Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google Scholar doi Crossref INDEX COPERNICUS ROAD ISJD OneSearch EBSCO OPEN ACCESS

DIGITAL FINANCIAL REPORTING: ANALYSIS OF THE QUALITY OF CYBER SECURITY VISUALIZATION VISUALIZATION AND DISCLOSURE IN INVESTOR RELATIONS OF GOVERNMENT BANKS

I Putu Indra ANDHIKA[1*], I Nyoman Satya Prawira JAYANTIKA[2], Anak Agung Bagus Surya Adi PUTRA[3], Gede Anantavijaya Satria PERKASA[4]

[1,2,3,4]Faculty of Economics and Business, Warmadewa University, Bali, Indonesia

Abstract:

This research analyses the financial report visualization and corporate cybersecurity risk management of four leading Indonesian state-owned banks: Bank Rakyat Indonesia (BRI), Bank Negara Indonesia (BNI), Bank Tabungan Negara (BTN), and Bank Mandiri, from 2022 to 2024. The research indicates that these four banks consistently demonstrate strong financial performance, characterized by solid growth in net profit, loans, and third-party funds. This growth is driven by aggressive digital transformation strategies and a focus on specific market segments, supported by maintained asset quality and a stable funding base. In terms of cybersecurity risk management, all banks show a strong commitment through the adoption of international frameworks (such as NIST and ISO 27001), the establishment of dedicated security units (CISO, CSIRT), and collaboration with the National Cyber and Crypto Agency (BSSN). Nevertheless, the level of transparency in public disclosure regarding cybersecurity policies and architecture details varies among the banks. Overall, these banks demonstrate robust financial health and an increasingly mature cybersecurity posture; however, there are opportunities to enhance financial report visualization and cybersecurity disclosure transparency, thereby strengthening investor confidence and operational resilience.

Keywords: Indicator, Financial Report Visualization, Cybersecurity, Risk Management, Investor Relations, State-Owned Banks

Article History:
Received: 2025-05-04
Revised: 2025-06-02
Accepted: 2025-07-15

Vol 2 Issue 3 2025
Corresponding Author*
(iputuindraandhika@gmail.com)

Page: 82-90

INTRODUCTION

In recent years, state-owned banks such as BNI, BRI, Mandiri, and BTN have entered a phase of massive digital transformation, which encompasses not only the digitization of banking services through mobile banking and super apps but also the presentation of financial reports digitally through their respective Investor Relations channels. This initiative incorporates the use of interactive visualization visualization, web-based dashboards, dynamic infographics, and financial reports in HTML and digital flipbook formats, which can be accessed globally by stakeholders. The primary objectives of this transformation are to enhance transparency, increase information accessibility, and foster investor engagement through the delivery of information that is not only factual but also visually appealing and easy to understand (Susanto, 2020). However, behind this progress, there are major challenges that threaten the sustainability of digitalization, namely the increasing threat of cybersecurity.

This challenge became even more apparent when the CISSReC report in June 2022 showed that the cybersecurity scores of large state-owned banks were still relatively low, with BNI and BTN each scoring only 64, while Mandiri was even lower at 54, placing them in the red zone of vulnerability. This assessment is based on indicators such as endpoint resilience, domain reputation, DNS performance, and the completeness of threat detection systems, all of which are crucial in anticipating attacks, including phishing, ransomware, DDoS, and data leaks (Rahmawati & Prasetyo, 2021).

This vulnerability is proven relevant, considering that from the end of 2021 to mid-2024, various cyber incidents have had a real impact on the national banking sector, such as the ransomware attack on Bank Syariah Indonesia (BSI) in May 2023 which paralyzed digital services and ATMs for several days (Yulianto, 2023), as well as the alleged data leak and cyberattack on BRI in December 2024, which

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

although officially denied, triggered uncertainty and concern for the public and investors (Hartono, 2024). Each bank showed a variety of responses to this issue.

Since 2021, Bank Mandiri has implemented a DevSecOps approach that integrates security into the digital technology development cycle, utilizing a multi-layered firewall strategy, intrusion detection systems, and the Zero Trust Architecture principle, which is regularly audited (Santoso, 2022). Meanwhile, BNI has adopted an infrastructure-strengthening approach by implementing international security standards, such as ISO 27001 and the NIST framework, and launched the super-app "Wondr by BNI" in July 2024, backed by a substantial investment of USD 100 million to build a robust and secure digital banking ecosystem (Sari & Nugroho, 2024). BTN and BRI are not left behind, with both significantly increasing their technology capital expenditure (IT Capex) since early 2024 and forming a Computer Security Incident Response Team (CSIRT) that has been certified by BSSN, equipped with a Security Operation Center (SOC) that operates 24 hours (Kusuma, 2024).

However, critical issues arise in the aspect of transparency or disclosure, where information regarding cyber incidents is still very minimal and normative, not explaining the impact, scale, or mitigation efforts carried out openly to the public and investors. This is partly due to the narrow interpretation of SEOJK No. 29/SEOJK.03/2022, which encourages banks to be cautious or even conceal details of cyber incidents in order to maintain their reputation, ultimately obscuring investor confidence in the bank's cyber readiness (Wahyudi, 2023).

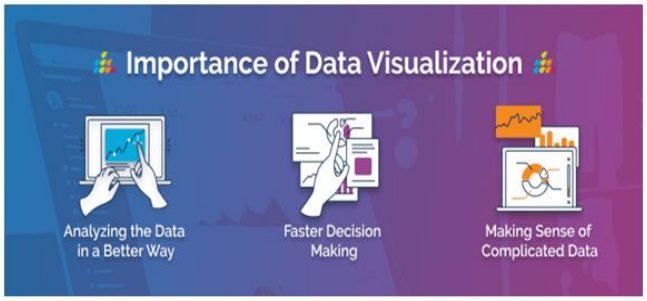
In this context, financial report visualization becomes increasingly strategic, as it serves not only as a means of conveying financial information but also reflects a commitment to digital risk governance (Putri & Hidayat, 2019). Unfortunately, the quality of this visualization visualization remains varied. BNI, for example, presents reports in an attractive, interactive flipbook format and is equipped with visual icons and infographics; however, it has not provided a real-time dashboard or explicitly displayed cybersecurity metrics. BRI relies on an integrated investor portal that provides access to quarterly and sustainability reports, utilizing a slide-based visual storytelling approach. However, it still does not present a history of incidents or cybersecurity indicators in a graphical format. Bank Mandiri is more advanced, presenting information in the form of interactive tables and spider diagram visualizations visualizations for ESG aspects. However, it still lacks historical graphs and quantitative data on cybersecurity readiness. Meanwhile, BTN tends to be the most conventional, with reports in static PDF format that contain basic financial ratio graphs but lack a description of the digitalization roadmap or comprehensive visualization of the cyber strategy (Hadi & Lestari, 2023).

This difference in approach highlights the lack of standards or best practices for digital report visualization visualization that integrates cybersecurity risk transparency. Amidst the complexity of digital threats, investors require clear and reliable visual information (Firdaus & Anwar, 2021). Therefore, this study is very important because it combines two crucial main dimensions: (1) evaluation of the quality of digital financial report visualization in investor relations channels as a strategic communication instrument and (2) assessment of the openness of cybersecurity disclosure as a representation of governance responsibility and risk mitigation. By understanding how BNI, BRI, Mandiri, and BTN display financial data and convey their cyber readiness digitally, this study aims to evaluate the effectiveness of digital information delivery, identify gaps in transparency, and develop practical recommendations so that digital financial reports not only function as a formal tool for fulfilling regulations, but also become a strategic medium for building investor trust, demonstrating digital accountability, and strengthening the resilience of public financial institutions in the era of increasingly complex and aggressive cyber threats (Rahman, 2022). It is hoped that the results of this study can encourage the birth of more informative, credible, and adaptive risk-based digital reporting standards, as well as become a reference for other banks in developing digital communication strategies that align financial performance and cybersecurity governance in a visual, structured, and convincing manner (Yusuf & Amalia, 2023).

Visualization Quality. Data visualization visualization is a crucial tool for simplifying complex financial information, making it easier for investors to understand (Uddin et al., 2024). According to

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google Crossref ROAD ISJD EBSCO OPEN ACCESS

Eberhard (2023), visualization visualization is a visual representation of information or ideas designed to communicate messages effectively and enhance understanding. With diagrams, graphs, and infographics, raw data is transformed into an attractive and easy-to-understand format (Perkhofer et al., 2019). This technique enables companies, including state-owned banks, to present complex financial data through interactive dashboards and graphs, facilitating users' ability to digest information and identify patterns, trends, and anomalies that may be overlooked in traditional reports (Shao et al., 2022). This capability is far superior to traditional reporting, which is less dynamic and interactive (Trigo et al., 2014).



Source: Kalluri (2020)

Figure 1. Importance of Data Visualization

Interactivity in data visualization is also crucial for enhancing user engagement, allowing investors to explore information in depth and gain a more comprehensive understanding of a company's financial condition. A study by Brown et al. (2021) showed that graphs have a significant impact on the investment decisions of non-professional investors, who are more interested in visual information, such as stock price changes in graphs, than in text-based reports. In investor relations, the visual presentation of data is crucial for facilitating the understanding of complex financial information that can often be confusing (Perdana et al., 2018). Transforming complex data into visual forms, such as line graphs and bar charts, makes it easier to interpret and digest, helping investors make better and more informed investment decisions (Chy & Buadi, 2023).

Cyber Security Disclosure. Cybersecurity can be defined as the protection of information and systems, networks, devices, programs, or electronic data from the threat of theft or damage. Awareness of protecting digital assets is crucial for companies, as cyber-attacks can significantly impact organizational organizational performance (Sari et al., 2024). Research by Alhassan et al. (2019) indicates that companies that implement effective cybersecurity practices not only protect important data but also increase the transparency of information provided to the public. Success in this aspect is highly dependent on clear and easy-to-understand delivery, which in turn can reduce internal audit costs. This indicates a correlation between effective cybersecurity practices and the level of accountability in financial reports.

In the banking sector, digital security threats frequently arise, particularly in the form of email fraud, malware, and data leaks. Email fraud is an action that attempts to deceive or deceive individuals by capturing their attention (Wibowo & Fatimah, 2017). Banking malware attacks have become increasingly frequent in recent years, posing significant risks to financial institutions and their clients. The consequences of these attacks can include the theft of important data, economic losses, and damage to the organization's organization's image (Fitria, 2023). Information leaks occur when sensitive data from clients or banks is exposed, either due to direct hacking or errors that occur within the organization organization. The primary goal of cybercrime is to generate illicit profits, particularly in the financial sector. Therefore, strengthening network security in the financial services sector is a top priority due to the increasing number of cyberattacks in this area (Azzahra et al., 2024).

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

In the banking sector, digital security threats frequently emerge, particularly in the form of email fraud, malware, and data breaches. Email fraud is an action that attempts to tempt or trap individuals by attracting their attention (Wibowo & Fatimah, 2017). Banking malware attacks have become increasingly frequent in recent years, posing significant risks to financial institutions and their clients. The consequences of these attacks can include the theft of sensitive data, economic losses, and damage to the organization's reputation (Fitria, 2023). Information leaks occur when sensitive data from clients or banks is exposed, either due to direct hacking or errors that occur within the organization organization. The primary objective of cybercrime is to generate illicit profits, particularly in the financial sector. Therefore, strengthening network security in the financial services sector is a top priority due to the increasing number of cyberattacks in this area (Azzahra et al., 2024).

Investor Relations. The National Investor Relations Institute (NIRI) defines investor relations as a strategic management responsibility that brings together financial, communication, marketing, and securities law compliance aspects. The goal is to establish the most efficient communication channels between the company, the financial community, and other stakeholders, which ultimately facilitates a fair assessment of the company's securities (Kurnia, 2021).

According to (Hanathasia, 2013), investor relations acts as a bridge between the company and sources of information for shareholders, analysts, and financial journalists (who are the main public in investor relations) and other relevant publics (especially among the financial community such as brokers and rating agencies, and so on). In Indonesia, the role of investor relations in companies listed on the stock exchange is regulated by the provisions of Bapepam (Kretarto, 2001). Therefore, the existence of this function is a must to support the principle of information transparency.

Investor relations are recognized as a crucial element for public companies, with an emphasis on ensuring that capital market participants receive relevant and accurate information and policies from the company. All activities in investor relations that are carried out effectively can help companies increase visibility in the capital market, enhance their public image, expand their analyst reach, and attract investor attention (Anita, 2017).

Government General Bank. A bank is a financial institution that functions as an intermediary, typically established with a license to accept deposits, provide loans, and issue promissory notes, commonly referred to as banknotes (Munajim & Anwar, 2016). The objectives of the banking system, as outlined in Article 3 of Law No. 10 of 1998, are to support national development by emphasizing equity, economic growth, and national stability, all of which aim to enhance the overall welfare of society.

According to Atahuu (2014), the financial performance of Government Commercial Banks shows less than satisfactory results, which can be seen from low efficiency, a high ratio of non-performing loans (NPL), and misallocation of credit. In the banking sector, a bank's competitiveness is not only determined by the amount of capital it has but also by several influential factors (Haryanto, 2012). A large banking company with significant capital does not necessarily guarantee better efficiency, as there are still many aspects that influence the level of efficiency, such as workforce or stakeholder factors (Ersangga & Atahau, 2019).

METHODS

This study employs a qualitative descriptive method, as its primary objective is to describe and comprehensively examine how state-owned banks present financial report visualizations and communicate cybersecurity risk management strategies to investors. This approach is appropriate because it allows for in-depth exploration of the observed phenomena without requiring specific hypothesis testing or searching for correlations between variables.

State-owned public banks that have gone public and have online investor relations platforms are the main focus of this study. The analysis focuses on two key dimensions: the effectiveness of the visualization of financial data presented and the transparency of the disclosure of company policies and strategies in addressing cybersecurity threats.

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

All information analyzed is sourced from published materials available on each bank's investor relations portal, including annual reports in digital format, disclosure documents related to risk management, and various other publicly accessible financial presentations and publications. The information-gathering process involves systematically exploring the company's official website, documenting various forms of visualization found, downloading relevant documents, and conducting structured observations of the visual components and substance of the published content.

The data analysis phase uses a content analysis approach that begins by identifying various visualization elements and cybersecurity-related materials available, then grouping them based on characteristics and types of information, describing the quality and clarity of data presentation, evaluating how effectively the information is communicated to stakeholders, and finally interpreting all findings within the framework of accountability and public information transparency. Data validity is maintained through the use of multiple sources of information from the same platform, cross-verification with primary sources, and detailed documentation of the entire research process.

RESULT AND DISCUSSION

Bank Rakyat Indonesia (BRI). Based on the results of research related to the analysis on the website of PT. Bank Rakyat Indonesia (Persero) Tbk. - Investor Relations: The accessibility of BRI's financial reports through the investor relations website is very good. The "Reports & Disclosure" section presents "Financial Reports". Annual and quarterly financial reports are available for download in Indonesian and English, including complete reports for 2022, 2023, and 2024. This ease of access increases transparency for investors.

BRI shows a strong commitment to cybersecurity management. The bank has a special work unit under the Director of Information Technology & Digital Operations that handles information security. This unit is responsible for Security Architecture Design, Operational Security, Cyber Risk and Cyber Intelligence, Data Loss and Fraud Prevention, Identity and Access Management, Program Management, Investigation and Forensics, and Security Governance. The results of the analysis related to cybersecurity at BRI are shown in the following table:

Table 1. Analysis related to cybersecurity at BRI

Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Cyber Security Framework	Based on the NIST Cyber Security Framework.	Cyber Security Framework
Special Security Unit	Special working unit under the Director of Information Technology & Digital Operations; Information Security Division.	Special Security Unit
Security Unit Responsibilities	Security Architecture Design, Operational Security, Cyber Risk and Cyber Intelligence, Data Loss and Fraud Prevention, Identity and Access Management, Program Management, Investigation and Forensics, and Security Governance.	Security Unit Responsibilities
Main Policy	Data Governance Framework, Data Privacy Policy, Information Security Policy, Customer Due Diligence Procedures, Data Development Life Cycle (DDLC) Procedures & Data Sharing.	Main Policy
Incident Response Mechanism	BRI CSIRT Cybersecurity Incident Response Framework (SE.38-DIR/ISC/06/2021)	Incident Response Mechanism
Awareness Program	Increased employee awareness, commitment to protecting customer privacy	Awareness Program
External Certification/Ratings	Most Trusted Company (CGPI 95.21, 2023), Low Risk (Sustainalytics ESG 18.8, Oct 2022)	External Certification/Ratings

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Cyber Security Framework	Based on the NIST Cyber Security Framework.	Cyber Security Framework

Bank Negara Indonesia (BNI). The analysis focuses on examining the bni.co.id website, where the Investor Relations section provides "Financial Reports" categorized as Annual, Quarterly, Monthly, and Others. The Annual Reports for 2022, 2023, and 2024 are explicitly listed on their financial report page. Quarterly reports for Q1-Q4 2022, 2023, and 2024 are also available.

BNI lists a "Risk Management Policy" under the "Governance Related Policies" section. The bank also has a "Data Protection and Privacy Policy" that outlines what personal data is collected and how it is used, shared, and protected, including measures such as identity verification, encryption, and access control. The results of the analysis related to cybersecurity can be seen in the following table:

Table 2. Analysis related to cybersecurity

Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Main Policy	Risk Management Policy, Data Protection and Privacy Policy	Main Policy
Security Steps	Verifikasi identitas, enkripsi, kontrol akses	Security Steps
Customer Protection Program	Microsite Digital Platform Customer Protection, Data Security Tips	Customer Protection Program
Security Awareness	“Security Awareness” Category in BNI News	Security Awareness
External Security Rating	Rated by Security Scorecard (Financial Services industry, 2.4K IPs, 28.4K employees)	External Security Rating
Limitations of Public Disclosure	Details of the specific cyber framework, CSIRT team, or comprehensive incident report are not explicitly available in the information snippet.	Limitations of Public Disclosure
Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Main Policy	Risk Management Policy, Data Protection and Privacy Policy	Main Policy
Security Steps	Verifikasi identitas, enkripsi, kontrol akses	Security Steps

Bank Tabungan Negara (BTN). Analysis conducted on the btn.co.id site reveals that BTN's investor relations website offers a "Company Report" section with direct download links for the 2022, 2023, and 2024 Annual Reports. This shows high transparency and ease of access for investors.

BTN has an IT Security Division under the IT Directorate, which is actively supervised by the Information Technology Steering Committee (KPTI) of the Board of Directors. The bank also has a Digital and Operational Risk Management Unit that independently monitors information security risks. The results of the analysis related to BTN's cybersecurity can be seen in the following table:

Table 3. BTN cybersecurity-related analysis

Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Special Security Unit	IT Security Division under IT Directorate, Digital and Operational Risk Management Unit	Special Security Unit
Supervision	Information Technology Steering Committee (KPTI) of the Board of Directors	Supervision
Main Policy	IT Procedure Policy No. K.K. 5-A, IT Security Policy No. K.K. 5-B, Data Governance Policy No. K.K. 9-M, Logical Access	Main Policy

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

	Control System Governance Policy No. K.K. 9-Q, Digital & Cyber IT Risk Management Policy No. K.K. 8-E	
Incident Response Team	Computer Security Incident Response Team (CSIRT) collaborates with BSSN and Komdigi.	Incident Response Team
Incident Response Phase	Preparation, Detection and Analysis, Handling, Eradication & Recovery	Incident Response Phase
Proactive Program	Ongoing cyber training, simulations, employee certification, Customer Cybersecurity Awareness Program	Proactive Program
External Certification	ISO 27001:2022 for Information Security Management Systems (ISMS)	External Certification
Security Approach	The "defence-in-depth" principle with advanced security tools at multiple layers	Security Approach
Audit	Annual internal and external audits	Audit

Bank Mandiri. Analysis results on the Bank Mandiri.co.id website indicate that the bank's investor relations website offers the following reports: "Annual Report & Sustainability Report", "Audited Financial Report", "Quarterly Financial Report", and "Monthly Financial Report". The Annual Reports for 2022, 2023, and 2024 are available in English and Indonesian. Quarterly reports for Q1 and Q2 2024 are also available.

Bank Mandiri has an Enterprise Data Analytics (EDA) Division with over 140 data scientists and analysts, as well as a CISO Division with 87 employees dedicated to managing cybersecurity threats. Their Investor Relations Division is responsible for managing communication and providing transparent information to help investors, including updates on the company's performance and key issues.

Table 4. Cyber Security Aspects and Governance Initiatives in the Banking Sector

Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Special Security/Data Unit	Enterprise Data Analytics (EDA) Division (140+ data scientists/analysts), CISO Division (87 employees)	Special Security/Data Unit
Regulatory Compliance	POJK No. 11/POJK.03/2022 concerning the Implementation of IT by Commercial Banks (POJK PTI)	Regulatory Compliance
Incident Response Team	Computer Security Incident Response Team (CSIRT) registered with BSSN	Incident Response Team
GRC & Sustainability Integration	Commitment to linking governance, risk, sustainability and financial reporting	GRC & Sustainability Integration
Recorded Cyber Incidents	Alleged cyberattack on Bank Mandiri Pension Fund (dapenbankmandiri.co.id) in March 2025	Recorded Cyber Incidents
Policy	Regular risk assessments, clear security policies, and integration of cybersecurity into business processes	Policy
Cyber Security Aspects	Initiative/Governance Details	Cyber Security Aspects
Special Security/Data Unit	Enterprise Data Analytics (EDA) Division (140+ data scientists/analysts), CISO Division (87 employees)	Special Security/Data Unit
Regulatory Compliance	POJK No. 11/POJK.03/2022 concerning the Implementation of IT by Commercial Banks (POJK PTI)	Regulatory Compliance

All four banks provide comprehensive financial reports (annual, quarterly, monthly) on their investor relations websites, often in multiple languages. This demonstrates a strong commitment to regulatory compliance and investor transparency.

However, the term "financial report visualization visualization" implies more than just a downloadable PDF. It suggests opportunities for interactive dashboards, trend analysis, and graphical

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

representations directly on the investor relations website, which are not explicitly detailed in the information pieces. While the fundamental data is accessible, enhancing the visualization aspect of financial reports could further enhance investor engagement and understanding, moving beyond mere compliance to best-in-class digital investor relations.

CONCLUSION

Overall, the analysis for the period 2022-2024 shows that the four Indonesian state-owned banks, Bank Rakyat Indonesia (BRI), Bank Negara Indonesia (BNI), Bank Tabungan Negara (BTN), and Bank Mandiri, have demonstrated solid financial performance and continue to grow. An aggressive digital transformation strategy, combined with a focus on specific market segments, including MSMEs by BRI, global corporate banking by BNI, KPR by BTN, and an ecosystem approach by Bank Mandiri, drives this growth. Although their growth strategies vary, all banks maintain a stable asset quality, with a low non-performing loan (NPL) ratio and high NPL coverage, as well as a stable funding base.

In terms of cybersecurity risk management, there is a strong commitment across banks, marked by the adoption of international frameworks such as NIST and ISO 27001, the establishment of a dedicated security division, and a cyber incident response team (CSIRT) that collaborates with the National Cyber and Crypto Agency (BSSN). However, the level of transparency in public disclosure regarding the details of cybersecurity policies and architecture varies, with BTN and Bank Mandiri tending to provide more detailed information than BNI. While all banks have met financial reporting standards by providing comprehensive reports on their investor relations websites, there remains an opportunity to enhance the visualization of financial reports through interactive dashboards, thereby improving investor understanding and engagement.

REFERENCES

Akhta, S., Sheorey, P. A., Bhattacharya, S., & Ajith, K. V. V. (2021). Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research, 12*(1), 82–97. https://doi.org/10.4018/IJBIR.20210101.oa5

Alhassan, I., Sammon, D., & Daly, M. (2019). Critical Success Factors for Data Governance: A Theory Building Approach. *Information Systems Management, 36*(2), 98–110. https://doi.org/10.1080/10580530.2019.1589670

Anita, A. V. (2017). Studi Eksploratif Aktivitas Investor Relations Sebagai Salah Satu Bidang Public Relations (Unit Investor Relations Pt. Bank Negara Indonesia (Persero) Tbk). Universitas Brawijaya.

Atahau, A. D. R. (2014). Loan portfolio structures, risk and performance of different bank ownership types: An Indonesian case. Curtin University.

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 Humaniora, Sosial Dan Bisnis, 2*(7), 692–700.

BNI. (2025). Investors - BNI. https://www.bni.co.id/id-id/investor

BRI. (2025). PT. Bank Rakyat Indonesia (Persero) Tbk. - Investor Relation. https://www.ir-bri.com/

Brown, N. C., Elliott, W. B., & Grant, S. M. (2021). How Do Non-GAAP Image Tweets Influence Investor Judgments? SSRN Electronic Journal, April.

BTN. (2025). BTN Investor Relations: Transparency and Trust | PT Bank Tabungan Negara (Persero) Tbk. https://www.btn.co.id/en/About/Investor-Relation/Investor-Relation

Chy, Md. K. H., & Buadi, O. N. (2023). Role of Data Visualization in Finance. *American Journal of Industrial and Business Management, 13*(08), 841–856. https://doi.org/10.4236/ajibm.2023.138047

Eberhard, K. (2023). The Effects of Visualization on Judgment and Decision-Making: A Systematic Literature Review. In Management Review Quarterly (Vol. 73, Issue 1). Springer International Publishing. https://doi.org/10.1007/s11301-021-00235-8

Maharati INSTITUTE
JSSCS Journal of Social Sciences and Cultural Studies
P-ISSN : 3031-0083 (PRINT)
E-ISSN : 3032-0631 (ONLINE)
Journal of Social Sciences and Cultural Studies
BASWASTI PT. BATARA SWASTIKA HARATI
Indexed By : GARUDA Google ROAD ISJD EBSCO OPEN ACCESS

Ersangga, D., & Atahau, A. D. R. (2019). Perbandingan Efisiensi Bank Umum Pemerintah Dan Bank Umum Swasta Dengan Pendekatan Data Envelopment Analysis. *Modus, 31*(1), 72–88.

Fitria, K. M. (2023). Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan. *Jurnal Informatika Dan Teknik Elektro Terapan, 11*(3). https://doi.org/10.23960/jitet.v11i3.3312

Hanathasia, M. (2013). The Application of Pr Communication Model in Investor Relations Through Web 2.0. *Journal Communication Spectrum, Vol. 2 No. 2, 2*(2), 186–199.

Haryanto, S. (2012). Kinerja dan efisiensi bank pemerintah (BUMN) dan BUSN yang go publik di Indonesia. *Jurnal Ekonomi Modernisasi, 8*(2), 165–179.

Kretarto, A. (2001). Investor relations: pemasaran dan komunikasi keuangan perusahaan berbasi kepatuhan. Grafiti Pres.

Kurnia, G. dan. (2021). Komunikasi Korporat (Teori dan Praktis). In Widina Bhakti Persada Bandung (Vol. 1, Issue September).

Mandiri. (2025). Investor Relations - IR. https://www.bankmandiri.co.id/web/ir

Munajim, A., & Anwar, S. (2016). Faktor yang mempengaruhi keputusan menjadi nasabah bank syariah. *Ilmiah Indonesia, 1*(2), 41–52.

Nst, P. S. S. Br., Lubis, F. K., Wulandari, K. F., & Simanjuntak, N. A. (2025). Peran Keamanan Siber Dalam Meningkatkan Transparansi Dan Akuntabilitas Terhadap Laporan Keuangan di Bank Syariah Indonesia. Jurnal Bisnis Net Volume: 8 No. 1 Juni, 2025 | ISSN: 2621 -3982 EISSN: 2722- 3574, 1, 496–505.

Perdana, A., Robb, A., & Rohde, F. (2018). Does visualization visualization matter? The role of interactive data visualization visualization to make sense of information. *Australasian Journal of Information Systems, 22.* https://doi.org/10.3127/ajis.v22i0.1681

Perkhofer, L. M., Hofer, P., Walchshofer, C., Plank, T., & Jetter, H. C. (2019). Interactive visualization visualization of big data in the field of accounting: A survey of current practice and potential barriers for adoption. *Journal of Applied Accounting Research, 20*(4), 497–525. https://doi.org/10.1108/JAAR-10-2017-0114

Sancaya, I. W. W., Saputra, K. A. K., & Sutama, N. (2025). Bullying Prevention Program in Elementary School, Peguyangan Kaja Village, Denpasar. *Community Services: Sustainability Development, 2*(2), 202-209.

Saputra, K. A. K., Darmawan, N. A. S., & Laksmi, P. A. S. (2024). Kajian Etnografi Kinerja Berkelanjutan.

Saputra, K. A. K., & Jayawarsa, A. K. (2025). Revealing The Hegemony of Selective Perception in Managing Ecotourism Based on Natural Environmental Preservation. *Journal of Sustainability Science and Management, 20*(6), 1138-1157.

Sari, L., Adam, M., Fuadah, L. L., & Yusnaini. (2024). Determinant Factors of Cyber Security Disclosure: A Systematic Literature Review. KnE Social Sciences, May. https://doi.org/10.18502/kss.v9i14.16113

Shao, C., Yang, Y., Juneja, S., & GSeetharam, T. (2022). IoT data visualization visualization for business intelligence in corporate finance. *Information Processing & Management, 59*(1), 102736.

Trigo, A., Belfo, F., & Estébanez, R. P. (2014). Accounting Information Systems: The Challenge of the Real-time Reporting. *Procedia Technology, 16,* 118–127. https://doi.org/10.1016/j.protcy.2014.10.075

Uddin, M. M., Ullah, R., & Moniruzzaman, M. (2024). Data Visualization Visualization in Annual Reports-Impacting Investment Decisions. *International Journal for Multidisciplinary Research (IJFMR), 6*(5), 1–16.

Verma, S., Sharma, J., Kaushik, K., & Vyas, V. (2022). Mounting cases of cyber-attacks and digital payment. Cybersecurity Issues, Challenges, and Solutions in the Business World, June, 59–80. https://doi.org/10.4018/978-1-6684-5827-3.ch005

Wibowo, M. H., & Fatimah, N. (2017). Ancaman Phishing Terhadap Pengguna Sosial Media Dalam Dunia Cyber Crime. *JoEICT (Journal of Education And ICT), 1*(1), 1–5.