

DOI: <https://doi.org/10.38035/sijal.v4i2><https://creativecommons.org/licenses/by/4.0/>

Received: 09-09-2026 | Revised: 30-10-2026 | Accepted: 05-10-2026

Prevention, Law Enforcement, and Protection Strategies in the Digital Economy Ecosystem: An Integrated Legal Governance Framework for Indonesia

Riyanto¹, Joko Sriwidodo², Lusia Sulastri³

¹Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, riyan.riyan19900@gmail.com

²Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, -

³Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, -

Corresponding Author: riyan.riyan19900@gmail.com¹

Abstract: Indonesia's digital economy expands financial inclusion, market access, and transactional efficiency, but also increases exposure to fraud, phishing, identity theft, data breaches, ransomware, and payment abuse. This study examines the adequacy of Indonesia's legal and institutional arrangements for preventing, investigating, and remedying economic cybercrime and formulates an integrated governance model. Using normative legal research, the study applies statutory, conceptual, comparative, and case approaches to legislation, regulatory instruments, institutional materials, and recent scholarship. The analysis finds that Indonesia possesses substantial criminal, data-protection, electronic-system, financial-sector, and consumer-protection rules, yet their operation remains fragmented across institutions and stages of response. Prevention still relies excessively on user awareness; enforcement is constrained by volatile evidence, uneven capacity, delayed asset freezing, and cross-border barriers; and remedies do not consistently restore victims' finances, identities, or procedural position. The study proposes an Integrated Digital Economic Security Governance framework comprising a shared risk taxonomy, prevention by design, differentiated platform duties, coordinated evidence preservation and enforcement, victim-centred remedies, accountable international cooperation, and continuous evaluation. Its novelty lies in allocating responsibility according to institutional capacity, knowledge, and control while linking cybersecurity, law enforcement, corporate accountability, and victim recovery within one rights-based and risk-responsive legal architecture.

Keywords: cybercrime, digital economy, law enforcement, victim protection, cybersecurity governance.

INTRODUCTION

Digital technology has altered the architecture of economic exchange. Payments, lending, investment, retail trade, logistics, advertising, and professional services increasingly depend on interconnected platforms that process large quantities of personal and commercial data. This

transformation reduces transaction costs, allows firms to reach customers beyond their physical locations, and enables consumers to obtain services almost instantly. For micro and small businesses, digital marketplaces and payment systems may overcome geographic isolation and limited access to conventional distribution. For financial institutions, automated identification, transaction records, and data analytics can support new products and more rapid risk assessment. Indonesia's digital transformation therefore has a genuine developmental dimension: it expands participation, supports innovation, and connects previously fragmented markets (World Bank, 2022).

The same infrastructure also creates new concentrations of vulnerability. A compromised account may provide access not only to personal communications but also to bank accounts, electronic wallets, marketplaces, cloud storage, and identity credentials. Criminal actors use phishing messages, malicious applications, social engineering, account takeovers, fraudulent online stores, investment schemes, and data obtained from security breaches to exploit this connectivity. Ransomware can interrupt business operations, while attacks on payment providers or financial institutions can create effects extending beyond a single victim. The digital economy magnifies both legitimate scale and criminal scale (World Economic Forum, 2024). Low-cost communication enables offenders to approach thousands of potential victims, automate deception, and relocate infrastructure across jurisdictions (INTERPOL, 2024).

Economic cybercrime is consequently more than traditional crime committed through a computer. It is produced by relationships among technology, incentives, information asymmetry, platform design, user behaviour, and institutional capacity. A fraudulent transaction may involve a victim in Indonesia, a platform incorporated elsewhere, cloud data stored in several states, a payment routed through multiple intermediaries, and an offender using an anonymous or synthetic identity. Legal rules that focus exclusively on the final act of deception cannot adequately address insecure system design, negligent credential management, delayed incident reporting, or weak cooperation among intermediaries. At the same time, a regulatory response that imposes unlimited responsibility on platforms may suppress innovation and transfer excessive compliance costs to smaller providers.

Indonesia has adopted several legal instruments relevant to this problem. Law No. 11 of 2008 on Electronic Information and Transactions, as amended most recently by Law No. 1 of 2024, recognizes electronic information and documents, regulates electronic systems, and criminalizes specified forms of unlawful conduct. Law No. 27 of 2022 on Personal Data Protection establishes rights of data subjects and obligations of controllers and processors, including security and breach-related responsibilities (Indonesia, 2022). Government Regulation No. 71 of 2019 addresses the operation of electronic systems and transactions (Indonesia, 2019). The financial sector is further governed by the Financial Sector Development and Strengthening framework, OJK regulations on technology-based innovation, governance, risk management, and consumer protection, and Bank Indonesia rules within the payment-system sphere. The new Indonesian Criminal Code also reshapes the relationship between general criminal law and special cybercrime legislation.

These instruments represent important progress, yet regulatory abundance does not automatically create effective protection. Cyber incidents cross boundaries between criminal enforcement, administrative supervision, data governance, consumer redress, and private contractual responsibility. Institutions may receive different reports concerning the same event without a unified classification or escalation mechanism. Victims frequently confront uncertainty about whether to complain to a platform, financial institution, police unit, regulator, or data-protection authority. Even when an offender is prosecuted, criminal proceedings may not restore stolen funds, repair identity misuse, or remove unlawfully disseminated data. The distinction between punishment and recovery is therefore central.

The literature has examined cybercrime offences, electronic evidence, personal data, financial technology, and consumer protection, but these fields are often treated separately. Studies of criminal law tend to focus on offence construction, jurisdiction, investigation, and admissibility. Cybersecurity research emphasizes controls, resilience, and incident response. Consumer-law scholarship examines information duties, unfair terms, and redress, while data-protection research addresses lawful processing, security, and institutional accountability. Fragmented scholarship mirrors fragmented governance. What remains insufficiently developed is an integrated legal model explaining how prevention, enforcement, and protection should interact across the lifecycle of an economic cyber incident.

This study addresses two questions. First, how adequately do Indonesia's laws and institutional arrangements prevent, investigate, and remedy cybercrime within the digital economy ecosystem? Second, how should responsibilities be reconstructed among the state, law-enforcement bodies, financial institutions, platforms, businesses, and users to create effective but proportionate protection? The article argues that cybercrime governance should move from isolated compliance toward coordinated ecosystem responsibility. Its novelty lies in the proposed Integrated Digital Economic Security Governance framework, which connects prevention by design, risk-based platform obligations, coordinated enforcement, digital-evidence readiness, and victim-centred recovery.

The argument is significant for three reasons. Normatively, security enables the exercise of autonomy, property, privacy, and access to digital economic services. Institutionally, public trust depends on whether authorities and service providers respond coherently when risks materialize. Economically, persistent fraud and insecure systems impose costs on consumers and legitimate enterprises and may discourage participation. Effective governance must therefore preserve the benefits of innovation while allocating the costs of foreseeable harm to actors capable of preventing, detecting, or mitigating it.

METHODS

This study applies normative legal research to evaluate the coherence and adequacy of rules governing economic cybercrime in Indonesia. Normative research is appropriate because the principal inquiry concerns the content, relationship, justification, and institutional implications of legal norms. The study does not measure the prevalence of cybercrime or claim causal effects from primary statistical observations. Instead, it assesses whether the existing legal architecture provides a defensible allocation of duties, powers, procedures, and remedies across the digital economy ecosystem.

Four approaches are combined. The statutory approach examines the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, the Criminal Code, Government Regulation No. 71 of 2019, financial-sector legislation, and relevant OJK and Bank Indonesia regulations. Vertical analysis evaluates consistency between statutes and implementing instruments; horizontal analysis identifies overlap, gaps, and potential conflict among criminal, administrative, data-protection, and consumer-protection regimes. The conceptual approach uses cybersecurity governance, responsive regulation, due diligence, victim-centred justice, and digital resilience as evaluative concepts. The comparative approach draws functional lessons from international cooperation and platform-accountability developments without presuming that foreign models can be transplanted unchanged. The policy approach evaluates institutional coordination, reporting, supervision, investigation, recovery, and public education.

Legal materials were selected according to authority, relevance, recency, and direct connection to the research questions. Primary materials were interpreted through grammatical, systematic, purposive, and contextual methods. Secondary sources were used to identify implementation challenges and contemporary debates. Analysis proceeded in four stages:

mapping prohibited conduct and responsible institutions; identifying procedural and remedial gaps; assessing the distribution of preventive capacity among ecosystem actors; and constructing an integrated framework based on legality, proportionality, accountability, technological neutrality, and effective protection. The analysis distinguishes three dimensions that are often conflated. Prevention concerns measures taken before or during an attempted offence to reduce likelihood and impact. Law enforcement concerns detection, investigation, evidence, attribution, prosecution, and international cooperation. Protection concerns immediate assistance, containment, compensation, restoration, data correction, complaint handling, and prevention of repeated harm. The effectiveness of the legal system is assessed not only by punishment but also by its capacity to connect these dimensions in a timely and rights-respecting manner.

RESULTS AND DISCUSSION

The Evolving Forms and Systemic Effects of Economic Cybercrime

The legal characterization of cybercrime begins with the interests harmed and the role played by technology. Some offences are cyber-dependent: they cannot occur without information systems, as in unauthorized access, malicious interference, malware deployment, and certain denial-of-service attacks. Others are cyber-enabled versions of established crimes, including fraud, extortion, identity theft, unlawful appropriation, and document falsification. The distinction matters because cyber-dependent conduct requires specialized technical investigation, whereas cyber-enabled conduct also requires analysis of traditional elements such as deception, intention, causation, benefit, and loss.

Phishing illustrates the layered nature of harm. A deceptive message may imitate a bank, public authority, marketplace, delivery provider, or colleague. The offender seeks a password, one-time code, identity number, payment, or installation of malicious software. The immediate legal issue may be fraud, but the incident may also involve unlawful access, interception, personal-data misuse, falsified electronic information, and money laundering. A victim's action does not remove the relevance of security design. Interfaces that obscure destination accounts, authentication processes vulnerable to social engineering, or delayed fraud warnings may substantially affect the probability and magnitude of loss.

Identity crime similarly reveals the limits of offence-based fragmentation. Stolen data can be used to open accounts, apply for loans, take control of existing profiles, register telephone numbers, or create synthetic identities. Harm continues after the first transaction because incorrect records may damage creditworthiness and expose the victim to repeated demands. Personal data are therefore not merely an object of privacy; they function as economic credentials. Effective protection requires the ability to freeze suspicious activity, correct records, invalidate compromised credentials, and coordinate among institutions that rely on the same identity data.

Ransomware and system interference produce organizational and systemic consequences. Encryption or exfiltration may interrupt payroll, customer services, supply chains, or essential financial functions. Payment of ransom does not guarantee restoration and may finance further criminal activity. The incident also raises notification, evidence preservation, business continuity, and third-party risk questions. An enterprise may depend on cloud, payment, verification, and software vendors; a weakness at one provider can affect many clients. Concentration risk means that cybersecurity cannot be evaluated solely at the level of each bilateral contract.

Digital payment abuse includes unauthorized transfers, manipulation of payment instructions, takeover of electronic wallets, merchant fraud, and exploitation of rapid settlement. Speed benefits legitimate users but narrows the period available to detect and reverse suspicious transactions. A victim-centred framework therefore requires real-time

controls, confirmation mechanisms, rapid reporting channels, and protocols for temporary holds that remain subject to safeguards against arbitrary restriction. Liability should reflect control, causation, compliance, and the capacity of each actor to prevent or mitigate loss rather than relying on a simplistic assumption that either the user or provider must bear all consequences.

Online investment and commerce fraud exploit information asymmetry and platform scale. False testimonials, manipulated advertising, cloned websites, impersonated professionals, and coordinated accounts can create artificial credibility. Platforms influence exposure through recommendation systems, verification practices, advertising approval, and complaint response. They should not be treated as guarantors of every user statement, but neither are they neutral when their design materially structures visibility, trust, payment, and continued access. Differentiated responsibility is needed according to function, scale, knowledge, risk, and capacity. The systemic effect of these offences is erosion of trust. Individual losses are important, yet aggregate insecurity also changes behaviour. Consumers may avoid digital financial products; small enterprises may return to inefficient cash transactions; institutions may impose friction that excludes legitimate users; and enforcement agencies may face overwhelming volumes of low-value but collectively significant complaints. Cybercrime thus operates as a tax on digital participation. Law and governance must respond to both individual justice and ecosystem resilience.

Indonesia's Regulatory Architecture and Its Fragmentation

The Electronic Information and Transactions Law provides the central legal basis for electronic information, systems, prohibited conduct, and electronic evidence. Its recognition of electronic documents supports digital economic activity and enforcement. Provisions concerning unlawful access, interference, manipulation, and specified harmful communications create criminal-law entry points. The 2024 amendment sought greater legal certainty and adjusted several contested provisions (Indonesia, 2024). Nevertheless, the statute cannot alone regulate every dimension of economic cybercrime. Its criminal provisions interact with the Criminal Code, sectoral financial rules, data-protection obligations, procedural law, and institutional powers.

The enactment and effective operation of the new Criminal Code require careful harmonization. General offences involving fraud, extortion, falsification, participation, attempt, and corporate liability may overlap factually with special electronic offences. The principle of *lex specialis* assists selection but does not automatically answer questions involving multiple protected interests or continuing conduct. Investigators and prosecutors need charging guidelines that explain when provisions are cumulative, alternative, or absorbed. Legal certainty also requires consistent treatment of corporate fault where a provider's organizational failure contributes to harm but no individual manager directly commits the predicate offence.

The Personal Data Protection Law shifts attention from punishment after misuse to governance before harm (Indonesia, 2022). Controllers and processors must establish a lawful basis, limit purposes, maintain accuracy and security, respect data-subject rights, and respond to breaches. These obligations are essential because large-scale fraud frequently relies on compromised or unlawfully traded data. However, data-protection compliance can become formalistic if organizations merely publish privacy notices without controlling access, minimizing collection, auditing vendors, or testing incident response. The law's effectiveness depends on supervision, enforceable standards, and an authority capable of coordinating with sectoral regulators and law enforcement.

Government Regulation No. 71 of 2019 imposes obligations on electronic-system providers regarding reliability, security, and responsible operation (Indonesia, 2019). Its

functional importance lies in connecting legal responsibility to systems, not only to content or completed offences. Yet the category of provider covers diverse actors, from small applications to large financial and marketplace infrastructures. Uniform rules may be either too burdensome for low-risk actors or too weak for systemic platforms. Risk differentiation should consider the sensitivity and volume of data, number of users, transaction value, substitutability, interconnection, history of incidents, and potential for cascading harm.

Financial regulation provides more developed risk-management and consumer-protection mechanisms. OJK Regulation No. 3 of 2024 on Financial Sector Technology Innovation requires governance, risk management, reliable information systems, cyber resilience, consumer protection, and personal-data protection (Financial Services Authority, 2024a). OJK's cybersecurity guidance emphasizes data protection, incident response, maturity assessment, training, collaboration, and information exchange (Financial Services Authority, 2024b). POJK No. 22 of 2023 strengthens consumer and public protection, while newer governance and risk-management rules for technology innovation and digital financial assets recognize operational, cyber, legal, compliance, strategic, and reputational risk (Financial Services Authority, 2023, 2026). These instruments show movement toward ecosystem governance, but coordination with general cybercrime reporting remains crucial.

Regulatory fragmentation arises not because the legal instruments necessarily contradict one another, but because they pursue different functions through separate institutions. Police investigate offences; prosecutors conduct prosecutions; courts decide liability; OJK and Bank Indonesia supervise regulated entities; communications authorities oversee electronic systems; the personal-data institution addresses data governance; and other bodies manage cybersecurity coordination or specific public services. A single incident may engage all of them. Without interoperable classifications and referral procedures, victims repeat reports, institutions hold partial information, and patterns remain invisible. The fragmentation is especially consequential at the boundary between administrative noncompliance and criminal harm. A security breach may result from weak governance without criminal intent by the provider, while external offenders exploit that weakness intentionally. Administrative enforcement against the provider and criminal prosecution of the offender serve different purposes and should proceed coherently. Evidence generated through a supervisory audit may be relevant to a criminal investigation, yet its transfer must respect authority, confidentiality, legality, and procedural integrity. Conversely, intelligence from criminal cases may reveal systemic weaknesses requiring regulatory intervention.

Prevention through Risk-Based and Human-Centred Governance

Prevention should be organized through the principle that responsibility follows capacity, knowledge, and control. Users must exercise reasonable care, but many risks cannot be managed by individual vigilance. Providers choose authentication architecture, transaction limits, monitoring systems, interface warnings, default privacy settings, vendor relationships, and response procedures. Regulators determine minimum expectations, and law-enforcement agencies generate intelligence about evolving methods. A credible strategy therefore distributes obligations rather than placing the burden primarily on consumers. Prevention by design incorporates security and fraud resistance into products before deployment. Relevant measures include multi-factor authentication proportionate to risk, secure credential recovery, encryption, privilege limitation, segmentation, logging, anomaly detection, transaction confirmation, and secure software development. These controls should not be reduced to a checklist. Institutions need threat modelling that identifies how a service may be abused, who is likely to be harmed, and which controls reduce both probability and severity. Material changes to products should trigger renewed assessment.

Human-centred design recognizes that many attacks manipulate attention, urgency, authority, and trust. Warnings must be timely, specific, and understandable. A generic statement that users should protect their passwords is less effective than a contextual alert explaining that an institution will never request a one-time code or that a destination account has recently changed. Confirmation screens should present meaningful information rather than encourage automatic acceptance. Vulnerable consumers may require additional safeguards, including accessible assistance and optional transaction delays.

Digital literacy remains important but should not become a doctrine of victim blame. Education enables users to recognize impersonation, verify communications, protect devices, and report suspicious conduct. Its effectiveness increases when messages are consistent across government, banks, platforms, schools, and community organizations. Programmes should be evaluated by behavioural outcomes, not merely participant numbers. Simulated phishing exercises, reporting tests, and targeted interventions can reveal whether knowledge changes practice. Education must also reach microenterprises whose employees may use personal devices and informal procedures for business transactions.

Institutional prevention requires board-level accountability. Cyber risk is not solely an information-technology matter because decisions regarding budgets, outsourcing, product speed, data collection, and staffing affect exposure. Boards and senior management should receive intelligible metrics on critical assets, unresolved vulnerabilities, incidents, recovery time, vendor risk, fraud losses, and complaints. Incentives should not reward transaction growth while externalizing security costs. Independent assurance should test whether reported controls function in practice. Third-party governance is indispensable. Contracts with cloud, identity, payment, analytics, and software providers should specify security requirements, audit rights, notification timelines, data return, subcontracting, continuity, and exit assistance. Contractual allocation does not eliminate regulatory accountability to users. Institutions must understand dependency and avoid configurations in which a single provider's failure disables essential functions. Sector-wide exercises can test coordinated response to common-provider incidents.

Information sharing supports early detection but creates legal and operational risks (European Union Agency for Cybersecurity, 2023). Participating institutions need standardized indicators, secure channels, confidentiality rules, quality controls, and limitations on reuse. Fraud intelligence may contain personal data or unverified allegations; indiscriminate circulation can harm innocent persons. A governed exchange should distinguish technical indicators, confirmed fraudulent accounts, suspicious patterns, and investigative information. Correction and review mechanisms are necessary when data affect access to services. Risk-based regulation must be proportionate. Systemic platforms and financial providers require demanding resilience, audit, and reporting obligations. Smaller low-risk enterprises may use simplified frameworks, shared services, and phased compliance. Proportionality does not mean allowing weak protection for vulnerable users; it means selecting requirements that address material risks without imposing irrelevant complexity. Regulators should publish outcomes and principles while allowing controlled technological flexibility.

Law Enforcement, Digital Evidence, and Cross-Border Cooperation

Effective enforcement begins with accessible reporting and rapid preservation. Digital evidence is volatile: logs may be overwritten, accounts deleted, devices altered, and funds transferred through multiple layers. Victims and first responders need clear instructions on preserving messages, transaction records, device information, and account identifiers without compromising privacy or chain of custody. Platforms and financial institutions need authenticated emergency channels through which authorized agencies can request preservation while formal legal process proceeds. Collection must satisfy legality, relevance, authenticity,

integrity, and accountability (Giova, 2023; Zhang, 2024). Investigators should document the source of evidence, method of acquisition, tools used, hash values where appropriate, transfers between custodians, and analytical steps. Digital evidence is not inherently infallible; metadata may be incomplete, accounts may be shared or compromised, and automated attribution can generate error. Courts must be able to evaluate both technical reliability and the inferential link between a device, account, action, and accused person.

Capacity disparities weaken consistency. Specialized cyber units may possess advanced tools, while local officers who receive initial complaints may lack training or access. Centralization alone is insufficient because victims require local accessibility and prompt action. A tiered model should combine standardized first-response procedures, regional forensic support, accredited national laboratories, and specialist assistance for complex cases. Continuing education must include emerging technology, procedural safeguards, and communication with victims. Prosecutorial involvement at an early stage can improve the legal relevance of collection. Investigators and prosecutors should jointly identify offence elements, jurisdiction, necessary evidence, corporate involvement, and cross-border needs. This reduces the risk that technically sophisticated collection fails to establish legally required facts. Judges and defence counsel also require digital-evidence competence to ensure equality of arms and meaningful challenge.

Cross-border investigations remain constrained by differences in jurisdiction, data-location rules, provider practices, and mutual legal assistance. Cloud architecture may make physical location unstable or unknown. Direct preservation can prevent deletion, but access to content may require formal cooperation. Traditional mutual legal assistance procedures are frequently slower than the lifecycle of relevant data (Internet & Jurisdiction Policy Network, 2021; United Nations Office on Drugs and Crime, 2021). Research on cross-border investigations shows that fragmented frameworks and time bottlenecks impair effective evidence exchange (Casino et al., 2022). Reform should accelerate standardized requests while retaining necessity, proportionality, authorization, and remedies. Indonesia should strengthen operational cooperation through designated contact points, common templates, secure transmission, emergency protocols, and participation in appropriate international mechanisms. Cooperation must not become a basis for unrestricted transnational surveillance. Requests should identify legal authority, targeted accounts or data, relevant period, offence, and safeguards. Providers should publish transparency information regarding government requests while protecting investigations and individuals.

Financial tracing requires collaboration beyond technology companies. Banks, payment providers, electronic-money issuers, virtual-asset actors, and merchants may each hold fragments of the transaction path. Rapid freezing can improve recovery, but false positives can affect innocent account holders. Procedures should distinguish preservation, temporary restriction, seizure, and forfeiture, with appropriate authorization and review. Beneficiary-account controls and know-your-customer measures must address mule accounts without indiscriminately excluding low-income users. Enforcement performance should not be measured only by arrests or convictions. Relevant indicators include time to preserve evidence, time to freeze suspected proceeds, proportion of losses recovered, quality of victim communication, repeat-offender disruption, dismantling of infrastructure, and reduction of recurring attack patterns. Strategic enforcement targets the organizational and financial systems enabling crime, not merely replaceable low-level participants.

Victim Protection and Platform Accountability

Victim-centred protection recognizes that cybercrime creates financial, informational, psychological, and procedural harm (Rosyidah, 2024). Individuals may lose essential savings, face debt created through identity misuse, experience humiliation, or spend months contacting

institutions. Businesses may suffer operational interruption, contractual penalties, reputational damage, and exposure of customer data. The response should therefore begin with containment and assistance rather than requiring victims to navigate institutional boundaries unaided. A single-entry reporting principle would allow a complaint received by one competent institution to be securely referred to others without repeated submission. Victims should receive a reference number, explanation of next steps, preservation guidance, status information, and contact channel. Reports should be classified consistently so that aggregate patterns can trigger warnings and investigation. This model requires lawful data sharing and clear institutional ownership of each action.

Financial recovery needs explicit timelines. Providers should offer continuous reporting for unauthorized or fraud-induced transfers, promptly assess temporary restrictions, communicate reasons, and coordinate tracing. A fair liability framework considers authentication, security controls, warnings, user conduct, provider knowledge, and response speed. Automatic denial because a valid credential was used ignores the possibility of manipulation or account takeover. Automatic provider liability regardless of facts could create moral hazard. Presumptions and burden allocation should reflect access to evidence and preventive capacity.

Identity restoration should be treated as a remedy. Victims need procedures to correct records, close fraudulent accounts, challenge debts, replace credentials, and prevent reuse. Institutions should not require separate proof of the same incident when reliable verification has already occurred. Data controllers must cooperate in correction and restriction, and credit-reporting consequences should be suspended during credible disputes. Where data have been unlawfully distributed, practical limits on erasure should be explained honestly while further dissemination is constrained.

Platform accountability should be differentiated. A platform that merely hosts low-risk content does not have the same role as a marketplace that verifies sellers, ranks offers, processes payment, stores credentials, and receives repeated fraud reports. Duties should increase with functional involvement, scale, systemic importance, knowledge, and capacity. Core duties include reasonable security, transparent identity and advertising policies, notice-and-action systems, preservation, cooperation, repeat-abuse controls, and meaningful appeal. Safe-harbour principles may protect intermediaries from impossible general monitoring obligations, but protection should be conditional on responsible conduct. Platforms should not retain immunity where they materially contribute to deception, ignore substantiated repeated abuse, or design systems that profit from foreseeable harm without proportionate controls. Conversely, regulation must guard against over-removal, arbitrary account restrictions, and private censorship. Due process requires notice, reasons, review, and correction where feasible.

Consumer redress should combine internal complaints, regulatory pathways, alternative dispute resolution, and courts. Internal mechanisms provide speed but may lack independence; regulators identify systemic conduct but may not compensate every claimant; courts provide authority but can be costly and slow. Integrated design allows escalation according to complexity and stakes. Collective mechanisms may be necessary where a breach or platform practice affects many persons with individually modest loss. Protection also requires communication that avoids secondary harm. Institutions should not use technical language to obscure decisions or imply that all victims were careless. Staff need training in trauma-informed and culturally accessible responses. Public warnings should protect potential victims without disclosing unnecessary personal information or compromising investigations. Reliable statistics should distinguish attempted incidents, confirmed losses, recovered funds, and data breaches to avoid both complacency and sensationalism.

An Integrated Digital Economic Security Governance Framework

The proposed Integrated Digital Economic Security Governance framework connects seven components. The first is a shared risk taxonomy covering offence methods, affected services, data types, transaction channels, losses, and systemic indicators. A common taxonomy enables institutions to recognize that apparently separate complaints form part of one campaign. It also supports evidence-based regulation and public reporting. The second component is prevention by design. Regulated and high-risk platforms should conduct documented assessments before launching or materially changing services. Assessments should address authentication, fraud scenarios, vulnerable users, data minimization, vendor dependencies, incident response, and recovery. Independent testing should be proportionate to systemic importance. Regulators should evaluate outcomes rather than accepting policy documents as proof of effectiveness.

The third component is differentiated platform duty. Obligations should be calibrated to function, scale, risk, and control. All providers owe baseline security and cooperation duties. Transactional and identity-intensive platforms owe enhanced monitoring, verification, complaint, preservation, and transparency duties. Systemically important providers owe resilience testing, independent audit, crisis coordination, and stricter reporting. This structure avoids treating every digital actor identically while ensuring that powerful intermediaries internalize foreseeable risks. The fourth component is coordinated enforcement and evidence readiness. A national protocol should define reporting routes, preservation standards, referral thresholds, emergency contacts, and lawful information exchange. It should connect police, prosecutors, regulators, cybersecurity bodies, data-protection institutions, financial providers, and platforms. Periodic joint exercises should test ransomware, payment fraud, data breach, and cloud-provider scenarios. Lessons should result in revised controls and published non-sensitive findings.

The fifth component is victim-centred remedy. Service standards should specify acknowledgement, containment, investigation, communication, and decision timelines. Victims should receive a coherent explanation of which institution is responsible for freezing funds, correcting data, investigating offences, and deciding compensation. Outcomes should be reviewable. Aggregate complaint data should inform supervision and product redesign. The sixth component is accountable cross-border cooperation. Indonesia needs efficient preservation and evidence channels supported by specialized contact points and standardized legal requests. Cooperation must incorporate legality, necessity, proportionality, data security, and contestability. Public reporting on aggregate requests and outcomes can strengthen legitimacy without exposing operations.

The seventh component is continuous evaluation. Cyber risk evolves as criminals adapt to controls, artificial intelligence reduces the cost of impersonation, and new payment or identity systems emerge. Governance cannot rely on static compliance. Metrics should include prevention, detection, response, recovery, repeat harm, consumer outcomes, institutional learning, and distributional impact. Independent evaluation can determine whether rules improve security or merely add paperwork. Implementation should occur in phases. The first phase maps mandates, reporting channels, data standards, and critical dependencies. The second establishes pilot information exchange and joint incident protocols in high-risk financial and marketplace sectors. The third evaluates effectiveness, legal safeguards, costs, and unintended exclusion. The fourth scales successful mechanisms and integrates them with international cooperation. Smaller actors should receive templates, shared tools, and technical assistance so that proportionality does not become abandonment.

The framework is consistent with responsive regulation. Education and guidance occupy the base of the regulatory pyramid; supervision, remediation orders, administrative sanctions,

license restrictions, and criminal enforcement escalate according to risk, harm, culpability, and responsiveness. Escalation should be credible, but authorities should also reward verified improvement and transparent reporting. Organizations may otherwise conceal incidents to avoid punishment, weakening collective learning. Rights remain central. Security measures can themselves intrude on privacy, expression, access, and procedural fairness. Identity verification may exclude persons lacking conventional documentation; automated fraud systems may discriminate; transaction monitoring may expand surveillance; and rapid removal may suppress legitimate conduct. Each intervention therefore requires purpose limitation, data minimization, human review, accessible challenge, and periodic testing for unequal effects. A secure digital economy is not one in which all activity is monitored, but one in which power is constrained and foreseeable harm is responsibly managed.

The model also clarifies the relationship between innovation and regulation. Innovation benefits from trust, predictable duties, and interoperable standards. Regulatory sandboxes should test not only commercial viability but also security, consumer outcomes, data governance, and exit arrangements. A product that scales before these questions are addressed can externalize risk to users and the public. Conversely, outcome-based rules and controlled experimentation can avoid prescribing technology that quickly becomes obsolete. Ultimately, digital security is a public value produced through distributed action. Government establishes legitimate rules and institutional capacity; law enforcement disrupts offenders; regulators supervise systemic conduct; firms design and operate secure services; platforms respond to abuse; and users exercise informed care. The allocation is not equal because capabilities are unequal. Actors with greater knowledge, control, and benefit should bear correspondingly greater duties. This principle gives normative coherence to the framework and prevents consumer responsibility from becoming a substitute for institutional accountability.

Corporate Responsibility, Compliance, and Regulatory Coordination

Corporate responsibility in the digital economy should be understood as an organizational duty rather than a search for one negligent employee after an incident. Cybersecurity outcomes arise from decisions about governance, investment, staffing, product development, outsourcing, incentives, and escalation. A company that promotes rapid onboarding while underinvesting in verification creates a foreseeable tension between commercial growth and fraud exposure. A provider that collects extensive data without retention limits expands the consequences of a breach. Legal evaluation should therefore examine whether management established a reasonable system for identifying, controlling, and responding to material cyber risks.

This organizational perspective is compatible with corporate criminal liability but should not collapse every control failure into a criminal offence. Criminal responsibility ordinarily requires a legally defined offence and attributable fault. Administrative and civil mechanisms are more suitable for many governance deficiencies, particularly where harm results from weak controls rather than deliberate facilitation. A calibrated enforcement pyramid can reserve criminal sanctions for intentional assistance, concealment, obstruction, serious recklessness, or repeated noncompliance producing grave harm. Remediation orders, compensation, governance requirements, and administrative penalties can address lesser but still consequential failures.

Compliance should be demonstrable. Written policies are necessary but insufficient when access logs are not reviewed, incident exercises are never conducted, vendors are not assessed, or complaints are routinely closed without analysis. Providers should maintain evidence of risk assessments, control testing, training, response decisions, recovery performance, and corrective action. Documentation supports supervision and legal accountability, but regulators must avoid encouraging paperwork that diverts resources from actual security. The relevant question is

whether records demonstrate that controls work and that institutions learn from incidents. Senior accountability improves the connection between legal obligation and operational practice. Boards should define risk appetite, approve critical policies, and challenge management about unresolved exposure. Named executives should coordinate security, fraud, privacy, consumer protection, and continuity functions. Separation remains necessary to preserve independent challenge, yet organizational silos should not prevent shared analysis. A surge in failed logins, complaints, password resets, and unusual transfers may be individually managed by separate teams but collectively indicate an active campaign.

Regulatory coordination should adopt a lead-and-support model. The institution with the clearest mandate for the principal issue coordinates the response, while other competent bodies contribute according to their powers. Leadership may change as facts develop: an apparent service complaint can reveal a systemic data breach and organized fraud. A joint protocol should identify triggers for referral, information that may be shared, confidentiality limits, urgent measures, and responsibility for communication. This avoids both duplicated directions and gaps created when every body assumes another is acting. Supervisory technology can improve coordination by enabling standardized reporting, trend analysis, and risk prioritization. Its use must be transparent and secure. Automated tools should not determine sanctions without accountable human assessment, and reported data must be validated (Organisation for Economic Co-operation and Development, 2022). Smaller providers may require simplified interfaces and clear definitions. The objective is a common operational picture, not an unlimited centralized database. Data architecture should incorporate access limitation, audit trails, retention rules, and separation between supervisory intelligence and evidence used in criminal proceedings.

Public-private cooperation is equally important because providers observe incidents before authorities possess a complete picture. Cooperation should be institutionalized rather than dependent on informal personal relationships. Sector groups can exchange indicators, coordinate warnings, and conduct exercises, while public agencies provide threat intelligence and legal guidance. Participation rules should prevent dominant firms from using security exchanges to obtain competitive information or exclude smaller actors. Aggregated lessons should be made available to the wider ecosystem when disclosure does not create additional risk.

Artificial Intelligence, Emerging Risks, and Sustainable Digital Trust

Artificial intelligence changes both offending and defence. Generative systems can produce persuasive messages, imitate organizational style, translate scams, create synthetic documents, and support voice or image impersonation (World Economic Forum, 2024). Automation reduces the cost of personalization, weakening older advice that fraudulent communication is easily recognized through poor language. Defensive systems can detect anomalies and prioritize alerts, but they may also generate false positives, reproduce historical bias, and be difficult to explain. Law should regulate outcomes, governance, and high-risk uses rather than assuming that technology is inherently protective or harmful.

Authentication practices must adapt to synthetic media. Voice, images, and apparent video presence should no longer be treated as conclusive identity proof. High-risk transactions require independent channels, cryptographic or device-based signals, contextual verification, and procedures for unusual requests. Organizations should establish internal protocols for urgent payment instructions, changes of beneficiary accounts, and executive impersonation. Public education should emphasize verification through known channels without creating generalized distrust in all digital communication. AI-enabled monitoring raises questions of privacy and equality (Organisation for Economic Co-operation and Development, 2024). Models may use device, location, behaviour, network, and transaction variables to assign risk.

Some variables correlate with poverty, disability, geographic isolation, or patterns associated with particular communities. Providers should test error rates and impacts across relevant groups, document features and purposes, and offer human review of consequential decisions. Fraud prevention cannot justify opaque exclusion from essential services. Data minimization remains relevant even when additional data may marginally improve prediction.

The state also needs capacity to audit algorithmic systems used in regulated sectors. This does not necessarily require disclosure of all source code. Regulators may examine documentation, training data governance, validation, performance thresholds, incident logs, vendor arrangements, and independent testing. Where providers rely on external models, contractual secrecy cannot defeat statutory supervision. Responsibility remains with the regulated entity for the system it chooses to deploy. Sustainable digital trust depends on institutional honesty. Claims that a service is completely secure are unrealistic and may discourage reporting. Trust is strengthened when institutions disclose material risks, respond promptly, admit failures, compensate fairly, and demonstrate improvement. Transparency must be calibrated so that it informs users without revealing exploitable details. Independent assurance and aggregate incident reporting allow the public to assess whether the ecosystem is becoming more resilient.

The distributional dimension is essential. Cybercrime often harms people who cannot absorb financial loss or retain professional assistance. Security controls can also impose higher burdens on older persons, persons with disabilities, rural users, migrant workers, and microenterprises. Inclusive design requires accessible interfaces, alternative verification, multilingual assistance, and non-digital channels for urgent support. Evaluation should measure who is protected, who is excluded, and who bears residual loss. The framework therefore links sustainability to institutional resilience and social inclusion. A digital economy cannot be considered sustainable if growth depends on persistent externalization of fraud, privacy, and recovery costs to users. Investment in security, competent enforcement, and effective redress is productive infrastructure. It preserves participation, reduces repeated harm, and supports legitimate innovation. Over time, the strongest indicator of success is not the absence of reported incidents, which may reflect underreporting, but improved detection, faster containment, greater recovery, fewer repeated weaknesses, and fairer outcomes.

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

Indonesia's digital economy has expanded opportunity while creating an environment in which fraud, identity theft, unlawful access, data breaches, ransomware, and payment abuse can operate at scale. The legal system already contains important foundations in the Electronic Information and Transactions Law, the Personal Data Protection Law, electronic-system regulation, criminal law, and financial-sector rules. The central weakness is not a complete absence of law, but fragmentation among preventive obligations, criminal enforcement, sectoral supervision, and victim remedies. The study finds that effective protection requires three connected transitions. Prevention must move from generic awareness toward security and fraud resistance by design. Enforcement must move from isolated case processing toward rapid preservation, reliable digital forensics, financial tracing, strategic disruption, and rights-respecting cross-border cooperation. Protection must move from complaint formalities toward containment, recovery, identity restoration, understandable communication, and reviewable decisions. Platform responsibility should be differentiated according to function, scale, knowledge, risk, and capacity.

The Integrated Digital Economic Security Governance framework provides a reconstruction based on a shared risk taxonomy, prevention by design, differentiated duties, coordinated enforcement, victim-centred remedies, accountable international cooperation, and

continuous evaluation. Its implementation should begin with mandate mapping, interoperable reporting, pilot protocols in high-risk sectors, independent evaluation, and phased scaling. Cybersecurity should be understood as a legal and institutional condition of trustworthy economic participation, not merely a technical expense or an issue addressed after criminal harm occurs.

Limitations

This study is doctrinal and relies primarily on legislation, regulatory materials, institutional publications, and scholarly literature. It does not measure incident prevalence, victim recovery rates, institutional response times, or the practical operation of reporting and evidence-preservation mechanisms. Rapid technological and regulatory change may also affect the continuing application of particular rules and risk categories. The findings should therefore be understood as a normative and institutional framework requiring empirical validation across sectors and regions.

Recommendations

Future empirical research should evaluate reporting journeys, recovery rates, institutional response times, and the distributional effects of fraud controls. Such evidence is necessary to refine proportionality and ensure that security measures do not exclude legitimate users. The enduring objective is a digital economy in which innovation and protection reinforce one another through clear responsibility, capable institutions, effective remedies, and respect for rights.

Author Contributions

All authors contributed to the conceptualization, legal analysis, development of the governance framework, manuscript preparation, critical revision, and final approval of this article.

REFERENCES

- Bank Indonesia. (2023). Indonesia payment systems blueprint and payment-system policy materials. <https://www.bi.go.id>
- Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1), tyac014. <https://doi.org/10.1093/cybsec/tyac014>
- European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. Publications Office of the European Union.
- Financial Services Authority. (2023). Financial Services Authority Regulation Number 22 of 2023 concerning consumer and public protection in the financial services sector.
- Financial Services Authority. (2024a). Financial Services Authority Regulation Number 3 of 2024 concerning the implementation of financial sector technology innovation.
- Financial Services Authority. (2024b). Cybersecurity guidelines for financial sector technology innovation providers. <https://ojk.go.id>
- Financial Services Authority. (2025). Cybersecurity guideline for digital financial asset trading operators. <https://ojk.go.id>
- Financial Services Authority. (2026). Governance and risk management for financial sector technology innovation and digital financial assets. <https://ojk.go.id>
- Giova, C. (2023). Electronic evidence management under the Budapest Convention: Principles and contemporary challenges. *International Information Security Research Journal*, 7(2), 41–58.
- Indonesia. (2008). Law Number 11 of 2008 concerning electronic information and transactions.

- Indonesia. (2019). Government Regulation Number 71 of 2019 concerning the operation of electronic systems and transactions.
- Indonesia. (2022). Law Number 27 of 2022 concerning personal data protection.
- Indonesia. (2023). Law Number 1 of 2023 concerning the Criminal Code.
- Indonesia. (2024). Law Number 1 of 2024 concerning the second amendment to Law Number 11 of 2008 concerning electronic information and transactions.
- Internet & Jurisdiction Policy Network. (2021). Toolkit: Cross-border access to electronic evidence. <https://www.internetjurisdiction.net>
- INTERPOL. (2024). Global financial fraud assessment. INTERPOL.
- Organisation for Economic Co-operation and Development. (2022). OECD policy framework on digital security. OECD Publishing.
- Organisation for Economic Co-operation and Development. (2024). Consumer vulnerability in the digital age. OECD Publishing.
- Rosyidah, A. A. (2024). Cybercrime against women's personal data in financial technology services. *Jurnal Kajian Media dan Informasi*, 13(2), 137–158.
- United Nations Office on Drugs and Crime. (2021). Practical guide for requesting electronic evidence across borders. United Nations.
- World Bank. (2022). Digital financial services and consumer risks: Supervisory approaches for emerging markets. World Bank.
- World Economic Forum. (2024). Global cybersecurity outlook 2024. World Economic Forum.
- Zhang, H. (2024). The research on an electronic evidence forensic system for cross-border cybercrime. *International Journal of Evidence & Proof*, 28(2), 147–168. <https://doi.org/10.1177/13657127231187059>