Adopting Agile in Cybersecurity

Petra Maria Asprion[1], Bettina Schneider[1], Patrick Consonni[1]
[1]University of Applied Sciences and Arts Northwestern Switzerland FHNW

petra.asprion@fhnw.ch, bettina.schneider@fhnw.ch, patrick.consonni@students.fhnw.ch

Abstract. The study underscores the growing applicability of agile principles beyond traditional software development, noting their relevance in diverse projects and industries. It suggests that cybersecurity management stands to benefit from agile methodologies due to their adaptability to evolving threats and internal challenges. As a result of this research, the 'M&RA Model' was developed as a readiness assessment tool for the adoption of agile in cybersecurity. The model comprises two steps - assessing cybersecurity maturity ('MA Model') and readiness for agile ('RA Model'). It was developed by analyzing established frameworks and guidelines for both agile and cybersecurity. Through iterative evaluation and refinement, informed by qualitative input from subject matter experts obtained via brainstorming sessions and semi-structured interviews, the model evolved to enhance cybersecurity practices within agile principles and methodologies. This approach aligns with design science methodology, ensuring the model's relevance and effectiveness in addressing contemporary cybersecurity challenges.

Keywords: Cybersecurity, Agile, Maturity, Readiness Assessment.

1 Relevance

Cybersecurity programs are crucial for safeguarding against data breaches and minimizing among others financial and reputational damage [1] (Donaldson et al., 2018). According to [2] WEF (2024), the global cost of cybercrime will rise (forecast) to $23.84 trillion by 2027, highlighting the urgency for efficient cyber defense strategies and related programs within organizations[1].

Cybersecurity related standards and frameworks provide valuable guidance to govern and manage cybersecurity but often rely on traditional project management methodologies [3] [4]. Traditional, mainly linear project and process management in cybersecurity hinder adaptability and flexibility, driving the need for more agile approaches [5] [6]. Agile principles and methodologies offer here a solution to cybersecurity challenges by emphasizing iterative, collaborative, and adaptive approaches [7] [8]. However, before adopting agile principles and methodologies, it's vital to assess an organization's readiness, considering the current cybersecurity program and familiarity with

[1] We used the term organizations as an umbrella term for profit and non-profit organizations, enterprises, companies, authorities, or other forms of organization.

Smuts, Hanlie & Hinkelmann, Knut (2024). Proceedings of the 4th Conference Society 5.0 - Innovation for Sustainable and Inclusive Social Good, Volume 2, Mauritius, 26-28 June 2024,
DOI: 10.5281/zenodo.11612759
DOI: 10.5281/zenodo.11658198

agile. Such an assessment ensures understanding among leaders, teams, and employees, as transitioning from traditional and well-known approaches to agile can be challenging [9] and cause risks [10] [11].

Agile methodologies prioritize adaptability through continuous feedback and incremental delivery, both crucial for responding to global changes efficiently [12] [13] they streamline processes, focusing on valuable outcomes, especially beneficial in cybersecurity [13]. A previously conducted literature analysis revealed that agile readiness has hardly been discussed at all in the literature and assessments for the adoption of agile methodologies in cybersecurity remain underexplored. Addressing this gap, our research aimed to develop a model to assess the readiness within organizations for agile cybersecurity management. We evaluated both – agile and cybersecurity (challenges) and assessed and selected appropriate standards or frameworks to guide the model's development. Based on literature the following research questions (RQs) were derived:

RQ 1 What agile methodologies suit cybersecurity?

RQ 2 What cybersecurity frameworks aid cybersecurity programs?

RQ 3 How to evaluate cybersecurity readiness for agile adoption?

2 Literature Review

The data collection, as part of the awareness phase, we addressed the subject of adopting agile in cybersecurity to get a solid understanding of the concepts and associated reference models or frameworks. The literature review was mainly based on an extensive and systematic literature review in which we analyzed multiple databases, including Google Scholar, Scopus, IEEE, ScienceDirect, and Taylor & Francis, as well as publications from cybersecurity related associations like CIS, ENISA, ISACA and NIST. The approach for the review was adapted from [14] by analyzing, synthesizing, and summarizing the relevant sources based on keywords including backward and forward queries, iterations and inclusion and exclusion criteria.

2.1 Agile

The term ‘agility’ denotes an organizational structure that is customer-centric and flexible [15]. An agility-promoting culture enables operational adaptability, fosters organizational flexibility and speed; factors that are essential for achieving strategic goals [16]. To achieve agility and self-organization guided by agile principles and team objectives is fundamental [17]. The agile manifesto [19], initially for software development released was influenced by various agile methodologies such as Cristal, Extreme Programming, Scrum or Test-driven Development and has evolved and expanded to diverse domains [18] [13] [6]. However, the methodologies and frameworks remain rooted in the values and principles of the agile manifesto [19]. So far, the most popular has been Scrum, a methodology of managing software projects and developing products with prescribed roles and practices. Agile methodologies and in particular Scrum are ideal for dynamic projects and activities requiring close team-stakeholder collaboration [20]. Table 1 contrasts agile and traditional methodologies, outlines the different

foci of both approaches and shows that agile methodologies excel in complex, fast-changing environments, promoting iterative problem-solving and collaboration.

Table 1. Agile vs traditional project management adopted from Nerur et al. (2005).

	Traditional Methodologies	**Agile Methodologies**
Project Approach	Process oriented	People oriented
Project Flow	Sequential	Iterative
Project Management Style	Command and control	Leadership and collaboration
Team Role	Individual team members' skills	Self-organized teams
Communication	Formal	Informal
Client Role	Important	Critical
Process Model	Traditional project management methodologies like Waterfall.	Agile project management methodologies such as Scrum
Project Lifecycle	Based on tasks or activities	Based on product features

Various agile-oriented frameworks build upon Scrum to extend its applicability beyond the team level [21]. Scrum is a versatile project management methodology applicable across various disciplines [12]. Projects are divided into sprints, each delivering a specific requirement within a defined period, contributing to the overall project goal [13]. According to [9], agile principles are increasingly adopted organization-wide, with Scrum being the most utilized methodology (87%), followed by SAFe (53%). The latter as scaled agile framework is widespread applied because its maturity, and suitability is high, and it is broadly accepted in large organizations [23]. Agile-oriented frameworks frequently use SAFe; one reason is its high maturity. But even Scrum of Scrums (SoS), Large-Scale Scrum (LeSS), or Disciplined Agile Delivery (DAD) are often used to scale Scrum. Table 2 shows a comparison of major agile frameworks organized according to criteria based on [22] and [9].

Table 2. Major agile frameworks compared.

	SAFe	**SoS**	**LeSS**	**DAD**
Team Size	50-120 people in agile release train 5-10 people/team	5-10 teams	10 Scrum teams	200 people or more
Differentiator	Many adaptable artifacts, roles, and guidelines.	Enables scrums for all situations and scales	Offers flexible suggestions.	Complex, with coverage of many models
Underlying Methodology	Scrum and other agile principles	Scrum	Scrum	Scrum, Lean
Maturity	High	High	Medium	Low
Complexity	High-Medium	Medium-Low	Medium-Low	Medium-Low
Global teams	Feasible	Feasible	Feasible	Difficult
Popularity	53 %	28 %	6 %	3 %

2.2 Cybersecurity

Cybersecurity as a term evolved from computer security in the late 20th century to address the changing threat landscape [24]. Initially focused on virus protection [25]

cybersecurity now encompasses a holistic approach to govern and manage technological, organizational, and human aspects of cybersecurity [26]. Main goal of cybersecurity is to safeguard IT assets and digital data against cyberthreats [1], supported by various reference models and standards provided by globally or nationally active organizations like (in alphabetical order) CIS, HITRUST, ISACA, ISO/IEC, NIST.

Creating an effective cybersecurity program poses significant challenges. Many organizations worldwide have selected and combined reference models and standards to support systematic program implementation, operation maintenance and monitoring of cybersecurity [3] [27] [28]. These reference models and standards facilitate primarily cybersecurity architecture (areas like system administration, network security, incident response), policies (defined rules for certain areas), programmatic elements (linkage of people, budget, and technology), IT life cycles (aligns cybersecurity with business strategy), and assessments (evaluate periodically program effectiveness) [1].

3 Research Design

Elaborated from various preliminary discussions with subject matter experts we knew that the successful adoption of agile in cybersecurity - as pre-condition - needs an assessment of (1) whether the organization's maturity level with regard to its cybersecurity program is sufficient and (2) whether an organization is ready and able to deal with the transition from traditional to agile management in cybersecurity. So, the idea was born to develop and evaluate such a maturity assessment as an artifact based on known reference models from both worlds - agile and cybersecurity.

To ensure a systematic approach and achieve rigor we selected ´Design Science Research´ (DSR) as guiding research design. DSR aims to develop and evaluate an artifact based on business needs in a certain environment by using an existing knowledge base which provides the foundations and methodologies from prior research, ensuring rigorous development whereas the environment defines specific business needs, both guide a thoroughness and traceable artifact development and evaluation [29].

4 Model Development

4.1 Methodology

Utilizing DSR, we developed the novel ´M&RA Model´ as an artefact that is suitable as an assessment tool to help organizations decide whether their organization is suitable in principle for the use of agile methods to manage cybersecurity.

The model itself is divided into two separate models – the ´MA Model´ and the ´RA Model´ (both together result in the M&RA model). The MA Model is foreseen to assess the maturity of the cybersecurity program within an organization. If the level of maturity is sufficiently high, it becomes logical to apply the second model – the RA model, to assess the agility maturity within an organization. The RA model can also be performed without the upstream MA model which is offered as pre-assessment (light

approach) but it is recommended only if the organization knows the (sufficient) maturity level of its cybersecurity program (full approach).

We followed DSR using an iterative five-phase process adapted from [30]: (1) '**Awareness**', to investigate and identify the suspected problem and its relevance in more detail, (2) '**Suggestion**', to develop and outline a solution path, (3) '**Development**', to develop a rigor artefact as potential solution, (4) '**Evaluation**', to evaluate the artifact, and (5) '**Conclusion**' to conclude the research and to outline further research recommendations and limitations of the research carried out. The process phases (3) and (4) have been iterated several times, incorporating new information and insights gathered per iteration.

In phase 1, we gathered and analyzed information on agile and cybersecurity to discover the research gap and to derive the RQs. In this phase, the basic aspects of agility and cybersecurity were compiled, and various reference models were compared in order to emphasize the relevance of the problem and gather initial ideas for a potential solution.

In phase 2, we utilized phase 1 results, particularly the analysis of reference models in the field of cybersecurity and agile. We assessed deeply relevant reference models regarding pre-defined criteria (e.g., linked to policy, completeness, useability, conciseness, acceptance, approved by an appropriate authority, collaborative, traceable, applicability across industries, mapping to other standards/frameworks, regularly updated), this resulted after careful comparison and consideration that we decided to use the NIST CSF 2.0 (2023)[2] [31] as foundation to assess the maturity of cybersecurity within organizations - as first step regarding the agile readiness assessment. This phase included understanding how to structure the planned M&RA Model, key elements to consider and based on an enhanced literature review we carried out in this phase we identified and categorized criteria for the model's design.

In phase 3, the M&RA Model was built on information gathered in the previous phases. Expert insights and iterations between phase 3 and phase 4 ensured rigor and solidified the decision to use the NIST CSF 2.0 (2023) [31] as a basis. Table 3 shows core function areas of the guiding framework; these functions were aligned with ´assessment statements´ also derived from the selected framework. Exemplary details for the ´GOVERN´ function area and derived assessment statements are shown in Table 4.

Table 3. NIST CSF 2.0 (2023) – Core functions.

Functions	Description
Govern (GV)	Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy.
Identify (ID)	Help determine the current cybersecurity risk to the organization.
Protect (PR)	Use safeguards to prevent or reduce cybersecurity risk.
Detect (DE)	Find and analyze possible cybersecurity attacks and compromises.
Response (RS)	Act regarding a detected cybersecurity incident.

[2] We worked with the NIST CSF 2.0 (2023) in its draft version, due to be released in the final version in February 2024.

Recover (RC)	Restore assets and operations that were impacted by a cybersecurity incident.

Table 4. Excerpt: MA Model assessment statements adopted from NIST CSF 2.0 (2023).

Sub-Categories	ID	Assessment Statement (shortened)
GOVERN (GV)		
Organizational Context Mission, stakeholder expectations, legal, regulatory, and contractual requirements are understood	GV.OC-1	Mission guides cybersecurity risk management.
	GV.OC-2	Internal and external stakeholders' needs understood.
	GV.OC-3	Legal, regulatory, and contractual requirements managed.
	GV.OC-4	Critical objectives, capabilities, and services communicated.
	GV.OC-5	Outcomes, capabilities, and services determined

To develop our artifact, we relied on advice from literature about how to develop maturity models. Based on Lasrado et. al (2015), three metamodels for developing a maturity model were derived as foundation: the (1) 6-phase approach for developing metamodels [32], (2) the 8-steps approach for developing metamodels [33]; and (3) the 5-steps approach for developing stage of growth for metamodels [34]. By combining relevant elements from the three metamodels, we could adopt them to develop the M&RA Model. Figure 1 visualizes the development phases adopted derived from [32] [33] [34]. Phase 5 and 6 (grey marked) were not utilized as part of this research, as we focused on the blue-marked phases with its iterative development cycle.

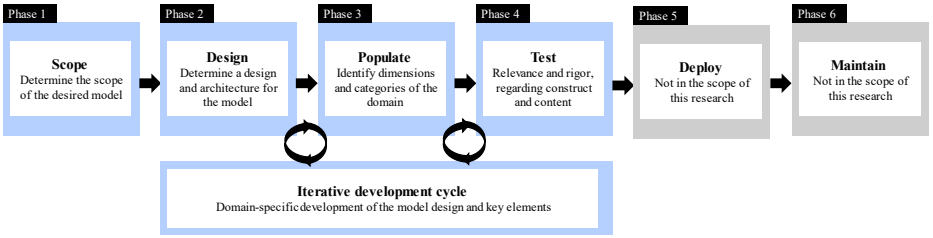

Fig. 1. Development phases for the M&RA Model.

In phase 4, the M&RA Model was assessed and evaluated with cybersecurity and agile experts to determine its validity, reliability, and generalizability.

In phase 5, a summary was drawn up, limitations were documented, and advice given on further research.

4.2 Final M&RA Model (Excerpts)

The M&RA Model is in its final version an Excel-based artefact which provides a comprehensive structure and functionality to assess and visualize an organization's maturity level regarding cybersecurity (MA Model) and agile readiness for cybersecurity (RA Model). Both sub models can also be carried out independently of each other. The M&RA Model is structured using consecutive Excel sheets as guiding path (Figure 2).

Fig. 2. Guided steps through the M&RA Model.

The first sheet ´M&RA Model Introduction´ gives an overview of the model´s structure, including an introduction into the artefact, how and when it can be applied and explains the two different Models (MA Model and RA Model) and its differences and application case with the help of a process flow and a descriptive explanation (below). The next sheet ´Step 1 -->´ leads to the ´**MA Model**´ followed by ´Step 2 -->´ and then going to the ´**RA Model**´. The artefact with its two models can be applied as ´Full Approach´ or ´Light Approach´ (Figure 3).

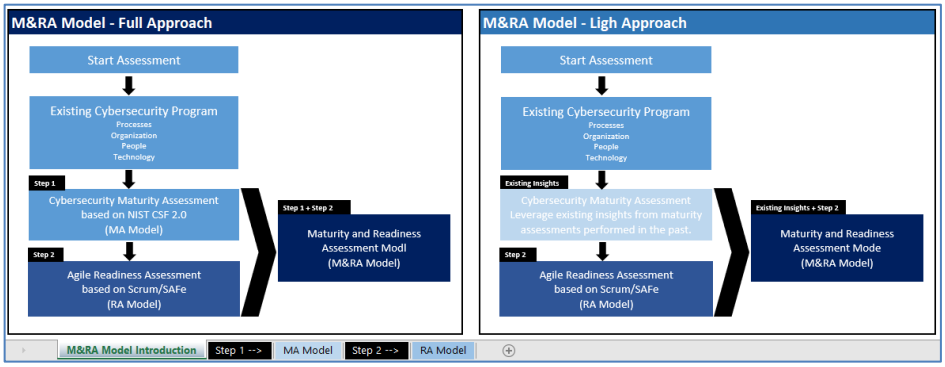

Fig. 3. Excerpt: ´M&RA Model Introduction´ with two selectable approaches.

The ´Full´ approach (Step 1 --> MA Model --> Step 2 --> RA Model) assesses first the maturity of the existing cybersecurity program supported by the MA Model; it can be evaluated which parts (dimensions) of the cybersecurity program have the potential for agile at a scale adoption due to sufficient maturity. Figure 4 shows an excerpt from the MA Model – the cybersecurity maturity assessment with the assessment statements that need to be evaluated. Based on the MA Model assessment results, the following Step 2 - the agile readiness assessment (based on the RA Model) can be carried out.

Cybersecurity Dimensions	Cybersecurity Sub-Categories	ID	Assessment Statement	Maturity Score	Weighting	Weighted Maturity Score	Maturity Assessment	Recommendation
Govern Establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy	Organizational Context	GV.OC-1	The enterprise mission is understood and informs cybersecurity risk management.	3	1	3		**Agile Readiness Assessment is recommended --> Step 2**
		GV.OC-2	Internal and external stakeholders are determined, and their needs and expectations regarding cyber risk management understood.	3	1	3		
		GV.OC-3	Legal, regulatory, and contractual requirements including data privacy and civil liberties regarding cybersecurity are understood and managed.	3	1	3		
		GV.OC-4	Critical objectives, capabilities and services provided to internal and external Stakeholders are determined and communicated.	3	1	3		
	Risk Management Strategy	GV.RM-1	Risk management objectives are established and agreed by stakeholders.	3	1	3		
		GV.RM-2	Risk appetite and risk tolerance statements are determined, communicated, and maintained.	3	1	3		
		GV.RM-3	Enterprise risk management processes include cybersecurity risk management activities and outcomes.	3	1	3		
		GV.RM-4	Strategic direction that describes appropriate risk response options is established and communicated.	3	1	3		
		GV.RM-5	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	3	1	3		
		GV.RM-6	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	3	1	3		
	Cybersecurity Supply Chain Risk Management	GV.SC-1	A cybersecurity supply chain risk management program, strategy, objectives, policies, andprocesses are established and agreed.	3	1	3		
		GV.SC-2	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	3	1	3		
		GV.SC-3	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	3	1	3		

Fig. 4. Assessment procedure of the MA Model – Basis of the ´Full´ approach.

Figure 5 shows an excerpt from the RA Model – the agile readiness assessment based on Scrum/SAFe with the assessment statements that need to be evaluated and further criteria (e.g., readiness score, weighting, weighted maturity score).

The ´Light´ approach (Step 2 --> RA Model) assesses the readiness for adopting agile in cybersecurity only (Figure 4 shows an excerpt). For this approach, existing insights from maturity assessments performed in the past are leveraged to evaluate which parts (dimensions) of the cybersecurity program have the potential for agile at a scale adoption due to sufficient maturity.

Cybersecurity Dimension							
Agile Dimension and Subcategories	ID	Assessment Statement	Readiness Score	Weighting	Weighted Maturity Score	Readiness Assessment	Recommendation
Cybersecurity Dimension Product and Services	CD.PS-1	Products and services are dynamically changing based on external requirements (e.g. Threat Landscape, Regulatory Requirements).	3	1	3		A traditional approach might be better suited or further enhancement towards agile is recommended.
	CD.PS-2	Products and services are dynamically changing based on internal needs and requirements.	3	1	3		
	CD.PS-3	Products and services require continuous improvement/changes/adjustments in relatively short intervals < 1 year.	3	1	3		
	CD.PS-4	Business operations can be negatively impacted if new or existing products and services are not provided timely.	3	1	3		
	CD.PS-5	The exact deliverables of a new product or service cannot be clearly defined from the beginning, and iterative procedures are beneficial to achieve the final deliverable.	3	1	3		
	CD.PS-6	The factor time in the product and service delivery is crucial; hence, prioritization and scoping are key.	3	1	3	3.0	
	CD.PS-7	Value delivery has priority over strict adherence to planned procedures and specifications when delivering products or services.	3	1	3		
	CD.PS-8	Decisions about products and services can be made quickly "just in time" and are not slowed by formal processes.	3	1	3		
	CD.PS-9	Products and services are not negatively impacted by enforced formalities and adherence to strictly defined approaches.	3	1	3		
	CD.PS-10	Product and services quality is improved when delivering in iteratively meaning in digestible pieces.	3	1	3		
	CD.PS-11	Many risk factors are related to the product and service, which need to be managed.	3	1	3		
Cybersecurity Dimension Team and People	CD.TP-1	Within the cybersecurity team, individuals with hands-on experience and education in agile methodology are available.	3	1	3		A traditional approach might be better suited or further enhancement towards agile is recommended.
	CD.TP-2	Within the cybersecurity team, individuals with knowledge in agile are available.	3	1	3		
	CD.TP-3	Within the cybersecurity team, the competencies are mixed and appropriately distributed, and required specialists for the different cybersecurity topics are available.	3	1	3		
	CD.TP-4	Key resources within the cybersecurity team are continuously available.	3	1	3		
	CD.TP-5	The cybersecurity team is stable, and fluctuations are rare.	3	1	3		

Fig. 5. Assessment procedure of the RA Model – can be carried out as ´Light´ approach.

The approach explained in Figure 3 (right box) offers an efficient initial assessment of agile readiness without the time-consuming assessment of the cybersecurity program's maturity (Full approach, first Step 1 --> MA Model). The ´Step 1´ part is then replaced by ´Existing Insights´ from other assessments or audits. The light approach provides a position statement. Both approaches, ´Full´ and ´Light´ can either identify gaps that require further development for agile readiness or confirm that agile is unsuitable in the selected cybersecurity dimension. An interpretation and weighting of the score is at the customer's discretion and depends on the customer's situation, needs, use case, goals, and strategy related to cybersecurity and the assessed organization.

Both models – the MA Model and the RA Model – outline assessment results as readiness score and levels along with recommendations (Excel-based table) and with visualizing the maturity assessment result. Figure 6 shows an exemplary assessment result from the RA Model (visualized view) – a spider diagram about the overall readiness of a model organization. The assessment within the RA Model results in statements related to organization-wide prerequisites, cybersecurity program requirements, and internal leadership support. The ´Readiness Score´ and ´Weighting´ are filled based on discussions and workshops with relevant teams and leadership, focusing on the chosen cybersecurity dimension. Interpretation and weighting of the score are discretionary. An average score of ≥ 4 across all agile dimensions suggests potential agile adoption, indicating possible benefits based on organization-wide prerequisites, requirements, and leadership support. The score serves as a positioning statement, identifying

gaps for further development or confirming agile unsuitability in the selected cybersecurity dimension. The recommended score simplifies assessment, aiding in identifying current status, gaps, and improvement areas through the M&RA Model.

Fig. 6. Exemplary RA Model assessment result (visualized view).

The evaluated and incrementally improved final artefact can be downloaded from the public SWITCHdrive: https://drive.switch.ch/index.php/s/rtWIQ3tTuEIfFRo.

5 Evaluation

Cybersecurity and agile experts evaluated the M&RA model in autumn 2023. Initially, input from two subject matter experts was gathered through three brainstorming sessions to ensure iterative improvement and practical adherence during artefact development. Subsequently, three semi-structured interviews were conducted with subject matter experts selected based on previously defined criteria. All experts for the evaluation met these four criteria: (1) expertise in cybersecurity and agile, (2) consulting experience, (3) management position and (4) experience over ten years.

As illustrated in Figure 7, introduction meetings with the experts were conducted first - a few days before the interviews were planned to explain the M&RA Model and the evaluation approach. This step ensured that the experts were prepared and could undertake initial considerations before the interview.

Fig. 7. M&RA Model evaluation approach

The sessions and interviews were held to evaluate the M&RA Model's regarding its (1) validity, incl. missing elements or improvement points, (2) reliability, and (3) generalizability to evidence rigor and relevance of the artefact. Within the discussion the completeness, accuracy, applicability, usability, and not at least the achievement of standardized applicability in the cybersecurity environment have been examined and (feasible) improvement elements have been worked out, documented and iterative improvements have been implemented.

Table 5 summarizes key evaluation findings, including areas for improvement. The experts evaluating the model confirmed the validity, reliability, and generalizability of the final M&RA Model in principle. However, the complexity, scope, and time constraints limited addressing certain points, earmarking them for future research.

Table 5. Conclusion of the conducted semi-structured expert interviews.

Evaluation Area	Summary
Validity	Experts affirmed the relevance of domain-specific elements: ´Score´, ´Levels´, ´Dimensions´, ´Sub-Categories´, and ´Statements´. The M&RA Model is robustly designed and encompasses necessary details. Additionally, experts endorsed the use of CSF 2.0 as it's widely recognized, holistic, and covers key cybersecurity aspects.
Reliability	Experts agreed on the M&RA Model design, confirmed the accuracy and consistency, and that the goal of assessing readiness for agile in cybersecurity is achieved. Experts agreed on the M&RA Model content and structure and calculation approach.
Generalisability	Experts agreed on the M&RA Model's applicability in the cybersecurity environment and confirmed that utilizing CSF 2.0 is appropriate and ensures a standardization model. The experts mentioned that they are interested in seeing the application of the M&RA Model in real-world scenarios.
Missing elements or improvement points (Part of validity)	It's suggested to consider or add, for instance, as starting points for future research: - benchmarking or further guidance for weighting assessment statements. - people, processes, and technology in the agile readiness level. - mapping to other frameworks like ISO/IEC 27001 in the MA Model.

6 Conclusion and Further Research

The novel M&RA Model aids cybersecurity, agile, and implicit organization leadership in achieving agile cybersecurity or benefiting from agile principles. It assesses cybersecurity maturity (MA Model) within an organization to ensure a foundation for agile adoption, then evaluates cybersecurity readiness (RA Model) based on prerequisites, requirements, and leadership support. Utilizing the NIST CSF 2.0 (2023) [31] combined with Scrum and SAFe, the developed M&RA model offers a comprehensive assessment model for the maturity of cybersecurity and agile within organizations. Promising areas for future research outlined in Table 5 and can be summarized as follows: (1) Simplifying the M&RA Model without compromising validity or reliability, achieved through detailed analysis of assessment statements with subject matter experts and surveys; (2) Developing practical guidelines for M&RA Model application, including methodology selection, and addressing common challenges; (3) Quantitatively evaluating the M&RA Model through surveys and expert interviews for further improvement insights.

References

1. Donaldson, S. E., Siegel, S. G., Williams, C. K., Aslam, A. (2018). Enterprise Cybersecurity Study Guide: How to Build a Successful Cyberdefense Program Against Advanced Threats (2018). Apress: Imprint. https://doi.org/10.1007/978-1-4842-3258-3
2. WEF. (2024). 2023 was a big year for cybercrime – here's how we can make our systems safer. https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/
3. Gregory, P. H. (2018). CISM certified information security manager all-in-one exam guide. McGraw-Hill Education
4. Amorim, A. C., Mira Da Silva, M., Pereira, R., Gonçalves, M. (2021). Using agile methodologies for adopting COBIT. https://doi.org/10.1016/j.is.2020.101496
5. Ciric, D., Lalic, B., Gracanin, D., Tasic, N., Delic, M., Medic, N. (2019). Agile vs. Traditional Approach in Project Management. Procedia Manufacturing, 39, 1407–1414. https://doi.org/10.1016/j.promfg.2020.01.314
6. He, Y., Zamani, E. D., Lloyd, S., Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. International Journal of Information Management, 62, 102435
7. Telemaco, U., Alencar, P., Cowan, D., Oliveira, T. (2022). Agile Assessment Methods: Current State of the Art. https://doi.org/10.48550/ARXIV.2212.10808
8. Asprion, P., Giovanoli, C., Scherb, C., Bhat, S. (2023). Agile Management in Cybersecurity. 21–28. https://doi.org/10.29007/9fg8
9. 16th State of Agile Report. (2022). Digital. AI. https://digital.ai/resource-center/analyst-reports/state-of-agile-report/
10. Anes, V., Abreu A., Santos, R. (2020). A New Risk Assessment Approach for Agile Projects. International Young Engineers Forum (YEF-ECE), 67-72. https://ieeexplore.ieee.org/document/9171808
11. Fogoroș, T. E., Olaru, M., Bitan, G. E., Dijmărescu, E. (2021). The Risks of Agile Methods in the Context of Digital Transformation. R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu eds, 756-764. https://basiq.ro/papers/2021/21096%20-%20Fogoros.pdf
12. Schwaber, K. (2004). Agile project management with Scrum. Microsoft Press
13. Hohl, P., Klünder, J., van Bennekum, A., Lockard, R., Gifford, J., Münch, J., Stupperich, M., Schneider, K. (2018). Back to the future: Origins and directions of the ´Agile Manifesto´ – views of the originators. Journal of Software Engineering Research and Development, 6(1), 15. https://doi.org/10.1186/s40411-018-0059-z
14. Paré, G., Trudel, M.-C., Jaana, M., Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, 52(2), 183–199. https://doi.org/10.1016/j.im.2014.08.008
15. Förster, K., Wendler, R. (2012). Theorien und Konzepte zu Agilität in Organisationen. Technische Universität Dresden. https://nbn-resolving.org/urn:nbn:de:bsz:14-qucosa-129603
16. Deeken, M., Fuchs, T. (2018). Agiles Management als Antwort auf die Herausforderungen der Digitalisierung. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-22706-7
17. Kaltenecker, S. (2018). Selbstorganisierte Teams führen: Arbeitsbuch für Lean & Agile Professionals (2. Ed.). dpunkt
18. Klünder, J., Schmitt, A., Hohl, P., Schneider, K. (2017). Fake News: Simply Agile. Gesellschaft für Informatik. http://dl.gi.de/handle/20.500.12116/4891
19. Schön, E. M., Escalona, M., Thomaschewski, J. (2015). Agile Values and Their Implementation in Practice. International Journal of Interactive Multimedia and Artificial Intelligence, 3(5), 61 https://doi.org/10.9781/ijimai.2015.358
20. Malik, R. S., Ahmad, S. S., Hussain, M. T. H. (2019). A Review of Agile Methodology in IT Projects. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3351064

21. Rosencrance, L. (2020). SAFe. Scaled Agile Framework. Techtarget. www.techtarget.com/whatis/definition/SAFe-Scaled-Agile-Framework
22. Kalenda, M., Hyna, P., & Rossi, B. (2018). Scaling agile in large organizations: Practices, challenges, and success factors. Journal of Software: Evolution and Process, 30(10), e1954. https://doi.org/10.1002/smr.1954
23. Scaled Agile. (2023). SAFe 6.0 Framework. Scaled Agile Framework. https://scaledagileframework.com/
24. Kasprowicz, D., Rieger, S. (Eds.). (2020). Handbuch Virtualität. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-16342-6
25. Parikka, J. (2007). Digital contagions: A media archaeology of computer viruses. Peter Lang
26. Touhill, G. J., Touhill, C. J. (2014). Cybersecurity for executives: A practical guide. John Wiley & Sons
27. Stallings, W. (2019). Effective cybersecurity: Understanding and using standards and best practices. Addison-Wesley.
28. Syafrizal, M., Selamat, S. R., Zakaria, N. A. (2022). Analysis of Cybersecurity Standard and Framework Components. International Journal of Communication Networks and Information Security (IJCNIS), 12(3). https://doi.org/10.17762/ijcnis.v12i3.4817
29. Hevner, A. R., March, S. T., Park, J., Ram, S. (2004). Design Science in information systems research. Management Information Systems Quarterly, 28(1). 75-105.
30. 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
31. NIST. (2023). The NIST Cybersecurity Framework 2.0 (draft). National Institute of Standards and Technology.
32. de Bruin, T., Freeze, R., Kulkarni, U., Rosemann, M. (2005). Understanding the Main Phases of Developing a Maturity Assessment Model. Australasian Conference on Information Systems.
33. Becker, J., Knackstedt, R., Pöppelbuß, J. (2009). Developing Maturity Models for IT Management: A Procedure Model and its Application. Business & Information Systems Engineering, 1(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5
34. Solli-Sæther, H., Gottschalk, P. (2010). The Modelling Process for Stage Models. Journal of Organizational Computing and Electronic Commerce, 20(3), 279–293. https://doi.org/10.1080/10919392.2010.494535