Journal of Ethics and Emerging Technologies

IEET

Review

The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices

Charles Ribeiro Quainoo [1,*] and Md Atiqur Rahman Ahad [2]

[1] University of East London, London, UK; u2572490@uel.ac.uk
[2] Department of Engineering & Computing, School of Architecture, Computing and Engineering, University of East London, London, UK; mahad@uel.ac.uk, atiqahad@gmail.com
* Correspondence: u2572490@uel.ac.uk

Abstract: The integration of Information Security (InfoSec) in Responsible AI (RAI) implementations has emerged as a critical focal point, particularly in addressing the unique challenges faced by Digital SMEs (*Digital Small and Medium-sized Enterprises are SMEs whose core operations rely heavily on digital technologies. They are further explained in chapter 2.1, "SMEs and Digital SMEs". SMEs, used throughout this paper, specifically refers to Digital SMEs*). This review examines the evolving role of InfoSec in shaping RAI implementations, emphasizing the importance of integrated frameworks to maximize resource efficiency and cohesively address both domains. While existing studies focus mainly on technical and policy-driven solutions, there is an under-representation of non-technical barriers, particularly the human factor, despite its critical role in InfoSec. Organizational culture, employee awareness, and stakeholder engagement are critical yet often overlooked components of InfoSec, despite their pivotal role in achieving a balance across the three core pillars of InfoSec, that is: people, processes, and technologies. With insights from significant studies and internationally recognized frameworks for AI governance and InfoSec, this analysis highlights the advantages of adopting integrated approaches for simplified and holistic InfoSec and RAI implementations. Emphasis shall also be placed on understanding the role of the Human Factor in these frameworks and identifying its significance in building sustainable and ethical AI practices. By synthesizing existing data, this study provides actionable insights to support SMEs in building resilient, secure, and ethical digital practices tailored to their unique needs.

Keywords: Responsible AI, Security Best Practices, Digital SMEs, AI Governance, AI Ethics, Information Security Governance

Citation: Quainoo, Charles and Md Atiqur Rahman Ahad. 2026. The Role of Information Security in Responsible AI for Digital SMEs: A Systematic Review of Frameworks, Challenges, and Best Practices. *Journal of Ethics and Emerging Technologies* 36: 1. https://doi.org/10.55613/jeet.v36i1.193

Received: 29/09/2025
Accepted: 19/01/2026
Published: 20/01/2026

1. Introduction

Throughout this paper, the term Digital SMEs refers to small and medium-sized enterprises whose core operations rely heavily on digital technologies such as cloud platforms/workloads and services, IoT technologies and devices, big-data analytics and pipelines, AI tools and agents, and digitally integrated business processes. This distinction matters because Digital SMEs typically operate with higher levels of technology and data dependency, broader digital footprints, and hence increased exposure to cyber and AI-related vulnerabilities compared to traditional SMEs. Their reliance on digital technologies and workflows magnifies the importance of adopting sound InfoSec practices and RAI

principles. Thus, the applicability and urgency of InfoSec–RAI risks are more prominent in Digital SMEs, making them a distinct focal group within this study.

1.1 Background of Study

The background section highlights the core aspects of InfoSec and RAI for SMEs and sets the tone for understanding the distinct perspectives and arguments of the reviewed papers, while identifying potential synergies, strength and gaps. The core aspects were analyzed and introduced at a high level in the upcoming subsections and further supported with deductions drawn from the selected frameworks and research materials from reputable sources such as the Information Systems Audit and Control Association (ISACA) (ISACA, 2024) and the International Information System Security Certification Consortium (ISC²) ((ISC)2, 2024).

During the systematic review, a comprehensive search of literature and resources from reputable sources revealed that the literature lacked studies that specifically addressed the role of InfoSec in RAI implementations within the SME context.

1.2 The Importance of Responsible AI in SMEs

Digitization, InfoSec and AI adoption is essential for the competitive advantage, resilience, and sustainability of SMEs today (Muhammad et al., 2024). For SMEs to thrive, they must adopt AI responsibly by ensuring ethical, transparent, secure, and fair use (Marwa et al., 2024). This nurtures trust, accountability, and compliance while addressing challenges like resource constraints, regulatory requirements, etc. within a competitive business landscape (Julia et al., 2024). This section highlights the critical role of InfoSec in supporting RAI for SME growth and resilience.

The reviewed papers agree on RAI's importance for SMEs but differ on key aspects. For instance, one of the studies advocates comprehensive AI adoption to drive innovation (Elias, 1475), while another warns against overreliance on AI systems and stresses for human oversight for transparency and accountability (Abdulmajeed et al., 2024). Resource constraints also elicit varied views, with some highlighting high financial investments for AI systems (Ben, 2024), while others see AI as a scalable and cost-effective long-term solution through, for example, automation (Elias, 1475). Ethical approaches differ as well, from ISO 42001's flexible, context-based but fair usage framework (Information et al., 4200) to strict universal standards advocated by AI in cybersecurity studies (Abdulmajeed et al., 2024). Finally, another differing view was on AI's role in SMEs, which ranges from operational resilience (Ben, 2024) to redefining SME competitiveness (Elias, 1475), reflecting diverse SME contexts.

1.3 The Role of Information Security in Responsible AI

InfoSec serves as a foundational pillar for RAI, particularly in the SME context where vulnerabilities like data breaches and algorithmic bias pose significant risks (Ehtehsam et al., 2024). InfoSec enhances the secure and ethical deployment of AI, by safeguarding data privacy, confidentiality, integrity, and availability (CIA). It further creates a foundation for aligning technical operations with governance principles essential for SMEs navigating complex business and regulatory landscapes (Center et al., 2024; Ernst, 2024). Though all the papers agree that the role of InfoSec in RAI is vital, there are a few opposing views on certain aspects. The studies present differing views on the necessity of formalized frameworks such as ISO 27001 (Information et al., 2700) and ISO 42001 (In-formation et al., 4200) versus more flexible, context-specific approaches (Ben, 2024).

Perspectives also differ on AI-specific risks. Some of the papers that extensively covered Large Language Models (LLMs) (IBM, 2025) and Generative AI (Gen AI) (IBM, 2025) debated whether traditional InfoSec protocols are sufficient to address AI-specific risks like adversarial attacks and algorithmic bias (Ben, 2024; Elias, 1475), while others argue that extending existing InfoSec protocols is sufficient to mitigate these risks (Ab-dulmajeed et al., 2024). Opinions diverge on whether high costs are a barrier to InfoSec investment for SMEs (Abdulmajeed et al., 2024) or if robust InfoSec investment is indispensable regardless of organizational size (Elias, 1475). These differences highlight the need for tailored strategies to integrate InfoSec into RAI effectively.

1.4 Objectives of the Systematic Review

The objective of this review is to systematically analyze the integration of InfoSec and RAI in SMEs as discussed and presented in the articles, focusing on evaluating challenges and gaps, identifying key guidance and practical frameworks, and synthesizing best practices. Specifically, the review aims to assess the selected articles to extract fundamental principles that can serve as guardrails for SMEs in navigating the complexities of InfoSec and RAI.

In addition to analyzing the articles, the review aligns its findings with reputable InfoSec and AI frameworks (that is; ISO/IEC 27001:2022 (Information et al., 2700) and ISO/IEC 42001:2023 (Information et al., 4200) respectively), to highlight practical guidance and actionable recommendations. The recommendations should bridge the gap be-tween theory and practical implementations and, hence, be more applicable and beneficial to SMEs.

Following the key research questions outlined below, the review paper will not only highlight existing gaps but also provide answers that contribute to advancing the narrative on InfoSec and RAI in SMEs.

1.5 Key Questions Guiding the Review

- What is the role of Information Security in Responsible AI implementations in SMEs?
- What are the challenges and gaps in existing Information Security and Responsible AI practices in the SMEs' context?
- Where does the Human Factor fit in?
- Which frameworks and best practices are best suited for SMEs?

The review starts with introducing the study's objectives and relevance, then follows with analyzing the theoretical foundations of RAI and InfoSec in SMEs. It then outlines the methodology used for the systematic review, presents findings on state-of-the-art practices, and identifies challenges and research gaps. The final sections synthesize best practices, examine synergies and opposing views, and conclude with recommendations for future research directions.

2. Theoretical Foundations

2.1 Defining Key Concepts

To establish a good foundation for the systematic review, this section explains key concepts vital to the discussions. This ensures that readers share a common understanding, regardless of background, to engage with the paper's insights.

Information Security (InfoSec)

InfoSec is the practice of protecting information and information systems from un-authorized access, disclosure, disruption, modification, or destruction to ensure confidentiality, integrity, and availability (CIA). It involves a holistic approach encompassing three critical components: People, Processes, and Technology (Information et al., 2700).

People: Users of information systems are often the first line of defense in maintaining its security. This includes employees, management, and third parties who interact with information systems and data (Information et al., 2700).

Processes: Effective processes ensure that security policies are implemented, monitored, and re-viewed. These include risk assessment processes, incident response processes, etc. (Information et al., 2700).

Technology: Technology is basically the tools, systems, and applications used by People to implement or operationalize the Processes for protecting information (Information et al., 2700). Technology is only effective when complemented by robust processes and informed people.

An imbalance among these pillars can create vulnerabilities or loopholes that adversaries may exploit, potentially compromising the CIA of information systems and data.

Responsible AI (RAI)

RAI refers to a framework of principles that ensures AI systems align with ethical standards, legal requirements, and societal values (IBM, 2024). Its goal is to foster trust by embedding ethics into AI workflows, maximizing benefits, and mitigating risks. As noted by IBM, there are about six (6) core principles of RAI (IBM, 2024), which address unique aspects of RAI implementation, as detailed in the explanations that follow.

Explainable AI (XAI) focuses on making AI systems transparent and their decisions understandable to humans (Stephanie et al., 2023). By enabling users to comprehend the reasoning behind AI outcomes, trust is fostered, which is critical for implementing other RAI principles like fairness and robustness. As discussed in "Explainable AI for Cybersecurity" by Pan and Mishra, XAI improves detection and mitigation of vulnerabilities (Zhixin et al., 2023). Similarly, Charmet et al. emphasize that XAI enhances AI's interpretability in cybersecurity, providing SMEs with a competitive edge through trustworthy AI solutions (Fabien et al., 2023).

Fair AI ensures equitable outcomes by avoiding discrimination against any group, particularly vulnerable ones (Brianna et al., 2112). Achieving fairness requires diverse da-ta collection, bias mitigation during training, and continuous monitoring to detect unintended consequences.

Robust AI is the ability of AI systems to maintain performance under new or adversarial conditions. This involves designing models resilient to data variability, environ-mental changes, and adversarial attacks. Hamon et al. highlights data sanitization as critical to ensuring robustness and preventing vulnerabilities like data poisoning (Ronan et al., 3004).

Transparent AI provides insights into how AI systems function and reach decisions. Transparency builds trust, facilitates informed decision-making, and ensures accountability by revealing potential biases and reliability (Joel, 2020).

Secure AI involves protecting AI systems against cyber threats and ensuring their integrity, availability, and safety. This includes measures to prevent unauthorized access and adversarial attacks (Microsoft, 2023).

Privacy in AI safeguards sensitive data by minimizing collection, ensuring transparency in data use, and adopting robust governance practices to address concerns about breaches and misuse (IBM, 2024).

SME and Digital SMEs

SMEs, defined by the European Commission as businesses with fewer than 250 employees and an annual turnover not exceeding €50 million (approximately $54 million) or a balance sheet total below €43 million (approximately $47 million), form over 99% of all businesses in the EU (sme-definition_en et al., 2024). SMEs are critical drivers of economic growth, innovation, and employment, making them pivotal to economic resilience and sustainability.

Digital SMEs, however, represent a subset of SMEs that rely extensively on digital technologies as part of their core operations to enhance efficiency, innovation, and competitiveness. By integrating tools such as cloud computing, artificial intelligence (AI), big data, Internet of Things (IoT), digital marketing, etc., they streamline processes and adapt to the fast-evolving digital economy (Harvard Business Review, 2023). Unlike traditional SMEs, digital SMEs adopt customer centric, innovative and data-driven strategies to scale operations and address resource limitations, ensuring competitiveness in a global digital market (Oxford Business Review, 2023). This high usage and reliance on technology increases operational efficiency and competitive advantage but also increases their exposure to cybersecurity risks, by broadening their attack surface and vulnerability exposures. The broadened attack surface is due to the inherent vulnerabilities in the digital tools and technologies used. As Digital SMEs are more exposed to these risks as compared to traditional SMEs, they face more complex InfoSec and RAI challenges. They therefore require robust frameworks to manage these complex challenges responsibly, particularly in the context of adopting RAI, which is vital for fostering both innovation and resilience (Harvard Business Review, 2023)

2.2 Interconnection Between Information Security and AI

This section highlights the connection between InfoSec and AI to emphasize the importance of InfoSec as a foundation for building robust and trustworthy AI systems.

Why Information Security is Foundational for Responsible AI

InfoSec integrates processes, people, and technology to establish a robust and secure foundation, enabling systems to operate securely. In the context of AI, InfoSec forms the backbone of safe, secure, and reliable AI operations by ensuring the CIA of AI systems and data. It is vital in protecting AI systems, models, and data from external interference, such as data poisoning, breaches, or adversarial attacks. It is, therefore, a critical pillar of robust AI systems. By harmonizing people, processes, and technology, InfoSec ensures the CIA of the information systems and data upon which AI fundamentally relies.

A key aspect of InfoSec in AI is protecting the CIA and privacy of data. AI systems rely heavily on large datasets for training and decision-making. Ensuring the integrity of this data is crucial, as compromised data can lead to inaccurate models and potentially harmful outcomes. Confidentiality is equally important to protect sensitive information from unauthorized access, while availability ensures that AI services remain accessible and functional when needed. Implementing robust InfoSec measures helps prevent issues such as data breaches, data poisoning, and adversarial attacks, which can undermine the reliability and trustworthiness of AI systems (Harvard Business Review, 2023).

Moreover, InfoSec plays a vital role in establishing governance frameworks for AI. According to ISACA (ISACA, 2024), developing an AI governance framework is essential for the responsible use of AI, as it addresses ethical implications, data quality, and risk management. Such frameworks integrate AI management with organizational processes, focusing on risk management and offering detailed implementation controls (ISACA, 2022).

Additionally, InfoSec professionals are crucial in ensuring that AI is developed and deployed in a manner that upholds safety, security, and responsible practices. Collaborating with compliance and legal teams, they help organizations meet relevant industry standards and regulations, such as the General Data Protection Regulation (GDPR) (ISACA, 2024) for data privacy. By following InfoSec best practices and learning from the experiences of others, organizations can unlock the full potential of AI while minimizing risk (ISACA, 2022).

Ethical, Operational, and Legal Implications

The integration of InfoSec with AI governance has critical ethical, operational, and legal implications.

Ethical Implications: Integrating InfoSec into AI governance prevents harm from biased or insecure systems. Ethical AI governance fosters trust and transparency, promoting responsible development and deployment. It also enhances brand trust, drives consumer loyalty, and reduces risks of negative AI experiences (European, 2025).

Operational Implications: Converging InfoSec with AI governance improves system reliability and resilience. Robust governance strategies enable responsible, transparent, and explainable AI workflows, minimizing risks and ensuring compliance with ethical and regulatory standards (ISACA, 2022).

Legal Implications: Integrating InfoSec with AI governance helps organizations comply with global regulations. Strong governance frameworks ensure adherence to data privacy laws and mitigate potential ethical and legal issues (ISACA, 2024).

For SMEs, these implications are vital. Ethical AI fosters trust, operational integration enhances resilience, and legal compliance prevents penalties. By integrating InfoSec into AI governance, SMEs can address these challenges and ensure sustainable growth in a complex technological environment.

3. Methodology

3.1 Approach and Rationale for Conducting a Systematic Review

According to IEEE, a systematic review is a literature review that uses rigorous, transparent methods to collect, appraise, and synthesize evidence on a specific research

question. Its objective is to minimize bias with reproducible procedures, ensuring reliable findings for decision-making (ISACA, 2024).

This study employed a systematic review to explore InfoSec and RAI integration in SMEs, ensuring a structured, transparent, and replicable process. It identifies current practices, research gaps, and minimizes biases, providing factual insights into the field.

3.2 Use of PRISMA:

The Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework was utilized to guide the review process, particularly the structured approach for non-bias selection of relevant research papers, articles, etc. This enabled clear documentation of study and paper selection, inclusion, and analysis, ensuring that the findings are well-founded and methodologically rigorous (IEEE, 2022). The PRISMA diagram below illustrates the systematic review process, detailing the identification, screening, eligibility, and inclusion of articles and studies.

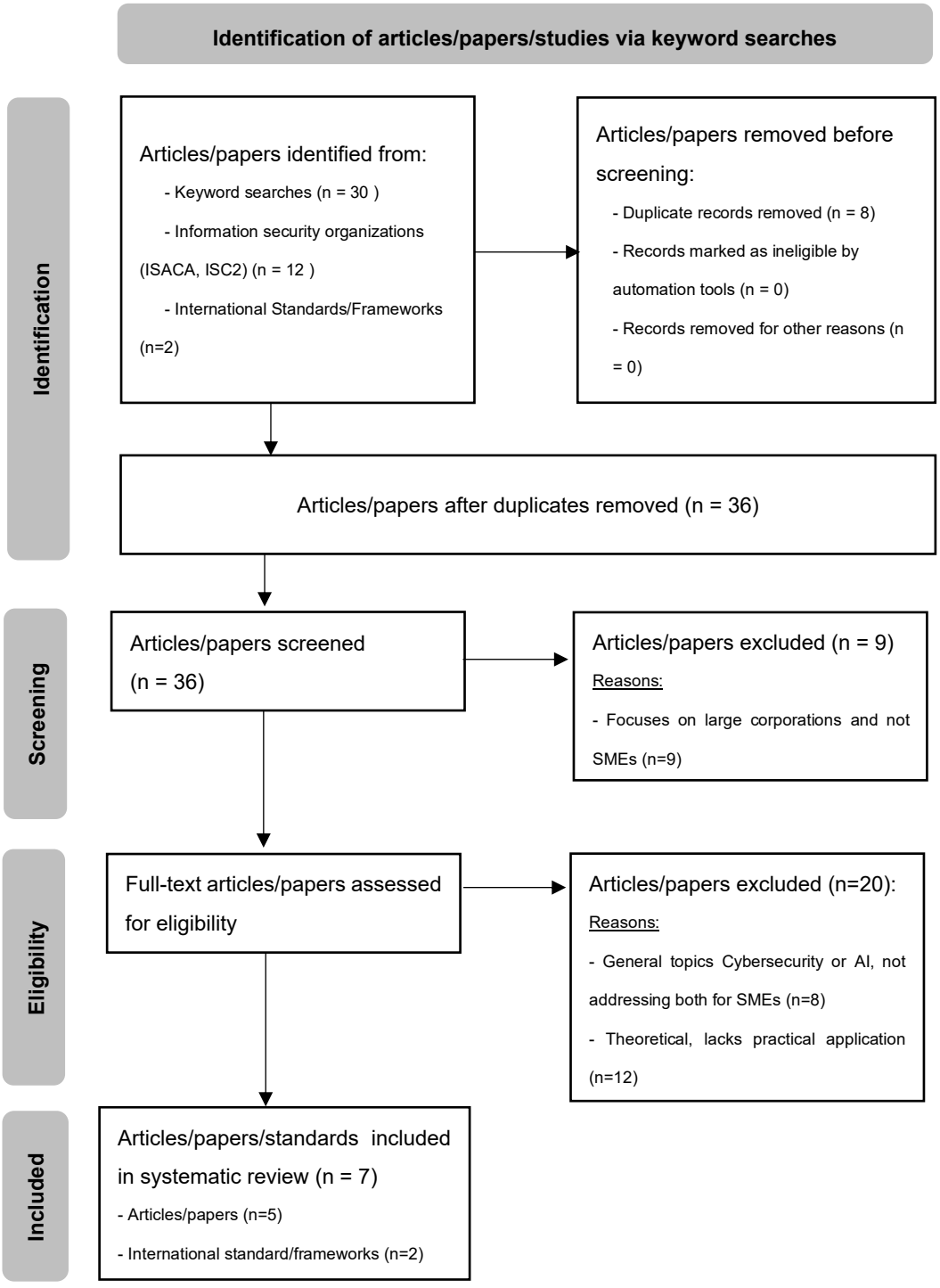

Figure 1: PRISMA Diagram: Identification and selection of studies via keyword searches.

PRISMA's Inclusion and Exclusion Criteria:

The PRISMA approach encompasses four (4) phases, beginning with the identification of potential papers, articles, or studies, followed by screening, determining eligibility, and ending in the inclusion of the final set of papers, articles, or studies (IEEE, 2022).

In the identification phase, multiple sources and methods were utilized to locate studies aligning with the objectives of this systematic review. The process included:

Keyword Searches in Scientific Databases: Predefined keywords such as Responsible AI, Security Best Practices, Digital SMEs, AI Governance, AI Ethics, and Information Security Governance, were employed to search for relevant studies in highly reputable academic databases including IEEE Xplore (Alessandro et al., 2009), ACM Digital Library (Institute et al., 2025), Scopus (Association, 2025), and ScienceDirect (Elsevier, 2025). These academic databases were selected for their extensive collections of high-quality, peer-reviewed research in technology and InfoSec. Boolean operators (e.g., AND, OR) were applied to refine the searches, yielding 30 records.

Journals and reports from InfoSec Organizations: To complement these database searches, 12 InfoSec industry-specific journals and reports affiliated with reputable organizations like ISACA (Information Systems Audit and Control Association) (ISACA, 2024) and ISC2 (International Information System Security Certification Consortium) ((ISC)2, 2024) were reviewed. These journals were prioritized because they are highly regarded for their contributions to the field of InfoSec and provide insights that bridge academic research and practical applications.

International Standards and Frameworks: Documents related to widely recognized standards and frameworks from ISO (International Organization for Standardization) (Elsevier, 2025) provided 2 more records. The total number of articles/papers identified at this stage was forty-four (44).

In the screening phase, eight (8) duplicates were removed, and the remaining thirty-six (36) unique articles/papers were subjected to further evaluation based on titles and abstracts. This step ensured that only studies addressing the intersection of RAI and InfoSec in SMEs were retained for further evaluation. A total of nine (9) articles/papers were further excluded due to the focus on large corporations instead of SMEs. The remaining twenty-seven (27) articles/papers proceeded to the eligibility phase.

During the eligibility phase, full texts of the 27 screened articles/papers were reviewed in detail against the inclusion and exclusion criteria. During this phase, a total of twenty (20) articles and papers were excluded. eight (8) of these were removed because they contained general discussions on cybersecurity or AI without specifically addressing both topics and their intersection in the context of SMEs. Additionally, twelve (12) papers were excluded due to their overly theoretical content, which lacked practical applications or implications for SMEs. The inclusion and exclusion criteria below guided the overall PRISMA selection process:

Inclusion Criteria:

The criteria for selecting papers for the systematic review focused on studies published between 2019 and 2024. This period reflected when major advancements in RAI, the revision of key InfoSec standards, and modern SME digital transformation practices emerged. Earlier publications were excluded as they predate contemporary AI governance models, large language models, and updated InfoSec frameworks, limiting their relevance to current SME contexts.

Only peer-reviewed articles, conference proceedings, internationally recognized standards (e.g., ISO/IEC 27001 and ISO/IEC 42001), governance frameworks (e.g., NIST CSF), and reputable industry reports from authoritative bodies such as ISACA and ISC² were considered. Including these non-academic sources was essential because high-quality, practice-oriented guidance in InfoSec and RAI is frequently produced by standards organizations and professional institutions rather than through traditional academic channels.

The research also had to explicitly address RAI, InfoSec, and their applications in SMEs, ensuring conceptual alignment with the review's core objectives. Additionally, studies were included if they provided frameworks, governance practices, or ethical and security considerations relevant to AI implementation in SME environments.

Finally, a criterion of practical SME relevance was applied to ensure that selected sources offered actionable insights suitable for SMEs' resource constraints, organizational structures, and operational realities. To maintain accessibility and consistency in interpretation, only publications in English were selected.

Exclusion Criteria:

Studies published before 2019 were excluded because of the high likelihood of not adequately covering and reflecting the rapid evolution of contemporary RAI practices, the revision of key InfoSec standards, or the emergence of modern AI governance frameworks critical to SME contexts. Earlier works predate major digital trends and technological shifts such as widespread cloud adoption, generative AI, and updated ISO standards, reducing their applicability to current SME challenges.

Non-peer-reviewed or low-rigor literature lacking methodological transparency was excluded unless it originated from authoritative bodies (e.g., ISACA, ISC², NIST, ISO). This ensured the review maintained high evidentiary quality and avoided speculative or commercially biased materials.

Literatures that did not relate to RAI, InfoSec and their impacts on or relations with SME themes were excluded to retain a focused evidence base aligned with the core objectives of this review. This included studies on AI unrelated to governance or security, cybersecurity research without an AI dimension, and work targeting large enterprises where assumptions, resources, and governance environments differ fundamentally from SME realities.

Papers that were overly theoretical with no practical implications, operational guidance, or actionable relevance for SMEs, were also excluded. Given SMEs' resource constraints, the review prioritized literature that covered applied frameworks, governance models, or implementation considerations rather than purely conceptual discussions.

Sources with insufficient methodological detail, unclear research design, or inadequate documentation were removed during the eligibility stage, as their inclusion would compromise analytical robustness and synthesis reliability.

Adaptation of PRISMA for Heterogeneous InfoSec and RAI Literature

PRISMA is traditionally applied to empirical, standardized and structured studies, this review required some methodological adjustments to accommodate the heterogeneous nature of the evidence base in InfoSec, RAI, and SME research. The body of evidence included not only academic publications but also internationally recognized standards (e.g., ISO/IEC 27001, ISO/IEC 42001), governance frameworks (e.g., NIST CSF), and practitioner-oriented industry reports from bodies such as ISACA and ISC². These materials do not follow uniform reporting structures and often lack methodological detail typically required in conventional PRISMA applications. To manage this diversity, PRISMA was adapted in three ways:

First, the definition of "eligible sources" was broadened to include authoritative non-academic documents where they fulfilled the review's objectives and provided domain-specific guidance relevant to SMEs.

Second, the screening stages were modified so that non-empirical sources such as standards, frameworks, and technical guidelines were assessed using relevance and credibility criteria rather than methodological rigor alone.

Third, the extraction process was adjusted to capture conceptual contributions and framework components, as these were essential for synthesizing best practices across InfoSec and RAI domains.

These adaptations ensured that the PRISMA process remained transparent and systematic while remaining flexible enough to incorporate diverse but authoritative sources central to understanding how InfoSec supports RAI implementations in SMEs. The modifications also allowed the selection process to reflect the realities of InfoSec and RAI literature, where high-quality evidence often emerges from standards bodies and industry organizations rather than traditional academic channels.

Quality Appraisal and Bias Mitigation

A structured quality appraisal procedure was integrated into both the screening and eligibility stages of the PRISMA process. This was to ensure that both the inclusion and exclusion criteria described, as well as the adaptations to the PRISMA process outlined above, were applied consistently and without bias. In the quality appraisal procedure, empirical studies were assessed for methodological transparency, clarity of research design, relevance to SME contexts, and alignment with the review's core objectives. Whiles, conceptual papers, standards, and industry frameworks, given their non-empirical nature, were appraised based on the authority of the issuing body, the applicability of their recommendations, and the practicality of their provided guidance for SMEs. This quality appraisal process ensured that decisions were grounded in a consistent rationale, reducing the likelihood of selection bias when dealing with heterogeneous materials covering academic, technical, and practitioner domains.

The final inclusion phase involved consolidating the eligible studies for systematic synthesis. Studies that met all inclusion criteria were included, ensuring the relevance, quality, and applicability of the selected literature to the research objectives. Seven articles/papers/standards were included in the review, consisting of five peer-reviewed articles that directly address Responsible AI (RAI) and Information Security (InfoSec) in the context of SMEs, along with two international standards or frameworks relevant to the research focus.

4. Categorization of Existing Work: InfoSec in RAI

4.1 Frameworks and Standards

As highlighted in most of the reviewed papers, AI is not an optional asset but a critical driver of digital transformation, competitive advantage, and business viability for SMEs (Noah et al., 2024; Nahid et al., 2024; Marwa et al., 2024; Ben, 2024; Leon et al., 2024). The integration of RAI and InfoSec is foundational for building trust and resilience, particularly for SMEs.

One main categorization of the existing work focused on: the urgency of practical frameworks and standards to guide SMEs in navigating uncertain environments. These frameworks are crucial for fostering resilience and securing their viability and competitive edge. SMEs constitute approximately 99% of all EU businesses (European Commission, 2024), making their success vital for the EU's economic growth. Supporting SMEs with robust RAI and InfoSec frameworks is not only commendable but essential for economic sustainability. *Chapter 6: Best practices and lessons learned* outline practical frameworks and standards that effectively address SMEs' unique challenges in securely adopting RAI.

4.2 Trends and Innovations

InfoSec and RAI are evolving rapidly through digital innovations, transforming the security landscape and enabling ethical AI adoption. These advancements were addressed as another categorization of existing works. Three (3) key advancements shaping these domains are highlighted below.

AI is empowering SMEs with tools to improve efficiency, customer engagement, and decision-making. The democratization of AI, driven by user-friendly platforms like low-code and no-code solutions, allows even nontechnical SMEs to leverage AI capabilities and compete with larger organizations (International, 2025).

AI is also driving hyper-personalization in customer engagement, enabling SMEs to deliver tailored experiences such as personalized marketing, dynamic product recommendations, and targeted advertising. This nurtures customer loyalty and enhances competitiveness in crowded markets (CXO, 2025).

In cybersecurity, AI-powered systems are essential as cyber threats become complex. Advanced machine learning technologies help SMEs detect vulnerabilities, respond swiftly to incidents, and safeguard sensitive data (Katherine, 2025).

These advancements underscore AI's pivotal role in enhancing productivity, optimizing customer experiences, and securing operations for Digital SMEs.

5. Challenges in Implementation

5.1 Security Challenges in RAI

All the reviewed articles examined security challenges in RAI adoption by SMEs, highlighting attack vectors, vulnerabilities, and the broader threat landscape. Below is a summary of the key challenges discussed, concluding with a core challenge inadequately addressed in the reviewed literature.

SMEs face significant security issues with RAI, particularly regarding data privacy and protection. AI's extensive data requirements elevate the risk of breaches and misuse, exacerbated by SMEs' limited resources to meet regulatory demands (Noah et al., 2024).

Algorithmic bias is another major concern, leading to unfair outcomes and reputational damage. SMEs often lack the expertise or tools to ensure security, fairness, and transparency in AI systems, exposing them to ethical, operational, and security risks (Leon et al., 2024).

AI system robustness presents further challenges, with adversarial attacks like data poisoning threatening reliability. SMEs frequently struggle to implement adequate safeguards against such vulnerabilities (Abdulmajeed et al., 2024).

A persistent imbalance exists across the three pillars of InfoSec, People, Processes and Technologies. SMEs often emphasize processes and technologies but neglect the critical role of people in maintaining security; this remains a challenge for SMEs and is discussed in *Chapter 7, "The Human Factor - Under-representation of Non-Technical Barriers"*.

5.2 SME-Specific Challenges

SMEs face specific barriers that hinder the adoption of comprehensive security and RAI frameworks. One of the primary issues is access to finance, as many SMEs struggle to secure adequate funding to sustain or expand their operations. According to the International Finance Corporation (IFC), approximately 40% of formal SMEs in developing economies face unmet financing needs, totaling around $5.2 trillion annually (Tom, 2025). There is insufficient access to reliable credit information, which further complicate SMEs' ability to grow and compete (International, 2021). Additionally, digitization gaps further hinder SMEs' competitiveness. While many SMEs are connected to the internet, their adoption of advanced technologies, such as AI, cloud computing and data analytics, remains limited (World, 2021).

Another challenge is their limited integration into Global Value Chains (GVCs). SMEs often face barriers like high costs and supply chain disruptions, such as delays in receiving inputs and increased shipping expenses, which were exacerbated during the COVID-19 pandemic (OECD, 2021). Lastly, SMEs are disproportionately affected by external shocks like economic downturns and global crises, with data showing higher closure rates and revenue losses among SMEs compared to larger firms (OECD, 2023)

5.3 Ethical, Legal and Regulatory Challenges

Efforts to integrate InfoSec and RAI into SMEs raise significant ethical, legal, and regulatory challenges, critical for fostering trust and ensuring compliance. The GDPR (ISACA, 2024) and the forthcoming EU AI Act (World, 2020) mandate strict requirements such as algorithmic accountability, data privacy, etc. to prevent undesirable outcomes.

Ethically, RAI adoption in SMEs faces hurdles such as algorithmic bias, which undermines trust and credibility. Transparency and accountability are challenging due to limited documentation and explainability in AI systems. Data privacy and consent management remain pressing issues, with SMEs often struggling to safeguard sensitive data while meeting ethical and business obligations.

Compliance with evolving regulations like the EU AI Act (World, 2020) poses a major legal and regulatory hurdle, as SMEs lack the resources to meet these requirements. Accountability is further complicated for SMEs, raising concerns about liability for AI-

driven decisions (Marwa et al., 2024). Data protection and privacy rights of EU citizens such as the EU General Data Protection Regulation (GDPR) (ISACA, 2024) adds to the burden, with SMEs facing difficulties in adequately securing sensitive information (Noah et al., 2024) due to limited resources and expertise. The absence of harmonized standards exacerbates these challenges for SMEs operating internationally (Leon et al., 2024).

6. Best Practices and Lessons Learned

6.1 Adoption of Effective and Well-Suited Frameworks and Standards

This section covers frameworks and standards that demonstrate effective integration of InfoSec into RAI implementations specifically within SMEs, to serve as a blueprint for SMEs. The key aspect is focusing on frameworks which are well suited for SMEs context and constraints.

Information Security Frameworks and Standards

According to the Verizon Data Breach Investigations Report (DBIR) (European, 2025), cybersecurity is now a critical topic across all business sectors, reaching board-level attention. The growing interest in cyber insurance (Verizon, 2023) further highlights an increasing organizational focus on InfoSec. This awareness has driven the development of numerous cybersecurity frameworks, standards, and best practices.

Key frameworks include the NIST (National Institute of Standards and Technology) Cybersecurity Framework (CSF) (Munich, 2024) and the ISO 27001 standard (National et al., 2024). The NIST CSF provides a versatile guide for organizations across industries, while ISO 27001 offers a structured approach to managing InfoSec, with the option for certification through independent audits. Both frameworks are practical, adaptable, and applicable to diverse organizational contexts.

Responsible AI (RAI) Frameworks and Standards

As Bill Gates once said, "AI can be our friend" (Gates, 2018), emphasizing two opposing notions. The first aspect highlights the enormous power AI wields, while the contradicting notion is expressed with the use of "can", implying the likelihood of unexpected outcomes. Several thought leaders and "godfathers" of AI such as *Geoffrey E. Hinton* (Geoffrey, 2023) have emphasized similar concerns, underscoring the need for frameworks and standards to govern the responsible use of AI within organizations to ensure it becomes a friend and not a foe.

Two of the most popular RAI frameworks and standards are the EU Ethics Framework for Trustworthy AI (High-Level Expert Group on Artificial Intelligence, 2019) and the ISO 42001 standard for AI Management Systems (ISO/IEC, 2023). These frameworks are practical, designed to suit organizations across all industry verticals and contexts, and have undergone strict peer review by experts from various sectors.

6.2 Adoption of Integrated Information Security and Responsible AI Frameworks for SMEs

Adopting an integrated InfoSec–RAI framework, that is; *aligning InfoSec processes (e.g., ISO 27001) with RAI obligations (e.g., ISO 42001, EU AI Act requirements),* represents a practical and highly efficient best practice for Digital SMEs. Even though the literatures reviewed did not explicitly promote integrated frameworks, they consistently highlighted fragmented security, governance, and AI practices across SMEs. These fragmented

approaches create duplicated effort, inconsistent controls, and gaps between technical safeguards and ethical or governance obligations. In response to these observed gaps, this review synthesizes an integrated approach as a best-practice recommendation for SMEs. Contrary to managing InfoSec and RAI as separate initiatives, an integrated framework enables SMEs to address InfoSec, AI governance, regulatory requirements, and operational needs through a unified management system. This is particularly relevant for Digital SMEs, whose high reliance on technological tools and services such as cloud platforms and services, IoT devices, AI-based tools, and data-intensive workflows increases both the volume and complexity of risks they face. By combining governance, compliance, training, and risk management activities, SMEs can reduce unnecessary complexity, avoid duplicated controls, and strengthen overall resilience. SMEs often have limited financial, technical, and human resources, making efficiency critical. Adopting an integrated approach allows SMEs to use a single set of aligned controls, documentation pathways, and decision-making structures. This integrated approach offers several advantages as highlighted in the following:

Simplified Compliance: A unified compliance structure reduces the effort required to meet multiple frameworks independently. For example, ISO 27001's requirements for risk assessment, incident management, identity and access management, data security and access control measures can complement ISO 42001's requirements around organizational governance, organizational AI objectives, AI system impacts on individuals and society, and the overall AI lifecycle oversight. Using an integrated governance approach allows SMEs to meet overlapping requirements more efficiently.

Streamlined Training and Awareness: Integrated training programs that cover both InfoSec (e.g., data security and handling, authentication, phishing risks) and RAI (e.g., bias and hallucination awareness, AI output interpretation, model misuse) help employees understand how InfoSec and RAI practices intersect. This reduces training duplication and helps employees develop a holistic understanding of their responsibilities in a digitally intensive environment. Furthermore, adversaries are using AI to enhance their tactics, techniques and procedures. Combining InfoSec and RAI awareness and training campaigns make the concepts comprehensible and tangible. For example, an organization's combined InfoSec and RAI training may cover a single scenario involving an AI-based customer support system. The training shall simultaneously cover InfoSec topics such as data protection and access control, alongside RAI issues such as bias, transparency, and human oversight. By addressing both dimensions within the same practical use case, abstract RAI principles become more concrete and easier to apply.

Integrated InfoSec and RAI governance gives SMEs a practical pathway to operationalizing secure and ethical AI use while remaining mindful of SME resource constraints. It also provides a structured foundation for further development as SMEs mature. However, the feasibility of adopting integrated frameworks is influenced by the cost, expertise, and time limitations that characterize most SMEs. Financial constraints often prevent SMEs from investing in parallel governance streams, specialized tooling, or external consultancy support. Expertise shortages further restrict their capacity to interpret and operationalize complex frameworks such as ISO/IEC 27001 or ISO/IEC 42001, as many SMEs rely on generalist IT personnel rather than security or AI specialists. Time constraints also pose significant barriers, as SMEs lack the capacity to maintain lengthy implementation cycles, extensive documentation requirements, or continuous audit activities while managing day-to-day operations. While these constraints raise legitimate concerns regarding feasibility and short-term return on investment, integrated governance approaches may offer longer-term value by streamlining oversight processes and establishing a scalable foundation for RAI adoption.

6.3 Recommendations for Policy and Governance Best Practices

This section addresses two key audiences: SMEs and Governance bodies such as policymakers, standard bodies, regulatory bodies, etc. For SMEs, it highlights strategic governance practices that align their operational realities with robust security frameworks. For Governance bodies such as policymakers, standard bodies, regulatory bodies, etc., it emphasizes the need to move away from rigid, one-size-fits-all approaches, advocating for adaptable frameworks that support SMEs' diverse contexts. These recommendations must also be understood within the context of the cost, expertise, and time limitations faced by SMEs. Many SMEs operate with constrained budgets that limit their ability to adopt comprehensive frameworks or procure dedicated InfoSec or AI governance expertise. Similarly, staff capacity is frequently overstretched, making it difficult to sustain governance activities that require ongoing documentation, monitoring, and internal audits as required by the frameworks. Time pressures further restrict the ability of SMEs to introduce new controls or processes without disrupting critical business operations. These combined constraints shape how far and how quickly SMEs can adopt the recommended governance practices, highlighting the need for scalable, lightweight, and phased approaches that reflect SME realities.

Strategic Governance Practices for SMEs

SMEs can adopt strategic governance practices to ensure effective RAI integration. A key step is to source AI-driven security solutions using RAI principles such as ethics, transparency, accountability, etc., as baseline inclusion criteria within a broader governance framework. This approach ensures alignment with organizational InfoSec, RAI, and regulatory requirements while fostering scalable, cost-effective security and procurement measures tailored to SME resources (Nahid et al., 2024).

Integrating data and AI-driven tools into security practices enhances efficiency in resource-limited environments and supports strategic decision-making. These tools help SMEs align security practices with organizational objectives to enable robust and adaptable governance frameworks (Ben, 2024). Furthermore, ethical and compliant governance models are vital for integrating transparency and accountability into security frameworks to build trust and support long-term sustainability (Noah et al., 2024).

Finally, cultivating a security-aware culture through targeted training and awareness programs is critical for effective governance and proactive responses to cybersecurity challenges (Abdulmajeed et al., 2024).

Flexible and Inclusive Frameworks and Standards

Organizations vary widely, with SMEs facing unique constraints in diverse environments. However, governance bodies such as policymakers, standards bodies, and regulators often create rigid frameworks that fail to align with SME contexts. These standards are frequently shaped by research and development initiatives led by larger enterprises, prioritizing their use cases at the expense of smaller entities. The study *Economic Power and Political Influence: The Impact of Industry Structure on Public Policy* highlights the correlation between organization size and influence over public policy, showing that larger firms shape policies to their advantage, further marginalizing SMEs (High-Level, 2019).

Policymakers and standards bodies must shift from one-size-fits-all approaches to adaptable frameworks that address the diverse needs of SMEs. Flexibility and scalability

in policy design can empower SMEs to thrive while maintaining essential security and compliance objectives.

6.4 Strengthening the Human Factor to uplift Information Security in Responsible AI for SMEs

SMEs must shift towards improving on the "People" aspect of the three (3) core pillars of InfoSec, people, processes and technologies, to achieve optimal balance and alignment with the SME's unique organizational context. As noted by renowned InfoSec practitioner Kevin Mitnick, "humans are the weakest link in the security chain" (Lester, 2020). This acknowledgment is not a vague criticism but a courtesy call to SMEs to strategically strengthen this critical link. To illustrate why this prioritization is essential, it is important to recognize how people-related vulnerabilities manifest in real SME environments. For example, human error may arise when an employee unknowingly uploads sensitive customer data into an AI tool for assistance, creating an unintentional data exposure risk. Culture gaps can emerge when frontline staff distrust a newly deployed AI-based scheduling or prediction system and therefore bypass or override system recommendations, undermining accuracy and governance. Similarly, AI misuse can occur when teams adopt freely available AI tools without understanding their data-logging behavior or security settings, inadvertently exposing proprietary information. These scenarios highlight the practical, everyday ways human factors materially influence secure and responsible AI adoption within SMEs. SMEs can address these risks and strengthen this critical link by:

Strengthen Human-Centric Strategies

SMEs should allocate resources to train employees in InfoSec best practices and trends. Training programs must be tailored to the organization's context, addressing employee motivation, openness to change, and cultural challenges. These efforts ensure that employees are equipped to play their role in implementing and following effective security measures and practices respectively for successful RAI initiatives (Information et al., 4200). To make such training practical and actionable for SMEs, programs should include concise, role-relevant modules that directly reflect everyday tasks and risk areas employees encounter. Examples of SME-appropriate training modules include:

Recognizing AI-Enabled Social Engineering: Awareness trainings are key for detecting social engineering attacks. The trainings must cover real-world and relevant scenarios and use cases to make them tangible for the employees. For example, awareness videos can be an Ai generated video of leadership team making requests to employees. Such trainings Help staff identify AI-assisted phishing attempts, voice-cloning scams, or AI-generated impersonation attacks that increasingly target SMEs.

AI Output Interpretation Basics: Teaching staff how to critically assess AI-generated results, identify anomalies, and escalate suspicious or inconsistent outputs instead of relying blindly on automated decisions.

Data-Handling and Privacy Routines: Covering essential practices such as secure data entry, anonymization techniques, appropriate use of customer information, and safe handling of sensitive datasets when interacting with AI tools.

Secure Use of Generative and Predictive AI Tools: Providing clear guidance on what types of information employees may or may not input into external AI systems, including examples of unsafe prompts and proper use of enterprise-secured AI platforms.

These short, scenario-oriented modules can typically be delivered in under 30 minutes, making them feasible for SMEs with limited time, resources, and staffing capacity while still significantly strengthening the human element of InfoSec and RAI adoption.

Build a Security-Aware Culture

SMEs can build a security-aware culture by engaging employees in regular awareness campaigns and workshops to emphasize their role and clarify their responsibilities in preventing and reporting breaches. Open communication should be encouraged to ensure employees feel empowered and free to report potential threats without fear of punishment. By empowering and fostering shared responsibility, organizations can develop security-aware cultures (Information et al., 2700) and hence create a solid foundation for effective RAI. To operationalize this security aware culture, SME leaders must demonstrate visible engagement and create lightweight participation mechanisms that fit the constraints of smaller organizations. Practical examples include scheduling monthly or quarterly AI/security check-ins where staff can raise concerns, discuss unusual AI outputs, or highlight emerging risks in a non-technical setting; establishing a simple, well-publicized internal reporting channel (such as a dedicated email address or form) to make it easy for employees to flag suspicious activity or AI misuse; and appointing "security and AI champions" within teams to serve as peer contacts for questions and early escalation. These initiatives embed infosec and RAI behaviors into everyday routines, strengthening participation and signaling that leadership prioritizes shared responsibility across the organization.

Balance People, Processes, and Technologies

SMEs must achieve a good balance among the three pillars of InfoSec. Though technologies and processes are essential, they require well-trained and motivated employees for effective implementation. Organizations should regularly assess and realign these elements with their unique context and incorporate proactive strategies such as role-based training, simulations, and safeguards like multi-factor authentication (MFA) to reduce human errors and improve overall security (ISACA, 2024). A practical way SMEs can operationalize this balance is by simplifying workflows to reduce friction points that lead to security lapses. For example, many SMEs implement MFA but find that employees frequently bypass or avoid it due to time pressure or overly complex login procedures. To resolve this, a single sign-on (SSO) solution that integrates MFA seamlessly can be introduced, reducing the number of logins staff must perform throughout the day. This technological upgrade is complemented by a one-page quick guide explaining how access controls work (process element) and reinforced through short, role-specific training that explains why MFA is critical and how to use it efficiently (people element). By aligning the three pillars through motivating people, clarifying processes, and streamlining technology, the SME strengthens security while making daily work easier rather than more burdensome.

6.5 Strategies for Ethical and Legal AI Adoption

SMEs should establish governance frameworks to align AI development with ethical principles and legal mandates such as GDPR (ISACA, 2024) and the forthcoming EU AI Act (World, 2020). These frameworks must prioritize algorithmic accountability, ensuring AI-driven decisions are explainable, traceable, and free from bias, fostering trust and compliance.

Furthermore, SMEs should appoint dedicated AI governance or compliance roles within the company to oversee adherence to evolving legal requirements and ethical AI practices. Legal or compliance experts already within the organization can assume such roles as a cost-saving measure.
Finally, SMEs should engage with relevant industry associations, communities, and opensource projects to advocate for harmonized global AI and InfoSec standards, reducing cross-jurisdictional uncertainties and creating a supportive environment for RAI adoption.

7. Discussion

This section shall connect theoretical insights with practical implications, raising a deeper understanding of how SMEs can effectively align InfoSec with RAI principles.

7.1 Findings and Critical Discussion

For a clear and structured evaluation, this subsection systematically compares insights from the reviewed studies. Elements such as the scope and focus of the paper/article, frameworks and standards used, identified challenges, methodological consistency, best practices, proposed best practices, and research gaps were contrasted to highlight converging themes and points of divergence across the literature.

A closer look at the reviewed standards reveals important contrasts in governance approaches and implementation logic, particularly between ISO-based standards and the NIST Cybersecurity Framework, while also highlighting areas of overlap. ISO/IEC 27001 and ISO/IEC 42001 are structured around mandatory management system clauses (Clauses 4 - 10) that are process-oriented rather than control-prescriptive, requiring organizations to define context, scope, leadership responsibilities, risk assessment practices, and continual improvement mechanisms. The selection and implementation of specific controls or measures are largely context-dependent and justified through a Statement of Applicability (SoA), allowing organizations, including SMEs, to exclude controls that are not relevant to their operational environment, provided that those exclusions are clearly reasoned and documented.

In contrast, the NIST Cybersecurity Framework adopts a non-certifiable, maturity and risk-based model that emphasizes iterative improvement, self-assessment, and incremental control adoption through its Core cybersecurity outcomes and activities, Implementation tiers, and Organizational profiles. While both ISO standards and NIST are fundamentally risk-driven and adaptable in principle, they differ in how flexibility is operationalized. ISO embeds flexibility within a formalized governance structure that prioritizes auditability, traceability, and management accountability, whereas NIST enables flexibility through informal prioritization and contextual tailoring without certification requirements. For SMEs, these differences translate into distinct governance burdens: ISO's flexibility is mediated through structured justification and documentation, while NIST's flexibility relies more heavily on internal judgement and organizational discipline.
Taken together, this comparison suggests that the primary challenge for SMEs is not a lack of flexible standards, nor a direct incompatibility between ISO and NIST, but a misalignment in governance execution models. Existing literature often treats ISO–NIST alignment as a technical or control-mapping problem, whereas the underlying difficulty lies in reconciling ISO's structured, audit-oriented flexibility with NIST's adaptive, maturity-driven approach. The absence of clear guidance on how SMEs can integrate

these differing governance logics represents a key gap in current understanding and helps explain the fragmented adoption patterns observed across the reviewed studies. To further clarify these differences and their implications for SME adoption, the following table contrasts ISObased standards and the NIST Cybersecurity Framework across key dimensions related to governance structure, flexibility, and practical scalability, considering ISO standards primarily from an implementation and best-practice compliance perspective rather than as certification objectives for resource-constrained SMEs.

Dimension	ISO/IEC 27001 (ISMS)	ISO/IEC 42001 (AIMS)	NIST Cybersecurity Framework (CSF)	NIST AI Risk Management Framework (AI RMF)
Primary focus	Information security management	AI system governance and lifecycle management	Cybersecurity risk management	AI-specific risk management
Governance logic	Process- and risk-oriented governance	Process-, risk-, and ethics-oriented governance	Adaptive and maturity-based	Risk- and lifecycle-based
Flexibility mechanism	Risk assessment and Statement of Applicability	Risk assessment and Statement of Applicability	Tiered maturity and prioritization	Contextual AI risk mapping
Control selection	Context-driven; exclusions justified and documented	Context-driven; AI-specific controls justified	Context-driven; informal selection	Context-driven; AI risk categories
Documentation effort	Moderate to high (governance traceability)	Moderate to high (AI governance evidence)	Low to moderate	Low to moderate
AI specificity	Indirect (supports AI via InfoSec controls)	Direct (AI governance focus)	Indirect (security baseline)	Direct (AI risk focus)
Alignment with RAI objectives	Supporting role	Core objective	Supporting role	Core objective
Risk assessment role	Mandatory and central	Mandatory and central	Central but flexible	Central and AI-specific
Financial burden for SMEs	Moderate (governance effort, not certification)	Moderate (AI governance setup)	Low	Low to moderate
Required expertise	General InfoSec governance knowledge	AI governance and lifecycle knowledge	Broad cybersecurity awareness	AI risk and impact analysis skills
Time and operational overhead	Moderate (process setup and review cycles)	Moderate to high (AI oversight activities)	Low (incremental adoption)	Moderate (use-case analysis)
Scalability for SMEs	Scalable through scoped implementation	Scalable with limited AI scope	Highly scalable	Scalable with focused AI use
Suitability for low-maturity SMEs	Feasible with narrow scope	Feasible if AI use is limited	Highly suitable	Suitable with guidance
Typical SME challenge	Sustaining documentation and reviews	Managing AI governance complexity	Maintaining consistency	Translating AI risks into controls

Table 1: Comparison of ISO and NIST Standards Relevant to InfoSec and RAI Adoption in SMEs

While the preceding comparison highlights differences in governance logic and implementation models across ISO and NIST standards, it does not fully capture how these differences manifest across the broader body of SME-focused literature. The reviewed studies vary not only in their choice of frameworks, but also in how they interpret feasibility, resource constraints, and the balance between technical, organizational, and human-centric controls. As a result, SMEs are presented with fragmented and sometimes inconsistent guidance, where similar challenges such as cost, expertise limitations, documentation burden, and practical implementation are addressed through clearly different assumptions and priorities.

To move beyond framework-level comparison and towards a synthesis of how these issues are treated in practice, it is necessary to examine how the literature collectively frames key SME concerns. This includes how studies position resource constraints, the extent to which practical implementation guidance is provided, and whether human and organizational factors are treated as central or unimportant. The following table therefore extends the analysis from standards to studies, consolidating core themes across the reviewed literature to provide a comparative overview of the key themes, areas of focus, and methodological approaches identified across the selected literature.

Element of Comparison	Leo & Archie (2024)	Kereopa-Yorke (2024)	Yuhan & Hamilton (2024)	Soudi & Bauters (2024)	Soudi & Bauters (2024)	This paper:
Scope and Focus	Balances SME AI security with ethics.	LLMs to enhance SME cybersecurity.	AI integration in SME security and ops.	Adoption of AI ethics in SMEs.	Review of SME AI adoption barriers.	InfoSec role in s SME RAI adopti
Frameworks and Standards	Ethical frameworks for efficiency/transparency.	LLM integration model for SME security.	Robust AI-driven security frameworks.	Tailored ethics and accreditation.	PRISMA review of SME AI adoption.	PRISMA + ISO s for AI security.
Challenges Identified	Privacy, bias, transparency dilemmas.	LLM clarity and compliance gaps.	Resource limits and underestimated risks.	Lack of SME ethics guidelines/training.	Financial and infrastructure barriers.	Neglect of huma in AI security.
Methodological consistency	Case studies with ethics framework.	Mixed-methods: review, cases, tests.	Qualitative literature/practice review.	Guideline review to find SME gaps.	Systematic PRISMA-based review.	PRISMA with SM and InfoSec/RAI
Proposed Best Practices	Risk-based, transparent, trust-building.	LLMs with human expertise.	AI-driven detection and response.	Ethics, training, explainable AI.	Infra, cost, and SME support.	Train staff, foste integrate InfoSec

Research Gaps	No scalable SME AI frameworks.	Few SME-specific benchmarks.	Weak AI-business alignment.	No SME ethical guidelines/support.	Limited SME strategies for costs/skills.	Neglect of peopl integrated RAI.
Future Directions	Ethical, explainable AI frameworks.	Transparent, scalable LLMs for SMEs.	AI frameworks linking growth/security.	Sector-specific ethics and training.	SME solutions reducing costs/infra gaps.	Stronger human integrated InfoS
Unique Contributions	Insights on ethical SME AI.	LLM integration framework for SMEs.	AI security + efficiency benefits.	Practical sector-specific ethics.	Systematic SME AI barriers overview.	Human factor fo integrated RAI.
Specific Trends or Patterns	Ethical AI trend: transparency, compliance.	LLM adoption with human collaboration.	Cybersecurity + operational efficiency.	Sector-specific ethics and explainability.	Cost/infra barriers persist in SMEs.	Regulation/acco driving integrate frameworks.

Table 2: Comparison of Key Themes and Aspects Across Reviewed Literature.

The comparison reveals that the fragmentation observed across the reviewed studies is not incidental but reflects deeper structural characteristics of the existing research landscape. Studies approach RAI and Information Security from distinct disciplinary and institutional starting points such as technical security, ethical governance, regulatory compliance, or digital transformation, which shape how risks, controls, and responsibilities are prioritized. As a result, AI-specific risks, human oversight, and automation are interpreted inconsistently, and often in isolation from one another. For SMEs, this fragmentation is amplified by the tendency of frameworks and studies to inherit assumptions from large-enterprise or regulatory contexts, leaving limited guidance on how competing requirements can be reconciled under resource constraints. These dynamics indicate that the primary gap in current understanding is not the absence of relevant principles, but the lack of integrative perspectives that account for how security, ethics, and organizational realities interact in practice. This insight provides the basis for the research gaps identified in the following section.

7.2 Identification of Research Gaps

Even though there is extensive research on InfoSec and RAI, and a systematic and thorough approach was used to select relevant literature from reputable sources, significant gaps remain, particularly in relation to the needs and constraints of SMEs. These gaps are not limited to the absence of specific solutions, but reflect deeper conceptual, methodological, and organizational shortcomings in existing research. In particular, the literature frequently treats InfoSec and RAI as separate domains, relies on assumptions derived from large-enterprise contexts, and provides limited empirically grounded insight into how SMEs can operationalize integrated governance under real resource constraints. The following subsections examine these gaps as structural weaknesses in the current body of work.

Insufficient Empirical SME-Specific Research

Inadequate focus on SME-specific challenges backed by empirical data in InfoSec and RAI was a key gap identified in the existing literature. Current research often emphasizes large enterprises, overlooking the distinct constraints faced by SMEs. This notion was highlighted by all the reviewed papers as well. For example, the paper titled *Investigation of Artificial Intelligence in SMEs* emphasizes that most AI-related research targets large enterprises, leaving SMEs underrepresented. It underscores the disparity in resources, data availability, and implementation strategies between large corporations and SMEs and calls for SME-specific frameworks (Leon et al., 2024). However, due to the limited availability of robust, SME-specific empirical evidence, the reviewed studies do not converge on a consistent interpretation of the severity or practical implications of resource constraints for SMEs adopting InfoSec or RAI governance. Some papers portray resource limitations such as restricted funding, minimal in-house technical expertise, and limited time for governance activities, as the primary barrier preventing SMEs from adopting structured InfoSec or AI governance practices. Others take a more optimistic stance, suggesting that lightweight, modular governance approaches or incremental adoption strategies can still be feasible for SMEs despite these constraints. Additionally, while some authors emphasize the urgent need for SME-tailored frameworks due to these limitations, others argue that existing general frameworks can be adapted with minor adjustments. These conflicting perspectives reveal a lack of consensus on the extent to which SME resource constraints fundamentally limit the feasibility of adopting coherent governance structures and highlight the need for more empirical evidence that reflects the diverse operating realities of SMEs.

Lack of Unified Frameworks for SMEs

Another crucial issue is the lack of integrated frameworks that seamlessly combine InfoSec with RAI governance strategies and policies specific to SMEs. Existing frameworks, such as those from the European Union's AI Act (European Commission, 2025) and international standards like ISO/IEC 27001 (ISO/IEC, 2022) and ISO/IEC 42001 (ISO/IEC, 2023), often operate in silos, creating inconsistencies and challenges such as resource duplication and overlaps, gaps in coverage, increased complexity, and managerial overhead. There is, nevertheless, a significant research gap in integrated InfoSec and RAI frameworks tailored to SME contexts.

Beyond structural fragmentation, the literature also reveals conceptual and operational incompatibilities between InfoSec and RAI frameworks that further hinder unified adoption. InfoSec standards primarily adopt a risk- and control-driven orientation, emphasizing confidentiality, integrity, and availability through technical safeguards and restrictive access controls based on core InfoSec principles such as "least privileged" concept, "security by obscurity" concept, and the "need to know" principle. On the contrary, RAI frameworks prioritize ethical principles such as transparency, accountability, fairness, and human oversight, which often require greater openness, explainability, and stakeholder involvement. These differing priorities can create tensions in practice, particularly where security-driven access restrictions conflict with transparency and explainability expectations associated with RAI.

The challenges identified above become more prominent when viewed through the lens of SME resource constraints. Fragmented frameworks require SMEs to duplicate risk assessments, policy development, documentation cycles, and training activities, which are tasks that are often beyond their financial and staffing capacity. Limited expertise further

complicates adoption, as SMEs frequently lack the specialized knowledge required to reconcile competing guidance from InfoSec and RAI standards. Time constraints, driven by lean staffing and high operational load, further reduce the feasibility of implementing and maintaining multiple governance structures in parallel.

These realities underscore the practical importance of integrated frameworks for SMEs. Such frameworks not only provide conceptual alignment between security and ethical considerations but also reduce operational friction, lower governance overhead, and make compliance and risk management more attainable for resource-constrained organizations. The absence of integrated, SME-oriented approaches that explicitly address both fragmentation and incompatibility remains a key gap in the current literature.

Insufficient Practical Aspects

Even though theoretical discussions on InfoSec and RAI are well developed, the reviewed literature provided limited actionable guidance for SMEs on how these principles can be operationalized in practice. Practical aspects such as implementing secure and responsible AI pipelines, addressing AI powered real-time security risks, and aligning restrictive and "closed" security strategies and AI operations with ethical and regulatory expectations are frequently addressed at a high level, with insufficient attention to day-to-day implementation realities faced by SMEs (Marwa et al., 2024). As a result, SMEs are often left with abstract recommendations that are difficult to translate into concrete operational practices.

The literature revealed that this limitation is not merely a matter of missing detail but reflects fundamentally different interpretations of what "practical implementation" means. Some studies implicitly equate practicality with technological sophistication, assuming that SMEs can adopt automation-heavy solutions, advanced AI-driven security tools, and complex monitoring infrastructures. Other contributions frame practicality in organizational terms, emphasizing governance processes, training, and oversight as more realistic levers for SMEs. These competing interpretations are not acknowledged or reconciled, resulting in guidance that is internally coherent within individual studies but inconsistent across the literature as a whole.

More critically, this divergence exposes a deeper analytical problem: much of the existing research evaluates practicality through assumptions inherited from large-enterprise or regulatory contexts, rather than from empirically grounded SME realities. In prioritizing conceptual completeness, technical robustness, or regulatory alignment, the literature often underestimates the cumulative burden of cost, expertise, documentation, and time imposed on SMEs. Consequently, many proposed practices are theoretically sound but structurally misaligned with the organizational capacity of SMEs, rendering them difficult to adopt or sustain in practice.

This misalignment has tangible consequences. Because SMEs lack the resources to experiment with multiple frameworks, tools, or governance models, impractical guidance does not simply delay adoption, it actively constrains it. SMEs are forced to make ad-hoc decisions, selectively implement fragments of guidance, or defer governance activities altogether. The persistence of limited practical guidance therefore reflects not only SME constraints, but also a systemic gap in the literature's ability to generate implementation pathways that are both feasible and scalable for resource-constrained organizations. This

gap reinforces the need for integrated approaches that translate high-level InfoSec and RAI principles into context-aware, operationally attainable practices for SMEs.

The Human Factor: Under-representation of Non-technical Barriers

Although organizational culture, employee awareness, and stakeholder engagement are frequently acknowledged as important, the reviewed literature tends to downgrade these factors in favor of technological, procedural, and policy-driven solutions. Much of the existing work treats human-related issues as secondary considerations or contextual background, rather than as core governance variables that actively shape the effectiveness of InfoSec and RAI practices. This tendency is particularly evident in studies that prioritize technical controls, formal processes, or regulatory compliance, while offering limited analysis of how these mechanisms are enacted, interpreted, or sustained by people within organizations.

From a critical perspective, this under-representation reflects a structural bias in the literature rather than an absence of evidence. Human factors are difficult to standardize, quantify, and audit, making them less open to the dominant analytical frameworks used in InfoSec and RAI research. As a result, people are often framed implicitly as sources of risk, through error or misuse, rather than as active agents of governance whose behavior, decision-making, and cultural context determine whether controls and processes are effective in practice. This framing leads to solutions that assume compliance and rational behavior, without adequately accounting for the social and organizational dynamics that shape everyday security and AI-related decisions.

The implications of this bias are particularly significant for SMEs. In SMEs, roles are less specialized, responsibilities overlap, and governance practices are closely intertwined with daily operations. When human factors are treated as peripheral, proposed frameworks and best practices risk becoming organizationally instable: technically sound on paper but poorly aligned with how work is actually performed. Empirical evidence indicating that a substantial proportion of security incidents involve non-malicious human actions underscores this misalignment, not as a failure of individuals, but as a failure of governance approaches that insufficiently integrate human behavior into their design.

The persistence of this gap suggests that existing research has not fully dealt with the human dimension as a first-order concern in InfoSec and RAI governance. Rather than reflecting a lack of awareness, the under-representation of human factors points to an analytical limitation in how governance is conceptualized by prioritizing controls and structures over organizational realities. For SMEs, this limitation is consequential: without explicit consideration of training, culture, leadership engagement, and shared responsibility, efforts to integrate InfoSec and RAI are likely to remain fragmented and difficult to sustain. This underscores the need for governance approaches that treat people not merely as a risk to be managed, but as a central component of effective, context-aware security and AI practices.

8. Limitations of the Review and Future Directions

Although the review leveraged the PRISMA methodology for the non-biased selection of relevant articles, it may still exclude relevant studies due to limitations in search terms,

databases, or accessibility of the publication, potentially narrowing the scope of the findings.
However, the main limitation of the review was the *lack of empirical validation*. Most of the selected papers were theoretical and relied on statistical analysis with minimal experiments. They lacked comprehensive experimental data or inputs drawn directly from real SME operations. Consequently, the findings have not been thoroughly tested in real-world SME scenarios, which may limit their robustness and practical applicability.

8.1 Future Research Opportunities

Future research in InfoSec and RAI should focus on generating empirical data to produce actionable and relevant insights, addressing two critical areas for SMEs.

Integrated Frameworks for InfoSec and RAI

Research should prioritize the development and validation of integrated frameworks that seamlessly align InfoSec and RAI objectives. Empirical studies can explore how SMEs can optimize resource utilization, avoid duplicate efforts, and improve scalability while ensuring compliance with evolving regulatory standards. Such frameworks should be tested across diverse SME environments to ensure practical applicability and adaptability.

Prioritizing and Improving the Human Factor

Understanding how SMEs can best prioritize and improve the human factor is essential to achieving a balanced approach to InfoSec and RAI. Future research should investigate effective strategies for training, awareness programs, and stakeholder engagement to empower individuals as key contributors to InfoSec initiatives. Empirical studies can explore how this balance supports ethical AI practices and strengthens SMEs' resilience against security challenges. By addressing these areas, future research can provide SMEs with robust, evidence-based tools to integrate InfoSec and RAI effectively, fostering sustainable and ethical business growth.

As a concrete next step, the integrated InfoSec and RAI approach discussed in this paper could be operationalized through a staged maturity model tailored to SME contexts, enabling incremental adoption based on organizational capacity and digital readiness. Such a model could be evaluated through small-scale, sector-specific pilot studies to assess feasibility, governance overhead, and practical impact in real SME environments. In parallel, targeted empirical studies can further examine how SMEs optimize resource utilization, avoid duplication, and scale governance practices while responding to evolving regulatory requirements. Finally, guidance for policymakers and standards bodies is needed to support the adaptation of existing frameworks for SMEs, for example through scoped compliance pathways, simplified implementation guidance, or sector-specific support mechanisms.

9. Conclusion

This review demonstrates that the responsible adoption of AI in SMEs hinges on integrated approaches that balance ethics, security, and operational efficiency. The studies collectively emphasize that while AI technologies such as LLMs and automation offer powerful opportunities to enhance SME competitiveness, their value is fully realized only when aligned with frameworks that embed transparency, trust, and compliance. For

SMEs with limited resources, integrated InfoSec–RAI frameworks are particularly vital, as they streamline processes, prevent duplication, and ensure that innovation can progress without undermining ethical or regulatory obligations.

Equally, the findings highlight that SMEs cannot achieve secure and sustainable AI adoption by focusing solely on processes and technologies; the human factor remains central. Training, awareness, and stakeholder engagement are essential to cultivate a culture where ethical awareness and cybersecurity are embedded into daily practice. Recognizing people as critical pillars alongside processes and technology ensures that SMEs are not only better protected against risks but are also equipped to leverage AI responsibly as they adapt to rapidly evolving digital and regulatory landscapes.

Author Contributions: Conceptualization, Md Atiqur Rahman Ahad and Charles Ribeiro Quainoo; methodology, Charles Ribeiro Quainoo; validation, Md Atiqur Rahman Ahad and Charles Ribeiro Quainoo; formal analysis, Charles Ribeiro Quainoo; investigation, Charles Ribeiro Quainoo; resources, Md Atiqur Rahman Ahad; data curation, Charles Ribeiro Quainoo; writing original draft preparation, Charles Ribeiro Quainoo; writing review and editing, Md Atiqur Rahman Ahad and Charles Ribeiro Quainoo; visualization, Charles Ribeiro Quainoo; supervision, Md Atiqur Rahman Ahad; project administration, Md Atiqur Rahman Ahad. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

ACM. (2025). ACM Digital Library. https://dl.acm.org

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–5). IEEE. https://doi.org/10.1109/CyberSA49311.2020.9139638

Baker, S., & Xiang, W. (2023). Explainable AI is responsible AI: How explainability creates trustworthy and socially responsible artificial intelligence. *arXiv*. https://doi.org/10.48550/arXiv.2312.01555

Carayannis, E. G., Dumitrescu, R., Falkowski, T., & Zota, N.-R. (2024). Empowering SMEs: Harnessing the potential of Gen AI for resilience and competitiveness. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2024.3456820

Center for Strategic and International Studies. (2024). Protecting data privacy as a baseline for responsible AI. https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai

Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P.-F., Han, Y., Jmila, H., Blanc, G., Takahashi, T., & Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: A literature survey. *Annals of Telecommunications, 78*(1–2), 45–67. https://doi.org/10.1007/s12243-022-00926-7

Coshow, T. (2024). Agentic AI: Behind the 2025 top tech trend.

CXO Today. (2025). 8 key trends in AI/ML product strategy for SMEs and enterprises in 2025.

Elsevier. (2025a). Scopus. https://www.scopus.com
Elsevier. (2025b). ScienceDirect. https://www.sciencedirect.com

Ernst & Young. (2024). Addressing AI risks: Preventing bias and achieving ethical AI use. https://www.ey.com/en_us/insights/emerging-technologies/addressing-ai-risks-preventing-bias-and-achieving-ethical-ai-use

European Commission. (2019). Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

European Commission. (2024). SME definition. https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en

European Commission. (2025a). Data protection: Rules for the protection of personal data inside and outside the EU.

European Commission. (2025b). Regulation (EU) 2024/1689 on artificial intelligence. https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Gates, B. (2018). AI can be our friend. CNBC.

Haan, K. (2023). How businesses are using artificial intelligence in 2025.

Hashmi, E., Yamin, M. M., & Yayilgan, S. Y. (2024). Securing tomorrow: A comprehensive survey on the synergy of artificial intelligence and information security. *AI and Ethics*. https://doi.org/10.1007/s43681-024-00529-z

High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. European Commission. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Hinton, G. E. (2023). Pioneering work in artificial intelligence and deep learning.

Hupe, A., Bretschneider, U., Lange, K., Trostmann, T., Stubbemann, L., Leimeister, J. M., & Refflinghaus, R. (2023). Barriers of SMEs in adopting crowdsourcing and -working and strategies to overcome them (Tech. Rep. No. 16). Kassel University Press.

IBM. (2024a). AI and privacy: Ethical challenges and best practices.
IBM. (2024b). Responsible AI. https://www.ibm.com/think/topics/responsible-ai
IBM. (2025a). Large language models. https://www.ibm.com/topics/large-language-models
IBM. (2025b). Generative AI: Insights, trends, and technologies. https://www.ibm.com/think/topics/generative-ai

IEEE Staff. (2022). Systematic reviews in engineering and technology. IEEE Xplore.
IEEE. (2025). IEEE Xplore Digital Library. https://ieeexplore.ieee.org

IFC. (2021). MSME finance gap: Assessment of the shortfalls and opportunities in financing micro, small, and medium enterprises.

ISC². (2024). About ISC². https://www.isc2.org/about

ISACA. (2021). Cyberresilience in an evolving threat landscape. *ISACA Journal, 3*.
ISACA. (2022a). Developing an artificial intelligence governance framework.
ISACA. (2022b). Information security, cybersecurity and privacy protection - Information security management systems - Requirements (ISO/IEC 27001:2022).
ISACA. (2024a). AI governance: Key benefits and implementation challenges.
ISACA. (2024b). Building a secure and compliant AI infrastructure: Lessons from the trenches.
ISACA. (2024c). Responsible AI governance in traditional and emerging ecosystems.
ISACA. (2024d). Who we are. https://www.isaca.org/about-us/who-we-are

Jalil, M. F., Lynch, P., Affizzah, D. B., Marikan, A., & Isa, A. H. B. M. (2025). The influential role of artificial intelligence adoption in digital value creation for SMEs: Does technological orientation mediate this relationship? *AI & Society, 40*(3), 1875–1896. https://doi.org/10.1007/s00146-024-01969-1

Kereopa-Yorke, B. (2023). Building resilient SMEs: Harnessing large language models for cybersecurity in Australia. *arXiv*. https://doi.org/10.48550/arXiv.2306.02612

Leo, N., & Archie, O. (2024). AI and cybersecurity for SMEs: Balancing ethical considerations and operational efficiency. https://doi.org/10.13140/RG.2.2.33120.49923

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., Clarke, M., Devereaux, P. J., Kleijnen, J., & Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Journal of Clinical Epidemiology, 62*(10), e1–e34. https://doi.org/10.1016/j.jclinepi.2009.06.006

Microsoft Azure. (2023). Security and responsible AI guide.

Mitnick, K. (2023). About Kevin Mitnick. https://www.mitnicksecurity.com/kevin-mitnick
Mitnick, K. (2024). 15 cybersecurity quotes from famous people in the field.

Munich Re. (2024). Cyber insurance risks and trends 2024. https://www.munichre.com/en/solutions/for-industry-clients/cyber/cyber-insurance-trends.html

National Institute of Standards and Technology (NIST). (2024). The NIST Cybersecurity Framework (CSF) 2.0. https://www.nist.gov/cyberframework

OECD. (2021a). Digitalization in SMEs: Progress and challenges.
OECD. (2023). SME and entrepreneurship outlook 2023.

Oldemeyer, L., Jede, A., & Teuteberg, F. (2024). Investigation of artificial intelligence in SMEs: A systematic review of the state of the art and the main implementation challenges. *Management Review Quarterly*. https://doi.org/10.1007/s11301-024-00405-4

Oxford Business Review. (2023). The role of digital transformation in scaling SME operations.

Pan, Z., & Mishra, P. (2023). Explainable AI for cybersecurity. Springer. https://doi.org/10.1007/978-3-031-46479-9

Richardson, B., & Gilbert, J. E. (2021). Fairness in artificial intelligence: Challenges and opportunities. *arXiv*. https://doi.org/10.48550/arXiv.2112.05700

Salamon, L. M., & Siegfried, J. J. (2020). Economic power and political influence: The impact of industry structure on public policy. *American Political Science Review, 114*(3), 763–781.

Schneier, B. (2023). About Bruce Schneier. https://www.schneier.com/about/
Schneier, B. (2022). Humans and cybersecurity: The weakest link or the best defense?

Schwaeke, J., Peters, A., Kanbach, D. K., Kraus, S., & Jones, P. (2025). The new normal: The status quo of AI adoption in SMEs. *Journal of Small Business Management, 63*(3), 1297–1331. https://doi.org/10.1080/00472778.2024.2379999

Soudi, M. S., & Bauters, M. (2024). AI guidelines and ethical readiness inside SMEs: A review and recommendations. *Digital Society, 3*(3). https://doi.org/10.1007/s44206-024-00087-1

Verizon. (2023). 2023 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
Verizon. (2024). 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/2024/

Walmsley, J. (2020). Artificial intelligence and the value of transparency. *AI & Society, 36*, 585–595. https://doi.org/10.1007/s00146-020-01066-z

World Bank. (2020). Small and medium enterprises in the pandemic: Impact, responses, and the role of development finance.
World Bank. (2021). Regulatory constraints and opportunities for SMEs in emerging economies.

Yuhan, N., & Hamilton, J. (2024). Strengthening SMEs through cybersecurity and AI: A path to operational excellence. https://www.researchgate.net/publication/384443733