DIJEFA:
Dinasti International Journal of Economics, Finance & Accounting
E-ISSN: 2721-303X
P-ISSN: 2721-3021
https://dinastipub.org/DIJEFA dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/dijefa.v6i1

Operational Risk Management in Digital Banks: Challenges and Solutions

Wirawan Widjanarko[1], Adler Haymans Manurung[2], Nera Marinda Machdar[3].
[1]Mahasiswa Program Doktoral Ilmu Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, wwidjanarko2@gmail.com.
[2]Dosen Program Doktoral Ilmu Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, adler.manurung@dsn.ubharajaya.ac.id.
[3]Dosen Program Doktoral Ilmu Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, nmachdar@gmail.com.

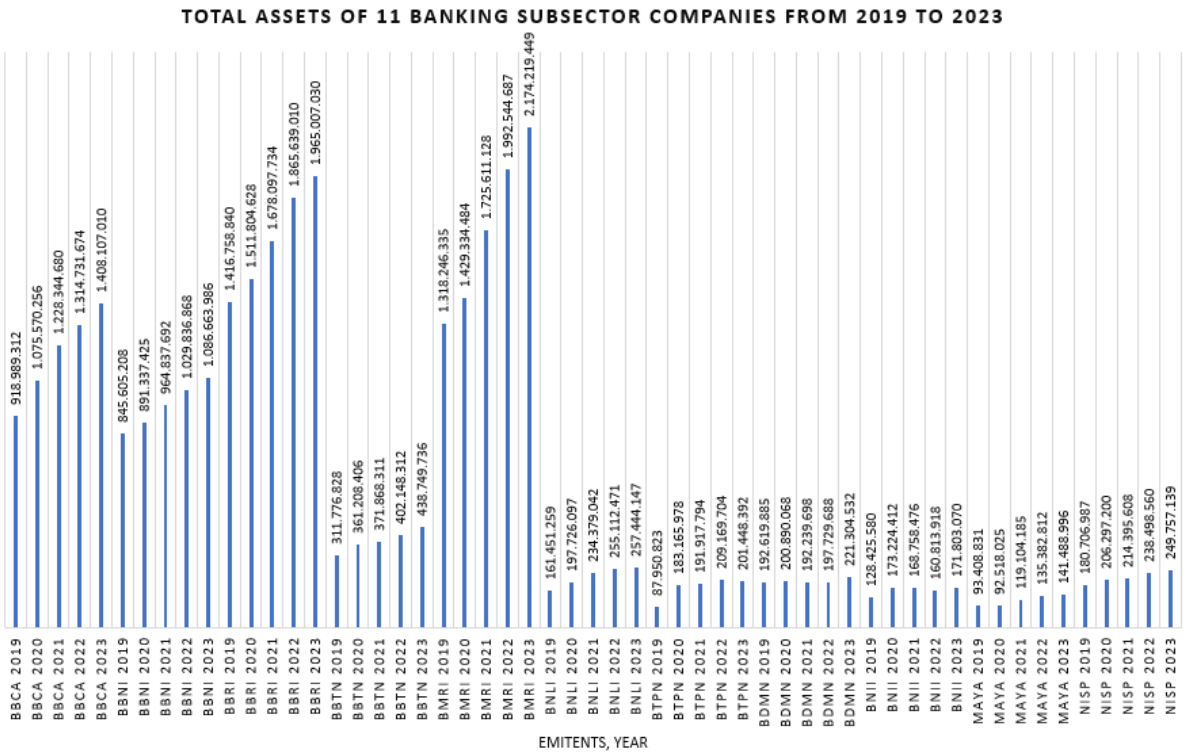
Corresponding Author: wwidjanarko2@gmail.com[1]

Abstract: The purpose of this research is to see the effect of system uptime and compliance regulations on operational risk management in digital banks (cybersecurity). The approach used in this literature review research is descriptive qualitative. The data collection technique is to use literature studies or conduct literature reviews of relevant previous articles. The data used in this research is secondary data, sourced from academic online media such as Thomson Reuters Journals, Sage, Springer, Taylor & Francis, Scopus Emerald, Elsevier, Sage, Springer, Web of Science, Sinta Journals, DOAJ, EBSCO, Google Scholar and digital reference books. In previous studies, 1 relevant previous article was used to review each independent variable. The results of this literature review article are: 1) System uptime affects Cyber Security at Digital Banks; and 2) Regulatory compliance affects Cyber Security in Digital Banks.

Keyword: Cyber Security, System Uptime, Regulatory Compliance.

INTRODUCTION

Banks are one of the business sectors in a country, and need special attention by stakeholders. Badruzaman, (2020) states that banks have a crucial role in the financial system of a country, and are a fundamental issue related to economic and financial theory. Assets and loans are indicators that show the role and growth of the banking sector. Assets owned by banking companies increased per year in the period 2019 to 2023. Then net income experienced a fluctuating increase in the period 2019 to 2023.



Source: Indonesia Stock Exchange, 2024

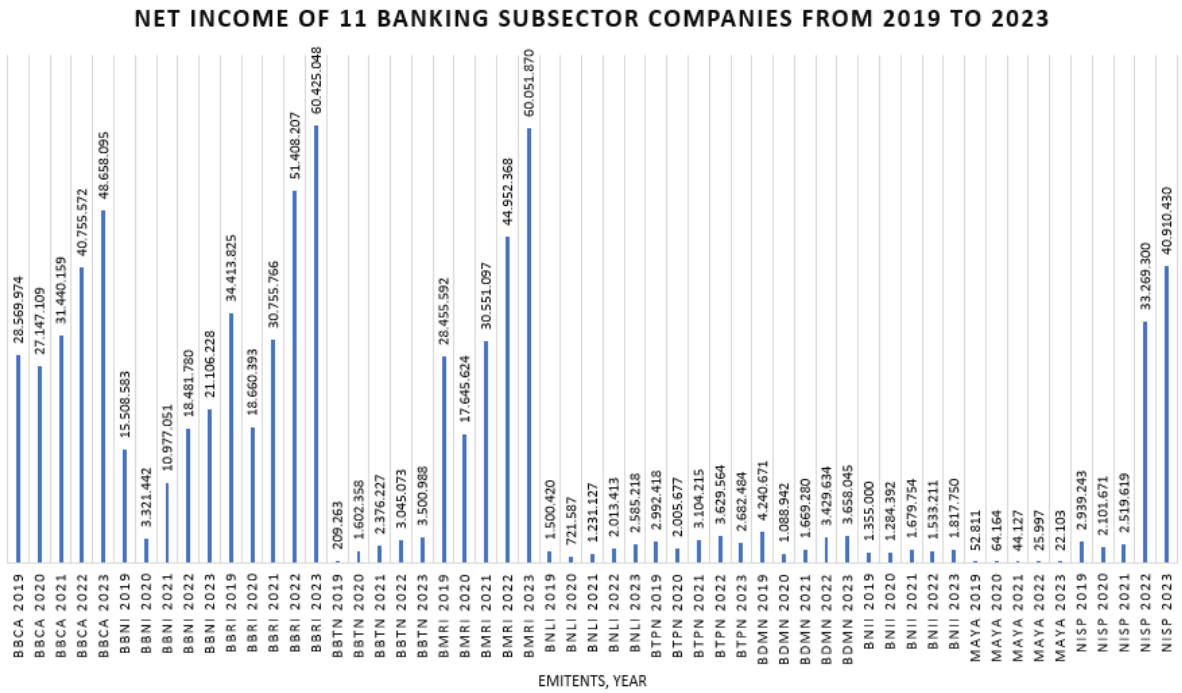
Figure 1. Total Assets of 11 Banking Subsector Companies from 2019 to 2023

Based on figure 1 above, there is a significant upward trend in assets for most companies in the banking sub-sector over the period. Bank BCA (BBCA) and BRI (BBRI) have the highest asset values, with consistent year-on-year increases. This shows their dominance in the Indonesian banking sector.

In addition, banks such as BNI (BBNI) and BTN (BBTN) also showed a significant increase in assets, albeit to a lesser extent than BCA and BRI. However, there are some issuers, such as MAYA and BNII, whose assets are smaller than those of the big banks, indicating a disparity in the scale of activity between companies.

The significant increase in assets of some large banks reflects the success of their growth strategies, which may involve operational risks, especially related to cybersecurity. On the other hand, the lower asset values of some other banks indicate opportunities for them to strengthen their market position. Overall, these trends reflect the intensifying competitive dynamics in the Indonesian banking industry and the importance of asset management strategies for sustainable growth.

The intense competition between these banking companies in grabbing the market can be characterized by the net profit they earn. According to Yulaeli et al., (2023), net income is the profit or loss earned by the company after deducting all costs and expenses during a certain period, including operating expenses, interest, taxes, depreciation, and amortization.



Source: Indonesia Stock Exchange, 2024

Figure 2. Net Income of 11 Banking Subsector Companies for the Period 2019 to 2023

Based on figure 2, there is a significant variation in the net profit earned by each bank in the banking subsector from year to year. Bank BCA (BBCA) has a consistently high net profit performance, reaching its peak in 2023. Bank BRI (BBRI) also shows a significant increase, especially in 2022, before experiencing a slight decline in 2023. In contrast, some banks such as BTN (BBTN) and MAYA have much lower net profit levels compared to the big players such as BBCA and BBRI, although there are slight fluctuations from year to year. This chart shows that financial performance varies widely among banks, which is most likely influenced by prevailing business strategies, digitalization, and cybersecurity. In general, large banks tend to be more stable in generating net income than small or medium-sized banks.

Based on the background of the problem above, the problem formulation in this study is determined as follows: 1) Does System Uptime affect Cyber Security at Digital Banks?; and 2) Does Regulatory Compliance affect Cybersecurity in Digital Banks?

METHOD

This research uses a descriptive qualitative approach. This method was chosen because it allows researchers to thoroughly understand cybersecurity-related research concepts, focusing on the context and meaning contained in system uptime and compliance regulations. Descriptive qualitative data collection and analysis allows researchers to tailor their approach to the needs of the research and the characteristics of the subject under study, (Dewi, 2024).

The data used in this study comes from previous research related to cybersecurity, system uptime and regulatory compliance. The researcher will analyze the existing literature to identify patterns and trends in the concept of cybersecurity. By using previous research and other references, researchers can develop stronger, evidence-based arguments and contribute to a broader understanding of cybersecurity.

The type of data used in this research is secondary data, which uses data from various leading academic journals, including Thomson Reuters Journal, Springer, Taylor & Francis, Scopus, Emerald, Sage, WoS, Sinta Journal, DOAJ, and EBSCO, as well as platforms such as Publish or Perish and Google Scholar. By using these sources, researchers can ensure that the

data they collect is valid and accountable. The use of multiple sources also allows researchers to gain a more comprehensive understanding of cybersecurity from various perspectives.

RESULTS AND DISCUSSION

Results

The following are the research findings considering the context and problem formulation:

Cyber Security

Cybersecurity is the practice of protecting systems, networks and data from digital threats that can cause financial loss, reputational damage or privacy breaches. It includes measures such as securing hardware, software and data, and implementing security protocols to prevent unauthorized access, hacking or other cyber-attacks, (Mauliza et al., 2022).

According to Alzoubi et al., (2022), cybersecurity is the activity of protecting digital information stored and processed by information systems, including hardware, software, and data, from threats or attacks that can cause damage, unauthorized access, or unauthorized modification, (Restika & Sonita, 2023).

Indicators or dimensions contained in Cyber Security include: 1) Confidentiality: Ensuring that information can only be accessed by authorized parties. Confidentiality ensures that data does not fall into the wrong hands or is not accessed by unauthorized parties; 2) Integrity: Protecting the accuracy and consistency of data from unauthorized changes, both intentional and unintentional. Integrity ensures that data remains authentic from the time it is created until it is accessed; 3) Availability: Ensuring that systems, applications, and data are always available for use by authorized users when needed, while minimizing downtime; 4) Authentication: The process of verifying the identity of a user or system before granting access to information or resources. Authentication is designed to prevent unauthorized access; and 5) Risk Management: The process of identifying, assessing, and controlling cybersecurity risks that could threaten an organization's information technology infrastructure and data.

Cyber Security has been researched and is relevant to the research conducted by: (Azzahra et al., 2024), (Luthfah, 2024), (R. Alfarizi et al., 2024).

System Uptime

Uptime refers to the amount of time a system, server or information technology service operates without interruption or downtime. Uptime is an important indicator of the reliability and efficiency of technology infrastructure, especially in business environments that rely heavily on IT-based operations. The higher the level of uptime, the less disruption to operations, which means that organizations can provide more consistent services to customers and internal users, (Pradana, 2021).

Indicators or dimensions contained in System Uptime include: 1) Uptime: The amount of time a system runs without interruption in a given time period, often calculated as a percentage of total time; 2) Downtime: Measures how long a system is inaccessible or inoperative due to damage, maintenance, or other external factors; 3) Server Performance: The ability of a server to consistently handle a workload without interruption. This indicator includes CPU, memory, and bandwidth usage; 4) System Reliability: The ability of the system to operate properly without failure over a period of time, reflecting operational stability; and 5) Responsiveness: The speed at which the system responds to user requests, which is a key factor in ensuring an optimal user experience, (Wardhana et al., 2020).

System Uptime has been researched and is relevant to research conducted by: (Ernawati & Rachmat, 2021), (Putra & Suroso, 2024), (Hindarti et al., 2023).

Compliance Regulation

Compliance regulations are rules, standards, or guidelines that organizations must follow to meet certain legal, industry, or international standard requirements. Compliance covers issues such as data protection, information security (ISO 27001), and risk management. Complying with these regulations not only protects the organization from legal fines or sanctions, but also helps maintain the trust of customers, business partners and other stakeholders, (Soleh et al., 2022).

Indicators or dimensions contained in the Compliance Regulations include: 1) Regulatory Compliance: The extent to which the organization complies with applicable regulatory standards, such as GDPR, HIPAA, or ISO 27001, in data management and operations; 2) Internal and External Audits: Periodic inspection processes to assess the extent to which the organization's policies, procedures, and practices meet compliance standards; 3) Compliance Training: Training programs to ensure that all employees understand the regulations and policies that must be followed in their work; 4) Document Management: Management of documents that provide evidence of compliance, such as policies, procedures, and audit reports; and 5) Sanctions and Corrective Action: The organization's ability to address compliance violations, including sanctioning and implementing corrective actions to prevent similar violations in the future, (Susilo, 2023).

Compliance regulations have been researched and are relevant to research conducted by: (Fadillah et al., 2020), (Husnaini et al., 2022), (Sebayang, 2020).

Previous Research

Based on the findings above and previous studies, the following research discussion is formulated:

Table 1. Relevant Previous Research Results

No	Author (Year)	Research Results	Similarities With This Article	Differences With This Article
1	(Razzanda & Koprawi, 2024)	-Intrusion Detection System variables affect Cyber Security -The System Uptime variable affects Cybersecurity -Intrusion Prevention System variables affect Cybersecurity	This article has in common that it examines the System Uptime variable in the independent variable, and examines the Cyber Security variable in the dependent variable.	The difference with previous research is in the Intrusion Detection System and Intrusion Prevention System variables as other independent variables.
2	(Restika & Sonita, 2023)	-The Information Exchange variable affects Cyber Security at Islamic Banks -The Regulation Compliance variable affects Cyber Security in Islamic Banks	This article has in common that it examines the Regulatory Compliance variable on the independent variable, and examines the Cybersecurity variable on the dependent variable.	- The difference with previous research is in the Information Exchange variable as another independent variable. -The difference with previous research is that there is an object of research conducted by Bank Syariah.

Discussion

Based on the formulation of the problem, results and previous research, the discussion in this study is as follows:

The Effect of System Uptime on Cyber Security in Digital Banks

In today's digital era, digital banking has become one of the main pillars in the financial industry. However, with the rapid advancement of technology, various operational risk management challenges arise that these financial institutions must face. An important aspect of operational risk is system uptime, which includes uptime, downtime, server performance, system reliability and responsiveness. Optimal uptime is critical to ensure that digital banking services are continuously available to customers. According to the report Walfajri, (2022), Downtime in digital services can cause significant financial loss, losing value from fee-based income. This highlights the importance of managing system uptime in the context of digital banking.

Furthermore, unexpected downtime can also negatively impact a digital bank's reputation. It causes thousands of customers to lose access to their accounts and leads to a decrease in public trust in banks that experience downtime. In this context, operational risk management should include strategies to minimize downtime, such as implementing redundancy systems and monitoring server performance in real time. According to the report Netmonk, (2023), shows that banks that implement advanced monitoring technology can reduce downtime by 30%, increase customer satisfaction and minimize financial losses.

System reliability is also an important part of operational risk management. System reliability is the ability of a system to operate consistently and reliably over time. In the context of digital banking, system reliability is closely related to cybersecurity which includes data confidentiality, integrity and availability. Banks that do not have reliable systems are at high risk of cyberattacks that could result in sensitive customer data being exposed. Therefore, digital banks must implement strict security policies, including multi-factor authentication and data encryption, to protect customer data.

In terms of responsiveness, digital banks must be able to respond quickly to incidents that may occur, be it cyber attacks or other technical issues. This speed of response is critical to minimize the impact of such incidents. A study by Diwanti & Kandiyah, (2020), shows that organizations with a good incident response plan can reduce recovery time by 50%. This shows that investing in the training and development of incident response teams is critical to maintaining system security and customer trust. In addition, digital banks should actively engage in simulations and testing to ensure their teams are prepared for a variety of potential threats.

To meet these challenges, digital banks must develop an integrated approach to operational risk management. This includes collaboration between IT, cybersecurity and risk management teams to create a comprehensive strategy. By adopting the latest technologies and best practices in risk management, digital banks can improve system uptime and service reliability. In this way, effective operational risk management not only improves cybersecurity, but also delivers value to customers and drives overall business growth for digital banks.

The Effect of Regulatory Compliance on Cybersecurity in Digital Banks

In the ever-evolving digital era, managing operational risk in digital banks has become an important issue for financial institutions. One of the main challenges is complying with the various regulations set by regulators. This compliance includes not only legal aspects, but also internal and external audits to ensure that all operational practices are in line with the set standards. In accordance with POJK 21 of 2023 concerning digital services by commercial banks, the development of digital services carried out by banks must pay attention to aspects of risk management, customer data security and consumer protection, (Otoritas Jasa Keuangan, 2023).

In addition to ensuring customer data security and consumer protection, internal and external audits are also an important part of operational risk management, as they serve as monitoring mechanisms that can detect potential problems before they become crises. Internal audits provide an assessment of the effectiveness of internal controls, while external audits provide an objective third-party view. One of Indonesia's digital banks, BCA, conducts internal and external audits to identify and fix security gaps that could threaten customer data, thereby increasing customer confidence in their services, (Laili et al., 2023).

Compliance training is also an important aspect of operational risk management. Without an adequate understanding of applicable regulations and procedures, employees may make mistakes that could potentially harm the bank. Institutions that invest in compliance training significantly reduce the incidence of regulatory violations by 33.8%, which in turn improves employee performance (Fibriany, 2019). Therefore, digital banks must develop a comprehensive training program to ensure that all employees understand and are able to comply with existing regulations.

Following compliance training for banking staff, document management also plays an important role in operational risk management. In the context of digital banking, good document management ensures that all records and data are securely stored and easily accessible when needed. This is not only important for compliance, but also for maintaining the integrity and confidentiality of customer data. Investing in the right document management technology can be a strategic step in mitigating operational risk, (Musyarofah & Bisma, 2021). Only after the implementation of document management technology can sanctions and remediation be applied, which is an integral part of operational risk management. When a bank violates regulations, regulatory sanctions can be crippling, both financially and reputationally. Therefore, it is important for digital banks to not only focus on compliance, but also develop effective corrective action plans to prevent future violations.

Overall, managing operational risk in digital banks requires a holistic and integrated approach. From regulatory compliance to document management to employee training, each element contributes to better cybersecurity. By understanding the challenges and implementing the right solutions, digital banks can reduce operational risk and increase customer trust, which in turn supports the sustainability and future growth of their business.

Conceptual Framework

The conceptual framework is determined based on the formulation of the problem, research objectives and previous studies that are relevant to the discussion of this literature research:

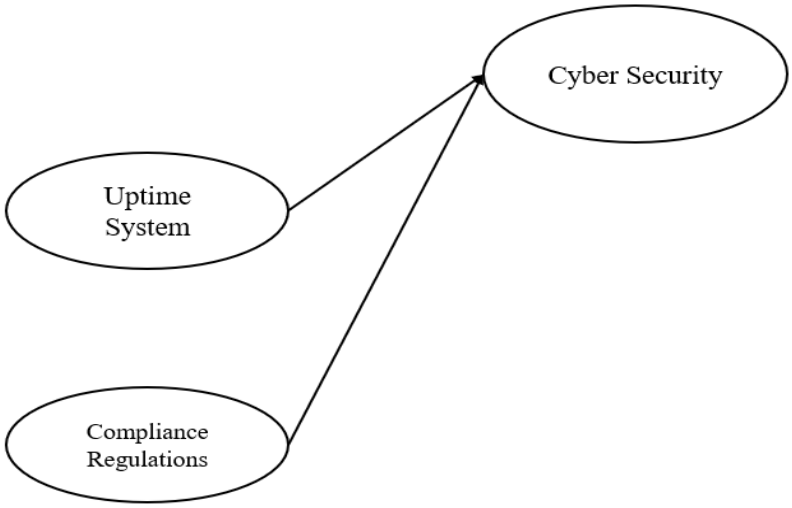


Figure 3. Conceptual Framework

Based on Figure 3 above, system uptime and compliance regulations affect cybersecurity in digital banks. However, in addition to the variables of system uptime and compliance regulations that affect cybersecurity in digital banks, there are other variables that influence, including:

1) Human Resource Competencies: (Ali et al., 2024), (M. I. Alfarizi, 2021), (Khusna et al., 2022).
2) Technology Innovation: (Nofrialdi et al., 2023), (Jumawan et al., 2023), (Widjanarko et al., 2023).
3) Data Encryption: (Firdaus et al., 2025), (Almadira et al., 2024), (Hidayatulloh et al., 2023), (Haryaman et al., 2024).

CONCLUSION

Based on the problem formulation, results and discussion above, the conclusions of this study are:

1) System Uptime affects Cyber Security at Digital Banks;
2) Regulatory Compliance affects Cybersecurity at Digital Banks.

REFERENSI

Alfarizi, M. I. (2021). Pengaruh Motivasi dan Kompetensi SDM Terhadap Kinerja Dengan Komitmen Organisasi Sebagai Variabel Intervening (Studi Kasus Pada PT. Indopangan Sensosa) (Issue 11170810000040).

Alfarizi, R., Satrio, A. J., Praseyto, Y. O., & Syahputra, M. F. (2024). ANALISIS PERKEMBANGAN TEKNOLOGI M-BCA DAN KEAMANAN SIBER DI BANK CENTRAL ASIA. Jurnal Akademik Ekonomi Dan Manajemen, 1(4), 43–53.

Ali, H., Candra Susanto, P., & Saputra, F. (2024). Faktor-Faktor Yang Mempengaruhi Manajemen Transportasi Udara: Teknologi Informasi, Infrastruktur dan Kompetensi Sumber Daya Manusia. Jurnal Siber Transportasi Dan Logistik, 1(4), 121–134. https://creativecommons.org/licenses/by/4.0/

Almadira, A., Pratama, Y., & Purwani, F. (2024). MELINDUNGI DATA DI DUNIA DIGITAL: PERAN STATEGIS ENKRIPSI DALAM KEAMANAN DATA. Journal of Scientech Research and Development, 6(2), 540–549.

Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022). Cyber security threats on digital banking. 2022 1st International Conference on AI in Cybersecurity (ICAIC), 1–4.

Azzahra, N. S., Tambunan, A. M., Aulia, N. N., Binarsih, A., & Saepudin, T. H. (2024). TINJAUAN LITERATUR TENTANG ANCAMAN CYBERCRIME DAN IMPLEMENTASI KEAMANAN SIBER DI INDUSTRI PERBANKAN. HUMANITIS: Jurnal Homaniora, Sosial Dan Bisnis, 2(7), 692–700.

Badruzaman, J. (2020). Analisis Efiensi Dan Kinerja Bank Syariah Di Indonesia. Jurnal Akuntansi, 15(1), 20–27.

Dewi, M. (2024). Metode Penelitian Research is Fun (A. Ambiyar (ed.); 1st ed.). CV. Muharika Rumah Ilmiah.

Diwanti, D. P., & Kandiyah, N. (2020). Pengaruh Capacity Building Terhadap Kinerja Karyawan Perbankan Syariah. Jurnal Bisnis, Manajemen, Dan Akuntansi, 7(1), 10–30.

Ernawati, T., & Rachmat, F. F. F. (2021). Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 5(1), 180–186.

Fadillah, D., Rahmayanti, D., & Syifa, I. F. (2020). Studi Literatur Manajemen dan Risiko Kepatuhan pada Bank Syariah. Jurnal Akuntansi Dan Manajemen, 17(1), 38–41.

Fibriany, F. W. (2019). Analisis Hubungan Pelatihan Terhadap Peningkatan Kinerja Karyawan Pada PT. Bank Bukopin, Tbk Jakarta. Cakrawala-Jurnal Humaniora, 19(1), 9–14.

Firdaus, S. E., Hidayah, S., & Putro, H. (2025). IMPLEMENTASI TEKNOLOGI UNTUK PENGUATAN KEAMANAN DATA PRIBADI NASABAH DALAM SEKTOR PERBANKAN. JURNAL ILMIAH NUSANTARA, 2(1), 1–11.

Haryaman, A., Amrita, N. D. A., & Redjeki, F. (2024). SECURE AND INCLUSIVE UTILIZATION OF SHARED DATA POTENTIAL WITH MULTI-KEY HOMOMORPHIC ENCRYPTION IN BANKING INDUSTRY. Journal of Economics, Accounting, Business, Management, Engineering and Society, 1(9), 1–13.

Hidayatulloh, N. W., Tahir, M., Amalia, H., Basyar, N. A., Prianggara, A. F., & Yasin, M. (2023). Mengenal Advance Encryption Standard (AES) sebagai Algoritma Kriptografi dalam Mengamankan Data. Digital Transformation Technology, 3(1), 1–10.

Hindarti, E., Hamdi, E., Indradewa, R., & Abadi, F. (2023). Operational Planning in E-Commerce Companies â€ œSimpel Omâ€ â€ œPT Simpel Om Unggulanâ€. Syntax Idea, 5(12), 2781–2798.

Husnaini, H., Dewi, A. A., Junita, D., Agustin, D., & Saputra, E. (2022). Pengelolaan Manajemen Risiko Kepatuhan Pada Bank Syariah. Jurnal Manajemen Bisnis Syariah, 2(2).

Jumawan, J., Saputra, F., & Prabowo, P. B. (2023). Determinasi Pelatihan Florist dan Kualitas Pelayanan Kewirausahaan Pada Kejutbypugo Kota Bekasi. OPTIMAL: Jurnal Ekonomi Dan Manajemen, 3(4), 216–227.

Keuangan, O. J. (2023). PERATURAN OTORITAS JASA KEUANGAN REPUBLIK INDONESIA NOMOR 21 TAHUN 2023 TENTANG LAYANAN DIGITAL OLEH BANK UMUM.

Khusna, K., Mirzania, A., Fauziyyah, S., & Muhsyi, A. (2022). ANALISIS KOMPETENSI HUMAN RESOURCE BUSINESS PARTNER DALAM MENCAPAI KESUKSESAN ORGANISASI PERGURUAN TINGGI. Jurnal of Business & Applied Management, XV(2), 125–132. https://doi.org/10.30813/jbam.v15i2.2691

Laili, I. N., Askandar, N. S., & Mahsuni, A. W. (2023). Pengaruh Pengendalian Internal dan Audit Internal Terhadap Pencegahan Kecurangan pada Bank BCA KCP Dinoyo Kota Malang. E_Jurnal Ilmiah Riset Akuntansi, 12(01), 514–524.

Luthfah, D. (2024). PENGUATAN KEAMANAN SIBER PADA SEKTOR JASA KEUANGAN INDONESIA. JURNAL PENELITIAN DAN KARYA ILMIAH LEMBAGA PENELITIAN UNIVERSITAS TRISAKTI, 259–267.

Mauliza, A. Y. I., Machmudi, R. D. S., & Indrarini, R. (2022). Pengaruh Perlindungan Data Dan Cyber Security Terhadap Tingkat Kepercayaan Menggunakan Fintech Masyarakat Di Surabaya. SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 1(11), 2497–2516.

Musyarofah, S. R., & Bisma, R. (2021). Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah. Teknologi: Jurnal Ilmiah Sistem Informasi, 11(1), 1–15. https://doi.org/10.26594/teknologi.v11i1.2152

Netmonk. (2023). Pentingnya Peran Server Monitoring dalam Menjaga Uptime Server. Netmonk.Id. https://netmonk.id/blog/peran-server-monitoring-dalam-menjaga-uptime-server

Nofrialdi, R., Saputra, E. B., & Saputra, F. (2023). Pengaruh Internet of Things: Analisis Efektivitas Kerja , Perilaku Individu dan Supply Chain. Jurnal Manajemen Dan Pemasaran Digital (JMPD), 1(1), 1–13. https://dinastires.org/JPKN/article/view/111/104

Pradana, J. A. (2021). Utility 1 server on queue service (Study: Bank account number conversion). AJIM (Airlangga Journal of Innovation Management), 2(2), 187–193.

Putra, F. A. W., & Suroso, J. S. (2024). Analysis of Benefit Considerations for Guarantee Company Upgrading to Tier 4 Colocation Data Center in Indonesia. Jurnal Indonesia Sosial Teknologi, 5(4), 1476–1484.

Razzanda, I. M., & Koprawi, M. (2024). Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding. The Indonesian Journal of Computer Science, 13(4).

Restika, R., & Sonita, E. (2023). TANTANGAN KEAMANAN SIBER DALAM MANAJEMEN LIKUIDITAS BANK SYARIAH: MENJAGA STABILITAS KEUANGAN DI ERA DIGITAL. Krigan: Journal of Management and Sharia Business, 1(2), 25–36.

Sebayang, S. (2020). Manajemen Kepatuhan Dan Meningkatkan Kesehatan Perbankan Syariah. Jurnal Kajian Ekonomi Dan Kebijakan Publik (JEpa), 5(2), 156–165.

Soleh, M., Yasin, Z., & Yusuf, H. (2022). Penerapan Kepatuhan Syariah dan Peraturan Jabatan Notaris pada Lembaga Keuangan Syariah di Indonesia:(Studi Kasus pada Perbankan Syariah di Kota Tangerang Selatan). Qonuni: Jurnal Hukum Dan Pengkajian Islam, 2(01), 15–24.

Susilo, A. (2023). REGULATORY TECHNOLOGY UNTUK DIGITALISASI PROSES KEPATUHAN (STUDI KASUS BANK SWASTA DI INDONESIA). INFOTECH Journal, 9(1), 252–258.

Walfajri, M. (2022). Begini Taksiran Kerugian BCA dan Mandiri Saat Layanan Mobile Banking Alami Kendala. Keuangan.Kontan.Co.Id. https://keuangan.kontan.co.id/news/begini-taksiran-kerugian-bca-dan-mandiri-saat-layanan-mobile-banking-alami-kendala?page=all

Wardhana, I., Dantes, G. R., & Aryanto, K. Y. E. (2020). Analysis of digital identity transactions with Ethereum blockchain ethereum in a case study of credit applications in banking. Journal of Physics: Conference Series, 1516(1), 12020.

Widjanarko, W., Hadita, H., Saputra, F., & Cahyanto, Y. A. D. (2023). Determinasi Kemudahan Akses Informasi Bagi Keputusan Investasi Gen Z. Digital Bisnis: Jurnal Publikasi Ilmu Manajemen Dan E-Commerce, 2(4), 248–264.

Yulaeli, T., Nugraheni, B., & Kuntadi, C. (2023). Analisis Pengaruh Hutang Jangka Panjang, Hutang Jangka Pendek dan Modal Kerja Bersih Terhadap Laba Pada PT. Griya Asri Prima. Journal of Economics and Business Academia, 1(1), 6–9.