International Conference of Innovation and Community Engagement - ICoICE
31 October – 1 November 2024
Universitas 17 Agustus 1945 Surabaya

Risk Management Information System in Educational Institution: Agile Scrum Approach

Intan Dzikria
Program Studi Sistem dan Teknologi Informasi, Universitas 17 Agustus 1945 Surabaya
Luvia Friska Narulita *
Program Studi Sistem dan Teknologi Informasi, Universitas 17 Agustus 1945 Surabaya
Achmad Rizal
Program Studi Teknik Informatika, Universitas 17 Agustus 1945 Surabaya
Nabila Amanda Maharani
Program Studi Teknik Informatika, Universitas 17 Agustus 1945 Surabaya
Yusrida Muflihah
Program Studi Sistem dan Teknologi Informasi, Universitas 17 Agustus 1945 Surabaya
Siti Mutrofin
Program Studi Sistem dan Teknologi Informasi, Universitas 17 Agustus 1945 Surabaya
Dian Anita Nuswantara
Program Studi Akuntansi, Universitas Negeri Surabaya
Meylia Elizabeth Ranu
Program Studi Pendidikan Ekonomi, Universitas Negeri Surabaya
Sri Setyo Iriani
Program Studi Manajemen, Universitas Negeri Surabaya
Luqman Hakim
Program Studi Pendidikan Ekonomi, Universitas Negeri Surabaya

Corresponding Author : *luvia@untag-sby.ac.id

Abstract

This study investigates the development of a Risk Management Information System (RMIS) for educational institutions using the Agile Scrum Methodology. The frequent regulatory changes and evolving risk management needs in educational environments require a flexible approach to system development. Agile Scrum, with its iterative and incremental process, was examined for its effectiveness in managing these changes. Data were collected through interviews and observations of Scrum sprints. The results of this study show that Agile Scrum can be used as a method for faster and rapidly changing requirements in the risk management process at educational institutions. This research contributes to both academic knowledge on Agile practices and provides practical insights for educational institutions seeking to improve their risk management systems.

Keywords: Risk Management, ISO 31000, Risk Management Information System, IT Governance, Agile Scrum

Introduction

Risk is about the unknown future due to the possible uncertainties, whether it comes from opportunities or challenges that an organization may face. Risk is defined as the "effect of future uncertainties on the objectives" [1], [2], [3]. Risk management has become critical for organizations in various sectors to govern their business process. According to [1], risk management is "coordinated activities to direct and control an organization with regard to risk". Risk management is traditionally used in the financial sector, and studies found that risk management can add 30% more shareholder value and there was an average increase of 20% in market value [2].

As institutions evolve and expand, they face various risks that can impact their ability to deliver their products or services, including educational institutions. These institutions – kindergarten, elementary, secondary, and higher education – face risks such as operational disruptions to cybersecurity threats. Risk management can support educational institutions to identify, assess and manage risks systematically and structured [4].

To mitigate and control their risks, educational institutions need an information system to analyze and control the risks in a structured manner. Information system plays an essential role in automating, monitoring, and improving risk management processes. However, there are challenges to developing a Risk Management Information System (RMIS) due to the adaptability and responsiveness requirements following the unique business process in educational institutions.

Agile Methodology has gained popularity as a framework for software development management due to its flexibility, iterative approach, and change management adaptability. One of the software development lifecycles that uses Agile and is mostly preferred by businesses is the Scrum framework [5]. Scrum focuses on team collaboration, product increments, and process interactions to achieve goals [6]. This methodology is particularly well-suited for developing information systems like RMIS in educational institutions, where educational stakeholders may evolve rapidly and users' feedback is crucial for system refinement.

Although there are various traditional software development lifecycle methodologies [7], [8] that can be utilized to develop RMIS, the approaches have proven to be rigid and less effective in responding to the continuous changes inherent in the educational environment [9]. Thus, the adoption of Agile practices in RMIS development can ensure that the system not only meets current institutional needs and ISO 31000 requirements but also adapts to future changes. Agile iterative cycles allow for the integration of regulatory updates, risk management process understanding evolution within the institution, and stakeholder engagements.

This study aims to explore the RMIS development for educational institutions using the Agile Scrum approach. This research examines the Scrum process at educational

institution setting, where RMIS is prone to extensive changes due to internal or external regulations, ISO 31000 understanding, and different risk management implementations at the institution. Moreover, this study examines challenges during the Scrum process and provides recommendations for best practices.

This research contributes to a growing body of knowledge aimed at enhancing organizational resilience within educational institutions, by the development of RMIS. The findings will be useful not only for system developers but also for organizations seeking to strengthen the risk management frameworks within their organizations.

Literature Review

ISO 31000 Risk Management

Every organization or institution has risks that can affect the achievement of targets or performance. In ISO 31000, risk is uncertainty that can affect the achievement of goals [3]. The influence can be positive in the form of an opportunity or negative in the form of a threat to achieving goals [1]. Usually, risks are expressed in the form of risk resources, risk events, and the likelihood that risks can occur.

Risk management is a coordinated activity to direct and control an institution with respect to risk [1], or in other words, a structured process that has a purpose in identifying, analyzing, evaluating, monitoring, and controlling risks. It aims to reduce the negative impact (threat) of risks that may arise or can take advantage of the positive impact (opportunity) that exists. In other words, risk management is part of the overall control system [10].

The application of risk management can be carried out in organizations in various sectors. The agribusiness sector, the application of risk management has a role in minimizing the occurrence of work accidents or risks that can threaten the safety of workers [11]. In the healthcare sector, risk management has a role in minimizing the number of accidents or errors in patients, visitors, or hospital employees [12]. It can be concluded that the use of risk management is beneficial to the organization.

According to ISO 31000. The risk management process includes (a) establishing the scope, context, and criteria, (b) identifying risks, (c) analyzing risks, (d) evaluating risks, (e) risk treatment, (f) recording and reporting, (g) monitoring and reviewing, (h) communication and consultation[2]. The process presented looks sequential, but in practice it is repetitive [1], [3].

Risk Management in Educational Institution

Risk management is recognized as a key aspect in the Good Corporate Governance (GCG) of successful institutions [13]. An educational institution should be recognized as a respectable institution that provides high-quality learning [4]. Risk management becomes very important in achieving strategic goals in educational institutions [4]. The implementation of risk

management in educational institutions can maximize in facing various possibilities. The goal is to anticipate and handle all risks, especially those of a high value. [14] revealed that risk management has a significant influence on business performance, including financial and non-financial performance.

The importance of implementing risk management in educational institutions is also written in the regulation of Indonesia's National Accreditation Board for Higher Education Number 3 year 2020 related to indicators and assessment descriptions at point d, namely "Availability of valid evidence related to good practices in the realization of Good University Governance (at least covering aspects of credibility, transparency, accountability, responsibility, and fairness) and risk management" [15]. In terms of compliance, educational institutions should implement risk management [4].

The study conducted by [16] showed that the implementation of risk management resulted in 35 identified risks[11]. The results of the risk findings that have been identified are relevant to universities that are transforming. This shows that the implementation of risk management can influence educational institutions in achieving the goals or objectives achieved.

Agile Scrum

Agile software development is a software development method that allows teams to develop software that has vague and rapidly changing requirements and is based on iterative and incremental models [17]. According to [17], Agile has several main principles that distinguish it from other classic methods, including faster-releasing software continuously, easily accepting changes in requirements, (teams being free to organize themselves, teams are free to work at a pace that can be maintained and being free to review their success and failure rates, and strive for excellence in technical design and implementation.

Almost the same as other classic methods, the process in agile also includes the planning and system analysis stages, but the significant difference lies in the agile timeline where the process will be passed, namely build & release and then testing according to a predetermined product backlog [17].

As the advantages of agile can overcome these problems based on these principles, this is considered an advantage of agile in theory, such as (1) iterative and incremental processes, (2) requirements can change at any time, (3) tracking requirements by looking at the product backlog, (4) active user involvement, (5) faster and periodic releases and functions released at the end of each iteration, (6) testing is done at any time [17].

There are many kinds of agile development methods, but agile scrum will be used in this research. Scrum addresses the gaps in previous frameworks effectively and each release is in line with changing customer demands, the whole process is completely transparent, well-vetted, and adaptable [18]. The product is released in phases called sprints, the duration of sprints is 30 days or less [18]. According to [18] there are 3 scrum phases, as follows (a) pregame, which this phase to defines a tentative vision based on customer expectations and market demand, This vision is continuously modified throughout the process The main objective in this initial phase is to create a Product Backlog which has a list of functional and non-functional requirements in this phase estimated time, cost estimated time and cost plus

need to be reported in number with a number of releases and expected delivery date, (b) game, in this phase Sprint run, A sprint is a process based on a period of one to four weeks in which create, wrap, inspect, and modify the product in question and (c) post-game, in this phase the final product is released, and integration tests are conducted after ensuring that all the set requirements have been met and user guides and training materials are also prepared to facilitate users.

In scrum there is a term called sprint cycle, this is the product backlog that sets guidelines for software, and the scrum master guides the team in its development phase and before the actual delivery of the product [18]. According to [18] the following steps are taken in the overall process called sprint planning and daily scrum, (a) the scrum master and the product owner decide on the requirements, the priority tasks are filtered and guidelines for understanding the user needs are established and (b) the mission is handed to the team members after clearly communicating the requirements. Each sprint is developed and tested as per the guidelines and established priority, as communicated by the master.

Methodology

This study utilised a qualitative research methodology to explore the Agile Scrum approach in the development of a Risk Management Information System (RMIS) for educational institutions. This study focuses on analyzing the Scrum process, emphasising its iterative nature which is essential for managing extensive changes. Data collection was conducted through a combination of systematic literature reviews, interviews with key stakeholders – such as risk management professionals, risk managers in the institution, and the institution's quality assurance department – and observation of the Scrum process. This study examined how Scrum frameworks, including product backlogs, sprint backlogs, sprint planning, and sprint reviews, are applied in the context of an educational institution to accommodate frequent changes.

Product Backlog

A product backlog is one of the core artefacts of the Scrum framework, which lists the requirements for the RMIS being developed in user story format [19]. RMIS product backlog was managed by the product owner, who was responsible for the requirement engineering process and project management. Therefore, the product owner works closely with RMIS users, such as risk managers in educational institutions, at the same time also performed systematic literature reviews on ISO 31000 as a risk management standard, prior studies of risk management at many industrial sectors, and other RMIS as references.

Requirement gathering was performed using interviews and focus discussion groups with a company in Surabaya that has professionally managed risk management. Interviews were also conducted with several managers in the educational institution’s quality assurance

department to understand the risk management process in their institution. Backlog items or requirements are then ordered by priority, with the most important tasks being addressed first in each Scrum sprint.

Sprint Backlog

Sprint backlog represents a subset of items taken from the product backlog, which the development team commits to completing during a specific sprint. Sprint backlog consists of requirements or backlog items that need to be developed during an iteration sprint, and task estimation and assignment [19].

Sprint Planning

A sprint generally lasts two to weeks, in which the team focuses on a set of tasks listed on the sprint backlog. The team, led by Scrum Master, decided which backlog items were placed into which sprint during sprint planning. This study utilized GitHub to help manage the Sprints.

Sprint

During the sprint, the sprint backlog is managed by Scrum Master and developed by the development team. The team processed each requirement into iterations, which consisted of design, development, testing, and release. The sprint backlog was locked during the development process to help the development team focus on the sprint goal, thus delivering a specific set of RMIS features. To support the sprint process, this study utilized Figma for designing the RMIS prototype, Laravel Livewire framework for RMIS web development, and HostedScan Security for system security penetration testing.

Sprint Review

At the end of the sprint, the team reviews the completed work during the sprint review meeting. Any incomplete tasks return to the product backlog for prioritization in future sprints. The sprint review was facilitated by the Scrum Master.

Results and Discussion

Product Backlog

This study has 111 user stories gathered from the requirement elicitation process, which was performed by close discussions with RMIS stakeholders and documentation analysis. RMIS stakeholders identified in this study are the institution, risk management unit, risk owner, and risk officer.

The user stories were included in the product backlog by the product owner, within one year of the requirement elicitation process. The long period of requirement elicitation happened in this study due to the methodologies that this study utilized. This study also used the prototyping method during requirement elicitation to help stakeholders understand the

translation of the risk management business process into an information system process. Table 1 shows a sample of 10 user stories included in the product backlog and the clusterization to the sprint backlogs.

Table 1. RMIS Scrum Product Backlog and Sprint Backlog

No	User Stories	Sprint Backlog
1	As an institution, I want to define and manage KPIs related to all units so that I can track the performance and effectiveness of the risk mitigation process	1
2	As a risk owner and risk officer, I want to manage (create, edit, and delete) the context of risks so that the risk assessment process can be aligned with each unit's KPIs and environment (internal or external).	2
3	As a risk owner and risk officer, I want to identify potential risks in my unit based on the predefined risk contexts, so that I can take proactive measures to mitigate them.	2
4	As a risk owner and risk officer, I want to define risk criteria (likelihood and impact) so that risks can be assessed and prioritized effectively.	3
5	As a risk owner and risk officer, I want to analyze identified risks based on predefined criteria using the Failure Mode and Effect Analysis (FMEA) method so that I can evaluate their potential impact on my unit by using the Risk Priority Number (RPN).	4
	As a risk management unit, I want to manage the effectiveness of risk control measures based on the institution's risk appetite so that I can ensure units are reducing risk to an acceptable level.	1
	As a risk owner and risk officer, I want to create and manage risk treatment plans so that I can assign mitigation actions and ensure timely resolution of risks.	5
	As a risk owner, I want to perform controls in my risk treatment plans so that I can monitor progress and make adjustments to the risk analysis method using FMEA as needed.	5
	As a risk owner and risk officer, I want to document the process of risk management activities communication and consultation with specified stakeholders so that I can monitor stakeholders who have been communicated with or consulted using various methodologies.	6
	As a risk owner and risk officer, I want to create and manage a RACI matrix for risk-related roles so that responsibilities are defined and accountability is established.	6

Sprint Backlog

From 111 user stories in the product backlog, this study separated them into 6 sprints. Each sprint was performed between two and four weeks depending on the development difficulty

levels. Table 1 also shows the sample of how each product backlog was clustered into different sprints based on release prioritization.

System Design Prototype

Figure 1 shows the prototype designed using Figma. This study created a high-fidelity prototype using the user stories that had been created. The prototype was tested using usability testing and resulted in several modifications depending on users' needs and satisfaction. The prototype is the continuation of a prior study by [4] which utilized House of Risk methodology for risk analysis. However, this study changed the method to Failure Mode and Effect Analysis and therefore caused many changes in the prototype design. The prototyping process is included in the Sprint. The final design was then given to the Scrum development team to be developed.

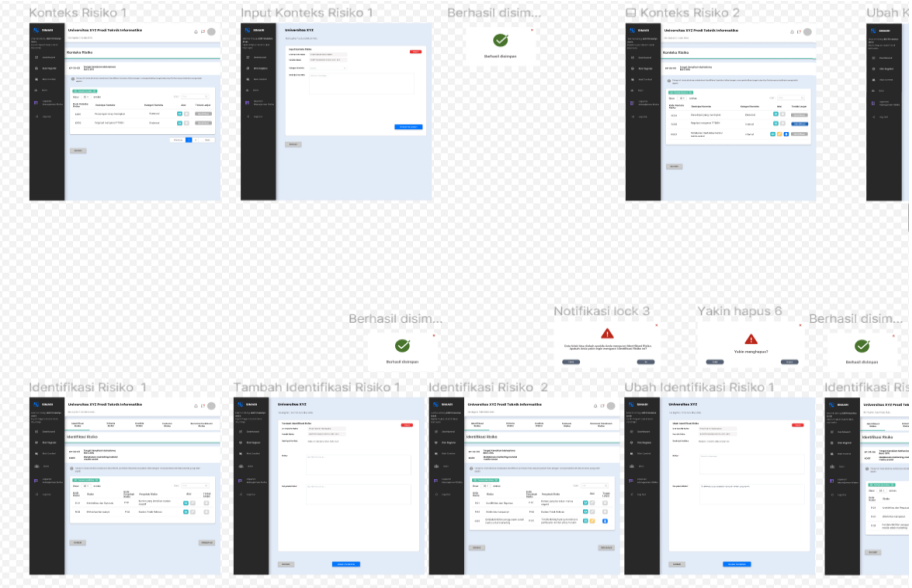

Figure 1. Risk Management Prototype

Actor Dashboard Interface

Figure 2 shows the web interface, that has been developed using the Laravel Livewire framework, of the risk owner dashboard. The dashboard shows the unit's risk owner the total amount of KPIs, risks, and risk controls. In addition, the dashboard also displays a list of risk-ranking based on their Risk Priority Number (RPN).

Risk Identification Interface

The risk identification interface is one of the most important processes because in this stage risk owner or risk officer identifies their risk based on the context that has been created before this stage. In this risk identification process, the actors must input several data such as the risk and its probable cause, as shown in Figure 3.

Risk Analysis Interface

Figure 4 shows the risk analysis phase when the risk owner or risk officer must decide if the risk control is effective. The actors also need to determine the value of three risk assessment criteria such as likelihood, impact, and detection, based on the Failure Mode and Effect Analysis (FMEA) method. The criteria selections are calculated as Risk Priority Number (RPN) values, which automatically decide each risk's severity level.

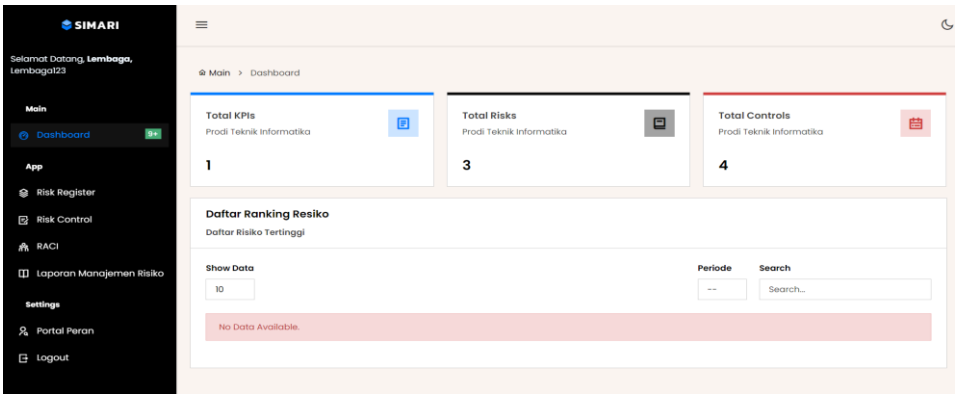

Figure 2. Dashboard Risk Owner Actor

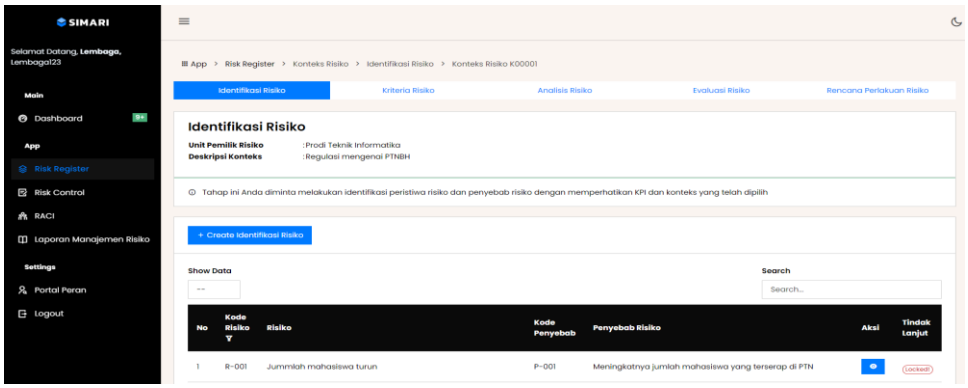

Figure 3. Risk Identification Interface

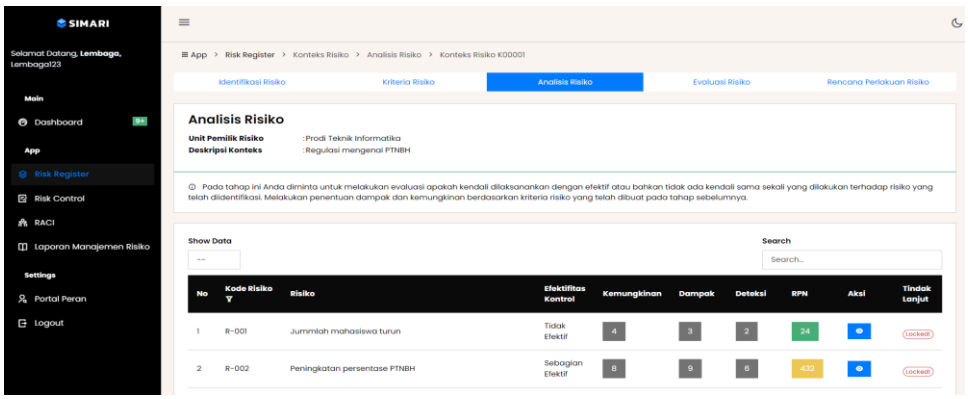

Figure 4. Risk Analysis Interface

Several risk severity level RPN criteria are (1) if the RPN value is under 250 then the risk has a low severity level which is labeled in yellow color, (2) if the RPN value is between 251 and 500 then the risk has medium severity level which is labeled in orange color, (3) if the RPN value is more than 500 then the risk has a high severity level which is labeled in red color.

Risk Control Interface

Figure 5 shows the Risk control web interface, where the risk owner or risk officer must decide on the stakeholders who need to be involved in communication and consultation. This phase shows the importance of the process of how each stakeholder will be communicated or consulted not only through specified stakeholders but also prepared by specified stakeholders.

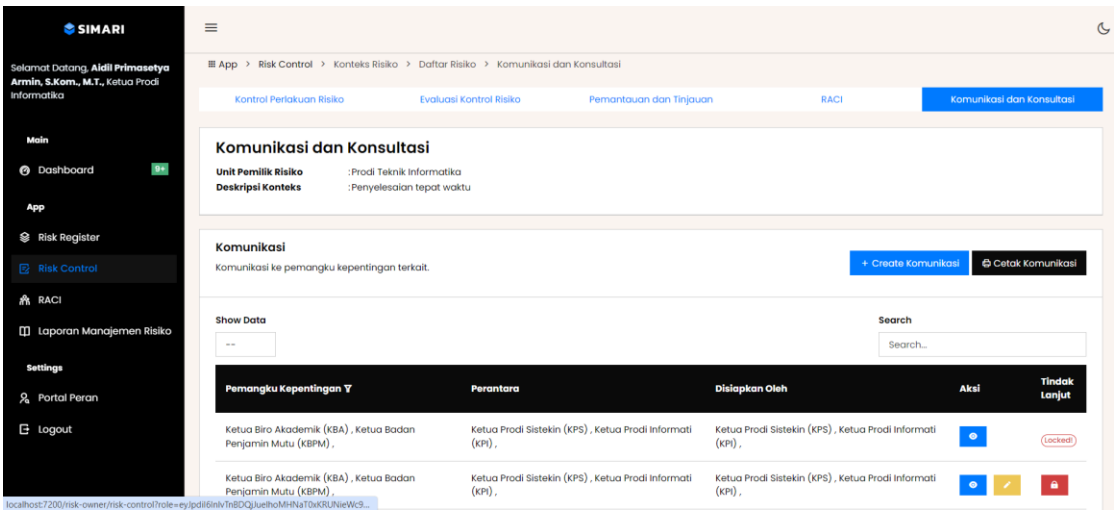

Figure 5. Risk Control Interface

RMIS Penetration Testing

Penetration testing is one of the most used methods to identify and exploit vulnerabilities for information systems, applications, and network infrastructure. In this study, penetration testing was performed by several methodologies using HostedScan Security software, such as Network Mapper (NMAP), Open Vulnerability Assessment System (OVAS), and Open Web Application Security Project (OWASP).

Network Mapper

NMAP is an open-source tool for network security exploration and auditing, NMAP uses raw IP packets to detect network-connected hosts along with the services used, operating system, type of firewall/packet filter used, and several other characteristics [20]. The output is a list of examined target hosts with the key factor being "table port" [20]. The main function of NMAP is as a scanning port, which scans a large amount of probe activities by using automated tools. According to Ronenelly and Pulungan, as cited by [20], a scanner is a program that attacks to TCP/IP ports and other services, and retrieves a response from the computer target, to get valuable information from the target host. According to [21] NMAP is

powerful when used to scan a big network and used to check computer conditions and its ports.

The result of NMAP shows two low vulnerabilities at two ports, which are Open TCP Port 443 and Open TCP Port 80. The vulnerabilities indicate that NMAP on RMIS can be handled without making it a top maintenance priority, although those ports are still need to be improved to increase network security.

Open Vulnerability Assessment System

The OpenVAS is an open-source vulnerability scanning framework that integrates multiple functions, It can scan the network device's related information through the computer network, and then analyze the threat of the target device according to the information contained in the library [22]. On the other side, according to [23] OpenVAS is a vulnerability scanner that is intended to be full vulnerability scanning with various built-in tests and web interfaces that are designed to make rules and operate fast and easy vulnerability scanning with high-level configuration feedback. In this study, OpenVAS results show two low vulnerabilities, such as TCP Timestamps Information Disclosure and ICMP Timestamp Reply Information Disclosure.

TCP Timestamps Information Disclosure is about the remote host implementing TCP timestamps and therefore allowing to compute the uptime as defined by RFC1323/RFC7323. The side effect of this vulnerability is the uptime of the remote host can sometimes be computed. On the other hand, ICMP timestamp reply information disclosure is about a remote host responding to an ICMP timestamp request, which consists of the originating timestamp sent by the sender of the timestamp as well as a receive timestamp and a transmit timestamp. This information could theoretically be used to exploit weak time-based random number generation in other services.

The mitigation of these vulnerabilities is by (a) disabling the support for ICMP timestamp on the remote host completely and (b) protecting the remote host with a firewall, and blocking ICMP packets through the firewall in either direction (either completely or only for untrusted networks). The conclusion is that OpenVAS on RMIS can be handled because the vulnerabilities are on the low level.

Open Web Application Security Project

OWASP is a tool for solving web security problems, such as exploitation, general prevalence, easy detection, and severity of impact this things is used to recognize hazards, understand the threat of web applications, and can also be utilized to better secure websites as well as reduce system risks [24]. According to [24], OWASP can be applied to security testing to obtain significant results. In conclusion, protecting against attacks from reckless parties can benefit from monitoring, detecting, and addressing the vulnerabilities described. According to [25], the main purpose of OWASP is to provide resources, tools, guidelines, and standards related to web application security that can be used by security professionals, software developers, and organizations to recognize, identify, and resolve security

vulnerabilities in web applications. The result of OWASP in RMIS is two vulnerabilities and one medium vulnerability.

Two low vulnerabilities are X-Content-Type-Options Header Missing and Strict-Transport-Security Header Not Set. Moreover, the medium vulnerability is Content Security Policy (CSP) Header Not Set.

X-Content-Type-Options Header Missing allows older versions of internet explorer and chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Therefore, RMIS ensures that the application/web server sets the Content-Type header appropriately, and sets the X-Content-Type-Options header to 'nosniff' for all web pages, to manage this low vulnerability.

On the other hand, HTTP Strict-Transport-Security (HTTS) Header is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) interact with it using only secure HTTPS connections. HSTS is an IETF standards track protocol and is specified in RFC 6797. To solve this low vulnerability, RMIS ensures the web server, application server, load balancer, etc., is configured to enforce Strict-Transport-Security.

Moreover, medium vulnerability is CSP Header Not Set which is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection. The solution to this vulnerability is to ensure that the RMIS web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Conclusion

This study explores the development of a Risk Management Information System (RMIS) tailored to educational institutions using the Agile Scrum Methodology, focusing on the Scrum process, challenges encountered during development, and recommendations for best practices to accommodate frequent changes due to evolving regulations and risk management needs.

The results of this study show that Agile Scrum can be used as a method for faster and rapidly changing requirements in the risk management process at educational institutions. Product owner could work together with the stakeholders to create a product backlog and negotiated the system process to have a clear understanding about the system's user stories. However, this study performed a long period of time to create the product backlog due to the difficulties in understanding risk management process based on ISO 31000.

Despite the long period of requirement elicitation, this study also shows that a complete user stories in product backlog can help the development by Scrum Team faster on the Sprint Backlog that has been divided. Therefore, the RMIS development could be finished at an expected time schedule. The results of the penetration testing also shown that RMIS's security system has been developed well, as can be seen by low level security vulnerabilities that can be fixed and managed.

This study contributes academically to the expansion of the body of knowledge on the application of Agile Scrum in the field of educational institutions and risk management. This study offers a valuable case study on the integration of ISO 31000 standards with information systems, which can be useful for future academic studies on good corporate governance. Moreover, this study also bridges the gap between information technology, risk management, and educational institutions.

From a practical perspective, this study proposes practical guidance for educational institutions on how to develop RMIS that is prone to changes due to regulations and institutional requirements, using the Agile Scrum approach. This study also enhances understanding of how to involve multiple stakeholders in risk management and the best practice implementation of ISO 31000 in an information system.

Although this study contributes to academics and practices, this study still has several limitations. The findings of this study are specific to educational institutions, and may not apply to other sectors or industries. This study does not deeply explore the specific technical platforms used in RMIS development, which could influence the implementation of Scrum. There is a possibility of bias during the interview for data collection, due to the research focus on the perspectives of specific educational institution key stakeholders.

Therefore, future studies may explore alternative methodologies such as Agile Kanban or Extreme Programming to determine the advantages of other Agile methodologies. Future studies may also use a quantitative approach to measure the specific impact of behavioral factors when an institution uses RMIS. Moreover, future research could focus on the user experience and cross-cultural studies in determining the impact of the development and implementation of RMIS in other sectors.

Acknowledgments

This research was supported by University Collaboration Grants from Universitas 17 Agustus 1945 Surabaya and Universitas Negeri Surabaya, for which the authors express their deepest gratitude.

References

[1] ISO, ISO 31000: Risk Management - Guidelines, 31000, 2018.
[2] S. Kumar, 'Risk Management and Enterprise Risk Management', Academia Letters, Jul. 2021, doi: 10.20935/AL2234.
[3] C. R. Vorst, D. S. Priyarsono, and A. Budiman, Manajemen Risiko Berbasis SNI ISO 31000, Jakarta., 2018.

[4] I. Dzikria and N. A. Maharani, 'Analisis Kebutuhan Arsitektur dan Desain Antarmuka Sistem Manajemen Risiko Berbasis Penilaian House of Risk pada Institusi Pendidikan', Jurnal Teknik Informatika dan Komputer, vol. 3, no. 1, pp. 31-39, 2024.
[5] F. A. Dzaky, 'Implementasi Metode Agile Framework Scrum dalam Pengembangan Sistem Informasi Manajemen Aset Terpadu Universitas Diponegoro Modul Inventarisasi', Jurnal Masyarakat Informatika, vol. 14, no. 1, 2023.
[6] I. F. Ashari, A. J. Aryani, and A. M. Ardhi, 'Design and Build Inventory Management Information System using The Scrum Method', JSiI, vol. 9, no. 1, pp. 27–35, Mar. 2022, doi: 10.30656/jsii.v9i1.4050.
[7] A. A. A. Adenowo and B. A. Adenowo, 'Software Engineering Methodologies: A Review of the Waterfall Model and Object-Oriented Approach', International Journal of Scientific & Engineering Research, vol. 4, no. 7, pp. 427–434, 2013.
[8] D. H. Sulistiyawati, L. F. Narulita, and I. A. Brahmaratih, 'Perancangan Sistem Informasi Bumdes Loh Jinawai Desa Galengdowo Wonosalam Jombang', Jurnal Leverage, Engagement, Empowerment of Community, vol. 1, no. 2, pp. 125–132, Nov. 2019, doi: https://doi.org/10.37715/leecom.v1i2.1092.
[9] I. Sommerville, Software engineering, Tenth edition, Global edition. Boston Columbus Indianapolis New York San Francisco Hoboken Amsterdam Cape Town Dubai London Madrid Milan Munich Paris Montreal Toronto Delhi Mexico City São Paulo Sydney Hong Kong Seoul Singapore Taipei Tokyo: Pearson, 2016.
[10] W. Sari, 'Manajemen Risiko pada Perguruan Tinggi', Universitas Trisakti, Jakarta, 2023.
[11] N. I. Mardlotillah, 'Manajemen Risiko Keselamatan dan Kesehatan Kerja Area Confined Space', HIGEIA Journal of Public Health Research and Development, vol. 4, no. 1, pp. 315–327, 2020.
[12] L. G. N. S. Wahyuningsih, N. D. Susanti, N. L. G. H. Nugrahini, P. A. S. Putra, and P. S. Dwwi, 'Implementasi Manajemen Risiko pada Pelayanan Kesehatan: A Literature Review', Jurnal Ilmiah Permas: Jurnal Ilmiah STIKES Kendal, vol. 14, no. 2, pp. 561–570, 2024.
[13] M. S. B. Ariff, N. Zakuan, M. N. M. Tajudin, A. Ahmad, N. Ishak, and K. Ismail, 'A Framework for Risk Management Practices and Organizational Performance in Higher Education', Review of Integrative Business and Economics Research, vol. 3, no. 2, pp. 422–432, 2014.
[14] G. K. Nair, H. Purohit, and N. Choudhary, 'Influence of Risk Management on Performance: An Empirical Study of International Islamic Bank', International Journal of Economics and Financial Issues, vol. 4, no. 3, pp. 549–563, 2014.
[15] Akreditasi Program Studi: Kriteria dan Prosedur, Jakarta., 2019.
[16] H. A. Pradesa, C. O. Purba, and R. Priatna, 'Menilai risiko dari organisasi yang bertransformasi: pelajaran terbaik untuk penguatan akuntabilitas pendidikan tinggi di Indonesia', JAMP, vol. 9, no. 2, pp. 146–158, Sep. 2021, doi: 10.21831/jamp.v9i2.40104.
[17] Fathiah, Z. Rahmi, and H. Nukman, 'PERBANDINGAN METODOLOGY KLASIK DAN AGILE DALAM PENGEMBANGAN SISTEM INFORMASI', Prosiding SNIKOM 204, Mei 2014.

[18] A. Akhtar, B. Bakhtawar, and S. Akhtar, 'EXTREME PROGRAMMING VS SCRUM: A COMPARISON OF AGILE MODELS', Int. J. TIM, vol. 2, no. 2, Oct. 2022, doi: 10.54489/ijtim.v2i2.77.

[19] S. Sachdeva, 'Scrum Methodology', IJECS, vol. 5, no. 6, pp. 16792–16799, Jun. 2016, doi: 10.18535/ijecs/v5i6.11.

[20] S. Dwiyatno, 'ANALISIS MONITORING SISTEM JARINGAN KOMPUTER MENGGUNAKAN SOFTWARE NMAP', Prosisko, vol. 7, no. 2, pp. 108–115, Sep. 2020, doi: 10.30656/prosisko.v7i2.2522.

[21] N. Ardi, S. Putra Pratama, and Y. Servanda, 'Analisis Serangan Forensik Terhadap Serangan Ddos Ping Of Death Menggunakan Tools Nmap Dan Hping3', Jurnal Jurnal Sains Dan Teknologi (JSIT), vol. 4, no. 2, pp. 2807–7393.

[22] Y. Xia, J. Wang, C. Liu, and K. Yu, 'Design and Implementation of Vulnerability Scanning Tools for Intelligent Substation Industrial Control System Based on Openvas', in IOP Conference Series: Earth and Environmental Science, Institute of Physics Publishing, Mar. 2020. doi: 10.1088/1755-1315/440/4/042031.

[23] D. Laksmiati, 'VULNERABILITY ASSESSMENT PADA SITUS WWW.HATSEHAT.COM MENGGUNAKAN OPENVAS', Jurnal AKRAB JUARA, vol. 5, no. 3, 2020.

[24] K. Nisa, A. Putra, R. A. Siregar, and M. Dedi Irawan, 'Bulletin of Information Technology (BIT) Analisis Website Tapanuli Tengah Menggunakan Metode Open Web Application Security Project Zap (Owasp Zap)', vol. 3, no. 4, pp. 308–316, 2022, doi: 10.47065/bit.v3i1.

[25] J. Khatib Sulaiman and U. Pakuan, 'Analisis Keamanan Website Menggunakan Open Web Application Security Web (OWASP) I Wayan Sriyasa, Victor Ilyas Sugara', Indonesian Journal of Computer Science.