Strategy Indicators for Secure Software Development Lifecycle in Software Startups Based on Information Security Governance

Doddy Ferdiansyah[1*], R. Rizal Isnanto[2] and Jatmiko E. Suseno[3]

[1*] Research Student, Department of Information System Doctoral, Diponegoro University, Semarang, Indonesia.
Department of Informatics Engineering, Pasundan University, Bandung, Indonesia.
doddyferdiansyah@students.undip.ac.id, Orcid: https://orcid.org/0000-0001-7552-3904

[2] Department of Computer Engineering, Diponegoro University, Semarang, Indonesia.
rizal@lecturer.undip.ac.id, Orcid: https://orcid.org/0000-0002-6044-0644

[3] Department of Physics, Diponegoro University, Semarang, Indonesia.
jatmikoendro@lecturer.undip.ac.id, Orcid: https://orcid.org/0000-0003-2218-2995

Received: July 26, 2023; Accepted: September 30, 2023; Published: November 30, 2023

Abstract

The development of startup software is massive because many services have turned digital. Various applications have emerged that match their functions by taking advantage of the momentum of digital transformation. For example, applications for the Education sector, industrial sector, and economic sector. With their top priority being generating applications, the security factor becomes less of a concern. This is evidenced by the many data breaches that have caused losses to serious companies and public institutions. This is where the role of top-level management emerges in restructuring the company's strategy, especially software startups, to support producing more secure applications. In this study, the RACI matrix is used to determine who is suitable for implementing a security strategy in information security governance within the organizational structure of the software startup. Where this study starts from stakeholder identification, top-level management roles in software startup, and activities in the secure software development lifecycle. And the results of this study are strategy indicators that are suitable for software startup.

Keywords: Information Security Governance, RACI Matrix, Software Startup, Strategy, Top-level Management.

1 Introduction

The development of software development used by some software startups began to leave the old methods slowly. They switched to agile and collaborative software development methods (Masood, Z., 2022). Likewise with software produced by startups, the security aspect of the product from startup software must be improved. Because software security is a very important concern and security activities need to support the software development cycle process (Alenezi, M., 2022). Various types of

Journal of Interner Services and Information Security (JISIS), volume: 13, number: 4 (November), pp. 104-113
DOI: *10.58346/JISIS.2023.I4.007*

*Corresponding author: Research Student, Department of Information System Doctoral, Diponegoro University, Semarang, Indonesia.

Department of Informatics Engineering, Pasundan University, Bandung, Indonesia.

technologies have been developed to address this need, such as static analysis tools, dynamic analysis tools, and penetration testing tools. However, despite the recognition of the need for cases that deal with the full lifecycle of secure software development, only a few have been reported (Saito, M., 2015). Developing software without prioritizing security can have a significant impact, such as data loss or leakage, loss of trust, and loss of reputation for software startups (Firdaus, A., 2014). So, for a software startup, besides assets in the form of software products such as software as a service, another asset that must be maintained is the software development method they apply (Parthasarathy, S., 2022) (Suominen, A., 2017). By applying a software development method that is suitable for software startups and has met the needs of stakeholders, the success rate of the resulting software product will be even better (Parthasarathy, S., 2022). One is increasing the security factor in the software development process or the secure software development lifecycle. For example, some of the safe software development methods that are used as best practices in the world today are the Microsoft security development lifecycle, the Building Security in Maturity Model (BSIMM), and the OWASP Software Assurance Maturity Model (OWASP SAMM), and others (Iovan, M., 2022).

However, not all software startups successfully implement good software development methods, the impact occurs in data loss and huge economic loss. This can happen because of the challenges of the startups themselves and high level of global interconnection and digitization of their operations (Romero, R., 2023). As mentioned by Suominen, software startups face challenges including the lack of experience, limited resources, influence from several entities (Suominen, A., 2017), and dynamic markets and technologies to enter the target market with high potential (Paternoster, N., 2014). Not only that, when it comes to software startups, the characteristics of the organizations within them are very different from those of larger companies (Grammatopoulos, A.V., 2022). And one of the characteristics that causes the failure of startup software is that they prefer risky decisions on the resulting product rather than a secure one (Nurcahyo, R., 2018). So, from the explanation above it can be concluded that the role of top-level management is needed in supporting making the right strategy in implementing secure software development lifecycle (SSDL) in producing their software products.

Top-level management roles in software startup determine the success of the SSDL implementation strategy. The main objective in this study, to determine the appropriate roles in software startup, we use the RACI Model with three main steps, namely identifying stakeholders related to startup software, then identifying what top-level roles are currently being carried out by startup software, and finally identify what activities are in SSDL. In this case, one of the SSDL methods is used, namely the Building Security in Maturity Model (BSIMM), which focuses only on the strategy section (Migues, S., 2022).

2 Methodology

In conducting this study, several steps were taken to solve the problems raised in this study. The steps taken are to determine the research framework, identify stakeholders, identify roles that will be determined as top-level management, and identify what activities are involved in the secure software development lifecycle (SSDL) process. One of the SSDL methods used in this study is BSIMM, where the domains in BSIMM consist of 4 domains namely governance, intelligence, SSDL touchpoints, and deployment. In this study, the domain that is our focus is Governance. For activities in the governance domain, it consists of 3 namely strategy & metrics (SM), Compliance & Policy (CP), and Training (T) (Migues, S., 2022). Specifically for this study, we only take strategy & matrix (SM) activities which will be mapped with identification results from stakeholders and the role of top-level management in startup software. After carrying out all these steps, the results require discussion regarding the results produced.

Research Framework

This study uses the RACI matrix method to determine the roles and responsibilities at the top-level management for all SSDL activities. The RACI matrix is a tool for describing job responsibilities (Suhanda, R.D.P., 2021) and the roles of stakeholders and using interests and influence to classify stakeholders in the form of a matrix (Hirmer, S.A., 2021). Usually, the RACI matrix describes the relationship between jobs and determines the roles, responsibilities, and levels of authority for each activity. Another term that is more often seen by others is called the RACI matrix RACI stands for

- Responsible: Who is going to be completing the task?
- Accountable: Who is ultimately responsible for a task and can also delegate to those who are Responsible?
- Consulted: Who will need consulting about the activity, and where will there be two-way communication on the matter?
- Informed: Who must be kept informed, although there is just one-way communication?

To create a RACI matrix, several steps must be met. The first step is to define or identify all tasks. The second step is to list all stakeholders with interest in the project. The third step is to fill the sections determining who is responsible and accountable. It would help if those who will be consulted and informed before doing every task are also mentioned. The fourth step is to ensure that everyone has at least one stakeholder, and they will be responsible for each task (Tom Hilman., 2021) (Templatelab., 2022). The RACI matrix is made into three stages, namely, process identification, stakeholder identification, and RACI matrix mapping (Lee, W.Y., 2021).

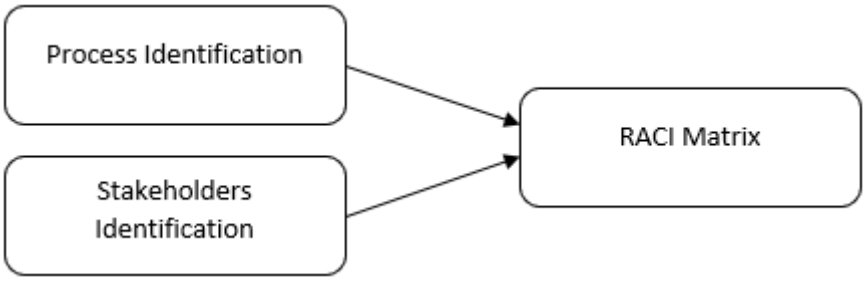

Figure 1: Three Stages of the RACI Matrix

Identification of Stakeholders in Software Startup

In this first study, we interviewed the Chief Executive Officer (CEO) of a software startup in Bandung, Indonesia. The results of interviews regarding what roles are in the startup software are as follows:

Table 1: List of Stakeholders and Description

No	Role	Description
1	CEO	The Chief Executive Officer (CEO) is the highest position in a company. His responsibilities as the Board of Trustees for the company's success or failure (Strutzel, D., 2020).
2	CTO	The Chief Technology Officer (CTO) is responsible for the technology vision and execution of a company (Alan Williamson., 2022).
3	Web Development Director	The Director of Web Development will manage team members and contribute to team web development and growth.

4	Mobile Development Director	The Director of Mobile Development will manage team members and contribute to team mobile development and growth.
5	Backend Developer	Backend Developers are the experts who build and maintain the mechanisms that process data and perform actions on websites.
6	Frontend Developer	A Frontend Developer is a person who will use any of the frameworks or the packages such as Jquery, Angular JS, Angular JS 2, NodeJS, ReactJs, backboneJS, and Bootstrap.
7	Mobile Developer	A mobile developer creates software for mobile devices and technology.
8	DevOps Engineer	A DevOps Engineer introduces processes, tools, and methodologies to balance the needs throughout the software development life cycle, from coding and deployment to maintenance and updates.
9	UI/UX Designer	A UX/UI Designer carries out user research first and then implements the findings in the visual design in mockups, wireframes, and prototypes.
10	Customer Service	Customer Service is the direct one-on-one interaction between a consumer making a purchase and a representative of the company selling it.

Identify Top-Level Roles in Software Startup

According to Shenghui et al., the role structure of top management is very important in cooperating among members of top management in directing the organization and forming strategy (Ma, S., 2022). In a formal organization, the structure of the top management team consists of various types of roles, such as the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Chief Strategy Officer (CSO), Chief Marketing Officer (CMO), Chief Digital Officer (CDO), Chief CSR officer (Ma, S., 2022), Chief Technology Officer (CTO) (Nathan J. Hiller., 2013) (Frank Tietze., 2007), and Chief Information Security Officer (CISO) (Monzelo, P., 2019). Each position in top management is very important in carrying out organizational activities according to their roles and responsibilities (Ma, S., 2022). Table 2 shows the mapping of the top-level management structure on startup software with the formal organizational structure based on (Ma, S., 2022).

Table 2: Mapping Top-level Management Structure to Formal Organization Structure in Software Startups

No	TLM software startup	TLM formal organization	Status
1	CEO	CEO	Suitable
2	CTO	CTO	Suitable
3	Web Development Director	COO	Not suitable
4	Mobile Development Director	CFO	Not suitable
5	Backend Developer	CSO	Not suitable
6	Frontend Developer	CMO	Not suitable
7	Mobile Developer	CDO	Not suitable
8	Dev Ops	Chief CSR Officer	Not suitable
9	UI/UX Designer	CISO	Not suitable
10	Customer Service	–	Not suitable

Table 2 shows that there are only two roles in top-level management in software startups that follow the organization's formal top-level management standards, CEO and CTO.

Activity Identification on SSDL

In the SSDL, many methods can be applied by a software startup. One of the SSDL methods applied in this study is the Building Security in Maturity Model (BSIMM). The BSIMM studies current software security initiatives or programs. It quantifies the application security (appsec) practices of different organizations across industries, sizes, and geographies while identifying the variations that make each organization unique (Migues, S., 2022). In the BSIMM, there is one clause called strategy and metrics. Table 3 shows some of the activities in this clause.

Table 3: Activity Strategy and Metrics in the Building Security in Maturity Model (BSIMM)

Code	Activity
SM1.1:98	Publish process and evolve as necessary
SM1.3:82	Educate executives on software security
SM1.4:117	Implement security checkpoints and associated governance.
SM2.1:73	Publish data about software security internally and use it to drive change
SM2.2:63	Enforce security checkpoints and track exceptions
SM2.3:69	Create or grow a satellite (security champions)
SM2.6:71	Require security sign-off prior to software release.
SM2.7:64	Create evangelism role and perform internal marketing
SM3.1:27	Use a software asset-tracking application with a portfolio view.
SM3.2:18	Make SSI efforts part of external marketing.
SM3.3:26	Identify metrics and use them to drive resourcing.
SM3.4:5	Integrate software-defined lifecycle governance.
SM3.5:0	Integrate software supply chain risk management.

3 Results

From the role mapping process under the organization's formal top-level management, the software startup case consists of two roles: CEO and CTO. From these two roles, a mapping of the activities in the SSDL in the BISMM is created, as shown in Table 4.

Table 4: Results from the RACI Matrix for Each Activity in the Secure Software Development Lifecycle (SSDL)

No	Activity	Stakeholder	
		CEO	CTO
A1	Publish process and evolve as necessary.	A, I	R
A2	Educate executives on software security.	R	C
A3	Implement security checkpoints and associated governance.	A, I	R
A4	Publish data about software security internally and use it to drive change.	R	C
A5	Enforce security checkpoints and track exceptions.	R	C
A6	Create or grow a satellite (security champions).	R	C
A7	Require security sign-off prior to software release.	A	R
A8	Create evangelism role and perform internal marketing.	R	C
A9	Use a software asset-tracking application with a portfolio view.	I	R
A10	Make SSI efforts part of external marketing.	R	C
A11	Identify metrics and use them to drive resourcing.	I	R
A12	Integrate software-defined lifecycle governance.	I	R
A13	Integrate software supply chain risk management.	R	C

Table 4 concludes that a software startup implementing an informal role structure in top-level management will result in interpersonal conflicts within the top management team. Additionally, the workload of the CEO and CTO will be even greater. From table 4 above, the number of roles that must be carried out by the CEO and CTO is very large. This can be analyzed using two ways, namely vertical analysis and horizontal analysis. first, the results of calculating R, A, C, I from the vertical direction are as follows.

Table 5: Total RACI of Vertical

CEO	Total	CTO	total
R	7	R	6
A	3	A	0
C	0	C	7
I	5	I	0

With a total of 7 responsible, the CEO has the most roles in carrying out his work followed by the CTO who has 6 responsible. In the second row, there are 3 accountable CEOs, while the CTO does not have an accountable role. then in the third row, the CEO does not have a consulted role while the CTO has a consulted role of 7. Finally, the CEO has an informed role of 5 and the CTO does not have an informed role. Now seen from the results of the horizontal analysis.

Tabel 6: Total RACI of Horizontal

Activities	Total			
	R	**A**	**C**	**I**
A1	1	1		1
A2	1		1	
A3	1	1		1
A4	1		1	
A5	1		1	
A6	1		1	
A7	1	1		
A8	1		1	
A9	1			1
A10	1		1	
A11	1			1
A12	1			1
A13	1			1

4 Discussion

By using the RACI Matrix, it has effectively mapped the responsibilities of top-level management, particularly the CEO and CTO, in ensuring information security. One key aspect of your research is the recognition that the roles of the CEO and CTO in software startups are numerous and intense in the context of information security. This finding emphasizes the significance of their involvement and active participation in driving secure software development practices. The results of the study show that with the many roles performed by CEOs and CTOs in developing secure software, startup software will experience a phase of performance instability. According to Shenghui Ma, if an organization applies for an informal role in the organizational structure, it will impact organizational performance (Ma, S., 2022). Moreover, according to Jose Santisteban and David Mauricio, a product and/or service's high performance satisfies customers' needs (Santisteban, J., 2021). When analyzed from the vertical, the

CEO and CTO have the most responsible roles. And this can be interpreted that both roles are critical roles which if one fails to carry out its role then the secure software development process will not be achieved. Then, the many responsible burdens that are owned by the two roles are very ineffective in an organization. But on the other hand, if analyzed horizontally (see Table 6), startup software has clear responsibilities. who does the work, who makes the decisions and who gets the information from the work.

When an organization's performance is disrupted, the resulting software product does not match the user's needs. What is very worrying is that when a startup shows symptoms like that, the startup software will be at risk of failure because perceived performance influences a startup's success. By implementing effective strategies and indicators, organizations can create a robust framework to safeguard their software products and sensitive data. This is especially critical for startups, as they often face resource constraints and heightened risk due to their innovative and dynamic nature. Therefore, to mitigate the risk of failure for software startups resulting from insecure software products and non-compliance with security practices or culture in software development, it is necessary to create an explicit security strategy roadmap. According to Volchkov, there are 5 indicators that are part of the security strategy (Volchkov, A., 2018):

1. External environment and business context
2. Legal and regulatory framework and its impact
3. Changes in threats, vulnerabilities, technologies, and risk appetite
4. Company culture
5. Requirements for explicit alignment with certain business initiatives or strategies.

The use of the RACI Matrix as a mapping tool provides a structured approach to identifying and assigning responsibilities within the organization. This methodology allows software startups to clearly define roles and ensure accountability for information security practices, contributing to a more secure software development lifecycle. RACI Matrix is a useful tool for assigning responsibilities and tasks, but it is not the only technique that should be used to implement ISG. Other techniques, such as risk management, business and security process management, are also needed to ensure that ISG is implemented in a way that meets the needs of the business (Moghadam, R.S., 2018). Therefore, with the above-mentioned strategy indicators and the implementation of the RACI matrix model for software startups, then in the next study, we will emphasize the need for a comprehensive strategy that involves the CEO and CTO, and involve from top management (Pinto, L., 2022) in all stages of the software development lifecycle. This includes formulating security policies, allocating resources, implementing security controls, and fostering a security-conscious culture within the organization. By engaging top-level management, software startups can prioritize information security and integrate it into their overall business strategy.

5 Conclusion

As said by Alenezi et al, a software that is less secure is because the developer does not have security knowledge itself (Alenezi, M., 2022) (Saito, M., 2015). This security knowledge does not only apply to programmers or operators, but also must be possessed by top-level management. So, what the startup software wants with the goal of SSDL can run together. A comprehensive strategy for secure software development lifecycle in software startups should heavily involve the CEO and CTO. Their responsibilities should encompass key aspects such as establishing security policies, allocating resources for security measures, monitoring security controls, and fostering a culture of information security within the organization.

In the case of this study, the roles of the CEO and CTO in software startups are numerous and have high intensity. The worry is that they will get stressed more quickly and result in ineffective decision-making by them as top-level management. As AlGhamdi et al said, top management is very importance to engage their responsibility toward providing the required support for ISG (AlGhamdi, S., 2020). Even though the roles and responsibilities are good. Suggestions for startup software that has the RACI matrix results above are that the CEO and CTO must be able to shift some of the responsibilities they carry to the middle level management and lower-level management. So that the load will be more evenly distributed and balanced, and the management will be better in determining the strategy in software startup. When they are on the same path, the resulting software product will be safer, although according to Al-Dhahri et al, in dealing with security in a system, no one can guarantee 100% security of the system (Al-Dhahri, S., 2017). So, the importance of information security governance in software startups and emphasizes the significant roles of the CEO and CTO in ensuring secure software development practices. By recognizing and addressing these responsibilities, software startups can enhance their overall security posture, security culture (AlGhamdi, S., 2020) and protect their software and sensitive data from potential threats.

References

[1] Alan Williamson. (2022). Think Like a CTO. *Published by Manning Publications*.
[2] Al-Dhahri, S., Al-Sarti, M., & Abdul, A. (2017). Information security management system. *International Journal of Computer Applications*, *158*(7), 29-33.
[3] Alenezi, M., Basit, H.A., Beg, M.A., & Shaukat, M.S. (2022). Synthesizing secure software development activities for linear and agile lifecycle models. *Software: Practice and Experience*, *52*(6), 1426-1453.
[4] AlGhamdi, S., Win, K.T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*.
[5] Firdaus, A., Ghani, I., & Jeong, S.R. (2014). Secure feature driven development (SFDD) model for secure software development. *Procedia-Social and Behavioral Sciences*, *129*, 546-553.
[6] Frank Tietze., Cornelius Herstatt. (2007). The Role of the Chied Technology Officer – Responsibilities, Skills & Qualifications and Organizational Integration. *14th International Product Development Management Conference*.
[7] Grammatopoulos, A.V., Politis, I., & Xenakis, C. (2022). Blind software-assisted conformance and security assessment of FIDO2/WebAuthn implementations. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *13*(2), 96-127.
[8] Hirmer, S.A., George-Williams, H., Rhys, J., McNicholl, D., & McCulloch, M. (2021). Stakeholder decision-making: Understanding Sierra Leone's energy sector. *Renewable and Sustainable Energy Reviews*, *145*.
[9] Iovan, M., Cruzes, D.S., & Johansen, E.A. (2022). A Framework for a Sustainable Software Security Program. *Evolving Software Processes: Trends and Future Directions*, 47-69.
[10] Lee, W.Y., Lee, S.H., Jin, C., & Hyun, C.T. (2021). Development of the RACI Model for Processes of the Closure Phase in Construction Programs. *Sustainability*, *13*(4), 1-25.
[11] Ma, S., Kor, Y.Y., & Seidl, D. (2022). Top management team role structure: A vantage point for advancing upper echelons research. *Strategic Management Journal*, *43*(8), O1-O28.
[12] Masood, Z., Hoda, R., Blincoe, K., Damian, D. (2022). Like, Dislike, or Just Do It? How developers approach software development tasks. *in Information and Software Technology 150*.
[13] Migues, S., Steven, J., Ware, M. (2022). Building Security in Maturity Model (BSIMM) Version 13. *Creative Commons Attribution-Share Alike 3.0*.
[14] Moghadam, R.S., & Colomo-Palacios, R. (2018). Information security governance in big data environments: A systematic mapping. *Procedia computer science*, *138*, 401-408.

[15] Monzelo, P., & Nunes, S. (2019). The Role of the Chief Information Security Officer (CISO) in Organizations.
[16] Nathan J. Hiller., Marie-Michele Beauchesne. (2013). Executive Leadership: CEOs, Top Management Teams, and Organizational-Level Outcomes. *in The Oxford Handbook of Leadership and Organizations*, 556-586.
[17] Nurcahyo, R., Akbar, M.I., & Gabriel, D.S. (2018). Characteristics of startup company and its strategy: Analysis of Indonesia fashion startup companies. *International Journal of Engineering & Technology*, *7*(2.34), 44-47.
[18] Parthasarathy, S. (2022). A Decision Framework for Software Startups to Succeed in COVID-19 Environment. *In Decision Analytic Journal 3*.
[19] Paternoster, N., Giardino, C., Unterkalmsteiner, M., Gorschek, T., & Abrahamsson, P. (2014). Software development in startup companies: A systematic mapping study. *Information and Software Technology*, *56*(10), 1200-1218.
[20] Pinto, L., Brito, C., Marinho, V., Pinto, P. (2022). Assessing the Relevance of Cybersecurity Training and Policies to Prevent and Mitigate the Impact of Phishing Attacks. *Journal of Internet Services and Information Security*, *12*(4), 23-38.
[21] Romero, R., Sanchez-Ancajima, R.A., Lopez-Cespedes. J.A., Saavedra-Lopez, M.A., Tarrillo, S.J.S., Hernandez, R.M. (2023). Security Model for a Central Bank in Latin America using Blockchain. *Journal of Internet Services and Information Security*, *13*(2), 117-127.
[22] Saito, M., Hazeyama, A., Yoshioka, N., Kobashi, T., Washizaki, H., Kaiya, H., & Ohkubo, T. (2015). A case-based management system for secure software development using software security knowledge. *Procedia computer science*, *60*, 1092-1100.
[23] Santisteban, J., Mauricio, D., & Cachay, O. (2021). Critical success factors for technology-based startups. *International Journal of Entrepreneurship and Small Business*, *42*(4), 397-421.
[24] Strutzel, D. (2020). *30 Days to a More Powerful Business Vocabulary: The 500 Words You Need to Transform Your Career and Your Life*. Gildan Media LLC aka G&D Media.
[25] Suhanda, R.D.P., & Pratami, D. (2021). RACI matrix design for managing stakeholders in project case study of PT. XYZ. *International Journal of Innovation in Enterprise System*, *5*(02), 122-133.
[26] Suominen, A., Hyrynsalmi, S., Still, K. (2017). Software Start-up Failure an Exploratory Study on the Impact of Investment. *In IWSECO*, 55-64.
[27] Templatelab. (2022). How to Make a RACI Matrix? https://templatelab.com/raci-chart/#How_to_Make_a_RACI_Matrix
[28] Tom Hilman. (2021). Make Governance Easy with A RACI Matrix. https://immutableinc.io/make-governance-easy-with-a-raci-matrix/
[29] Volchkov, A. (2018). *Information security governance: Framework and toolset for CISOs and decision makers*. CRC Press.

Authors Biography

Doddy Ferdiansyah is a doctoral student in the Information Systems department at Diponegoro University in Semarang. His area of expertise lies in information security and information security management, which are also the focus of his current dissertation research. He obtained his master's degree in 2014 and currently works as a lecturer at Pasundan University in Bandung.

R. Rizal Isnanto is a digital economics lecturer in the doctoral program of information systems at Diponegoro University in Semarang. He completed his doctoral program in the field of electrical engineering in 2013 at Gadjah Mada University in Yogyakarta. Recently, he obtained the position of full professor and the title of professor at Diponegoro University in Semarang. Currently, he serves as the secretary of the doctoral program in information systems at Diponegoro University in Semarang.

Jatmiko Endro Suseno is a lecturer and physicist who teaches in the physics program at Diponegoro University in Semarang. He earned his PhD in electrical engineering in 2012 from the Universiti Teknologi Malaysia. He holds a certification as a medical physicist and currently serves as the secretary of the undergraduate physics program at Diponegoro University in Semarang.