International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

Application of Structural Equation Modelling to Cyber Security Maturity Level in Indonesian Private Sector

Dinisfusya'ban[1], *Bambang Suharjo[2], Richardus Eko Indrajit[3]*

[1]*Master of Cyber Defense Engineering*
Indonesian Defense University
Bogor, Indonesia
dinisfuyaban@tp.idu.ac.id

[2]*Science and Technology Indonesia Naval Academy*
STTAL
Jakarta, Indonesia
bambang_suharjo@tnial.mil.id

[3]*Pradita University*
Banten, Indonesia
eko.indrajit@pradita.ac.id

Abstract — This study investigates cybersecurity maturity in the Indonesian private sector, vital for sustaining operations in the Industry 4.0 era. Using Structural Equation Modeling (SEM), data from 23 companies were analyzed to evaluate the relationship between 5 key aspects—Governance, Identification, Protection, Detection, and Response—and their 29 sub-aspects. While significant correlations were observed between aspects and their sub-aspects, the relationships among the main aspects themselves were weak, indicating their independence. Sub-aspects such as compliance, identification reporting, and user management emerged as critical contributors to maturity levels, emphasizing the need for adherence to standards, robust reporting mechanisms, and user management. This research provides a theoretical model that enables organizations to assess their cybersecurity maturity, identify improvement areas, and enhance strategic responses to evolving threats. The findings contribute to developing more effective cybersecurity policies and frameworks, ensuring the private sector can adapt to emerging challenges while laying the groundwork for future studies.

Keywords — mathematical modelling, cybersecurity maturity level, cybersecurity framework, structural equations modelling.

I. INTRODUCTION

The development and deployment of information technology (IT) and operational technology (TO) in the era of Industry 4.0 has resulted in substantial changes in a variety of industrial sectors. The implementation of Industry 4.0 concepts and technology has found applications in different fields of industry, revolutionizing the production and distribution of products or services in terms of boosting productivity, quality and. efficiency [1]. This change not only affects the standard of functioning of people and the state as a whole, but it also presents new risks linked to the implementation of modern technology [2].

In this context, cybersecurity is a key pillar in ensuring the long-term viability of production and industry. Cybersecurity is also an important part of a nation's resilience to complex threats, which have become an important obstacle to global security in the twenty-first century [3]. Globalization, increased use of digital technology, demography, geopolitics, and inter-country conflict have all contributed to the multifaceted nature of complex threats. Countries around the world have taken significant steps to improve their ability to deal with complex threats and to improve resilience, that include in the area of cybersecurity [4].

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

Cybersecurity plays an important role in modern society due to rising cybercrime and increasing reliance on digital platforms [5]. This is important to protect sensitive information, systems, and networks from cyber attackers who aim to disrupt normal processes and steal valuable data [6]. Organizations and governments implement policies and regulations to prevent cybercrime, highlighting the importance of cybersecurity in safeguarding information in various sectors [7].

Given the increasingly challenging cybersecurity landscape, the private sector in Indonesia faces an urgent need to measure and improve cybersecurity maturity levels. The level of Cybersecurity Maturity (CSM), is an important indicator that reflects the extent to which organizations can protect their information assets from cyber threats. CSM is a measurement tool for Cyber Security instruments introduced by the National Cyber and Crypto Agency (BSSN) [8]. This CSM provides guidelines covering five main aspects: governance, identification, protection, detection, and response. Each of these aspects consists of more specific sub-aspects, which can be measured through a series of related questions.

This study aims to apply Structural Equation Modelling (SEM) as an analytical tool to measure and understand the relationship between aspects and sub-aspects of CSM in the private sector in Indonesia. Structural Equation Modeling (SEM) is a powerful multivariate quantitative technique used to analyze complex relationships between observed variables [9] [10] [11]. SEM allows researchers to test theoretical models, validate hypotheses, and explore complex relationships among constructs [12]. Using SEM, researchers can uncover the factors that are most significant in influencing cybersecurity maturity and how interactions between them can optimize cybersecurity strategies. This is particularly relevant given that the private sector is often a prime target for cyberattacks because it has sensitive data and valuable assets.

In Indonesia, the importance of cybersecurity maturity level analysis is becoming increasingly relevant (BSSN, 2023). This study aims to apply SEM structural equation modeling to analyze the level of cybersecurity maturity in Indonesian private sector organizations. The application of CSM is important to identify and classify cyber threats according to emerging trends and solve them with new emerging techniques [13].

Through this research, it is hoped that a robust and reliable SEM model can be obtained to measure the level of cybersecurity maturity. This model will not only provide insight into the current state of cybersecurity, but will also assist organizations in identifying areas that require attention and improvement. In addition, the results of this study are expected to contribute to the development of more effective cybersecurity policies and practices in Indonesia, as well as provide references for similar research in the future.

Problem and Research Questions

Given the importance of cybersecurity in supporting the resilience of private sector organizations in Indonesia, this study aims to develop a basic theoretical model of the factors influencing the level of cybersecurity maturity. This research will answer the following research questions:

1. How can Structural Equation Modelling (SEM) be used to analyze and measure the level of cybersecurity maturity (CSM) in Indonesia's private sector?
2. What are the most significant factors influencing the level of cybersecurity maturity in Indonesia's private sector?
3. How is the correlation between CSM aspects and sub-aspects in the assessment of cybersecurity maturity in Indonesia's private sector?

This study used data obtained from questionnaires addressed to respondents in Indonesian private sector organizations during 2022. The data is evaluated and analyzed using confirmatory factor analysis and SEM methods.

II. Research Data and Tool

A. Research Data

This research based on data obtained from January 2022 to December 2022, with a sample of private companies that have information technology services. Data samples were obtained from 23 private companies in Indonesia.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

B. Research Tool

In this study, the scope of CSM measurement instruments consists of 5 main aspects with the number of derivatives as many as 29 sub-aspects. Each sub-aspect is measured by a number of questionnaire questions that vary with a total of 267 questions, so it can be described as follows:

1. The Governance aspect consists of 6 sub-aspects (Awareness, Audit, Control, Compliance, Policy, and Process);
2. The Identification aspect consists of 6 sub-aspects (Asset Management, Inventory, Risk Management, Priority, Reporting, and Classification);
3. The Protection Aspect consists of 6 sub-aspects (Network, Application, User, Identity and Asset Management, Cloud, and Data);
4. The Detection aspect consists of 6 sub-aspects (Change, Monitor, Alert, Notification, Intelligence, and Reporting);
5. The Response Aspect consists of 5 sub-aspects (Containment, Countermeasures, Recovery, Post-Incident Activities, and Reporting).

This questionnaire was distributed to respondents in electronic form (excel file format) as a component of study on the perceived level of cybersecurity maturity in their organizations. Before starting filling, the respondents were introduced to the purpose and content of the CSM measurement instrument. In this study, respondents' data was kept confidential and only displayed as public data of a private sector company in Indonesia. This measurement itself is carried out as part of an organization's evaluation in assessing the level of cybersecurity management to determine the difference in current cybersecurity management conditions against ideal conditions so that they can plan strategies for better cybersecurity management [14].

The modeling used in this study is SEM, which is a statistical analysis approach that allows to model relationships between complex variables and measure their relatedness. To analyze CSM instruments, confirmatory factor analysis (CFA) was chosen as one of the modeling. It is based on the CFA concept that uses the number of indicators studied to have been precisely determined. The application of SEM will enable researchers to analyze and understand the relationship between aspects and sub-aspects of CSM within the private sector in Indonesia.

III. METHOD

This study uses a quantitative approach by collecting data from 23 private companies in Indonesia that have information technology services. The survey questions are developed based on a cybersecurity framework that is widely accepted in 5 (five) main aspects as well as related sub-aspects. The survey data is then analyzed using Structural Equation Modelling (SEM) to identify factors that influence the level of cybersecurity maturity and the relationship between those aspects.

Figure 1 depicts the CFA model for 5 (five) indicators (sub-aspects) and 2 (two) factors under consideration (aspects). Figure 1 illustrates the CFA model, which assumes that factors A and B are measured by the indicators X1-X3 and X4-X5.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

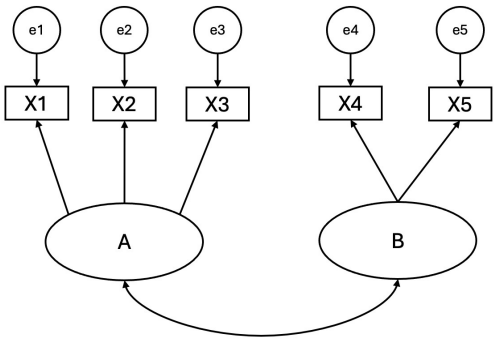

Figure 1. CFA Model Theories

In a standard CFA model with two or more factors, some coefficients are zero. As illustrated in Figure 1, there is no direct path from B to indicators X1, X2, or X3. However, the absence of values between the B and X1 does not imply that they do not correlate. There could be an undirected relationship between B and X1, which can be expressed as follows:

$$X1 \rightarrow A \leftrightarrow B \qquad (1)$$

The path evaluated between B and X1 could represent statistical relationships, but not necessarily causality.

Furthermore, for the correlation between A and X1 or B with X4, there is a correlation that has the meaning of causality. So it can be expressed as follows:

$$X1 \rightarrow A \text{ or } X2 \rightarrow B \qquad (2)$$

Finally, in the CFA model, the indicator e1 has a causality relationship with X1, so this relationship can be expressed as follows:

$$e1 \rightarrow X1 \qquad (3)$$

Based on these findings, confirmatory factor analysis, one of the structural equation modeling tools, was selected as the best way of analyzing the data obtained and the assumptions made within the theoretical framework of factor model development.

Model of Cyber Security Maturity

The basic theoretical model developed regarding cybersecurity maturity is shown in figure 2. The factor model consists of 29 variables representing sub-aspects of the research instrument, and respondents determine the maturity level of their organization's cybersecurity implementation for each of the questions given with ratings on a scale of 1 (initial implementation) to 5 (optimal implementation). From these 29 sub-aspects, a relationship will be made with 5 (five) aspects of cybersecurity measured. As for theoretically, the shape of the CSM model can be seen in figure 2.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

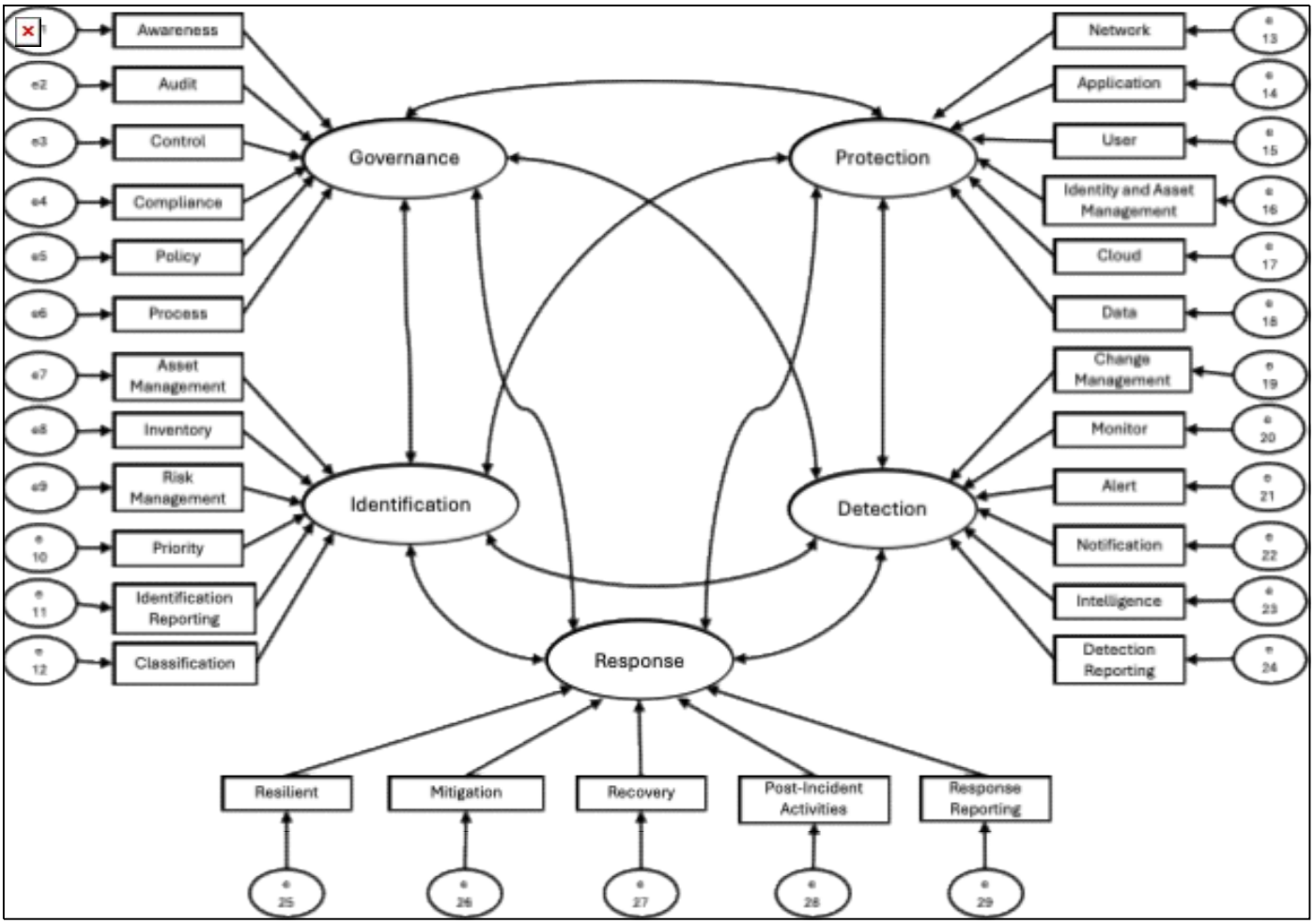

Figure 2. Factor Model Theories in CSM

Several basic statistical indicators are used to make assumptions about the factor models being analyzed using the CFA. In the first phase, the theoretical model (Figure 2) is used to define hypothetical data structures (aspects, sub-aspects, and relationships between them). In this study, the results of CSM modeling statistical calculations will be tested for Goodness of Fit Test in order to get a model that is fit or in accordance with the data that has been obtained. The match test analysis will use the test model provided from the semopy library in python programming. Some of the fit tests used are Chi-square (chi2), Comparative Fit Index (CFI), Goodness of Fit Index (GFI), Adjusted Goodness of Fit Index (AGFI), Normed Fit Index (NFI), Tucker-Lewis Index (TLI), Root Mean Square Error of Approximation (RMSEA) and chi2 p-value,. The evaluation criteria for the CSM model can be seen in table I.

TABLE I. CRITERIA FOR THE CSM MODEL

Indeks Fit	Indeks Fit Sempurna	Indeks Fit Dapat Diterima
x^2/df	$0 \leq x^2/df \leq 2$	$2 \leq x^2/df \leq 3$
CFI	$0{,}95 \leq CFI \leq 1{,}00$	$0{,}90 \leq CFI \leq 0{,}95$

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

GFI	0,95 ≤ GFI ≤ 1,00	0,90 ≤ GFI ≤ 0,95
AGFI	0,90 AGFI < 1,00	0,85 AGFI < 0,90
NFI	0,95 ≤ NFI ≤ 1,00	0,90 ≤ NFI ≤ 0,95
TLI	0,97 ≤ TLI ≤ 1,00	0,95 ≤ TLI ≤ 0,97
RMSEA	0,00 ≤ RMSEA ≤ 0,05	0,05 ≤ RMSEA ≤ 0,08
p-value	p > 0,05	

IV. RESULTS

A. *Statistical Results*

The findings of the 5-aspect cybersecurity model (figure 2) for the entire series of studies with respondents from up to 23 organizations will be presented in separate tables for each aspect measured.

B. *Estimation of CSM's Aspects and Its Sub-aspects*

After data processing and statistical calculations, the estimation value between the 5 aspects and their sub-aspects (as many as 29 sub-aspects) can be seen in Table II below:

TABLE II. ESTIMATION OF CSM ASPECTS AND ITS SUB-ASPECTS

lval	op	rval	Estimate	Std. Err	z-value	p-value
Governance	~	Awareness	0.164	0.037	4.423	9.73E-06
Governance	~	Audit	0.169	0.054	3.101	0.0019268
Governance	~	Control	0.166	0.042	3.969	7.22E-05
Governance	~	Compliance	0.165	0.022	7.495	6.64E-14
Governance	~	Policy	0.166	0.031	5.305	1.12E-07
Governance	~	Process	0.166	0.038	4.324	1.53E-05
Identification	~	Management_Asset	0.166	0.026	6.287	3.23E-10
Identification	~	Inventory	0.164	0.026	6.226	4.78E-10
Identification	~	Management_Risk	0.169	0.039	4.271	1.94E-05
Identification	~	Priority	0.163	0.033	4.920	8.67E-07
Identification	~	Reporting_Identification	0.165	0.019	8.677	0
Identification	~	Classification	0.166	0.025	6.755	1.43E-11
Protection	~	Network	0.163	0.025	6.640	3.14E-11
Protection	~	Application	0.163	0.027	6.141	8.19E-10
Protection	~	User	0.165	0.013	12.36	0
Protection	~	Management_Identity_dan_Asset	0.168	0.029	5.801	6.61E-09
Protection	~	Cloud	0.162	0.016	9.966	0
Protection	~	Data	0.168	0.026	6.416	1.40E-10

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

Detection	~	Management_Change	0.165	0.024	6.744	1.54E-11
Detection	~	Monitor	0.170	0.076	2.232	0.02562314
Detection	~	Alert	0.168	0.042	3.972	7.14E-05
Detection	~	Notification	0.169	0.038	4.423	9.74E-06
Detection	~	Intelligence	0.160	0.048	3.297	0.00097649
Detection	~	Reporting_Detection	0.165	0.025	6.512	7.41E-11
Response	~	Resilient	0.199	0.033	6.084	1.17E-09
Response	~	Mitigation	0.199	0.017	11.393	0
Response	~	Recovery	0.197	0.040	4.932	8.14E-07
Response	~	Post_Incident_Activity	0.197	0.019	10.187	0
Response	~	Reporting_Response	0.197	0.023	8.483	0

From Table II, it can be seen that the Governance variable has a positive correlation with all sub-aspects studied. All of these sub-aspects exhibit significant z-values, which indicates that the relationship between these variables is very close. Notably, the Fulfillment sub-aspect showed the strongest correlation with Governance, with the highest z-value of 7.494 and a very low p-value of 6.64E-14, indicating that this relationship is very statistically significant. This shows that the better the compliance with standards or regulations, the better the quality of governance carried out.

The Identification variable has a positive correlation with all sub-aspects studied. All of these sub-aspects exhibit significant z-values, which indicates that the relationship between these variables is very close. Notably, Reporting_Identification sub-aspect showed the strongest correlation with Governance, with the highest z-value of 8.677 and a very low p-value of 0, indicating that this relationship is very statistically significant.

The Protection variable has a significant correlation with all its sub-aspects. Network, Application, User, Identity and Asset Management, Cloud, and Data variables positively contribute to the Protection factor in the context of cybersecurity. Standard regression estimates show that the relationship between the Protection factor and the Network variable has an estimated value of 0.163, with a standard error of 0.025, resulting in a z value of 6.64 and a very significant p-value (3.14E-11). The same is true of other variables, such as Application, User, Identity and Asset Management, and Data, with statistically significant regression estimates and near-zero p-values.

The Detection has a positive relationship with various sub-aspects related to Detection activity. The strongest relationship was found with Change (z-value = 6.744, p-value < 0.0001), which showed a significant correlation.

Lastly, the Response factor is significantly influenced by several relevant variables. For example, the estimated regression value for the Containment variable is 0.199 with a standard error of 0.032, resulting in a z-value of 6.08 and a p-value of 1.17E-09. Likewise, the Countermeasures variable has an estimated regression value of 0.199 with a standard error of 0.017, resulting in a z-value of 11.39 and a p-value close to zero. This suggests that the relationship between response factors and such variables is strong and statistically significant. Similarly, the variables Recovery, Post-Incident Activities, and Post-Incident Reporting also had a significant influence on the Response factor, with regression estimates and other statistics supporting these findings.

Based on analysis, the correlation between each Aspects and their Sub-aspects can be drawn, as shown in figure 3.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

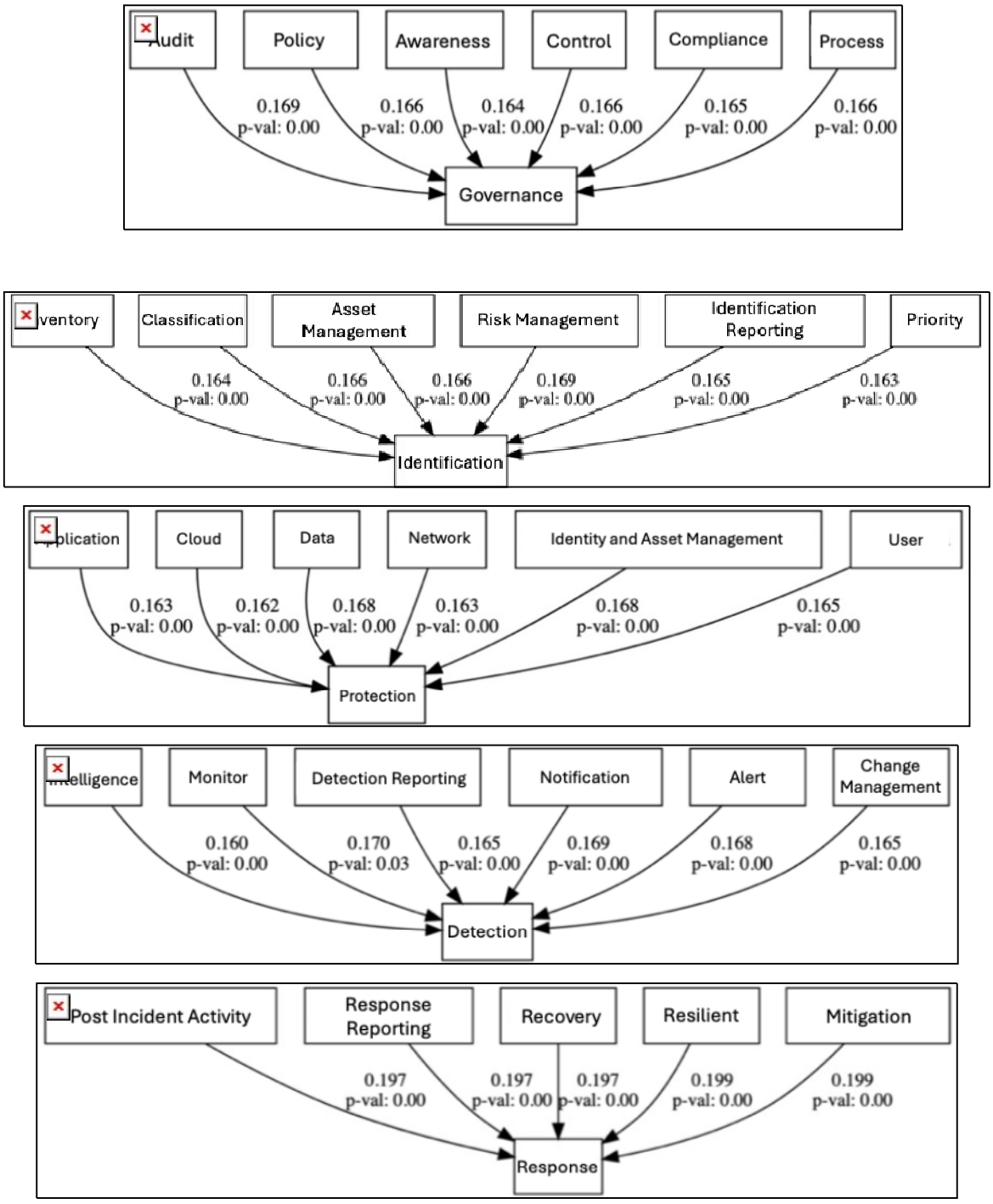

Figure 3. Correlation of Aspect and their Sub-aspects

C. Correlation Between Aspects

Finally, this study tried to calculate the correlation value between 5 aspects of CSM. After data processing, statistical calculations are obtained as shown in Table III as follows:

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

TABLE III. CORRELATION BETWEEN ASPECTS

lval	op	rval	Estimate	Std. Err	z-value	p-value
Governance	~~	Identification	6.82E-07	0.000	0.001	0.999
Governance	~~	Protection	1.36E-06	0.000	0.004	0.997
Governance	~~	Detection	2.72E-06	0.001	0.004	0.997
Governance	~~	Response	2.39E-06	0.001	0.004	0.997
Identification	~~	Protection	-3.43E-06	0.000	-0.010	0.992
Identification	~~	Detection	1.07E-06	0.001	0.002	0.999
Identification	~~	Response	4.14E-06	0.001	0.007	0.994
Protection	~~	Detection	6.25E-07	0.001	0.001	0.999
Protection	~~	Response	-2.41E-06	0.000	-0.005	0.996
Detection	~~	Response	2.23E-06	0.001	0.003	0.998

From the results of the analysis, it can be seen that the relationship between Governance and aspects of Identification, Protection, Detection, and Response has a very low Estimate value, which indicates that the correlation between these variables is very weak. This is supported by a low z-value and a high p-value (all above 0.99), which suggests that the relationship is not statistically significant. This shows that in the context of measuring cybersecurity maturity levels, Governance factors do not have a significant influence on other factors. Similarly, there was no significant relationship between Identification and Protection, Detection, and Response factors, and between Protection and Response. However, there is a significant relationship between Detection and Response factors, although the contribution is relatively small with relatively low regression estimation values.

Based on this analysis, a correlation can be drawn between 5 aspects of CSM, as shown in figure 4.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 48 No. 1 December 2024, pp. 149-159

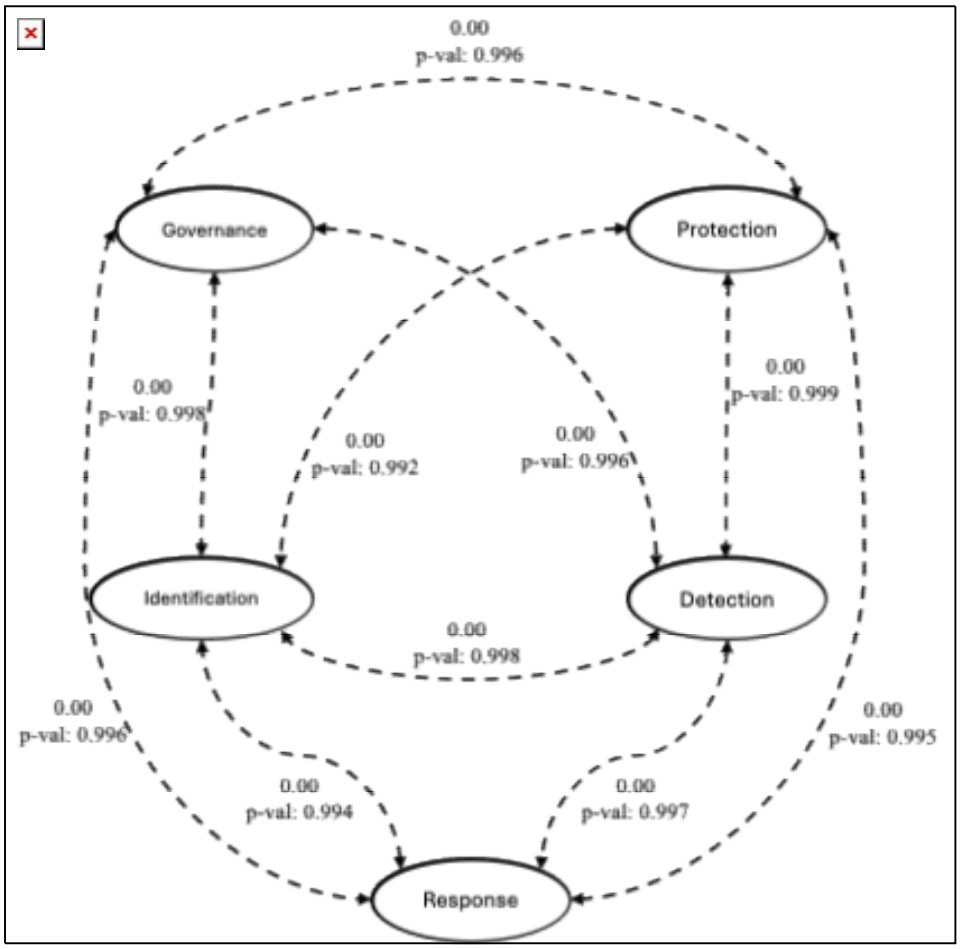

Figure 4. Correlation Between CSM's Aspects

V. Conclusion and Recommendations

Based on the analysis that has been carried out in Chapter IV, the conclusions that can be drawn are as follows:

1. Structural Equation Modelling (SEM) has proven effective in analyzing and measuring the level of cybersecurity maturity (CSM) in Indonesia's private sector. SEM enables modeling of complex relationships between aspects and sub-aspects of CSM, providing a deeper understanding of the dynamics affecting cybersecurity maturity.
2. The most significant factors influencing the level of cybersecurity maturity in Indonesia's private sector include Governance, Identification, Protection, Detection, and Response. Sub-aspects such as Compliance, Reporting_Identification, and Users show a strong correlation with key aspects, indicating the importance of standards and regulations, effective reporting, and user management in improving cybersecurity maturity.
3. The correlation between these aspects and sub-aspects of CSM shows that each aspect has a significant contribution to the cybersecurity maturity assessment. However, the relationship between key aspects (Governance, Identification, Protection, Detection, and Response) shows a weak correlation, indicating that each aspect operates with a high degree of independence in the context of cybersecurity.

To increase the level of cybersecurity maturity in Indonesia's private sector, it is recommended that organizations improve compliance with standards and regulations, strengthen user reporting and management processes, and integrate aspects of CSM more effectively to create better synergies.

ACKNOWLEDGMENT

The researcher would like to express his sincere appreciation and deepest gratitude to the Republic of Indonesian Defense University for the invaluable support throughout this research process, from begin until publication. The assistance and resources they provide play an important role in facilitating the successful completion of these studies

REFERENCES

[1] Gombár, Vagaská, Korauš, and Račková, "Application of Structural Equation Modelling to Cybersecurity Risk Analysis in the Era of Industry 4.0," Mathematics, vol. 12, no. 2, p. 343, Jan. 2024, doi: 10.3390/math12020343.

[2] Rahmawati, "Revolusi Industri 4.0: Big Data, Implementasi Pada Berbagai Sektor Industri (Bagian 2)," Jurnal Sistem Informasi Universitas Suryadarma, vol. 10, no. 1, Jun. 2014, doi: 10.35968/jsi.v10i1.991.

[3] Narindra, "Keamanan dan Ancaman Cyber Bagi Sektor Privat dan Industry Militer Di Era 4.0," Jurnal Diplomasi Pertahanan, vol. 7, no. 1, Feb. 2021, doi: 10.33172/jdp.v7i1.675.

[4] Rahmawati, "Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0," Senastindo AAU, vol. 1, no. 1, pp. 299–306, Sep. 2019.

[5] Lee and Chua, "The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States," Crime & Delinquency, Jun. 2023, Published, doi: 10.1177/00111287231180093.

[6] Haripriya, "Cyber Security Unveiled: Trends and Protections in the Digital World," Interantional Journal Of Scientific Research In Engineering And Management, vol. 07, no. 07, Jul. 2023, doi: 10.55041/ijsrem24720.

[7] Khan, "Cyber Security," Interantional Journal Of Scientific Research In Engineering And Management, vol. 06, no. 06, Jun. 2022, doi: 10.55041/ijsrem14173.

[8] BSSN, "Tingkatkan Tata Kelola Keamanan Siber Industri Pertahanan, BSSN Adakan Diseminasi Kebijakan dan Monitoring Evaluasi Pengukuhan CSM Pada DEFEND ID | www.bssn.go.id," BSSN, Sep. 19, 2023.

[9] Hasman, "An Introduction to Structural Equation Modeling," Studies in Health Technology and Informatics, vol. 213, pp. 3–6, 2015.

[10] Yang, "Structural equation modelling," Advanced Research Methods for Applied Psychology, pp. 246–258, Aug. 2018, doi: 10.4324/9781315517971-24.

[11] Thakkar, "Introduction to Structural Equation Modelling," Structural Equation Modelling, pp. 1–11, 2020, doi: 10.1007/978-981-15-3793-6_1.

[12] Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, "An Introduction to Structural Equation Modeling," Classroom Companion: Business, pp. 1–29, 2021, doi: 10.1007/978-3-030-80519-7_1.

[13] Cisco, "Studi Cisco: Indonesia Teratas dalam Kematangan Keamanan Siber," Cisco, Mar. 29, 2023.

[14] BSSN, "BSSN Serahkan Hasil Pengukuran Tingkat Kematangan Keamanan Siber Sektor Industri Tahun 2023," bssn, Nov. 15, 2023.