Applying Antifragility in Design Principles for a Cyber Resilience Maturity Model

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

In an increasingly hyperconnected world rising uncertainty threatens both business continuity and society, prompting new regulatory responses from the EU and the US. Traditional, deterministic approaches to cyber resilience which focus merely on returning to a 'status quo' state after a disruption are no longer sufficient. Instead, organizations must evolve toward antifragility: the ability to thrive and exploit opportunities emerging from chaos. Drawing on an iterative design science research methodology this study proposes a theoretically grounded framework consisting of two design goals and twelve design principles to help organizations achieve antifragility within a cyber resilience context and guide the development of future cyber resilience maturity models.

DOI
https://doi.org/10.18690/um.fov.4.2026.24

ISBN
978-961-299-152-4

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

University of Maribor Press

1 Introduction

In today's volatile, uncertain, complex, and ambiguous (VUCA) environments, organizations face unprecedented cyber threats and disruptions (Bennett & Lemoine, 2014; Saeed et al., 2023) which impact business operations, society, the global economy, and public trust (Eling et al., 2021; Reeder & Hall, 2021). Governments, including the EU and US, are addressing these challenges through cyber resilience legislation based on existing frameworks (Carroll, 2024; Tasheva & Kunkel, 2022; Vostoupal et al., 2023).

Traditional deterministic approaches to risk management and cyber security such as NIST CSF v2.0, ISO 27005, ISO 3100, NIST 800-30 and NIST 800-37 (Cerqueira Junior & Arima, 2023; NIST, 2023; Putra & Soewito, 2023; Taherdoost, 2022) are effective in complicated domains ("known unknowns") because of their reliance on checklists and static risk assessments. These frameworks are however less useful in chaotic and complex domains ("unknown unknown") because they fail to adapt to the dynamic nature of current cyber threats and emergent behavior of organizations (S. Ashby et al., 2018; Eling et al., 2021; Herley, 2016).

Predicting unknowns to protect existing value is not viable due to the infinite effort required. Organizations must instead build resilience to create value amid unforeseen disruptions (Adobor & Kudonoo, 2025; Aven, 2015a). This leads to the following **Problem Statement:** *Organizations struggle to create business value in chaotic and unpredictable contexts.* To assist organizations a Cyber Resilience Maturity Model (CRMM) may serve as a valuable tool (e.g., Imran et al., 2022; Sepúlveda Estay et al., 2020). However, despite extensive research (Botjes et al., 2026a), no existing CRMM adequately addresses the essential capability of responding to unforeseen events. In response the present paper proposes a theoretically grounded framework consisting of two design goals and twelve design principles to help organizations achieve antifragility within a cybersecurity context and guide the development of future cyber resilience maturity models. This leads to the **Research Question:** *What are the design goals and design principles for a Cyber Resilience Maturity Model (CRMM) that adequately addresses the capability to gain value in response to unforeseen events?*

To answer this question, we apply an iterative DSR approach (Section 2). We first capture the relevant theoretical constructs identified in our *diagnosis phase* (Figure 1, Section 3). In our *design objective and requirements phase* we subsequently draw on design theory to propose the design goals (Table 1) and design principles (Table 2) for such a CRMM.

2 Methodology

To enhance rigor in developing the CRMM we apply Design Science Research (DSR) throughout the CRMM lifecycle (Adekunle et al., 2022; Becker et al., 2009a). Recognizing our domain as a wicked, socio-technical problem, we follow an iterative DSR to develop our design knowledge (Vom Brocke et al., 2020) relevant to the creation of our knowledge artifact. We integrate 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 (Mullarkey & Hevner, 2019). This paper shares the results from the iteration in and between the *diagnosis phase*, and the *design objectives and requirements phase*.

Within the *diagnosis phase* we applied exploratory searches using open databases (Botjes et al., 2026b) and proprietary AI tools (OpenAI ChatGTP and Google Gemini) to identify relevant models and constructs, and in doing so refining a coherent theoretical framework for both the problem- and solution-space (Kuechler & Vaishnavi, 2008; Rivard, 2021).

We define the *design objective and requirements* of the CRMM using these two design theory principles (Gregor, 2006; Gregor & Hevner, 2013): design goals define the artifact's purpose and scope (Gregor & Jones, 2007; Walls et al., 1992) and design principles translate goals into actionable guidelines (Markus et al., 2002). Both of these principles need to be grounded in justificatory knowledge (Baskerville & Pries-Heje, 2010; Fischer et al., 2010). We ensure transparency and traceability from goals to principles (Lukyanenko & Parsons, 2020), in support of the development of new knowledge (Hevner et al., 2024; Maedche et al., 2024), which involves balancing

specificity and generality to maximize re-usability and validation (Gregor et al., 2020).

To ensure replicability, independence, precision, and falsifiability (Recker, 2021) we practice open notetaking, documenting the process, design knowledge, and contributions (Hevner et al., 2024; Maedche et al., 2024), respecting the FAIR-principles (Wilkinson et al., 2016). We used open-source tools for editing, versioning, and reference management (Botjes et al., 2026b). Furthermore, open and proprietary databases are used for the literature review. Finally, proprietary AI (OpenAI ChatGPT, Mistral La Chat and Google Gemini) are used for spelling, grammar and word-reduction.

3 Conceptual Background

3.1 Resilience

Generally, resilience refers to how long an organization takes to recover from disruptions (e.g., context changes) and restore its original function and value (Linkov & Kott, 2019). It is central to business continuity (Steen et al., 2024) because changes in context can alter the value proposition of products or services (Lusch & Nambisan, 2015). For example, negative news about a bank can shift public perception leading to rapid withdrawal of digital assets and potential insolvency (Smeets, 2021). Detailed definitions on resilience vary, e.g., prescriptive or descriptive, as one layer or as a multi layered concept, as a capacity, ability, characteristic, outcome, process, behavior, strategy, approach, or as a type of performance (Hillmann & Guenther, 2021; Hosseini et al., 2016).

We adopt Martin-Breen and Anderies (2011), who distinguishes three sub-types of resilience: (1) Engineering Resilience (which maintains both construction and function through rigorous design); (2) Systems Resilience (which preserves function while adapting construction (e.g., using backup systems)); (3) Complex Adaptive Systems (CAS) Resilience (whichenables changes in both function and construction, by empowering autonomy and mastery). For cyber resilience all three sub-types are relevant, whereas traditional cyber resilience frameworks incorporate only the first two types of resilience.

3.2 Cyber Resilience

Digital transformation has made cyber resilience critical for all organizational stakeholders (Caon et al., 2025). This urgency stems from: (1) rising global cyber incident frequency (Dupont et al., 2023); (2) increasing threats to business continuity (Eling et al., 2021); (3) expanding global and regional regulations (Chiara, 2022; IMF, 2024; Tasheva & Kunkel, 2022; The World Bank, 2023; Vostoupal et al., 2023), which now address cyber resilience across product life-cycles and supply chains; and (4) the evolution of security, from physical, infrastructure, operational, information security to cybersecurity into cyber resilience at the overlap of enterprise risk management and business continuity (Eling et al., 2021; Linkov & Kott, 2019; Munusamy & Khodadi, 2023; Tzavara & Vassiliadis, 2024). Cyber resilience involves managing the complexity of socio-technical and cyber-physical systems, particularly the dynamic interplay between human and machine (Alrumaih et al., 2023; Belinski et al., 2020; Dupont et al., 2023), aimed to uphold business continuity by addressing the organization and its environment (Eling et al., 2021).

3.3 Cyber Resilience Frameworks

Traditional cyber resilience frameworks aim to identify risks and mitigate their negative impact on people, processes, and technology by using Engineering and Systems Resilience to absorb (internal and external) disruptions and restore original functions (Bharathy & McShane, 2014; Hosseini et al., 2016; Ruiz-Martín et al., 2018). However, risk events are inherently unpredictable, subjective, and too numerous to manage comprehensively (Aven, 2015a; 2018; Derbyshire & Wright, 2014; Eling et al., 2021; Fjaeran & Aven, 2021) due to nonlinear dynamic behavior (Boeing, 2016; Lorenz, 1963), knowledge gaps (Heylighen, 2002; Raviv et al., 2022), and black swan events that lie beyond current imagination (Thekdi & Aven, 2024). This means risk events are in the chaotic and complex ("unknown unknown") domain. According to the law of requisite variety (W. R. Ashby, 1958; Beer, 1974), the vast variety of risk events to be absorbed in our hyper-connected, nonlinear dynamic reality, renders traditional risk management approaches and frameworks impractical, resource-intensive, and fundamentally non-viable.

CAS Resilience introduces a proactive dimension to cyber resilience. By increasing internal variety through the adaptation of function and structure it empowers organizations to seize new opportunities and deliver greater value (Axenie et al., 2024; Martin-Breen & Anderies, 2011). It leverages the adaptive cycle of exploitation, conservation, release, reorganization and exploration, driving continuous evolution (Walker et al., 2004; Sundstrom & Allen, 2019). Proactive risk management enables organizations to identify and capitalize on upside risks (Aven, 2015b; Florea & Florea, 2016). By maximizing the frequency of exploitation and exploration cycles organizations can better handle the "unknown unknowns", thereby fostering antifragility.

3.4 Antifragility

Antifragility, introduced by Taleb (2012), goes beyond resilience by enabling systems to thrive in unpredictable environments and creating value in new realities (Adobor, 2024; Sagala & Őri, 2024). It optimizes conditions to trigger CAS Resilience, enabling organizations to adapt and capitalize on unforeseen events through learning (Axenie et al., 2024; Johnson & Gheorghe, 2013). Antifragility ensures organizations remain relevant to stakeholders by adapting their value propositions and internal structures (Adobor & Kudonoo, 2025; Parmar et al., 2010; Spitz & Desbiey, 2025). Given the dynamic internal and external contexts organizations operate in, cyber resilience must integrate antifragility to address the unexpected and sustain business continuity.

3.5 Sensemaking

Because of the continuous change in and around organizations, sensemaking is essential for building resilience (Bennett & Lemoine, 2014; Weick et al., 2005). Sensemaking is the process of interpreting reality between subjective and objective perspectives (Mukumbang et al., 2023; Mutch, 2010). Sensemaking guides decision-making in ambiguous contexts, helping organizations navigate uncertainty and adapt their actions effectively (Snowden, 2005; Thompson, 1995; Weick, 1995). It enables organizations to achieve sustainable competitive advantages through organizational learning and by creating, acquiring and integrating knowledge (Alashwal et al., 2017; Al-Shehab et al., 2005).

3.6 Organizational Learning

Managing uncertainty is the core objective of enterprise risk management, business continuity management, and cyber resilience. To achieve this, organizational learning must be embedded in cyber resilience from the boardroom down to the operational level (Dupont et al., 2023; Park et al., 2013). This process relies on continuous sensemaking by translating observations into actionable strategies and leveraging feedback loops to foster flexibility, improvement, and self-healing (Argyris & Schön, 1978; Huang et al., 2022; Nonaka & Takeuchi, 1995).

Organizational learning operates in two complementary domains: (1) empirical realism, where knowledge is treated as objective, and (2) social constructivism, where shared understanding emerges through interaction (Brøns Kringelum & Brix, 2021). For a cyber resilience maturity model to be effective it must address both the knowledge itself and the social interactions required to create collectively understood knowledge and integrate it across the organization (Belinski et al., 2020; Raviv et al., 2022).

3.7 Maturity Models

Maturity models are ubiquitous across business and academia, numbering in the hundreds (Becker et al., 2009a; Monteiro & Maciel, 2020; Wendler, 2012). Maturity Models serve as a structured approach to sensemaking and as a knowledge artifact and they aid practitioners, expert groups, and scholars in achieving excellence, fostering collective expertise, and developing theories (Buckle, 2018; Oltra-Rodríguez et al., 2025). They define discrete maturity levels that represent qualitative and quantitative stages of progression for a defined class of objects, e.g., increasing organizational capability within a specific context (Becker et al., 2009a; Lasrado, 2018; Wendler, 2012).

Maturity models typically include: [a] levels (usually 3-6), [b] descriptions of each level, [c] number of dimensions, [d] factors for each dimension, and [e] performance descriptions for activities/elements at each level (Becker et al., 2009a). They are constructed as either staged fixed-level models, continuous fixed-level models, focus area models, or set-theoretic approach for maturity models (Monteiro & Maciel, 2020; Adekunle et al., 2022). As summarized by Lasrado (2018, p. 23): "[maturity

assessment models] represent theories about how organizational capabilities evolve in a stage-by-stage manner along an anticipated, desired, or logical maturation path".

At their core, maturity models assume that a desired future state (normative/prescriptive) can be achieved by effectively applying knowledge and following identified improvement steps from the current state (descriptive) (Kazanjian & Drazin, 1989; Pullen, 2007; Solli-Sæther & Gottschalk, 2010). In this way, they aim to support organizational development, process improvement, and benchmarking (internal or external) of the object under study. However, their effectiveness and ability to fulfill their intended purpose remain contentious (Adekunle et al., 2022; Buckle, 2018). Critiques often highlight challenges in generalization and validation, particularly in VUCA contexts (i.e., wicked problem) where rigor in design and validation is difficult to achieve (Adekunle et al., 2022; Becker et al., 2009b).

3.8 Conceptual Model

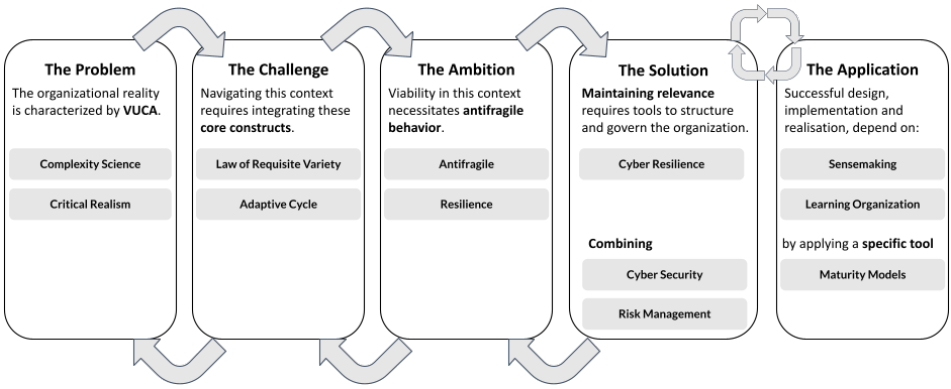

Figure 1: Conceptual model

Navigating within VUCA environments constitutes a wicked socio-technical problem that necessitates a deep understanding of the dynamic interplay between humans, machines, and their broader environment. Before formulating specific design guidelines it is essential to synthesize the theoretical foundations into a coherent structure that encompasses both the problem and solution spaces. Through the iterative exploration of these spaces during the *diagnosis phase* we developed a conceptual model (Figure 1) incorporating the core constructs

previously discussed. This model serves as a logical bridge to the design process: it informs the design goals and design principles of the proposed Cyber Resilience Maturity Model (CRMM) and establishes the foundation for the subsequent *design objectives and requirements phase*.

4 Design Goals and Principles

To answer our research question during the *diagnosis phase* we elicited the relevant constructs as part of a conceptual model (Figure 1, Section 3) of the problem and solution space. During the *design objectives and requirements phase* we formulate two design goals as design objective (Table 1), and 12 actionable design principles as requirements (Table 2) following the prescribed syntax.

4.1 Design Goals

Business continuity is not only about sustaining operations but also about maintaining relevance to all stakeholders. In complex environments static stability leads to obsolescence. Thus, organizations must dynamically adjust to preserve their relevance (e.g., Eling et al., 2021; Reeder and Hall, 2021; Saeed et al., 2023; Snowden, 2005). This we capture in Design Goal 01 (DG 01).

Reactive adaptation alone is insufficient for long-term survival. Organizations must convert volatility into value to remain relevant. In a context of continuous chaos the capacity to derive value from disorder requires antifragile behavior (e.g., Adobor, 2024; Axenie et al., 2024; Johnson and Gheorghe, 2013; Sagala and Őri, 2024). To stipulate this we formulated Design Goal 02 (DG 02).

Table 1: Design Goals

DG 01.	Support organizations in staying relevant for all stakeholders by adapting to change to ensure business continuity. *e.g., Eling et al., 2021; Reeder and Hall, 2021; Saeed et al., 2023; Snowden, 2005*
DG 02.	Support organizations in achieving antifragile behavior: to derive business value from the continuous chaos in and around them. *e.g., Adobor, 2024; Axenie et al., 2024; Johnson and Gheorghe, 2013; Sagala and Őri, 2024*

4.2 Design Principles

Design principles on supporting the user to envision how to uphold business continuity

Cyber resilience, just like cyber security and risk management, aims to preserve business continuity. This is why the first design principles are generic, defining the general function of the CRMM. Business continuity relies on managing known risks ("known unknowns", DP 01) while acknowledging the boundaries of our knowledge ("unknown unknowns", DP 02) (e.g., S. Ashby et al., 2018; Metcalf et al., 2021; Snowden, 2005; Spitz and Desbiey, 2025; Taleb, 2012; Weick et al., 2005). These domains contrast with the baseline of "known knowns". By recognizing the limits of what we know we mitigate the fragility that arises from false certainty. Upholding business continuity starts with preparing the organization to deal with these two domains. How the risks can be identified and converted into action is addressed in more detail in the other design principles.

Design principles on supporting the user in conserving the current situation

One way to maintain business continuity is to preserve the current situation. Engineering Resilience, Systems Resilience, and standard risk management frameworks (including cybersecurity) focus on identifying risks (DP 03) and protecting against negative impacts (DP 04) (e.g., Aven, 2018; Dupont et al., 2023; Eling et al., 2021; Florea and Florea, 2016; Mizrak, 2023). This approach aims to attenuate variety and aligns with the conservation phase of the adaptive cycle.

Design principles on supporting the user in improving the current situation

Value creation requires mechanisms for exploration, reorganization, and the exploitation phases of the adaptive cycle. This involves exploring upside risk and opportunities (DP 05) and capitalizing on them (DP 06), amplifying variety to enable Complex Adaptive Systems (CAS) Resilience (e.g., Adobor and Kudonoo, 2025; Sundstrom and Allen, 2019; Walker et al., 2004).

Design principles on supporting the user in improving sensemaking

Central to all design principles is the requirement for user agency and emancipation, specifically empowering individuals to determine their actions (DP 07) (e.g., Bennett and Lemoine, 2014; Mutch, 2010; Weick et al., 2005). However, in socially interconnected organizations individual agency must align with coordinated collaboration (DP 08) (e.g., Dupont et al., 2023; Snowden, 2005; Thompson, 1995). Through collective coordination, organizations can intentionally reshape their context (DP 09), enabling double-loop organizational learning and structural adaptation (e.g., Adekunle et al., 2022; Brøns Kringelum and Brix, 2021; Lasrado, 2018).

Design principles on supporting the user in improving learning

Learning includes an increased understanding of the interplay between objective reality (empirical realism) and inter-subjective reality (social constructivism). These perspectives define the scope of both the individual user's practice of personal mastery (DP 10) (e.g., Belinski et al., 2020; Brøns Kringelum and Brix, 2021; Raviv et al., 2022) as well as the team's learning discipline (DP 11) (e.g, Belinski et al., 2020; Brøns Kringelum and Brix, 2021; Raviv et al., 2022).

Design principles on supporting the user in becoming antifragile

The cultivation of learning disciplines relies on the response to volatility. While Engineering and Systems Resilience seek to resist shocks and CAS Resilience aims to adapt, antifragility extends these capacities to gain value from disorder and stress. Because novelty resides in the unknown, shielding individuals from exposure leads to systemic fragility. Therefore, to transition from surviving to thriving, individuals need support in their transition from acknowledging (DP 02) to actively embracing exposure to the unknown (DP 12) (e.g., Beer, 1974; Sundstrom and Allen, 2019; Taleb, 2012). This engagement with volatility generates learning signals, which increase the opportunities of exploiting opportunities, and consequently securing the upside of uncertainty.

Table 2: Design Principles

	Design principles on supporting the user to envision how to uphold business continuity
DP 01	Support individuals (actors) to determine how to prepare their organization (users) to uphold business continuity (aim) when their organization is confronted with known unknown events (context). *e.g., S. Ashby et al., 2018; Metcalf et al., 2021; Snowden, 2005; Weick et al., 2005*
DP 02	Support individuals (actors) to determine how to prepare their organization (actors) to uphold business continuity (aim) when their organization is confronted with unknown unknown events (context). *e.g., Metcalf et al., 2021; Snowden, 2005; Spitz and Desbiey, 2025; Taleb, 2012*
	Design principles on supporting the user in conserving the current situation
DP 03	Support individuals (actors) to uphold business continuity by identifying downside risks, also known as known threats, (aim) of their organization (user). *e.g., Aven, 2018; Dupont et al., 2023; Florea and Florea, 2016*
DP 04	Support individuals (actors) to limit the negative impact of materialized threats, also known as risk events, on people, process and technology (aim) of their organization (user). *e.g., Eling et al., 2021; Mizrak, 2023*
	Design principles on supporting the user in improving the current situation
DP 05	Support individuals (actors) to uphold business continuity by identifying upside risks, also known as known opportunities, (aim) of their organization (user). *e.g., Sundstrom and Allen, 2019; Walker et al., 2004*
DP 06	Support individuals (actors) in exploiting opportunities, as changing the function and construction of a system to optimize the value proposition in a new reality (aim), in their organization (user). *e.g., Adobor and Kudonoo, 2025; Sundstrom and Allen, 2019; Walker et al., 2004*
	Design principles on supporting the user in improving sensemaking
DP 07	Support individuals (actor, user) in their sensemaking to determine their next action (aim). *e.g., Bennett and Lemoine, 2014; Mutch, 2010; Weick et al., 2005*
DP 08	Support individuals (actors) in their sensemaking to determine their next action (aim) as part of their organization (user). *e.g., Dupont et al., 2023; Snowden, 2005; Thompson, 1995*
DP 09	Support individuals (actors) to determine the growth-path from the current state to a desired state (aim) of their organization (user). *e.g., Adekunle et al., 2022; Brøns Kringelum and Brix, 2021; Lasrado, 2018*
	Design principles on supporting the user in improving learning
DP 10	Support individuals (actor, users) in their learning (aim) from an empirical realist and a social constructivist viewpoint (mechanism). *e.g., Belinski et al., 2020; Brøns Kringelum and Brix, 2021; Raviv et al., 2022*
DP 11	Support individuals (actors) as part of the group (user), in their organizational learning (aim) from an empirical realist and a social constructivist viewpoint (mechanism). *e.g., Belinski et al., 2020; Brøns Kringelum and Brix, 2021; Raviv et al., 2022*
	Design principles on supporting the user in becoming antifragile
DP 12	Support individuals (actors) as part of an organization (user) in embracing exposure to the unknown to increase the possibilities of exploiting opportunities and learning (aim). *e.g., Beer, 1974; Sundstrom and Allen, 2019; Taleb, 2012*

Collectively these design principles address the reduction of fragility (by acknowledging the unknown), the improvement of resilience (by limiting the impact of the unknown), adaption (by navigating the unknown) and the achievement of antifragility (feeding on the unknown); these are summarized below in Table 2.

5 Conclusion, Discussion, and Future Research

Stakeholders in the cyber resilience domain require a sensemaking artifact to navigate complexity. Existing frameworks and models in cyber resilience and related fields (such as risk management and cybersecurity) focus primarily on risk prediction and mitigation, but they often overlook organizational learning and value creation. Consequently, these frameworks and models fail to foster antifragility, as they do not account for the potential to grow from disruptions. This mismatch leaves stakeholders ill-equipped to address the VUCA nature of their environments. This requires new cyber resilience artifacts (e.g., maturity models) for which we proposed design goals (Table 1) and design principles (Table 2) in our research.

The design goals and principles are intentionally generic to ensure a broad applicability across domains such as cybersecurity, business continuity, risk management, and enterprise governance. This high-level approach addresses a common critique of specific knowledge artifacts (such as rigid risk processes) which lose value when the organizational context shifts. By prioritizing generic principles before building specific artifacts we ensure the model remains relevant across diverse environments. This generic approach fits the statement variety eats variety from the law of requisite variety (Figure 1). The design goals and design principles therefore support the actors and users during their iterations of the adaptive cycle phases, enabling them to absorb the shifting variety within both internal and external organizational contexts.

The practical implication of this approach is that the model that results from the suggested design principles should be agnostic to changes in the (shared) reality of what individuals perceive as real and should even support these changes. The set of design goals and principles also affects existing risk management and cybersecurity frameworks since none of the existing frameworks meets all these requirements. Therefore, these frameworks are fragile in the face of changes in context and changes within the user and actors.

A key limitation of our research is the lack of empirical validation. We have not yet interviewed various experts and practitioners to validate the proposed design goals and principles. In future research we will attempt to validate the design goals and principles with experts. Additionally we will continue our literature review to catalog relevant cyber resilience frameworks in an open database, combined with insights into their coverage of our proposed design principles. Furthermore we seek to foster collaboration on this database among researchers and practitioners in the cyber security and risk management domains with the goal of creating a validated dataset and an openly available body of knowledge. Concurrently, we will develop a new Cyber Resilience Maturity Model (CRMM) to validate the operationalization of the validated design principles.

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. (2024). How organizations can benefit from volatility: The promise of antifragility and some cautionary notes. Organizational Dynamics, 101098. https://doi.org/10.1016/j.orgdyn.2024.101098

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

Alashwal, A. M., Abdul-Rahman, H., & Asef, A. (2017). Influence of organizational learning and firm size on risk management maturity [Publisher: American Society of Civil Engineers (ASCE)]. Journal of Management in Engineering, 33(6), 04017034. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000553

Alrumaih, T. N., Alenazi, M. J., AlSowaygh, N. A., Humayed, A. A., & Alablani, I. A. (2023). Cyber resilience in industrial networks: A state of the art, challenges, and future directions [Publisher: Elsevier BV]. Journal of King Saud University - Computer and Information Sciences, 35(9), 101781. https://doi.org/10.1016/j.jksuci.2023.101781

Al-Shehab, A. J., Hughes, R. T., & Winstanley, G. (2005). Facilitating organisational learning through causal mapping techniques in IS/IT project risk management [ISSN: 0302-9743 Journal Abbreviation: Wissensmanagement]. In K.-D. Althoff, A. Dengel, R. Bergmann, M. Nick, & T. Roth-Berghofer (Eds.), Professional knowledge management (pp. 145–154, Vol. 3782). Springer Berlin Heidelberg. https://doi.org/10.1007/11590019_18

Argyris, C., & Schön, D. A. (1978). Organizational learning: A theory of action perspective. Addison-Wesley.

Ashby, S., Buck, T., Nöth-Zahn, S., & Peisl, T. (2018). Emerging IT risks: Insights from german banking [Publisher: Springer Science and Business Media LLC]. The Geneva Papers on Risk and Insurance – Issues and Practice, 43(2), 180–207. https://doi.org/10.1057/s41288-018-0081-8

Ashby, W. R. (1958). Requisite variety and its implications for the control of complex systems [ISBN: 978-1489907202 Publisher: Springer US]. Cybernetica, 1(2), 83–99. https://doi.org/10.1007/978-1-4899-0718-9_28

Aven, T. (2015a). 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. (2015b). The concept of antifragility and its implications for the practice of risk analysis [Publisher: Wiley]. Risk Analysis, 35(3), 476–483. https://doi.org/10.1111/risa.12279

Aven, T. (2018). The call for a shift from risk to resilience: What does it mean? [Publisher: Wiley]. Risk Analysis, 39(6), risa.13247. https://doi.org/10.1111/risa.13247

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

Baskerville, R., & Pries-Heje, J. (2010). Explanatory design theory. Business & Information Systems Engineering, 2(5), 271–282. https://doi.org/10.1007/s12599-010-0118-4

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009a). 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

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009b). Entwicklung von Reifegradmodellen für das IT-Management: Vorgehensmodell und praktische Anwendung [Publisher: Springer Nature]. WIRTSCHAFTSINFORMATIK, 51(3), 249–260. https://doi.org/10.1007/s11576-009-0167-9 Beer, S. (1974, January). Designing freedom (Vol. 27) [ISSN: 0030-3623 Publication Title: Operational Research Quarterly (1970-1977)]. John Wiley & Sons. https://doi.org/10.2307/3008834

Belinski, R., Peixe, A. M., Frederico, G. F., & Garza-Reyes, J. A. (2020). Organizational learning and industry 4.0: Findings from a systematic literature review and research agenda [Publisher: Emerald]. Benchmarking: An International Journal, 27(8), 2435–2457. https://doi.org/10.1108/bij-04-2020-0158

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

Bharathy, G. K., & McShane, M. K. (2014). Applying a systems model to enterprise risk management [Publisher: RELX Group (Netherlands)]. Engineering Management Journal, 26, 38–46. https://doi.org/10.1080/10429247.2014.11432027

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

Brøns Kringelum, L., & Brix, J. (2021). Critical realism and organizational learning [Publisher: Emerald Publishing Limited]. The Learning Organization, 28(1), 32–45. https://doi.org/10.1108/TLO-03-2020-0035

Buckle, P. (2018). Maturity models for systems thinking [Publisher: MDPI AG]. Systems, 6(2), 23. https://doi.org/10.3390/systems6020023

Caon, M., Panetti, E., Meier, E., & Baldegger, R. J. (2025). The dual effect of COVID-19: Diverse digitalization approaches in micro- and small businesses. Journal of the International Council for Small Business, 6(2), 216–228. https://doi.org/10.1080/26437015.2024.2404184

Carroll, J. (2024). The u.s. national cybersecurity strategy: A vehicle with an international journey [Publisher: Academic Conferences International Ltd]. European Conference on Cyber Warfare and Security, 23(1), 107–115. https://doi.org/10.34190/eccws.23.1.2300

Cerqueira Junior, A. S., & Arima, C. H. (2023). Cyber risk management and ISO 27005 applied in organizations: A systematic literature review [Publisher: Faculdade Novo Milênio]. REVISTA FOCO, 16(2), e1188. https://doi.org/10.54751/revistafoco.v16n2-215

Chiara, P. G. (2022). The cyber resilience act: The EU commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. International Cybersecurity Law Review, 3(2), 255–272. https://doi.org/10.1365/s43439-022-00067-6

Derbyshire, J., & Wright, G. (2014). Preparing for the future: Development of an 'antifragile' methodology that complements scenario planning by omitting causation. [Publisher: Elsevier BV]. Technological Forecasting and Social Change, 82, 215–225. https://doi.org/10.1016/j.techfore. 2013.07.001

Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers & Security, 132, 103372. https://doi.org/10.1016/j.cose.2023.103372

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

Fischer, C., Winter, R., & Wortmann, F. (2010). Design theory. Business & Information Systems Engineering, 2(6), 387–390. https://doi.org/10.1007/s12599-010-0128-2

Fjaeran, L., & Aven, T. (2021). Creating conditions for critical trust – how an uncertainty-based risk perspective relates to dimensions and types of trust [Publisher: Elsevier BV]. Safety Science, 133, 105008. https://doi.org/10.1016/j.ssci.2020.105008

Florea, R., & Florea, R. (2016). Internal audit and risk management. ISO 31000 and ERM approaches. Economy Transdisciplinarity Cognition, 19(1), 72–77. https : / / www. ugb . ro / etc / etc2016no1 / 13 _ Florea _Radu__Florea_Ramona.PDF

Gregor, S. (2006). The nature of theory in information systems. MIS Quarterly, 30(3), 611–642. https://doi.org/10.2307/25148742

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS Quarterly, 37(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. Journal of the Association for Information Systems, 8(5), 312–335. https://doi.org/10.17705/1jais.00129

Gregor, S., Kruse, L., & Seidel, S. (2020). Research perspectives: The anatomy of a design principle. Journal of the Association for Information Systems, 21, 1622–1652. https://doi.org/10.17705/1jais.00649

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

Heylighen, F. (2002). The science of self-organization and adaptivity. In L. D. Kiel (Ed.), Knowledge management, organizational intelligence and learning, and complexity. (Vol. 3). EOLSS Publishers Co Ltd. https://researchportal.vub.be/en/publications/the- science- of- self-organization-and-adaptivity

Hillmann, J., & Guenther, E. (2021). Organizational resilience: A valuable construct for management research? International Journal of Management Reviews, 23(1), 7–44. https://doi.org/10.1111/ijmr.12239

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience [Publisher: Elsevier BV]. Reliability Engineering & System Safety, 145, 47–61. https://doi.org/10.1016/j.ress.2015.08.006

Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement learning for feedback-enabled cyber resilience [Publisher: Elsevier BV]. Annual 20 Reviews in Control, 53, 273–295. https://doi.org/10.1016/j.arcontrol.2022.01.001

IMF. (2024, April). Cyber risk: A growing concern for macrofinancial stability (chapter 3). In Global financial stability report, april 2024: The last mile: Financial vulnerabilities and risks (p. 26). International Monetary Fund. https://doi.org/10.5089/9798400257704.082

Imran, H., Salama, M., Turner, C., & Fattah, S. (2022). Cybersecurity risk management frameworks in the oil and gas sector: A systematic literature review [ISSN: 2367-3389 Series Title: Lecture Notes in Networks and Systems]. In K. Arai (Ed.), Advances in information and communication (pp. 871–894, Vol. 439). Springer International Publishing. https://doi.org/10.1007/978-3-030-98015-3_59

Johnson, J., & Gheorghe, A. V. (2013). Antifragility analysis and measurement framework for systems of systems [Publisher: Springer Science and Business Media LLC]. International Journal of Disaster Risk Science, 4(4), 159–168. https://doi.org/10.1007/s13753-013-0017-7

Kazanjian, R. K., & Drazin, R. (1989). An empirical test of a stage of growth progression model. Management Science, 35(12), 1489–1503. https://doi.org/10.1287/mnsc.35.12.1489

Kuechler, B., & Vaishnavi, V. (2008). On theory development in design science research: Anatomy of a research project. European Journal of Information Systems, 17(5), 489–504. https://doi.org/10.1057/ejis.2008.40

Lasrado, L. A. (2018). Set-theoretic approach to maturity models [Doctoral dissertation, Copenhagen Business School] [ISSN:0906-6934 OCLC: 1175940135 ISBN: 978-87-93579-77-4, 978-87-93579-76-7]. 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

Lorenz, E. N. (1963). Deterministic nonperiodic flow [Publisher: American Meteorological Society]. Journal of the atmospheric sciences, 20(2), 130–141. https://journals.ametsoc.org/downloadpdf/journals/atsc/20/2/1520-0469_1963_020_0130_dnf_2_0_co_2.pdf

Lukyanenko, R., & Parsons, J. (2020). Research perspectives: Design theory indeterminacy: What is it, how can it be reduced, and why did the polar bear drown? Journal of the Association for Information Systems, 21(5), 1343–1369. https://doi.org/10.17705/1jais.00639

Lusch, R. F., & Nambisan, S. (2015). Service innovation: A service-dominant logic perspective. MIS Quarterly, 39(1), 155–175. https://doi.org/10.25300/MISQ/2015/39.1.07

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

Markus, M. L., Majchrzak, A., & Gasser, L. (2002). A design theory for systems that support emergent knowledge processes. MIS Quarterly, 26(3), 179–212. https://aisel.aisnet.org/misq/vol26/iss3/4/

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

Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. Pressacademia, 3. https://doi.org/10.17261/Pressacademia.2023.1807

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

Mukumbang, F. C., De Souza, D. E., & Eastwood, J. G. (2023). The contributions of scientific realism and critical realism to realist evaluation [Publisher: Taylor & Francis]. Journal of Critical Realism, 22(3), 504–524. https://doi.org/10.1080/14767430.2023.2217052

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

Munusamy, T., & Khodadi, T. (2023). Building cyber resilience: Key factors for enhancing organizational cyber security [Publisher: Multimedia University]. Journal of Informatics and Web Engineering, 2(2), 59–71. https://doi.org/10.33093/jiwe.2023.2.2.5

Mutch, A. (2010). Technology, organization, and structure—a morphogenetic approach [Publisher: Institute for Operations Research and the Management Sciences (INFORMS)]. Organization science, 21(2), 507–520.

NIST. (2023, August 8). The NIST cybersecurity framework 2.0 (NIST CSWP 29 ipd) (Author long name: National Institute of Standards and Technology; Backup Publisher: National Institute of Standards and Technology). NIST. Gaithersburg, MD. https://doi.org/10.6028/NIST.CSWP.29.ipd

Nonaka, I., & Takeuchi, H. (1995). The knowledge-creating company. How japanese companies create the dynamics of innovation. Oxford University Press.

Oltra-Rodríguez, M. A., Stonehouse, P., Afonso-Alonso, N., & Holgado-Terriza, J. A. (2025). Disciplined delivery and organizational design maturity: A socio-technical evolutionary journey. Systems, 13(5), 374. https://doi.org/10.3390/systems13050374

Park, J., Seager, T. P., Rao, P. S. C., Rao, P. S. C., Rao, P. S. C., Rao, P. S. C., Convertino, M., Linkov, I., Linkov, I., Linkov, I., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems [Publisher: Wiley]. Risk Analysis, 33(3), 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x

Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., & De Colle, S. (2010). Stakeholder theory: The State of the Art [Publisher: Routledge]. Academy of Management Annals, 4(1), 403–445. https://doi.org/10.5465/19416520.2010.495581

Pullen, W. (2007). A public sector HPT maturity model. Performance Improvement, 46(4), 9–15. https://doi.org/10.1002/pfi.119

Putra, A. P., & Soewito, B. (2023). Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector [Publisher: Science and Information Organization]. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/IJACSA.2023.0140468

Raviv, L., Lupyan, G., & Green, S. C. (2022). How variability shapes learning and generalization [Publisher: Elsevier BV]. Trends in Cognitive Sciences, 26(6), 462–483. https://doi.org/10.1016/j.tics.2022.03.007

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

Rivard, S. (2021). Theory building is neither an art nor a science. it is a craft. Journal of Information Technology, 36(3), 316–328. https://doi.org/10.1177/0268396220911938

Ruiz-Martín, C., Lopez-Paredes, A., & Wainer, G. (2018). What we know and do not know about organizational resilience [Publisher: Universitat Politecnica de Valencia]. International Journal of Production Management and Engineering, 6(1), 11 https://doi.org/10.4995/ijpme.2018.7898

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23(15), 6666. https://doi.org/10.3390/s23156666

Sagala, G. H., & Őri, D. (2024). Antifragility, resilience and collaborative networks of SMEs: A theoretical foundation [Publisher: Emerald Publishing Limited]. European Journal of Innovation Management. https://doi.org/10.1108/EJIM-09-2023-0797

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks [Publisher: Elsevier BV]. Computers & Security, 97, 101996. https://doi.org/10.1016/j.cose.2020.101996

Smeets, M. E. (2021, August). Fear drop and fear change. perceptions of security in the 21st century: Their formation, trends, and impact in society [Doctoral dissertation, University of Cardiff].

Snowden, D. (2005). Strategy in the context of uncertainty [Publisher: Emerald]. Handbook of Business Strategy, 6(1), 47–54. https://doi.org/10.1108/08944310510556955

Solli-Sæther, H., & Gottschalk, P. (2010). The modeling process for stage models [Publisher: Taylor & Francis]. Journal of Organizational Computing and Electronic Commerce, 20(3), 279–293. https://doi.org/10.1080/10919392.2010.494535

Spitz, R., & Desbiey, O. (2025). The future of risk and insurability in the era of systemic disruption, unpredictability and artificial intelligence. The Journal of Operational Risk. https://doi.org/10.21314/JOP.2025.003

Steen, R., Haug, O. J., & Patriarca, R. (2024). Business continuity and resilience management: A conceptual framework. Journal of Contingencies and Crisis Management, 32(1), e12501. https://doi.org/10.1111/1468-5973.12501

Sundstrom, S. M., & Allen, C. R. (2019). The adaptive cycle: More than a metaphor. Ecological Complexity, 39, 100767. https://doi.org/10.1016/j.ecocom.2019.100767

Taherdoost, H. (2022). Cybersecurity vs. information security [Publisher: Elsevier BV]. Procedia Computer Science, 215, 483–487. https://doi.org/10.1016/j.procs.2022.12.050

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

The World Bank. (2023, June). Sectoral cybersecurity maturity model (SCMM). Worldbank. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099062623085028392/p17263707c36b702309f7303dbb7266e1cf

Thekdi, S., & Aven, T. (2024, October 7). Decoding black swans and other historic risk events: Themes of progress and opportunity for risk science (1st ed.). CRC Press. https://doi.org/10.1201/9781003437031

Thompson, F. (1995). Business strategy and the boyd cycle [Publisher: Wiley]. Journal of Contingencies and Crisis Management, 3(2), 81–90. https://doi.org/10.1111/j.1468-5973.1995.tb00060.x

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

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review [Publisher: Springer Science and Business Media LLC]. International Journal of Information Security, 23(3), 1695–1719. https://doi.org/10.1007/s10207-023-00811-x

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

Vostoupal, J., Stupka, V., Harašta, J., Kasl, F., Loutocký, P., & Malinka, K. (2023). The legal aspects of cybersecurity vulnerability disclosure: To the NIS 2 and beyond. https://doi.org/10.2139/ssrn.4640775

Walker, B. H., Holling, C. S., Carpenter, S. R., & Kinzig, A. (2004). Resilience, adaptability and transformability in social–ecological systems [Publisher: The Resilience Alliance]. Ecology and society, 9(2).

Walls, J. G., Widmeyer, G. R., & Sawy, O. A. E. (1992). Building an information system design theory for vigilant EIS. Information Systems Research, 3(1), 36–59. http://www.jstor.org/stable/23010780

Weick, K. E. (1995). Sensemaking in organizations. Sage Publications.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. Organization Science, 16(4), 409–421. https://doi.org/10.1287/orsc.1050.0133

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study [Publisher: Elsevier BV]. Information and Software Technology, 54(12), 1317–1339. https://doi.org/10.1016/j.infsof.2012.07.007

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.