JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i4

Legal Protection for Investors' Personal Data Against Cybercrime Threats in Capital Market Based on IOSCO Principles

Kevin Darmawan[1], Aninditha Sekar Putri[2].
[1]Law Study Program, Faculty of Law, Universitas Padjadjaran, kevindarmawan50@gmail.com.
[2]Law Study Program, Faculty of Law, Universitas Indonesia, anindithasekarputri@gmail.com.

Corresponding Author: kevindarmawan50@gmail.com[1]

Abstract: The increasing threat of cybercrime, particularly in the capital market sector, poses a serious risk to investors' personal data protection in Indonesia. This challenge requires a robust and adaptive regulatory approach to maintain trust and security within the capital market. As a member of IOSCO, Indonesia has access to principles designed to protect investors and minimize cyber risks. This study employs a normative juridical method using secondary data in the form of primary and secondary legal materials to examine the effectiveness of IOSCO principles in national law. The study's findings indicate that IOSCO applies 38 principles forming a policy framework for investor protection through preventive and educational efforts for its member countries. However, although Indonesia's positive law has established a framework for personal data protection, certain aspects of IOSCO principles remain unaccommodated, particularly in terms of oversight and cyber risk management. Therefore, the establishment of a Personal Data Protection Supervisory Body in Indonesia is essential to enhance investor protection and ensure functional harmonization alongside the Indonesia Financial Services Authority.

Keyword: Cybercrime, IOSCO Principles, Personal Data Protection.

INTRODUCTION

The capital market plays a crucial role in the economy of every country by bridging investors with surplus funds and issuers in need of funding (Erman R. and Rosa A. 2010). Investors place their funds in the capital market to gain profits, but investments do not always perform as expected, necessitating legal protection for investors. In Indonesia, investor protection in the capital market is regulated through Law Number 8 of 1995 on the Capital Market ("Capital Market Law"). Prior to the enactment of this regulation, an international organization called the International Organization of Securities Commissions ("IOSCO") was established in 1983 as a global capital market regulator. To this day, IOSCO operates to ensure the continuity of global capital markets, particularly for member countries. Headquartered in Madrid, Spain. the organization has issued the IOSCO Objectives and Principles of Securities Regulation, which aims to protect investors, ensure fair, efficient, and transparent capital markets, and mitigate systemic risks (Dyah Ayu Purboningtyas and Adya Prabandari).

Indonesia has been a member of IOSCO since 1984 through the Ministry of Finance, which oversaw the Capital Market Supervisory Agency ("Bapepam"). After the establishment of the Capital Market Law and the Financial Services Authority ("OJK"), OJK officially represented Indonesia as an IOSCO member in 2014, replacing Bapepam (OJK, 2016). With the advent of technology and the digital era, personal data breaches have become increasingly detrimental to investors. The threat of cybercrime, which involves computer media and technology, has risen significantly. Cybercrime refers to crimes utilizing computers, computer networks, and/or technology to steal or damage data, disrupt systems, and potentially harm the capital market (Abi Tyas Tunggal, 2019). One of the most serious threats is the leakage of investors' personal data by hackers, which includes sensitive information such as names, email addresses, phone numbers, and other data that may be used for personal gain or sold on dark web forums. Article 1 Number 1 of Law Number 27 of 2022 on Personal Data Protection ("PDP Law") defines personal data as "data about an individual who is identified or can be identified either independently or in combination with other information, directly or indirectly, through electronic or non-electronic systems."

IOSCO has acknowledged the threat of cybercrime to personal data. This is evidenced by IOSCO's issuance of a policy aimed at protecting the personal data of its member countries: Personal Data Protection Policy and Assignment of Image Rights for Participants in Events and Meetings Organized by IOSCO (the “Event”). This policy aims to safeguard member countries' personal data from cybercrime, though it allows the data to be shared with third parties under specific conditions. In light of the cybercrime threats to investors in Indonesia and IOSCO principles, this research is titled: “Legal Protection for Investors’ Personal Data Against Cybercrime Threats in Capital Market Based on IOSCO Principles". The study aims to examine IOSCO's role and principles in protecting investors from cyber threats in the capital market and to identify aspects of IOSCO principles that have not yet been accommodated in Indonesia's positive laws. The research questions addressed are: (1) How do IOSCO's role and principles provide protection to investors in member countries from cyber threats in the capital market? (2) What aspects of IOSCO principles are not yet accommodated in Indonesia's positive laws? This study will discuss the urgency of IOSCO's role in achieving its objectives and its implementation in line with the prevailing laws and regulations in Indonesia.

METHOD

This study employs using a normative juridical research method, which involves drawing on secondary data, including primary and secondary legal materials (Nanda Dwi Rizkia, 2021). The data employed in this research consists of secondary data, including primary and secondary legal materials. Primary legal materials refer to authoritative legal sources that have binding power over society. In this study, the primary legal materials include international agreements, which are highly relevant for examining the applicable regulations related to the research subject. Additionally, secondary legal materials are used, which provide explanations and context regarding the primary legal materials (Soerjono Soekanto, 2019).

RESULTS AND DISCUSSION

The Role of IOSCO Institutions and Principles in Providing Protection for Investors in Member Countries from Cyber Threats in the Capital Market

Provisions of IOSCO Principles in Providing Protection for Investors

To enhance the effectiveness of the capital market, IOSCO continually strives to fulfill its objectives, particularly in providing protection to investors engaging in capital market activities. One of the key steps taken is the formulation of policies aimed at creating an effective and efficient capital market. These policies are designed for IOSCO members to promote enforcement and the exchange of information. Although not legally binding, IOSCO principles

provide moral and professional commitments for capital market authorities and industry players to maintain the integrity and stability of the capital market (Bambang Poernomo, 2022).

In Indonesia, IOSCO principles have been adopted and implemented through various national regulations, such Law Number 1 of 2024 on the Second Amendment to the Law Number 11 of 2008 on Electronic Information and Transactions ("EIT Law"), the Personal Data Protection Law (PDP Law), and Law Number 4 of 2023 on the Development and Strengthening of the Financial Sector. However, certain aspects, such as international coordination in handling cyber threats, effective law enforcement, and stringent oversight and audits of capital market entities, have yet to be fully addressed as outlined in the IOSCO Principles.

IOSCO has issued several principles to guide industry players in the capital market in conducting their activities. These principles consist of 38 standards within capital market policies, built around three core objectives: 1) Protecting investors. 2) Ensuring fair, efficient, and transparent capital markets. 3) Reducing systemic risk (International Organization of Securities Commissions, 2017).

As an international standard, IOSCO principles serve as valuable guidance in formulating national regulations and ensuring that capital markets operate with high transparency and integrity. In Indonesia, the Financial Services Authority (OJK) uses these principles as a reference in developing capital market policies and regulations. The successful implementation of these 38 principles under the relevant legal framework is essential for achieving the objectives of these policies. The principles are categorized into 10 sections, including (International Organization of Securities Commissions, 2017):

a. Principles Relating to the Regulators

1. The responsibilities of the regulator must be clearly stated and objectively defined.
2. The regulator must be operationally independent and accountable in exercising its functions and authority.
3. The regulator must have adequate authority, resources, and capacity to perform its functions and exercise its powers.
4. The regulator must adopt clear and consistent regulatory processes.
5. The regulator's staff must adhere to the highest professional standards, including appropriate confidentiality standards.
6. The regulator must have or contribute to processes for identifying, monitoring, mitigating, and managing systemic risks, in accordance with its mandate.
7. The regulator must have or contribute to processes for regularly reviewing regulatory boundaries.
8. The regulator must ensure that conflicts of interest and misalignment of incentives are avoided, eliminated, disclosed, or managed.

b. Principles for Self-Regulation

If the regulatory system uses Self-Regulatory Organizations (SROs) that carry out some direct supervisory responsibilities within their respective areas of competence, such SROs must be subject to regulatory oversight and must adhere to fairness and confidentiality standards when exercising the delegated powers and responsibilities.

c. Principles for the Enforcement of Capital Market Regulation

1. Regulators must have comprehensive inspection, investigation, and oversight authority.
2. Regulators must have comprehensive enforcement powers.
3. The regulatory system must ensure the effective and credible use of inspection, investigation, oversight, and enforcement powers, as well as the implementation of an effective compliance program.

d. Principles for Information Transparency

1. Regulators must have the authority to share both public and non-public information with domestic and foreign counterparts.

2. Regulators must establish information-sharing mechanisms that govern when and how they will share both public and non-public information with their domestic and foreign partners.
3. The regulatory system must facilitate assistance to foreign regulators who need to inquire while performing their functions and exercising their powers.

e. Principles for Issuers

1. There must be full, accurate, and timely disclosure of financial results, risks, and other material information relevant to investor decision-making.
2. Security holders within a company should be treated fairly and equitably.
3. The accounting standards used by issuers to prepare financial statements should be of high quality and internationally accepted.

f. Principles for Auditors, Credit Rating Agencies, and Other Information Service Providers

1. Auditors must be subject to adequate levels of supervision.
2. Auditors must be independent from the entities they audit.
3. Auditing standards should be of high quality and internationally accepted.
4. Credit rating agencies must be subject to adequate levels of supervision. The regulatory system must ensure that credit rating agencies, whose ratings are used for regulatory purposes, are subject to registration and ongoing oversight.
5. Other entities offering analytical or evaluative services to investors must be subject to appropriate oversight and regulation, depending on their impact on the market or the extent to which the regulatory system depends on them.

g. Principles for Collective Investment Schemes

1. The regulatory system must set standards for the eligibility, governance, organization, and operational behavior of those wishing to market or operate collective investment schemes.
2. The regulatory system must provide rules governing the form and legal structure of collective investment schemes, as well as the segregation and protection of client assets.
3. Regulations must require disclosure, as outlined in the principles for issuers, necessary to evaluate the suitability of a collective investment scheme for specific investors and the value of their interest in the scheme.
4. Regulations must ensure that there are proper and disclosed grounds for the valuation of assets and the pricing and redemption of units in collective investment schemes.
5. Regulations must ensure that hedge funds and/or hedge fund managers/advisors are subject to appropriate supervision.

h. Principle for Market Intermediaries

1. Regulations must establish minimum entry standards for market intermediaries.
2. There must be initial and ongoing capital and prudential requirements for market intermediaries that reflect the risks undertaken by the intermediaries.
3. Market intermediaries must be required to establish internal functions that meet standards for internal organization and operational behavior, aimed at protecting client interests and assets and ensuring proper risk management, through which the intermediary's management assumes primary responsibility for these matters.
4. There must be procedures in place to handle market intermediary failures to minimize damage and losses to investors and contain systemic risks.

i. Principles for Secondary Markets and Other Markets

1. The establishment of trading systems, including stock exchanges, must be subject to authorization and regulatory oversight.
2. There must be ongoing regulatory oversight of exchanges and trading systems to ensure that the integrity of trading is maintained through fair and balanced rules that achieve the right balance between the demands of different market participants.

3. Regulations must encourage transparency in trading.
4. Regulations must be designed to detect and prevent market manipulation and other unfair trading practices.
5. Regulations must aim to ensure proper management of large exposures, default risks, and market disruptions.

j. Principles relating to Clearing and Settlement

Securities settlement systems, central securities depositories, trade repositories, and central counterparties must be subject to regulatory requirements and oversight designed to ensure that they are fair, effective, and efficient, and will reduce systemic risks.

The Active Role of IOSCO in Providing Protection to Investors

Some preventive efforts undertaken by IOSCO, besides the principles, include informative and educational approaches. IOSCO will receive warnings from its members regarding companies that are unauthorized to provide investment services in certain jurisdictions. One example of such a warning involves companies that are unauthorized or use names similar to legitimate companies, thus potentially deceiving investors due to the resemblance (OICV-IOSCO, 2024). This, of course, involves fraudulent activity. These warnings are voluntarily provided by IOSCO members, and the warnings issued must be accountable.

In its informative function, IOSCO advises investors to always check whether the company's operations are regulated by the relevant competent national authority. It is important to know if the regulatory body has granted authorization and licenses to the regulated company to conduct specific business types and provide investment services. Each jurisdiction has its own complaint procedure and compensation scheme, making it crucial for investors to understand the rights they have within the selected jurisdiction. In the Investor Alerts Portal, investors can suspect fraud or illegal investment activities. However, prospective investors should not make assumptions, as the absence of relevant alerts in the portal after verification does not guarantee legitimacy.

In relation to the educational function provided by IOSCO, one of its initiatives is the World Investor Week program. This initiative is conducted by IOSCO's Committee 8 on Retail Investors (C8), aimed at raising awareness about the importance of investor education and protection. A key focus of this program is on education and investor protection in jurisdictions with limited resources. Through the IOSCO network, the initiative facilitates coordination and collaboration between members by providing information on frameworks for each jurisdiction. One report from Indonesia highlights the authority of OJK (Financial Services Authority). In the 2018 World Investor Week report, OJK collaborated with the Indonesia Stock Exchange (IDX), Indonesia Central Securities Depository (KSEI), Indonesian Clearing and Guarantee Corporation (KPEI), and several capital market companies (OICV-IOSCO, 2019). This cooperation facilitated educational activities in Indonesia, including campaigns on social media, radio, and the culminating event, Investival (Indonesia Investment Festival).

Additionally, the IOSCO Research Department (RD) has worked to identify risks that are most relevant to IOSCO's three main goals each year, based on market intelligence, analysis of reports, and data used to design the IOSCO Risk Survey (OICV-IOSCO, 2016). The final results of this research are shared with IOSCO members and market experts to gather diverse and global perspectives on emerging risks. One of the risks assessed, relevant to the securities market, is the threat of cyberattacks (Prasetyo, 2022). This is crucial for maintaining investor trust and participation in the capital market and for protecting them from financial and non-financial losses due to cybercrime. In the securities market, potential vulnerabilities from cyber threats arise from: connections to insecure third parties, exploitation of information and communication platforms, patching and configuration errors, threats to exchanges, and confusion about customer responsibilities. Emphasizing the impact of cyberattacks on the

securities market, it is expected that cyber threats will increase with the role of technology in financial services, the growing interdependence of financial systems, and the expanding motives behind cyberattacks (OICV-IOSCO, 2016).

A concrete example of a cyber threat affecting the financial services sector is the "New Zealand Stock Exchange Shutdown Due to Cyberattack" case (Eka Yudha Saputra, 2013). Trading on the NZ Stock Exchange (NZX) was halted for several hours after a cyberattack targeted the exchange over several days, disrupting the servers by flooding internet traffic until they became non-operational. Stock trading, the NZX website, and the market announcement platform were also affected. The attack flooded the online services with more traffic than the servers or networks could handle, rendering the website or services inoperable. In this case, New Zealand required its spy agency to activate a crisis security plan to counter external attacks on its stock market. IOSCO has outlined various aspects related to cybercrime in the securities market, including: size of threats, complexity, incentive structure, effects on market integrity and efficiency, and awareness and transparency (Rohini Tendulkar, 2013). With these indicators, IOSCO has acknowledged the possibility of cyberattacks within the international capital market related to financial services. Such attacks could affect the stability of national and international capital markets and the stabilization of money supply in a country (Dyah Ayu Purboningtyas and Adya Prabandari, 2019).

The establishment of the Investor Protection Fund (DPP) is another form of protection for investors recommended by IOSCO and considered a best practice in capital markets across countries. This fund is designed to improve the protection of investor assets. The Investor Protection Fund is a pool of funds established to protect against the loss of investor assets held by securities firms, differing from the guarantee fund managed by PT Kliring Penjaminan Efek Indonesia (KPEI) to protect investors from settlement risk. The Investor Protection Fund has already been implemented by other countries, known as Investor Protection Funds or Compensation Funds, though initiatives for its establishment in Asia have emerged only in recent years. As an organization, IOSCO plays a vital role in disseminating data to its member countries. These data are collected through warnings or reports from members about unauthorized companies providing investment services in the jurisdictions issuing the warnings. This information can be accessed through the "Investor Alerts Portal" on IOSCO's website. Through this, investors are informed about stock exchanges that may pose problems and are protected from cyber threats that could harm both their assets and personal data.

Based on the above description, it is clear that IOSCO actively implements roles that align with the principles upon which the international organization for capital market regulators stands, particularly in providing protection to investors.

Relevance of IOSCO Principles to Indonesian Positive Law Regarding Protection Against Cybercrime on Investor's Personal Data in Indonesia

Personal Data Protection in Relation to IOSCO's Investor Protection Principles

With the advancement of technology, investment activities are no longer limited to Indonesian national companies, but can also be conducted internationally, often removing the boundaries of sovereignty of each country (M Ngafifi, 2014). These technological advancements have certainly facilitated the process and activities of investment, trading, and information exchange in the capital market (LA Adha, 2020). However, this also introduces cyber threats, as previously discussed. Given these cyber threats, IOSCO, based on its principles prioritizing investor protection, focuses on safeguarding data and information related to investors in international capital market activities.

To protect personal data, IOSCO members themselves are protected under the "Personal Data Protection Policy and assignment of image rights for participants in events and meetings organized by IOSCO (the 'Event')." This policy is implemented by the regulators' staff who must adhere to the highest professional standards and are given clear guidelines on behavioral

aspects, including "the proper observance of confidentiality and secrecy provisions and the protection of personal data."

From the investor's perspective, cyber threats and attacks can disrupt and threaten investors if confidential information stored by financial institutions is leaked or if assets are misused due to a hacked account. One example of cyber threats and attacks within the financial sector occurred in August 2015, when the U.S. Securities and Exchange Commission announced a fraud case involving 32 perpetrators who stole personal data from companies containing their earnings information, with the intent of profiting from it. Two of the perpetrators were Ukrainian nationals who hacked a newswire service, and 30 others, located both inside and outside the United States, traded the stolen information, generating illegal profits of $100 million (OICV-IOSCO, 2016).

To provide legal protection against cyber threats, particularly in protecting investor personal data in the capital market, Indonesia accommodates this under the Personal Data Protection Law (PDP Law). Similarly, IOSCO has its own "Personal Data Protection Policy and assignment of image rights for participants in events and meetings organized by IOSCO (the 'Event')" that governs various aspects related to personal data protection. The personal data of participants will be processed as long as needed to fulfill the purposes of data collection, which generally involve event management and organization. If the personal data is no longer required for these purposes, it will be retained for as long as any potential obligations may arise, but no longer than 6 years, after which it will be blocked.

Although IOSCO is committed to safeguarding investors' personal data, it does not automatically prevent the sharing of participants' personal data with third parties. IOSCO may share personal data with third parties where explicitly permitted by law. Additionally, IOSCO may share the collected personal data with third parties for purposes such as data processing, company audits, consulting services, IT services, event agents, and event organizers.

In carrying out its mission and objectives, IOSCO implements measures to protect investors by sharing personal data of its members with each other and with third-party countries in the European Economic Area (EEA) that have established adequate decisions on personal data protection as determined by the European Commission (OICV-IOSCO, 2024). However, IOSCO also acknowledges that this sharing can present vulnerabilities to cyber threats through connections with insecure or untrusted third parties. This indicates the involvement of third-party vendors used by companies, but the companies may not have expanded their cybersecurity practices or monitored the actions of third-party vendors concerning the information and data entrusted to them (OICV-IOSCO, 2016).

Nevertheless, protecting investor personal data can be further ensured, and trust in Indonesia's capital market can continue to be strengthened. These measures will help create a safe and transparent investment environment, in line with IOSCO's primary goal of protecting investors and maintaining the integrity of the capital market.

Comparison of IOSCO Principles with Relevant Positive Law Regarding Protection of Investor's Personal Data in the Capital Market Sector in Indonesia

Cyber threats refer to all forms of potential and actual cyber risks, including cyber attacks, cyber-crime, or other cyber disruptions. Cyber threats are harmful and planned disruptions intentionally carried out by certain individuals, not caused by errors or negligence, not due to natural disasters, and not examples of technological "disruptions" or software malfunctions. Personal data protection is one of the fundamental elements of modern law, especially with the increasing prevalence of cyber threats in the capital market due to advancements in information and communication technology (S.R. Azura, Izari, and S.G. Maharani, 2023). In Indonesia, the urgency to protect personal data is realized through the Personal Data Protection Law (PDP Law), which provides an essential legal foundation for

protecting individuals' rights related to their personal data, including in the highly vulnerable capital market sector against cybercrime.

The capital market sector has specific characteristics that distinguish it from other sectors. Investor trust is highly dependent on the integrity and security of the data they provide to financial service providers and capital market entities. Cybercrime, such as data breaches, identity theft, and digital fraud, can result in significant financial losses and damage public trust in the capital market. Therefore, personal data protection in this sector requires special and stringent attention and regulation (Muhammad Yudistira and Ramadani, 2023). Although the PDP Law regulates various aspects of personal data protection, there are some critical areas that are not fully addressed, especially when compared to international standards such as the IOSCO Principles (International Organization of Securities Commissions). IOSCO principles are designed to ensure fair, efficient, and transparent capital markets while protecting investors from various threats, including cybercrime. For example, IOSCO Principle 8 emphasizes the importance of effective risk management, including cyber risks, while Principles 10 and 15 focus on supervision, law enforcement, and investor protection specifically.

Legal experts emphasize that personal data protection in the capital market sector must be complemented by a strong oversight mechanism and strict law enforcement. Without a stringent oversight framework, the implementation of personal data protection becomes less effective and vulnerable to abuse (Sudrajat, 2021). Furthermore, it should be noted that the capital market sector requires more specific regulation due to the high risk of cybercrime that may affect investors (Yuliandra, 2022). When linked to the IOSCO Principles, there are several aspects that have not been optimally addressed. These include the following:

a. Relevant IOSCO Principles

IOSCO principles set international standards to ensure fair, efficient, and transparent capital markets while protecting investors from various threats, including cybercrime. Three key principles that are relevant are:

1. Principle for Risk Management Regulation
   Emphasizes the importance of capital market entities having an effective framework to manage risks, including cyber risks.
2. Principle for Supervision and Enforcement
   Requires effective oversight and enforcement mechanisms to address violations of capital market regulations.
3. Principle for Investor Protection
   Aims to protect the rights and interests of investors, including protection against fraud and cybercrime.

b. Comparison with the Personal Data Protection Law (PDP Law)

The PDP Law provides the legal foundation for personal data protection in Indonesia, but there are several shortcomings when compared to the IOSCO Principles. The following is an analysis of this comparison:

1. Cyber Risk Management
   The IOSCO Principles require capital market entities to have an effective framework for managing cyber risks. However, the PDP Law does not explicitly regulate the cyber risk management that capital market entities must adopt. Articles 38-39 of the PDP Law mention the obligation of data controllers to protect personal data from unauthorized processing and prevent unauthorized access. However, these articles do not provide specific details regarding technical and operational steps for managing cyber risks in the capital market sector. It is undeniable that without a clear cyber risk management framework, capital market entities remain vulnerable to cyber threats (Yusuf Daeng, et al., 2023). In the context of the capital market, cyber risk management should cover various aspects, from employee training, the application of advanced security technologies, to clear incident response

procedures (IBM, 2024). Without clear regulation in the PDP Law on cyber risk management, capital market entities may not be prepared to face cyberattacks that could damage investor trust and market integrity (Swammy, Sarah, and Michael McMaster, 2018).

2. Shortcomings in Law Enforcement and Oversight
   The IOSCO Principles emphasize the importance of effective oversight and law enforcement to protect investors. However, the PDP Law does not specifically regulate oversight and enforcement mechanisms aimed at the capital market sector, which is highly vulnerable to cybercrime. Article 35 of the PDP Law regulates that data controllers must protect and ensure the security of the personal data they process. However, there are no specific details regarding oversight and enforcement mechanisms in the context of cybercrime in the capital market sector. The need for personal data protection in the capital market sector requires stricter oversight due to higher risks of fraud and cyberattacks. Without specific oversight mechanisms for this sector, capital market entities may lack sufficient incentives to implement necessary cybersecurity measures (Elvira Fitriyani Pakpahan, Eric Kurniawan, et al., 2020). This places investors at higher risk, as there is no guarantee that their personal data will be adequately protected from cyber threats.
3. Special Protection for Investors
   The IOSCO Principles focus on protecting the rights and interests of investors from fraud and cybercrime. The PDP Law focuses on the rights of personal data subjects in general but provides less specific protection for investors in the context of cybercrime. Article 46 of the PDP Law regulates the obligation of data controllers to notify data protection failures, but there are no provisions that specifically address the protection of investors in the capital market sector. Special protection for investors is crucial, given the complexity and sensitivity of data in this sector. Investments in the capital market involve large sums of money and sensitive personal data. Cybercrime can include identity theft, investment fraud, and attacks on the capital market infrastructure. Without special protection for investors, these risks may reduce investor confidence in Indonesia's capital market, which in turn could negatively impact economic stability and growth.

This comparison shows several gaps that have not been addressed to ensure optimal protection for investors in Indonesia. Without detailed regulations on cyber risk management, specific oversight and law enforcement, and special protection for investors, the PDP Law has not fully met the international standards set by IOSCO. In reality, the government could establish a task force under the Financial Services Authority (OJK) to oversee cybersecurity related to personal data in the capital market sector, including technical guidelines that specifically cover mechanisms for monitoring compliance with reporting obligations and audits. Additionally, Indonesia needs to strengthen cooperation with international data protection and cybersecurity agencies, such as with coordinated incident response protocols with international bodies, to handle cross-border cyberattacks quickly and effectively. The implementation of relevant IOSCO principles and the adoption of more specific and detailed rules regarding oversight, cyber risk management, and protection of investors from cybercrime threats to personal data would not only enhance a secure, fair, and transparent capital market but also promote a healthier and more sustainable digital economy for investors.

CONCLUSION

In providing protection to investors in the capital market, IOSCO applies 38 principles divided into 10 key principles as a binding policy foundation for its member countries. IOSCO also takes preventive measures through informative and educational approaches, such as the annual issuance of The IOSCO Risk Survey by the IOSCO Research Department, the establishment of the Investor Protection Fund (DPP) to safeguard investor assets, and the implementation of the "Personal Data Protection Policy and assignment of image rights for participants in events and meetings organized by IOSCO (the 'Event')." On the other hand, the

PDP Law, as Indonesia's positive law, has gaps that have not been addressed to ensure optimal protection for investors in Indonesia. Without detailed provisions on cyber risk management, specific oversight and law enforcement, and special protection for investors, the PDP Law has not fully met the international standards set by IOSCO.

In facing the growing threat of cybercrime, especially in the capital market sector in Indonesia, the implementation of IOSCO principles is increasingly pertinent safeguarding investors by ensuring robust personal data protection within Indonesia's capital market. The discourse on establishing a Personal Data Protection Supervisory Agency, as mandated by the PDP Law, requires steps to harmonize functions with existing supervisory agencies, especially the Financial Services Authority (OJK). This approach is crucial to avoid regulatory overlaps and inter-agency functional conflicts that may undermine the effectiveness of oversight. With stronger institutional integration and coordination, it is expected that synergy will be created, which will not only enhance operational efficiency but also strengthen the capacity for comprehensive personal data protection within the financial sector. This integration will encourage more comprehensive protection for investor data, thereby increasing public trust and enhancing the competitiveness of Indonesia's capital market in the digital era.

REFERENCE

Abi Tyas Tunggal, "What is a Cyber Threat?", from: https://www.upguard.com/blog/cyber-threat, 2019, accessed July 28, 2024.

Bambang Poernomo, Principles of Equality Before the Law in the Frame of Indonesian Positive Law, Jakarta: Jendela Hukum Publishing, 2022.

Christian Calliess and Ansgar Baumgarten, "Cybersecurity in the EU: The Example of the Financial Sector - A Legal Perspective", German Law Journal, 2020.

Constitution of 1945

Diny Luthfah, "Strengthening Cybersecurity in Indonesia's Financial Sector", Journal of Research and Scientific Work of the Trisakti University Research Institute, Vol. 9, No. 1, 2024.

Dyah Ayu Purboningtyas and Adya Prabandari, "Legal Protection for Investors in Indonesia's Capital Market by the Securities Investor Protection Fund", Notary Journal, Vol. 12, No. 2, 2019.

Eka Yudha Saputra, "New Zealand Stock Exchange Halted Due to Cyber Attack", from: https://dunia.tempo.co/read/1379714/bursa-saham-selandia-baru-terhenti-karena-serangan-siber, accessed July 29, 2024.

Elvira Fitriyani Pakpahan, Eric Kurniawan, et al., "The Role and Authority of the Financial Services Authority (OJK) in Securing Transactions in the Capital Market", Ius Civile Journal, Vol. 4, No. 1, 2020.

IBM, "What is Cyber Risk Management?", IBM Cyber Risk Management, 2024, from: https://www.ibm.com/id-id/topics/cyber-risk-management, accessed July 30, 2024.

International Organization of Securities Commissions 2017, "Methodology for Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation (OIVC-IOSCO)", 2017, from: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD562.pdf, accessed July 28, 2024.

IOSCO, Cyber Security in Securities Markets – An International Perspective, IOSCO, 2016.

Kadek Desy Pramita and Kadek Diva Hendrayana, "Legal Protection for Investors as Consumers in Online Investments", Pacta Sunt Servanda Journal, Vol. 2, No. 1, 2021.

LA Adha, "Digitization of Industry and Its Impact on Employment and Labor Relations in Indonesia", Journal of Legal Compilation, Vol. 5, No. 2, 2020.

Law No. 1 of 2024 on the Second Amendment of Law No. 11 of 2008 on Electronic Information and Transactions

Law No. 25 of 2007 on Investment

Law No. 27 of 2022 on Personal Data Protection
Law No. 4 of 2023 on Development and Strengthening of the Financial Sector
M Ngafifi, "Technological Advancements and Human Lifestyle in the Social-Cultural Perspective", Journal of Educational Development: Foundations and Applications, Vol. 2, No. 1, 2014.
Muhammad Yudistira and Ramadani, "Juridical Review on the Effectiveness of Handling Cybercrimes Related to Personal Data Theft Under Law No. 27 of 2022 by Kominfo", Unes Law Review Journal, Vol. 5, No. 4, 2023.
Nanda Dwi Rizkia, Legal Research Methods, Bandung: Universitas Padjadjaran, 2021.
Nyoman Amie Sandrawati, "Anticipating Cybercrime and the Digital Divide in the Application of Tik in the General Election Commission", Electoral Governance Journal of Indonesia Election Governance, Vol. 3, No. 2, 2022.
OICV-IOSCO, "Investor Alerts Portal", from: https://www.iosco.org/investor_protection/?subsection=investor_alerts_portal, accessed July 28, 2024.
OICV-IOSCO, "Personal Data Protection Policy and Assignment of Image Rights for Participants in Events and Meetings Organized by IOSCO (the 'Event')", 2024, from: https://www.iosco.org/meeting-registration/pdf/Personal-Data-Protection-Policy.pdf, accessed July 28, 2024.
OICV-IOSCO, "What to Do When Suspecting a Scam", from: https://www.iosco.org/investor_protection/?subsection=what_to_do_when_suspecting_a_scam, accessed July 28, 2024.
OICV-IOSCO, Securities Market Risk Outlook 2016, Madrid: IOSCO Publishing, 2016.
OICV-IOSCO, World Investor Week 2018 Public Report, Madrid: IOSCO Publishing, 2019.
OJK, "International Organization of Securities Commissions Growth and Emerging Market Committee Meeting (IOSCO GEM Meeting)", from: https://ojk.go.id/id/kanal/pasar-modal/berita-dan-kegiatan/info-terkini/Documents/Pages/IOSCO-GEm-c-2016-nusa-dua-bali-info-rundown-dan-acara/IOSCO-GEMC-2016-BALI.pdf, 2016, accessed July 28, 2024.
Prasetyo, Cybersecurity in the Financial Sector, Jakarta: Media Digital Publishing, 2022.
Rohini Tendulkar, Cyber-crime, Securities Markets, and Systemic Risk, Madrid: IOSCO Publishing, 2013.
S.R. Azura, Izari, and S.G. Maharani, "Electronic Crimes in Transactions (Fraud Cyber Crime) at Indonesia Stock Exchange PT DSFI", Journal of Regional Accounting & Finance, Vol. 16, No. 1, 2023.
Soerjono Soekanto, Introduction to Legal Research, 3rd edition, Jakarta: Universitas Padjadjaran, 2019.
Sudrajat, Personal Data Protection in the Digital Era, Bandung: Nusantara Publishing, 2021.
Swammy, Sarah, and Michael McMaster, Governance, Compliance, and Supervision in the Capital Markets, + Website. Hoboken, NJ: John Wiley & Sons, 2018.
Yuliandra, Cyber Law and Personal Data Protection in Indonesia, Jakarta: Andalas Publishing, 2022.
Yusuf Daeng, et al., Personal Data Protection in the Digital Era: A Review of the Legal Framework for Privacy Protection, Pekanbaru: Innovative Journal Of Social Science Research, 2023.