

Security Infrastructure Service and Information Security Management Capability Audit to Improve System Security in Preventing Cyber Attacks using COBIT 2019

Salim^{1✉}, Alva Hendi Muhammad²

^{1,2} Master of Informatics, School of Postgraduate, Universitas Amikom Yogyakarta, Indonesia

✉ Corresponding Author : Salim (e-mail: salim@students.amikom.ac.id)

Article Information	ABSTRACT
Article History Received : December 30, 2024 Revised : January 10, 2025 Published : January 16, 2025	Cyber-attacks have become a serious concern in recent years, as hackers can attack systems, databases, and even steal personal data from a particular organization's database and sell it on the dark web. The individual identity data will be used to carry out various financially profitable activities such as online fraud, selling data containing detailed account information, and asking for ransom from data owners. The failure of an organization to protect data assets from cyber-attacks stems from several internal factors such as the vulnerability of the information security system it has, the less than optimal awareness of users in the organization of the importance of maintaining safe behavior in cyberspace, and routine processes related to information security that are missed. COBIT 2019 can be used as an audit framework to assess the level of maturity of the governance. Network infrastructure services in an organization can be measured in terms of the level of capability in terms of the application of technology assets and their configuration using the DSS05 and APO13 domains. This study aims to provide guidelines in assessing system security infrastructure in IT governance by assessing areas that are still not comply with the framework used, and providing recommendations for improving these inconsistencies so that the level of infrastructure capability will be maximized then.
Keywords: <i>COBIT 2019; Cyber Attack; Cyber Security; IT Audit; IT Governance.</i>	

INTRODUCTION

In recent years, data leaks and breaches in several large organizations have been widely reported in the mainstream media. These incidents not only harm the organization financially and public trust, but the organization is even required to meet certain regulatory requirements according to applicable laws (Schmitz et al., 2021)(Aslan et al., 2023). For example, in Indonesia, based on the results of Cyber Threat Intelligence monitoring and analysis, BSSN also conducted investigations into alleged cyber incidents with a total of 399 alleged cyber incidents in 2022 and 347 alleged cyber incidents in 2023. The highest number of types of alleged incidents in 2 years, namely data breach (BSSN, 2023) (BSSN, 2024).

Data loss and leakage are often caused by cybercrime attacks (Oluwasanmi Richard Arogundade, 2023), one of the most common of which is ransomware attacks. The main entry point for cyber-attacks is the organization's internet access. In this digital era, most companies rely on Internet Service Providers (ISPs) for internet access. However, along with the rapid growth of the internet, ISPs themselves are also increasingly facing various security challenges including

cyber-attacks and data breaches. Variations of attacks that change and the emergence of new variations can cause damage or disruption to large and small organizations and even individuals (Modisane, 2023). This damage certainly disrupts the organization's business operations, especially if the damage is very severe; it is possible that the organization will have to create a security system from scratch.

The role of Information Technology (IT) is becoming increasingly important for the running of a large organization's business. Cybersecurity is a top priority in IT management to protect the organization's systems and data safely. The interaction between IT governance and compliance with IT standards in each area must be in harmony in order to anticipate the development of very fast and massive cyber-attacks. Cybersecurity is often still a low priority within companies and is not embedded in corporate strategy. Even applicable standards are rarely implemented in companies. This is where IT is needed as a bridge that can connect technology with business needs (Ulrich & Stockert, 2023).

Cybersecurity or information security systems protect the cyber world from various threats to reduce overall business risks, and ensure the continuity of business operations. High cybersecurity can be achieved well through the use of an appropriate security governance framework. To achieve this goal, various IT governance and cybersecurity frameworks have been reviewed for their benefits and limitations (Melaku, 2023) (Adrian & Wang, 2023).

Researchers conducted research that focused on the level of information security system capabilities of IT governance that had been implemented in the research object organization using the COBIT 2019 framework. COBIT 2019 was chosen as the research framework because of the characteristics and capabilities of COBIT as a guideline for IT governance as well as a guideline in conducting IT governance audits with focus on domain APO13 and DSS05 (Viamianni et al., 2023) (Christiadi & Sutomo, 2023) (Darmi et al., 2024) (Mubarak & Fianty, 2023) (Hadi et al., 2023).

The results of the study are recommendations for improvements and increasing the value of the capability level in the APO13 and DSS05 domains so that the level of awareness and willingness to ward off cyber-attacks will continue to increase, especially awareness of the importance of safety and protection of personal data.

RESEARCH METHODS

The type of research used by the researcher is qualitative research with a case study approach examining descriptive data obtained from data sources from case studies on research objects through documents, observation and IT team interview results at company XYZ as one of oil and gas company in Indonesia. The collected data is mapped into a quantitative data format by analyzing the value grouping guide based on the framework used. The results of this study are in the form of measurable numbers from a certain domain capability level.

Research Planning

Research planning is carried out in detail and maximally so that the research is appropriate in scope, timely and appropriate in the results determined. The process of identifying and formulating the problems studied as the earliest stage of this research will provide input for other processes, namely the research framework used, the selection of the right research method, the research flow from start to finish, the type of data and methods of obtaining data used in the research, data analysis, assessment, validation and confirmation, to the preparation of recommendations for research results.

Data Collection

The types of data used in this study are primary data and supporting data. Primary data are obtained from three data collection methods, namely respondent data on the questionnaire provided, qualitative data from descriptive information through interviews with the IT department responsible for networks and security and direct review data of network and security infrastructure (Tulus & Tanaamah, 2023). Supporting data in this study are data obtained from organizational

documents related to network infrastructure and security, statistical data on security-related events whose data types are based on the matrix contained in the COBIT 2019 framework in each of its domain activities.

Respondents in the study were XYZ employees, their position namely IT Manager (IT MGR), IT Infrastructure Officer (IT INF) and IT Network & Security Analyst (IT NSA). The questionnaire as primary data was created based on activity data from the APO13 domain of 19 data and from the DSS05 domain of 49 activities (ISACA, 2019b).

Data Analysis

The process of analyzing qualitative data derived from a combination of questionnaires, interview results, and observations to produce quantitative data can be done by transcribing all collected data into text data, then grouping the narrative text data into certain categories or themes that are relevant and measurable to present the results of the analysis. After the analysis results are made, discussions with the audited organization must be carried out to align understanding of the quantitative data that is used as a basis for the next stage.

Activities in each COBIT 2019 domain process can be assessed based on a simple pass or fail rating, or by using the achievement rating (Mubarak & Fianty, 2023). Table 1 defines the achievement rating at the level of capability for each domain, the percentage of achievement figures is a guide to determining the ranking group based on the number of activities or the number of components fulfilled.

Tabel 1. Capability Level Achievement Ranking

Capability Criteria	Achievement Percentage
Fully Achieved (F)	>85%
Largely Achieved (L)	50% - 85%
Partially Achieved (P)	15% - 50%
Not Achieved (N)	<15%

Capability Level Measurement

Domain APO13 and DSS05 specifically relate to the management of physical IT security and security service management, including consistent and responsive service delivery. Use the COBIT 2019 five-level maturity model to assess current practices against recommended best practices using data analyzed for each activity in the data analysis phase. The assessment is carried out by evaluating all activities in each subdomain at a certain level, if all activities at a level have been carried out thoroughly, then the assessment can be continued to the next level, but if there are still activities that have not been carried out thoroughly, the assessment can be stopped at that level (I Nyoman Rai Widartha Kesuma, Irman Hermadi, 2023).

Using the above approach, organizations can monitor and evaluate the maturity of the APO13 and DSS05 domains in COBIT 2019 and formulate action plans for further continuous improvement. The levels of capability and general characteristics of each level are depicted in Figure 1 (ISACA, 2019a).

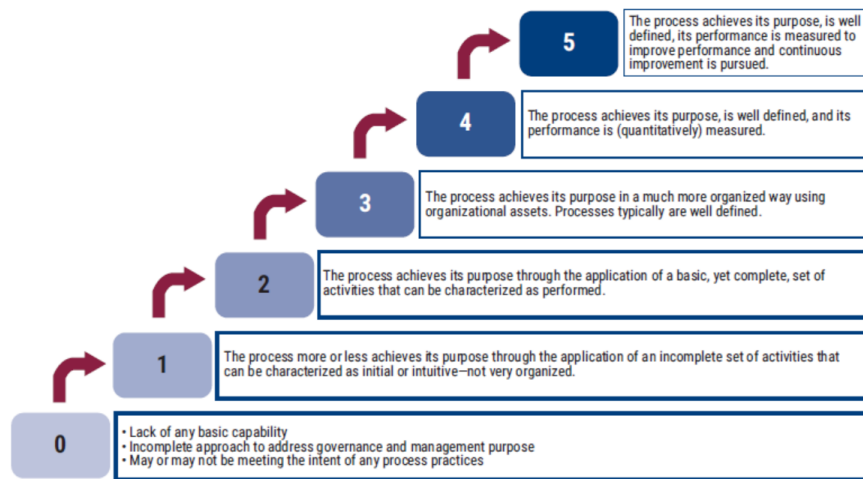


Figure 1. Capability Levels for Processes

Finding and Recommendation Arrangement

The results of all stages of the audit assessment are recommendations for improvement based on findings or non-conformities in the current conditions of each audited object. Determining priorities in making recommendations for IT governance audit results using COBIT 2019 takes into account elements such as the organization's business objectives, impacts and risks to the business, costs and time required for improvement. An improvement roadmap is created to provide guidance on the order of improvements from the time of their implementation.

RESULTS AND DISCUSSION

Company XYZ has been operating for more than 30 years with stable production and product distribution according to the target. Companies with conditions like this, one of their business strategies is to focus on the sustainability of their best services and guarantee the availability of service products. The IT Division as a service provider related to computerized systems, must be able to ensure that the services provided are in line with the business strategy being carried out.

The availability of IT services must be available at all times and the IT division must ensure that the services provided are equipped with a high security system to anticipate the threat of incoming cyber attacks so that the business can continue to run normally without any disruption. The operation of company has threats from external parties, especially companies that are already stable, the main threat is not from competitors and products, but rather from threats that can destroy the condition of operational stability in the form of physical threats of cyber attacks into the company's information system.

Company that operates in a high threat landscape requires a very reliable security-related process so that the domains that must be managed properly are Manage Security (APO13) and Manage Security Service (DSS05) as a design factor needs by company (Katili et al., 2023) (Nugroho & Ginardi, 2024).

Enterprise Goals and Alignment Goals

The synergy between enterprise goals and alignment goals as part of an important role in ensuring that organizational and IT goals are aligned with business strategy. The main enterprise goal of company XYZ type is EG06 (ensuring continuity and availability of business services), alignment goals ensure that IT initiatives are not only aligned with business goals, but also contribute effectively to achieving them.

IT as a support system for company XYZ type organizations ensures that the alignment goals AG07 (information security, processing and application infrastructure, and privacy) taken must be able to contribute effectively by prioritizing IT management practices that are aligned with

business conditions. Mapping enterprise goals EG06 to alignment goals AG07 based on existing conditions refers to the mapping guide in the COBIT 2019 framework as in Figure 2 (ISACA, 2019a).

	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
	Portfolio of competitive products and services	Managed business risk	Compliance with external laws and regulations	Quality of financial information	Customer-oriented service culture	Business service continuity and availability	Quality of management information	Optimization of internal business process functionality	Optimization of business process costs	Staff skills, motivation and productivity	Compliance with internal policies	Managed digital transformation programs	Product and business innovation
AG01	I&T compliance and support for business compliance with external laws and regulations	S	P								S		
AG02	Managed I&T-related risk	P				S							
AG03	Realized benefits from I&T-enabled investments and services portfolio	S			S			S	S			P	
AG04	Quality of technology-related financial information			P			P		P				
AG05	Delivery of I&T services in line with business requirements	P			S	S		S				S	
AG06	Ability to turn business requirements into operational solutions	P			S			S				S	S
AG07	Security of information, processing infrastructure and applications, and privacy		P			P							
AG08	Enabling and supporting business processes by integrating applications and technology	P			P			S		S		P	S
AG09	Delivering programs on time, on budget and meeting requirements and quality standards	P			S			S	S			P	S
AG10	Quality of I&T management information			P			P		S				
AG11	I&T compliance with internal policies		S	P							P		
AG12	Competent and motivated staff with mutual understanding of technology and business				S					P			
AG13	Knowledge, expertise and initiatives for business innovation	P		S								S	P

Figure 2. Mapping Enterprise Goals and Alignment Goals for Company XYZ.

RACI Chart Mapping

Determining the right RACI is very important to ensure that every activity or decision related to the implementation of IT governance has a clear party who is responsible, who must report, who needs to be consulted and who is informed. The audit stages in collecting data using the interview method must also refer to the RACI mapping so that the data produced is valid data from respondents who are responsible for the activities carried out on a daily basis. Table 2 and Table 3 are RACI mappings in XYZ company for the APO13 domain and the DSS05 domain according to the applicable personnel and organizational structure.

Tabel 2. RACI Chart Mapping for Domain APO13 in Company XYZ

Domain APO13 Activities	IT MGR	IT INF	IT NSA
APO13.01 Establish and maintain an Information Security Management System (ISMS)	A	R	R
APO13.02 Define and manage an information security and privacy risk treatment plan	A	R	R
APO13.03 Monitor and review the ISMS	A	R	R

Tabel 3. RACI Chart Mapping for Domain DSS05 in Company XYZ

Domain DSS05 Activities	IT MGR	IT INF	IT NSA
DSS05.01 Protect against malicious software	C	A	R
DSS05.02 Manage network and connectivity security	C	A	R
DSS05.03 Manage endpoint security	C	A	R
DSS05.04 Manage user identity and logical access	C	A	R
DSS05.05 Manage physical access to I&T assets	C	A	R
DSS05.06 Manage sensitive documents and output devices	A	R	R
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	A	R	R

APO13 Capability Level

The assessment of the APO13 domain capability level at company XYZ produces a number at level 2 towards 3, the highest capability level in APO13 COBIT 2019 is level 5 (ISACA, 2019b), so there is a gap of 3 levels between the actual condition and the maximum condition. The implementation of information security management in IT governance has achieved its objectives with processes that need to be defined in more detail, well and regularly.

Table 4 describe the number of activities in each APO13 subdomain and the number of activities that have been fully achieved at each capability level with details of capability level 2 there are 7 activities fully achieved out of 7 activities, capability level 3 there are 5 activities fully achieved out of 6 activities, capability level 4 there is 1 activity fully achieved out of 5 activities and at capability level 5 there is only 1 activity and 1 activity has been fully achieved.

Tabel 4. Capability Level Achievement for Domain APO13 in Company XYZ

Capability Level	Total Activities	Fully Achieved Activities
Level 2	7	7
Level 3	6	5
Level 4	5	1
Level 5	1	1

DSS05 Capability Level

The assessment of the DSS05 domain capability level at PT. XYZ produces a number at level 3 towards 4, the highest capability level in DSS05 COBIT 2019 is level 4 (ISACA, 2019b), so there is a gap of 1 level between the actual condition and the maximum condition. The implementation of information security infrastructure in IT governance has achieved its goal of using company assets with well-defined and orderly processes.

Table 5 is mapping of the number of activities in each DSS05 subdomain and the number of activities that have been fully achieved at each capability level with details of capability level 2, there are 26 activities fully achieved out of 26 activities, capability level 3 there are 18 activities fully achieved out of 18 activities and capability level 4 there are 3 activities fully achieved out of 5 activities.

Tabel 5. Capability Level Achievement for Domain DSS05 in Company XYZ

Capability Level	Total Activities	Fully Achieved Activities
Level 2	26	26
Level 3	18	18
Level 4	5	3

The management of information security infrastructure at company XYZ is very good in terms of technology implementation, configuration, and daily operational processes. Several activities regarding periodic process reviews need to be carried out to increase awareness of all parties involved in preventing possible cyber attacks, considering that the growth of types of cyber attacks changes all the time and is increasingly unpredictable, so continual improvement needs to be carried out continuously.

Finding

There are 4 findings in the APO13 domain and 5 findings in the DSS05 domain that are very important and fundamental. Table 6 presents the details of the findings in APO13 more about

policies that have not been created and ratified and the findings in the DSS05 domain are more about the configuration process that has not been carried out on the technology used.

Tabel 6. Finding List for Domain APO13 and DSS05 in Company XYZ

Finding No	Sub Domain	Finding Detail
1	APO13.01	The company does not yet have a policy document approved by top management regarding information security applicable in the company, so that the information security policy and components that have been determined do not yet have official guidelines.
2	APO13.01	The company does not yet have a competency matrix to measure the adequacy of competency for units and personnel involved in information security management, so that the role and responsibility of information security management is still attached to workers who carry out daily activities related to information security.
3	APO13.02	The company has not yet carried out a structured identification of risks related to information security in the form of a risk register.
4	APO13.03	The company has not conducted periodic internal information security audits and management reviews to ensure that the implementation of security in the company is in accordance with applicable standards.
5	DSS05.04	The company does not yet have adequate control in managing access rights.
6	DSS05.05	The company has not established a clear and applicable physical security perimeter (zoning) in the company.
7	DSS05.06	The company does not yet have a policy regarding information labeling, including rules regarding the transfer of confidential information.
8	DSS05.06	The company has not implemented Data Leakage Prevention (DLP) technology to prevent leakage of personal or sensitive information.
9	DSS05.07	The company does not yet have a formal mechanism for reporting information security incidents.

Finding Fixing Recommendation

Recommendations are given to the company based on the findings generated to be able to increase the level of capability in each domain after improvements are made. Table 7 contains recommendations that must be carried out by the company in each sub-domain activity.

Tabel 7. Finding Fixing Recommendation List for Domain APO13 and DSS05 in Company XYZ

Finding No	Sub Domain	Recommendation Detail
1	APO13.01	Create an information system security management policy document that is approved by the company's top management and disseminated to all company stakeholders. Attention from top management is very important to lead cyber security awareness (Shaikh & Siponen, 2023).
2	APO13.01	Create a competency matrix, tasks, and responsibilities in managing information system security and have it approved by the relevant management.

3	APO13.02	Create a structured risk register regarding information security management system.
4	APO13.03	Schedule and conduct internal audits of information system security periodically, at least once a year.
5	DSS05.04	Create a complete control matrix regarding access rights to all infrastructure related to information system security (Angelina & Fianty, 2023) (Yeoh et al., 2023).
6	DSS05.05	Establish a physical zoning perimeter to ensure that areas containing information assets are adequately protected from unauthorized physical access or other physical threats.
7	DSS05.06	Create company information policies and labeling to ensure that information is controlled in an appropriate manner.
8	DSS05.06	Implementing DLP can help minimize the risk of unwanted information leaks.
9	DSS05.07	Create clear and documented procedures is necessary to ensure that any information security incidents can be reported, analyzed and handled quickly and effectively, minimizing the impact on the company.

CONCLUSION

The management of services and the implementation of information system security infrastructure technology are currently very good in preventing cyber attacks. This can be seen from the mature infrastructure configuration and clearly defined operational processes, ensuring optimal security. In addition, the use of the latest technology also supports the effectiveness of the security system, providing stronger and more responsive protection to potential threats that develop over time. Overall, the implementation of infrastructure technology in XYZ company provides a solid foundation for protecting information systems from various cyber attack risks. Several processes need to be carried out related to the use of technology to protect information from cyber attacks.

The management of information system security management in XYZ company has been carried out well in accordance with the COBIT 2019 APO13 domain framework. However, to increase the effectiveness and awareness of the importance of information security, it is necessary to create an official policy that is approved by the company's top leadership. This policy must be conveyed to all stakeholders in the company so that all elements can understand and comply with the security measures that have been set, and are aware of the potential dangers of cyber-attacks that can threaten the continuity of the company's operations.

Recommendations given in each finding can be immediately implemented in the first year to be able to increase the level of information security system capabilities, especially in the APO13 and DSS05 domains and maximize the implementation of reliable infrastructure in preventing cyber-attacks that enter at certain times. The following year the company can review the information security infrastructure after improvements have been applied, audit activities can be added with more detailed standards in terms of system security such as ISO 27001:2022 to maximize the reliability end to end of the information security infrastructure.

ACKNOWLEDGEMENTS

This research accomplished from the maximum support by company XYZ which has provided the opportunity to become a research object.

REFERENCES

- Adrian, F. X., & Wang, G. (2023). Measure the Level Capability IT Governance in Effectiveness Internal Control for Cybersecurity Using the COBIT 2019 in Organization: Banking Company. *Journal of Theoretical and Applied Information Technology*, 15(5). www.jatit.org
- Angelina, A., & Fianty, M. (2023). Capability Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners Assessment Capabilities. *G-Tech: Jurnal Teknologi Terapan*, 8(1), 91–103. <https://doi.org/10.33379/gtech.v8i1.3509>
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. In *Electronics (Switzerland)* (Vol. 12, Issue 6). MDPI. <https://doi.org/10.3390/electronics12061333>
- BSSN. (2023). *Landskap Keamanan Siber Indonesia 2022*.
- BSSN. (2024). *Landskap Keamanan Siber Indonesia 2023*.
- Christiadi, R. N., & Sutomo, R. (2023). Measurement of IT Security Governance Capabilities Using COBIT 2019 at Indonesian Business Sector. *G-Tech: Jurnal Teknologi Terapan*, 7(4), 1498–1508. <https://doi.org/10.33379/gtech.v7i4.3170>
- Darmi, Y., Fernandez, S., Fathoni, M. Y., & Wijayanto, S. (2024). Evaluation of Governance in Information Systems Security to Minimize Information Technology Risks. *INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi*, 8(1), 40–51. <https://doi.org/10.29407/intensif.v8i1.21221>
- Hadi, D., Jentama, G., Adisty, M., & Sutabri, T. (2023). Transformasi Teknologi Digital dalam Keamanan dan Privasi pada Institusi BUMN. *Kohesi: Jurnal Multidisiplin Saintek*, 01, 97–104.
- I Nyoman Rai Widartha Kesuma, Irman Hermadi, Y. N. (2023). Evaluasi Tata Kelola Teknologi Informasi di Dinas Pertanian Gianyar Menggunakan COBIT 2019. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK)*, 10, 513–522.
- ISACA. (2019a). *COBIT 2019 Design guide designing an information and technology governance solution*. ISACA.
- ISACA. (2019b). *COBIT 2019 Framework Governance and Management Objectives*.
- Katili, M. R., Amali, L. N., & Suhada, S. (2023). Design Factors in Evaluating and Formulating IT Governance Systems in Public Organizations. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 7(5), 1182–1191. <https://doi.org/10.29207/resti.v7i5.4939>
- Melaku, H. M. (2023). A Dynamic and Adaptive Cybersecurity Governance Framework. *Journal of Cybersecurity and Privacy*, 3(3), 327–350. <https://doi.org/10.3390/jcp3030017>
- Modisane, P. (2023). Assessing Information Security Maturity Levels in ISP Organizations Using COBIT 2019. *ResearchGate*. <https://www.researchgate.net/publication/373295617>
- Mubarak, R. F., & Fianty, M. I. (2023). Leveraging COBIT 2019 to Implement IT Governance in Mineral Mining Company. *Journal of Information Systems and Informatics*, 5(3), 1058–1071. <https://doi.org/10.51519/journalisi.v5i3.545>
- Nugroho, A., & Ginardi, H. (2024). Information Technology Governance Analysis to Reduce

- Information Security Risks Using Cobit 2019: A Case Study of Manufacturing Companies. *Jurnal Indonesia Sosial Teknologi*, 5(8), 3722. <http://jst.publikasiindonesia.id/>
- Oluwasanmi Richard Arogundade. (2023). Network Security Concepts, Dangers, and Defense Best Practical. *Computer Engineering and Intelligent Systems*. <https://doi.org/10.7176/ceis/14-2-03>
- Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers and Security*, 108. <https://doi.org/10.1016/j.cose.2021.102306>
- Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers and Security*, 124. <https://doi.org/10.1016/j.cose.2022.102974>
- Tulus, B. V., & Tanaamah, A. R. (2023). Design of Information Technology Governance in Educational Institutions Using COBIT 2019 Framework. *Journal of Information Systems and Informatics*, 5(1), 31–43. <https://doi.org/10.51519/journalisi.v5i1.408>
- Ulrich, P. S., & Stockert, F. (2023). IT Governance and IT Compliance in Family Firms - the Special Case of Cyber Security. *Procedia Computer Science*, 225, 2781–2789. <https://doi.org/10.1016/j.procs.2023.10.270>
- Viamianni, A., Mulyana, R., & Dewi, F. (2023). COBIT 2019 Information Security Focus Area Implementation for Reinsurco Digital Transformation. *JIKO (Jurnal Informatika Dan Komputer)*, 6(2). <https://doi.org/10.33387/jiko.v6i2.6366>
- Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers and Security*, 133. <https://doi.org/10.1016/j.cose.2023.103412>