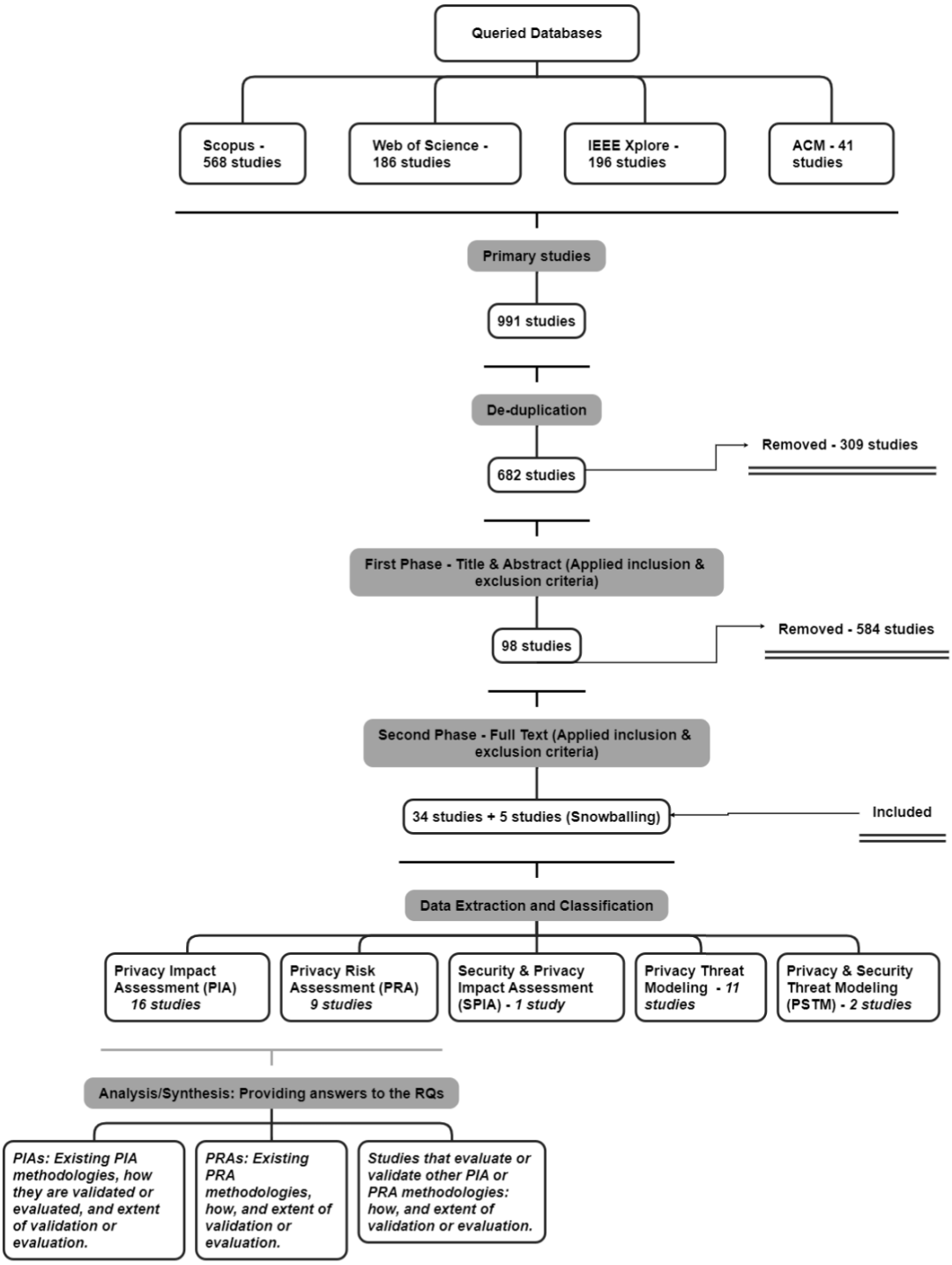

FIGURE 2. Overview of this SLR.

Having read the full text and applied the inclusion/exclusion criteria, a total of 34 studies remained while 64 studies were excluded after careful reading. Additionally, 5 studies were retrieved through forward and backward snowballing [44], resulting in a total of 39 studies relevant to this SLR. Bibliographies of the final results were exported to Zotero to share all included studies among authors.

3) DATA EXTRACTION

In this study, the following key characteristics from the included studies were extracted systematically based on the information within the publication type, i.e., conference papers and journal articles. This information is relevant to the next section, where we analyze and synthesize the data.

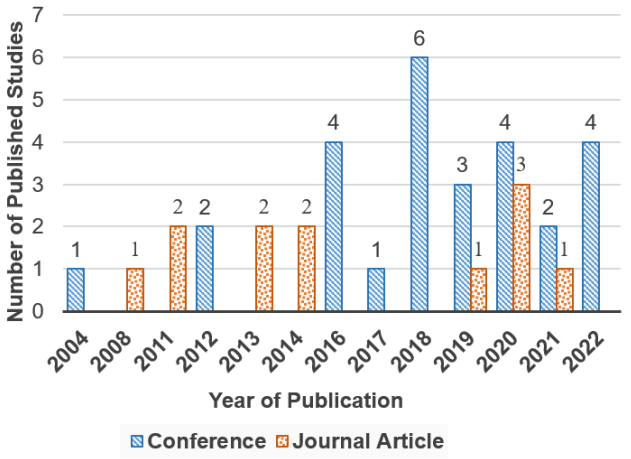

FIGURE 3. Distribution of published studies with regards to publication type.

i. Main contributions of each study.
ii. Key information of the PIA or PRA methodologies, such as name, scope of analysis, and type of risk analysis (qualitative or quantitative).
iii. Validation and evaluation methods used for the proposed PIA or PRA methodology.
iv. The extent of evaluation or validation - the scale of evaluation activity that is measured, e.g., the number of surveys, expert interviews, etc.
v. Information on whether the PIA or PRA methodologies assess privacy harms or how they conceptualize risks.
vi. Conclusions from each study.

Bibliographic information such as title, authors' names, year of publication, publisher, and publication type was automatically extracted by Rayyan.

V. RESULTS

The following section presents the result of this SLR. It provides an in-depth synthesis and evaluation of the findings of the studies outlined in Table 5. These findings are intended to address the RQs outlined in Section IV-A3.

A. STUDIES DEMOGRAPHICS

Fig. 3 shows the distribution of the 39 studies included in this study. The studies ranged from 2004 to 2022, with the selected studies (represented by each length of the bar) proposing a PIA or a PRA. We also included studies that proposed a Security & Privacy Impact Assessment (SPIA), PTM, or Privacy & Security Threat Modeling (PSTM). The rationale for incorporating the latter is addressed at a later stage under the categorization of the methodologies (Section V-B). While the rise of PIAs became more common in the mid-1990s [4], scientific studies published before 2004 that proposed a PIA or PRA methodology were not found.

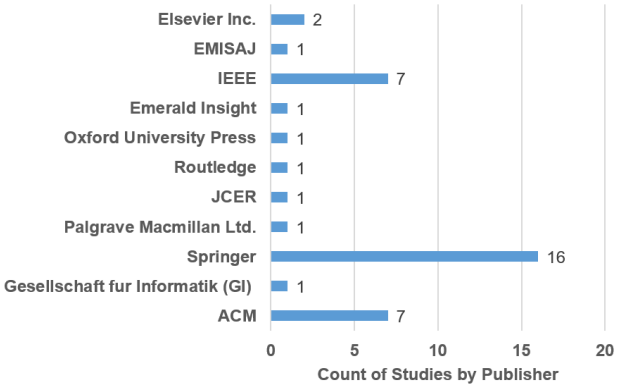

FIGURE 4. Overview of publishers against studies published.

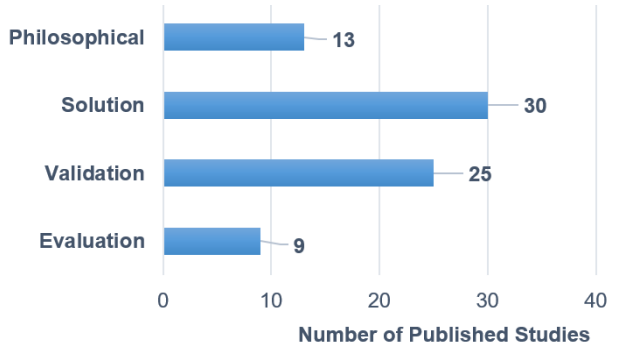

FIGURE 5. Overview of studies based on research type [70].

Nevertheless, we found an increased peak in published studies from 2018 to 2022. The increased rise could be attributed to the implementation of the EU GDPR [3], which mandates a DPIA for processing personal data that would likely result in high risks to data subjects. The figure also depicts the type of publications of the studies included in this SLR, where 69% of the studies belong to the publication type conference proceedings, while 31% belong to journal articles. It is worth noting that 26% of the studies in our analysis focused on validating or evaluating PIAs or PTMs solutions proposed elsewhere, either by the authors or by other researchers. These studies are discussed further in the synthesis in section V-D.

Fig. 4 shows the publishers of the included studies. It can be noted that the studies are distributed across various publishing companies. As evidenced by the bar chart, Springer tops the list with 41.02% of the included studies published under them. ACM Digital Library and IEEE follow this with 18% of the publications each. This distribution shows the diversity of scholarly dissemination regarding the topic of research.

Fig. 5 illustrates the classification of the included studies based on the type of research proposed by Wieringa et al. [70].

The studies were grouped into evaluation, solution, validation, and philosophical research. Wherein:

TABLE 5. Outline of the selected studies included in this SLR. Each individual study is denoted by a unique study ID.

Study ID	Year	Title and Reference
S1	2021	Approaching the Data Protection Impact Assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to Identity Management systems [45]
S2	2020	Data protection impact assessment in identity management with a focus on biometrics [46]
S3	2019	Privacy impact assessment: Comparing methodologies with a focus on practicality [47]
S4	2018	Supporting privacy impact assessment by model-based privacy analysis [11]
S5	2014	A systematic methodology for privacy impact assessments: A design science approach [21]
S6	2013	A comparative analysis of privacy impact assessment in six countries [41]
S7	2013	Evaluating privacy impact assessments [40]
S8	2011	An evaluation of privacy impact assessment guidance documents [19]
S9	2019	Evaluating privacy impact assessment methods: guidelines and best practice [30]
S10	2020	The Data Protection Impact Assessment as a Tool to Enforce Non-discriminatory AI [48]
S11	2016	Privacy impact assessment template for provenance [49]
S12	2016	A process for data protection impact assessment under the European General Data Protection Regulation [50]
S13	2020	DPMF: A Modeling Framework for Data Protection by Design [51]
S14	2020	DPIA in Context: Applying DPIA to Assess Privacy Risks of Cyber Physical Systems [52]
S15	2020	Methodology and workflow to perform the Data Protection Impact Assessment in healthcare information systems [53]
S16	2021	Data Protection Impact Assessments in Practice: Experiences from Cases Studies [31]
S17	2020	A Proposed Privacy Impact Assessment Method Using Metrics Based on Organizational Characteristics [33]
S18	2022	Modelling privacy harms of compromised personal medical data - Beyond data breach [54]
S19	2020	Fuzzy-based approach to assess and prioritize privacy risks [55]
S20	2018	Towards an effective privacy impact and risk assessment methodology: Risk assessment [32]
S21	2017	A refinement approach for the reuse of privacy risk analysis results [56]
S22	2016	PRIAM: A privacy risk analysis methodology [22]
S23	2016	Developing a structured metric to measure privacy risk in privacy impact assessments [57]
S24	2018	Privacy risk assessment: from art to science, by metrics [26]
S25	2021	Quantitative Privacy Risk Analysis [58]
S26	2004	Privacy risk models for designing privacy-sensitive ubiquitous computing systems [59]
S27	2020	A Developer Driven Framework for Security and Privacy in the Internet of Medical Things [34]
S28	2021	P-STORE: Extension of STORE Methodology to Elicit Privacy Requirements [60]
S29	2012	Privacy-by-design based on quantitative threat modeling [35]
S30	2008	Addressing privacy requirements in system design: the PriS method [61]
S31	2018	Interaction-Based Privacy Threat Elicitation [62]
S32	2022	PTMOL: A Suitable Approach for Modeling Privacy Threats in Online Social Networks [63]
S33	2022	Mitigation Lost in Translation: Leveraging Threat Information to Improve Privacy Solution Selection [64]
S34	2019	Knowledge is power: Systematic reuse of privacy knowledge for threat elicitation [65]
S35	2018	Effective and efficient privacy threat modeling through domain refinements [66]
S36	2014	Empirical evaluation of a privacy-focused threat modeling methodology [67]
S37	2011	A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements [29]
S38	2012	Comparing privacy requirements engineering approaches [68]
S39	2018	Identifying privacy risks in distributed data services: A model-driven approach [69]

i. Studies categorized under evaluation encompass research that analyzes or applies a methodology in real-world practice, e.g., using case studies [71].
ii. Studies grouped under the solution category present original methodologies or notable enhancements to existing ones without necessarily any form of validation.
iii. In the validation category, studies critically assess a proposed solution, whether by the authors themselves or other researchers, for example, through comparative analyses or other forms of rigorous scrutiny (e.g., experiments, simulation, prototyping, mathematical analysis), without actually evaluating it in practice.
iv. Lastly, studies falling under the philosophical category ''sketch a new way of looking at things, a new conceptual framework'' [70].

During data extraction and classification, we observed that the studies fell into multiple categories of research type. In other words, while a study can be classified as a solution proposal, the author(s) can also investigate the proposed solution in practice. For example, studies S9 [30] and S4 [11] fall into multiple categories. That is, S9 falls in both the validation and proposal of solution research, whereas S4 falls under evaluation, solution proposal, and validation research. We also observed that studies proposing solutions

were higher in number while the least were studies under evaluation research type.

B. STATE-OF-THE-ART: A DETAILED ACCOUNT OF THE IDENTIFIED METHODOLOGIES

This subsection critically assesses the PIAs and PRA methodologies documented in the scientific literature to answer the RQs. We identified 16 studies proposing PIAs and 9 studies on PRAs. Additionally, we examined the evaluation and validation of SPIA (1 study), PSTM (2 studies), and PTM (11 studies) methodologies, considering the extent of validation and evaluation for the following reasons:

i. Similar to PIAs, PTMs aim to elicit and assess privacy risks early in a project or system design, proposing corresponding privacy measures. While PSTM incorporates a security risk assessment element, they also examine privacy threats in the design phase. Conversely, SPIAs are PIAs that include a security risk assessment component, making them relevant methodologies to consider.
ii. During a systematic description of the envisaged processing, both PTMs and PIAs, as well as PSTMs, map the flow of information using Data Flow Diagrams (DFDs) or Information Flow Diagrams. DFDs illustrate system architecture in the form of processes, external entities, data flows, and data stores [29], [72].
iii. Some studies, for instance, Bisztray and Gruschka [47], Georgiadis and Poels [36], and Hart et al. [55] identified LINDDUN, an example of PTM, as similar to a PIA, hence justifying their consideration.

Fig. 6 depicts the classification of the studies into five categories. Additionally, we further classified the identified methodologies in terms of whether they had been validated or evaluated based on the definition by Wieringa et al. [70]. This illustrates the existing methodologies that have been validated or evaluated, thereby answering RQ1. Nevertheless, the classification does not consider studies that validate or evaluate other methodologies (we however consider S9 since the authors propose a PIA even though they validate other methodologies), as these are discussed in subsection V-D. In the following stages, we provide a brief description, detailed evaluation, and discussion of the identified methodologies for each category.

1) PRIVACY IMPACT ASSESSMENTS

PIAs serve to identify privacy risks and implement appropriate technical and organizational measures, thus addressing privacy from the beginning. To support this process, several PIA methodologies, as depicted in Fig. 6, have been proposed and published in scientific literature. In the following section, we provide a brief description of each methodology. Subsequently, we delve into an in-depth analysis of the methodologies identified in the following sections. As a reminder to readers, while we explore these methodologies by examining their shared characteristics and distinctions to reveal their scope and focus, our primary focus in this analysis centers on validated and evaluated PIAs.

a: OVERVIEW OF PROPOSED PIAS

Table 6 briefly describes each PIA methodology we identified in our study. A takeaway from the overview and description of the methodologies is that there is no concrete methodology that the authors followed when proposing a PIA methodology. We note a distinction in the guidance on the process for conducting a PIA for each methodology. However, while there are distinctions, we still identified similarities. We discuss this under scope and focus.

b: SCOPE AND FOCUS

A detailed analysis of the identified PIAs revealed a spectrum of shared characteristics and distinctions that pointed to the individual scope and focus of these methodologies. Studying the scope and focus provides a better understanding of what the methodology addresses and does not address. While contrasting (in terms of guidance), a common denominator connecting all these PIAs is that they play an integral part in ''data protection by design and by default'' (Art.25 of the GDPR) as they enable the identification and minimization of risks through appropriate technical and organizational measures. In addition, they explicitly reference the GDPR [3] in terms of either identifying privacy targets or referencing Art.35 (based on the minimum requirements that a DPIA should satisfy). Given this, we compared these methodologies based on the minimum requirements for a DPIA as articulated in Art. 35(7) of the GDPR, i.e., an assessment shall contain at least:

(a) *a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
(b) *an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
(c) *an assessment of the risks to the rights and freedoms of data subjects; and*
(d) *the measures envisaged to address the risks, including safeguards, security measures, and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

The comparison overview in Table 7 outlines the scope and focus of these methodologies. We observed that the methodologies did not address certain requirements; however, it is notable that the authors concentrated on specific requirements in their proposals. For example, in S10 [48], Art. 35(7)(a) is considered out of scope because the specific outcome of the systematic envisaged processing relies on the AI model and its designated use; nevertheless, they address other requirements. In addition, we observed that while 50% of the methodologies identified measures to address the risks (Art. 35(7)(d), i.e., S4, S5, S10, S11, and S12, Vemou

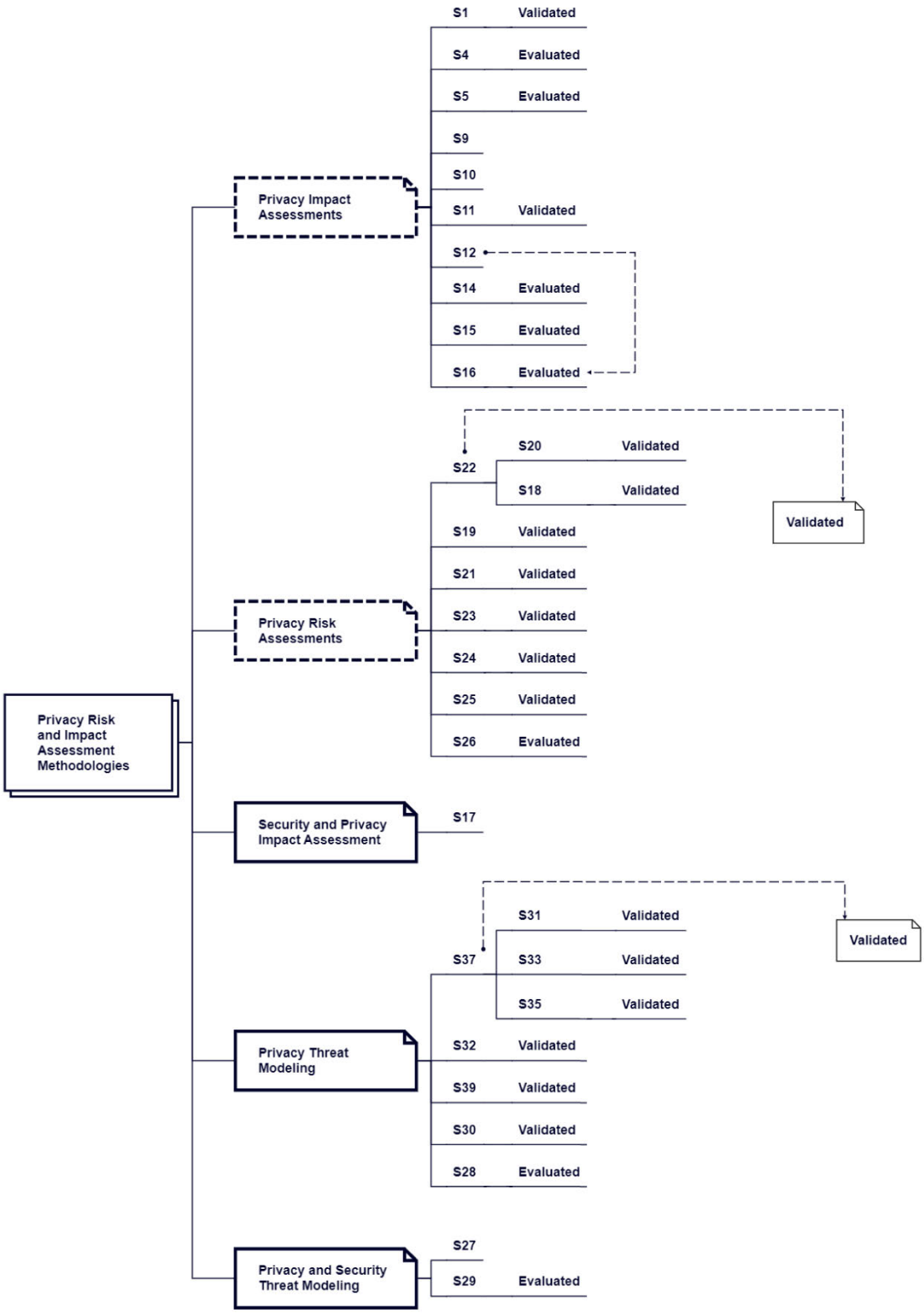

FIGURE 6. A classification of included studies categorized in terms of PIAs, PRAs, SPIAs, PSTMs, and PTMs, and in terms of whether they have been validated or evaluated. Labels S1, S4, and so forth refer to the study IDs in Table 5. Note that this classification reflects only the studies marked as "Solution Proposal".

TABLE 6. Overview and description of the identified proposed PIAs. The Study ID reflects the study in which the methodology has been proposed (Refer to Table 5).

Study ID	Description
S1	Timón López, Alamillo Domingo, and Valero Torrijos [45] proposed a two-layer DPIA methodology for the study of the level of privacy by design attained by systems before their implementation. The first layer of the methodology occurs before the system's design by providing an initial description, contextual information, and data flows, as well as considering risk sources and assessing risks. The second layer assesses the level of compliance based on the assessment conducted in the first layer.
S5	Oetzel and Spiekermann [21] introduced a seven-step methodology to provide a robust and easily applicable PIA. The seven steps: (i) system characterization, (ii) definition of privacy targets, (iii) evaluation of the degree of protection demand for each privacy target, (iv) threat identification, (v) identification of existing or new controls, (vi) residual risk and control implementation plan and (vii) documentation and generation of PIA report, provide a step by step PIA process that aids in analyzing and assessing privacy risks.
S4	Having been inspired by S5, Ahmadian et al. [11] proposed a PIA methodology that is supported by model-based privacy analysis. The PIA methodology proposed consists of six steps: (i) system specification, (ii) privacy and security analysis, (iii) threat identification, (iv) impact assessment, (v) identification of appropriate controls, and (vi) documentation. Each step generates an artifact that is incorporated into the next step, akin to the seven-step PIA methodology by [21].
S9	In their study, Vemou and Karyda [30] undertook an appraisal of multiple PIA methods and guidelines. They developed a set of criteria to appraise the strengths and weaknesses of each method. Building upon their findings and drawing insights from privacy literature, a PIA process that incorporates the most effective elements identified for PIAs was proposed. This process is composed of six steps: (i) PIA preparation, (ii) system analysis, (iii) risk analysis, (iv) risk mitigation, (v) generation of PIA report, and (vi) PIA follow-up.
S10	Ivanova [48] proposed a DPIA methodology that takes into context the assessment of risks that emerge from the use of AI systems. The author outlines the process and application of the methodology, specifically to AI, which involves systematically assessing data processing operations, identifying potential risks to individuals' rights and freedoms, and implementing measures to mitigate those risks.
S11	Reuben et al. [49] proposed a PIA Template for data provenance that is inspired by the privacy and data protection impact assessment framework for RFID Applications [23]. The primary objective is the identification of privacy risks and privacy safeguards associated with data provenance. By leveraging the EU GDPR, instead of Directive 95/46/EC as the DPIA-RFID framework, the authors extract privacy targets that allow them to extrapolate on potential privacy threats and subsequently determine appropriate countermeasures.
S12	Work by Bieker et al. [50] proposed a high-level DPIA process that operationalizes the requirements of a DPIA as established in Article 35 of the GDPR. It consists of three stages: Preparation, Evaluation, and Report and Safeguards stage. The evaluation stage identifies protection goals [73], potential attackers, motives and objectives, evaluation criteria and benchmarks, and risk evaluation.
S16	Considering the proposed methodology in S12 that operationalizes the requirements of a DPIA, Friedewald et al. (S16) [31] further operationalized the methodology to identify if the methodology is applicable, or not, to all types and sizes of organizations, regardless of the sector, through case studies. The three stages in the previous DPIA methodology described in S12 are expanded into five phases, i.e., initiation, preparation, execution, implementation, and sustainability phase.
S14	Henriksen-Bulmer et al. [52] applied a proposed DPIA data wheel [74] that is based on contextual integrity in the context of Cyber-Physical Systems. The methodology, represented in terms of a spreadsheet, is question-based and aims to provide a comprehensive perspective of the system being evaluated. The questions assess the need for a DPIA, questions relating to the DPIA data wheel activity flow (explanation, risk assessment, and decision), and supporting questionnaires in the form of a Data Register and Life of the Form.
S15	Due to the absence of established approaches in the scientific literature for performing DPIAs in the healthcare sector, Todde et al. (S15) [53] proposed a DPIA methodology for Healthcare, and in particular for Hospital Information Systems (HISs). The DPIA methodology is depicted as a workflow where a hospital information system, device, or application is assessed from context definition to risk mitigation.

and Karyda (S9) [30] argued that such measures can be misleading to PIA practitioners as they might not be sufficient to address the risks identified. However, we argue that identifying measures for sector-specific risks could provide a knowledge base that would guide analysts to address risks that arise within a given sector. We note that only a few specific PIAs have proposed measures to address risks for a given area, i.e., in AI models (S10) and the provenance of specific data (S11).

As aforementioned, PIAs serve to identify privacy risks and implement appropriate technical and organizational measures, thus addressing privacy from the onset. Given this, it can be observed that all PIAs fulfill Art.35(7)(c) on assessing the risks to the rights and freedoms of data subjects. However, it is argued that the key difference between the assessment of security risks and the assessment of privacy risks is the primary consideration of potential harm to data subjects in a privacy risk assessment, as compared to security risk assessment, which is of secondary concern [26], [55]. In addition, Recital 75 of the GDPR identifies that risk to data subjects of varying likelihood and severity may result in harm, for instance, physical or non-physical [3]. Hence, we identified some methodologies, i.e., S5 [21] and S4 [11] that assess harmful activities and the "degree of protection demand" for each privacy target, which, when exploited, would result in privacy harms. It has been argued

TABLE 7. Summary of identified PIAs with their methodological scope and focus. (✓) indicates fulfillment of the requirement, (✗) denotes unaddressed requirements within the scope of the methodology.

Study ID	Art.35(7)(a)	Art.35(7)(b)	Art.35(7)(c)	Art.35(7)(d)
S1 [45]	✓	✓	✓	✗
S4 [11]	✓	✓	✓	✓
S5 [21]	✓	✓	✓	✓
S9 [30]	✓	✓	✓	✗
S10 [48]	✗	✓	✓	✓
S11 [49]	✓	✗	✓	✓
S12 [50]	✓	✓	✓	✓
S14 [52]	✓	✓	✓	✗
S15 [53]	✓	✗	✓	✗
S16 [31]	✓	✓	✓	✗

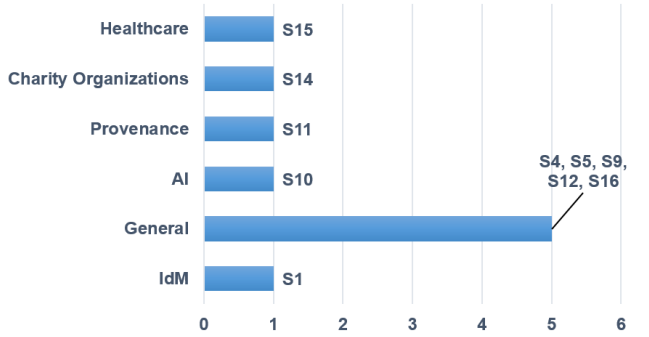

FIGURE 7. Overview of Sector-specific PIAs.

that by assessing and mapping privacy targets (derived from GDPR [3] and Directive 95/46/EC [75]) to appropriate controls during a privacy impact assessment, harmful activities defined by Solove [76] can be addressed [21]. The consideration of assessing harm during privacy risk assessment was also discussed in S16 [31], and S9 [30]. However, unlike in S4 and S5, the authors of S16 brainstorm potential harms for their assessment, whereas, in S9, they cite CNIL [17] for further inspiration into harms.

c: SECTOR-SPECIFIC PIAS

Article 29 Working Party on the Data Protection Impact Assessment guidelines supports the development of sector-specific methodologies that leverage the knowledge from stakeholders in these particular sectors [18]. In alignment with this, and as depicted in Fig. 7, we observed the introduction of sector-specific methodologies, such as those tailored for healthcare, Identity Management (IdM), and charity organizations. Such methodologies can be extended beyond individual assessments to cover a common processing environment across the same sector, as highlighted in Recital 92 and Article 35(1) of the GDPR [3]. However, this does not imply that such methodologies cannot be applied across different sectors, as they provide guidelines for conducting PIA. While proportional, we also identified methodologies that are not sector-specific and, hence, could be applicable across different sectors.

d: VALIDATED AND EVALUATED PIAS

Based on Fig. 6, it is evident that a significant number (50%) of the identified PIAs have been assessed in practice, for instance, through case studies, thus demonstrating their effectiveness and reliability. Conversely, only 20% of the PIAs were validated, indicating that the methodologies were not tested in practice. Interestingly, we identified a few PIA methodologies that have not been validated or evaluated, i.e., S9, S10, and S12. Hence, while such methodologies could be termed comprehensive, their reliability is unknown, and challenges could arise due to unforeseen complexities. Nevertheless, while the methodology in S12 was never validated or evaluated when it was initially proposed, it was eventually evaluated in a subsequent study by its authors (S16), hence its inclusion in this SLR and the relationship link between S12 and S16 in Fig. 6.

> ***Takeaway:*** *We noted that there was no concrete methodology that the identified PIAs followed, leading to distinct guidance for a PIA process. As a result, the controllers are left to choose a methodology that best suits them; however, the methodology needs to align with the guidelines for a DPIA as highlighted by Article 29 of the Working Party [18]. Hence, we observed that each identified methodology can be considered compliant. Nevertheless, we recommend that further evaluation be conducted to assess whether each step under each criterion is covered during the PIA process. We also observed that few PIA methodologies assess privacy harms, akin to the impact on the rights and freedom of data subjects based on the risks from the processing of personal data.*

2) SECURITY AND PRIVACY IMPACT ASSESSMENT

The need to also take into consideration security requirements in a PIA has also been discussed by Makri, Georgiopoulou, and Lambrinoudakis (S17) [33] in their proposal for a PIA that handles both security and privacy risks and takes into consideration organizational characteristics. The authors argue that traditional PIAs fail to use metrics and account for the unique attributes of organizations, leading to incomplete privacy risk assessments [57] e.g., type, activities, etc. While the PIA methodologies identified in the earlier analysis reference the GDPR, the methodology in S17 incorporates OECD principles[4] in its PIA approach and quantifies their severity, including data sensitivity. Given that these principles are reflected in the GDPR, we find their use in the methodology as abstract, i.e., ''they are semantically different and often more generic than concrete system functions that engineers can build or that can be scrutinised in a PIA'' [21]. In addition, while the assessment of both security and privacy risks can suggest the comprehensiveness of the methodology, it can be observed from Fig. 6 that the methodology is neither validated nor evaluated; thus, issues with the complexity and practicality of the methodology could be questioned.

> ***Takeaway:*** *The SPIA methodology adds complexity as it proposes the use of independent methodologies to elicit privacy and security requirements. Although this is comprehensive, we argue that the introduction of independent methodologies can incur extra overhead.*

3) PRIVACY RISK ASSESSMENTS

As shown in Table 7, it can be established that all the identified PIAs cover or fulfill Art. 35(7)(c) within their scope. This underscores Privacy Risk Assessment (PRA) as the core element of a PIA. However, PIAs have been criticized for their inadequacy, notably the lack of clear guidance on

[4]OECD Privacy Principles (http://oecdprivacy.org/)

how to conduct a comprehensive PRA [21], [22], as well as an efficient approach to evaluate and prioritize risks [55]. As such, several independent PRAs have been developed over time to contribute to assessing privacy risks as an independent method or part of a PIA.

In the following sections, we describe the identified PRAs, analyze the evaluation and validation of these methodologies, and assess their scope and focus. These findings further contribute to the identification of the weaknesses and strengths of these methodologies.

a: OVERVIEW OF PROPOSED PRAS

Table 8 outlines the descriptions of the privacy risk assessments identified in our study. Based on these descriptions, the following general observations can be made:

i. **The need to reduce subjectivity in privacy risk assessments** – Several studies have identified the importance of moving far from subjectivity when evaluating privacy risks.
ii. **Assessment of privacy harms** – The majority of the methodologies identified, i.e., S22, S18, S20, S21, S23, S24, and S25 mention the assessment of privacy harm during risk assessment.

We delve further into the aforementioned observations, including an in-depth analysis of the identified PRAs in the next segment.

b: SCOPE AND FOCUS

In our study, we observed the absence of dedicated studies that explicitly examined independent methodologies for PRA. Consequently, there is a lack of well-defined criteria for analyzing these methodologies, such as for PIAs, for instance, in S3 [47] and S9 [30]. Nevertheless, we argue that a risk assessment method should cover some important steps, i.e., *risk identification, the evaluation of risks to prioritize them (determined in terms of the likelihood and impact/severity of a given risk) and countermeasures* [30]. In addition, given the need to assess the impact on privacy in a PIA [5], the assessment of privacy harm is also noted as a primary consideration in privacy risk assessments [26], [30], [55]. Hence, we used these criteria to compare and analyze the methodologies.

Table 9 outlines the scope and focus of the methodologies for privacy risk assessment based on risk evaluation, type of evaluation, and harm assessment.

From the information presented, it can be observed that based on the scope, all methodologies except S18 [54] evaluated the level of identified risks. The methodologies determine the level of risk based on likelihood and impact (or severity/damage) (S19, S23, S24, S25, and S26) or by determining the risk levels for a given privacy harm based on severity and likelihood (S20, S21, and S22). However, the modification of PRIAM in S18 assesses the severity of privacy harms instead (based on victims and intensity) and does not consider the likelihood of risks, hence the (✗) on the risk evaluation. Nevertheless, it identifies the actual harm to data subjects (patients) after a data breach. Furthermore, we point out the type of assessment used to evaluate the severity of privacy harms, which is semi-quantitative – the purpose of the asterisk is to show that the type of evaluation differs from other types of evaluations that include likelihood in their evaluation.

Regarding the types of evaluation, the rest of the methodologies assess the level of risks based on different types of assessments. For instance, despite the discretion in selecting the type of evaluation, S26 [59] suggested using a qualitative approach to evaluate risks in their proposal. This type of evaluation has been challenged as it fails to provide a structured way to monitor and measure privacy risks [57]. Hence, it can be observed that most methodologies use a semi-quantitative approach to evaluate the level of risk, except for one methodology (S22) that combines both qualitative and semi-quantitative approaches. This can be attributed to the two-phase approach taken in S22, that is, the information gathering and risk assessment phase, where the use of a qualitative assessment is within the information gathering phase for the assessment of the severity of privacy harms and the semi-quantitative assessment assesses the likelihood under the risk assessment phase. Nevertheless, while semi-quantitative approaches measure the level of risk based on a numerical value, they are noted as subjective and less scientific [26], [55]. As such, some researchers have proposed methodologies such as S19, S24, and S25, which are asserted to be objective, thus reducing inconsistencies. We use the term assertion as these methodologies have not been tested in practice.

We further analyzed the methodologies based on an assessment of privacy harm. We found that 77.8% of the PRAs assessed privacy harms, albeit differently. For instance, S18 [54], S20 [32], and S21 [56] built upon S22 [22], which groups privacy harms into five categories (physical, financial, societal, dignity, and psychological) and assesses the risk levels for a given privacy harm based on severity and likelihood. Nevertheless, while the methodology in S20 refines the harm trees and assesses the risk levels for a given privacy harm based on severity and likelihood, the approach in S18 uses a semi-quantitative approach, as discussed earlier, to assess the severity of privacy harms. S21 follows the same approach as S22 but with the aim of reusing the generated results following a generic methodology. On the other hand, S23 [57] and S25 [58] assessed harm based on Solove's harmful activities [76], while S24 [26] mentions harm from Recital 75 of the GDPR [3]. In S23, a numerical value (i.e., 1) was assigned to each harmful activity, whereas in S24, the authors proposed using a Likert scale to assess harms. However, in S25, harm evaluation was based on a severity scale that relied on the non-normative nature of harm. To scale severity, the authors suggest using surveys or experimental studies involving individuals (data subjects) who have been affected.

TABLE 8. Overview and description of the identified proposed PRAs. The Study ID reflects the study in which the methodology has been proposed (Refer to Table 5).

Study ID	Description
S22	De and Le Métayer [22] introduced PRIAM, which takes into account all factors affecting privacy risks, including the evaluation of these impacts and their overall contributions to risk assessment by describing seven components: system, stakeholders, data, risk sources, feared events, privacy harms, and privacy weaknesses, each associated with specific categories and attributes. These components form the foundation of a rigorous risk assessment that uses harm trees to assess risks.
S18	In PRIAM [22], the authors assert that ''a harm may result from one feared event or a combination of different feared events''. However, in a modification of PRIAM for assessing the impact on patients' privacy after a data breach, Wairimu and Fritsch [54] pointed out that one feared event might lead to several privacy harms, thus forming the basis of separate assessments for each category of privacy harm in their proposed approach. The approach focuses on three PRIAM components: data, feared events, and privacy harms.
S20	Alshammari and Simpson [32] extended PRIAM [22] by laying emphasis on four components of PRIAM [22]: privacy harms, feared events, privacy weakness, and risk sources, thus resulting in a four-step methodology. Unlike PRIAM, which is discussed in S22, the authors in S20 enhance their methodology by refining harm trees by introducing an additional level, specifically an intermediate node, to assess the exploitation of vulnerabilities in primary assets by the most probable risk sources.
S21	De and Le Métayer [56] proposed a systematic and cost-effective privacy risk assessment approach that reuses the results from the assessment within a PIA. The methodology follows three phases, each with steps to guide the assessment of each phase. Given that the methodology is incremental, the results of a given phase may be reused in a subsequent phase. Essentially, each phase generates privacy harm trees that are necessary for the computation of the likelihood of privacy harm.
S23	Agarwal [57] proposed a three-step privacy risk scoring methodology that provides a structured metric to evaluate privacy risks. The first step involves the identification of privacy threats that are derived from privacy targets. This was based on Directive 95/46/EC [75]. The second step involves modeling risks, and the final step involves the evaluation of risks by defining the impact based on Solove privacy harms [76] and likelihood based on Lipton's work [77] on mapping privacy online.
S24	In S23, the method measures privacy risks semi-quantitatively. However, Wagner and Boiten [26] argue that semi-quantitative types of privacy risk measurement are rather subjective and unstructured. To assess privacy risks quantitatively, they quantify both the impact and likelihood of risks. Four fundamental elements are used in this case: scale, sensitivity, expectation, and harm. On the other hand, the likelihood metrics are based on three key components: the probability of an attack, an adverse consequence, and exploitability.
S19	Hart, Ferrara, and Paci [55] proposed a privacy risk assessment approach to assess and prioritize privacy risks whilst reducing subjectivity. The methodology defines the evaluation criteria and leverages the fuzzy set theory for privacy risk assessment. A fuzzy multiple-criteria decision-making approach is applied to assess the privacy risk based on the evaluation criteria defined, which contains the rating, aggregation, and selection stages to achieve a more objective and systematic evaluation of privacy risks.
S25	Cronk and Shapiro [58] proposed a methodology based on Factor Analysis of Information Risk (FAIR), called FAIR-P, for quantifying and analyzing privacy risks based on a probabilistic model. The quantification is based on the harm magnitude and threat frequency (i.e., opportunity, motivation, capability, and difficulty) to avoid privacy harms identified by Solove [76]. The point of departure for such a proposal was rooted in the idea that a number of quantified privacy analysis methods are subjective and lack solid rationale.
S26	Hong et al. [59] proposed privacy risk models based on questions intended to assist designers in analyzing and managing privacy risks to design privacy-sensitive ubiquitous computing systems. Basically, under privacy risk management, the authors assess privacy management based on the likelihood, damage, and cost of privacy protection and propose using qualitative assessment.

TABLE 9. Summary of identified PRAs with their methodological scope and focus. (✓) denotes the fulfillment of the requirement, whereas (✗) signifies that the requirement is not addressed within the methodology's scope.

Study ID	Risk evaluation	Type of evaluation	Harm assessment
S18 [54]	✗	Semi-quantitative*	✓
S19 [55]	✓	Quantitative	✗
S20 [32]	✓	Semi-quantitative	✓
S21 [56]	✓	Semi-quantitative	✓
S22 [22]	✓	Qualitative & Semi-quantitative	✓
S23 [57]	✓	Semi-quantitative	✓
S24 [26]	✓	Quantitative	✓
S25 [58]	✓	Quantitative	✓
S26 [59]	✓	Qualitative	✗

c: VALIDATED AND EVALUATED PRAS

During our study, it became evident that a significant proportion of PRAs, precisely 88.9% are validated (See Fig. 6). This means that although the authors proposed the methodologies and validated them to some extent (e.g., hypothetical case study), they did not rigorously evaluate them in real-world practice. Notably, only one methodology S26 [59], was tested in practice. Given this, it can be suggested that while independent methods for assessing privacy risks have been proposed, little has been done to practically test them.

> ***Takeaway:*** *In contrast to the previously discussed PIA methodologies, we note a difference in the assessment of privacy harms in that, the majority of the independent PRAs assess privacy harms. This suggests that the assessment of potential impacts on data subjects is growing in maturity compared to the same assessment in PIAs, which are less focused on harm to data subjects.*

4) PRIVACY THREAT MODELING

Designing software with a strong emphasis on privacy requires consideration of such concerns in the early design stages and throughout the entire software development process. Hence, threat modeling provides an approach for identifying and addressing potential security and privacy threats in the design phase before software implementation [78]. To support privacy by design, incorporating

privacy threat modeling becomes a fundamental aspect of the software development process, ensuring that privacy requirements are proactively considered from the outset. In the next phases, we provide an in-depth analysis of the scope and focus of the identified PTM methodologies and the state of validation and evaluation. First, we provide an overview of the identified PTMs.

a: OVERVIEW OF PROPOSED PTMS

Table 10 summarizes the methodologies identified for conducting a PTM. Based on the description, a general observation can be observed:

i. **Enhancing LINDDUN** – Three studies identified areas of enhancement and addressed limitations in LINDDUN, i.e., S31, S33, and S35.

In what follows, we analyze the identified methodologies in greater detail.

b: SCOPE AND FOCUS

Similar to PRAs, there is a lack of concrete evaluation criteria in the literature that can be applied directly to compare the scope and focus of PTMs. While LINDDUN (S37) [29] can be compared to a PIA process [36], [47], [55], we argue that the minimum requirements from Art.35(7) of the GPDR cannot be applied in this case since not all PTMs are from Europe, for instance, S28 and S32. Nevertheless, we identify important steps of a PTM that we consider necessary:

(a) *a system description;*
(b) *identification of privacy properties;*
(d) *an evaluation of potential risks; and*
(e) *privacy measures envisaged.*

Hence, based on the above steps, we compared the PTMs identified in terms of their scope and focus as outlined in Table 11. Given the aforementioned general observation, we provide a detailed analysis of the enhancement of LINDDUN (S37). Previous research has identified that the LINDDUN methodology has some limitations that have been addressed over time. For instance, the issues of threat explosion and efficiency and effectiveness are addressed in S31 and S35, while the issue of selecting appropriate privacy measures is addressed in S33. This implies that efforts have been made to improve or refine LINDDUN to overcome identified challenges. Nevertheless, LINDDUN has been criticized for missing a risk assessment part [46], which we observe with other identified methodologies except for S28 and S39. For LINDDUN, we argue that the criticism is essentially unfair, as LINDDUN was specifically designed for threat modeling, and hence the risk assessment part was out of scope. This logic could also be applied to the rest of the methodologies that do not have a risk assessment part. However, in a follow-up study to evaluate LINDDUN, Wuyts et al., [67] state that the risk-based quantification of attack trees step of the quantitative threat modeling methodology (QTMM) [35] *"can be integrated into the LINDDUN method to provide a more objective prioritization of elicited threats."*

While all methodologies include a description of a given system, they model the systems differently. For instance, in S37, the authors used a DFD to represent data flows within a system. This is the same as the studies that refine LINDDUN, i.e., S31, S33, and S35. S39 also creates DFDs, in addition to leveraging Model-Driven Engineering (MDE). Leveraging MDE advocates using models during software development to define, design, and implement software [81]. On the other hand, in S30, the authors used a conceptual model. However, two studies, S28 and S32, take a different approach. In S32 [63], the authors only state the requirement of the system description (they do not provide a system model, such as DFDs). In S28 [60], they also do not provide a system model, but provide an approach for eliciting privacy goals in a given system, that is, through interviews or brainstorming.

Regarding privacy properties, we observe what type of privacy properties each methodology aims to preserve. We note that S28 integrates the privacy properties of LINDDUN (S37). This is the same for S31 and S35, which refine LINDDUN, except S33, which focuses on LINDDUN's hard privacy threats. In S30 and S32, we observed that the privacy properties included some security properties, i.e., Identification, Authentification, and Authorization. Nevertheless, it is stated that these are also necessary to protect privacy [61]. Given this, we state that such methods can be considered comprehensive in eliciting privacy requirements. However, S39 [69] only covers two privacy properties. In addition, we assessed the methodologies in terms of privacy measures. We observed that only S30, S33, and S37 provided privacy measures, while the rest did not. We assume, however, that the methodologies that refine S37 (LINDDUN), that is, S31 and S35, while they focus on specific steps of the LINDDUN methodology, the authors could have excluded privacy measures to avoid redundancy.

> ***Takeaway:*** *Our analysis of PTMs shows that LINDDUN has emerged as the most evolved research method based on the published improvements of the method. Notably, the LINDDUN website (linddun.org) has undergone recent updates. For instance, the LINDDUN threat trees are exemplified, and the method is being offered in three versions: LINDDUN GO [78] – for novices, LINDDUN PRO – for experts, and LINDDUN MAESTRO soon to be released as a third option (for model-driven analysis).*

c: VALIDATED AND EVALUATED PTMS

From Fig. 6, it can be observed that only one PTM has been evaluated in real-world practice, that is, S28. The rest have only been validated. This includes studies that also refine LINDDUN. However, in a separate study (S36) [67], S37 was evaluated in real-world practice. We discuss this further in Section V-C2.

TABLE 10. Overview and description of the identified proposed PTMs. The Study ID reflects the study in which the methodology has been proposed (Refer to Table 5).

Study ID	Description
S39	Grace et al. [69] presented a model-based methodology that leverages model-driven engineering (MDE) to identify and analyze privacy risks during the design phase of a system. To identify and analyze privacy risks, the methodology begins with constructing a DFD, which is later used to generate a Labelled Transition System (LTS) privacy model (with the elements state and transition) that represents the state of the user's privacy in a given system.
S37	Deng et al. [29] proposed a model-based methodology that is comparable to STRIDE [79] but different in that while STRIDE elicits security requirements, the methodology known as LINDDUN elicits privacy requirements. LINDDUN is an acronym that stands for privacy threats categories that the methodology aims to prevent through hard and soft privacy properties. To elicit privacy threats, the methodology is divided into a problem and solution phase [62], [80].
S33	The problem of selecting appropriate mitigation strategies in the solution space with regards to the LINDDUN is addressed by Al-Momani et al. [64] in their proposed methodology to enhance threat-modeling solution spaces. While the methodology is generic, the authors apply it to LINDDUN, specifically on hard privacy threats, in a manner that allows suitable solutions to be selected through the definition and ranking of possible solutions, construction of questions, and representation of the output of solutions.
S35	While identifying privacy threats, the challenge of threat explosion was an inherent aspect within LINDDUN. Hence, Wuyts et al. [66] proposed an approach to improve the efficiency and effectiveness of the problem space, specifically mapping privacy threats to DFD elements and eliciting privacy threats. The approach improves LINDDUN by proposing domain refinement questions that reduce threats by asking system-specific and DFD-specific questions that, in turn, reduce threats by getting rid of irrelevant threat trees.
S31	Considering that LINDDUN [29] is an element-based methodology given that privacy threats are mapped to DFD elements, Sion et al. [62] proposed an interaction-based methodology, as a variant to LINDDUN, that maps privacy threats on basis of element interactions, i.e., source, data flow, and destination. Eliciting privacy requirements based on the methodology reduces the amount of iteration needed when mapping privacy threats and better identification of privacy threats due to the analysis of architectural-level interaction.
S30	PriS [61] is a methodology that describes a systematic approach to integrate privacy considerations by framing privacy requirements in terms of organizational goals, thus connecting the disparity between software design and implementation phases. Particularly, privacy requirements are treated as privacy goals that play a role in influencing or constraining the way organizational goals are transformed into operational processes. To identify privacy goals, PriS leverages eight fundamental privacy requirements, i.e., authorization, authentication, identification, anonymity, data protection, pseudonymity, unobservability, and unlinkability.
S28	Ansari [60] proposed P-STORE as an extension of the STORE (Security Threat Oriented Requirements Engineering) methodology, specifically designed to elicit privacy requirements. Similar to the original STORE methodology, P-STORE comprises ten steps. By incorporating the LINDDUN threat categories, the authors leverage an established methodology for the systematic identification and categorization of privacy threats within the P-STORE framework.
S32	Privacy Threat MOdeling Language (PTMOL) is a methodology for eliciting privacy threats in online social networks (OSN) that was proposed by Rodrigues, Villela, and Feitosa [63] to enable designers to identify privacy risks during the design phase and choose suitable measures to address these issues in the context of OSNs. To facilitate the comprehensive analysis of privacy threats, the designer must undertake a series of steps, initiated using a template, to identify assets, threats, risk sources actions, and countermeasures.

TABLE 11. A summary of the identified PTMs and their methodological scope and focus. (✓) indicates fulfillment of the criterion while (✗) indicates a criterion not covered within the scope of the methodology.

Study ID	System Description	Privacy properties	Risk evaluation	Measures
S28 [60]	✓	LINDDUN's privacy properties (S37)	✓	✗
S30 [61]	✓	Identification, Authentication, Authorisation, Data protection, Anonymity, Pseudonymity, Unlinkability and Unobservability	✗	✓
S31 [62]	✓	LINDDUN's privacy properties (S37)	✗	✗
S32 [63]	✓	Unlinkability, Anonymity and Pseudonymity, Confidentiality, Authentication and Identification, Authorization	✗	✗
S33 [64]	✓	Hard privacy properties (S37) - Unlinkability, Anonymity & Pseudonymity, Plausible deniability, Undetectability and unobservability, Confidentiality	✗	✓
S35 [66]	✓	LINDDUN's privacy properties (S37)	✗	✗
S37 [29]	✓	Unlinkability, Anonymity and Pseudonymity, Plausible deniability, Undetectability & unobservability, Confidentiality, Content awareness, Policy & consent compliance	✗	✓
S39 [69]	✓	Confidentiality and Pseudonymisation	✓	✗

5) PRIVACY AND SECURITY THREAT MODELING

Model-based methodologies that leverage a PTM and a Security Threat Model (STM), have also been proposed. These methods can elicit both privacy and security threats.

a: OVERVIEW OF PROPOSED PSTMS

Work conducted by Luna, Suri, and Krontiris (S29) [35] yielded a quantitative threat modeling methodology (QTMM) that elicits privacy and security requirements by basing its methodology on STRIDE and privacy protection goals [82]. Unlike PRIAM [22], which uses harms trees, or LINDDUN [29], which suggests the use of threat trees for its risk quantification, QTMM suggests the use of attack trees. The authors also introduced a risk assessment to quantify privacy and security risks.

Treacy, Loane, and McCaffery (S27) [34], by leveraging a Developer-Driven Threat Modeling [83], proposed a

TABLE 12. A summary of the identified PTSMs and their methodological scope and focus. (✓) indicates fulfillment of the criterion while (✗) indicates a criterion not covered within the scope of the methodology. Note: System description (S. Desc.), Risk evaluation (R. Eval.), Measures (Mes).

Study ID	S. Desc.	Privacy properties	Security properties	R. Eval.	Mes.
S27 [34]	✓	(i.) LINDDUN's privacy properties (S37)	(i.)STRIDE's security properties (ii.)ISO/IEC 27033-3:2010 security properties	✗	✗
S29 [35]	✓	(i.) Unlinkability, Transparency, and Intervenability	(i.) STRIDE	✓	✓

methodology that elicits both security and privacy requirements of the Internet of Medical Things (IoMT) by featuring both STRIDE and LINDDUN. The methodology comprises six stages: contextual knowledge, which connects security and privacy aspects; system decomposition using DFDs; identification of potential security and privacy threats; analyzing these threats; determining security and privacy properties; and selecting appropriate countermeasures for the identified threats.

b: SCOPE AND FOCUS

To analyze the scope and focus of the identified PSTMs, we used the criteria we applied for assessing and comparing PTMs. Instead of identification of privacy properties, we also add security properties as well as security measures, hence, the following:

(a) *a system description;*
(b) *identification of privacy and security properties;*
(d) *an evaluation of potential risks; and*
(e) *privacy and security measures envisaged.*

The two studies that proposed PTSMs have similarities and differences in scope and focus, as outlined in Table 12. The similarities are that the methodologies provide a systematic description based on DFDs and that they both elicit privacy and security requirements. Although this is the case, some differences can be identified. Given that the methodologies identify security and privacy properties, this is different for both of them. In S27, the authors use LINDDUN's privacy properties within their methodology. In S29, however, the authors introduce the privacy protection goals of unlinkability, transparency, and intervenability [82]. Compared with the privacy properties identified in LINDDUN, it can be noted that the privacy properties in S29 are limited [67].

When it comes to the security properties, both use STRIDE security properties. Given each threat elicited in STRIDE,[5] the security properties desired are authentication, integrity, non-repudiation, confidentiality, availability, and authorization [84]. However, in S27, the authors add security properties from ISO/IEC 27033-33:2010[6] on top of the desirable properties from STRIDE, i.e., access control, communication security, and opacity. Given this, we argue that the methodology introduced in S27 is extensive compared with that in S29 regarding eliciting security and privacy requirements. However, S29 provides a risk evaluation based on the DREAD methodology [85], which has been extended to assist in the quantification of security and privacy risks, and in addition, provides measures or controls for the identified threats. S27 does not include either risk evaluation or measures in its scope but maps the threats to the OWASP Top 10.[7]

c: VALIDATED AND EVALUATED PSTMS

As illustrated in Fig. 6, only one of the identified methodologies was tested in a real-world context, that is S29 [35]. However, the other methodology (S27) has not been evaluated or validated, which could challenge its practical applicability.

> ***Takeaway:*** *A key observation is that the maturity of both LINDDUN [29] and STRIDE [84] suggests that combining these methods will produce further benefits, as suggested in S27. This could elicit a comprehensive analysis of both security and privacy threats; however, there is no evidence of the performance of a combination.*

C. VALIDATION AND EVALUATION METHODS USED IN PIA AND PRAS

RQ1 aimed to identify the existing PIA and PRA methodologies in the scientific literature that have been validated or evaluated. Hence, we provided a classification as depicted in Fig. 6 based on the classification scheme proposed by Wieringa et al. [70]. In addition, it is essential to document the extent to which each methodology has been rigorously tested [71], [86]. This information not only instills confidence in the reliability of the methodology but also helps researchers and practitioners make informed decisions about its applicability and potential limitations. Hence, RQ2 aimed to identify how and to what extent the identified methodologies were scientifically validated or evaluated. For this reason, we identified the methods used to validate or evaluate the existing methodologies that have been validated or evaluated as per Fig. 6.

1) METHODS OF VALIDATION PERFORMED ON SELECTED METHODOLOGIES

Table 13 presents the studies that validated the methodologies and method of validation used. From the table, we see different use of validation methods that have been used to assess the reliability of the proposed methodologies. It is important to mention that we adopted these terms (validation methods) from the studies we analyzed. We observed that

[5]The STRIDE acronym stands for Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of Privilege [84].

[6]ISO/IEC 27033-3:2010, Information technology, Security techniques, Network security (https://www.iso.org/standard/51582.html)

[7]OWASP Top Ten (https://owasp.org/www-project-top-ten/)

TABLE 13. Summary of studies that validate privacy risk and impact assessment methodologies.

Validation Methods	Study ID
Invented use-case	S1
Illustrative scenario	S11 and S33
Illustrative example	S18 and S20
Illustrative use-case	S22
Realistic scenario	S19
Case study	*S21, S23, S24, S25, S30 and S39*
Comparative analysis	S31
Experiment	S32 and S35
Example application	S37

most of the studies that validated their methodologies used case studies, i.e., *S21, S23, S24, S25, S30 and S39*. However, while the authors have claimed to use case studies in these studies, we discovered that these case studies are based only on illustrative scenarios that helped the authors contextualize and exemplify the use of their proposed methodologies. By definition, a case study is *"an empirical inquiry that investigates a contemporary phenomenon (the "case") in depth and within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident."* [87]. This definition is supported in the context of software engineering [88]. Therefore, such proposals should be categorized just as a validation instead of an evaluation. This is because the methods of investigation are theoretical means and do not rely on real-world evidence. For instance, using an illustrative scenario (or example, use-case) or example application are abstract concepts that the authors of the various studies outlined in Table 13 use to exemplify the reliability of their methodologies. Technically, the authors of these papers describe a hypothetical situation designed to provide an example of how the methodology would perform in practice. This is the same as the invented and realistic scenarios where the authors depict circumstances that could occur in the real world.

The use of experiments in S32 and S35 falls under validation. In S32, the authors conducted practical experiments with students. However, these results are not based on real-world context or phenomena since they describe a scenario that provides the basis for the experiment. This is the same for S35, where they exemplify their proposal using illustrative DFD. Nevertheless, in *S25*, while their example case study was not truly in practice, they considered conducting a survey to analyze certain factors that could support the investigation of their methodology. In addition, the authors performed a comparative analysis (an example of validation) of four privacy risk assessment methodologies concerning the risks they aim to avoid, the measure of the likelihood of the risks, and the severity. Essentially, a comparative analysis compares two different objects (in our case, methodologies) based on defined criteria [89]. While certain studies, such as *S21*, *S22* and *S37* demonstrate a comprehensive and methodological validation of their approach, their successful methodological transfer to an industrial setting may be difficult based on the context, i.e., the use of fictitious examples or cases.

TABLE 14. Summary of studies that evaluate privacy risk and impact assessment methodologies.

Method of Evaluation	Study ID
Case study	S4, S14, S15, S16, S26, S28 and S29
Action research	S5
Empirical studies	S36

> ***Takeaway:*** *From the analysis of techniques used to validate the identified methodologies, we noticed that the case study method is interpreted and applied with great variation. This means the authors' term "case studies" refers to different concepts of case study validation, not only to the Case Study research method. This has also been observed in the research by Tuma, Calikli, and, Scandariato [38].*

2) METHODS OF EVALUATION PERFORMED ON SELECTED METHODOLOGIES

The evaluation methods used in the selected studies are listed in Table 14. Like in Table 13, we also observed that the "case study" method of evaluation was the most frequently used. However, the difference is that the methodologies in the studies outlined in Table 14 were conducted in real-world settings. That is, the authors of the studies test their proposed methodologies within a real-life context, for example, in the context of a Charity Organization as in the case of S14 [90], and not theoretically as identified in Table 13. The methods used for evaluation, for example, a case study, facilitate a deeper understanding of the application of the proposed methodologies within their real-world context.

In addition, we outline the context in which the methodologies were evaluated and the extent of evaluation in Table 15. In this case, context refers to the conditions or environment in which the methodology was evaluated. The extent, on the other hand, refers to the scope or range of evaluation of a given methodology. Concerning the information in the table, it can be seen that each methodology has been subjected to a certain degree of evaluation. For example, in S4, the authors evaluate the methodologies using three industrial case studies as well as a comparative analysis. We argue that such information can be used to infer the effectiveness and scalability of the methodologies.

Based on Ivarsson's scoring rubric for evaluating relevance [71], the methods of evaluation indicated in Table 14 are classified as contributing to relevance. For example, the use of action research in *S5* involves investigation of the methodology in practice, with the results generated aiming at improving the methodology and emphasizing its relevance in the industry. This is the same for study (*S36*), which

TABLE 15. Context and extent of evaluated methodologies.

Study ID	Context	Extent
S4	Industrial case studies from the VisiOn EU project	Three case studies & Comparative analysis - (CNIL, UK PIA, and BSI)
S5	Workshops with IT industry experts	Interviews, three comprehensive scenarios, and comparative analysis between the proposed PIA methodology, ISO 31000 and UK PIA Handbook based on the seven PIA quality criteria by Wright and De Hert [91].
S14	Charity organization	over 3-month case study, 3 evaluations - DPIA questions assessments (by three of each: practitioners, academics and peers), review workshop with delegates from 40 local charities, training of 29 staff
S15	Public Healthcare Enterprise (ASUGI - Azienda Sanitaria Universitaria Giuliano Isontina)	11 IT software devices that are already in use or the enterprise healthcare intends to use.
S16	DPIA in practice - analysis of real data processing operations	12 organizations - 3 start-ups, 2 SMEs, 5 large companies and 2 public administrations.
S26	Development of privacy-sensitive ubiquitous computing systems	Lo-fi prototypes, interviews with 20 people and a test with three users
S28	Application to Healthcare Management Software Project	Usability analysis - survey with 59 requirement engineers
S29	Quantitative threat analysis of a privacy-attribute based credential scenario	-
S36	LINDDUN from the perspective of requirement engineers and software architects	2 studies (Threat modeling in requirements engineering and architectural design) and a case study (with privacy experts)

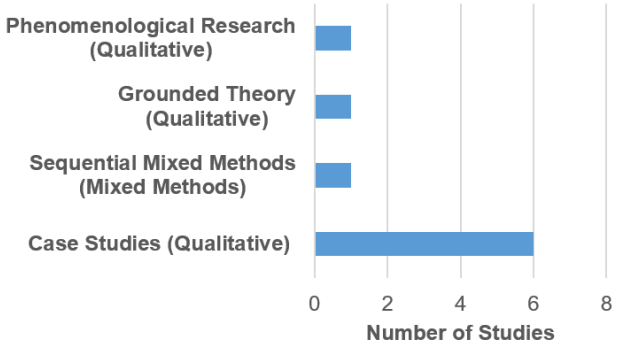

FIGURE 8. Research designs of studies that evaluate privacy risk and impact assessment methodologies.

is LINDDUN - out of the identified PTM methodologies, LINDDUN is observed as the only PTM that has been evaluated; this is, however, in a different context, i.e., a study that evaluates a methodology that the authors have previously proposed. Such methods have been shown to provide scientific rigor [92] as, in this case, they build the reliability of the proposed methodologies.

Furthermore, we classified the studies outlined in Table 14 based on the selection of research design, as depicted in Fig. 8, as described by Creswell and Creswell [93].

The aim was to conduct a critical appraisal to assess the quality of the studies in terms of methodological appropriateness [94]. Hence, we critically appraised these studies by conducting a critical appraisal of qualitative study using the critical appraisal questionnaire from the Center for Evidence-Based Management (CEBMa) [95]. The checklist contains 10 appraisal questions, where each question critically appraises a given study and assigns a ''Yes'', ''Can't tell'', or ''No'' answer. In this case, we used the questions from the checklist to assess how a study under review is reported, including the transferability of the proposed methodology. To do so, we assessed this based on the rigor and relevance of the research. Two authors were involved in critically appraising the studies; one performed the appraisal, and the other verified it. A discussion session was held to reach a common understanding in case of disagreements. The results of the critical appraisal are outlined in the subsequent section.

a: CRITICAL APPRAISAL OF QUALITATIVE STUDIES

Table 16 outlines the critical appraisal results of the qualitative studies identified in Fig. 8. Based on the appraisal, it is evident that all the studies identified that evaluated methodologies address a focused question/issue, follow an appropriate study design, and describe the context of their assessment clearly. However, most studies were found to have methodological weaknesses, particularly concerning the description of the methods for data collection and analysis. For instance, in S5 [21], the authors only briefly mentioned the methods of collecting data, i.e., the use of interviews. However, they did not clearly describe whether they were individual interviews or group interviews and how long the data collection method took. However, only two methodologies fulfilled the ***Q4***, i.e., **S14 and S36**. These two studies clearly described how they collect data. For example, *S14* provided a protocol for their case study [90] that indicated how they intended to collect data; however, they do not provide a procedure for data analysis. With regard to relevance, all studies checked where findings could be transferred or adapted to other settings.

Nevertheless, out of the methodologies, only *S36*, which is LINDDUN, checks all the questions within the CEBMa checklist, thus establishing rigorous standards and relevance.

TABLE 16. Critical appraisal of qualitative studies that evaluate methodologies - checklist from CEBMa [95] (Comment - yes is ✓, No is ✗).

Study ID	Quest. 1	Quest. 2	Quest. 3	Quest. 4	Quest. 5	Quest. 6	Quest. 7	Quest. 8	Quest. 9	Quest. 10
S4	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S5	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S14	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓
S15	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S16	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S26	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S28	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S29	✓	✓	✓	✗	✗	✗	✗	✓	✓	✓
S36	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Questions from the CEBMa Checklist: ***Quest. 1:*** *Did the study address a clearly focused question/issue?* ***Quest. 2:*** *Is the research method (study design) appropriate for answering the research question?* ***Quest. 3:*** *Was the context clearly described?* ***Quest. 4:*** *How was the fieldwork undertaken? Was it described in detail? Are the methods for collecting data clearly described?* ***Quest. 5:*** *Could the evidence (fieldwork notes, interview transcripts, recordings, documentary analysis, etc.) be inspected independently by others?* ***Quest. 6:*** *Are the procedures for data analysis reliable and theoretically justified? Are quality control measures used?* ***Quest. 7:*** *Was the analysis repeated by more than one researcher to ensure reliability?* ***Quest. 8:*** *Are the results credible, and if so, are they relevant for practice?* ***Quest. 9:*** *Are the conclusions drawn justified by the results?* ***Quest. 10:*** *Are the findings of the study transferable to other settings?*

The methodology provides not only data analysis but also a clear description of how the data used for evaluation were collected. They further provided supporting materials that could be independently inspected by others. The results of the studies are relevant for practice as the methodologies have been assessed in real-world settings; hence, the findings are transferable to other settings as the authors provide evidence of their use.

D. INDEPENDENT STUDIES THAT VALIDATE AND EVALUATE OTHER METHODOLOGIES

Considering that proposed PIA methodologies can be evaluated or validated by authors who propose the methodology, there are instances where these methodologies can be evaluated or validated in separate instances. On the one hand, the authors may choose to validate or evaluate their methodologies themselves. On the other hand, the evaluation or validation can be carried out by other researchers. This type of assessment helps ensure a more comprehensive and impartial examination of PIA methodologies. This is also the case for PTM and PRA methodologies. Table 17 summarizes the studies that validated previously proposed PIAs, PRAs, and PTMs. Given that study (S36) [67] was evaluated separately, we do not mention it here as we had already outlined it under the studies that evaluated privacy risk and impact assessment methodologies.

Technically, the studies in Table 17 use a comparative analysis type of methodology as they either compare selected methodologies (second column) based on a given criterion or based on a framework. For example, S6 appraises PIA methodologies based on a set of criteria, whereas S38 analyses studies based on a conceptual framework. We also observed that *CNIL* and *LINDDUN (S37)* appeared as some of the methodologies that were frequently analyzed as outlined in Table 17. Considering this, it can be concluded that the two methodologies (CNIL and LINDDUN) are the most popular in the privacy community.

VI. DISCUSSION

In this study, we identified existing PIA and PRA methodologies published in the scientific literature that have been validated or evaluated. In addition, we analyzed how and to what extent the methodologies were scientifically evaluated. Our results provide valuable insight into the state-of-the-art methodologies, i.e., PIA and PRA methodologies, in addition to PTMs, PSTMs, and SPIA. As follows, we will first summarize and discuss our main findings and, finally, consider potential directions for future research on the topic.

A. SUMMARY OF RESULTS

Several proposed methodologies were identified through this systematic review of the literature (refer to Fig. 5). However, the findings reveal that most of the proposed methodologies have only been validated, meaning that they have not yet been implemented and evaluated in real-world practice, for example, through empirical research, but only as illustrative scenarios. Based on Fig 5 – which indicates the type of research study, it can be identified that the overall share of studies that evaluate methodologies, i.e., 9 out of 39, is relatively small. This suggests that the topic is still growing in maturity in terms of empirical research on the assessment of methodologies that identify and evaluate privacy risks.

Out of the methodologies we identified as validated, the majority of them emerge from PRAs (8 methodologies out of 9), with the least coming from PIAs (2 out of 10 methodologies). In addition, we also noted that a significant number of PTMs have also been validated. Given that the context of validation differs, the validation methods are not as disparate as some of them use the terms ''illustrative'', ''experiment'', and ''case study''. Hence, such methodologies may become difficult to transfer to an industrial setting as they may lack relevance due to how their reliability is assessed [71] and insufficient scientific rigor [92]. We also observed the loose use of the terminology ''case study'' as a method of validation where authors claim using a case study research design

TABLE 17. Summary of studies that validate previously proposed PIAs or PTMs.

Study ID	Methodologies	Description
S2	ISO/IEC 29134:2017 & CNIL	A comparative analysis of results from the SWAN project to assess the performance of both ISO 29134:2017 and CNIL. The outcome of the analysis shows that CNIL performed better.
S3	S37, CNIL & ISO/IEC 29134:2017	A comparative assessment of DPIA methodologies based on evaluation questions and comparative metric. From the assessment, the ISO/IEC 29134:2017 performed well compared to CNIL and LINDDUN.
S6	Australia, Canada, Ireland, New Zealand, UK, and USA	A comparative analysis based on a set of 18 evaluation criteria to determine best elements for a DPIA
S7	The AICPA/CICA privacy risk assessment tool, The SPIA tool, GS1 EPC/RFID PIA Tool, iPIA tool, and Cloud computing PIA tool	A comparative analysis based on the operational and contextual usability, applicability, thoroughness, accessibility and privacy focus. In addition, a PIA evaluation and Grading System (PEGS) based on a set of criteria and weights is applied to the New Zealand Google Street View PIA and the Australian EVI PIA.
S8	PIA Guidance documents from 10 jurisdictions	Application of a set of 10 evaluation criteria for appraising PIA guidance documents. The results indicated that PIA documents with best practices are those of Ontario (1999/2001 and 2005), Alberta (2005/2009), the UK (2007), and Victoria (2009).
S9	S5, S12, UK PIA code of practice, New Zealand PIA toolkit, Australian ICO PIA guide, CNIL PIA method, Canada directive on PIA, PIAF methodology, and ISO/IEC 29134:2017	A comparative analysis based on a set of 17 evaluation criteria. The outcome is a comprehensive PIA methodology that is composed of six steps. However, we criticize the evaluation as we notice that S5 is crossed off as not fulfilling the legal framework column (legal framework used as a reference for defining privacy targets [30]); we point out that [21] derived the privacy targets from Directive 95/46/EC [75], and the then proposed GDPR.
S13	S5, S12, S37, CNIL, SDM, among others	An analysis of different approaches based on the description of processing activities, support of a DPIA methodology, coverage of concepts in Art. 29 Working Party, support for soundness criteria, tool support, document generator, and model management.
S34	S37 (and S35), STRIDE, CWE, CAPEC, OWASP, and CNIL	Comparison of existing privacy and security knowledge bases based on semantics, selection criteria, solution integration, extensibility and abstraction level. S37 is shown to fully support the description of threat type but partially support the condition and relationship of threat types. The difference between S37 and S35 is that while S37 partially supports the properties of selection criteria, it does not support application properties. This differs from S35, which partially supports application properties, including selection criteria properties. CNIL Knowledge base partially supports the description of threat types but does not support the properties.
S38	S30, S37, and Framework for Privacy-Friendly System Design	A comparison of the methodologies using terms and notions from a conceptual framework extended for privacy requirement engineering.

when they are, in fact, only using an illustrative example or hypothetical scenario for assessing the fulfillment of their methodology's requirements. Such types of illustrative or hypothetical scenarios are not directly attached to a real-world phenomenon from which empirical evidence can be gathered (through multiple sources of data) to enable an in-depth analysis of a case. For this reason, such studies would be best classified as ''use cases'' rather than more rigorous case studies, yet still serving validation purposes.

Based on our findings, we further observed that a few of the selected studies evaluate their methodologies. Five studies are from the category PIA, while one is in the PRA category. The other studies that follow are PSTM and PTM. From this, we identify that the overall share of evaluated PIAs is higher than the other methodologies. These studies used methods such as ''case study'', ''action research'', and ''empirical studies'' for evaluation purposes. The use of such methods further contributes to relevance [71] as the authors investigate the methodology in practice, hence gaining feedback from practitioners, as well as providing the practitioners with what they need. This helps to close the gap between research and practice, where the methodology is implemented and evaluated, and findings can be transferred in an industrial setting.

In addition to studies that evaluate and validate methodologies, we identified studies that validated methodologies that had been previously proposed. We observed that the majority of these studies validated these methodologies through comparative analysis. Essentially, they compare properties of these methodologies, for instance, risk analysis, knowledge bases, support of a PIA methodology, etc.

We, however, noted that four methodologies, as depicted in Fig. 6, have so far neither been validated nor evaluated, i.e., S9 [30], S10 [48], S17 [33], and S27 [34].

Concerning the scope and focus of the methodologies, we identified differences between certain requirements in their methodological scope. Under PIAs, we identified that whereas all methodologies addressed different requirements, the component of risk assessment was a core element in all (refer to Table 7). However, only a few address or assess privacy harms, which suggests the need to have full-blown PIA methodologies that assess privacy harms. Additionally, we identified a sub-set of sector-specific methodologies, thus highlighting the main focus and application of the methodology. The existence of system-specific PIAs creates heterogeneity within the methodologies, where we have PIAs that focus on particular systems, for example, the methodology in S1 [45] focuses on IdM systems and the methodology in S10 focuses on AI systems [48]. This suggests that there are a few methods, which assess from onset privacy risks in underlying systems such as AI models. In light of this, we expect to see more proposals that target

specific systems in the scientific literature. Evidently, given the shift towards Large Language Models (LLMs) and AI systems, we expect to see methodologies that assess AI systems and Machine or Deep Learning models, including the datasets involved, to assess if they can result in high risks to the rights and freedoms of natural persons. With such an emergence, and with the existing sector-specific methodologies we have identified, practitioners can easily review existing methodologies in the area and choose the ones that best fit their needs and organizations.

We also analyzed the scope and focus of PRAs. We observed that semi-quantitative and qualitative types of risk evaluation are often considered subjective, leading to further studies that proposed quantification techniques for risk assessment as a way of moving toward objectivity. However, none of the methodologies that proposed a quantitative PRA assesses the method in practice to prove its acceptability and feasibility with real stakeholders. We also identified that a majority of the PRA methodologies assess privacy harms, indicating the need to assess how data subjects can be impacted when processing personal data.

Similarly, during the analysis of the scope and focus of PTMs, we identified that the methodologies differed based on the privacy properties, as well as concerning risk evaluation and privacy measures. Nevertheless, as discussed earlier, a key takeaway is that LINDDUN [29] emerged as the most evolved methodology, with several publications enhancing it having been identified during the analysis. The same goes for methodologies identified under PTSMs, where the scope and focus differ regarding privacy and security properties. We note, however, that both methodologies leverage STRIDE to elicit security threats. However, given the role of PTMs and PSTMs, which are to elicit privacy and security threats, we argue that privacy harms are not part of the scope of such methodologies.

Regarding the critical appraisal of the evaluated methodologies, it was observed that most of the studies still need to improve in terms of methodological soundness. It is, however, important to emphasize here that conducting research on the evaluation of PIAs, PRAs, and other methodologies is significantly challenging. For such methodologies to be implemented and evaluated in the real world, researchers must have strong collaborations with organizations, involving several practitioners and assessing real systems. Ethical considerations must also be observed when involving organizations and human subjects, as well as the potential need for non-disclosure agreements to protect intellectual property and confidentiality. Therefore, it is important to think about realistic and feasible research designs in which researchers and industry can cooperate without setting impossible requirements for evaluation research studies. Notwithstanding, one particular example of a well-evaluated methodology is LINDDUN, which has so far surpassed the rest in terms of methodological soundness and can be used as inspiration for future studies in the area. Hence, it can also be argued that critical appraisal methods, such as the ones adopted in the SLR, could also be employed by individual researchers or practitioners to draw conclusions and make informed decisions about the methodological strengths or weaknesses of the available research.

B. RESEARCH DIRECTIONS

1) EVALUATION RESEARCH

This SLR shows that although several studies have proposed solutions for PIAs, PRAs, PTMs, and other related methodologies, the number of studies that have validated or evaluated their solutions is still significantly small. The empirical investigation of such methodologies in practice is key to providing insight and feedback on what practitioners require and encouraging the integration of academic contributions (such as PIA and PRA methodologies) into industrial practices.

Therefore, further evaluation studies for prominent methodologies (e.g., S22 [22], S30 [61], S31 [62]) that have so far only been validated can be considered as promising pathways for future research. In addition, some methodologies that have already been evaluated (e.g., LINDDUN [29], [67], S14 [52], S28 [60]) also still lack independent evaluations from other researchers (i.e., besides the original authors), opening fronts for rigorous replication studies to corroborate or add new findings. Two PIA methods, S9 [30] and S10 [48], have yet to be validated in future research.

We also recommend that future evaluation studies consider the quality requirements, such as the ones used for critical appraisal [95], in the inception of the research design. Case studies are shown to be one of the most common methodologies for evaluation; nonetheless, other methodologies could be considered, such as using grounded theory in the context of socio-technical systems [96]. This need for further evaluation research has also been discussed in the broader area of privacy engineering [14], [97].

2) PRIVACY RISK ASSESSMENTS

During our analysis, we identified studies that assess PIAs based on a defined criteria, for instance, S2 [46], S3 [47], S6 [41], S7 [40], S8 [19], and S9 [30]. However, we found that such studies that assess PRAs are still missing. Hence, this can be considered as a track for further research where PRA methodologies can be compared to assess their properties and comprehensiveness. We argue that such an analysis would provide detailed information on the usability, reliability, and adoption of the methodology in the assessment of privacy risks during the development phase of a system.

Based on Fig. 6, we also observed that most of the identified PRAs are validated. Given that these independent PRA methodologies are developed to be integrated with PIAs, a lack of evaluation can hinder such integration. As such, further research can be conducted where PRA methodologies are evaluated and integrated within PIA processes. This

will further indicate the level of maturity of the identified methodologies and how they can be further improved.

In addition, the practicality of assessing privacy harms within PRA methodologies that assess harms needs to be considered. While a single study identifies actual privacy harms to data subjects, i.e., S18 [54], we argue that the integration of such harms into PRAs as well as full-fledged PIAs is needed to enhance risk assessments. We assert that by extrapolating PRAs with actual privacy harms, there could be an adequate understanding of the impact on the privacy of data subjects during the processing of personal data and hence uptake of appropriate countermeasures that could reduce/prevent privacy risks that can result in the identified privacy harms.

3) PRIVACY AND SECURITY THREAT MODELING AND SECURITY AND PRIVACY IMPACT ASSESSMENT

As seen in Fig. 6, there are few studies that proposed both PSTMs and SPIAs. This suggests that these areas could be further explored as potential research pathways. We believe such methodologies can provide a more comprehensive elicitation of both privacy and security threats since security plays a crucial role in maintaining or ensuring privacy. Such approaches would not only address privacy risks during the design stage but also security risks.

In addition, we also observed a lack of evaluation on two methodologies, i.e., S17 and S27. Evaluating these methodologies in practice can be an advantage to demonstrate reliability with regard to handling security and privacy risks. Additionally, a comparison between these methodologies would be beneficial in providing an analysis of the scope and focus. This would further provide an overview of the comprehensiveness of a given methodology.

VII. THREATS TO VALIDITY

Here, we identify and discuss the main threats to validity related to this SLR in terms of publication type bias, study selection bias, and data extraction bias.

A. PUBLICATION TYPE BIAS

Considering we agreed to include studies that have been peer-reviewed, we excluded publications, for example, books or book chapters. Hence, focusing on peer-reviewed publications could have led to the omission of other publication types that propose a methodology that could have been relevant to our research. This limitation is nonetheless justified since SLRs should concentrate on the scientific literature, seeking evidence of the highest quality in the field.

B. STUDY SELECTION BIAS

During the selection process (the first screening phase (Title & Abstract) and second screening phase (Full-Text Format)) were based on the inclusion and exclusion criteria. Therefore, unintentional bias can potentially be introduced by excluding studies that seemed ineligible but had a chance of being eligible. To avoid this as much as possible, we used a double-blind approach with two independent reviewers, also discussing any emerging conflicts in both screening phases, thus ensuring that the studies relevant to our research were included. This ensured that the review we conducted was impacted less by selection bias. In addition, we have provided a replication package that other researchers can use to replicate the review, ensuring the reliability and validity of the findings. Hence, while a potential limitation can also be identified in the lack of maintaining the number of articles excluded based on and per each criterion, we believe the replication package can be useful in articulating how studies were screened and selected, including reasons for exclusion.

C. DATA EXTRACTION BIAS

While we identified the information that needed to be extracted for our review, we acknowledge that the process of data extraction can be subjective, and hence, the interpretation of the data to be extracted could have introduced bias. Nevertheless, given that we had designed a data extraction form and agreed upon it, we ensured that we followed good practices by ensuring uniformity in the data extraction process, thus reducing bias and increasing reliability. Therefore, every study included in the review has its data extraction form that originates from a standardized data extraction form.

VIII. CONCLUDING REMARKS AND OUTLOOK

This SLR was undertaken with the objective of critically examining existing methodologies for PIAs and PRAs that have been subjected to either scientific validation or evaluation. The scope of the validation or evaluation, as well as the methodology and techniques employed, was of particular interest. This inquiry was necessitated by prevailing criticisms, which suggest a deficiency in these methodologies, particularly in terms of their lack of a rigorous and systematic evaluation process [9], [14].

The findings of this SLR indicate that a significant proportion of existing methodologies have only been validated, or lack a rigorous and systematic evaluation. This validation often does not involve implementation and evaluation in real-world scenarios but rather relies on illustrative examples or hypothetical situations. This observation underscores the existence of substantial empirical and practical gaps in the field, which could hinder the effective translation of research findings into industrial applications. There is a pressing need for rigorous empirical studies to systematically evaluate existing PIA and PRA methodologies. Currently, only a handful of scientifically published methodologies have undergone practical testing. Therefore, it is crucial that the methodologies proposed by researchers are evaluated in real-world settings to foster their adoption in industrial contexts. Our review also revealed that many studies exhibit common methodological shortcomings, with the notable exception of LINDDUN, which emerged as a well-researched methodology in our analysis. We posit that further research

on existing methodologies could provide valuable evidence to inform decision-making among researchers and practitioners.

In light of the findings from this SLR on evaluation research, we contend that it would also be beneficial to explore the current landscape of security risk assessment methodologies. These methodologies are utilized for enumerating security threats, impacts, and risk levels. Investigating these would allow us to ascertain the present maturity level of validation and evaluation studies in this closely related area. This could yield a comprehensive overview of the evaluated methodologies in both the privacy and security domains.

A. FUTURE WORK

Given that we identified the practicality of assessing privacy harms within PRAs, our future work will focus on the integration of actual privacy harms within a privacy risk assessment to enhance DPIA methodologies. We argue that this will not only increase the quality of privacy risk assessments in terms of assessing harms but also enhance the understanding of privacy risks. Based on this, appropriate countermeasures (or privacy-enhancing technologies) can be selected to reduce or prevent privacy harm.

In addition, we hope to revisit the topic in the future to assess whether the state has changed, i.e., in terms of the evaluation of privacy impact assessment and privacy risk assessment methodologies, as well as to extend the study. Based on new studies, we will aim to see whether more PIAs and PRAs have been evaluated.

REFERENCES

[1] A. Cavoukian, "Privacy by design: The 7 foundational principles," Inf. Privacy Commissioner, ON, Canada, pp. 1–12, 2009, vol. 5.
[2] G. Greenleaf, "Global Data Privacy Laws 2023: 162 National Laws and 20 Bills," 181 Privacy Laws Bus. Int. Rep. (PLBIR) 1, 2-4, UNSW Law Res. Paper 23-48, 2023. [Online]. Available: https://ssrn.com/abstract=4426146 and http://dx.doi.org/10.2139/ssrn.4426146
[3] European Commission, "Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation)," *J. Eur. Union*, vol. 119, pp. 1–88, Apr. 2016.
[4] R. Clarke, "Privacy impact assessment: Its origins and development," *Comput. Law Secur. Rev.*, vol. 25, no. 2, pp. 123–135, Jan. 2009.
[5] D. Wright, "The state of the art in privacy impact assessment," *Comput. Law Secur. Rev.*, vol. 28, no. 1, pp. 54–61, Feb. 2012.
[6] S. J. De and D. Le Métayer, "Privacy risk analysis," in *Privacy Risk Analysis*. Berlin, Germany: Springer, 2016, pp. 63–79.
[7] C. T. Di Iorio, F. Carinci, J. Azzopardi, V. Baglioni, P. Beck, S. Cunningham, A. Evripidou, G. Leese, K. F. Loevaas, G. Olympios, M. O. Federici, S. Pruna, P. Palladino, S. Skeie, P. Taverner, V. Traynor, and M. M. Benedetti, "Privacy impact assessment in the design of transnational public health information systems: The BIRO project," *J. Med. Ethics*, vol. 35, no. 12, pp. 753–761, Dec. 2009. [Online]. Available: https://jme.bmj.com/content/35/12/753
[8] B. Stewart, "Privacy impact assessment: Optimising the regulator's role," in *Privacy Impact Assessment*. Dordrecht, The Netherlands: Springer, 2012, pp. 437–444.
[9] M. Friedewald, I. Schiering, N. Martin, and D. Hallinan, "Data protection impact assessments in practice: Experiences from case studies," in *Proc. Int. Workshops Comput. Secur. (ESORICS)* (Lecture Notes in Computer Science), vol. 13106. Cham, Switzerland: Springer, 2022, pp. 424–443.
[10] F. Ferra, I. Wagner, E. Boiten, L. Hadlington, I. Psychoula, and R. Snape, "Challenges in assessing privacy impact: Tales from the front lines," *Secur. Privacy*, vol. 3, no. 2, p. e101, Mar. 2020.
[11] A. S. Ahmadian, D. Strüber, V. Riediger, and J. Jürjens, "Supporting privacy impact assessment by model-based privacy analysis," in *Proc. 33rd Annu. ACM Symp. Appl. Comput.* New York, NY, USA: Association for Computing Machinery, 2018, pp. 1467–1474, doi: 10.1145/3167132.3167288.
[12] J. van Puijenbroek and J.-H. Hoepman, "Privacy impact assessments in practice: Outcome of a descriptive field research in The Netherlands," in *Proc. Int. Workshop Privacy Eng., 3rd Int. Workshop Privacy Eng., 38th IEEE Symp. Security Privacy*. San Jose, CA, USA, 2017, pp. 1–8.
[13] L. Fritsch and H. Abie, "Towards a research road map for the management of privacy risks in information systems," in *SICHERHEIT 2008—Sicherheit, Schutz und Zuverlässigkeit. Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft Fü Informatik*. Bonn, Germany: Gesellschaft Für Informatik, 2008, pp. 1–15.
[14] L. H. Iwaya, M. A. Babar, and A. Rashid, "Privacy engineering in the wild: Understanding the practitioners' mindset, organisational aspects, and current practices," *IEEE Trans. Softw. Eng.*, vol. 49, no. 9, pp. 4324–4348, Sep. 2023.
[15] B. Kitchenham, "Procedures for performing systematic reviews," *Keele, UK, Keele Univ.*, vol. 33, pp. 1–26, Jul. 2004.
[16] D. Moher, P.-P. Group, L. Shamseer, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, P. Shekelle, and L. A. Stewart, "Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement," *Systematic Rev.*, vol. 4, no. 1, pp. 1–9, Dec. 2015.
[17] Commission Nationale de l'Informatique et des Libertés (CNIL). *Privacy Impact Assessment (PIA) Methodology (How To Carry Out a PIA)*. Accessed: Jun. 2015. [Online]. Available: https://www.cnil.fr/sites/cnil/files/typo/document/CNIL-PIA-1-Methodology.pdf
[18] *Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing is 'Likely to Result in a High Risk' for the Purposes of Regulation 2016/679*. Accessed: 2017. [Online]. Available: https://ec.europa.eu/newsroom/article29/items/611236
[19] R. Clarke, "An evaluation of privacy impact assessment guidance documents," *Int. Data Privacy Law*, vol. 1, no. 2, pp. 111–120, May 2011.
[20] R. Clarke, "What's privacy," in *Proc. Austral. Law Reform Commission Workshop*, vol. 28, 2006, pp. 1–8.
[21] M. C. Oetzel and S. Spiekermann, "A systematic methodology for privacy impact assessments: A design science approach," *Eur. J. Inf. Syst.*, vol. 23, no. 2, pp. 126–150, Mar. 2014.
[22] S. J. De and D. Le Métayer, "PRIAM: A privacy risk analysis methodology," in *Data Privacy Management and Security Assurance*. Crete, Greece: Springer, 2016, pp. 221–229.
[23] European Commission. *Privacy and Data Protection Impact Assessment Framework for RFID Applications*. Accessed: 2011. [Online]. Available: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
[24] *Conducting Privacy Impact Assessments Code of Practice*, V. 1.0, Inf. Commissioner's Office (ICO), London, U.K., 2014.
[25] D. Wright, K. Wadhwa, M. Lagazio, C. Raab, and E. Charikane, "Integrating privacy impact assessment in risk management," *Int. Data Privacy Law*, vol. 4, no. 2, pp. 155–170, May 2014.
[26] I. Wagner and E. Boiten, "Privacy risk assessment: From art to science, by metrics," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Barcelona, Spain: Springer, 2018, pp. 225–241.
[27] L. D. Corte and R. Van Brakel, "Data protection impact assessment methods for the urban environment," Rep. Commissie Persoonsgegevens Amsterdam (CPA), 2022, pp. 1–69.
[28] L. Sion, D. Van Landuyt, K. Wuyts, and W. Joosen, "Privacy risk assessment for data subject-aware threat modeling," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2019, pp. 64–71.
[29] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements," *Requir. Eng.*, vol. 16, no. 1, pp. 3–32, 2011.
[30] K. Vemou and M. Karyda, "Evaluating privacy impact assessment methods: Guidelines and best practice," *Inf. Comput. Secur.*, vol. 28, no. 1, pp. 35–53, 2019.
[31] M. Friedewald, I. Schiering, N. Martin, and D. Hallinan, "Data protection impact assessments in practice: Experiences from case studies," in *Proc. Eur. Symp. Res. Comput. Secur.* Cham, Switzerland: Springer, 2021, pp. 424–443.
[32] M. Alshammari and A. Simpson, "Towards an effective privacy impact and risk assessment methodology: Risk assessment," in *Trust, Privacy and Security in Digital Business*. Regensburg, Germany: Springer, 2018, pp. 85–99.

[33] E.-L. Makri, Z. Georgiopoulou, and C. Lambrinoudakis, "A proposed privacy impact assessment method using metrics based on organizational characteristics," in *Computer Security*. Luxembourg City, Luxembourg: Springer, 2020, pp. 122–139.
[34] C. Treacy, J. Loane, and F. McCaffery, "A developer driven framework for security and privacy in the," in *Systems, Software and Services Process Improvement*. Düsseldorf, Germany: Springer, 2020, pp. 107–119.
[35] J. Luna, N. Suri, and I. Krontiris, "Privacy-by-design based on quantitative threat modeling," in *Proc. 7th Int. Conf. Risks Secur. Internet Syst. (CRiSIS)*, 2012, pp. 1–8.
[36] G. Georgiadis and G. Poels, "Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review," *Comput. Law Secur. Rev.*, vol. 44, Apr. 2022, Art. no. 105640.
[37] W. Xiong and R. Lagerström, "Threat modeling—A systematic literature review," *Comput. Secur.*, vol. 84, pp. 53–69, Jul. 2019.
[38] K. Tuma, G. Calikli, and R. Scandariato, "Threat analysis of software systems: A systematic literature review," *J. Syst. Softw.*, vol. 144, pp. 275–294, Oct. 2018.
[39] J. Biolchini, P. G. Mian, A. C. C. Natali, and G. H. Travassos, "Systematic review in software engineering," Syst. Eng. Comput. Sci. Dept., COPPE/UFRJ, Rio de Janeiro, Tech. Rep., ES 679, 2005.
[40] K. Wadhwa and R. Rodrigues, "Evaluating privacy impact assessments," *Innov., Eur. J. Social Sci. Res.*, vol. 26, nos. 1–2, pp. 161–180, Mar. 2013.
[41] D. Wright, R. Finn, and R. Rodrigues, "A comparative analysis of privacy impact assessment in six countries," *J. Contemp. Eur. Res.*, vol. 9, no. 1, pp. 161–180, Jan. 2013.
[42] D. Giustini and M. N. K. Boulos, "Google scholar is not enough to be used alone for systematic reviews," *Online J. Public Health Informat.*, vol. 5, no. 2, p. 214, Jun. 2013.
[43] M. Gusenbauer and N. R. Haddaway, "Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of Google scholar, PubMed, and 26 other resources," *Res. Synth. Methods*, vol. 11, no. 2, pp. 181–217, Mar. =2020.
[44] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, May 2014, pp. 1–10.
[45] C. T. López, I. A. Domingo, and J. V. Torrijos, "Approaching the data protection impact assessment as a legal methodology to evaluate the degree of privacy by design achieved in technological proposals. A special reference to identity management systems," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, 2021, pp. 1–9.
[46] T. Bisztray, N. Gruschka, V. Mavroeidis, and L. Fritsch, "Data protection impact assessment in identity control management with a focus on biometrics," in *Proc. Open Identity Summit*, 2020, pp. 185–192.
[47] T. Bisztray and N. Gruschka, "Privacy impact assessment: Comparing methodologies with a focus on practicality," in *Secure IT Systems*. Aalborg, Denmark: Springer, 2019, pp. 3–19.
[48] Y. Ivanova, "The data protection impact assessment as a tool to enforce non-discriminatory AI," in *Privacy Technologies and Policy*. Lisbon, Portugal: Springer, 2020, pp. 3–24.
[49] J. Reuben, L. A. Martucci, S. Fischer-Hübner, H. S. Packer, H. Hedbom, and L. Moreau, "Privacy impact assessment template for provenance," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, 2016, pp. 653–660.
[50] F. Bieker, M. Friedewald, M. Hansen, H. Obersteller, and M. Rost, "A process for data protection impact assessment under the European general data protection regulation," in *Privacy Technologies and Policy*. Frankfurt, Germany: Springer, 2016, pp. 21–37.
[51] L. Sion, P. Dewitte, D. Van Landuyt, K. Wuyts, P. Valcke, and W. Joosen, "DPMF: A modeling framework for data protection by design," *Enterprise Model. Inf. Syst. Architectures (EMISAJ)*, vol. 15, pp. 1–10, Jan. 2020.
[52] J. Henriksen-Bulmer, S. Faily, and S. Jeary, "DPIA in context: Applying DPIA to assess privacy risks of cyber physical systems," *Future Internet*, vol. 12, no. 5, p. 93, May 2020.
[53] M. Todde, M. Beltrame, S. Marceglia, and C. Spagno, "Methodology and workflow to perform the data protection impact assessment in healthcare information systems," *Informat. Med. Unlocked*, vol. 19, Jan. 2020, Art. no. 100361.
[54] S. Wairimu and L. Fritsch, "Modelling privacy harms of compromised personal medical data–beyond data breach," in *Proc. 17th Int. Conf. Availability, Rel. Secur.*, Aug. 2022, pp. 1–9.
[55] S. Hart, A. L. Ferrara, and F. Paci, "Fuzzy-based approach to assess and prioritize privacy risks," *Soft Comput.*, vol. 24, no. 3, pp. 1553–1563, Feb. 2020.
[56] S. J. De and D. Le Métayer, "A refinement approach for the reuse of privacy risk analysis results," in *Privacy Technologies and Policy*. Berlin, Germany: Springer, 2017, pp. 52–83.
[57] S. Agarwal, "Developing a structured metric to measure privacy risk in privacy impact assessments," in *Proc. IFIP Int. Summer School Privacy Identity Manag.*, Edinburgh, U.K. 2016, pp. 141–155.
[58] R. J. Cronk and S. S. Shapiro, "Quantitative privacy risk analysis," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Sep. 2021, pp. 340–350.
[59] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in *Proc. 5th Conf. Designing Interact. Syst., Processes, Practices, Methods, Techn.*, 2004, pp. 91–100.
[60] M. T. J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar, and R. A. Khan, "P-STORE: Extension of STORE methodology to elicit privacy requirements," *Arabian J. Sci. Eng.*, vol. 46, no. 9, pp. 8287–8310, Sep. 2021.
[61] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: The PriS method," *Requirements Eng.*, vol. 13, no. 3, pp. 241–255, Sep. 2008.
[62] L. Sion, K. Wuyts, K. Yskout, D. Van Landuyt, and W. Joosen, "Interaction-based privacy threat elicitation," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Apr. 2018, pp. 79–86.
[63] A. Rodrigues, M. L. Villela, and E. Feitosa, "PTMOL: A suitable approach for modeling privacy threats in online social networks," in *Proc. 21st Brazilian Symp. Human Factors Comput. Syst.*, Oct. 2022, pp. 1–12.
[64] A. Al-Momani, C. Bösch, K. Wuyts, L. Sion, W. Joosen, and F. Kargl, "Mitigation lost in translation: Leveraging threat information to improve privacy solution selection," in *Proc. 37th ACM/SIGAPP Symp. Appl. Comput.*, Apr. 2022, pp. 1236–1247.
[65] K. Wuyts, L. Sion, D. Van Landuyt, and W. Joosen, "Knowledge is power: Systematic reuse of privacy knowledge for threat elicitation," in *Proc. IEEE Secur. Privacy Workshops (SPW)*, May 2019, pp. 80–83.
[66] K. Wuyts, D. Van Landuyt, A. Hovsepyan, and W. Joosen, "Effective and efficient privacy threat modeling through domain refinements," in *Proc. 33rd Annu. ACM Symp. Appl. Comput.*, Apr. 2018, pp. 1175–1178.
[67] K. Wuyts, R. Scandariato, and W. Joosen, "Empirical evaluation of a privacy-focused threat modeling methodology," *J. Syst. Softw.*, vol. 96, pp. 122–138, Oct. 2014.
[68] K. Beckers, "Comparing privacy requirements engineering approaches," in *Proc. 7th Int. Conf. Availability, Rel. Secur.*, Aug. 2012, pp. 574–581.
[69] P. Grace, D. Burns, G. Neumann, B. Pickering, P. Melas, and M. Surridge, "Identifying privacy risks in distributed data services: A model-driven approach," in *Proc. IEEE 38th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2018, pp. 1513–1518.
[70] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requirements Eng.*, vol. 11, no. 1, pp. 102–107, Mar. 2006.
[71] M. Ivarsson and T. Gorschek, "A method for evaluating rigor and industrial relevance of technology evaluations," *Empirical Softw. Eng.*, vol. 16, no. 3, pp. 365–395, Jun. 2011.
[72] P. D. Bruza and T. Van der Weide, *The Semantics of Data Flow Diagrams*. Citeseer, 1989.
[73] M. Hansen, M. Jensen, and M. Rost, "Protection goals for privacy engineering," in *Proc. IEEE Secur. Privacy Workshops*, San Jose, CA, USA, May 2015, pp. 159–166.
[74] J. Henriksen-Bulmer, S. Faily, and S. Jeary, "Implementing GDPR in the charity sector: A case study," in *Proc. IFIP Int. Summer School Privacy Identity Manag.*, 2019, pp. 173–188.
[75] (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data*. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
[76] D. J. Solove, "A taxonomy of privacy," in *University of Pennsylvania Law Review*. HeinOnline, 2006, pp. 477–564.
[77] J. D. Lipton, "Mapping online privacy," *Nw. UL Rev.*, vol. 104, p. 477, Jan. 2010.
[78] K. Wuyts, L. Sion, and W. Joosen, "LINDDUN GO: A lightweight approach to privacy threat modeling," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, Sep. 2020, pp. 302–309.
[79] M. Howard and S. Lipner, *The Security Development Lifecycle*, vol. 8. Redmond, WA, USA: Microsoft Press, 2006.
[80] K. Wuyts and W. Joosen, "LINDDUN privacy threat modeling: A tutorial," Tech. Rep. CW 685, Jul. 2015.

[81] Z. Mardani Korani, A. Moin, A. Rodrigues da Silva, and J. C. Ferreira, "Model-driven engineering techniques and tools for machine learning-enabled IoT applications: A scoping review," *Sensors*, vol. 23, no. 3, p. 1458, Jan. 2023.
[82] H. Zwingelberg and M. Hansen, "Privacy protection goals and their implications for eID systems," in *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*. Berlin, Germany: Springer, 2011, pp. 245–260.
[83] D. Dhillon, "Developer-driven threat modeling: Lessons learned in the trenches," *IEEE Secur. Privacy*, vol. 9, no. 4, pp. 41–47, Jul. 2011.
[84] A. Shostack, *Threat Modeling: Designing for Security*. Hoboken, NJ, USA: Wiley, 2014.
[85] M. Howard and D. LeBlanc, *Writing Secure Code*. London, U.K.: Pearson, 2003.
[86] M. Ivarsson and T. Gorschek, "Technology transfer decision support in requirements engineering research: A systematic review of REj," *Requirements Eng.*, vol. 14, no. 3, pp. 155–175, Jul. 2009.
[87] R. K. Yin, *Case Study Research: Design and Methods*, vol. 5. Thousand Oaks, CA, USA: SAGE, 2009.
[88] P. Runeson and M. Höst, "Guidelines for conducting and reporting case study research in software engineering," *Empirical Softw. Eng.*, vol. 14, no. 2, pp. 131–164, Apr. 2009.
[89] R. Bolbakov, A. Sinitsyn, and V. Y. Tsvetkov, "Methods of comparative analysis," *J. Phys., Conf.*, vol. 1679, no. 5, 2020, Art. no. 052047.
[90] J. Henriksen-Bulmer and S. Faily. (Oct. 2020). *GDPR Implementation Case Study Protocol*. [Online]. Available: https://figshare.com/articles/online_resource/GDPR_Implementation_Case_Study_Protocol/12220250
[91] D. Wright and P. De Hert, *Privacy Impact Assessment*, vol. 6. Berlin, Germany: Springer, 2012.
[92] T. Dyba, B. A. Kitchenham, and M. Jorgensen, "Evidence-based software engineering for practitioners," *IEEE Softw.*, vol. 22, no. 1, pp. 58–65, Jan. 2005.
[93] J. Creswell, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Thousand Oaks, CA, USA: SAGE, 2007. [Online]. Available: https://books.google.se/books?id=DetLkgQeTJgC
[94] E. Barends, D. Rousseau, and R. Briner. (2017). *CEBMa Guideline for Critically Appraised Topics in Management and Organizations*. [Online]. Available: https://cebma.org/wp-content/uploads/CEBMa-CAT-Guidelines.pdf
[95] Center for Evidence-Based Management. (2014). *Critical Appraisal of a Qualitative Study)*. [Online]. Available: https://cebma.org/wp-content/uploads/Critical-Appraisal-Questions-for-a-Qualitative-Study-July-2014-1.pdf
[96] R. Hoda, "Socio-technical grounded theory for software engineering," *IEEE Trans. Softw. Eng.*, vol. 48, no. 10, pp. 3808–3832, Oct. 2022.
[97] L. H. Iwaya, G. H. Iwaya, S. Fischer-Hübner, and A. V. Steil, "Organisational privacy culture and climate: A scoping review," *IEEE Access*, vol. 10, pp. 73907–73930, 2022.

SAMUEL WAIRIMU was born in 1988. He received the master's degree in cybersecurity from the University of Chester, U.K., in 2019. He is currently pursuing the Ph.D. degree in computer science with the Department of Mathematics and Computer Science, Karlstad University, Sweden. In 2002, he joined Karlstad University, where he is with the Privacy and Security (PriSec) Research Group, contributing to the DigitalWell Arena Project through his research on the security and privacy of mobile medical systems. His research interests include cybersecurity, cyberwarfare, information security and privacy, digital health, and privacy engineering.

LEONARDO HORN IWAYA (Member, IEEE) was born in 1988. He received the B.Sc. degree in computer science from Santa Catarina State University, Brazil, the M.Sc. degree in electrical engineering from the University of São Paulo, and the Ph.D. degree in computer science from Karlstad University, Sweden. From 2011 to 2014, he was a Research Assistant with the Laboratory of Computer Networks and Architecture (LARC), PCS-EPUSP. From 2019 to 2021, he was a Postdoctoral Researcher with the School of Computer Science, The University of Adelaide, Australia, as part of the Cyber Security Cooperative Research Centre (CSCRC). From 2021 to 2022, he was a Postdoctoral Researcher with the Interdisciplinary Research Group on Knowledge, Learning and Organizational Memory (KLOM), Federal University of Santa Catarina. He is currently an Associate Senior Lecturer with the Department of Mathematics and Computer Science, Karlstad University. He is also with the Privacy and Security (PriSec) Research Group, Karlstad University, contributing to projects, such as CyberSecurity4Europe, TRUEdig, SURPRISE, DHINO, and DigitalWell Arena. His research interests include privacy engineering, cybersecurity, human factors, mobile and ubiquitous health systems, and the privacy impacts of new technologies.

LOTHAR FRITSCH was born in 1970. He received the Diploma degree in computer science from Saarland University, Saarbrücken, Germany, in 1999, the Ph.D. degree from Goethe University, Frankfurt, Germany, in 2009, and the Docent degree in computer science from Karlstad University, Sweden, in 2016. From 1999 to 2001, he was the Product Manager in financial transactions security and digital signatures with fun communications in Karlsruhe, Germany. In 2006, he was the Co-Founder of the ESA Galileo-funded start-up Samango GmbH, Darmstadt, Germany. In 2020, he joined Oslo Metropolitan University, Oslo, Norway, as a Professor of applied information security. His research interests include information privacy, information security risk assessment, cybersecurity, ethical AI, and digital identity.

STEFAN LINDSKOG was born in 1967. He received the Licentiate and Ph.D. degrees in computer engineering from the Chalmers University of Technology, Gothenburg, Sweden, in 2000 and 2005, respectively, and the Docent degree in computer science from Karlstad University, Karlstad, Sweden, in 2008. In 1990, he joined the Department of Computer Science, Karlstad University, where he is currently a Full Professor. He has authored/coauthored one textbook, eight book chapters, and more than 70 journals and conference papers. His research interests include the design of tunable and adaptable security services and security and performance analysis of security services and protocols.