Journal of Global Information Management
Volume 33 • Issue 1 • January-December 2025

Information Security Policy Compliance: A Structured Review Using Scientometric Analysis and Topic Modeling

Anuj Sharma
https://orcid.org/0000-0001-6602-9285
Jindal Global Business School, O.P. Jindal Global University, India

Alex Koohang
https://orcid.org/0000-0002-4565-0408
Middle Georgia State University, USA

Satender Pal Singh
T.A. Pai Management Institute, India

ABSTRACT

Protecting key information assets from security attacks, cyber threats, and data breaches is critically important for organizations. Information security policies (ISPs) establish guidelines to safeguard sensitive data, reduce risks, and promote secure employee behavior. However, internal employees' careless or malicious actions often lead to significant security vulnerabilities. Consequently, information security policy compliance (ISPC) has become a vital focus for both academics and practitioners. Given the diverse and vast ISPC literature, an integrative review is needed to unify scattered knowledge and identify future research hotspots. This study uses scientometric analysis and topic modeling to provide a structured retrospective, highlighting key contributors, influential articles, institutions, and evolving themes to guide future research directions.

KEYWORDS

Information Security Policy Compliance, Information Security, Scientometric Analysis, Topic Modeling, Structural Topic Models, Co-Citation Analysis

1. INTRODUCTION

Information security breaches have detrimental consequences for business organizations in the contemporary interconnected digital economy (Almuqrin, 2024; Alraja, Butt, & Abbod, 2023). Despite numerous information security mechanisms adopted by business organizations, information security threats continue to sabotage business operations and financial performance, including financial losses, reputational damage, lost productivity, operational disruptions, legal complications, and damage to customer confidence (Bolek, Romanová, & Korček, 2023; Ganye & Smith, 2025; Jeong, Lee, & Lim, 2019; Koohang et al., 2021). Among all the security threats and attacks on information assets that organizations face, internal employees' actions and their non-compliant security behavior have been reported as the greatest risk (Ganye & Smith, 2025; Gerdin, Grönlund, & Kolkowska, 2025; Herath & Rao, 2009a; Hu et al., 2012). Employees have different roles and responsibilities in the organization. Accordingly, they are granted access to the organization's sensitive information and key digital assets stored in enterprise systems to execute their routine work activities. Literature

DOI: 10.4018/JGIM.389715

reports that organizations authorize users and restrict access to enterprise information systems based on a tiered structure known as Role-Based Access Control (RBAC) that grants access to roles rather than persons (Ferraiolo et al., 1999). However, RBAC can not prevent the misuse of granted access. Although business organizations implement information security policies (ISPs) to protect sensitive information and guide employees' security behavior, most data leaks occur due to insider threats such as human error, insider abuse of enterprise systems, compromised credentials, lack of security awareness, and negligence of ISPs (Aggarwal & Srivastava, 2024; Alrawhani et al., 2025; Arif et al., 2025; Brooks, Williams, & Lee, 2024; Gerdin et al., 2025; Vedadi et al., 2024). Hence, the malevolent and irresponsible behavior of employees leads to a lack of understanding of security policies, making them the weakest link in organizational information security (Bulgurcu, Cavusoglu, & Benbasat, 2010; Moody, Siponen, & Pahnila, 2018; Siponen et al., 2014; Warkentin & Willison, 2009).

ISPs specify roles, responsibilities, rules, guidelines, standard operating procedures, obligations, and technical controls to ensure the confidentiality, integrity, and availability of data and information assets (Bulgurcu et al., 2010; D'Arcy & Teh, 2019; D'Arcy, Hovav, & Galletta, 2009; Ifinedo, 2014). Further, ISPs help employees contest security threats and breaches, identify and assess potential vulnerabilities, detect and prevent human errors, manage security incidents, minimize response time, recover compromised information, and restore information systems quickly and effectively (Flowerday & Tuyikeze, 2016; Höne & Eloff, 2002; Sohrabi Safa, Von Solms, & Furnell, 2016). Hence, ISPs ensure that organizational information assets are protected against misuse, abuse, and destruction (Koohang et al., 2021; Moody et al., 2018). However, research reports that developing and enforcing a comprehensive ISP may not lead to adequate information security in an organization because employees knowingly or unknowingly violate the ISP, resulting in security breaches, risks, and vulnerabilities (Alec Cram, D'Arcy, & Proudfoot, 2019; Amankwa, Loock, & Kritzinger, 2021; D'Arcy & Teh, 2019; Vedadi et al., 2024). Therefore, fostering employees' compliance with ISPs has become a top strategic priority where the security-conscious behavior of employees is guided, monitored, encouraged, and rewarded (Alrawhani et al., 2025; Vedadi et al., 2024). Moreover, non-compliance with ISPs is discouraged through sanctions such as formal disciplinary actions, as well as training, awareness, and engagement programs (Aggarwal & Dhurkari, 2023; Aggarwal & Srivastava, 2024; D'Arcy et al., 2009; Gerdin et al., 2025).

Information Security Policy Compliance (ISPC) has garnered considerable attention from the academic and practitioner communities. Wylder (2003) concluded that information security professionals have to face severe challenges while enforcing policies related to corporate information security (Wylder, 2003). Moreover, due to inherent complexities related to human factors such as employees' security behavior, ensuring compliance with ISP is a formidable task (Vroom & von Solms, 2004). Siponen, Mahmood, & Pahnila (2009) discovered that employees' self-efficacy and response efficacy play an important role in shaping their behavior toward complying with the ISPs. Moreover, this study also reported that awareness and knowledge about organizational vulnerabilities and the severity of security threats also shape the compliance behavior of users (Siponen, Mahmood, & Pahnila, 2009). Further, IPSC researchers reported that extrinsic factors, such as subjective norms and peer behaviors, had a significant influence on the compliance behavior of employees, while penalties and punishment could not shape appropriate security behaviors (Herath & Rao, 2009a). To tackle the issues related to non-compliance with ISPs, researchers have suggested that training programs that stimulate systematic cognitive processing and intensive reasoning of information security-related knowledge are more effective in ensuring ISPC (Puhakainen & Siponen, 2010).

The extant literature on behavioral information security suggests that both individual and organizational factors lead to ISPC. The factors bring conceptual diversity in terms of the constructs used and the theories employed to explain the compliance and non-compliance behavior related to ISPs. At an individual level, previous studies have explored the role of factors such as attitude and perceived behavioral control (Bulgurcu et al., 2010), self-efficacy and response efficacy (Ifinedo, 2014), habits and personal coping mechanisms (Vance, Siponen, & Pahnila, 2012), individuals'

rational decision-making related to the benefits and repercussions of ISPC (Moody et al., 2018), employees normative and moral considerations (D'Arcy & Lowry, 2019), commitment, belief, and attachment (Choi & Song, 2018), fear (Koohang et al., 2021), cognitive load, efficacy, and coping methods (Ganye & Smith, 2025) etc., in influencing ISPC as an outcome variable.

Similarly, at the organizational level, researchers report that persuasive communication, such as fear appeals (Mwagwabi, McGill, & Dixon, 2018), perceived organizational support and social influence (Vedadi et al., 2024), organizational culture (Allahawiah, Altarawneh, & Al-Hajaya, 2024; Alrawhani et al., 2025; Nasir et al., 2022), supervisor and leadership factors (Kim, Choi, & Han, 2019; Wang & Xu, 2021), leadership style (Feng et al., 2019), organizational structures and perceived organizational formalization (Hong & Furnell, 2022), perceived organizational and management support (Sharma & Warkentin, 2019), and effectiveness of training and awareness programs (Kim et al., 2019; Puhakainen & Siponen, 2010) have a strong influence on ISPC. Finally, there are numerous studies that have examined the combined influence of organizational and individual factors (Amankwa et al., 2021; Koohang et al., 2020).

Furthermore, other than conceptual diversity, ISPC research has employed theories from diverse domains to explain ISP compliance and non-compliance. The most popular theories used in ISPC research are the Theory of Planned Behavior (Bulgurcu et al., 2010; Hong & Furnell, 2022; Ifinedo, 2012), Protection Motivation Theory (Alrawhani et al., 2025; Ifinedo, 2012; Vance et al., 2012), Deterrence Theory (D'Arcy & Herath, 2011; Guan & Hsu, 2020; Wang & Xu, 2021), Rational Choice Theory (Moody et al., 2018), Social Bond Theory (Ali, Dominic, & Ali, 2020; Feng et al., 2019), Social Exchange Theory (S. Sharma & Warkentin, 2019; Zhen & and Chen, 2022), Social Action Theory (Hedström, Karlsson, & Kolkowska, 2013), and Theory of Reasoned Actions (Siponen et al., 2014). However, ISPC research is still evolving, and researchers are still trying to explore new theories and constructs to explain the conceptual inconsistencies (Gerdin et al., 2025).

In light of the above, researchers have concluded that the scope of the ISPC literature is vast, and the intellectual and conceptual diversity of ISPC research leads to fragmentation in the overall body of knowledge (Alassaf & Alkhalifah, 2021; R. F. Ali, Dominic, Ali, Rehman, & Sohail, 2021). It is imperative that the existing literature on ISPC should be critically reviewed to report the patterns, trends, and impact of the vast literature. Such an endeavor can provide a comprehensive overview of the existing research that can help potential researchers identify avenues of future research, seek collaborations, and explore funding and employment opportunities. With an objective of consolidating the state-of-the-art on ISPC and providing a unified view of the scattered knowledge, previous studies have attempted to review ISPC research from different perspectives (Alassaf & Alkhalifah, 2021; BalaGopal & Mathew, 2024; Gerdin et al., 2025). However, most of the previous reviews have limited scope and restricted coverage of the literature. Moreover, all of these studies have adopted a narrative and theme-based approach in which the issues related to subjective bias may not be ignored. Hence, a scientific mapping and comprehensive analysis of the intellectual and conceptual structure of literature, with performance analysis of key authors, institutions, countries, themes, and topics, is urgently required.

To address the research gap identified above, this study conducts an introspective evaluation of ISPC research using scientometric analysis and topic modeling. Given this objective, the present study aims to examine the following research questions:

RQ1: What are the most impactful articles, influential researchers, productive institutions, and research-supportive countries for ISPC?

RQ2: What are the main themes and key topics of high academic interest, and how do these themes progress and evolve?

RQ3: What types of patterns can be reported from intellectual collaborations between authors and keywords co-occurrence analysis?

RQ1 is addressed by performance analysis that will facilitate understanding the development and impact of scholarly outcomes in ISPC. Further, topic modeling on the ISPC literature is conducted to address RQ2. Additional assessment of emergent topics and themes will assist in developing an agenda for future research. Finally, RQ3 will be addressed by performing a scientometric analysis that will consist of mapping author collaboration, co-citation associations, and keyword co-occurrences, enabling an inclusive understanding of the vast and voluminous ISPC research. The methodology, search protocol, methods, results, discussion, and limitations of the present study are explained in the next subsections.

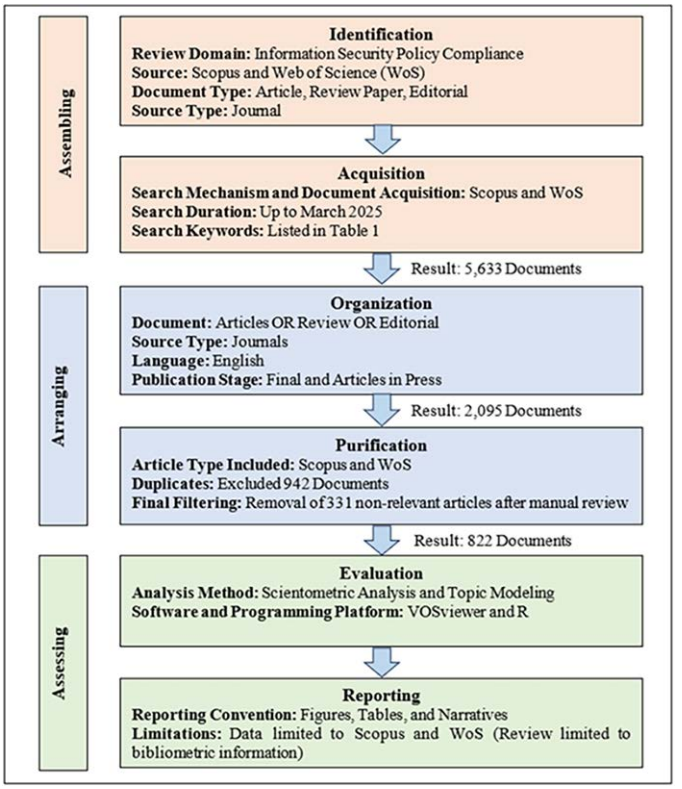
2. METHODOLOGY

This study uses a systematic and scientific approach to review the extant literature on ISPC. Figure 1 describes our three-stage and six-step literature review approach. The first stage (Assembling) involves the identification and acquisition of relevant literature using appropriate databases. This study used both Scopus and Web of Science (WoS) to acquire the literature following previous studies (Sharma, Rana, & Nunkoo, 2021; Singh et al., 2020, 2023). The current study used the bibliometrix approach reported by Lim et al. (2024) to combine and clean data. An extensive literature search was performed to list all the keywords related to ISPC. The primary keywords and their synonyms and variations were checked, listed, and refined in an iterative way. Subsequently, the final list of keywords was consulted and validated by four independent experts with more than two decades of experience, of whom two were from academia and the rest were from industry. This study involved industry experts to cover the ISPC domain-specific terminology. Table 1 provides the final keywords that were used using proper Boolean operators "OR" for an entire set and "AND" to combine with another set. The next stage involved data filtering, where this study used several inclusion and exclusion criteria to remove non-English, duplicate, and irrelevant documents and retrieve the final set of articles consisting of 822 articles. Finally, in the assessing stage, the current study used scientometric analysis and topic modeling to report the results.

Table 1. List of keywords

Set A	Set B	Set C	Set D
Information Security	Policy/Policies	Compliance	Management
Cybersecurity	Standard/Standards	Adherence	Leadership
IT Security	Governance	Conformance	Strategy
Information Technology Security	Regulation	Enforcement	Supervision
Data Security	Regulatory	Noncompliance	Administration
Computer Security	Protocol	Non-compliance	
Network Security	Strategy	Violation	
Computer System Security	Rule		
Data Protection	Behavior/Behaviour		
Information Systems Security	Plan		
IS Security			

Figure 1. Search protocol with inclusion and exclusion criteria



2.1. Topic Modeling Based on STM

This study has used a contemporary approach to perform topic modeling based on structural topic models (STM), which is quite popular for similar analyses (Nunkoo, Sharma, So, Hu, & Alrasheedi, 2025; A. Sharma et al., 2021; Singh et al., 2023). STM works well with research documents, as it involves the incorporation of document-level metadata in the topic model-building process, which enables researchers to explore the latent topics as well as the temporal trends related to topics (Das et al., 2023). In the current study, the title, keywords, and abstract form the text corpus, and the publication year are used as document-level metadata. The tm package in the R language is adapted to preprocess the text corpus because raw text data contains irrelevant information, such as punctuation, numbers, special characters, stop words, publisher's information, etc., that can negatively impact the accuracy of the STM algorithm. Tokenization converts the clean text into tokens, which is a crucial step for document vectorization. However, an n-gram tokenizer preprocessed the important bigrams and trigrams into unigrams to preserve their semantics in document vectors. Bigrams (two-word combinations such as *security policy*) and trigrams (three-word combinations such as *information security policy*) are processed separately in topic modeling because they capture multi-word concepts. Extracting these frequent n-grams and processing them separately improves the semantic quality of topics. This also preserves the meaning and domain-specific terminology of multi-word phrases. The stm package in R programming was used to experiment with different topic models with a number of topics ranging from 4 to 30. Finally, the optimal topic model with six (6) topics was selected after checking the semantic coherence and exclusivity scores, which are standard measures suggested by previous studies (Baker et al., 2021; Sharma et al., 2021). The top words from each topic and documents related to each topic were explored further to derive meaningful patterns related to predominant topics and their trends.

2.2. Scientometric Analysis

Scientometrics is a quantitative assessment method for understanding and evaluating the conceptual, intellectual, and social structure of research (Das et al., 2023). The conceptual structure of research is mapped using keyword density visualization, keyword co-occurrence analysis, and keyword overlay networks (Sharma et al., 2023). Further, the intellectual structure of literature is scientifically mapped using co-citation analysis and bibliometric coupling, which visualize the studies that form the core of knowledge in a specific domain (Shiwangi Singh et al., 2020). The co-citation analysis uses the PageRank algorithm and cluster centrality score to report landmark articles that greatly influence the intellectual structure of research. Finally, the social structure of the research is explored and reported using co-authorship network analysis and world collaboration networks. This study has used VOSviewer (van Eck & Waltman, 2014) to perform scientometric analysis on ISPC research. The keyword analysis reveals interesting patterns related to key concepts and their evolution. Moreover, the author's co-authorship network analysis discovers the main scientific actors of ISPC research and their social interrelationships that help in advancing ISPC knowledge. Finally, a co-citation analysis on ISPC visualizes the clusters of research that bring novelty, develop perspectives, drive innovation, and fuel progress in the domain of ISPC.

3. RESULTS

3.1. Performance Impact Assessment

Table 2 summarizes the ISPC research evaluated in the present study. ISPC has been explored in 822 studies published in 320 different Scopus-indexed outlets with an impressive growth rate of 17.13 percent. Figure 2 confirms that ISPC research has endured substantial growth in the last five years, which makes it an active area of scientific inquiry. The left-skewed distribution of research articles in annual growth visualization suggests that previous knowledge on the current topic significantly impacts the development of new knowledge, perspectives, theories, and methods. Although the average citation per document is more than 30, the average life of articles is only 4.6 years, indicating a contemporary significance of ISPC that attracts ample scholarly attention. A total of 157 authors have published 182 solo-authored articles, which shows that some solo authors have published more than one single-authored article. Moreover, on average, there are three co-authors in other studies, with more than 27 percent collaboration with international researchers. A larger number of international collaborations in ISPC studies indicates a greater impact and extensive recognition of this domain by the global scientific community.

Table 2. An overview of the ISPC studies

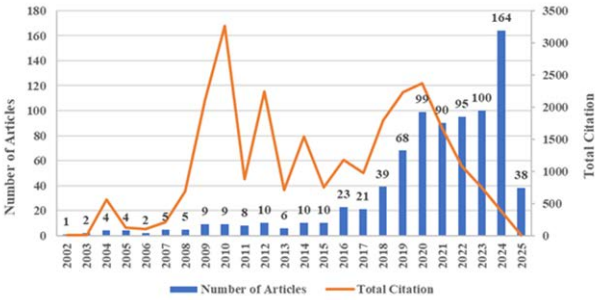
Description	Results
Period of studies on ISPC	2002:2025
Total number of documents	822
Total number of unique outlets publishing ISPC research	320
Annual Growth Rate (%) of ISPC research	17.13
Average Age of each article (years since publication)	4.63
Average citations garnered by ISPC articles	30.48
Total number of references used in ISPC articles	39,446
Number of research keywords used in ISPC articles	2,280

continued on following page

Table 2. Continued

Description	Results
Total number of unique contributors	2,040
Authors of single-authored research papers	157
Articles contributed by a single author	182
Average co-authors per document	3
International co-authorships %	27.62

Figure 2. Annual Growth of ISPC Articles for 2002 - 2025



3.1.1. Author Impact Assessment

Author impact assessment provides a quantitative method to measure the contribution, reach, influence, and scholarly value of various scientific actors in a domain (A. Sharma et al., 2023). It is also crucial for benchmarking researchers against peers, promoting collaboration, identifying best practices for optimizing research impact, and raising awareness about impactful research within the scientific community (Das et al., 2023; Shiwangi Singh et al., 2020). Previous research on assessing the researcher's impact has recommended that the total number of publications (NP), the accumulated total citations (TC), and the citable durations indicated by the year of the first publication (starting year) are established measures of impact (Singh et al., 2020). Table 3 reports the top 20 high-impact authors and their current affiliations as per Scopus databases. The readers may note that there can be a small variation in counting the number of citations by various public and proprietary databases. It is evident that Prof. Mikko Siponen at the University of Alabama, Prof. John D'Arcy at the University of Delaware, and Prof. Merrill Warkentin at Mississippi State University lead the ISPC community by producing valuable and meaningful work.

Table 3. Most prolific authors and their details

Rank	Author	Current Affiliation	NP	TC	Starting Year
1	Siponen, Mikko	University of Alabama, USA	11	3359	2009
2	D'Arcy, John	University of Delaware, USA	9	1220	2011
3	Warkentin, Merrill	Mississippi State University, USA	9	520	2018
4	Kolkowska, Ella	Örebro University, Sweden	8	280	2011

continued on following page

Table 3. Continued

Rank	Author	Current Affiliation	NP	TC	Starting Year
5	Han, Jinyoung	Chung-Ang University, Republic of Korea	7	184	2017
6	Vance, Anthony	Virginia Polytechnic Institute and State University, USA	7	1979	2009
7	Dominic, P.D.D.	Universiti Teknologi Petronas, Malaysia	6	141	2020
8	Karlsson, Fredrik	Örebro University, Sweden	6	273	2011
9	Dhillon, Gurpreet	University of North Texas, USA	6	125	2006
10	Furnell, Steven	University of Nottingham, UK	6	339	2016
11	Koohang, Alex	Middle Georgia State University, USA	5	112	2020
12	Lowry, Paul Benjamin	Virginia Polytechnic Institute and State University, USA	5	718	2013
13	Paliszkiewicz, Joanna	Warsaw University of Life Sciences, Poland	5	135	2019
14	Nord, Jeretta Horn	Oklahoma State University, USA	5	104	2020
15	Ali, Rao Faizan	University of Kent, UK	5	141	2020
16	Cram, W. Alec	University of Waterloo, Canada	5	214	2017
17	Pahnila, Seppo	University of Oulu, Finland	5	1722	2009
18	Rao, H. Raghav	University of Texas at San Antonio, USA	5	240	2006
19	Barati, Masoud	Carleton University, Canada	4	113	2019
20	Fensel, Anna	Wageningen University, Netherlands	4	47	2022

3.1.2. Most Impactful Articles

Reporting highly impactful articles in research is crucial, as they represent significant advancements and discuss influential discoveries related to important research avenues (Das et al., 2023; Sharma et al., 2021). Total citation and total citation per year are the two most popular measures that reflect the quality and impact of research (Sharma et al., 2023). Table 4 lists the top 20 highly cited articles that shape the intellectual core of the field and serve as a solid foundation for future research endeavors. Bulgurcu, Cavusoglu, & Benbasat (2010), Herath & Rao (2009b), Siponen & Vance (2010), Herath & Rao (2009a), and Ifinedo (2012) are the most impactful studies that have explored important research questions and generated valuable insights. The measures TC and TC per year reported in Table 4 are as per the Scopus database, and minor variations may be reported in other databases. It is worth reporting that while citations may not be a perfect measure of scholarly quality and impact, the citation count can provide a significant understanding of key concepts, important research questions, methodological advancements, and theoretical foundations of existing research that serve as a basis for further exploration.

Table 4. Scholarly impact assessment of the top 20 seminal studies on ISPC

Rank	Researchers	Study Title	TC	TC per Year
1	(Bulgurcu et al., 2010)	"Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness"	1,494	99.6
2	(Herath & Rao, 2009b)	"Protection motivation and deterrence: A framework for security policy compliance in organisations"	1,052	65.7

continued on following page

Table 4. Continued

Rank	Researchers	Study Title	TC	TC per Year
3	(Siponen & Vance, 2010)	"Neutralization: New insights into the problem of employee information systems security policy violations"	887	59.1
4	(Herath & Rao, 2009a)	"Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness"	674	44.9
5	(Ifinedo, 2012)	"Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory"	655	50.4
6	(Vance et al., 2012)	"Motivating IS security compliance: Insights from Habit and Protection Motivation Theory"	602	46.3
7	(Puhakainen & Siponen, 2010)	"Improving employees' compliance through information systems security training: An action research study"	523	37.4
8	(Siponen et al., 2014)	"Employees' adherence to information security policies: An exploratory field study"	428	42.8
9	(D'Arcy, Herath, & Shoss, 2014)	"Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective"	424	42.4
10	(Hu et al., 2012)	"Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture"	419	34.9
11	(Moody et al., 2018)	"Toward a unified model of information security policy compliance"	388	64.6
12	(Soomro, Shah, & Ahmed, 2016)	"Information security management needs more holistic approach: A literature review"	351	43.9
13	(D'Arcy & Herath, 2011)	"A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings"	338	26
14	(Vroom & von Solms, 2004)	"Towards information security behavioural compliance"	329	16.5
15	(Ifinedo, 2014)	"Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition"	322	32.2
16	(Sohrabi Safa, Von Solms, & Furnell, 2016)	"Information security policy compliance model in organizations"	286	35.8
17	(Alec Cram et al., 2019)	"Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance"	251	50.2
18	(Myyry, Siponen, Pahnila, Vartiainen, & Vance, 2009)	"What levels of moral reasoning and values explain adherence to information security rules? An empirical study"	249	16.6
19	(Li et al., 2019)	"Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior"	239	47.8
20	(Chen, Ramamurthy, & Wen, 2012)	"Organizations' information security policy compliance: Stick or carrot approach?"	239	19.9

3.1.3. Most Productive Universities

Knowing which universities are most productive in research is vital for researchers for numerous reasons, including understanding scholarly patterns, seeking collaborations, exploring research funding opportunities, and making educational and career decisions. Previous studies have adapted research output as a quantitative measure for reporting the most productive universities and institutions (Singh et al., 2020; Sharma et al., 2023). Table 5 reports the universities with strong reputations and a strong track record of publishing groundbreaking discoveries related to ISPC. Aspiring researchers in the area of ISPC may note that this study uses bibliometric data to map a network of universities as nodes and co-authorships as links. The frequency and strength of co-authorship links are used to report the most productive universities that foster significant collaborations and become central to ISPC research. The top five universities, namely Chung-Ang University (South Korea), KU Leuven (Belgium), Vrije Universiteit Brussel (Belgium), Örebro University (Sweden), and the University of Luxembourg (Luxembourg), contribute significantly to the field of ISPC research.

Table 5. Top 25 universities identified as major research hubs

Rank	Affiliations	Articles
1	Chung-Ang University	15
2	KU Leuven	14
3	Vrije Universiteit Brussel	14
4	Örebro University	13
5	University of Luxembourg	12
6	University of Alabama	12
7	Mississippi State University	11
8	Oklahoma State University	10
9	Tilburg University	9
10	University of Glasgow	9
11	University of Oulu	9
12	Universiti Teknologi Petronas	9
13	Tilburg Institute for Law, Technology, and Society	8
14	University of South Africa	8
15	Leiden University	8
16	University of Delaware	8
17	University of Memphis	7
18	Virginia Polytechnic Institute and State University	7
19	University of North Texas	7
20	Middle Georgia State University	6

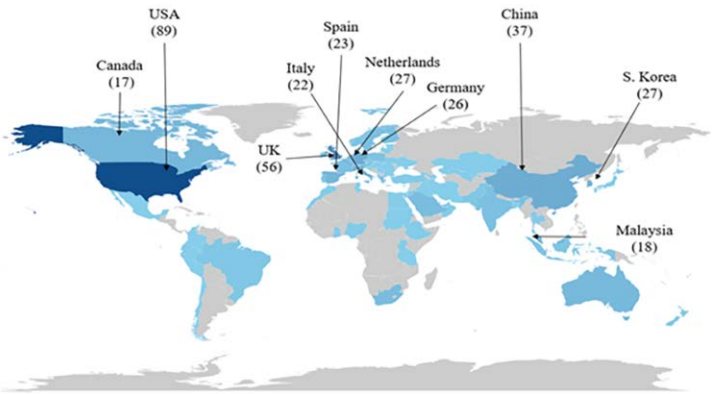
3.1.4. Research Productivity of Nations

Analyzing and reporting research productivity of nations is crucial for recognizing the intellectual potential, global trends, research priorities, and economic standing (Gaurav & Panigrahi, 2022). Table 6 lists the most active countries that have a significant impact on ISPC research. As evident in Figure 3, the top 3 countries are the United States, the United Kingdom, and China based on the corresponding author's region. While the USA alone accounted for approximately 11% of global scholarly output on ISPC, the top 5 countries, including South Korea and the Netherlands, contribute 28.7% of research productivity. The research productivity across countries may be used to benchmark advancements and technological innovations in ISPC. Further, a high number of single-country publications (SCP) and a smaller number of multiple-country publications (MCP) for a country in Table 6 indicate the need for more global collaboration in ISPC research. Moreover, researchers, practitioners, and policymakers may explore and extend these findings in assessing the effectiveness of educational systems, research funding, research collaborations, and scientific progress.

Table 6. Research productivity of nations

Rank	Country	No. of Studies	Articles %	SCP	MCP	MCP Ratio
1	USA	89	10.8	70	19	21.3
2	United Kingdom	56	6.8	47	9	16.1
3	China	37	4.5	26	11	29.7
4	South Korea	27	3.3	21	6	22.2
5	Netherlands	27	3.3	23	4	14.8
6	Germany	26	3.2	21	5	19.2
7	Spain	23	2.8	12	11	47.8
8	Italy	22	2.7	12	10	45.5
9	Malaysia	18	2.2	9	9	50
10	Canada	17	2.1	13	4	25
11	Sweden	17	2.1	14	3	17.6
12	Greece	15	1.8	10	5	33.3
13	India	15	1.8	8	7	46.7
14	South Africa	15	1.8	11	4	26.7
15	Australia	13	1.6	8	5	38.5
16	Belgium	13	1.6	10	3	23.1
17	Portugal	12	1.5	10	2	16.7
18	Saudi Arabia	11	1.3	7	4	36.4
19	Austria	10	1.2	6	4	40
20	Finland	10	1.2	4	6	60

Figure 3. Global representation of top prolific countries



3.2. Results From Topic Modeling

Topic modeling algorithms statistically map frequently co-occurring words within a corpus of documents to distinct topics. Subsequently, each document is represented as a probabilistic distribution of these underlying topics (Sharma et al., 2021). However, STM advances and extends traditional

topic modeling by incorporating document-level metadata in the modeling process so that relevant variables present in the metadata can be used as covariates to estimate their effects on the topic's content and prevalence (Roberts, Stewart, & Airoldi, 2016). The article's publication year is one such metadata-based variable used as a covariate to explore how the latent topics and their formation vary over the years.

Table 7 displays the six latent topics, their representative top words as per frequency, and the Frequency–Exclusivity (FREX) measures. The top terms in a topic, as per frequency, may also appear in other topics, so the FREX score reports those terms that are unique to a topic and do not appear in other topics. Each extracted topic can be labeled and examined further using the top words and representative articles (Sharma et al., 2022). Figure 4 represents the top 40 most frequent words related to each topic as a word cloud, which can be explored further to understand the formation of topics. Further, the relative proportions of each extracted topic are also provided with the topic labels. Topic 5- "GDPR Compliance and Personal Data Protection" (28.5%), Topic 4- "Organizational and Contextual Factors in ISPC" (17.9%), and Topic 2- "Cybersecurity Awareness and Information Security Compliance" (16%) are the most prominent topics, covering more than 60% of total research on ISPC.

Table 7. Topic, proportion, representative terms, and exemplary studies

Topic and Proportion	Most Frequent Terms	FREX Score Terms	Seminal Studies
Topic 1- ISPC in Banking and Digital Payment Systems (9.3%)	Payment Card Industry, Risk, Compliance, Data Security Policy, Privacy, Analysis, Digital Payment System, Best Practice, Payment Card, Data Security Standard	Payment Card Industry, Credit Card, Merchant, Payment System, Data Security Standard, Critical Success Factor, Privacy Policy, Regulatory Compliance, Assessor, Bank	(Aggarwal & Srivastava, 2024; Akanfe, Valecha, & Rao, 2023; Bauer & Bernroider, 2017; Serrado et al., 2020; Tambunan, Legowo, & Tambunan, 2024)
Topic 2- Cybersecurity Awareness and Information Security Compliance (16%)	Cybersecurity Awareness, Compliance, Governance, Healthcare, Organization, Regulatory Compliance, Cyber Threats, Risk, Analysis, Cybersecurity Standards	Firm, Government, Cyber Threats, Governance, Framework, Risk Assessment, Cybersecurity Policy, Safety, Resilience, Cybersecurity Controls	(AlQadheeb, Bhattacharyya, & Perl, 2022; Marotta & Madnick, 2022; Oroni, Xianping, Ndunguru, & Ani, 2025a, 2025b; Yusif & Hafeez-Baig, 2023)
Topic 3- Individual Factors in ISPC (13.9%)	Employee, Compliance, Management, Leadership, Behaviour, Violation, Attitude, Intention, Information Security Policy, Noncompliance	Stress, BYOD, Neutralization, Emotion, Technostress, Security Policy, Coping, Deterrence Theory, Information Security, Competence	(Arif et al., 2025; Choi, 2016; D'Arcy & Lowry, 2019; Hong & Furnell, 2022; Ifinedo, 2012)
Topic 4- Organizational and Contextual Factors in ISPC (17.9%)	Organization, Norms, Culture, Incentives, Deterrence, Sanctions, Organizational Climate, Rewards, Organizational Justice, Security Culture	Punishment, Organizational Commitment, Motivation, Intentions, Organizational Culture, Organizational Justice, Response Efficacy, Cultural Differences, Appraisal, Contextual	(Aebissa, Dhillon, & Meshesha, 2023; Amankwa et al., 2021; Brooks et al., 2024; Nasir et al., 2022; Zhao, Hong, Chen, & Chen, 2024)
Topic 5- GDPR Compliance and Personal Data Protection (28.5%)	Data Protection, General Data Protection Regulations, Personal Data, Privacy, Legal, Regulation, Compliance, Requirement, Enforcement, Consent	Data Subjects, Data Controllers, Surveillance, Informed Consent, Personal Data Processing, Facial Recognition, Data Governance, Data Protection, Cookies, Data Transfer	(Chhetri, Fensel, & DeLong, 2024; S.-C. Li, Chen, & Huang, 2021; Rodriguez, Del Alamo, Fernandez-Aller, & Sadeh, 2024; Tauqeer & Fensel, 2024; Varela-Vaca, Gómez-López, Morales Zamora, & M. Gasca, 2025)
Topic 6- Role of Emerging Technologies - AI and Blockchain (14.4%)	Blockchain, Security, Data, Compliance, Cloud, Software, Service, Data Privacy, Internet of Things, Smart Contracts	Compliance Verification, Edge Computing, Access Control, Regulation Compliance, Blockchain, Cloud, Internet of Things, Verification, Checking, Privacy Requirements	(Ahmad & Aujla, 2023; Ansar, Ahmed, Malik, Helfert, & Kim, 2024; Hristov & Dimitrov, 2019; Truong, Sun, Lee, & Guo, 2020)

Topic 1 – "ISPC in Banking and Digital Payment Systems" represents the extent of research on ensuring and enhancing information security policy compliance in banking, the payment card industry, and digital payment systems such as mobile wallets and remittance services (Akanfe et al., 2023; Ullah et al., 2024; Willey & White, 2013). Safeguarding information and digital assets has become a paramount concern for banks and financial services providers due to intentional and unintentional behavioral incidents that lead to security breaches and organizational vulnerabilities (Aggarwal & Srivastava, 2024; Bauer & Bernroider, 2017). Hence, studies have reported that there is a strong need to address the conceptual inconsistencies and unclarities in measuring compliance (Gerdin et al., 2025) and align security policies and frameworks to specific industries such as banking (Serrado et al., 2020).

Topic 2 – "Cybersecurity Awareness and Information Security Compliance" mainly focuses on the impact of cybersecurity policy awareness on the compliance of information security policy (Oroni et al., 2025a). Previous studies report that understanding and awareness related to cyber threats and adherence to cyber safety measures can lead to shaping a compliance attitude of stakeholders for ISPs (Luidold & Jungbauer, 2024; Wong et al., 2022), which further guarantees privacy protection and maintains trust (Marotta & Madnick, 2022).

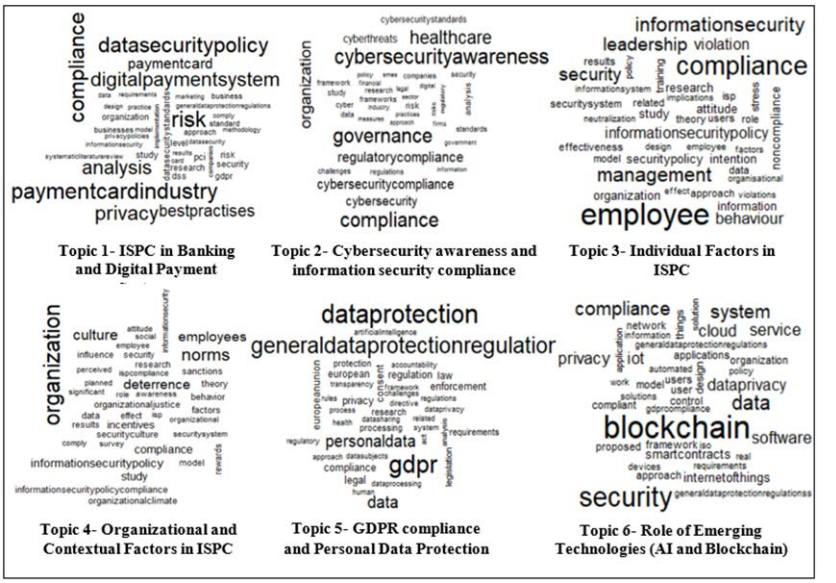
Topic 3 – "Individual Factors in ISPC" deals with human factors related to employees that affect compliance with an organization's ISP (Arif et al., 2025). The extant research on ISPC has reported that employees' attitudes and perceptions related to behavioral control profoundly influence employees' intention to comply with ISPs (Hong & Furnell, 2022). Moreover, research reports that self-efficacy, attitude, response efficacy, and perception of vulnerability also shape ISPC behavior (Ifinedo, 2012). Similarly, individual coping mechanisms and perceptions about security threats also ensure adherence to ISPC (Vance et al., 2012). ISPC behavior is also driven by the rational decision-making abilities of individuals (Moody et al., 2018). Furthermore, other human factors, such as the perception of deterrence (Wang & Xu, 2021) and cognitive, affective, normative, and moral aspects (D'Arcy & Lowry, 2019), also shape employees' security behavior and ensure ISPC.

Topic 4 – "Organizational and Contextual Factors in ISPC" concerns the research on organizational and contextual factors that affect employees' compliance or non-compliance with ISPs (Brooks et al., 2024; Kraushaar & Bohnet-Joschko, 2025). Recent studies report that organizational information security culture plays an important role in shaping security behaviors and fostering employees' compliance with ISPs (Allahawiah et al., 2024; Alrawhani et al., 2025). Moreover, other organizational factors such as psychological capital (Zhao et al., 2024), organizational justice (Aebissa et al., 2023), and organizational justice (Aebissa et al., 2023) are also reported in the literature as significant influencers of ISP compliance attitudes and behavioral intentions of firm employees. Several leadership styles, such as relational leadership (Ajabnoor, 2023), ethical leadership (Wang & Xu, 2021), and paternalistic leadership (Feng et al., 2019) have a positive effect on employees' compliance intentions. On the contrary, abusive leadership may result in deviant behaviors that lead to non-compliance with ISPs (Wang & Xu, 2021).

Topic 5 – "GDPR Compliance and Personal Data Protection" deals with research on protecting personal data, confidential corporate data, privacy regulation, data governance, and general data protection regulation (GDPR) compliance (Chhetri, Fensel, & DeLong, 2024; Li, Chen, & Huang, 2021). The contemporary advancements in the data-driven economy involve the collection, processing, and sharing of personally identifiable information that requires lawful data processing under GDPR compliance (Gao, Sun, & Wang, 2023; Piasecki, 2023; Tauqeer & Fensel, 2024). Compliance with GDPR is challenging for business firms as the relevant contractual obligations require firms to ensure fair and transparent personal data processing (Guamán, Rodriguez, del Alamo, & Such, 2023). Research confirms that a multi-stakeholder perspective can be adopted to achieve an optimal trade-off among the conflicting goals of all the stakeholders related to ensuring data privacy and security (Mollaeefar & Ranise, 2023).

Topic 6 – "Role of Emerging Technologies - AI and Blockchain" primarily involves the scholarly exploration that adopts emerging technologies such as AI (S. M. Ali, Razzaque, Yousaf, & Shan, 2025) and blockchain (Ahmad & Aujla, 2023; Daudén-Esmel, Castellà-Roca, & Viejo, 2024; Y. Zhang et al., 2024). Blockchain-based approaches have gained significant scholarly attention as smart contracts can automate user-centric compliance verification processes (Ahmad & Aujla, 2023; Akanfe, Lawong, & Rao, 2024). Moreover, artificial intelligence (AI) based methods have also started gaining momentum in automating compliance verification (Azeem & Abualhaija, 2024; Eszteri, 2022)

Figure 4. Word cloud from top 40 most frequent words in each topic



3.3. Key Insights From Scientometrics

The quantitative investigation using scientometrics reveals interesting patterns related to scholarly literature's intellectual and conceptual structure (Sharma et al., 2021). In the current study, the structure, evolution, and dynamics of ISPC research are mapped and reported using co-citation analysis, research keywords density visualization, co-occurrence analysis, and the authors' collaboration network analysis.

3.3.1. Co-Citation Clusters

By analyzing how frequently two research documents are cited together, the co-citation mapping uncovers the intellectual structure of the research landscape. (Small, 1973). The co-citation clusters are based on the interconnectedness of research that helps researchers report seminal studies that significantly shape the intellectual core of the domain (Sharma et al., 2023; H. Zhang et al., 2024). Hence, a co-citation cluster has articles that are cited together and are pivotal to the scientific field's intellectual foundations. This study has used VOSviewer (van Eck & Waltman, 2014) to create a network of the top 50 most co-cited articles. Figure 5 shows that these co-cited studies form four distinct clusters based on their semantic similarity. Articles featuring a high number of co-citations are semantically associated and may represent a common theme. A careful analysis of these clusters in Figure 5 may reveal interesting patterns related to how different research themes are interconnected. Cluster 1 (Red color) contains studies related to modeling antecedents to ISPC using different theories. Moreover, Cluster 2 (Green color) is dominated by issues related to organizational factors that lead to

ISPC. Further, Cluster 3 (Blue color) maps issues related to ISPC, such as neutralization, fear appeal, deterrence, and risk. Finally, the yellow cluster (Cluster 4) embodies works related to beliefs, attitudes, and values. Table 8 provides a few landmark studies in all clusters identified using centrality and PageRank measures. It is worth reporting that many of these landmark studies may not be directly related to ISPC, but these studies have a profound impact on the intellectual structure of ISPC.

Figure 5. Co-citation clusters

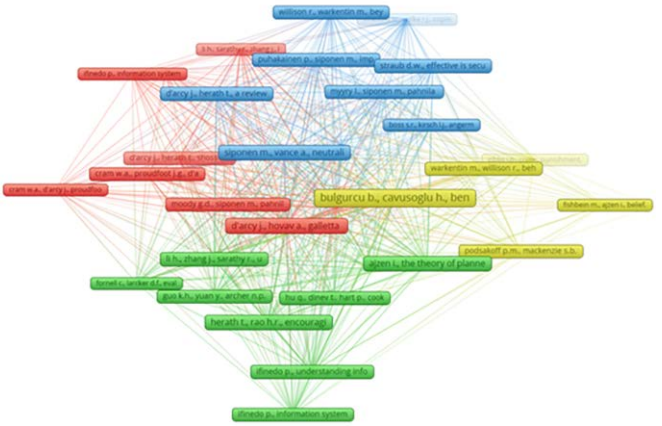


Table 8. Seminal articles in Co-cited clusters

Cluster	Reference	Study Title	Centrality	PageRank
1	(Herath & Rao, 2009b)	"Protection motivation and deterrence: A framework for security policy compliance in organisations"	37.68	0.04
1	(D'Arcy et al., 2014)	"Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective"	30.75	0.04
1	(Cram, Proudfoot, & D'Arcy, 2017)	"Organizational information security policies: A review and research framework"	7.98	0.02
2	(Herath & Rao, 2009a)	"Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness"	156.25	0.05
2	(Ifinedo, 2012)	"Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory"	7.82	0.01
2	(Hu et al., 2012)	"Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture"	3.75	0.01
3	(Siponen & Vance, 2010)	"Neutralization: New insights into the problem of employee information systems security policy violations"	14.28	0.03
3	(Myyry et al., 2009)	"What levels of moral reasoning and values explain adherence to information security rules? An empirical study"	5.72	0.02
3	(Puhakainen & Siponen, 2010)	"Improving employees' compliance through information systems security training: An action research study"	2.98	0.01

continued on following page

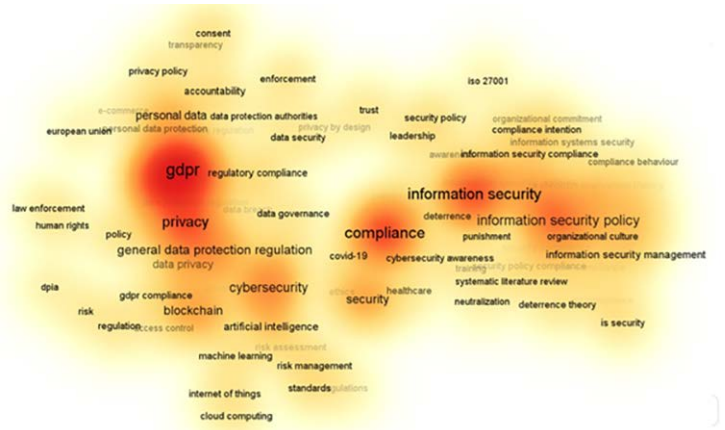
Table 8. Continued

Cluster	Reference	Study Title	Centrality	PageRank
4	(Bulgurcu et al., 2010)	"Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness"	64.57	0.05
4	(Warkentin & Willison, 2009)	"Behavioral and policy issues in information systems security: the insider threat"	7.17	0.03
4	(Gibbs, 1968)	"Crime, Punishment, and Deterrence"	4.02	0.02

3.3.2. Density Visualization and Key Themes

Keywords density analysis facilitates understanding the regularity and prominence of specific keywords within literature related to a particular topic or domain (A. Sharma et al., 2023). The outcome of density analysis is a visualization that provides crucial insights related to research trends and core themes. ISPC research explored in the current study uses a total of 2,280 research keywords, which is a huge number to map the core concepts. Hence, Figure 6 depicts the central themes and concepts that define ISPC research using density visualization. It is clearly evident that research on "GDPR", "Compliance", "Information Security", "Privacy", "Cybersecurity", "Blockchain", and "Organization Culture" has attracted significant scholarly attention. Hence, a more detailed examination may be focused on these themes to have an in-depth insight into the ISPC research landscape. Moreover, the subthemes that are connected to these central themes or are in proximity to the central themes are emerging topics that are gaining attention. There is a strong possibility that these subthemes will emerge as dominant themes in the near future.

Figure 6. Keywords density visualization



3.3.3. Keyword Co-Occurrence Analysis

The research keywords used in the articles are crucial for the categorization of studies and identifying patterns, themes, and gaps in existing research. Keyword co-occurrence analysis facilitates scientific mapping of research keywords into a network of clusters, where relationships between keywords of research literature are determined based on their co-occurrence frequency (Singh et al., 2020). The research terms become the network nodes, and the normalized co-occurrence frequency determines the link that connects the nodes. A clustering algorithm applied to the keyword network

identifies clusters of keywords. These clusters represent thematic areas or research hotspots (Sharma et al., 2023). The research hotspots specify avenues of high research activity and provide a broader understanding of the conceptual structure of the research field. Figure 7 shows the main themes and subthemes that dominate the ISPC research. Due to a huge number of research keywords (n=2280), this study has used a threshold frequency of 5 to limit the keywords in the visualization for revealing only the central themes and their subthemes. A total of 90 most frequent keywords are clustered into four major themes. The clusters can be explored further to understand how different keywords are associated with each other, enabling conceptual interaction between different research areas.

Moreover, Table 9 details each cluster, its content, and average citations that indicate the scholarly impact of research represented by a cluster. The keywords and the related studies can be explored further for a more profound and comprehensive understanding of the literature. Table 9 confirms that keywords within a cluster are semantically associated and share a single topical focus. The cluster label is derived from the cluster's content in a data-driven way that may further facilitate gaining more insights into the central focus theme and organization of a cluster. For example, Cluster 1 (red color) is labeled as "ISPC and Organizational Factors," and the related studies of this cluster are well cited by other research works.

Figure 7. Keywords co-occurrence network

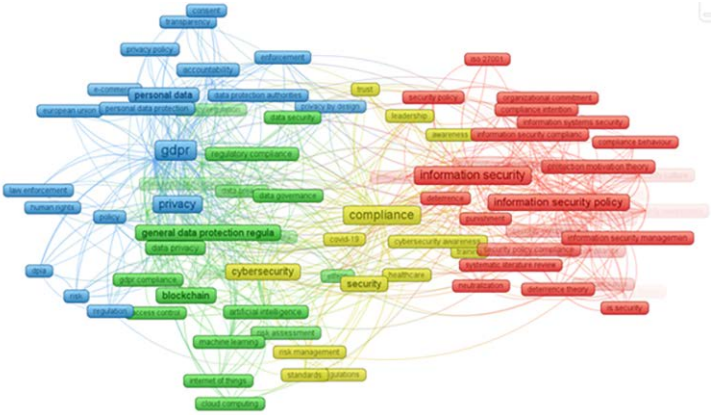


Table 9. Description of clusters from keywords co-occurrence analysis

S. No.	Cluster Color	Title	Most Frequent Research Keywords	Average Citation
1	Red	ISPC and Organizational Factors	Information Security (92), Information Security Policy (60), Information Security Policy Compliance (31), Theory of Planned Behavior (17), Information Security Management (15), Information Security Policies (15), Protection Motivation Theory (15), Information Security Awareness (13), Information Security Culture (12), Organizational Culture (11)	83.35
2	Green	Compliance and Emerging Technologies	Data Protection (42), Blockchain (34), Data Privacy (20), Artificial Intelligence (17), Regulatory Compliance (13), Big Data (10), Data Security (9), Cloud Computing (9), Machine Learning (9), Data Governance (8)	23.8

continued on following page

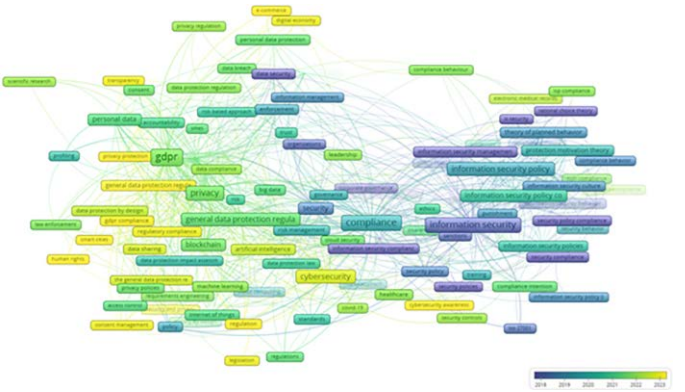
Table 9. Continued

S. No.	Cluster Color	Title	Most Frequent Research Keywords	Average Citation
3	Blue	GDPR Compliance	GDPR (144), Data Protection (107), Privacy (81), Personal Data (26), Accountability (12), Consent (10), Enforcement (10), Personal Data Protection (10), Policy (10), Regulation (9)	12.98
4	Yellow	Cybersecurity Compliance	Compliance (105), Cybersecurity (54), Security (35), Risk Management (9), Trust (9), Healthcare (8), Leadership (8), Standards (8), Cybersecurity Awareness (7), Awareness (7)	19.87

3.3.4. Keywords Overlay Visualization

Keywords overlay visualization complements keywords co-occurrence analysis by illustrating the yearly trends related to emerging themes. By exploring the evolving co-occurrence trends over the past years, overlay visualization can report emerging research patterns and themes attracting scholarly focus. Hence, while keywords co-occurrence analysis reports the current state of research, being a retrospective analysis method, keywords overlay visualization provides a prospective view of the research landscape by identifying potential areas for future exploration (van Eck & Waltman, 2014). Figure 8 shows that cybersecurity awareness, transparency, privacy protection, regulatory compliance, regulation, and AI have been the most active themes in the last two years. A careful inspection of the overlay visualization confirms the significance of cybersecurity awareness in ISPC, as researchers confirm that the knowledge about the consequences of cyber-attacks, security breaches, and human errors facilitates the understanding of the scope and the purpose of ISP and reduces the risks related to non-compliance (Oroni et al., 2025b).

Figure 8. Keywords overlay network



3.3.5. Author Collaboration Analysis

Scientific collaborations are crucial for advancing research as they group researchers with diverse skills, knowledge, and perspectives. Author collaboration analysis reveals interesting patterns related to scientific collaborations in research. Author collaboration analysis results in a network where nodes represent researchers, connecting edges represent co-authorship connections, and the link strength represents the frequency of co-authorship. Figure 9 illustrates the co-authorship networks of key researchers of ISPC who have collaborated on a minimum of three studies. This threshold measure is defined using prior research (Sharma et al., 2023), which has enabled the identification of 75 authors

from the pool of a total of 2,040 authors. However, after removing the isolated authors, the final network of connected authors is inspected to identify groups of authors who are highly interconnected.

Table 10 reports key researchers, influential affiliations, and patterns of co-authorship. The first cluster (red color) is anchored by Prof. John D'Arcy from the University of Delaware. Similarly, the second cluster (green color) is headed by Prof. Paul Benjamin Lowry from the Virginia Polytechnic Institute and State University, USA. The third cluster (blue color) is formed by Prof. Siponen, Mikko, from the University of Alabama, USA. Finally, cluster 4 (yellow color) is formed by Prof. Dominic from Universiti Teknologi Petronas, Malaysia, and cluster 5 (purple color) is formed by Prof. Alex Koohang from Middle Georgia State University, USA. Figure 10 depicts the collaboration among countries that can provide significant insights related to research funding decisions, policies, and priorities for fostering scientific growth in ISPC research. By identifying key collaborators and collaborative hubs, researchers can understand how cooperation among authors and universities fosters combining diverse perspectives, intellectual capital, and resources for advancing knowledge and encouraging scientific progress.

Figure 9. Co-authorship network

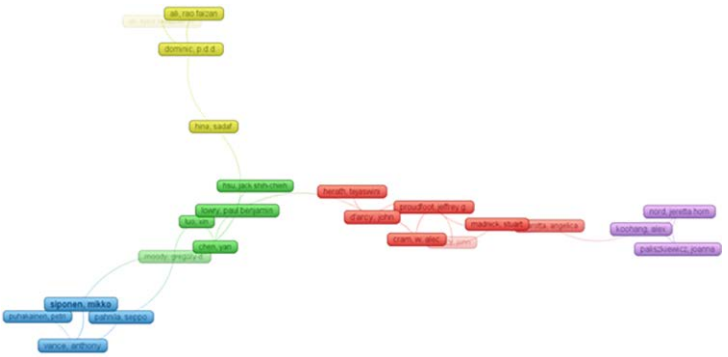


Table 10. Prolific authors anchoring collaboration

Cluster	Lead Scholar	Primary Association	Links	Link Strength	No. Of Documents	Citations
1	D'Arcy, John	University of Delaware, USA	4	8	7	1220
2	Lowry, Paul Benjamin	Virginia Polytechnic Institute and State University, USA	6	7	5	718
3	Siponen, Mikko	University of Alabama, USA	4	14	11	3359
4	Dominic, P.D.D.	Universiti Teknologi PETRONAS, Malaysia	3	7	5	141
5	Koohang, Alex.	Middle Georgia State University, USA	3	9	5	112

Figure 10. World collaboration network

4. DISCUSSION

Employee compliance or violation of the ISP has become strategically important for global business organisations. Hence, researchers, practitioners, and policymakers have confirmed that understanding compliance and violations of ISPs may help in formulating and implementing robust security programs for maintaining data integrity, preventing security breaches, and promoting a culture of information security awareness (Hong & Furnell, 2022; Ifinedo, 2012; Koohang et al., 2021; Vance et al., 2012). The multitude of variations in cyber laws and data protection standards across different countries complicates global information management. ISPC plays a crucial role in global information management by safeguarding sensitive information, ensuring adherence to global standards, maintaining the trust of global customers, and establishing consistent practices for global operations. Multinational enterprises usually operate across multiple countries in a global digital environment where global information management involves data sharing across subsidiaries, suppliers, government regulators, and customers. ISPC ensures that cross-border data flows are handled securely while creating a global security culture that reflects proactive risk management, accountability, and assurance. However, the current body of literature on ISPC is vast and fragmented, which makes it challenging to identify, access, and critically evaluate the scientific progress. This study found that ISPC research has grown significantly in the last two decades, with approximately 17% annual growth. The year 2024 reports more than 160 articles published on ISPC. Therefore, this structured review comprehensively examines the key concepts and intellectual landscape of the overall body of knowledge.

The first research question (RQ1) uncovers the knowledge frontier of ISPC. This study maps research productivity to identify influential researchers as thought leaders of ISPC research. Prof. Mikko Siponen at the University of Alabama is the top scholar of ISPC, contributing significantly to the field. Knowing the most productive scholars (Table 3) helps early-career researchers in searching for mentors and fostering impactful collaborations. This study discovers that authors from the USA lead the cutting-edge research on ISPC due to the strong research environment and favorable policies for research.

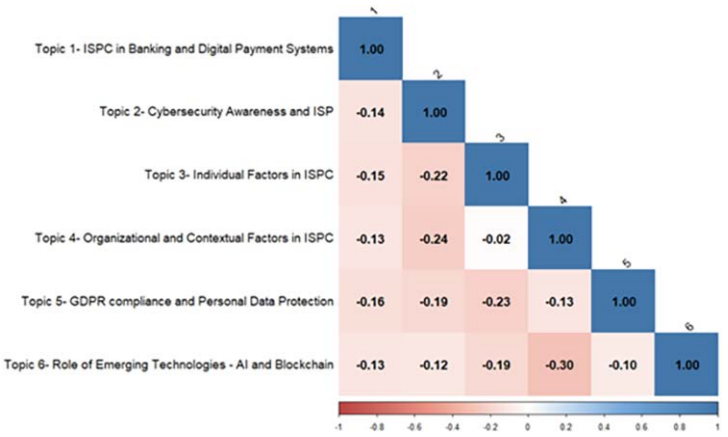
Further, the most impactful articles of ISPC literature form the foundational research that helps scholars to comprehend the key breakthroughs that shape the ISPC field. The potential scholars may refer to Table 4 to stay updated on the foundational discoveries and key breakthroughs of ISPC research. In terms of total citations as a proxy of research impact, the study by Bulgurcu et al. (2010) gained the highest number of citations. The scholars from Chung-Ang University (South Korea) contributed the maximum number of articles related to ISPC. However, the USA leads with 89 articles

published on ISPC. Hence, mapping the most productive universities and countries (Tables 5 and 6) facilitates researchers in assessing strong academic ecosystems. Moreover, this knowledge helps policymakers in strategic decision-making related to designing funding programs that boost innovation and high-impact collaborations.

4.1. Key Topics and Scholarly Trends

The second research question (RQ2) systematically maps the key research topics of ISPC research and their topical trends. The current study uses STM to examine and explore the key topics from the ISPC literature. STM advances and outperforms classical topic modeling approaches such as Latent Dirichlet Allocation (LDA) by leveraging both text content and document-level metadata in the model estimation. The document-level metadata used as a covariate improves topic assignment and enhances topic interpretability (Sharma et al., 2021). Thus, it is possible to explore how a document metadata-based external variable may affect the content of topics and their prevalence. The topical trends over the years are derived by using the year of publication as a covariate in the topic model. Moreover, STM provides a more realistic representation of topics because traditional topic models, such as LDA, assume that topics are semantically independent and there is no correlation among topics. However, the correlation plot for ISPC topics represented in Figure 11 shows that all six topics share a negative correlation with less than 0.4, which indicates that these topics usually do not co-occur in the same document.

Figure 11. Correlation analysis for the extracted topics

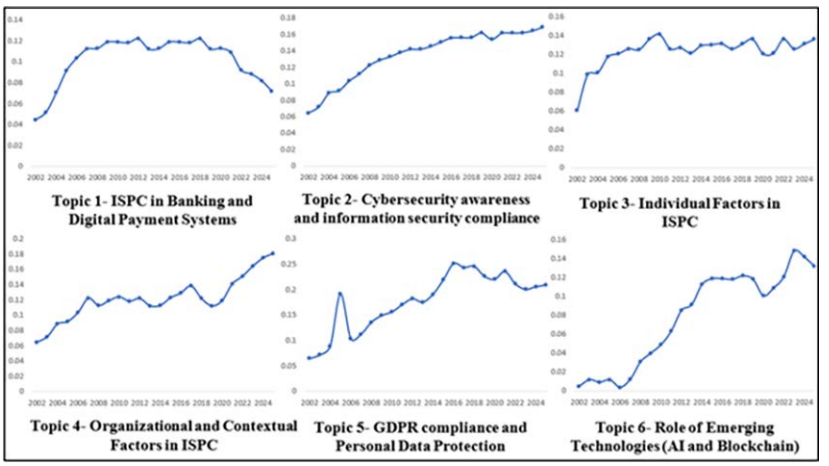


Furthermore, STM allows for assessing the impact of a metadata-based independent variable, such as publication year, on the prevalence of topics. Hence, it is possible to explore in case certain topics become more or less prevalent over time. Figure 12 provides an estimate of topic prevalence over time for ISPC research during 2002-2024. Topic 1 (ISPC in Banking and Digital Payment Systems) shows growth in the initial years but registers a decline in scholarly interest over the years after 2018. A similar trend is evident for Topic 5 (GDPR Compliance and Personal Data Protection), which attracted a significant research focus from the initial years till 2016 and then had a declining trend subsequently. Further, Topic 3 (Individual Factors in ISPC) shows a rising trend in the early years, but the trend becomes almost flat subsequently, which confirms a possible saturation in the scholarly interest in this area. On the contrary, Topic 2 (Cybersecurity Awareness and Information Security Compliance), Topic 4 (Organizational and Contextual Factors in ISPC), and Topic 6 (Role of Emerging Technologies - AI and Blockchain) show a rising trend, confirming that the research on these topics

may evolve more in the years to come (Quan et al., 2024; Sun et al., 2023). Previous research has confirmed that topics with rising trends have enough scope for future exploration, and potential scholars may leverage these growing research interests to advance the knowledge (Das et al., 2023; Sharma et al., 2022).

The rising trend related to the research on cybersecurity awareness is explainable as cybersecurity awareness empowers individuals and organizations to understand the main causes of data breaches, minimize human errors, protect key information assets, and ensure compliance with regulations to reduce security incidents and the related costs (Oroni et al., 2025a). Likewise, the current ISPC research related to emerging technologies like AI, Machine Learning, Blockchain, IoT, and Cloud Computing, etc. has reported the promising implications of these technologies in enhancing security incidents detection, compliance automation, access control, and building a culture of information security in organisations (Ahmad & Aujla, 2023; Akanfe, Lawong, & Rao, 2024; Duvivier & Gupta, 2023). AI models can continuously verify data tampering and content authenticity using blockchain. Moreover, machine learning based predictive systems may predict vulnerable systems for real-time risk management. Similarly, AI-driven intrusion detection and anomaly discovery systems can strengthen enforcement of ISPs. The role of emerging technologies in ISPC is still under development, but evolving rapidly, and it is believed that technologies like AI and Blockchain have the potential to significantly impact ISPC research in the coming years (Ahmad & Aujla, 2023; Daudén-Esmel, Castellà-Roca, & Viejo, 2024). However, the adoption of blockchain is hindered by various barriers that need to be carefully addressed (Chavali et al., 2024; Chen et al., 2023).

Figure 12. Trends related to topic prevalence



4.2. Key Insights From Scientometric Analysis

The third research question (RQ3) deals with the intellectual and conceptual evolution of ISPC research. The present study performs a scientometric analysis that quantitatively examines the citations, keywords, and authorship networks. The co-citation analysis reveals four clusters that are formed using co-cited articles. The co-citation analysis maps the evolution of scientific knowledge and helps in identifying the landmark articles that are core to the intellectual structure of ISPC research. For example, Cluster 1 identifies Herath & Rao (2009b), D'Arcy et al. (2014), and Cram et al. (2017) as a few landmark articles that are significant to follow for a deeper understanding of the evolution of ISPC research. Hence, by examining co-citation patterns, the resulting clusters, and the landmark articles, future researchers can spot implicit relationships between research and track down the foundational works that have significantly impacted the intellectual landscape of ISPC research.

Further, this study provides a comprehensive keywords analysis using density visualization, co-occurrence analysis, and overlay visualization. The density visualization helps in modeling the key themes and subthemes from the overall ISPC research. The results reveal that "Privacy", "Cybersecurity", "Blockchain", and "Organization Culture" are important themes that have gained significant attention from scholars. It is worth reporting that the themes from density visualization complement the topic modeling results, and many common themes are clearly evident. Further, the keyword co-occurrence analysis clusters the research keywords into four conceptually distinct clusters, which are labeled "ISPC and Organizational Factors", "Compliance and Emerging Technologies", "GDPR Compliance", and "Cybersecurity Compliance". Such a type of key concept mapping empowers future researchers to identify core themes and reveal relationships among them. Finally, the overlay visualization presented in this study reports that cybersecurity awareness, transparency, privacy protection, regulatory compliance, and AI have emerged in the last two years and can potentially shape the direction of future research. Thus, this study offers researchers an easy-to-follow roadmap for tracking conceptual evolution, identifying emerging themes, and predicting potential unexplored areas for future research.

Furthermore, the author collaboration analysis offers remarkable value to future researchers by uncovering collaboration patterns, categorizing communities of like-minded scholars, and identifying potential collaborators. The network structure of author collaboration reveals that there is a significant number of ISPC scholars who work in isolation and do not form research communities for the dissemination of knowledge and ideas. However, it is noteworthy to report influential individuals and their research groups (for example, Prof. John D'Arcy from the University of Delaware, USA, Prof. Siponen, Mikko, from the University of Alabama, USA, and Prof. Alex Koohang from Middle Georgia State University, USA, to name a few) who promote collaboration to provide diverse perspectives and facilitate knowledge transfer to encourage more comprehensive, innovative, and impactful research.

4.3. Implications for Research

Cyber threats are evolving, and the sophistication of security attacks in the contemporary world has made the role of ISPC more critical than ever. Ensuring ISPC has become an overriding strategic mandate in business organizations for detecting, preventing, and responding to security breaches and unauthorized access. Moreover, in light of stricter data protection regulations, non-compliance may lead to business disruptions, loss of revenue, legal repercussions, loss of customer trust, and reputational damage. Hence, understanding the role of ISP and examining the current body of literature on ISPC is significant and critical for both researchers and practitioners. The community of ISPC scholars needs a unified view of the scattered knowledge, and this review integrates the conceptual and intellectual structure of existing research. The results are crucial for future explorations where potential scholars may comprehend the current state of knowledge, identify landmark studies, discover key research themes and subthemes, recognize influential authors, and locate emerging topics to avoid redundant research. The data-driven approach used in the current work avoids the subjective bias of traditional narrative reviews (Sharma et al., 2021). Moreover, this study highlights areas of future research that are likely to receive more scholarly attention and help policymakers in making informed decisions about research collaborations and funding decisions. Hence, this study significantly contributes to the advancement of ISPC knowledge.

4.4. Limitations and Future Research

Retrospective overviews of the literature are valuable for summarizing, integrating, and interpreting the scattered knowledge. However, there are some usual limitations that can affect the comprehensiveness and practical implications of the systematic review. The current study reviews only peer-reviewed articles on ISPC published in journals. Hence, future researchers may explore conference proceedings and other literature, such as trade journals. Moreover, the current study finds that research on ISPC is dynamic and evolving continuously. In light of this, the themes and topics

discovered in this study may change in the future. Therefore, this study proposes that future researchers may replicate the current methods to cover the latest research and provide a comprehensive overview of topical innovations.

5. CONCLUSION

ISPC has become strategically important for protecting organizations and users from security threats, data breaches, and related negative consequences. The research on ISPC has grown significantly because business organizations have realized that well-defined ISPs and user compliance with ISPs are critical for business continuity. However, the increasing importance of ISPC has motivated scholars to explore diverse perspectives, methods, theories, and contexts, resulting in conceptual inconsistencies and fragmentation in the body of knowledge. Hence, a comprehensive retrospection is required to summarize the knowledge and present a unified view. This structured literature review aims to unify the scattered knowledge on ISPC. A total of 822 research articles are reviewed by adopting a combined methodology leveraging scientometric analysis and topic modeling based on STM. This study scientifically maps the most impactful articles, influential authors, research ecosystems, key research areas, topics, and the intellectual landscape of ISPC research. Finally, this study highlights emerging trends and research areas to guide future research directions.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

FUNDING STATEMENT

No funding was received for this work.

PROCESS DATES

Received: June 24, 2025, Revision: September 5, 2025, Accepted: September 6, 2025

CORRESPONDING AUTHOR

Correspondence should be addressed to Anuj Sharma; f09anujs@iimidr.ac.in

REFERENCES

Aebissa, B., Dhillon, G., & Meshesha, M. (2023). The direct and indirect effect of organizational justice on employee intention to comply with information security policy: The case of Ethiopian banks. *Computers & Security*, *130*. Advance online publication. DOI: 10.1016/j.cose.2023.103248

Aggarwal, A., & Dhurkari, R. K. (2023). Association between stress and information security policy non-compliance behavior: A meta-analysis. *Computers & Security*, *124*. Advance online publication. DOI: 10.1016/j.cose.2022.102991

Aggarwal, A., & Srivastava, S. K. (2024). Synthesizing Information Security Policy Compliance And Non-compliance: A Comprehensive Study And Unified Framework. *Journal of Organizational Computing and Electronic Commerce*, *34*(4), 338–369. DOI: 10.1080/10919392.2024.2381303

Ahmad, H., & Aujla, G. S. (2023). GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment. *Computers & Electrical Engineering*, *109*. Advance online publication. DOI: 10.1016/j.compeleceng.2023.108747

Ajabnoor, N. (2023). A Neutrosophic Model for Identifying and Analyzing the Effect of Relational Leadership on Information Security Policy Compliance: A Case Study of the Hotel Industry. *International Journal of Neutrosophic Science, 21*(2), 204–215. Advance online publication. DOI: 10.54216/IJNS.210217

Akanfe, O., Lawong, D., & Rao, H. R. (2024). Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, *76*. Advance online publication. DOI: 10.1016/j.ijinfomgt.2024.102753

Akanfe, O., Valecha, R., & Rao, H. R. (2023). Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services. *IEEE Transactions on Engineering Management*, *70*(3), 864–876. DOI: 10.1109/TEM.2020.3015222

Alassaf, M., & Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 162687–162705. DOI: 10.1109/ACCESS.2021.3132574

Alec Cram, W., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly: Management Information Systems*, *43*(2), 525–554. DOI: 10.25300/MISQ/2019/15117

Ali, R. F., Dominic, P. D. D., & Ali, K. (2020). Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees. *Sustainability (Switzerland)*, *12*(20), 1–27. DOI: 10.3390/su12208576

Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences (Switzerland)*, *11*(8). Advance online publication. DOI: 10.3390/app11083383

Ali, S. M., Razzaque, A., Yousaf, M., & Shan, R. U. (2025). An Automated Compliance Framework for Critical Infrastructure Security Through Artificial Intelligence. *IEEE Access : Practical Innovations, Open Solutions*, *13*, 4436–4459. DOI: 10.1109/ACCESS.2024.3524496

Allahawiah, S., Altarawneh, H., & Al-Hajaya, M. (2024). The Role of Organizational Culture in Cybersecurity Readiness: An Empirical Study of the Jordanian Ministry of Justice. *Calitatea*, *25*(202), 74–84. DOI: 10.47750/QAS/25.202.08

Almuqrin, A. (2024). How About Enhancing Organizational Security: Critical Success Factors in Information Security Management Performance. *Journal of Global Information Management*, *32*(1), 1–18. DOI: 10.4018/JGIM.358745

AlQadheeb, A., Bhattacharyya, S., & Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior. *Array (New York, N.Y.)*, *14*. Advance online publication. DOI: 10.1016/j.array.2022.100146

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*. Advance online publication. DOI: 10.1016/j.cose.2023.103208

Alrawhani, E. M., Romli, A. B., Al-Sharafi, M. A., & Alkawsi, G. (2025). Integrating Information Security Culture and Protection Motivation to Enhance Compliance with Information Security Policies in Banking: Evidence from PLS-SEM and fsQCA, 1-22. *International Journal of Human-Computer Interaction*. Advance online publication. DOI: 10.1080/10447318.2025.2464900

Amankwa, E., Loock, M., & Kritzinger, E. (2021). Information security policy compliance culture: Examining the effects of accountability measures. *International Journal of Technology and Human Interaction*, *17*(4), 75–91. DOI: 10.4018/IJTHI.2021100105

Ansar, K., Ahmed, M., Malik, S. U. R., Helfert, M., & Kim, J. (2024). Blockchain based general data protection regulation compliant data breach detection system. *PeerJ. Computer Science*, *10*. Advance online publication. DOI: 10.7717/peerj-cs.1882

Arif, M., Badila, M., Warden, J. M., & Ur Rehman, A. (2025). A study of human factors toward compliance with organization's information security policy. *Information Security Journal: A Global Perspective, 34*(3), 235-250. DOI: 10.1080/19393555.2025.2457702

Azeem, M. I., & Abualhaija, S. (2024). A Multi-solution Study on GDPR AI-enabled Completeness Checking of DPAs. *Empirical Software Engineering*, *29*(4). Advance online publication. DOI: 10.1007/s10664-024-10491-3

Baker, H. K., Kumar, S., Goyal, K., & Sharma, A. (2021). International review of financial analysis: A retrospective evaluation between 1992 and 2020. *International Review of Financial Analysis*, *78*, 101946. DOI: 10.1016/j.irfa.2021.101946

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *The Data Base for Advances in Information Systems*, *48*(3), 44–68. DOI: 10.1145/3130515.3130519

Bolek, V., Romanová, A., & Korček, F. (2023). The Information Security Management Systems in E-Business. *Journal of Global Information Management*, *31*(1), 1–29. DOI: 10.4018/JGIM.316833

Brooks, R. R., Williams, K. J., & Lee, S.-Y. (2024). Personal and Contextual Predictors of Information Security Policy Compliance: Evidence from a Low-Fidelity Simulation. *Journal of Business and Psychology*, *39*(3), 657–677. DOI: 10.1007/s10869-023-09878-8

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems*, *34*(3), 523–548. DOI: 10.2307/25750690

Chavali, K., V, A. K. V., Mavuri, S., Tiwari, C. K., & Pal, A. (2024). Investigation and Modelling of Barriers in Adoption of Blockchain Technology for Accounting and Finance: An ISM Approach. *Journal of Global Information Management*, *32*(1), 1–23. DOI: 10.4018/JGIM.353960

Chen, F. H., Hu, K. H., Lin, S.-J., & Hsu, M. F. (2023). A Decision Framework for Assessing and Improving the Barriers of Blockchain Technology Adoption. *Journal of Global Information Management*, *31*(7), 1–34. DOI: 10.4018/JGIM.330134

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157–188. DOI: 10.2753/MIS0742-1222290305

Chhetri, T. R., Fensel, A., & DeLong, R. J. (2024). GDPR consent management and automated compliance verification tool. *SoftwareX*, *27*. Advance online publication. DOI: 10.1016/j.softx.2024.101821

Choi, M. (2016). Leadership of information security manager on the effectiveness of information systems security for secure sustainable computing. *Sustainability (United States)*, *8*(7). Advance online publication. DOI: 10.3390/su8070638

Choi, M., & Song, J. (2018). Social control through deterrence on the compliance with information security policy. *Soft Computing*, *22*(20), 6765–6772. DOI: 10.1007/s00500-018-3354-z

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, *26*(6), 605–641. DOI: 10.1057/s41303-017-0059-9

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. DOI: 10.1057/ejis.2011.23

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. DOI: 10.2753/MIS0742-1222310210

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*, *20*(1), 79–98. DOI: 10.1287/isre.1070.0160

D'Arcy, J., & Lowry, P. B. (2019). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, *29*(1), 43–69. DOI: 10.1111/isj.12173

D'Arcy, J., & Teh, P. L. (2019). Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization. *Information & Management*, *56*(7). Advance online publication. DOI: 10.1016/j.im.2019.02.006

Das, K., Patel, J. D., Sharma, A., & Shukla, Y. (2023). Creativity in marketing: Examining the intellectual structure using scientometric analysis and topic modeling. *Journal of Business Research*, *154*, 113384. DOI: 10.1016/j.jbusres.2022.113384

Daudén-Esmel, C., Castellà-Roca, J., & Viejo, A. (2024). Blockchain-based access control system for efficient and GDPR-compliant personal data management. *Computer Communications*, *214*, 67–87. DOI: 10.1016/j.comcom.2023.11.017

Duvivier, F., & Gupta, G. (2023). Unleashing Digital Agility: A Review of Literature on Agile Responses to Digital Challenges. *Journal of Global Information Management*, *31*(8), 1–22. DOI: 10.4018/JGIM.331092

Eszteri, D. (2022). Blockchain and artificial intelligence: Connecting two distinct technologies to comply with gdpr's data protection by design principle. *Masaryk University Journal of Law and Technology*, *16*(1), 59–87. DOI: 10.5817/MUJLT2022-1-3

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences it security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems*, *20*(11), 1650–1691. DOI: 10.17705/1jais.00581

Ferraiolo, D. F., Barkley, J. F., & Kuhn, D. R. (1999). A role-based access control model and reference implementation within a corporate intranet. *ACM Transactions on Information and System Security*, *2*(1), 34–64.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security*, *61*, 169–183. DOI: 10.1016/j.cose.2016.06.002

Ganye, D., & Smith, K. (2025). Examining the effects of cognitive load on information systems security policy compliance. *Internet Research*, *35*(1), 380–418. DOI: 10.1108/INTR-04-2023-0329

Gao, B., Sun, J., & Wang, B. (2023). Personal Information Protection in Government Data Openness Using Decision Tree Model. *Journal of Global Information Management*, *31*(9), 1–23. DOI: 10.4018/JGIM.332815

Gaurav, A., & Panigrahi, P. K. (2022). Analysis of Security Paradigms for Resource and Infrastructure Management in Global Organizations. *Journal of Global Information Management*, *31*(2), 1–11. DOI: 10.4018/jgim.320528

Gerdin, M., Grönlund, Å., & Kolkowska, E. (2025). Conceptual inconsistencies in variable definitions and measurement items within ISP non-/compliance research: A systematic literature review. *Computers & Security*, *152*. Advance online publication. DOI: 10.1016/j.cose.2025.104365

Gibbs, J. P. (1968). Crime, Punishment, and Deterrence. *The Southwestern Social Science Quarterly*, *48*(4), 515–530.

Guamán, D. S., Rodriguez, D., del Alamo, J. M., & Such, J. (2023). Automated GDPR compliance assessment for cross-border personal data transfers in android applications. *Computers & Security*, *130*. Advance online publication. DOI: 10.1016/j.cose.2023.103262

Guan, B., & Hsu, C. (2020). The role of abusive supervision and organizational commitment on employees' information security policy noncompliance intention. *Internet Research*, *30*(5), 1383–1405. DOI: 10.1108/INTR-06-2019-0260

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals the importance of user rationale. *Information Management & Computer Security*, *21*(4), 266–287. DOI: 10.1108/IMCS-08-2012-0043

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. DOI: 10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. DOI: 10.1057/ejis.2009.6

Höne, K., & Eloff, J. H. P. (2002). Information security policy—What do international information security standards say? *Computers & Security*, *21*(5), 402–409. DOI: 10.1016/S0167-4048(02)00504-7

Hong, Y., & Furnell, S. (2022). Motivating Information Security Policy Compliance: Insights from Perceived Organizational Formalization. *Journal of Computer Information Systems*, *62*(1), 19–28. DOI: 10.1080/08874417.2019.1683781

Hristov, P., & Dimitrov, W. (2019). The blockchain as a backbone of GDPR compliant frameworks. *Calitatea*, *20*(S1), 305.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. DOI: 10.1111/j.1540-5915.2012.00361.x

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. DOI: 10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. DOI: 10.1016/j.im.2013.10.001

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, *56*(5), 681–695. DOI: 10.1016/j.im.2018.11.003

Kim, H. L., Choi, H. B. S., & Han, J. (2019). Leader power and employees' information security policy compliance. *Security Journal*, *32*(4), 391–409. DOI: 10.1057/s41284-019-00168-8

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. DOI: 10.1108/IMDS-07-2019-0412

Koohang, A., Nord, J. H., Sandoval, Z. V., & Paliszkiewicz, J. (2021). Reliability, Validity, and Strength of a Unified Model for Information Security Policy Compliance. *Journal of Computer Information Systems*, *61*(2), 99–107. DOI: 10.1080/08874417.2020.1779151

Koohang, A., Nowak, A., Paliszkiewicz, J., & Nord, J. H. (2020). Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. *Journal of Computer Information Systems*, *60*(1), 1–8. DOI: 10.1080/08874417.2019.1668738

Kraushaar, J., & Bohnet-Joschko, S. (2025). The Role of the Organization in Promoting Information Security-Related Behavior Among Resident Physicians in Hospitals in Germany: Cross-Sectional Questionnaire Study. *Journal of Medical Internet Research*, *27*. Advance online publication. DOI: 10.2196/46257

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. DOI: 10.1016/j.ijinfomgt.2018.10.017

Li, S.-C., Chen, Y. W., & Huang, Y. (2021). Examining compliance with personal data protection regulations in interorganizational data analysis. *Sustainability (Switzerland)*, *13*(20). Advance online publication. DOI: 10.3390/su132011459

Lim, W. M., Kumar, S., & Donthu, N. (2024). How to combine and clean bibliometric data and use bibliometric tools synergistically: Guidelines using metaverse research. *Journal of Business Research*, *182*, 114760.

Luidold, C., & Jungbauer, C. (2024). Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. *Frontiers in Medicine*, *11*. Advance online publication. DOI: 10.3389/fmed.2024.1379852

Marotta, A., & Madnick, S. (2022). Cybersecurity as a unifying factor for privacy, compliance and trust: The Haga Hospital case. *Issues in Information Systems*, *23*(1), 102–116. DOI: 10.48009/1_iis_2022_108

Mollaeefar, M., & Ranise, S. (2023). Identifying and quantifying trade-offs in multi-stakeholder risk evaluation with applications to the data protection impact assessment of the GDPR. *Computers & Security*, *129*, 103206. DOI: 10.1016/j.cose.2023.103206

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly: Management Information Systems*, *42*(1), 285–311. DOI: 10.25300/MISQ/2018/13853

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. *Communications of the Association for Information Systems*, *42*(1), 147–182. DOI: 10.17705/1CAIS.04207

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, *18*(2), 126–139. DOI: 10.1057/ejis.2009.10

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2022). Information Security Culture Concept towards Information Security Compliance: A Comparison between IT and Non-IT Professionals. *International Journal of Integrated Engineering*, *14*(3), 157–165. DOI: 10.30880/ijie.2022.14.03.017

Nunkoo, R., Sharma, A., So, K. K. F., Hu, H., & Alrasheedi, A. F. (2025). Two decades of research on customer satisfaction: Future research agenda and questions. *International Journal of Contemporary Hospitality Management*, *37*(5), 1465–1496. DOI: 10.1108/IJCHM-03-2024-0436

Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025a). Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students. *Education and Information Technologies*, ●●●, 1–40. DOI: 10.1007/s10639-025-13366-2

Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025b). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. *Computers & Security*, *150*. Advance online publication. DOI: 10.1016/j.cose.2024.104276

Paliszkiewicz, J. (2019). Information Security Policy Compliance: Leadership and Trust. *Journal of Computer Information Systems*, *59*(3), 211–217. DOI: 10.1080/08874417.2019.1571459

Piasecki, S. (2023). Expert perspectives on GDPR compliance in the context of smart homes and vulnerable persons. *Information & Communications Technology Law*, *32*(3), 385–417. DOI: 10.1080/13600834.2023.2231326

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly: Management Information Systems*, *34*(4), 757–778. DOI: 10.2307/25750704

Quan, C., Yuan, Y. H., Wang, G., & Wu, H. T. (2024). Optimization of Enterprise Financial Risk Management and Crisis Early Warning System Supported by AI. *Journal of Global Information Management*, *32*(1), 1–21. DOI: 10.4018/JGIM.356490

Roberts, M. E., Stewart, B. M., & Airoldi, E. M. (2016). A Model of Text for Experimentation in the Social Sciences. *Journal of the American Statistical Association*, *111*(515), 988–1003. DOI: 10.1080/01621459.2016.1141684

Rodriguez, D., Del Alamo, J. M., Fernandez-Aller, C., & Sadeh, N. (2024). Sharing is Not Always Caring: Delving Into Personal Data Transfer Compliance in Android Apps. *IEEE Access : Practical Innovations, Open Solutions*, *12*, 5256–5269. DOI: 10.1109/ACCESS.2024.3349425

Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy*. *Regulation & Governance*, *22*(3), 227–244. DOI: 10.1108/DPRG-02-2020-0019

Sharma, A., Koohang, A., Rana, N. P., Abed, S. S., & Dwivedi, Y. K. (2022). Journal of Computer Information Systems: Intellectual and Conceptual Structure. *Journal of Computer Information Systems*, *63*(1), 37–67. DOI: 10.1080/08874417.2021.2021114

Sharma, A., Rana, N. P., & Nunkoo, R. (2021). Fifty years of information management research: A conceptual structure analysis using structural topic modeling. *International Journal of Information Management*, *58*, 102316. DOI: 10.1016/j.ijinfomgt.2021.102316

Sharma, S., & Warkentin, M. (2019). Do I really belong?: Impact of employment status on information security policy compliance. *Computers & Security*, *87*. Advance online publication. DOI: 10.1016/j.cose.2018.09.005

Singh, S., Dhir, S., Das, V. M., & Sharma, A. (2020). Bibliometric overview of the Technological Forecasting and Social Change journal: Analysis from 1970 to 2018. *Technological Forecasting and Social Change*, *154*, 119963. DOI: 10.1016/j.techfore.2020.119963

Singh, S., Singh, S., Koohang, A., Sharma, A., & Dhir, S. (2023). Soft computing in business: Exploring current research and outlining future research directions. *Industrial Management & Data Systems*, *123*(8), 2079–2127. DOI: 10.1108/IMDS-02-2023-0126

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management, 51*(2), 217–224. Advance online publication. DOI: 10.1016/j.im.2013.08.006

Siponen, M., Mahmood, M. A., & Pahnila, S. (2009). Technical opinion are employees putting your company at risk by not following information security policies? *Communications of the ACM*, *52*(12), 145–147. DOI: 10.1145/1610252.1610289

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly: Management Information Systems*, *34*, 487–502. DOI: 10.2307/25750688

Small, H. (1973). Co-citation in the scientific literature: A new measure of the relationship between two documents. *Association for Information Science & Technology*, *24*(4), 265–269. DOI: 10.1002/asi.4630240406

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. DOI: 10.1016/j.cose.2015.10.006

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.009

Sun, Y., Zhu, X., Wu, W., & Yang, K. (2023). Blockchain Technology and Corporate Default Risk: Empirical Evidence From Public Firms in China. *Journal of Global Information Management*, *31*(7), 1–19. DOI: 10.4018/JGIM.331088

Tambunan, P. N. P., Legowo, N., & Tambunan, D. R. (2024). Strengthening payment card data security: A study on compliance enhancement and risk mitigation through mfa implementation under pci dss 4.0. *Journal of Theoretical and Applied Information Technology*, *102*(9), 4093–4102.

Tauqeer, A., & Fensel, A. (2024). GDPR Data Sharing Contract Management and Compliance Verification Tool. *Software Impacts*, *21*. Advance online publication. DOI: 10.1016/j.simpa.2024.100653

Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2020). GDPR-Compliant Personal Data Management: A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746–1761. DOI: 10.1109/TIFS.2019.2948287

Ullah, M. W., Alam, M. T., Sultana, T., Rahman, M. M., Faraji, M. R., & Ahmed, M. F. (2024). A systematic review on information security policies in the USA banking system and global banking: Risks, rewards, and future trends. *Edelweiss Applied Science and Technology, 8*(6), 8437–8453. Advance online publication. DOI: 10.55214/25768484.v8i6.3816

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3-4), 190–198. DOI: 10.1016/j.im.2012.04.002

Varela-Vaca, Á. J., Gómez-López, M. T., Morales Zamora, Y., & Gasca, M., R. (2025). Business process models and simulation to enable GDPR compliance. *International Journal of Information Security*, *24*(1). Advance online publication. DOI: 10.1007/s10207-024-00952-7

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Information & Management*, *61*(5). Advance online publication. DOI: 10.1016/j.im.2024.103968

Vroom, C., & von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security*, *23*(3), 191–198. DOI: 10.1016/j.cose.2004.01.012

Wang, X., & Xu, J. (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tourism Management, 84*. DOI: 10.1016/j.tourman.2021.104282

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, *18*(2), 101–105. DOI: 10.1057/ejis.2009.12

Willey, L., & White, B. J. (2013). Do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education*, *24*(3), 181–188.

Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*. Advance online publication. DOI: 10.1016/j.ijinfomgt.2022.102520

Wylder, J. O. (2003). Improving security from the ground up: Moving toward a new way of enforcing security policy: Encouraging personal accountability for corporate information security policy. *Information Systems Security : ... International Conference, ICISS ... : Proceedings*, *11*(6), 29–38. DOI: 10.1201/1086/43324.11.6.20030101/40429.6

Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity Policy Compliance in Higher Education: A Theoretical Framework. *Journal of Applied Security Research*, *18*(2), 267–288. DOI: 10.1080/19361610.2021.1989271

Zhang, H., Lv, Y., Zhang, S., & Liu, Y. D. (2024). Digital Supply Chain Management: A Review and Bibliometric Analysis. *Journal of Global Information Management*, *32*(1), 1–20. DOI: 10.4018/JGIM.336285

Zhang, Y., Yang, J., Lei, H., Bao, Z., Lu, N., Shi, W., & Chen, B. (2024). PACTA: An IoT Data Privacy Regulation Compliance Scheme Using TEE and Blockchain. *IEEE Internet of Things Journal*, *11*(5), 8882–8893. DOI: 10.1109/JIOT.2023.3321308

Zhao, J., Hong, Y., Chen, W., & Chen, C. (2024). Psychological Capital and Information Security Policy Compliance, 1-17. *Journal of Computer Information Systems*. Advance online publication. DOI: 10.1080/08874417.2024.2403571

Zhen, J., Xie, Z., Dong, K., & Chen, L. (2022). Impact of negative emotions on violations of information security policy and possible mitigations. *Behaviour & Information Technology*, *41*(11), 2342–2354. DOI: 10.1080/0144929X.2021.1921029

Anuj Sharma is a Professor of Information Systems and Analytics at the Jindal Global Business School, O. P. Jindal Global University, Haryana, India. He is a Fellow of the Indian Institute of Management Indore. His current research interests focus primarily on the development and use of information systems, scientometrics, data analytics, e-commerce, digital marketing, and innovation. He has over 14 years of experience in management, teaching, research, and consultancy at both Indian and international organizations.

Alex Koohang is the dean and professor at the School of Computing at Middle Georgia State University, USA. He holds the Peyton Anderson Endowed Chair in IT. He's a driving force behind expanding and modernizing the university's computing education offerings. He is the author of influential works on trust in technology, knowledge management, organizational performance, e-learning usability, IoT, AI, and digital transformation. He has presented and moderated sessions at major conferences, including IACIS (2024), focusing on AI ethics, trust, and student perspectives.

Satender Pal Singh is an Assistant Professor in the Operations and Decision Science department at TAPMI. He received his Ph.D. in Operations Management from the Indian Institute of Management, Ranchi. He has published his research work in international journals, including Transportation Research Part E: Logistics and Transportation Review, The TQM Journal, Journal of Multi□Criteria Decision Analysis, etc. He has presented his works at various national and international conferences and made a conference publication in IEEE Xplore. He has also won the best paper award in the Management Doctoral Colloquium organized by the Indian Institute of Management Visakhapatnam. He has six years of industry experience in Samsung Heavy Industries India Private Limited, Noida. He holds an engineering degree in Mechanical Engineering.