DOCTORAL CONSORTIUM

CREATING BUSINESS VALUE IN UNPREDICTABLE TIMES AIMING FOR ANTIFRAGILITY

EDZO A. BOTJES, TIM HUYGH, LAURY BOLLEN, REMKO W. HELMS

Open Universiteit, Heerlen, the Netherlands
edzo.botjes@ou.nl, tim.huygh@ou.nl, laury.bollen@ou.nl, remko.helms@ou.nl

Cyber resilience is conceptualized as a socio-technical form of risk management aimed at mitigating the business impact of both foreseen and unforeseen disruptions. While traditional cybersecurity overlaps with this domain, true resilience requires more than mere impact reduction; organizations must extract strategic value from the unknown, a state characterized as antifragility. Organizational learning serves as the fundamental mechanism for fostering this antifragile posture. This PhD research project proposes the development of a Cyber Resilience Maturity Model (CRMM) designed to facilitate organizational learning and enable firms to gain value from uncertainty.

DOI
https://doi.org/10.18690/um.fov.4.2026.73

ISBN
978-961-299-152-4

Keywords:
antifragility, cyber resilience, cyber security, enterprise risk management, enterprise architecture, maturity models

University of Maribor Press

1 Introduction

Modern society is characterized by the seamless integration of organizations and individuals within a complex network of information and processes, creating an environment defined by volatility, uncertainty, complexity, and ambiguity (VUCA) (Bennett & Lemoine, 2014). Disruptions within a value chain result in significant impact at global, national, and individual levels. A series of events has contributed to the creation of multiple stringent legislative frameworks, e.g., NIS2, RED, CRA, DORA, PLR, and the MDR (Reeder & Hall, 2021; Tasheva & Kunkel, 2022), each of which prescribes the application of (existing) risk management and cyber security controls and practices.

Virtually all enterprise risk management and cyber security frameworks incorporate the fundamental steps of identification, treatment and monitoring of possible threats (Diefenbach et al., 2019). However, this approach often proves insufficient due to the inherent unpredictability of an organization's internal and external contexts, which cannot be adequately addressed through deterministic checklists (Aven, 2015; Boeing, 2016; Metcalf et al., 2021). In addition, risk management and cyber security traditionally start by identifying value, followed by managing the protection of this value. Security is achieved when expectations regarding a specific value overlap with actual observations (Huang et al., 2010; Schneier, 2008). Hence, the security of value is dynamic in a VUCA context, as is the value itself (Van Gils, 2023), rendering investments to secure value essentially unfalsifiable (Herley, 2016).

The primary goal of both risk management and cybersecurity is to ensure business continuity. Both disciplines encompass the organization and its environment, where the scope of causality is dominated by the interplay between human and machine, also addressed as 'cyber'. These commonalities lead to the unification of risk management and cyber security into cyber resilience (Eling et al., 2021; Linkov & Kott, 2019).

2 Problem definition

Where traditional approaches focus on managing potential threats (the "known unknown"), cyber resilience needs to address the "unknown unknown" (Aven, 2017). Recognizing that our reality is inherently unpredictable, Taleb (2012) coined

the term antifragile as the antithesis of fragile. Whereas fragility leads to diminished value caused by stress, antifragility leads to enhanced value caused by stress, and is therefore closely aligned with resilience (e.g., Axenie et al., 2024).

Martin-Breen and Anderies (2011) distinguish three subtypes of resilience within the literature. First, Engineering Resilience where the function (what) and the construction (how) are well engineered to uphold the continuity of value delivery. Second, Systems Resilience where the construction can alter, to uphold the function to deliver value. Finally, Complex Adaptive Systems (CAS) Resilience where the function and construction both can be altered to deliver a more suitable value. The concept of antifragility extends beyond these forms of resilience (Hillson, 2023), by optimizing the conditions for CAS Resilience while simultaneously integrating the two other subtypes of resilience to mitigate fragility toward "known" and "known unknown" events. Although various studies have investigated the requirements for achieving antifragility (e.g., Adobor and Kudonoo, 2025; Axenie et al., 2024; Botjes et al., 2021), none have yet been incorporated into cyber resilience guidance, such as a framework or maturity model.

Maturity models are a popular tool for guiding organizational management (van Looy et al., 2017). These models define discrete maturity levels for specific classes of objects, representing qualitative and/or quantitative stages of capability (Becker et al., 2009). By evaluating the current state, these models provide insights into progress and provide insights used to create roadmaps for transitioning from the present to a desired future state. Maturity models are widely used as sensemaking tools, across hundreds of disciplines in both business and academia (Adekunle et al., 2022).

While existing Cyber Resilience Maturity Models (CRMMs) offer valuable guidance, such as roadmapping, they often overlook two critical concepts. Firstly, the concept of antifragility as the capacity to not only withstand disruptions, but to gain value from them, thereby optimizing resilience. Secondly, the concept of the learning organization, which emphasizes fostering a culture that advances in resilience maturity, and prepares for unknown challenges. These omissions limit the effectiveness of CRMMs in addressing the dynamic and evolving nature of both internal and external organizational contexts.

Critiques on maturity models, and knowledge artifacts in general, often center on the lack of replication regarding causal relationships (Adekunle et al., 2022; Gräubig & Bley, 2023; Monteiro & Maciel, 2020) and the subjective perspective in sensemaking, namely, the notion that what is unknown cannot be observed (Aven, 2015; Lasrado, 2018; Uppström, 2017; Vom Brocke et al., 2020). These two points of critique are fundamentally rooted in the volatile, uncertain, complex, and ambiguous (VUCA) nature of both internal and external organizational contexts. This research systematically accounts for these concerns within its methodology.

Our research objective is to address the following central research question: *How can organizations exploit a chaotic context to generate more business value?* We formulated the following research questions;

RQ1: *What is a Cyber Resilience Maturity Model (CRMM) that adequately addresses the exploitation of unforeseen events?*

RQ2: *How does the (extended) Cyber Resilience Maturity Model (CRMM) offer guidance and value when applied by organizations?*

RQ3: *What are the key lessons learned from the application of the Cyber Resilience Maturity Model (CRMM) and how can these lessons be incorporated into a refined version of the CRMM?*

Upon answering these questions, this PhD research will deliver a validated Cyber Resilience Maturity Model (CRMM) designed to facilitate organizational learning in the face of chaos. This novel framework transcends traditional, static risk management approaches by providing a pathway for organizations to navigate 'unknown unknowns'. Ultimately, this research will demonstrate that by embracing antifragile behavior and enabling organizational learning, organizations can do more than merely withstand disruptions; they can actively gain value from exposure to the 'unknown unknowns'.

3 Methodology

Embarking onto research of cyber resilience implies an inquiry in the socio-technical domain, which presents significant challenges regarding generalization and replication (Kaleliglu, 2021; Pyle, 2023; Stevenson, 2023). Replication is essential to

prove the causal relationship between actions and results. The lack of research on the causality between actions and results is a central critique on maturity models (Monteiro & Maciel, 2020).

Critical realism as a research lens offers a way to address socio-technical reality while accounting for the replication crisis and the generalization challenge (Edwards et al., 2014; Tsang & Kwan, 1999; Uppström, 2017). Critical realism maintains that an objective reality exists independently of our subjective observations; consequently, retroduction is applied to uncover underlying, unobservable structures.

In line with this perspective, and respecting the 'wicked' nature of the problem domain, we apply iterative Design Science Research (DSR), by integrating the eADR (Mullarkey & Hevner, 2019) and the eDSR (Tuunanen et al., 2024) into five phases: (1) Diagnosis, (2) Design Objectives and Requirements, (3) Design and Development, (4) Implementation, and (5) Evolution. Each phase follows five steps: (a) Problem Formulation, (b) Artifact Creation, (c) Evaluation, (d) Reflection, and (e) Formalization of Learning (Figure 1). The aim of this approach is to optimize learning during the research and deliver intermediate (small) knowledge artifacts to be validated and reused (Hevner et al., 2024; Maedche et al., 2024).

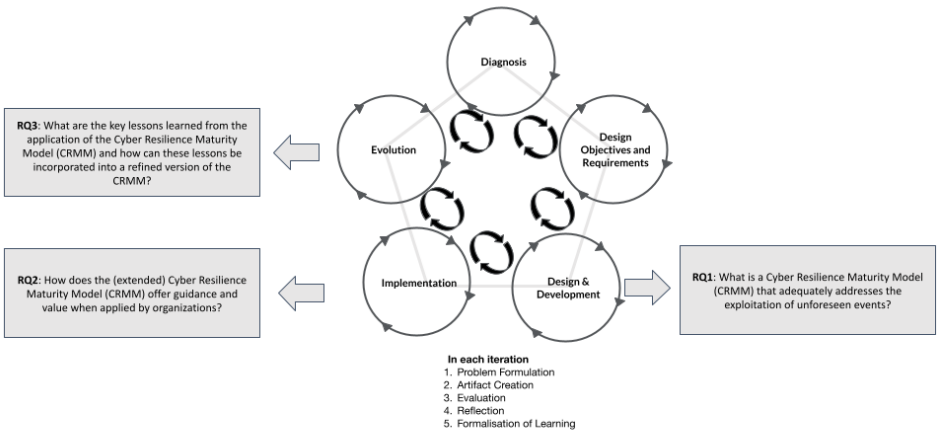

Figure 1: Applied research method based on eADR (Mullarkey & Hevner, 2019) and on eDSR (Tuunanen et al., 2024)

We embrace open science (UNESCO & Canadian National Commission for UNESCO, 2022) and the FAIR-principles (Wilkinson et al., 2016) in support of replicability, independence, precision, and falsifiability (Recker, 2021). Therefore, our research infrastructure (Botjes et al., 2026b) consists out of primarily open-source tooling for each of the four phases from the open science framework: search and discover, design study, collect and diagnose data, and publish reports (Open Science Collaboration, 2015).

4 Preliminary/Expected results

During our iterations in and between the *diagnosis phase* and the *design objectives and requirements phase* (Figure 1), we formalized CRMM design goals and design principles based on relevant constructs and kernel theories. These form requirements for a CRMM that are used for the iterations of the *design and development phase*. In multiple iterations, in which we searched in literature and among experts, we were unable to find an existing CRMM (related) framework (Botjes et al., 2026a) which adheres to the formulated design goals and principles.

The focus of existing frameworks is on keeping the status quo, by determining the variety of the external context and to dampen it for the internal context. Our current objective for the next iterations of the *design and development phase* is how to capture these observations in a rigorous way to be replicated by others. Key challenges in achieving this include a lack of clear documentation on how the identified frameworks were constructed, and few experts are available to validate our observations for multiple frameworks.

Currently we are running various experimental iterations of the *design and development phase* to determine the viability of extending existing CRMM (related) frameworks. We do this together with masters students at multiple universities to determine the viability of extending existing models to adhere to the requirements from the *design objectives and requirements phase*. If not, the conclusion will be that it is inevitable to create a new CRMM that adheres to the requirements (caputered as design goals and design principles) and is grounded in the academic knowledge base.

In support of the *evaluation step* in the *design and development phase* and future replication iterations of this phase, we created an open data set of existing frameworks for cyber resilience practitioners to collaborate on.

5 Future development

Based on our analysis in the *diagnosis phase* and on the preliminary requirements being the design goals and principles as deliverable from the *design objective and requirements phase* we are currently of the opinion that it will probably not be viable to alter existing CRMM (related) frameworks, to cover all the formulated requirements. The existing frameworks are focused on not only minimizing the impact, but also focused on a specific expert domain, and thus not designed to offer guidance to non-experts. Extending existing frameworks to cover as many as possible of the CRMM requirements has the upside of utilizing the current adoption in the field by experts and practitioners of these frameworks. This will improve the existing resilience of organizations, which in itself adds to the purpose of business continuity.

We hence foresee the need for creating a new CRMM which enables decision-makers of varying experience and backgrounds, to make sense of their current domain and envision future steps to evolve towards antifragility. This might also imply adopting language in the CRMM that resonates well with practitioners, to encourage adoption and application. Therefore, the research might need to deliver multiple models where one is the core model, which adheres to a high level of scientific rigor, and other models which are derivatives of the core model that are tailored to relevant domains in practice.

We also anticipate a challenge in shifting the mental models of current practitioners. For instance, many risk managers are conditioned, or primed, to associate risk solely with negative outcomes. As a result, even if risk management is defined to inlcude opportunities, as in ISO 31000, this may not automatically translate into the integration of opportunity management within the actual risk management practices. This is an example of the tension between scientific rigor, and model adoption and application.

Therefore, the *design and development phase* will deliver multiple models, of which each will have their own evaluation step for validation. We will select multiple models (at least three) from the *design and development phase* to enter the *implementation phase*. In this phase we will apply each model in multiple groups, to measure the perceived value to reach the defined design goals.

As the proposed design goals and principles do not prescribe specific sectors or criteria for applying the CRMM to improve maturity in resilience, we will favor a randomized approach for group selection model application. The model(s) will be evaluated on their perceived overall value, their contribution to the design goals, their coverage of the design principles, and the frequency of learning that is supported. The outcomes of the formulation of learning steps of the various iterations over the *implementation phase*, will be used as input to the *evolution phase* looping back to the *diagnosis phase* for re-evaluation of the problem and solution domain.

During our research for a CRMM, which enables organizations to move towards antifragility, we will provide various validated building blocks to add to the design knowledge on how to achieve antifragility as an organization to uphold business continuity in a VUCA context.

References

Adekunle, S. A., Aigbavboa, C., Ejohwomu, O., Ikuabe, M., & Ogunbayo, B. (2022). A critical review of maturity model development in the digitisation era [Publisher: MDPI AG Publisher: Multidisciplinary Digital Publishing Institute]. Buildings, 12(6), 858. https://doi.org/10.3390/buildings12060858

Adobor, H., & Kudonoo, E. C. (2025). Antifragility and organizations: An organizational design perspective. Leadership & Organization Development Journal. https://doi.org/10.1108/LODJ-03-2024-0185

Aven, T. (2015). Implications of black swans to the foundations and practice of risk assessment and management [Publisher: Elsevier]. Reliability Engineering & System Safety, 134, 83–91. https://doi.org/10.1016/j.ress.2014.10.004

Aven, T. (2017). A conceptual foundation for assessing and managing risk, surprises and black swans [ISSN: 2191-530X]. In The illusion of risk control: What does it take to live with uncertainty? (pp. 23–39). Springer International Publishing. https://doi.org/10.1007/978-3-319-32939-0

Axenie, C., López-Corona, O., Makridis, M. A., Akbarzadeh, M., Saveriano, M., Stancu, A., & West, J. (2024). Antifragility in complex dynamical systems [Publisher: Springer Science and Business Media LLC]. Nature Partner Journals (NPJ) Complexity, 1(12). https://doi.org/10.1038/s44260-024-00014-y

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing maturity models for IT management: A procedure model and its application [Publisher: Springer Nature]. Business & Information Systems Engineering, 1(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Bennett, N., & Lemoine, G. J. (2014). What a difference a word makes: Understanding threats to performance in a VUCA world. [Publisher: Elsevier BV]. Business Horizons, 57(3), 311–317. https://doi.org/10.2139/ssrn.2406676

Boeing, G. (2016). Visual analysis of nonlinear dynamical systems: Chaos, fractals, self-similarity and the limits of prediction [Publisher: Multidisciplinary Digital Publishing Institute]. Systems, 4(4), 37. https://doi.org/10.3390/systems4040037

Botjes, E. A., Huygh, T., Bollen, L., & Helms, R. (2026a, January 21). Cyber resilience maturity model keywords. https://doi.org/10.5281/ZENODO.18323583

Botjes, E. A., Huygh, T., Bollen, L., & Helms, R. (2026b, February 4). Open research infrastructure - CRMM. Zenodo. https://doi.org/10.5281/ZENODO.18487444

Botjes, E. A., van den Berg, M., van Gils, B., & Mulder, H. (2021). Attributes relevant to antifragile organizations. In J. P. A. Almeida, D. Bork, G. Guizzardi, M. Montali, H. A. Proper, & T. P. Sales (Eds.), 2021 IEEE 23nd conference on business informatics (CBI) (pp. 62–71, Vol. 01). IEEE. https://doi.org/10.1109/CBI52690.2021.00017

Diefenbach, T., Lucke, C., & Lechner, U. (2019). Towards an integration of information security management, risk management and enterprise architecture management – a literature review [Place: Sydney, Australia Journal Abbreviation: 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)]. 2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 326–333. https://doi.org/10.1109/CloudCom.2019.00057

Edwards, P. K., O'Mahoney, J., & Vincent, S. (2014). Studying organizations using critical realism: A practical guide (First edition, Vol. 15) [ISSN: 1476-7430 Publication Title: Journal of Critical Realism]. Oxford University Press. https://search.worldcat.org/en/title/847725011

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions [Publisher: Blackwell Publishing Ltd]. Risk Management and Insurance Review, 24(1), 93–125. https://doi.org/10.1111/rmir.12169

Gräubig, D. M., & Bley, K. (2023). A configurational set-theoretic approach to an innovation capability maturity model. AMCIS 2023 Proceedings, 13. https://aisel.aisnet.org/amcis2023/sig_scuidt/sig_scuidt/13/

Herley, C. (2016). Unfalsifiability of security claims. Proceedings of the National Academy of Sciences, 113(23), 6415–6420. https://doi.org/10.1073/pnas.1517797113

Hevner, A. R., Parsons, J., Brendel, A. B., Lukyanenko, R., Tiefenbeck, V., Tremblay, M. C., & Vom Brocke, J. (2024). Transparency in design science research. Decision Support Systems, 182, 114236. https://doi.org/10.1016/j.dss.2024.114236

Hillson, D. (2023). Beyond resilience: Towards antifragility? Continuity & Resilience Review, 5(2), 210–226. https://doi.org/10.1108/CRR-10-2022-0026

Huang, D.-L., Rau, P.-L. P., & Salvendy, G. (2010). Perception of information security [Publisher: Informa UK Limited]. Behaviour & Information Technology, 29(3), 221–232. https://doi.org/10.1080/01449290701679361

Kaleliglu, U. B. (2021). Replicability: 21st century crisis of the positivist social sciences. International Journal of New Approaches in Social Studies, 2021, 5(2), 400–425. https://doi.org/10.38015/sbyy.1003103

Lasrado, L. A. (2018). Set-theoretic approach to maturity models [Doctoral dissertation, Copenhagen Business School] [OCLC: 1175940135]. https://www.econstor.eu/bitstream/10419/209064/1/cbs-phd2018-15.pdf

Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview [Journal Abbreviation: Cyber Resilience of Systems and Networks]. In A. Kott & I. Linkov (Eds.), Cyber resilience of systems and networks (pp. 1–25, Vol. abs/1806.02852). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

Maedche, A., Elshan, E., Höhle, H., Lehrer, C., Recker, J., Sunyaev, A., Sturm, B., & Werth, O. (2024). Open science: Towards greater transparency and openness in science [Publisher: Springer Nature]. Business & Information Systems Engineering. https://doi.org/10.1007/s12599-024-00858-7

Martin-Breen, P., & Anderies, J. M. (2011). The bellagio initiative, background paper, resilience: A literature review [event-place: Brighton:IDS]. Resilience: A Literature Review. http://opendocs.ids.ac.uk/opendocs/handle/123456789/3692

Metcalf, G. S., Kijima, K., & Deguchi, H. (Eds.). (2021). Handbook of systems sciences. Springer Singapore. https://doi.org/10.1007/978- 981- 15-0720-5

Monteiro, E. L., & Maciel, R. S. P. (2020). Maturity models architecture: A large systematic mapping [Publisher: Sociedade Brasileira de Computacao - SB]. iSys - Brazilian Journal of Information Systems, 13(2), 110–140. https://doi.org/10.5753/isys.2020.761

Mullarkey, M. T., & Hevner, A. R. (2019). An elaborated action design research process model (P. Ågerfalk, Ed.) [Publisher: Informa UK Limited]. European Journal of Information Systems, 28(1), 6–20. https://doi.org/10.1080/0960085X.2018.1451811

Open Science Collaboration. (2015). Estimating the reproducibility of psychological science [Publisher: American Association for the Advancement of Science]. Science, 349(6251), aac4716. https://doi.org/10.1126/science.aac4716

Pyle, B. (2023). Knowledge generation and uncertainty in an unpredictable social world. Boston University Law Review, 103(7), 2049–2063. https://www.bu.edu/bulawreview/files/2023/12/PYLE-.pdf

Recker, J. (2021). Scientific research in information systems: A beginner's guide [ISSN: 2196-8705 Publication Title: Progress in IS]. Springer International Publishing. https://doi.org/10.1007/978-3-030-85436-2

Reeder, J. R., & Hall, T. (2021). Cybersecurity's pearl harbor moment: Lessons learned from the colonial pipeline ransomware attack. The Cyber Defense Review, 6(3), 15–40. https://www.jstor.org/stable/48631153

Schneier, B. (2008). The psychology of security [Series Title: Lecture Notes in Computer Science]. In S. Vaudenay (Ed.), Progress in cryptology –AFRICACRYPT 2008 (pp. 50–79, Vol. 5023). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-68164-9_5

Stevenson, M. T. (2023). Cause, effect, and the structure of the social world. Boston University Law Review, 103, 2001–2047. https://doi.org/10.21428/cb6ab371.77eda2fb

Taleb, N. N. (2012, November). Antifragile: Things that gain from disorder [ISSN: 1059-5422 Publication Title: Competitiveness Review: An International Business Journal]. Random House. https://doi.org/10.1108/10595421311319852

Tasheva, I., & Kunkel, I. (2022). In a hyperconnected world, is the EU cybersecurity framework connected? [Publisher: SAGE Publications]. European View, 21(2), 186–195. https://doi.org/10.1177/17816858221136106

Tsang, E. W. K., & Kwan, K.-M. (1999). Replication and theory development in organizational science: A critical realist perspective [Publisher: Academy of Management]. The Academy of Management Review, 24(4), 759. https://doi.org/10.2307/259353

Tuunanen, T., Winter, R., & Vom Brocke, J. (2024). Dealing with complexity in design science research: A methodology using design echelons. MIS Quarterly, 48(2), 427–458. https://doi.org/10.25300/MISQ/2023/16700

UNESCO & Canadian National Commission for UNESCO. (2022, November). An introduction to the UNESCO recommendation on open science. UNESCO. https://doi.org/10.54677/XOIR1696

Uppström, E. (2017). Designing, theorizing, and reflecting on information systems artifacts and value co-creation in e-government [Doctoral dissertation, Department of Computer and Systems Sciences, Stockholm University]. https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1092699&dswid=-2989

van Looy, A., Poels, G., & Snoeck, M. (2017). Evaluating business process maturity models. Journal of the Association for Information Systems, 18(6), 461–486. https://doi.org/10.17705/1jais.00460

Van Gils, B. (2023). Data in context: Models as enablers for managing and using data. Springer Nature Switzerland. https://doi.org/10.1007/978- 3-031-35539-4

Vom Brocke, J., Winter, R., Hevner, A., & Maedche, A. (2020). Special issue editorial – accumulation and evolution of design knowledge in design science research: A journey through time and space. Journal of the Association for Information Systems, 21(3), 520–544. https://doi.org/10.17705/1jais.00611

Wilkinson, M. D., Dumontier, M., Aalbersberg, I. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., Da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., . . . Mons, B. (2016). The FAIR guiding principles for scientific data management and stewardship. Scientific Data, 3(1), 160018. https://doi.org/10.1038/sdata.2016.18

About the authors

Edzo A. Botjes MSc is a PhD candidate in cyber resilience at the Open Universiteit, the Netherlands. His research interests are on how to improve business continuity and focuses on the overlap between risk management, cyber security, enterprise architecture, enterprise governance, resilience, and is specialised in antifragility. He is supervising several MSc students at the Antwerp Management School, and is an external teacher for the MSc course Enterprise Architecture at the University of Applied Sciences Utrecht. His research activities resulted in (cited) publications.

Prof.dr.ir. **Remko Helms** is a professor in Business Analytics at Open Universiteit (the Netherlands) in the Information Systems group. His teaching and research interests are mainly focused on how organizations realize value from exploring and exploiting data, including topics such as data analytics processes, data analytics strategy, data governance and analytics governance. He is supervising several Phd students and groups of master students on these topics. His work appeared in different Information Systems and Knowledge Management conferences as well as journals. He is a member of Association for Information Systems (AIS).

Dr. **Laury Bollen** is an associate professor of Information Management at the Open Universiteit, the Netherlands. He holds a PhD in Business Economics from Maastricht University. His research interest focuses on IT Governance, Information Security Governance and Platform Governance.
His research activities have resulted in publications in a broad range of international academic journals including Information & Management, the Journal of Information Systems, Information Systems Management, the Journal of Cleaner Production, the European Accounting Review, and the Journal of Business Ethics.

Dr. **Tim Huygh** is assistant professor at the department of information science at the faculty of science of the Open Universiteit, the Netherlands. He is also a visiting professor at the Antwerp Management School. He received his PhD in 2019 on IT governance from the University of Antwerp. His research interests include the governance and (strategic) management of information and technology, information security governance, and cyber resilience. His research has been published in SCI-indexed journals like Information Systems Journal (ISJ) and Decision Support Systems (DSS), and various conference proceedings including the International Conference on Information Systems (ICIS) and the Hawaii International Conference on System Sciences (HICSS). He also co-authored three books on the topic of IT governance (published by Springer). Since 2020, he is co-chairing the minitrack "IT governance and its mechanisms" at HICSS.