JURNAL KONSTATERING
published by
Master of Notary Law, Faculty of Law
Sultan Agung Islamic University
Volume 5 No. 1, January 2026
ISSN: 2828-4836
https://garuda.kemdiktisaintek.go.id/journal/view/43046

Notary Public Responsibility for the Implementation of Cyber Resilience and Business Continuity Plan as a Legal Obligation in the Governance of the Notary Profession

Kholidin Alkhalifi Atmadinata
Faculty of Law, Universitas Islam Sultan Agung, Semarang, Indonesia, E-mail: kholidin.atmadinata@gmail.com

Abstract. *The digital transformation of notarial practice has expanded the exposure of notarial offices to cyber disruption, while Indonesian law still lacks an explicit norm obliging notaries to implement cyber resilience and a business continuity plan (BCP). This study examines the legal position of that obligation and formulates a regulatory model to close the resulting normative gap. Employing normative legal research with statutory, conceptual, and case approaches, the analysis applies Radbruch's construction of legal certainty, the risk management theory of Mehr and Hedges, and the doctrine of legal liability, complemented by an Islamic law perspective. The study finds, first, that cyber notary in Indonesia operates in a hybrid form in which the digitalized pre- and post-deed stages coexist with a conventional execution stage, producing nine structural weaknesses. Second, cyber resilience and BCP already constitute an implicit legal obligation derived from the notarial office duty, the duties of a personal data controller, and the duties of an electronic system operator; what is absent is not the legal basis but the standard. Third, the obligation should be transformed into an explicit, tiered, and technology-neutral norm, and can be operationalized immediately through cyber resilience clauses within notarial provisions under Article 15(1) of the Notary Office Law.*

Keywords: *Business; Cyber; Legal; Notary; Resilience.*

1. Introduction

A notary is a public official who is authorized to make authentic deeds and has other powers as determined by law.[1]This authority is attributive, obtained directly from the law and not from the parties who use his services, so that the position of Notary is attached to the state's function in guaranteeing legal

1 Law of the Republic of Indonesia Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning the Position of Notary, Article 1 number 1, State Gazette of the Republic of Indonesia 2014 Number 3, Supplement to the State Gazette of the Republic of Indonesia Number 5491.

certainty in the field of civil law.[2]The consequence of this position is that the failure of a Notary to maintain his/her official instruments not only harms the client individually, but also erodes the evidentiary value of authentic deeds as an institution.

For more than a century and a half, the instruments of office were physical: minutes of deeds on paper, protocols in filing cabinets, and services conducted in offices. The framework of the Notary Law was formulated with this assumption in mind. However, Indonesian notarial practice in the last decade has shifted substantially to electronic means, from communication with clients and the preparation and storage of work files to reporting and registration through electronic government systems. This shift has occurred more rapidly than the normative adjustments.[3]

The problem isn't just regulatory delays, but rather the changing nature of the risks faced by offices. Conventional risks like fire or document loss are local, visible, and can be mitigated with physical security measures. Cyber risks are remote, invisible, and can cripple an office's entire electronic archives in minutes without leaving any immediately visible traces. Threats like ransomware, database breaches, and identity theft attack precisely the three attributes that underpin the evidentiary value of documents: confidentiality, integrity, and availability.[4]

Indonesian notarial literature has addressed this issue, but with a distinctive emphasis. Most studies focus on the validity of electronic deeds and the authority of cyber notaries, namely, whether deeds can be created electronically and what the regulatory and technical obstacles are.[5]Others discuss the responsibility of Notaries for protecting clients' personal data after the Personal Data Protection Law comes into effect.[6]These studies are important, but both stop at the descriptive normative level: pointing out the gaps, then recommending that the government create regulations.

There is an unfilled gap between these two streams. First, no study has yet positioned cyber resilience and service continuity as a single job obligation, rather than as separate issues of data security and operational continuity.

2GHS Lumban Tobing, Regulations on the Position of Notary (Jakarta: Erlangga, 1983), 31.

3Puteri Chintami Oktavianti, "Regulatory and Technical Barriers Related to the Implementation of Cyber Notary in Indonesia," Journal of Indonesian Legal Development 6, no. 2 (2024): 243–259, https://doi.org/10.14710/jphi.v6i2.243-259.

4Meta Andriani, Ade Padiya, and Maria Ulfah, "Digital Transformation in Notary Practice: A Legal Analysis of the Implementation of Cyber Notary in Indonesia," Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory 3, no. 2 (2025): 2006–2014, https://doi.org/10.62976/ijijel.v3i2.1202.

5Oktavianti, "Regulatory and Technical Barriers," 245–248.

6Ahmad Najib, "Legal Protection of Cyber Notary Data Security Based on the Personal Data Protection Law," Acta Diurnal: Journal of Notary Law 7, no. 1 (2023): 43–59, https://doi.org/10.23920/acta.v7i1.1680.

Second, and more fundamentally, no study has examined whether these obligations truly lack a legal basis, or whether they do exist but lack standards. The distinction between these two possibilities determines the nature of the solution: the first requires the creation of new norms, the second requires the derivation and standardization of existing norms. Third, no study has yet offered a solution that notaries can pursue without waiting for regulatory changes.

This article answers three questions: What is the current state of cyber notary implementation in Indonesia, and what are its inherent weaknesses? Is implementing a cyber resilience and business continuity plan a recommendation or a legal obligation? What regulatory and operational models can address these gaps?

This article's contribution is both theoretical and practical. Theoretically, it proposes a repositioning: cyber resilience is treated not as a technological issue inherent in notarial practice, but as a derivative obligation of existing official obligations, shifting the issue from a lack of legal basis to a lack of standards. Practically, it formulates a hierarchical model of obligations proportional to the scale of the office and provides readily applicable deed clauses.

2. Research Methods

This research is a normative legal study that places legal norms as the object of study. The choice of this method is based on the nature of the problem, namely examining the position of an obligation within the prevailing normative framework, rather than empirically measuring notary compliance behavior. It should be emphasized from the outset that the consequence of this choice is limited empirical generalization: the findings of this article describe how the law should be read, not how extensive cybersecurity practices have been implemented in Indonesian notary offices.

Three approaches were used simultaneously. The statute approach was used to explore and reconcile norms scattered across the Notary Law, the Electronic Information and Transactions Law, the Personal Data Protection Law, and their implementing regulations, while identifying any disharmonies among them. The conceptual approach was used to develop an analytical framework for the concepts of cyber resilience, business continuity plans, and job responsibilities, which lack normative equivalents in Indonesian notary law. The case approach was used on a limited basis to test the framework against real-life operational disruptions.

Primary legal materials include the aforementioned laws and regulations along with the Civil Code. Secondary legal materials include books, accredited journal articles, and relevant international standards, particularly ISO 31000:2018, ISO 22301:2019, and the NIST Cybersecurity Framework 2.0. These standards are not

treated as legal sources, but rather as materials that help provide content to the concept of prudence, which in notarial law is still formulated abstractly. All materials were collected through literature review and analyzed descriptively and qualitatively using deductive reasoning.

The analysis is conducted through three mechanisms. Gustav Radbruch's construct of legal certainty is used to test the quality of existing norms. Mehr and Hedges' risk management theory is used to assess the adequacy of risk management as a precautionary measure. The doctrine of legal responsibility is used to map the legal consequences of failure to implement it. Complementarily, a review of Islamic law is used to test whether conclusions drawn from positive law are supported by other normative frameworks.

3. Results and Discussion

3.1. Overview and Weaknesses of Cyber Notary Implementation in Indonesia

The term cyber notary gained its first normative footing in the Explanation of Article 15 paragraph (3) of the Notary Law, which states that the authority to certify transactions carried out electronically is one of the other authorities of a Notary.[7] The foothold was never followed by implementing regulations, so for more than a decade it served as a door that was opened but never passed through.

In practice, what has developed is not a cyber notary in the full sense, but rather a hybrid form. Digitization has reached the pre- and post-deed drafting stages, while the deed formalization stage remains conventional. At the pre-deed stage, sending required documents, reviewing drafts, and initial identity verification takes place via email, messaging apps, and video calls. At the deed drafting stage, the only legal act that can explicitly take place electronically is the General Meeting of Shareholders via teleconference, as stipulated in Article 77 of the Limited Liability Company Law.[8] At the post-deed stage, digitalization is mandatory: legal entity validation, fiduciary guarantee registration, will reporting, and electronic land services are all carried out through the government's electronic system.[9] At the inauguration stage, the reading and signing were still carried out physically.

This picture raises an often overlooked implication. Because the entire ecosystem supporting notarial deeds is now electronic, cybersecurity threats don't need to affect the deeds themselves to cripple notarial services. The

7Law Number 2 of 2014, Explanation of Article 15 paragraph (3).

8Law of the Republic of Indonesia Number 40 of 2007 concerning Limited Liability Companies, Article 77, State Gazette of the Republic of Indonesia 2007 Number 106, Supplement to the State Gazette of the Republic of Indonesia Number 4756.

9Regulation of the Minister of Agrarian Affairs and Spatial Planning/Head of the National Land Agency Number 1 of 2021 concerning Electronic Certificates, State Gazette of the Republic of Indonesia 2021 Number 78.

encryption of work files by ransomware, the loss of access to government systems, or the leak of client databases are enough to halt services and cause losses. In other words, the argument that notarial deeds are still physically executed and therefore safe from cyber risks misrepresents the object of the risk.

From this description, nine structural weaknesses can be identified. The first weakness is normative in nature, in the form of disharmony between norms: Article 15 paragraph (3) of the Notary Law opens up the authority of cyber notaries, Article 16 paragraph (1) letter m of the same law requires the physical presence of the person appearing, while Article 5 paragraph (4) letter b of the Electronic Information and Transactions Law actually excludes documents that must be in the form of a notarial deed from the definition of electronic documents that are valid as evidence.[10]These three norms have never been harmonized.[11]

The second weakness concerns meeting the requirements for authenticity. Article 1868 of the Civil Code requires that an authentic deed be drawn up by or before an authorized public official at the location where the deed is drawn up.[12] Holding meetings via teleconference raises issues regarding venue selection and meeting the required requirements, especially when participants are located in different positions. A third weakness concerns identity and intent verification: video call verification is not equivalent to a physical identity document check, while advances in facial and voice impersonation technology increase the risk of impersonation without mandatory biometric verification.[13]

The fourth weakness concerns the lack of regulation of electronic minutes and protocols. All protocol provisions in the Notary Law are formulated based on the assumption of physical documents, thus lacking standards regarding storage formats, guarantees of long-term legibility, mechanisms for submitting digital protocols, or procedures for their destruction.[14] The fifth weakness concerns the lack of binding information security standards, so the use of personal email, free cloud services without data processing agreements, and shared passwords is still common.

10Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024, Article 5 paragraph (4) letter b.

11Dinda Fauziah, "Challenges in Applying the Cyber Notary Concept to the Authority to Make Authentic Deeds by Notaries," Al-Zayn: Journal of Social Sciences & Law 3, no. 4 (2025): 4949–4958, https://doi.org/10.61104/alz.v3i4.2067.

12Civil Code (Burgerlijk Wetboek), Article 1868.

13Syahrul Abdillah and Hendra Hadi Saputra, "The Urgency of Cyber Notary Regulation in Supporting Legal Certainty in the Digital Era," Lex Stricta: Jurnal Ilmu Hukum 4, no. 1 (2025): 1–12, https://doi.org/10.46839/lexstricta.v4i1.1367.

14Anisa Sitaresmi and Rosa Ristawati, "Post-Mortem Personal Data Protection by Notaries Through Notarial Protocol Storage: Prospects and Challenges," Halu Oleo Law Review 9, no. 1 (2025): 42–58, https://doi.org/10.33561/holrev.v9i1.125.

The sixth weakness concerns human resource readiness and infrastructure gaps between regions. The seventh weakness concerns oversight: the Notary Supervisory Board lacks the instruments and competence to review information technology aspects, so periodic inspections are still limited to physical protocols.[15] The eighth weakness concerns the continuity of service, which is exacerbated by the Notary's office's dependence on a single key figure; if the Notary is absent or their equipment is damaged, access to the system can be lost entirely. The ninth weakness concerns the lack of a standard for distinguishing between force majeure and negligence, which is detrimental to both parties: it is difficult for the parties to claim compensation, while the Notary is uncertain about the limits of his or her duty of care.

3.2. Cyber Resilience and BCP as Legal Obligations, Not Recommendations

The core question of this article is whether implementing a cyber resilience and business continuity plan is a recommendation or a legal obligation. This distinction is not a matter of terminology. If it is merely a recommendation, failure to implement it has no legal consequences, and a notary who loses all of their electronic records due to failure to perform backups is in the same position as one who has done everything properly. If it is an obligation, such failure opens them up to liability.

This article argues that both have the status of legal obligations, with three sources that reinforce each other.

The first source is the law of office. Article 16 paragraph (1) letter a of the Notary Law requires Notaries to act in a trustworthy, honest, thorough, independent, impartial manner and to protect the interests of the related parties; letter b requires Notaries to make and keep minutes of deeds as part of the protocol; and letter f requires Notaries to keep confidential everything regarding the deeds they make.[16] These three obligations are imperative and allow no exceptions based on the medium. In digitalized practices, the obligation to store and maintain confidentiality cannot be fulfilled without system security and recovery. The obligation to implement cyber resilience and BCP is therefore a derivative obligation inherent in the primary obligation, and the nature of the primary obligation is contagious to the medium. Article 65 of the same law reinforces this reasoning by emphasizing that a notary remains responsible for the deeds they draft even after the protocol has been submitted.[17]

The second source is data protection law. The Personal Data Protection Law places Notaries as controllers of personal data and requires them to protect and

15Yulia Marlina, Ifrani Faniyah, and Syofiarti, "Guidance and Supervision of Notaries in Efforts to Enforce the Duties and Functions of the Position by the Regional Supervisory Board," Unes Journal of Swara Justisia 9, no. 3 (2025): 549–558, https://doi.org/10.31933/6ct0z286.

16Law Number 2 of 2014, Article 16 paragraph (1) letters a, b and f.

17Law Number 2 of 2014, Article 65.

ensure the security of the data they process, along with the obligation to notify failures in data protection within specified deadlines, with the threat of administrative or criminal sanctions.[18] This obligation applies directly without requiring the intermediary of the Notary Law, and it is precisely at this point that the Notary's information security obligation obtains the firmest basis in Indonesian positive law.[19]

The third source is electronic transaction law. Article 15 of the Electronic Information and Transactions Law requires every electronic system provider to operate its system reliably and securely and to be responsible for ensuring the system operates properly.[20] which is further detailed in the Government Regulation concerning the Implementation of Electronic Systems and Transactions.[21] As long as the Notary's office maintains an electronic system for the purposes of its services, this obligation also applies to it.

These three sources yield one important conclusion that needs to be stated explicitly: what is missing in Indonesian law is not the basis for the obligation, but rather its standards and measurements. The common assertion in the literature that there is a legal vacuum regarding notaries' obligations in the field of cybersecurity therefore needs to be refined. The true vacuum lies not in the fundamental level of the obligation, but in the technical norms that provide measurable content to that obligation.

The consequences of liability are multi-layered. Administratively, failure to manage information security can result in sanctions from the Supervisory Board. Civilly, negligence that results in losses can be classified as an unlawful act as long as it meets the elements of fault, loss, and a causal relationship. Criminally, liability only arises if there is an element of intent or gross negligence, so not every cyber incident gives rise to criminal liability. Ethically, failure to maintain the confidentiality of client data violates the integrity and prudence requirements of the Notary Code of Ethics.[22]

3.3. Testing with Radbruch's Legal Certainty Construction

18Law of the Republic of Indonesia Number 27 of 2022 concerning Protection of Personal Data, Article 35 and Article 46, State Gazette of the Republic of Indonesia 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820. [NEED TO VERIFY the numbering of the article on notification of data protection failure]

19Jihan Alifia, Denny Benny, and Sofyan Maman, "Notary's Responsibilities in Protecting Client's Personal Data Based on Law No. 27 of 2022 concerning Personal Data Protection," Journal of Law, Humanities and Politics 5, no. 1 (2024): 653–662, https://doi.org/10.38035/jihhp.v5i1.3204.

20Law Number 11 of 2008, Article 15.

21Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, State Gazette of the Republic of Indonesia 2019 Number 185.

22Salsabila Khairunnisa, "Repositioning the Notary Organization in the Statutory Regulatory System by Examining the UUJN and Permenkum 24 of 2025," Notaire 9, no. 1 (2026): 127–142, https://doi.org/10.20473/ntr.v9i1.82985.

Gustav Radbruch built the doctrine of legal certainty on four elements: that positive law is statute; that law is based on facts, not on the formulation of judgments that are only determined later by judges; that these facts must be formulated clearly so as to avoid misinterpretation and be easy to implement; and that positive law should not be changed frequently.[23] These four elements function as tools for testing the quality of norms, not merely as values to be aspired to.[24] Tested against these four elements, the current legal situation demonstrates a systematic failure. In the first element, notaries' cyber resilience obligations do have a basis, but this basis is spread across three different laws and must be derived through reasoning, not read directly from the text. For notaries in regions without access to legal assistance, an obligation that can only be discovered through multi-level reasoning is practically the same as a non-existent obligation.

In the second element, the assessment of whether or not a notary was negligent in the current cyber incident relies on an abstract standard of reasonableness, specifically a formulation of an assessment that will only be determined later by the judge a point Radbruch rejects. Yet observable and measurable facts are readily available: the presence or absence of data backups, audit trails, encryption, and proven recovery procedures. In the third element, the absence of minimum standards leaves the norm of prudence open to differing interpretations among notaries, the supervisory board, and judges. In the fourth element, the absence of norms actually invites instability, as regulations that are later established reactively after a major incident tend to be formulated technically and therefore quickly become outdated. This test yields specific normative implications. The required norm is not one that specifies a specific technology, but rather a principle-based and outcome-based norm that specifies what should be achieved integrity, confidentiality, and availability of minutes and data while leaving the choice of means to technological developments. This technology-neutral formulation satisfies the fourth element of Radbruch's construct while remaining within the third.

3.4. Adequacy of Risk Management as a Prudential Measure

If obligations exist but standards do not, the next question is where to draw the content of those standards. Risk management theory provides the framework. Mehr and Hedges, who laid the foundation for risk management as a discipline independent of insurance, defined risk management as a five-stage cycle: risk identification, measurement and evaluation, selection of treatment techniques,

23Gustav Radbruch as quoted in Satjipto Rahardjo, Ilmu Hukum (Bandung: Citra Aditya Bakti, 2014), 19–20. [PLEASE VERIFY the page numbers on the print used]

24Gustav Radbruch, “Statutory Lawlessness and Supra-Statutory Law (1946),” trans. Bonnie Litschewski Paulson and Stanley L. Paulson, Oxford Journal of Legal Studies 26, no. 1 (2006): 1–11, https://doi.org/10.1093/ojls/gqi041.

decision implementation, and periodic evaluation and review.[25] Williams and Heins expanded its coverage to include property, liability, legal, and personnel risk exposures.[26] The value of this framework for notarial law lies in its ability to translate abstract precautions into a verifiable course of action. A notary who has never identified their risk exposure cannot claim to have acted prudently, as due care requires knowledge of what to guard against. Conversely, a notary who has followed all five steps has a factual basis for proving that the incident occurred beyond the limits of reasonable control.

At the operational level, the theoretical framework has been standardized in international standards: ISO 31000:2018 for risk management processes,[27]NIST Cybersecurity Framework 2.0 which structures cyber risk management into the functions of govern, identify, protect, detect, respond, and recover,[28]and ISO 22301:2019 for business continuity management systems.[29]These standards are not sources of law and cannot be treated as binding norms. Their purpose is different: they serve as tested material to provide substance to abstract legal concepts, just as professional standards in other fields are commonly used to determine the limits of appropriate action. This framework can also be used to formulate a standard for distinguishing between force majeure and negligence, which has previously been lacking. A cyber incident is considered force majeure if the Notary can demonstrate that the risk has been identified, assessed, handled with proportionate techniques, and periodically reviewed, yet it still occurred. Conversely, an incident involving a risk that was never identified at all is difficult to qualify as force majeure, as ignorance of a reasonably foreseeable risk is itself a form of negligence.

3.5. Review of Islamic Law

As a cross-examination, conclusions derived from positive law can be examined against the Islamic legal framework. Within the *maqasid al-syari'ah* framework, notarial deed minutes and protocols are instruments of *hifz al-mal* because they serve as evidence of ownership and obligations over assets, while the parties' personal data falls within the scope of *hifz al-'ird* because its leakage could potentially damage a person's *honor*.[30] Considering that the loss of minutes is

25Robert I. Mehr and Bob A. Hedges, Risk Management in the Business Enterprise (Homewood: Richard D. Irwin, 1963), 6–12. [PLEASE VERIFY page numbers]

26C. Arthur Williams Jr. and Richard M. Heins, Risk Management and Insurance, ed. 6th (New York: McGraw-Hill, 1989), 11.

27International Organization for Standardization, ISO 31000:2018 — Risk Management: Guidelines (Geneva: ISO, 2018).

28National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29 (Gaithersburg: US Department of Commerce, 2024), https://doi.org/10.6028/NIST.CSWP.29.

29International Organization for Standardization, ISO 22301:2019 — Security and Resilience: Business Continuity Management Systems — Requirements (Geneva: ISO, 2019).

30Abu Ishaq al-Syatibi, Al-Muwafaqat fi Usul al-Syari'ah, Volume II (Beirut: Dar al-Kutub al-'Ilmiyyah, 2003), 8–12.

irreversible and results directly in the loss of perfect evidence, protection against it reaches the level of *daruriyyat*, not *tahsiniyyat*. Several Islamic jurisprudence principles support this assessment. The principle of *"la darara wa la dirara"* (the "precautionary principle") prohibits causing harm, so leaving the notary office's work system vulnerable is unjustifiable. The principle of *"dar'u al-mafasid muqaddamun 'ala jalbi al-masalih"* addresses the dilemma between the efficiency of digitalization and its attendant risks: convenience should not be taken at the expense of security.[31] However, the most decisive rule is ma la *muridmu al-wajib illa bihi fa-huwa wajib*, namely that the means which are a condition for the perfection of an obligation also have the status of *wajib*.[32]

The reasoning parallels the positive legal reasoning in the second section. Maintaining the integrity of minutes and maintaining official secrecy are obligations; in digitized practice, these obligations cannot be met without cyber resilience and continuity planning; therefore, both are mandatory. The convergence of conclusions from these two different normative frameworks strengthens this article's argument that the mandatory status is not the result of forced interpretation. It should be added that the acceptance of electronic instruments in *muamalah* has received normative support in Indonesian Islamic law through the recognition of the validity of contracts conducted using modern communication means as long as they fulfill their pillars and requirements.[33]

3.6. Hierarchical Arrangement Model and Operationalization through Deed Clauses

The solution proposed in this article rests on two pillars. The first is a tiered arrangement, and the second is operationalization that can be implemented immediately without waiting for regulations. On the first level, establishing uniform obligations for all Notary offices would impose a disproportionate burden on small, regional offices, and disproportionate obligations are likely to be neglected, thus weakening the norm. Therefore, a distinction is proposed between basic and advanced obligations. Basic obligations apply to all Notaries without exception and include regular data backups with three copies on two types of media, with one copy off-site, device encryption, management of access rights based on the principle of minimum necessity, incident response procedures, and a simple continuity plan that includes storing emergency credentials for replacement Notaries. Advanced obligations are tailored to the size of the office and include information security management system certification, recovery locations, and periodic penetration testing.

31Jalaluddin al-Suyuti, Al-Ashbah wa al-Naza'ir (Beirut: Dar al-Kutub al-'Ilmiyyah, 1990), 83.

32Abu Hamid al-Ghazali, Al-Mustasfa min 'Ilm al-Usul, Volume I (Beirut: Dar al-Kutub al-'Ilmiyyah, 1997), 71.

33Regulation of the Supreme Court of the Republic of Indonesia Number 2 of 2008 concerning Compilation of Sharia Economic Law, Book II concerning Contracts.

The legal instruments are also tiered. In the short term, professional organizations can establish standard guidelines and incorporate cybersecurity competencies into continuing education. In the medium term, Ministerial Regulations can establish minimum standards for digital governance of Notary offices, incident reporting obligations, and the legal status of electronic minutes, while also equipping the Supervisory Board with a digital governance audit checklist. In the long term, amendments to the Notary Law need to harmonize Article 15 paragraph (3) and Article 16 paragraph (1) letter m with the Electronic Information and Transactions Law. On the second leg, there is a road that has so far been underused. Article 15 paragraph (1) of the Law on the Position of Notaries gives the Notary the authority to make deeds regarding all actions, agreements and stipulations desired by interested parties as long as other officials do not exclude them.[34] This authority allows the principles of cyber resilience and service continuity to be incorporated directly into the formulation of the deed, without waiting for implementing regulations.

In the minutes of a meeting held via teleconference, such clauses may include matching each participant's face with their original identity document in front of the camera as a control for the risk of impersonation; recording the meeting proceedings encrypted with hash value recording as a control for the risk of future objections; setting a meeting postponement for a certain period of time in the event of a connection disruption; providing a backup teleconference channel; and affirming the limits of the Notary's liability for network disruptions beyond his control as long as security measures have been implemented. This last clause directly translates the benchmark for distinguishing between force majeure and negligence formulated in the fourth section. The second instrument is a deed of custody for electronic archives, which, through the inclusion of a hash value, allows for authentic proof of the integrity of a file at a specific point in time, and, through the provision of transfer to the notary holding the protocol, addresses the risk of dependence on key figures. Both demonstrate that the gap between ideal norms and prevailing practices does not entirely have to await legislators. It should be noted that the formulation of such clauses is not yet established practice, so their binding force and acceptability in court still require further testing.[35]

4. Conclusion

The implementation of cyber notary services in Indonesia is currently a hybrid process, with digitalization reaching the pre- and post-deed stages, while the official deed formalization stage remains conventional. This approach has given rise to nine structural weaknesses stemming from disharmonious norms, the

34Law Number 2 of 2014, Article 15 paragraph (1).

35Mutiara Dwi Riyanti, "Notary as Responsible Person for Draft Deeds Generated by Artificial Intelligence (AI)," Notaire 8, no. 3 (2025), https://doi.org/10.20473/ntr.v8i3.78295.

absence of information security standards, and the absence of a standard for distinguishing between force majeure and negligence. Because the entire ecosystem supporting deed processing is electronic, cyber disruptions can paralyze notary services without affecting the deed itself. The implementation of cyber resilience and business continuity plans is not a recommendation, but rather an implicit legal obligation stemming from the obligations of a Notary in Article 16 paragraph (1) of the Notary Law, the obligations of personal data controllers, and the obligations of electronic system administrators. The same conclusion is drawn from the Islamic legal framework through the principle of *ma la muridmu al-wajib illa bihi fa-huwa wajib*. Thus, what is not yet available in Indonesian law is not the basis for the obligation, but rather its standards and measurements. The necessary step therefore is to transform implicit obligations into explicit and measurable ones through hierarchical arrangements according to office scale and formulated in a technology-neutral manner, accompanied by the use of the authority of Article 15 paragraph (1) of the Notary Law to include cyber resilience clauses in deeds as a step that can be taken immediately. This article has limitations that need to be acknowledged. As a normative legal study, it does not provide data on the extent to which cybersecurity practices have been implemented in Indonesian notary offices. Therefore, the postulated level of urgency relies on reasoning about the risk structure, not empirical measurement. Further socio-legal research, including surveys of notary offices in regions with varying levels of infrastructure, would test and enrich the hierarchical obligation model proposed here. Empirical testing of the acceptability of cybersecurity clauses in courts is also an open agenda.

5. References

Journals:

Abdillah, Syahrul, dan Hendra Hadi Saputra. "Urgensi Regulasi Cyber Notary dalam Mendukung Kepastian Hukum di Era Digital." *Lex Stricta: Jurnal Ilmu Hukum* 4, no. 1 (2025): 1–12. https://doi.org/10.46839/lexstricta.v4i1.1367.

Alifia, Jihan, Denny Benny, dan Sofyan Maman. "Tanggung Jawab Notaris dalam Perlindungan Data Pribadi Klien Berdasarkan UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi." *Jurnal Ilmu Hukum, Humaniora dan Politik* 5, no. 1 (2024): 653–662. https://doi.org/10.38035/jihhp.v5i1.3204.

Andriani, Meta, Ade Padiya, dan Maria Ulfah. "Transformasi Digital dalam Praktik Kenotariatan: Analisis Yuridis terhadap Penerapan Cyber Notary di Indonesia." *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory* 3, no. 2 (2025): 2006–2014. https://doi.org/10.62976/ijijel.v3i2.1202.

Fauziah, Dinda. "Tantangan Penerapan Konsep Cyber Notary terhadap Kewenangan Pembuatan Akta Otentik oleh Notaris." *Al-Zayn: Jurnal*

Ilmu Sosial & Hukum 3, no. 4 (2025): 4949–4958. https://doi.org/10.61104/alz.v3i4.2067.

Khairunnisa, Salsabila. "Reposisi Organisasi Notaris dalam Sistem Peraturan Perundang-undangan dengan Mengkaji UUJN dan Permenkum 24 Tahun 2025." Notaire 9, no. 1 (2026): 127–142. https://doi.org/10.20473/ntr.v9i1.82985.

Najib, Ahmad. "Perlindungan Hukum Keamanan Data Cyber Notary Berdasarkan Undang-Undang Perlindungan Data Pribadi." *Acta Diurnal: Jurnal Ilmu Hukum Kenotariatan* 7, no. 1 (2023): 43–59. https://doi.org/10.23920/acta.v7i1.1680.

National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. *Gaithersburg: U.S. Department of Commerce*, 2024. https://doi.org/10.6028/NIST.CSWP.29.

Oktavianti, Puteri Chintami. "Hambatan Regulasi dan Teknis Terkait Implementasi Cyber Notary di Indonesia." *Jurnal Pembangunan Hukum Indonesia* 6, no. 2 (2024): 243–259. https://doi.org/10.14710/jphi.v6i2.243-259.

Radbruch, Gustav. "Statutory Lawlessness and Supra-Statutory Law (1946)." Diterjemahkan oleh Bonnie Litschewski Paulson dan Stanley L. Paulson. *Oxford Journal of Legal Studies* 26, no. 1 (2006): 1–11. https://doi.org/10.1093/ojls/gqi041.

Marlina, Yulia, Ifrani Faniyah, dan Syofiarti. "Pembinaan dan Pengawasan Notaris dalam Upaya Penegakan Tugas serta Fungsi Jabatan oleh Majelis Pengawas Daerah." *Unes Journal of Swara Justisia* 9, no. 3 (2025): 549–558. https://doi.org/10.31933/6ct0z286.

Riyanti, Mutiara Dwi. "Notaris sebagai Penerima Tanggung Jawab atas Draft Akta yang Dihasilkan oleh Kecerdasan Buatan (AI)." *Notaire* 8, no. 3 (2025). https://doi.org/10.20473/ntr.v8i3.78295.

Sitaresmi, Anisa, dan Rosa Ristawati. "Perlindungan Data Pribadi Post-Mortem oleh Notaris Melalui Penyimpanan Protokol Notaris: Prospek dan Tantangannya." *Halu Oleo Law Review* 9, no. 1 (2025): 42–58. https://doi.org/10.33561/holrev.v9i1.125.

Books:

Al-Ghazali, Abu Hamid. *Al-Mustasfa min 'Ilm al-Usul*. Jilid I. Beirut: Dar al-Kutub al-'Ilmiyyah, 1997.

International Organization for Standardization. ISO 22301:2019 — Security and Resilience: Business Continuity Management Systems — Requirements. Geneva: ISO, 2019.

International Organization for Standardization. ISO 31000:2018 — Risk Management: Guidelines. Geneva: ISO, 2018.

Lumban Tobing, G. H. S. Peraturan Jabatan Notaris. Jakarta: Erlangga, 1983.

Mehr, Robert I., dan Bob A. Hedges. Risk Management in the Business Enterprise. Homewood: Richard D. Irwin, 1963.
Rahardjo, Satjipto. Ilmu Hukum. Bandung: Citra Aditya Bakti, 2014.
Al-Suyuti, Jalaluddin. Al-Asybah wa al-Naza'ir. Beirut: Dar al-Kutub al-'Ilmiyyah, 1990.
Al-Syatibi, Abu Ishaq. Al-Muwafaqat fi Usul al-Syari'ah. Jilid II. Beirut: Dar al-Kutub al-'Ilmiyyah, 2003.
Williams, C. Arthur, Jr., dan Richard M. Heins. Risk Management and Insurance. Edisi ke-6. New York: McGraw-Hill, 1989.

Regulation:

Civil Code (Burgerlijk Wetboek).
Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024.
Law of the Republic of Indonesia Number 40 of 2007 concerning Limited Liability Companies.
Law of the Republic of Indonesia Number 2 of 2014 concerning Amendments to Law Number 30 of 2004 concerning the Position of Notary.
Law of the Republic of Indonesia Number 27 of 2022 concerning Protection of Personal Data.
Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.
Regulation of the Supreme Court of the Republic of Indonesia Number 2 of 2008 concerning the Compilation of Sharia Economic Law.
Regulation of the Minister of Agrarian Affairs and Spatial Planning/Head of the National Land Agency Number 1 of 2021 concerning Electronic Certificates.