Journal of Applied Business, Taxation and Economics Research (JABTER)
Vol. 2, No. 6, August 2023 (Page: 690-704) P-ISSN 2828-4976
DOI: 10.54408/jabter.v2i6.223 E-ISSN 2808-263X

Analysis of Needs with the PIECES Concept: How Urgency is the Involvement of Ethical Hackers in Accounting Information Systems?

Yayang Novealita Wahono Putri[1*], Kurnia Ekasari[2], Kartika Dewi Sri Susilowati[3]

[1*,2,3] State Polytechnic of Malang, Indonesia

Corresponding Author: yayangnovealitawahonoputri@gmail.com[1)]*

Keywords : *Accounting Information System, Analysis of Needs, Ethical Hacking, Ethical Hacker, PIECES Framework*

Abstract:
This study aims to identify the needs analysis of a company in involving ethical hackers to achieve the desired goals. This research focuses on accounting information systems which are vital systems in business processes. The company's goals will be translated into a need analysis using the PIECES framework (Performance, Information, Economy, Control, Efficiency, and Service). The research method used is a quantitative descriptive method and uses documentation techniques in collecting data. This study uses secondary data in the form of a literature review of 80 journal articles published in 2018-2023. Only ISSN indexed journals are used as data sources to ensure the quality of research output remains relevant. The results of this study are that the information aspect holds the highest urgency at 31.25% and the control aspect ranks second with a score of 25.00%. While the aspect with the lowest urgency is the economic aspect with an achievement of only 6.25%. Comparison of the scope of research and how researchers explore in more detail in linking opportunity costs can be input for further research. Furthermore, future research can also link several concepts such as urgency needs analysis with the PIECES framework, opportunity costs, and user trust in ethical hackers. So that the results of the research conducted will be more interesting and can be a reference for companies in making policies.

Introduction

Currently technology dominates all aspects of life. Life developed into complex systems. The relationship in the end cannot be separated from one another (Wylie, P. L., & Crawley, 2020). Information systems which are part of technology are able to connect one human being to another, one data to another, and one interest to another. This freedom ultimately has positive and negative impacts (Callen, J., & James, 2020). With information systems, humans can get whatever they need to cause high dependency. In addition, the level of convenience for a person in receiving and sending digital information is a new challenge in the aspect of cybersecurity. In the world of cybersecurity, the term hacker becomes "appearing ghost" (Georg, T., Oliver, B., & Gregory, 2018). Cyber security is not a new innovation, but has existed since the beginning when data was stored on computers and required protection via passwords. However, according to Jofre, (2023) the need for cyber security is irrelevant because at first only a handful of people operated the first computer that was produced. Therefore, no outsiders would interfere with the system. This opinion was later refuted by research conducted by Quasim, M. T., Al Hawi, A. N., & Meraj, (2023) where they stated that system vulnerabilities were often used as a weapon for reconnaissance. Pre-attack is the stage of preparation before (attacker) launches an attack, where the main focus are gathers as much information about the target as possible. This method involves scanning the network from both inside and outside the network without proper permission (Kasim, M., Saidu, M. B., Isa, A., & Utulu, 2022; Smith et al., 2022).

In a more detailed scope, this research will examine how cyber security is applied and needed in the field of accounting information system (Yaacoub et al., 2021). The selection of this scope is based on the urgency of the need for cyber security in a system that contains data or company financial information in the framework of decision making. Accounting is a cycle, where the cycle is called the accounting information system. So, based on these conclusions, accounting information systems require attention related to cybersecurity needs and planning strategy (Smith et al., 2022; Turner, L., Weickgenannt, A. B., & Copeland, 2022). The term ethical hacking will be associated with the practice of planning for cyber security which is preceded by a need analysis using the PIECES framework. PIECES is a framework consisting of 6 dimensions of classification and problem solving, namely Performance, Information, Economy, Control, Efficiency, and Service (Astriyani et al., 2020).

Companies through an analysis of the needs of their accounting information systems can determine what they want to achieve in carrying out cyber security practices (Santoso & Rukmana, 2023). Ethical hackers, namely people who work within the scope of ethical hacking ethic (Jean, 2023). They are individuals who test the security of systems owned by companies with the aim of exploiting them and looking for vulnerabilities so that they can find risks caused by these vulnerabilities. Ethical hackers come up with another term white hat hacker (Kumawat et al., 2023). Apart from that, the term black hat hacker is also known, which of course has the opposite position and goal from the white hat hacker (Wylie, P. L., & Crawley, 2020). Ethical hackers use the same methods as unethical hackers. However, they only target systems that have given them permission to test their security measures. Their goal is to

P-ISSN 2828-4976
E-ISSN 2808-263X

improve the security of IT systems. As a result, ethical hacking is not considered illegal (Georg, T., Oliver, B., & Gregory, 2018).

The issue of ethical hacking in accounting information systems (for accounting and finance) has grown rapidly (Hardiana et al., 2023). In order to motivate businesses to protect their data, many organizations offer guidance and support to companies and governments who wish to reward security vulnerabilities (Wallingford, J., Peshwa, M., & Kelly, 2019). HackerOne, which provides a wide range of cybersecurity solutions, including penetration testing, promotes their program as a "hacker-powered security platform" that can save costs and increase compliance. In 2016, HackerOne published a "How to Run a Bug Bounty Program" summary document which provides an overview of the program's benefits, estimated costs, and suggestions for working with the hacker community (Real & Mesa, 2022; Rudenko et al., 2023). Ethical hacking, also known as penetration testing or white hat hacking, is the practice of testing the security of computer systems and networks with permission to identify and address vulnerabilities that could be exploited by malicious attackers. In the context of accounting information systems (AIS), ethical hacking has an important role that can help improve data security and integrity, and protect organizations from security threats.

Here are some reasons why ethical hacking is important in accounting information systems. Identifying vulnerabilities, ethical hacking allows security teams to identify vulnerabilities in accounting information systems (Ding, A. Y., De Jesus, G. L., & Janssen, 2022). By executing ethically controlled attacks, security professionals can test systems to see if there are any loopholes that could be exploited by attackers. By finding and fixing these vulnerabilities before attackers do, organizations can reduce the risk of costly attacks (Pattison, 2020). Protect sensitive data, Accounting Information Systems often contain highly sensitive data, including financial information, customer data, and transaction details. Ethical hacking helps protect this data by identifying and addressing vulnerabilities that could lead to leakage or unauthorized use. By protecting this sensitive data, ethical hacking helps prevent identity theft, loss of customer trust, and possible legal consequences (Dorofeev et al., 2022). Maintain data reliability and integrity, Accounting Information Systems must be reliable in producing financial reports and other accounting information. Ethical hacking helps ensure the reliability and integrity of data by testing systems to see if there is a risk of data manipulation or attacks that could affect the accuracy of financial reports (Holt et al., 2021). By preventing unauthorized or undetectable changes to data, ethical hacking ensures that the information generated by accounting systems can be trusted (Kieslich, K., Keller, B., & Starke, 2022).

Compliance with security regulations and standards, many organizations are governed by specific security regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS) or the General Data Protection Regulation (GDPR). Ethical hacking helps ensure that organizations comply with these requirements by testing systems for vulnerabilities that might violate these regulations or standards (Christen, M., Gordijn, B., & Loi, 2020, p. 384). By conducting periodic security testing, organizations can ensure that they remain compliant with relevant security requirements. Increase security awareness, through

the process of ethical hacking, organizations can increase security awareness among their employees (Walker, 2022, p. 156). The results of security testing can be used to provide training and education to employees about security threats and best practices to follow. Based on this phenomenon, it is important to review the company's needs and relate them to the level of urgency associated with the opportunity cost aspect (Formosa, P., Wilson, M., & Richards, 2023). Is it possible that paying a high price for an ethical hacker will increase value creation in the company's system? and how important is it that an ethical hacker is involved to meet the needs and goals of the company?

Literature Reviews and Development of Hypotheses

Many studies have been conducted to examine the role of ethical hacking in cyber security. Kadir et al., (2023) identified these threatening risks that could endanger the security and privacy of individuals and organizations, as well as the stability and security of society as a whole (Vandervelden, S., Chowdhury, M. M., & Latif, 2019). To combat this threat, it is necessary to have efficient cybersecurity by taking appropriate measures, such as using strong passwords, firewalls, encryption, and performing regular software updates. In addition, the presence of skilled cybersecurity professionals is essential to identify and deal with threats in a timely and effective manner (Aljebry, A. F., Alqahtani, Y. M., & Sulaiman, 2022). One of the main challenges in cybersecurity is unethical hacking. In its evolution in the world of cyber-crime, this has resulted in the use of new names for perpetrators (Hartono, 2022).

Ethical hacking, also known as "white hat hacking," refers to acts of hacking performed without malicious intent, with the goal of finding vulnerabilities before they are taken advantage of by unauthorized parties. Well-resourced businesses often arrange ethical hacking through contracts with cybersecurity experts, known as penetration tests or pen tests (Shoemaker, D., Kohnke, A., & Laidlaw, 2019). However, the pen test does not cover all types of ethical hacking and costs a significant amount of money. Therefore, we suggest a bug bounty program (Real & Mesa, 2022). Assessing data and arguments, using logic and evidence, and asking assumptions are the essence of critical thinking (Endaryati, 2021; Kadir et al., 2023). In the context of hacking, critical thinking is used to evaluate security vulnerabilities in systems and applications, assess the potential risks and consequences of different types of attacks, and select the most effective methods to exploit those vulnerabilities (Atil et al., 2018; Smith et al., 2022).

The PIECES framework allows companies to identify their needs in achieving cybersecurity goals (Brilliant, 2023). The accounting information system contains financial data and business processes (Kelrey & Muzaki, 2019). Because it is included in the system, the accounting information system needs to get an allocation for implementing cybersecurity planning through ethical hacking using various tools and perspectives (Vignesh & Rohini, 2022; Yaacoub et al., 2021). Within the PIECES framework, each aspect will be described so that it can be determined whether the decision to involve an ethical hacker is appropriate, (Jean, 2023) and efficient (not a wasteful act).

Other studies also use the PIECES framework to measure the most urgent aspects in each standard (Brilliant, 2023; Komarudin et al., 2022; Novriani et al., 2023). They concluded

P-ISSN 2828-4976
E-ISSN 2808-263X

that in management information systems and tax information systems, Performance and Information (PI) aspects are the two highest standard requirements. Meanwhile (Hardiana et al., 2023) stated that tax information systems tend to require Performance, Control, Efficiency, and Service (PCES) standards. Within the scope of accounting information systems, several researchers state that Performance, Information, Economics, and Efficiency (PIEE) standards are the most important (Astriyani et al., 2020; Nugroho, 2021; Prakasita N & Nugroho, 2018; Sundari et al., 2020).

Even though ethical hacking is not a crime, in essence they are still human. But it is important to remember that there is no complete guarantee in system security. Companies also need to have strong internal security measures in place and carry out regular security testing to protect their data. To believe in an ethical hacker, at least some of these benchmarks can be used as a basis. Study the background and certifications, companies should check the background and certifications of an ethical hacker before trusting them. Experience and references, companies can ask for proof of experience and references from previous projects that have been completed by ethical hackers. Evaluation of technical capabilities, test the technical capabilities of an ethical hacker through security tests or relevant challenges. This allows companies to see the extent of their capabilities in finding vulnerabilities and protecting systems.

Check ethics and integrity, they must have strong ethical principles, such as respecting data confidentiality and not abusing the access granted (Manjikian, 2022, p. 89). Nondisclosure contracts and agreements, establishes clear boundaries and obligations to keep company information confidential (Dorofeev, Aleksandr V., Alexey S. Markov, 2022). Collaboration and monitoring, build long-term working relationships with trusted ethical hackers. In some cases, they may contract with them as a security consultant to continuously monitor systems and help identify new vulnerabilities. Recommendations from trusted sources, seek recommendations from trusted sources, such as reputable cybersecurity firms, ethical hacker communities, or other security professionals (Wylie, P. L., & Crawley, 2020). But it is important to remember that there is no complete guarantee in system security. Companies also need to have strong internal security measures in place and carry out regular security testing to protect their data (Harper et al., 2022).

What's more, the demand for the use of big data in accounting information systems has led to an increasingly advanced level of its constituent technology (Demirkan, S., Demirkan, I., & McKee, 2020). And the higher the threat that might be faced. This threat can be in the form of data theft and sabotage (Raewf, M. B., & Jasim, 2020). Furthermore, focused in accounting information system, although ethical hacking activities have positive goals, sometimes ethical hackers commit illegal actions and turn into black hat hackers who use their knowledge to commit crimes (Babys, 2021; Muria, R. M., Muntasa, A., Yusuf, M., & Hamzah, 2022). Therefore, ethical hacking activities must be carried out by individuals who have received certification, adhere to ethics, and have legal awareness in carrying out their duties (Putra et al., 2023). A person who wants to become an ethical hacker must be given training on the strategies and methods used by black hat hackers (Wardhana et al., 2023).

This needs to be done with care because it can add to the number of bad hackers, not just to improve the situation. Ultimately, the individual's decision will determine whether he will use his knowledge and skills ethically or illegally. In addition to adequate knowledge and skills, strong and positive moral values must also be the focus of ethical hacking training.

Research Method

The method used in conducting this research is a quantitative descriptive method. This method is suitable for knowing the value of the independent variable without having to compare or make connections between other variables (Hardani, 2020). The research was conducted using secondary data with data collection techniques in the form of documentation. Overall, the purpose of documentation is to provide information related to the contents of the document to the user, provide evidence and data related to the contents of the document, maintain and physically store the document, and prevent damage to the document. The research sampling technique used was purposive sampling. The determination of the sample is based on the topic of research discussion, namely accounting ethics and cyber security and research quality (Munandar, 2022). The advantage of this technique is that researchers can direct clearly and produce information in a directed manner regarding the field to be studied (Sugiyono, 2020). This technique has been used by several studies on ethical hacking (Azzahra & Heniarti, 2022; Kadir et al., 2023; Misesani et al., 2020).

The observed data is in the form of research related to issues, roles, and the level of need for ethical hacking in a company in order to create cybersecurity (Haq et al., 2022). Meanwhile, this study chose to focus on the level of need for the use of ethical hacker services in accounting information systems through ethical hacking programs. The use of data sources is ensured to come from journal articles that have been indexed by ISSN. A total of 80 articles published in the 2018-2023 timeframe are detailed with the aim of obtaining an assessment of each aspect within the PIECES framework.

Result and Discussion

Today, maximum data transfer is done via the internet. No network is completely secure. Every individual has some weaknesses, sometimes overlooked by hackers (Silic, M., & Lowry, 2021). Since data is so valuable, it is important for every company or organization to detect weaknesses in the network as quickly as possible. However, how are network weaknesses detected. Do we have to wait for unwanted events? This is why cyber security experts or ethical hackers are here (Mouheb, D., Abbas, S., & Merabti, 2019). The main goal of ethical hacking is to find and fix flaws in the network. To achieve this goal, white hat hackers perform penetration tests. Penetration testing (abbreviated pen testing) is a cyber-attack simulation that is carried out to find potential threats and vulnerable parts of the network so that black hat hackers cannot access the network and harm the company.

Disclosure of research results begins with the presentation of a systematic framework of thinking. This framework of thinking serves as the basis for facilitating the research process and ensuring that research is carried out in a structured manner (Hawamleh et al., 2020).

P-ISSN 2828-4976
E-ISSN 2808-263X

Based on Figure 1, it is clear that the research process will begin by examining current issues related to accounting ethics and information security. Accounting ethics is often associated with information security issues because both contain values that are positively related (Callen, J., & James, 2020). Information security will be of higher quality if it is accompanied by intelligent and dignified user ethics in accordance with the principles of their respective professions.

The PIECES Framework (Performance, Information, Economy, Control, Efficiency, and Services) is a framework used in system requirements analysis. Using the PIECES framework has several advantages. Comprehensive, covers important aspects of system requirements analysis. Taking into account Performance, Information, Economy, Control, Efficiency and Service, this framework ensures that no important aspect is overlooked in understanding system requirements. Systematic approach, helps in carrying out a need analysis with a systematic approach. Each aspect is analyzed separately and then integrated into a complete whole. This approach ensures that all aspects of system requirements are considered holistically. Focus on business goals, places focus on an organization's business goals. By analyzing system requirements in the context of performance, economy, efficiency and service, this framework helps ensure that the developed system can support broader business goals.

Identify exact requirements, helps in identifying exact requirements for the system. This allows the requirements analyst to understand the functional and non-functional requirements that must be met by the system. Better risk management, helps in identifying potential risks related to system requirements. Taking into account the necessary controls and information, as well as the expected efficiency and performance, this framework helps in better managing risks during the analysis of needs stage.

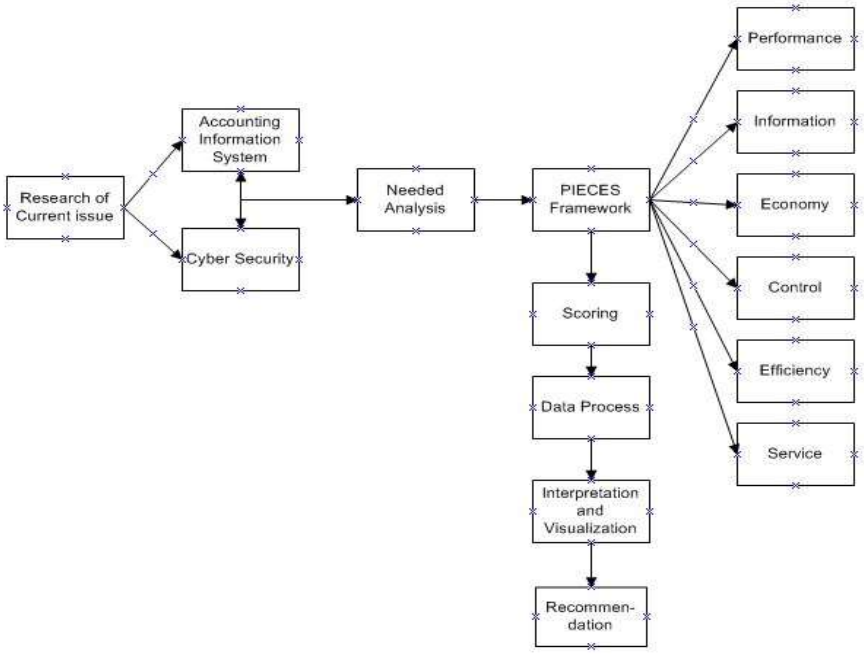

Figure 1. Theoritical Framework

Sources: Data processed by author, 2023

Based on the 100 selected journal articles, 80 journal articles were obtained that met the qualifications for both the scope of the research and the quality of the journal articles. Based on comparisons per year, it appears that 2022 and 2023 will be the years with the highest ethical hacking research results. This is then supported by (Ernawatiningsih, N. P. L., & Kepramareni, 2019). Figure 2 is a research trend related to ethical hacking in the scope of cyber security and the scope of accounting information systems. The increase in the number of studies is because various parties feel the importance of ethical hacking studies, especially in the field of accounting information systems to tackle cyber-crime. Many people say that the costs incurred by companies in order to secure their business processes are in accordance with the benefits they get if they can analyze needs properly and find third parties or what are known as ethical hackers correctly. The issue of ethical trust in the ethical hacker profession is also highlighted in more than 40% of the data used in this study. In addition, it can be concluded that the trend of cyber security in AIS always increases every year by the number 87,50% ((80-70)/80) x 100%.

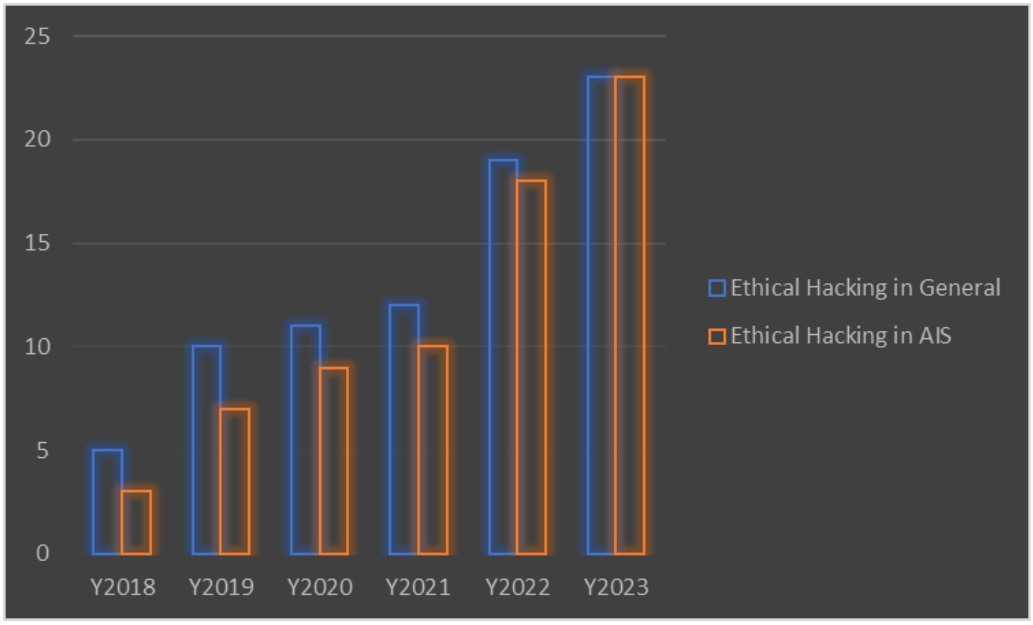

Figure 2. Trend of Research in Ethical Hacking Scope

Sources: Data processed by author, 2023

Table 1.
Analysis of Needs of Ethical Hacking in AIS

No.	Aspects	Criteria of Aspect
1.	Performance	Can ethical hackers assess the performance of AIS and can they find system vulnerabilities that may be misused by internal companies?
2.	Information	Can ethical hackers ensure that the system has generated relevant information according to the company's business processes? and can they ensure there are no debugging and data processing failures?
3.	Economy	Can ethical hackers judge that a company's system is not a waste? Can they assess how much the value creation of the system they are testing is for the company?

P-ISSN 2828-4976
E-ISSN 2808-263X

No.	Aspects	Criteria of Aspect
4.	Control	How can ethical hackers check the control capabilities of AIS in the company's business processes? Are the controls accessible to multiple authorities? and who might be able to do system damage?
5.	Efficient	How can ethical hackers evaluate the system's ability to process data so that it can produce reliable information in a short time? Can ethical hackers find gaps in system efficiency leaks such as using inappropriate anti-virus, etc.?
6.	Service	How can ethical hackers assess the level of service provided by AIS in supporting the company's business processes? Is the quality of this service independent or can it be intervened by several parties in order to take personal advantage? Can the system be manipulated? and how to detect it?

Sources: Data processed by author, 2023

Furthermore, the following table will describe the analysis of ethical hacker needs in the scope of accounting information systems using the PIECES framework. Each aspect is described according to the appropriate points. So, based on this table, conclusions can be drawn for the level of urgency of each aspect. Table 1 contains the PIECES framework using the relevant reference base (Novriani et al., 2023). In a broader context, the PIECES framework is not limited to being used as a tool for needs analysis. Furthermore, this framework is also used as a basis for evaluation-based decision making. Thus, the use of the PIECES framework is expected to maximize the analysis process to produce the right decisions. Based on this analysis, an emphasis will be presented on the need to apply ethical hacking in an accounting information system as shown in the table below.

Table 2.
Calculation of Urgency (per Aspect)

No.	Aspects	Ranking of Criteria	Priority's Aspects
1.	Performance	15	18,75%
2.	Information	25	31,25%
3.	Economy	5	6,25%
4.	Control	20	25,00%
5.	Efficient	9	11,25%
6.	Service	6	7,50%
	Grand Total	80	100%

Sources: Data processed by author, 2023

In accordance with the calculation results above, it is clear that the level of urgency of needs has been described in detail. Research shows that accounting information systems require the involvement of ethical hacking in assessing and providing security guarantees for company systems. So that business processes can take place properly and smoothly without causing material or non-material losses to the company. The information aspect is the need with the highest urgency reaching 31.25% ((25/80) x 100%), followed by the control aspect with the second level of urgency reaching 25.00%. The interesting thing is that the economic aspect is the least urgent aspect (has the lowest urgency ranking compared to other aspects). Research proves that companies tend to choose to use paid accounting information systems as long as they get advanced benefits. Companies will not be "stingy" to invest in technology in order to support the smooth running of their work systems or business processes. And these results are in accordance with the phenomenon that technology is the main asset and

has become something to be reckoned with (Marcelina & Yulianti, 2022). This means that the more companies judge that their technology is valuable, the higher the tendency to secure it (Sibero, 2022).

Figure 3 visually presents the urgency of using or making decisions about the implementation of ethical hacking. This study proves that the information aspect holds the highest rank because the basic concept of an accounting information system is information itself both in quantity and quality. Ethical hacking is expected to be able to assess and provide recommendations for improvements to vulnerabilities and review AIS resistance in dealing with cyber-attack both internally and externally. Based on the results of the data processing presented above, it can be seen that ethical hacking really needs to be involved in the process of cyber security in accounting information systems.

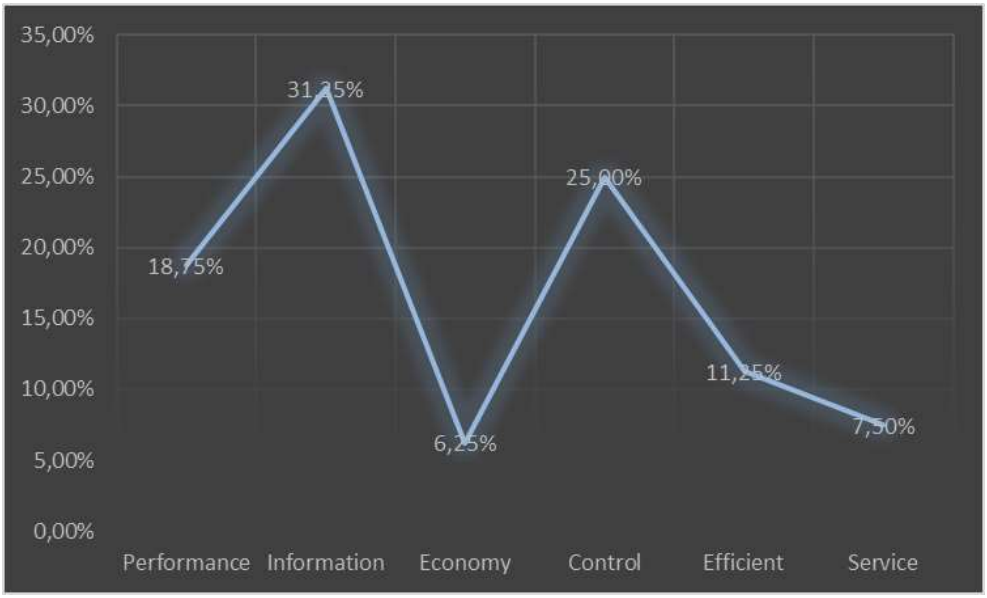

Figure 3. Urgency Mapping of Needs
Sources: Data processed by author, 2023

The results of this study are in accordance with the research conducted Santoso & Rukmana, (2023) although they did not explicitly mention the aspects studied and were not included with the display of the results of the comparison of needs. Ethical hackers who are engaged in ethical hacking have a major role in the field of cybersecurity of accounting information systems. Apart from that, the information system is a system that is prone to being used as a target of crime.

Conclusion

Based on the research that has been done, several points can be concluded, including the following:

1. The PIECES framework contains six aspects that can be used to analyze needs, consisting of Performance, Information, Economy, Control, Efficiency, and Service.

P-ISSN 2828-4976
E-ISSN 2808-263X

2. Apart from being used as a needs analysis, furthermore the PIECES framework can also be used to analyze results or system evaluation.
3. Based on the results of an analysis of the literature review of research data on articles published in the 2018-2023 range (as many as 80 articles) it shows that the performance aspect is in the accounting information system and is disbursed by the information aspect.
4. The economic aspect is the aspect with the lowest level of urgency. This is supported by the phenomenon of purchasing a license (paid system) from a third party as well as independent development carried out by the company. This policy is carried out in order to expedite business processes.

So that, the relationship between ethical hacking and accounting information systems are as here. Identification of security weaknesses, security testing, data and information protection, customer data security, increasing security awareness. However, it is important to note that ethical hacking must be done with permission and within established boundaries. It must be performed by security professionals who have the appropriate knowledge and skills to maintain the integrity and confidentiality of accounting information systems without causing damage or breach of privacy.

Implication

1. Theoretical implications

Research examines new perspectives on ethical hacking that may have been studied by many parties. The perspective referred to in this case is to provide a study of the perspective of ethical hacking practices using the PIECES concept. This concept can be used as a tool or framework that serves as an analysis and evaluation tool.

2. Practical implications

The PIECES concept used in analyzing the needs of an Accounting Information System (AIS) can be adopted as a framework for analyzing other things in everyday life. The PIECES framework in the concept of ethical hacking can be adapted to other contexts in the other research to develop a new concept or finding.

Limitations and Future Studies

1. The data from this study is in the form of a literature review which does not mention in detail where the trend of Accounting Information Systems (AIS) requires ethical hacking.
2. It is not presented how much the percentage of ethical hacking awareness in the Accounting Information System (SIA) is in a particular process. For example, Accounting Information Systems (AIS) of payroll, Accounting Information Systems (AIS) of cash in and out cash, or Accounting Information Systems (AIS) of budgeting.

Future research may have Add data or instead choose to focus and discuss in detail the need for ethical hacking in a developed country or a developing country. The selection of objects must of course be based on clear and rationally understandable assumptions.

Suggestion

As for suggestions and recommendations that researchers can provide as ideas or considerations for further research, namely by linking the level of urgency of involving ethical

hacking in accounting information systems to involving opportunity costs. This is interesting for further study considering that opportunity cost is a fundamental consideration for management in making decisions. At the same time answering whether paying ethical hackers will increase the company's value creation or actually cause cost inefficiencies. Furthermore, future research can also link several concepts such as urgency needs analysis with the PIECES framework, opportunity costs, and user trust in ethical hackers. So that the results of the research conducted will be more interesting and can be a reference for companies in making policies.

References

Aljebry, A. F., Alqahtani, Y. M., & Sulaiman, N. (2022). Analyzing Security Testing Tools for Web Applications. In International Conference on Innovative Computing and Communications. *Proceedings of ICICC*, 411–419.

Astriyani, E., Putri, F. N., & Widianingsih, N. E. (2020). Desain Sistem Informasi Monitoring Aset. *Jurnal Teknologi*, *6*(1), 87–99. https://media.neliti.com/media/publications/318262-desain-sistem-informasi-monitoring-aset-025e1d45.pdf

Atil, S. H. P., Hole, A. K. D., Ilak, A. N. N., Ol, R. O. P., & Amble, P. O. K. (2018). ETHICAL HACKING : Need of Security. *IJARIIE*, *4*(5), 112–117.

Azzahra, R. N., & Heniarti, D. D. (2022). Pertanggungjawaban Pidana Anggota Polisi sebagai Pelaku Tindak Pidana Penjualan Senjata Api kepada Kelompok Kriminal Bersenjata. *Bandung Conference Series: Law Studies*, *2*(1), 278–285. https://doi.org/10.29313/bcsls.v2i1.802

Babys, S. A. (2021). Ancaman Perang Siber Di Era Digital Dan Solusi Keamanan Nasional Indonesia. *Oratio Directa (Prodi Ilmu Komunikasi)*, *3*(1), 5–14.

Brilliant, P. (2023). Penerapan Analisis PIECES pada Rancangan Sistem Informasi Manajemen Human Asset Value Berbasis Website. *Jurnal Rekayasa Informasi Swadhrama*, *03*(01), 15–23.

Callen, J., & James, J. E. (2020). CYBERSECURITY ENGINEERING: THE GROWING NEED. *Issues in Information Systems*, *21*(4), 5–11.

Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity*. Springer Nature.

Del-Real, C., & Rodriguez Mesa, M. J. (2022). From black to white: the regulation of ethical hacking in Spain. In *Information and Communications Technology Law* (Vol. 0, Issue 0). https://doi.org/10.1080/13600834.2022.2132595

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189–208.

Ding, A. Y., De Jesus, G. L., & Janssen, M. (49 C.E.). Ethical hacking for boosting IoT vulnerability management: A first look into bug bounty programs and responsible disclosure. *In Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing*, 55.

Dorofeev, Aleksandr V., Alexey S. Markov, and Y. V. R. (2022). Ethical hacking training. *In CEUR Workshop Proceedings*, 47–56.

Endaryati, E. (2021). *Sistem Informasi Akuntansi* (Indra Ava Dianta (ed.); 2nd ed.). Universitas Telkom.

Ernawatiningsih, N. P. L., & Kepramareni, P. (2019). Effectiveness of accounting information

P-ISSN 2828-4976
E-ISSN 2808-263X

systems and the affecting factors. *International Journal of Applied Business and International Management (IJABIM)*, *4*(2), 33–40.

Formosa, P., Wilson, M., & Richards, D. (2023). A principlist framework for cybersecurity ethics. *Computers & Security*, *10*(9), 102–111.

Georg, T., Oliver, B., & Gregory, L. (2018). Issues of implied trust in ethical hacking. *The ORBIT Journal*, *2*(1), 1–19.

Haq, H. B. U., Hassan, M. Z., Hussain, M. Z., Khan, R. A., Nawaz, S., Khokhar, H. R., & Arshad, M. (2022). The Impacts of Ethical Hacking and its Security Mechanisms. *Pakistan Journal of Engineering and Technology*, *5*(4), 29–35.

Hardani. (2020). *Metode Penelitian Kualitatif & Kuantitatif*. CV ALFABETA.

Hardiana, R. D., Sugiharti, H., Mardiani, R., Kurniati, F., & Indonesia, U. P. (2023). Metode Fast : Analisis dan Desain Sistem Informasi. *ACCOUNTHINK : Journal of Accounting and Finance*, *8*(01), 13–37.

Harper, A., Linn, R., Sims, S., Baucom, M., Fernandez, D., Tejeda, H., & Frost, M. (2022). *Gray hat hacking: the ethical hacker's handbook*. McGraw-Hill Education.

Hartono, B. (2014). Hacker Dalam Perspektif Hukum Indonesia. *Masalah-Masalah Hukum*, *43*(1), 23–30.

Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, *63*(5), 7894–7899.

Holt, T. J., Cale, J., Brewer, R., & Goldsmith, A. (2021). Assessing the role of opportunity and low self-control in juvenile hacking. *Crime & Delinquency*, *67*(5), 662–688.

Jean, P. (2023). TOOL FOR HACKING PHASES. *International Research Journal of Modernization in Engineering Technology and Science*, *752*(01), 1308–1317.

Jofre, M. (2023). Networks and Systems. *Seminar on Quantum Technologies for Cybersecurity*, 5–9.

Kadir, A., Mahamood, B. I. N., Fadli, M., & Zolkipli, B. I. N. (2023). Critical and Creative Thinking in A Hacker ' s Work. *Borneo International Journal*, *6*(1), 53–60.

Kasim, M., Saidu, M. B., Isa, A., & Utulu, S. C. A. (2022). *A Proposal for Social Ethical Hacking Framework for Detecting and Managing Human-Induced Vulnerabilities in Organizational Cybersecurity*.

Kelrey, A. R., & Muzaki, A. (2019). Pengaruh Ethical Hacking Bagi Keamanan Data Perusahaan. *Cyber Security Dan Forensik Digital*, *2*(2), 77–81. https://doi.org/10.14421/csecurity.2019.2.2.1625

Kieslich, K., Keller, B., & Starke, C. (2022). Artificial intelligence ethics by design. Evaluating public perception on the importance of ethical design principles of artificial intelligence. *Big Data & Society*, *9*(1), 55–64.

Komarudin, D., Pratama, P. A., & Paramadina, U. (2022). ANCAMAN DISTRIBUSI SMALL ARMS & LIGHT WEAPONS (SALW) SERTA IMPRESINYA TERHADAP. *Jurnal Dinamika Global*, *7*(1), 138–162. https://doi.org/https://doi.org/10.36859/jdg.v7i01.982 140

Kumawat, V., Pal, P., & Jha, P. (2023). Ethical Hacking: White Hat Hackers. *SCRS Proceedings of International Conference of Undergraduate Students*, *3*(1), 13–17. https://doi.org/10.52458/978-81-95502-01-1-2

Manjikian, M. (2022). *Cybersecurity ethics: an introduction*. Taylor & Francis.

Marcelina, D., & Yulianti, E. (2022). WORKSHOP TEKNOLOGI INFORMASI " DASAR CYBER SECURITY " PADA SMK PGRI TANJUNG RAJA OGAN ILIR (OI). *Jurnal Abdimas*, *6*(2), 67–72.

Misesani, D., Janggo, W. O., & Wuwur, M. S. N. (2020). Need Analysis in ADDIE Model to Develop Academic Speaking Materials. *Ethical Lingua: Journal of Language Teaching and Literature*, *7*(2), 438–446. https://doi.org/10.30605/25409190.226

Mouheb, D., Abbas, S., & Merabti, M. (2019). Cybersecurity curriculum design: A survey. *Ransactions on Edutainment XV*, *4*(2), 93–107.

Munandar, dkk. (2022). *Metodologi Penelitian Kuantitatif dan Kualitatif* (Arif Munandar (ed.); 1st ed.). CV. Media Sains Indonesia.

Muria, R. M., Muntasa, A., Yusuf, M., & Hamzah, A. (2022). Studi Litelatur: Peningkatan Kinerja Digital Forensik Dan Pencegahan Cyber Crime. *Jurnal Aplikasi Teknologi Informasi Dan Manajemen (JATIM)*, *3*(1), 12–20.

Novriani, M., Pa, E. D., Tiswiyanti, W., Ekonomi, F., & Jambi, U. (2023). Analisis Kinerja Sistem Aplikasi SMDD (Sistem Manajemen Dokumen Digital) dalam Pengelolaan Transaksi Keuangan dan Arsip Digital pada PT . Jasa Raharja Cabang Jambi dengan menggunakan Metode Pieces. *Jurnal Pendidikan Tambusai*, *7*(1), 2912–2925.

Nugroho, P. (2021). *Pemanfaatan aplikasi appsheet untuk meningkatkan kinerja manajemen proyek pada kontraktor*. Universitas Islam Indonesia.

Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, *5*(2), 233–254.

Prakasita N, D., & Nugroho, M. A. (2018). Perancangan Sistem Informasi Akuntansi Penjualan Dan Persediaan Di Central Steak and Coffee Boyolali. *Nominal, Barometer Riset Akuntansi Dan Manajemen*, *7*(1), 69–81. https://doi.org/10.21831/nominal.v7i1.19360

Putra, I. K. O. K., Darmawan, I. M. A., & Juliana, I. P. G. (2023). TINDAKAN KEJAHATAN PADA DUNIA DIGITAL DALAM BENTUK PHISING. *Cyber Security Dan Forensik Digital*, *5*(2), 77–82.

Quasim, M. T., Al Hawi, A. N., & Meraj, M. (2023). *System Penetration: Concepts, Attack Methods, and Defense Strategies*. EasyChair.

Raewf, M. B., & Jasim, Y. A. (2020). Information technology's impact on the accounting system. *Cihan University-Erbil Journal of Humanities and Social Sciences*, *4*(1), 50–57.

Rudenko, E., Gnatenko, A., Milich, A., Hedgecock, K., & Malekos, Z. (2023). Leveraging Ethical Hacking in Russia : Exploring the Design and Potential of Bug Bounty Programs. *Information Technology and Computer Science*, *3*(2), 1–15.

Santoso, B. P., & Rukmana, O. (2023). Pengembangan Sistem Informasi Pengelolaan Baitulmal dengan Multi Platform. *Bandung Conference Series: Industrial Engineering Science*, *3*(1), 276–284. https://doi.org/10.29313/bcsies.v3i1.6618

Shoemaker, D., Kohnke, A., & Laidlaw, G. (2019). Ethics and cybersecurity are not mutually exclusive. *EDPACS*, *60*(1), 1–10.

Sibero. (2022). Website dan Jaringan Komputer Dasar. *Jurnal Sains Dan Informatika*, *3*(1), 35.

Silic, M., & Lowry, P. B. (2021). Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes. *Information Systems Frontiers*, *2*(3), 329–341.

Smith, L. A., Chowdhury, M., & Latif, S. (2022). Ethical hacking: Skills to fight cybersecurity threats. *EPiC Series in Computing*, *82*(5), 102–111. https://doi.org/10.29007/vwww

Sugiyono. (2020). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. CV Alfabeta.

Sundari, C., Susilo, G., & Lukita Anggraeni, D. (2020). Analisis Kebutuhan Sistem Informasi Keuangan Pada CV Rahayu Karya. *Jurnal TRANSFORMASI*, *16*(2), 74–81.

Turner, L., Weickgenannt, A. B., & Copeland, M. K. (2022). *Accounting information systems: controls and processes*. John Wiley & Sons.

P-ISSN 2828-4976
E-ISSN 2808-263X

Vandervelden, S., Chowdhury, M. M., & Latif, S. (2019). Managing the cyber world: Hacker edition. *International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 1–6.

Vignesh, R., & Rohini, K. (2022). Analysis to determine the scope and Challenging responsibilities of Ethical Hacking employed in Cyber Security. *International Journal of Engineering and Technology(UAE)*, *7*(3.27), 196–199. https://doi.org/10.14419/ijet.v7i3.27.17759

Walker, M. (2022). *CEH Certified Ethical Hacker Bundle*. McGraw-Hill Education.

Wallingford, J., Peshwa, M., & Kelly, D. (2019). Towards understanding the value of ethical hacking. In International Conference on Cyber Warfare and Security. *Academic Conferences International Limited*, 639.

Wardhana, A., Pradana, M., Kartawinata, B. R., & Akbar, A. (2023). Financial Technology 4.0 Indonesia Perspective. *Accounting and Finance*, *4*(11), 89–95.

Wylie, P. L., & Crawley, K. (2020). *The Pentester Blueprint: Starting a career as an ethical hacker*. John Wiley & Sons.

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). A Survey on Ethical Hacking: Issues and Challenges. *A Preprint*, *3*(1), 1–46. http://arxiv.org/abs/2103.15072