

# Introduction and Preface to the 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research

Stephan Kuehnel<sup>1</sup>, Ilja Nastjuk<sup>2</sup>, Stefan Sackmann<sup>1</sup>, and Simon Trang<sup>2,3</sup>

<sup>1</sup> Chair of Information Systems, esp. Business Information Management, Martin Luther University Halle-Wittenberg, Universitaetsring 3, 06108 Halle (Saale), Germany

<sup>2</sup> Chair for Information Security and Compliance, Georg August University of Goettingen, Platz der Goettinger Sieben 5, 37073 Goettingen, Germany

<sup>3</sup> Chair for Information Systems, esp. Sustainability, Paderborn University, Warburger Straße 100, 33098 Paderborn, Germany

## Abstract

This volume contains the proceedings of the 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR 2023), held at the 18th International Conference on Wirtschaftsinformatik (WI 2023) in Paderborn, Germany, on September 18, 2023.

## Keywords

CIISR 2023, WI 2023, Information Security, Compliance, IT, ISR

## 1. Introduction

In a connected world of people, data, and things, enterprises are caught between the need for rapid digital growth, regulatory compliance, and securing their information assets across all stakeholders [1]. Effective compliance and security governance as well as the appropriate implementation of corresponding measures are becoming a central factor for digital responsibility and sustainable security [2].


Nowadays, information security and compliance are approached from a variety of different perspectives in information systems research (ISR). As part of information security management, for instance, it is examined which operational measures may result in desired employee behavior [1, 3]. In the context of cloud computing, for instance, it is examined how compliance with service-level agreements can be achieved in hybrid cloud architectures [4]. In the context of business process management, for instance, it is examined how information security and compliance measures in business processes can be ensured sustainably and economically in digitalized and electronic markets [5, 6].


As part of the third edition of this workshop, we acknowledged the thematic link between compliance and information security and decided also to reflect this in the title of the workshop, which is now called the *International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR)*. This year's edition, held on September 18, 2023, in conjunction with the 18th International Conference on Wirtschaftsinformatik in Paderborn, Germany, consisted of several presentations and a poster session. Based on the main theme of the conference—DIGITAL RESPONSIBILITY—we discussed current issues related to the


---

CIISR 2023: 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research, co-located with the 18th International Conference on Wirtschaftsinformatik (WI 2023), September 18, 2023, Paderborn, Germany

✉ stephan.kuehnel@wiwi.uni-halle.de (S. Kuehnel); ilja.nastjuk@wiwi.uni-goettingen.de (I. Nastjuk); stefan.sackmann@wiwi.uni-halle.de (S. Sackmann); simon.trang@uni-paderborn.de (S. Trang)

 0000-0002-6959-9555 (S. Kuehnel)

 © 2023 Copyright for this paper by its authors.  
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

 CEUR Workshop Proceedings (CEUR-WS.org)

responsible handling of information security and compliance, which are of great importance for ISR in an increasingly digitalized world.

## **2. Target Group, Submission Types, and Paper Selection**

The target audience of the CIISR workshop are scientists whose research focuses on current information security and compliance issues, practitioners working in the field of information security and/or compliance, and all other interested parties. This workshop provides the opportunity for (senior) researchers and practitioners to present their latest findings but also serves as a forum for young scientists and doctoral students to present early or ongoing research results.

We invited authors to submit empirical studies, systematic literature reviews, design science research papers, as well as practitioner papers related to the workshop theme, e.g., information security and compliance at the interface with business processes, cloud computing, or current events such as the COVID-19 pandemic, as well as current challenges in the context of IT compliance and information security policies. We called for submissions from the subject areas listed above that fell into one of the following three submission categories:

### **1. Full papers (research papers/practical reports)**

This submission type includes both advanced research with at least partial evaluation and comprehensive practical contributions.

### **2. Short papers (research in progress papers/short practical reports)**

Short papers represent ongoing research or ongoing practical projects. In addition to presenting initial results, these papers should also contain an outlook on further research or further project progress, including planned future work steps.

### **3. Extended abstracts**

Extended abstracts present and discuss high-quality results of already published contributions (or dissertations/postdoctoral theses) with relevance to the workshop topic.

Full papers were not allowed to exceed 12 pages in the submitted version, and short papers as well as extended abstracts were not allowed to exceed six pages, including title, abstract, and placeholders for author information and acknowledgments. The bibliography and appendices were not included in the page count.

Full and short papers were subjected to rigorous double-blind review by two reviewers, where at least one of the reviewers was a member of the Program Committee. Extended abstracts were reviewed single-blind. All reviews focused on five criteria: 1) quality of the theoretical contribution, 2) appropriate use of research methods, 3) degree of innovation and significance of the contribution, 4) presentation and language, and 5) potential of the contribution to foster discussion. Program Committee members were asked to make recommendations to accept, revise, or reject the submissions, which were then discussed by the four workshop chairs to arrive at the final decisions.

A total of 11 papers were submitted for the workshop, of which one full paper was directly accepted and seven were accepted under conditions. Authors of full papers were allowed an additional two pages to incorporate reviewer comments, and authors of short papers and extended abstracts were allowed one page each. In addition to the final version of each paper, a response letter was required to provide information on how and to what extent the reviewer comments were addressed. After another review of the papers and the response letters by the workshop chairs, four full papers, three short papers, and one extended abstract could be accepted. The acceptance rate for full papers was 80% and 60% for short papers. In addition, the extended abstract was also accepted.

### 3. Contents of the CIISR 2023 Workshop

In line with WI 2023, the CIISR workshop was held locally in Paderborn, Germany. In total, more than 30 participants have registered. The CIISR 2023 workshop and these workshop proceedings include 8 papers:

1. The full paper **Interaction Patterns for Regulatory Compliance in Federated Learning** written by Mahdi Sellami, Tomas Bueno Momčilović, Peter Kuhn, and Dian Balta deals with federated learning (FL), where organizations share local machine learning models while the data remain on-premise. For this context, the paper develops four interaction patterns that enable compliance-by-design and trust-context-sensitive analyses of an FL system by combining different privacy-preserving approaches.
2. The full paper **A User-centric View on Data Breach Response Expectations** by Felix Hillmann, Tim Klauenberg, Lennart Schroeder, and Till Ole Diesterhöft focuses on individual customer expectations after data breaches in different situations and business environments. Building on prior research on data breaches that have been integrated into expectation confirmation theory, individual customer expectations are analyzed by conducting twelve qualitative interviews. The findings reveal the individual nature of customer expectations about data breach responses, which are shaped by multiple factors.
3. The full paper **Integrating IT Security Aspects into Business Process Models: A Taxonomy of BPMN Extensions** written by Leonard Nake deals with Business Process Model and Notation (BPNM) extensions from the information/IT security domain. Based on a systematic literature review, a taxonomy is developed that provides an overview of common features and dimensions of security-related BPMN extensions and provides profound insights into existing work.
4. The full paper **From Pixels to Generalization: Ensuring Information Security and Model Performance with Design Principles for Synthetic Image Data in Deep Learning** authored by Martin Böhmer deals with the effective and ethical use of synthetic image data for deep learning in computer vision. Based on challenges in obtaining real training data, design principles for the selection, generation, and integration of synthetic images are proposed, including aspects such as ethical compliance, privacy protection, scene diversity, and complexity management.
5. The short paper **Privacy-Enhancing Technologies in the Process of Data Privacy Compliance: An Educational Perspective** by Alexandra Klymenko, Stephen Meisenbacher, Florian Messmer, and Florian Matthes explores the educational needs of practitioners working in the field of data privacy compliance. Drawing on 11 semi-structured interviews and a survey of 24 respondents, the study discusses the learning goals of privacy-enhancing technologies and explores how these goals can be aligned with practitioners' role-specific needs.
6. The short paper **Nudging Towards Compliance? Assessing the Impact of Nudging Strategies on Information Security Policy Adherence** by Theresa Pfaff explores how employee behavior towards information security policy compliance can be influenced by the concept of nudging. The core of the paper is the presentation of a research model that will be used in future research to investigate the effectiveness of nudging strategies as part of an online experiment.

7. The short paper entitled **How to Foster Compliance in Non-Integrated IT-Landscapes? The Case of Manual Medical Data Transfers** written by Gilbert Georg Hövel and Tizian Matschak addresses the issue that medical professionals often have to manually transfer medication data between different health information systems, which can lead to errors with serious consequences for patients (medication non-compliance). The paper presents a research design that will be used in future research to investigate how different formal sanction mechanisms of deterrence theory relate to different types of medication errors.
8. The extended abstract **The Structure of Data Privacy Compliance** by Alexandra Klymenko, Stephen Meisenbacher, and Florian Matthes deals with data privacy compliance and interprets it as a dynamic process that depends on the roles involved and the nature of their interactions. Based on the results of a previously published interview study, the extended abstract briefly presents a graphical structure that maps the various roles and interactions diagrammatically.

## 4. Organization and Acknowledgement

The workshop organization lay in the hands of Dr. Stephan Kuehnel (workshop chair and web chair), Dr. Ilja Nastjuk, Prof. Dr. Stefan Sackmann, and Prof. Dr. Simon Trang (workshop co-chairs). We would like to express our deepest gratitude to the members of the Program Committee for their active participation in the review and paper selection process:

- Prof. Dr. Jörn Altmann (Seoul National University, South Korea)
- Prof. Dr. Alfred Benedikt Brendel (TU Dresden, Germany)
- Prof. Dr. Nadine Guhr (OWL University of Applied Sciences and Arts, Germany)
- Ass. Prof. Dr. Simon Hacks (Stockholm University, Sweden)
- Dr. Kristin Masuch (University of Göttingen, Germany)
- Mohammed Mubarkoot, Ph.D. (Seoul National University, South Korea)
- Prof. Dr. Jana Rhese (University of Mannheim, Germany)
- Prof. Dr. Michael Schulz (NORDAKADEMIE Hochschule der Wirtschaft, Germany)
- Michael Seifert, M.Sc. (GISA GmbH, Germany)
- Dr. Tobias Seyffarth (Federal Office for Information Security, Germany)
- Prof. Dr. Nils Urbach (Frankfurt University of Applied Sciences, Germany)

We would also like to thank the additional reviewers and sub-reviewers Laura Bauer, Martin Böhmer, Johannes Damarowsky, Gilbert Georg Hövel, Julia Klein, Luis Laemmermann, Tizian Matschak, Leonard Nake, Theresa Pfaff, and Florian Rampold for their active support as well as the organizers and the staff of the 18th International Conference on Wirtschaftsinformatik for including our CIISR Workshop in the conference program and for their continued assistance in organizational and technical matters. Last but not least, we are grateful to all the speakers, poster presenters, and participants who made the CIISR Workshop 2023 a great event.

## References

- [1] S. Trang, B. Brendel, “A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research,” *Information Systems Frontiers*, vol. 21, no. 6, pp. 1265–1284, 2019.
- [2] D. Schatz, R. Bashroush, “Economic valuation for information security investment: a systematic literature review,” *Information Systems Frontiers*, vol. 19, no. 5, pp. 1205–1228, 2017.

- [3] S. Hengstler, S. Kuehnel, K. Masuch, I. Nastjuk, S. Trang, "Should i really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior," *Computers & Security*, vol. 133, p. 103370, 2023.
- [4] M. Seifert, S. Kuehnel, S. Sackmann, "Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions," *ACM Computing Surveys*, vol. 55, no. 11, pp. 1–35, 2023.
- [5] T. Seyffarth, S. Kuehnel, "Maintaining business process compliance despite changes: a decision support approach based on process adaptations," *Journal of Decision Systems*, vol. 31, no. 3, pp. 305–335, 2022.
- [6] S. Sackmann, S. Kuehnel, T. Seyffarth, "Using Business Process Compliance Approaches for Compliance Management with Regard to Digitization: Evidence from a Systematic Literature Review," in *Business process management: 16th International Conference, BPM 2018, Sydney, NSW, Australia, September 9-14, 2018: proceedings*, M. Weske, M. Montali, I. M. Weber et al., Eds., vol. 11080, pp. 409–425, Springer, Cham, 2018.