Techniques for strengthening the Digital Business Ecosystem: selection and implementation in the organization

Beāte Krauze[1]

[1]Institute of Information Technology, Riga Technical University, 6A Kipsalas Street, Riga LV-1048, Latvia

Abstract

Digital Business Ecosystems (DBEs) are becoming increasingly critical for delivering digital services; however, their resilience remains a challenge due to the complexity of regulations and technological interdependencies. Recent EU legislation, such as the NIS2 Directive, the Digital Operational Resilience Act, the Cyber Resilience Act, and the Artificial Intelligence Act, among others, introduces new requirements for resilience that apply to DBEs and must be ensured not only at the individual organizational level but also across the entire ecosystem. This doctoral research proposes a Design Science Research methodology to develop practical artifacts to strengthen DBE resilience. Through iterative analysis and phased artifact development, the research will result in a conceptual model, methodological guidelines, and a decision support algorithm that improve the resilience of DBE and ensure compliance with regulations. The research also outlines a framework for continuous improvement, combining AI-assisted updates with expert validation.

Keywords

digital business ecosystems, design science research, resilience, EU law, cybersecurity

1. Introduction

The increasing reliance on interdependent digital infrastructures across sectors has made Digital Business Ecosystems (DBEs) a key topic in both the technology and the European Union (EU) legislative agendas [1]. DBE is a dynamic, interconnected, and technology-driven environment, comprising individuals, organizations, and digital entities that co-create value using information and communication technologies [2], [3]. The concept has evolved from traditional business ecosystems by integrating digital technologies, automation, and real-time data exchange, fostering more interconnected and interdependent networks of digital and physical entities.

As DBEs evolve in complexity and scale, their ability to remain operational under conditions of stress, such as cybersecurity incidents, disasters, or system failures, becomes critical. However, achieving resilience within such ecosystems poses substantial challenges due to the variety of actors, technologies, and governance structures involved [2], [4].

Recent disruptions and emerging threats have led the EU to enact a series of regulatory instruments aimed at strengthening operational and digital resilience. These include the NIS2 Directive, Digital Operational Resilience Act (DORA), Cyber Resilience Act (CRA), and Artificial Intelligence Act (AI Act), among others. Although these legal frameworks impose specific obligations on organizations, the fragmented nature of existing technical tools and governance methodologies limits the extent to which resilience requirements can be effectively operationalized across DBEs. Frameworks like COBIT or ITIL include legal compliance as a general principle, but they lack resilience-centric design.

Although most legislative provisions are applied to individual organizations, DBEs consist of multiple interconnected entities that rely on shared digital infrastructures, services, and governance structures. DBEs include core service providers, SMEs, public institutions, and orchestrators, each contributing distinct capabilities such as infrastructure, domain expertise, regulatory oversight, or coordination [5].

BIR-WS 2025: BIR 2025 Workshops and Doctoral Consortium, 24rd International Conference on Perspectives in Business Informatics Research (BIR 2025), September 17-19, 2025, Riga, Latvia

beate.krauze@edu.rtu.lv (B. Krauze)

0009-0005-9630-2234 (B. Krauze)

This interconnectedness escalates resilience challenges, as regulatory compliance must be ensured not only at the individual organizational level, but also across the entire ecosystem [6].

Current research tends to address resilience from isolated perspectives, such as cybersecurity [7], enterprise architecture [8], [9], or compliance [10], [11], without offering integrated approaches. This doctoral research proposes a Design Science Research (DSR) based methodology to develop practical artifacts that support resilience-strengthening efforts in DBEs [12]. The research aligns with critical EU priorities (cybersecurity, operational resilience) and has real-world implications for SMEs, public institutions, and policymakers. EU regulations are legally binding and sector-specific, designed to enforce minimum resilience and cybersecurity standards across critical sectors. In contrast, frameworks such as the NIST Cybersecurity Framework are voluntary, risk-based, and more flexible, emphasizing best practices over compliance.

This paper is organized as follows. Section 2 reviews the background and related work, introducing the concept of DBEs, resilience considerations, and the relevant European legislative landscape. Section 3 presents the research approach, including the problem statement, research questions, and objectives, grounded in the Design Science Research methodology. Section 4 outlines the anticipated contributions, including the initial findings of the literature review and legal analysis, the methodological roadmap, and a plan for continuous improvement. Section 5 concludes the paper and discusses future research directions.

2. Background and related work

Resilience in DBEs refers to the ability of an ecosystem to withstand, adapt to, and recover from disruptions while maintaining continuous operations and minimizing negative impacts [13]. Resilience is achieved through a combination of technological, organizational, and regulatory measures, including cybersecurity measures, risk management, and compliance with legal requirements.

As these ecosystems grow in scope and complexity, the need for resilience becomes crucial, particularly in the context of security, regulations, and operations [14], [15]. Previous studies primarily explore DBE governance, digital infrastructure, security, and regulatory aspects, but rarely address these issues in an integrated way under the lens of resilience [2].

The EU has implemented several acts and directives to enhance its resilience, focusing on cybersecurity and operational stability. In addition, there is a growing gap between semiformal models (i.e. UML, BPMN, ArchiMate) and methodologies (i.e. TOGAF, ITIL, COBIT) and real-world regulatory requirements, particularly as shaped by EU laws like the NIS2, DORA, CRA, and AI Act, and others [10], [11], [16], [17], [18], [19], [20], [21]. These regulations impose explicit obligations, reporting deadlines, risk quantification criteria, etc., which may require machine-readable rules, auditability, and traceability that semiformal models do not fully support.

3. Research approach

Doctoral research aims to develop methodological support for strengthening the resilience of DBEs in the EU. The research addresses compliance challenges, technical and operational complexities, and knowledge fragmentation. Therefore, with the results, it would be possible to help organizations navigate regulations, manage risks, and strengthen their resilience.

3.1. Problem statement

DBEs are increasingly critical for the successful delivery of services and the resilience of the entire organizational technology ecosystem. However, achieving resilience in DBE is challenging due to:

1. Complex regulatory environment and knowledge problems as compliance with EU law requires organizations to navigate legal texts for operational resilience, cybersecurity, and incident reporting [10], [11], [16], [17], [18], [19], [20], [21];

2. Technological integration and interoperability (e.g., modular architectures, digital transformation barriers) [8], [9], [14], [22];
3. Cybersecurity and digital trust (e.g., threat complexity, digital security-by-design) [7], [23], [24], [25], [26], [27];
4. Operational resilience, especially in contexts like e-government, open banking, and medical data ecosystems [14], [28].

3.2. Research questions

The research question, which serves as the central query summarizing the entire research concept and guiding the investigation, can be characterized as follows.

What techniques can strengthen the resilience of Digital Business Ecosystems to ensure the integrity and continuous functionality of technological infrastructures during disruptions?

To enhance clarity, the main question should be deconstructed into four subquestions. In this context, four research questions emerge.
RQ1: What are the key technical complexities and vulnerabilities within DBEs, particularly in the context of enterprise architecture, risk management, and cybersecurity, that impact operational resilience?
RQ2: What are the specific resilience requirements imposed by European Union acts and directives, and how do they affect DBE operations?
RQ3: What are the limitations of current frameworks, strategies, and tools in supporting DBE resilience, and how can these gaps be addressed to ensure better regulatory alignment and compliance?
RQ4: What methodological support can be developed to improve DBE resilience while addressing regulatory demands and operational challenges?

By addressing these questions, this research aims to establish a comprehensive framework for enhancing the resilience of DBEs, ensuring alignment with regulatory requirements, mitigating technical and operational vulnerabilities, and supporting informed decision-making.

3.3. Research objectives

The research objectives follow the principles of DSR [12]. This methodology emphasizes the iterative creation and evaluation of innovative artifacts to solve real-world problems effectively. Through iterative analysis and phased artifact development, the research will result in a conceptual model, methodological guidelines, and a decision support algorithm that improve the resilience of DBE and ensure compliance with regulations. Based on the RQs, the research objectives are:

1. Analyse the technical complexities and vulnerabilities within DBE, focusing on enterprise architecture, risk management, and cybersecurity, and identify key operational issues impacting resilience.
2. Investigate the technical and operational resilience requirements arising from European Union legislative enactments.
3. Identify gaps in existing frameworks, strategies, and tools for DBE resilience, and align resilience compliance requirements with the European regulatory environment.
4. Develop methodological support, including a conceptual model and practical guidelines, to enhance DBE resilience by addressing compliance requirements, risk management, and operational complexities, while ensuring regulatory alignment.
5. Design a decision-making algorithm to guide the effective implementation of resilience-strengthening techniques within DBE.

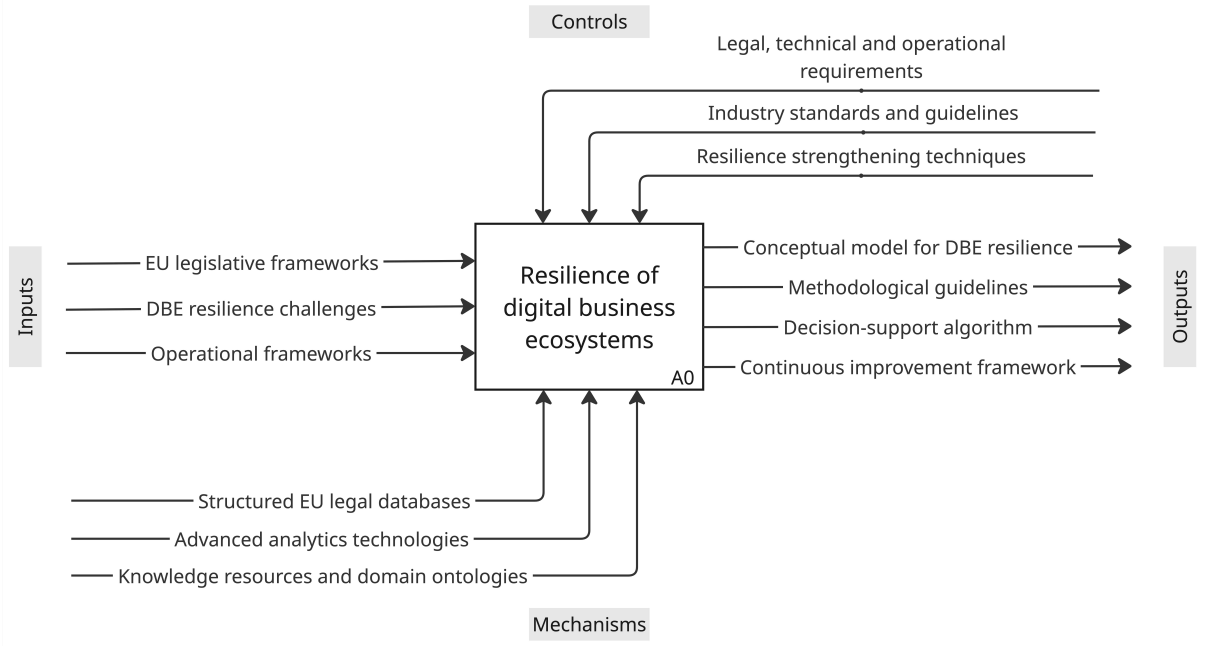

Figure 1: DBE resilience IDEFØ model A0.

To visualize the above-mentioned research objectives, an IDEFØ method is used, which is helpful in understanding the functions and interactions within complex systems. The different arrows in Figure 1 are identified by the side of the activity box. Thus, inputs are on the left, controls at the top, outputs on the right, and mechanisms at the bottom.

4. Contributions

4.1. Research methodology

The methodology follows the general DSR process model, encompassing the following phases [12] (Figure 2).

The DSR approach is structured into three interconnected components: Environment, DSR, and Knowledge Base [12]. The Environment encompasses the practical context, including people (e.g., IT professionals, policymakers), organizational systems (e.g., SMEs and public institutions), technical systems (e.g., DBE platforms, cybersecurity infrastructure), and core challenges such as regulatory complexity and the lack of integrated techniques. The DSR section outlines the phased artifact development process, including the conceptual model, methodological guidelines, and decision-making algorithm. These are assessed and refined through empirical analysis, expert interviews, and practical applications. To ensure the effectiveness and applicability of the proposed artifacts, the research includes a multi-phase validation strategy. This will involve stakeholder interviews with domain experts (e.g., regulators, IT professionals working with DBEs, cybersecurity professionals), pilot testing in selected DBE contexts (e.g., open banking), and empirical evaluation based on domain-specific KPIs. These validation activities will be iteratively applied to refine the artifacts and confirm their practical utility and regulatory alignment. The Knowledge Base provides foundational input, such as EU regulations, resilience requirements, IT governance practices, risk frameworks, and gap analyses. Two feedback loops – relevance cycle and rigor cycle – ensure the research remains focused on practical needs and scientifically validated knowledge.

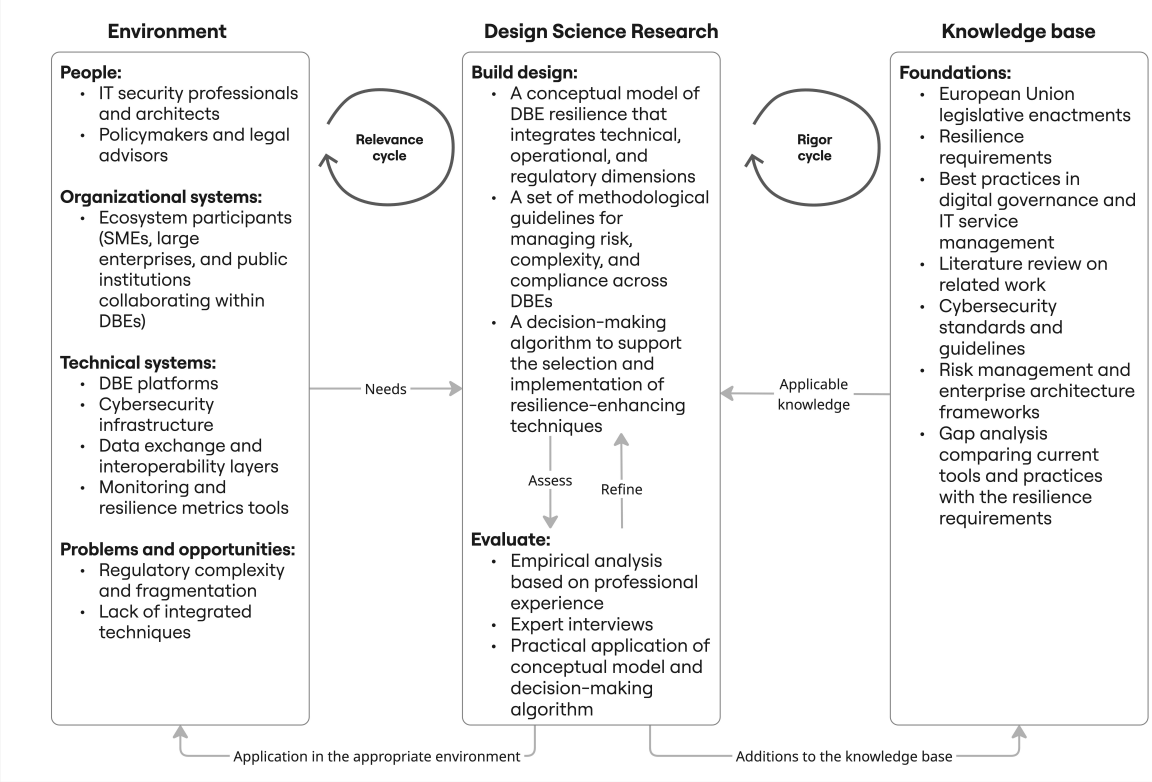

Figure 2: DSR methodology.

4.2. First results

The first results have been obtained after performing a literature review to investigate the key challenges associated with resilient DBEs. The analysis included identifying key resilience challenges and mapping them to relevant legislative enactments, ensuring a comprehensive understanding of how resilience is impacted within DBEs.

The categorization of challenges was derived through thematic coding and synthesis of recurring themes from the literature. This included analysing previous studies, extracting key topics, and grouping them based on their conceptual similarities and practical implications in DBE resilience. While some challenges, such as technological integration, supply chain and operational resilience, cybersecurity, and digital trust challenges, as well as regulatory compliance challenges, have been extensively studied, they have relatively few solutions, potentially indicating significant research or implementation gaps.

To support this analysis, a graph was constructed to map relevant legislative enactments to specific resilience constructs (Figure 3). This visual representation enables the identification of legal requirements for resilience, highlights areas of regulatory coverage, and facilitates a clearer understanding of how legal obligations intersect with technological and organizational resilience.

4.3. Plan for continuous improvement

In the future, given the evolving nature of European digital regulations and the increasing complexity of DBEs, the proposed methodological support must remain adaptable and up to date. To address this need, the research incorporates a structured plan for continuous improvement, combining automated mechanisms with expert oversight. Although this research is in its early stages, a framework is envisioned to enable continuous improvement.

Artificial intelligence (AI), particularly natural language processing (NLP) and machine learning, could be used to monitor and analyse changes in legislative enactments from official EU legal repositories (e.g., EUR-Lex, EU Open Data Portal). Without further analysis at this stage, for example, mechanisms

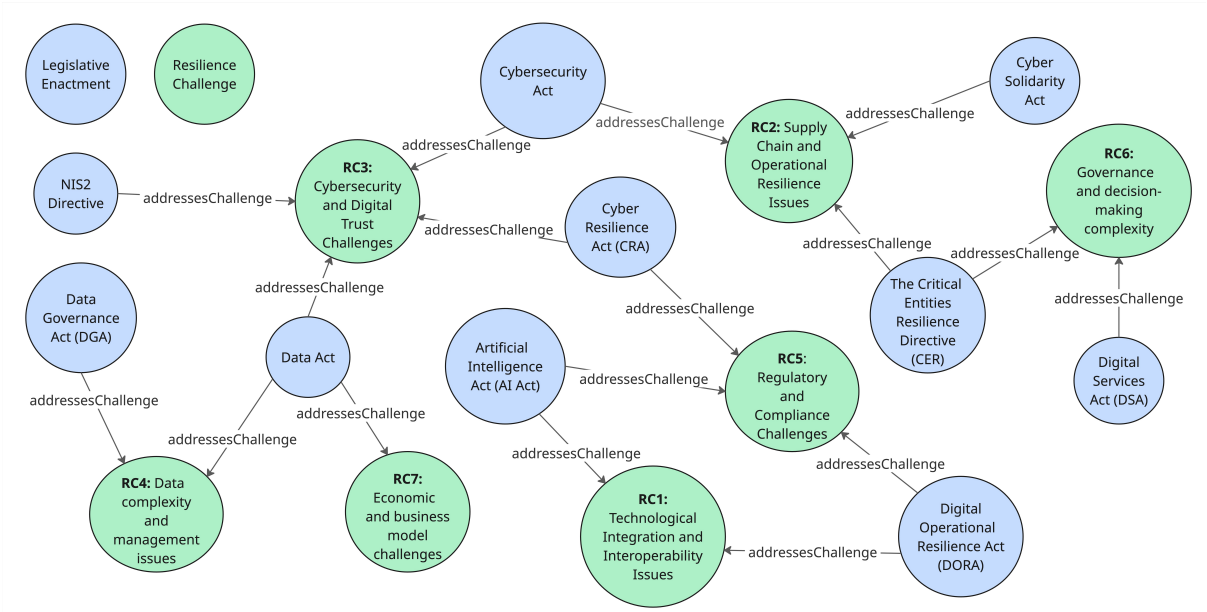

Figure 3: Graph of legislative enactments and resilience constructs.

such as RSS feed monitoring can support the identification of new regulatory requirements, map them to resilience components, and trigger structured updates to the conceptual model, guidelines, and decision-making algorithm. A mechanism (rule orchestration), supported by legal ontologies and machine-readable logic, could allow integration of new requirements. The effectiveness of this process may be evaluated using performance metrics such as update latency, mapping accuracy, coverage of impacted components, and alignment with legal interpretations. However, human-in-the-loop validation remains essential to ensure accuracy and regulatory alignment. Given that AI (particularly NLP) is aimed at supporting the continuous monitoring and updating of artefacts, the following fallback mechanisms could be deployed: expert review cycles, version control, and scenario testing.

To ensure practical relevance and transferability, the framework and artifacts will undergo pilot testing in a specific DBE context with domain-specific KPIs, for example, open banking. The framework will evolve through empirical validation, stakeholder engagement, and technical analysis. As the research progresses, the scope and reliability of AI-assisted updates will be further assessed and evaluated based on domain-specific quantifiable KPIs.

4.4. Discussion and next steps

Building on the literature review and EU law analysis, this research outlines key objectives to enhance DBE resilience through the phased development of models, guidelines, and a decision-support algorithm. Next steps include systematically extracting resilience-related requirements from relevant laws and formulating a conceptual model for resilience. A multi-criteria decision analysis algorithm will be developed to support strategic prioritization, followed by the creation of adaptable guidelines for various DBE contexts. Finally, the approach will be empirically validated through action research and expert interviews.

5. Conclusion

In this doctoral consortium paper, the author has presented an overview of the research agenda focused on enhancing the resilience of DBEs in the EU. The research addresses the intersection of regulatory compliance, technological integration, and operational continuity by proposing a DSR-based methodology. Initial results from a literature review and legislative analysis have identified key resilience

challenges and gaps in current practices. The proposed future work includes the development of a conceptual model, methodological guidelines, and a decision-support algorithm, along with a framework for continuous improvement supported by AI and expert validation. As the doctoral research is still in its early stages, the current research questions, objectives, and methodological components represent a preliminary framework. These elements are expected to evolve and be refined through iterative development, empirical validation, and continuous feedback from stakeholders and domain experts. The research aims to bridge the gap between EU regulatory requirements and practical resilience techniques.

Acknowledgments

This doctoral research is conducted under the supervision of Prof. Dr. sc.ing. Jānis Grabis from the Riga Technical University (Latvia), Institute of Information Technology.

Declaration on Generative AI

The author has not employed any Generative AI tools.

References

[1] E. Kun, Challenges in regulating cloud service providers in eu financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the digital operational resilience act, Computer Law & Security Review 52 (2024) 105931. doi:https://doi.org/10.1016/j.clsr.2023.105931.

[2] P. K. Senyo, K. Liu, J. Effah, Digital business ecosystem: Literature review and a framework for future research, International Journal of Information Management 47 (2019) 52–64. doi:https://doi.org/10.1016/j.ijinfomgt.2019.01.002.

[3] K. Korpela, U. Kuusiholma, O. Taipale, J. Hallikas, A framework for exploring digital business ecosystems, in: 2013 46th Hawaii International Conference on System Sciences, 2013, pp. 3838–3847. doi:10.1109/HICSS.2013.37.

[4] Øyvind Toftegaard, G. Grøtterud, B. Hämmerli, Operational technology resilience in the 2023 draft delegated act on cybersecurity for the power sector—an eu policy process analysis, Computer Law & Security Review 54 (2024) 106034. doi:https://doi.org/10.1016/j.clsr.2024.106034.

[5] X. Zhang, Y. Yang, Y. Chen, History and future of business ecosystem: a bibliometric analysis and visualization, Environment, Development and Sustainability (2024) 1–24. doi:10.1007/s10668-024-05318-6.

[6] B. Krauze, An analysis of resilience in digital business ecosystems, in: Research Challenges in Information Science, Springer Nature Switzerland, Cham, 2025, pp. 162–171. doi:10.1007/978-3-031-92471-2_13.

[7] V. Tzavara, S. Vassiliadis, Tracing the evolution of cyber resilience: a historical and conceptual review, International Journal of Information Security 23 (2024) 1695 – 1719. doi:10.1007/s10207-023-00811-x.

[8] A. Coskun-Setirek, M. Carmela Annosi, W. Hurst, W. Dolfsma, B. Tekinerdogan, Architecture and governance of digital business ecosystems: A systematic literature review, Information Systems Management 41 (2024) 58 – 90. doi:10.1080/10580530.2023.2194063.

[9] K. Lenkenhoff, U. Wilkens, M. Zheng, T. Süße, B. Kuhlenkötter, X. Ming, Key challenges of digital business ecosystem development and how to cope with them, Procedia CIRP 73 (2018) 167–172. doi:https://doi.org/10.1016/j.procir.2018.04.082, 10th CIRP Conference on Industrial Product-Service Systems, IPS2 2018, 29-31 May 2018, Linköping, Sweden.

[10] C. Schmittner, O. Veledar, T. Faschang, G. Macher, E. Brenner, Fostering cyber resilience in europe: An in-depth exploration of the cyber resilience act, in: Systems, Software and Services

Process Improvement, Springer Nature Switzerland, Cham, 2024, pp. 390–404. doi:10.1007/978-3-031-71139-8_26.

[11] J. G. Proudfoot, W. A. Cram, S. Madnick, Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations, European Journal of Information Systems 34 (2025) 436 – 459. doi:10.1080/0960085X.2024.2345867.

[12] A. Hevner, A three cycle view of design science research, Scandinavian Journal of Information Systems 19 (2007).

[13] T. Farmakis, A. Koukopoulos, G. Zois, I. Mourtos, S. Lounis, K. Kalaboukas, Developing a circular and resilient information system: A design science approach, in: Advances in Production Management Systems. Production Management Systems for Volatile, Uncertain, Complex, and Ambiguous Environments, Springer Nature Switzerland, Cham, 2024, pp. 64–79. doi:10.1007/978-3-031-71622-5_5.

[14] A. Q. Gill, M. Hansnata, Digital government ecosystem: Adaptive architecture for digital and ict investment decision making, in: Proceedings of the 25th Annual International Conference on Digital Government Research, dg.o '24, Association for Computing Machinery, New York, NY, USA, 2024, p. 555–564. doi:10.1145/3657054.3657119.

[15] B. Krauze, J. Grabis, A conceptual model of digital immune system to increase the resilience of technology ecosystems, in: Research Challenges in Information Science, Springer Nature Switzerland, 2024, pp. 82–96. doi:10.1007/978-3-031-59465-6_6.

[16] L. A. Bygrave, The emergence of eu cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes, Computer Law and Security Review 56 (2025). doi:10.1016/j.clsr.2024.106071.

[17] D. Eke, B. Stahl, Ethics in the governance of data and digital technology: An analysis of european data regulations and policies, Digital Society 3 (2024). doi:10.1007/s44206-024-00101-6.

[18] S. Fischer-Hübner, C. Alcaraz, A. Ferreira, C. Fernandez-Gago, J. Lopez, E. Markatos, L. Islami, M. Akil, Stakeholder perspectives and requirements on cybersecurity in europe, Journal of Information Security and Applications 61 (2021) 102916. doi:https://doi.org/10.1016/j.jisa.2021.102916.

[19] M. W. Hodgins, The perils of cybersecurity regulation, Review of Austrian Economics (2024). doi:10.1007/s11138-024-00660-4.

[20] M. Kianpour, S. Raza, More than malware: unmasking the hidden risk of cybersecurity regulations, International Cybersecurity Law Review 5 (2024) 1–44. doi:10.1365/s43439-024-00111-7.

[21] S. Salvaggio, N. González, The european framework for cybersecurity: strong assets, intricate history, International Cybersecurity Law Review 4 (2022). doi:10.1365/s43439-022-00072-9.

[22] A. Chen, Y. Lin, M. Mariani, Y. Shou, Y. Zhang, Entrepreneurial growth in digital business ecosystems: an integrated framework blending the knowledge-based view of the firm and business ecosystems, Journal of Technology Transfer 48 (2023) 1628 – 1653. doi:10.1007/s10961-023-10027-9.

[23] P. G. Chiara, The cyber resilience act: The eu commission's proposal for a horizontal regulation on cybersecurity for products with digital elements; [il cyber resilience act: La proposta di regolamento della commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali], Rivista Italiana di Informatica e Diritto 5 (2023) 143 – 153. doi:10.32091/RIID0108.

[24] T. Hasani, N. O'Reilly, A. Dehghantanha, D. Rezania, N. Levallet, Evaluating the adoption of cybersecurity and its influence on organizational performance, SN Business and Economics 3 (2023). doi:10.1007/s43546-023-00477-6.

[25] D. Markopoulou, V. Papakonstantinou, P. de Hert, The new eu cybersecurity framework: The nis directive, enisa's role and the general data protection regulation, Computer Law and Security Review 35 (2019). doi:10.1016/j.clsr.2019.06.007.

[26] A. Pigola, F. de Souza Meirelles, Unraveling trust management in cybersecurity: insights from a systematic literature review, Information Technology and Management (2024). doi:10.1007/s10799-024-00438-x.

[27] P. Radanliev, Digital security by design, Security Journal 37 (2024) 1640 – 1679. doi:10.1057/s41284-024-00435-3.

[28] K. Degen, T. Teubner, Wallet wars or digital public infrastructure? orchestrating a digital identity data ecosystem from a government perspective, Electronic Markets 34 (2024). doi:10.1007/s12525-024-00731-1.