Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

Information Security Integration with Agile Software Development: Systematic Literature Review and Expert Judgement

Tengku Chavia Zagita, Teguh Raharjo
tengku.chavia11@ui.ac.id, teguhr2000@gmail.com
Faculty of Computer Science, Universitas Indonesia, Jakarta, Indonesia

Article Information

Submitted : 12 Dec 2023
Reviewed: 16 Dec 2023
Accepted : 30 Dec 2023

Keywords

information security, agile software development, scrum, systematic literature review

Abstract

Many businesses are using the Agile Software Development (ASD) to react to changing needs and provide functional values quickly. Information security, on the other hand, is seen as a non-functional requirement. In consequence, information security is frequently ranked lower than functional needs in ASD. The goal of this study is to present a unified perspective on how researchers integrate information security into agile software development. This study uses Systematic Literature Review (SLR) approach from ACM, IEEE, ScienceDirect, and Scopus. This study identified several key groups related to the integration of information security with ASD: agile methodologies, agile ceremonies, advantages, and issues. According to the findings of this study, all agile ceremonies contain some form of enhancement in process or artifacts linked to security. These findings have also been validated by expert judgment who have experience working in the project team that have integrated information security into agile software development process.

A. Introduction

The rapid development of today's software development business requires rapid delivery of software products by development teams. To deliver products faster than before, developers are transforming traditional software development lifecycles into agile development methods that can deliver software faster while maintaining customer satisfaction [1]. While some agile practices could be beneficial for security, others contradict established approaches to security assurances [2]. Information security is considered a non-functional requirement, also known as quality requirements, which are software specifications that explain how the software should work [3]. Non-functional requirements are defined as being ambiguous and difficult to describe, and are frequently unclear and undocumented. This is particularly evident in Agile Software Development (ASD), which favors functioning software above detailed documentation. [3].

There are many factors that can affect the level of information security in general, in this case. Information security has three domains that are generally accepted, namely people, process, and technology [4]. Many companies are adopting the agile methodology for software development or Agile Software Development (ASD) to adapt shifting requirements and rapidly deliver functional values [5]. In return, information security is not considered a fundamental value and often put in lower priority compared to functional requirements in ASD [5]. With the number of security threats for organizations are increasing, there needs to be an alignment between Agile Software Development (ASD) and Information Security (InfoSec) to minimize the security threats which can create its own risks, such as financial and reputational loss. Table 1 represents statistics of main impacts when companies suffered cyberattacks and breaches from [6].

Table 1. Impact of Security Breaches in Organization

Impact	Statistic
Reputational loss (i.e. reduced market share, higher capital cost, rating downgrade)	37%
Business disruption (i.e. staff downtime, costs of business interruption)	31%
Response costs (i.e. managing disruption, notifying customers/stakeholders)	27%
Direct losses (i.e. financial theft, compensation to victims)	21%
Opportunity costs (i.e. foregone gains due to diverted management attention)	19%
Replacement costs (i.e. repair/replace capital assets, recover data)	19%

Information Security

Information is an asset for an organization that has a role in the decision-making process by management. Information can be defined as a business asset that has a value similar to other important business assets, thus information needs to be adequately protected [7]. Information is a valuable resource that needs to be protected from possible security risks and threats from within, as well as attacks from outside [8]. In today's digital world, companies have a priority to secure information system assets in order to protect companies from cyber-attacks.

Information security in technology now extends to areas such as authentication and authorization, network security, software security, and the use of data [9]. Information security is the collection of procedures, strategies, measures, and management processes used to secure IT assets and their capacity to withstand both internal and external threats [10]. Information security is described as the prevention of illegal access, use, disclosure, interference, alteration, or destruction of information and information systems [11]. Fundamentally, information security is comprised on three concepts: confidentiality, integrity, and availability, or the CIA triad. Figure 1. represents the CIA triad from [11].

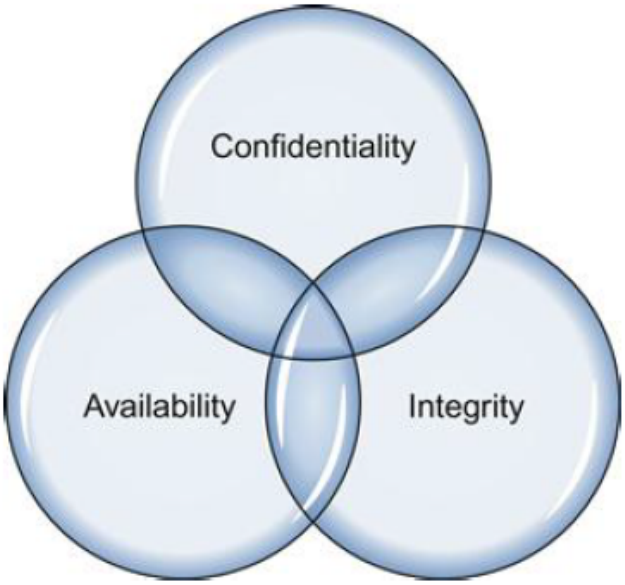

Figure1. CIA Triad

Confidentiality is defined as "the ability to store information so that unauthorized persons can access it" [11]. Integrity is defined as "the ability to protect information from unwanted changes". Availability is defined as "having access to information when you need it" [11]. The CIA concept is now the standard for information security in the context of industry and government technology [10].

Agile Software Development

Agile software development (ASD) is a popular approach to software development that focuses on iterative and incremental development, with a strong emphasis on customer satisfaction, collaboration, and flexibility. ASD is not a technique in and of itself, but rather a collection of guiding principles from which other ways have emerged [5], [12]. Agile methodologies are frameworks that provide a structured approach to implementing agile principles. Scrum is the most widely used of these methodologies, although other prominent approaches include extreme programming, Kanban, Lean, and hybrid approaches [5]. In general, these approaches seek to create development that is sensitive to the demands of both clients and developers. They also share a common preference for short "time-boxed" iterative development cycles, regular client communication, continual adaptation, and change tolerance [12].

Agile development aims to deliver software quickly, respond to changing requirements, and enhance customer satisfaction. Agile, being a flexible approach to software development, enables the delivery of high-quality products to customers. Several studies have been done regarding quality management, risks, critical success factors, and integration agile software development with other subjects. Study in [13] examines the aspects of coordination in Agile development projects. [12] performed study to understand the risks of agile software development based on the participants' views of ASD practices. Figure2 provides statistics of most popular agile approaches used by practitioners from [14].

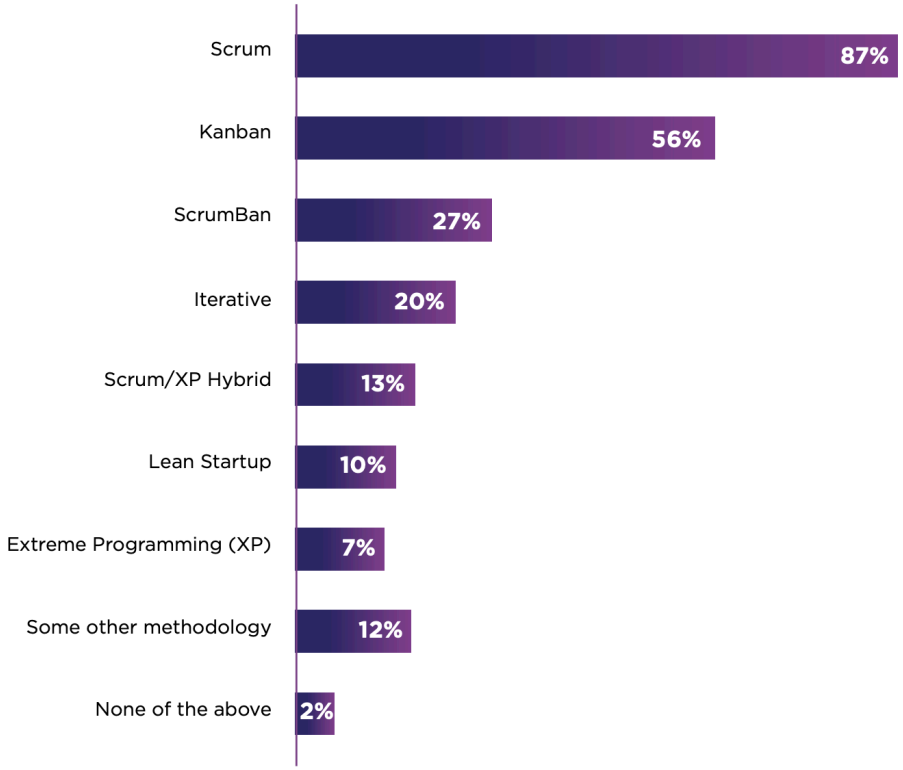

Figure2. Statistics of Agile Approaches

Information Security in Agile Software Development

Agile software development needs information security to safeguard against online threats and data breaches. Due to Agile's rapid pace and iterative process, security may be neglected or foregone in favor of efficiency [15]. Frequent code changes that are common in agile development might make it challenging to manage security and make sure that vulnerabilities are fixed. Additionally, security is frequently treated as a stand-alone activity rather than as an essential component of Agile development, which can result in security being added as an afterthought rather than being incorporated into the development process [15]–[17].

Information security in agile software development has been researched in different aspects. Study in [18] gives information about the technique utilized by one security professional at a SME to impact the importance of security in the company's software development projects. There are 5 categories in which organisation to pay

attention to when it comes to influencing security to agile development, namely driving forces, visibility, motivation, room to manoeuvre, and process match.

Study in [5] shows that there are four categories of critical success factors, which are team practices, organisational practices, technical practices, and project practices, that organisations must focus on in order to integrate information security to agile software development process successfully. Study in [2] provides a view on tensions and challenges of managing security in scrum. This study will focus more on the proposed framework or methodology used in previous research to integrate information security with agile software development.

There are existing academic literatures that seek to identify this tension between information security and ASD and recommend solutions that include security-oriented agile methodologies and techniques for documenting and prioritizing non-functional requirements related to information security [19], [20]. However, we still need a unified view to integrate security requirements into agile practices. This study focuses on how security requirements are handled in integration with agile methodology using different approaches.

B. Research Method

This research refers to [21] for Systematic Literature Review, and includes of planning, execution, and reporting processes. The first stage is to determine the primary goal of this research. Search methods are built around the selection of key terms and synonyms.

Research Objectives and Questions

The research objective is to identify the solutions found for integrating information security into agile software development. The research questions for this study are as following:

- **RQ1**: Which agile methodologies have the approaches been presented or implemented in?
- **RQ2**: How is information security integrated to agile software development process?

Search Strategy and Criteria

The search string in this study is (("Information Security" OR "Security") AND ("Agile Approach" OR "Agile Software Development") AND ("Integration") AND ("Organization" OR "Enterprise")). The query is searched in several paper databases, namely ACM, IEEE Xplore, Scopus, and ScienceDirect which are then imported to Mendeley for citation process. In this phase, literatures are filtered based on the following criteria:

- Literature in English.
- Literature in the form of journals or proceedings.
- Literature within the last ten years, namely 2014 to 2023.
- Literature that has been peer-reviewed.
- Complete downloadable literature (full text).
- Literature that has an abstract and a title appropriate to the research topic.

After filtering based on the above criteria, we narrowed down to 57 literatures. Then, we proceeded to read the entire documents to further validate what was filtered previously only from abstract. We narrowed down 15 literatures to be used in this study. Table 2 provides summary of articles selection process.

Table 2. Summary of Articles Selection

Phase	Inclusion Criteria	Total Articles
Initiation Phase	Boolean search string	275
Phase 1. Selection based on year of publication	2014 to 2023	154
Phase 2. Selection based on title and abstract	Related to integration security to agile software development	57
Phase 3. Selection based on full text	Related to integration security to agile software development	15

C. Result and Discussion

Overview of Studies

Figure3 indicates the number of selected articles related to integration of information security to agile software development. This figure shows that information security has been a topic discussed with agile software development, more so in the recent years where agile software development, especially scrum, has been more popular.

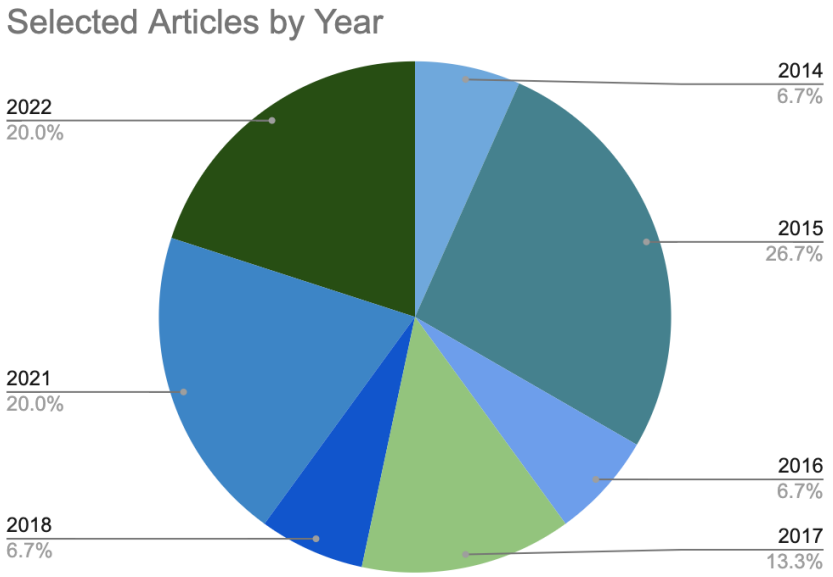

Figure 3. Selected Articles by Year

We also summarize the studies based on the objectives and type of study. This process aims to help with the analysis of each study. Table 3 provides summary of the 15 literatures based on the description of the literature.

Table 3. Summary of Selected Articles

Code	Ref.	Description	Type
P1	[22]	Demonstrated the connection between security principles and security in each scrum phase. Also enhancing the previous proposed Scrum model.	CS
P2	[23]	Provided an accessory to the Scrum agile method named (ScrumS).	MOD
P3	[20]	Provided secure scrum (S-Scrum) methodology, an extension of the software development framework Scrum	CS
P4	[24]	Proposed a hybrid model based on Feature Driven Development (FDD) and Scrum principles to accommodate quality focus	MTH
P5	[25]	Presented a set of approaches, tools, techniques, and changes to the Scrum software development method to meet security compliance levels	CS
P6	[26]	Describes a case of building a secure identity management system and its management processes	CS
P7	[27]	Proposed guidelines for documenting NFRs in ASD	MOD
P8	[28]	Presented challenges of adoption of Microsoft threat modelling in agile development projects	MOD
P9	[29]	Presents a proposal for integrating security activities into Scrum process for developing secure Web applications.	CS
P10	[30]	Presented a Human Centered Design (HCD) approach to security and privacy-focused software development, incorporated within scrum agile methodology	MOD
P11	[31]	Created a framework to ensure security is included in the development process	FRM
P12	[17]	Verified how software security engineering practices are used	CS
P13	[32]	Created approach to review information security risks in IT projects	MTH
P14	[15]	Created model to influence security prioritisation in Agile software development	MOD
P15	[16]	Proposed framework that integrates security into SDLC phases	FRM

CS: case study, MTH: methodology, FRM: framework, APL: application, MOD: model, TOL: tool, OTH: other.

Findings Related to Research Questions

RQ1: Which agile methodologies have the approaches been presented or implemented in?

Based on our review, we noted that 8 out of 15 literatures are using scrum as the methodology for the research. This is not surprising knowing that scrum is the most used methodology compared to other agile methodologies. However, P4 is combining scum and feature-driven development (FDD) in the research. Moreover, 7 other literatures are claiming the result of the research can be applied to all agile methodologies.

RQ2: How is information security integrated to agile software development process?

There are different approaches used in integrating security into agile software development. Most studies used the methods of merging security development process into the agile process itself. Some is adding only specific task in product backlog, others completely added several security developments processes to every single phase in standard agile phases. Some studies also add new roles to be included in the agile phases, such as security expert. We also summarize if the articles provides any advantages or issues while integrating information

security into agile software development. Table 4 provides summarized view of processes added to each agile or scrum ceremonies.

Table 4. Summary of Security Integration to ASD

Key Group	Items
Agile Approaches	General [15] [16] [17] [27] [29] [31] [32]
	Scrum [20] [22] [23] [24] [25] [26] [28] [30]
	Feature-Driven Development (FDD) [24]
Agile Ceremonies	Initial product backlog creation [24] [25] [30] [31]
	Product backlog refinement [3] [20] [22] [25] [29] [30] [31]
	Sprint planning [20] [22] [23] [29] [30]
	Sprint review [25] [26] [30]
	Sprint retrospective [25] [30]
	The sprint [20] [15] [16] [17] [24] [25] [26] [28] [29] [30] [31] [32]
Advantages	Improve agility [22] [25] [28]
	Cost-effective [16] [28]
	Reduce security complexity [15] [16] [23] [32]
	Improve level of security [20] [16] [17] [31]
	Improve documentation tracability [27]
Issues	Slowing down process of creating functionality [29]
	Less agility [31]

All agile or scrum ceremonies have some sort of additional process or artifacts added to the standard process based on the 10 literatures reviewed in this study. Agile ceremony with the most modification or addition within the process is the sprint itself. The addition between studies varies from additional process to additional role. [7], [22], [23], [28] all have new process or even phase added into the standard sprint. [21] adds documentation and security hardening process for the entire development process. [27] adds several small processes into the entire sprint. On the other hand, [26] adds a new role into the sprint which is a security expert. In summary, there are 12 out of 15 studies with integration in the sprint itself. In contrast, daily stand-up or daily scrum do not have additional process.

Agile ceremony with the most similar modification or addition is product backlog refinement where [3], [7], [20], [23], [27], [28], [29] have similar things added into the process. This might be related to how product backlog refinement process can be modified by considering the security aspects of each product backlog. Some studies also add security aspects or features in the initial product backlog creation [22], [23], [28] to ensure that security consideration is done from the beginning. During sprint planning, there are also some security aspects being added, mostly in sprint backlog which are done by [20] and [21]. Moreover, [7] and [28] add an entirely new process related to security to be integrated with sprint planning. [23] and [28] both add new process into sprint review and sprint retrospective, while [24] only adds process into sprint review. [7] and [22] adds new security aspects into definition of done.

The integration of security into Agile software development methodologies gives numerous advantages, as found by various studies [22] [25] [28]. While there is evidence supporting the claim that this integration enhances overall agility, [31] suggests that the inclusion of security components might lesen the agility of the

Software Development Life Cycle (SDLC). Despite this potential drawback, the amalgamation of security and Agile practices offers compelling benefits. Notably, it has been shown to contribute to cost effectiveness [16] [28]. Furthermore, the integration is associated with a reduction in security complexity [15] [16] [23] [32]. Another significant positive outcome is the improvement of the overall security posture of the product [20] [16] [17] [31]. However, the integration of security components may introduce a degree of deceleration in the creation of functional elements [29], considering that security aspects are often classified as non-functional requirements within the development process.

Expert Judgment

Afterward, to determine the most significant items in the key groups, expert judgment assesses each significant category using a thorough online questionnaire with several questions. Experts refer to stakeholders who have experience working in the project team that have integrated information security into agile software development process. The criteria for selecting them as expert judgment is having at least 4 years of experience. These experts work in various industries in Indonesia including IT consulting, banking, e-commerce, and telecommunications industries. The judgments of 10 agile team members for each item in the key groups are summarized in several graphs. Figure4 shows the agile approaches used by experts in this study.

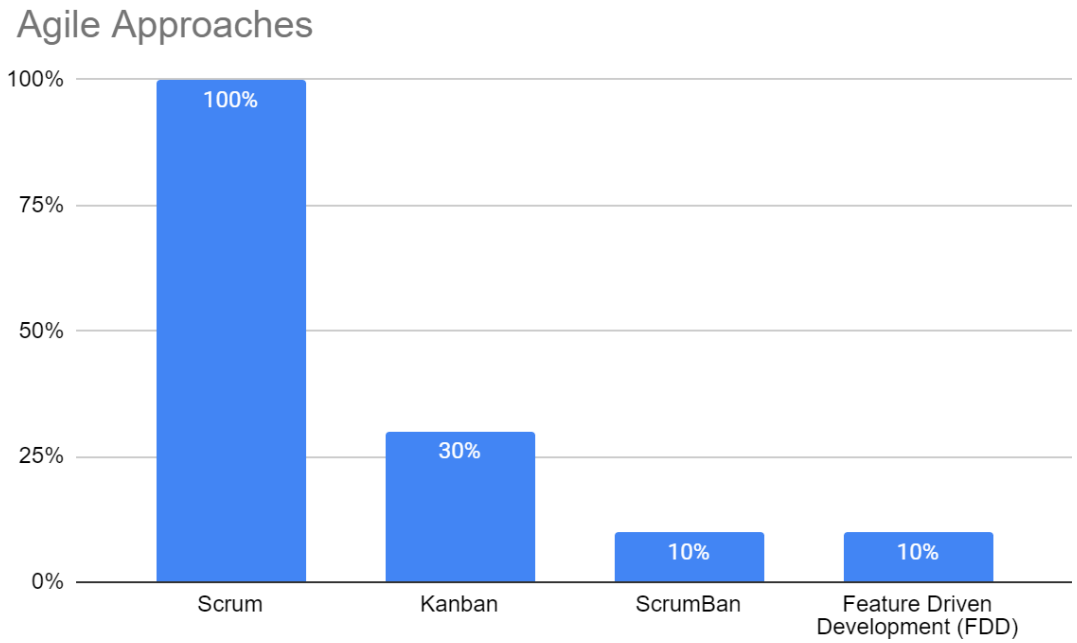

Figure 4. Agile Approaches used by Expert Judgment

Based on the 15 articles, agile ceremony most significantly influenced by modifications or additions related to security measures is the sprint itself, followed by product backlog refinement and initial product backlog creation. Compared to the judgments of 10 experts, 90% agreed that security is integrated into agile software development during product backlog refinement. This integration

manifests in diverse forms, including the introduction of a specific security backlog or the incorporation of risk analysis for each element within the product backlog. There are also integration within sprint review processes, such as security testing, review, and audit. We also noted security verification criteria that's integrated into definition of done. Figure5 shows the result of Agile Ceremonies Integration with Security assessed by Expert Judgment.

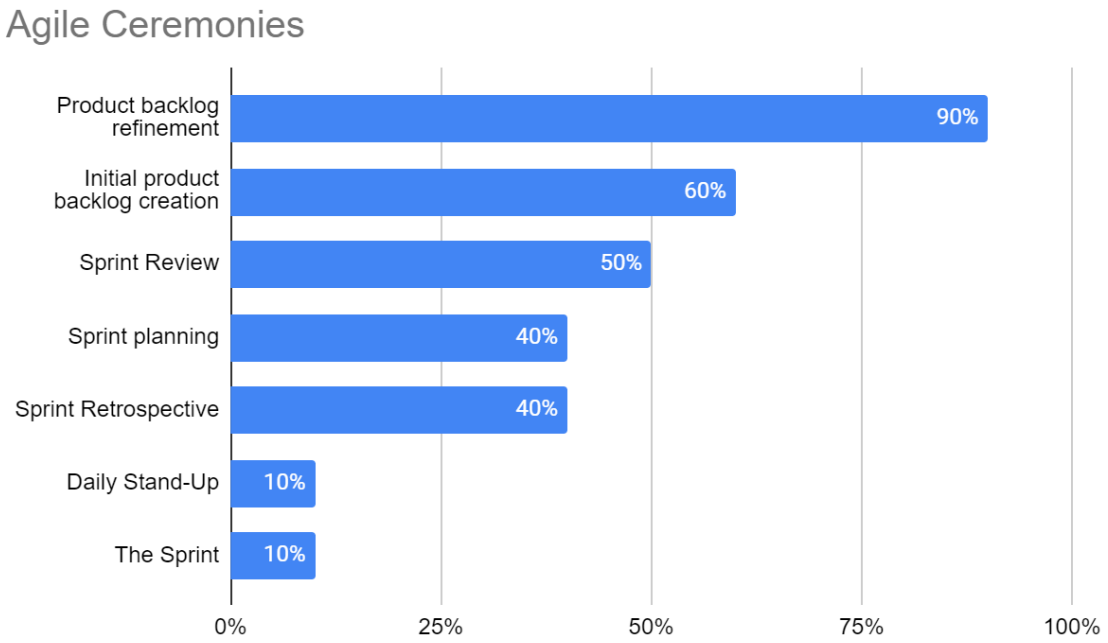

Figure 5. Agile Ceremonies Integration with Security assessed by Expert Judgment

There are several advantages in integrating security with agile software development, including the improvement of security level, cost effectiveness, reduce in security complexity, and improved agility. These advantages are very useful that can support the success of agile software development itself. The graph of advantages can be seen on Figure6, where the advantage that is most agreed upon by the experts is the improvement security level.

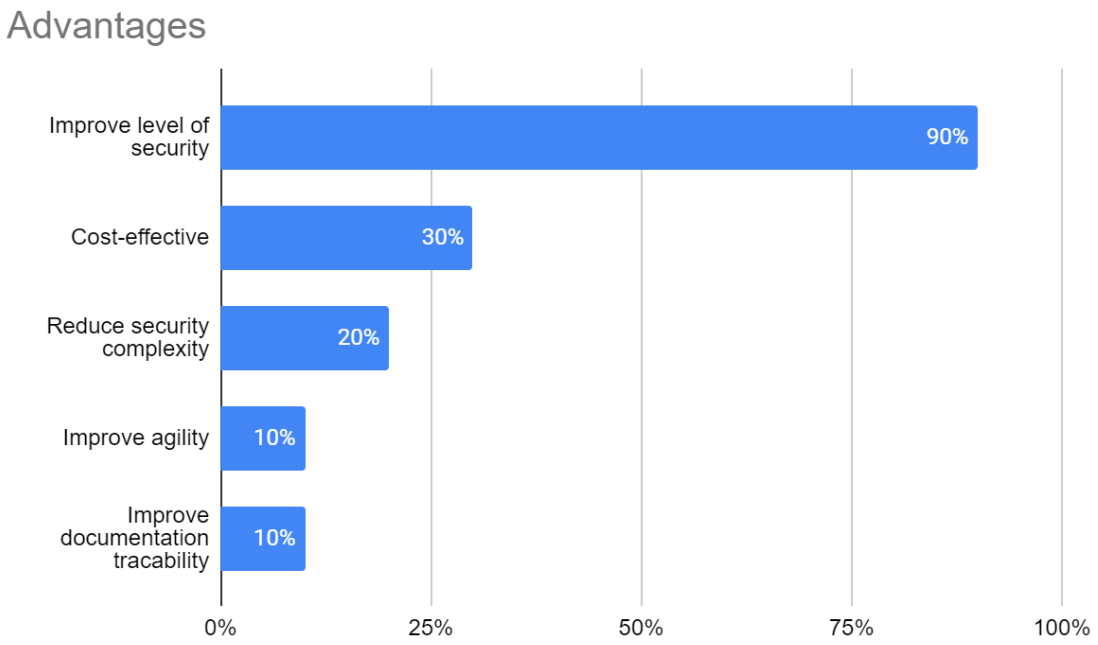

Figure 6. Advantages of Agile Integration with Security assessed by Expert Judgment

Besides the advantages, integrating security into agile software development. This study found two issues, namely slowing down the process of creating functionality and creating less agility within the development process, in which experts agreed 60% and 50% respectively as seen on Figure7. However, 1 expert stated that there is no issue in integrating security into agile software development. It's noted that this expert is working at an well-established company with security already completely integrated into the entire software development process.

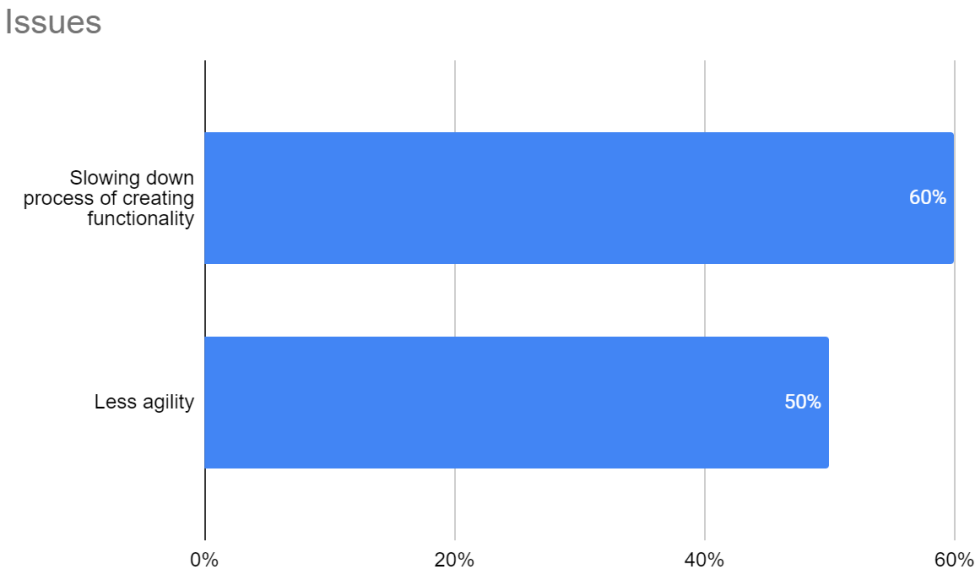

Figure 7. Issues of Agile Integration with Security assessed by Expert Judgment

D. Conclusion

This paper presents the result of systematic literature review on integrating information security with agile software development process. A total of 15 studies between 2014 and 2023 are found in this study. We analyze the studies on how they integrate the framework of information security or just security in general work with agile software development. Based on our review, we noted that most approaches are using scrum methodology. We found that all agile ceremonies have some sort of additional process or modification within the process for integrating security, mostly in product backlog refinement. We noted several advantages in integrating security into agile software development, namely the improvement of level of security, cost-effectiveness, and reduce security complexity. We also found issuses related to security integration with agile software development, namely slowing down the process of creating functionality and decrease in agility within the agile software development process.

E. References

[1] Z. Azham, I. Ghani, and N. Ithnin, "Security backlog in scrum security practices," *2011 5th Malaysian Conference in Software Engineering, MySEC 2011*, pp. 414–417, 2011, doi: 10.1109/MySEC.2011.6140708.

[2] S. Türpe and A. Poller, "Managing security work in scrum: Tensions andchallenges," *CEUR Workshop Proc*, vol. 1977, no. SecSE, pp. 34–49, 2017.

[3] W. Behutiye, P. Karhapää, D. Costal, M. Oivo, and X. Franch, "Non-functional requirements documentation in agile software development: Challenges and solution proposal," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10611 LNCS, pp. 515–522, 2017, doi: 10.1007/978-3-319-69926-4_41.

[4] H. F. Tipton and M. Krause, *Information Security Management Handbook*, 6th ed. Boca Raton: Auerbach Publication, 2008.

[5] N. Newton, C. Anslow, and A. Drechsler, "Information Security In Agile Software Development Projects: A Critical Success Factor Perspective," pp. 0–17, 2019.

[6] ThoughtLab, "Cybersecurity Solutions for a Riskier World," 2023. Accessed: Nov. 18, 2023. [Online]. Available: https://thoughtlabgroup.com/cyber-solutions-riskier-world/

[7] International Organization for Standardization, "Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO 27000)," 2018.

[8] E. Kritzinger, A. Da Veiga, and W. van Staden, "Measuring organizational information security awareness in South Africa," *Information Security Journal*, 2022, doi: 10.1080/19393555.2022.2077265.

[9] A. I. Awad and M. Fairhurst, *Information Security: Foundations, technologies and applications*. The Institution of Engineering and Technology, 2018.

[10] Y. Normandia, L. Kumaralalita, A. N. Hidayanto, W. S. Nugroho, and M. R. Shihab, "Measurement of employee information security awareness using analytic hierarchy process (AHP): A case study of foreign affairs ministry," in *Proceedings - 2018 4th International Conference on Computing, Engineering,*

and Design, ICCED 2018, Faculty of Computer Science, University of Indonesia, Indonesia, 2019, pp. 52–56. doi: 10.1109/ICCED.2018.00020.

[11] J. Andress, *The Basic of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, 2nd ed. Syngress, 2011.

[12] A. Elbanna and S. Sarker, "The Risks of Agile Software Development: Learning from Adopters," *IEEE Softw*, vol. 33, no. 5, pp. 72–79, Sep. 2016, doi: 10.1109/MS.2015.150.

[13] A. Zaitsev, U. Gal, and B. Tan, "Coordination artifacts in Agile Software Development," *Information and Organization*, vol. 30, no. 2, p. 100288, Jun. 2020, doi: 10.1016/j.infoandorg.2020.100288.

[14] Digital.ai, "16th State of Agile Report," 2023. Accessed: Nov. 18, 2023. [Online]. Available: https://digital.ai/resource-center/analyst-reports/state-of-agile-report/

[15] I. A. Tøndel, D. S. Cruzes, M. G. Jaatun, and G. Sindre, "Influencing the security prioritisation of an agile software development project," *Comput Secur*, vol. 118, p. 102744, Jul. 2022, doi: 10.1016/j.cose.2022.102744.

[16] M. Humayun, N. Jhanjhi, M. Fahhad Almufareh, and M. Ibrahim Khalil, "Security Threat and Vulnerability Assessment and Measurement in Secure Software Development," *Computers, Materials & Continua*, vol. 71, no. 3, pp. 5039–5059, 2022, doi: 10.32604/cmc.2022.019289.

[17] K. Rindell, J. Ruohonen, J. Holvitie, S. Hyrynsalmi, and V. Leppänen, "Security in agile software development: A practitioner survey," *Inf Softw Technol*, vol. 131, p. 106488, Mar. 2021, doi: 10.1016/j.infsof.2020.106488.

[18] I. A. Tøndel, D. S. Cruzes, M. G. Jaatun, and G. Sindre, "Influencing the security prioritisation of an agile software development project," *Comput Secur*, vol. 118, p. 102744, 2022, doi: https://doi.org/10.1016/j.cose.2022.102744.

[19] G. Bostrm, J. W yrynen, M. Bodn, K. Beznosov, and P. Kruchten, "Extending xp practices to support security requirements engineering," *Proceedings - International Conference on Software Engineering*, vol. 2006-May, pp. 11–17, 2006, doi: 10.1145/1137627.1137631.

[20] C. Pohl and H.-J. Hof, "Secure Scrum: Development of Secure Software with Scrum," *The Ninth International Conference on Emerging Security Information, Systems and Technologies - SECURWARE 2015, Venice, Italy, 2015*, 2015, [Online]. Available: http://arxiv.org/abs/1507.02992

[21] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering – A systematic literature review," *Inf Softw Technol*, vol. 51, no. 1, pp. 7–15, Jan. 2009, doi: 10.1016/j.infsof.2008.09.009.

[22] I. Ghani, Z. Azham, and S. R. Jeong, "Integrating software security into agile-Scrum method," *KSII Transactions on Internet and Information Systems*, vol. 8, no. 2, pp. 646–663, 2014, doi: 10.3837/tiis.2014.02.019.

[23] R. E. Maria, L. A. Rodrigues, and N. A. Pinto, "ScrumS - A model for safe agile development," *7th International ACM Conference on Management of Computational and CollEctive Intelligence in Digital EcoSystems, MEDES 2015*, pp. 43–47, 2015, doi: 10.1145/2857218.2857225.

[24] U. Rafi, T. Mustafa, N. Iqbal, and W.-I. Zafar, "US-Scrum: A Methodology for Developing Software with Enhanced Correctness, Usability and Security," *Int*

J Sci Eng Res, vol. 6, no. 9, pp. 377–383, 2015, [Online]. Available: http://www.ijser.org

[25] K. Rindell, S. Hyrynsalmi, and V. Leppänen, "Securing scrum for VAHTI," *CEUR Workshop Proc*, vol. 1525, pp. 236–250, 2015.

[26] K. Rindell, S. Hyrynsalmi, and V. Leppänen, "Case Study of security development in an agile environment: Building identity management for a government agency," *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pp. 556–563, 2016, doi: 10.1109/ARES.2016.45.

[27] W. Behutiye, P. Karhapää, D. Costal, M. Oivo, and X. Franch, "Non-functional requirements documentation in agile software development: Challenges and solution proposal," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10611 LNCS, pp. 515–522, 2017, doi: 10.1007/978-3-319-69926-4_41.

[28] P. Maier, Z. Ma, and R. Bloem, "Towards a secure SCRUM process for agile web application development," *ACM International Conference Proceeding Series*, vol. Part F1305, 2017, doi: 10.1145/3098954.3103171.

[29] D. Soares Cruzes, M. Gilje Jaatun, K. Bernsmed, and I. A. Tondel, "Challenges and Experiences with Applying Microsoft Threat Modeling in Agile Development Projects," in *2018 25th Australasian Software Engineering Conference (ASWEC)*, IEEE, Nov. 2018, pp. 111–120. doi: 10.1109/ASWEC.2018.00023.

[30] M. Teresa Baldassarre, V. Santa Barletta, D. Caivano, and A. Piccinno, "Integrating security and privacy in HCD-scrum," *ACM International Conference Proceeding Series*, no. Section 3, 2021, doi: 10.1145/3464385.3464746.

[31] G. G. Kagombe, R. Waweru Mwangi, and J. Muliaro Wafula, "Achieving Standard Software Security in Agile Developments," in *2021 The 11th International Conference on Information Communication and Management*, New York, NY, USA: ACM, Aug. 2021, pp. 24–33. doi: 10.1145/3484399.3484403.

[32] P. Loft, Y. He, I. Yevseyeva, and I. Wagner, "CAESAR8: An agile enterprise architecture approach to managing information security risks," *Comput Secur*, vol. 122, p. 102877, Nov. 2022, doi: 10.1016/j.cose.2022.102877.