Penyusunan Kebijakan Pengamanan dan Pengelolaan Infrastruktur Operasi Keamanan Siber Menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022

Hafizh Ghozie Afiansyah[1)], Nur Annisa Kadarwati Febriyani[2)]
(1) Badan Siber dan Sandi Negara, hafizh.ghozie@bssn.go.id
(2) Badan Siber dan Sandi Negara, nur.annisa@bssn.go.id

Abstrak

Penelitian ini membahas mengenai pengelolaan dan perlindungan terhadap aset teknologi informasi organisasi terutama untuk operasi keamanan siber dari ancaman siber yang semakin meningkat. Operasi keamanan siber terdiri dari enam kategori kegiatan yang melibatkan perencanaan, pengelolaan, dan pengaturan terhadap aset teknologi informasi. Salah satu standar yang dapat diterapkan dalam pengelolaan dan pengamanan infrastruktur operasi keamanan siber adalah ISO/IEC 27001:2022. Penelitian ini menguraikan integrasi konsep govern pada NIST CSF 2.0 dengan ISO/IEC 27001:2022 untuk merancang kebijakan tata kelola dan manajemen infrastruktur operasi keamanan siber. Kerangka kebijakan ini mencakup tujuan organisasi, penjelasan kegiatan pengelolaan dan pengamanan infrastruktur, rincian kegiatan, ketentuan penerapan, pemantauan, evaluasi, audit internal, ulasan manajemen, perbaikan berkelanjutan, serta dampak dan sanksi jika kebijakan tidak dilaksanakan dengan baik. Penelitian ini bertujuan agar organisasi dapat lebih efektif dalam menghadapi ancaman siber dan memastikan layanan operasi keamanan siber berjalan optimal.

Kata kunci: ISO/IEC 27001, Kebijakan Keamanan Informasi, NIST CSF 2.0, Operasi Keamanan Siber, Tata Kelola Keamanan Siber.

Abstract

This research discusses the management and protection of organizational information technology assets, especially for cyber security operations from increasing cyber threats. Cybersecurity operations consist of six activities that involve planning, managing, and managing information technology assets. A standard that can be applied in managing and securing cyber security operations infrastructure is ISO/IEC 27001:2022. This study describes integrating the govern concept in NIST CSF 2.0 with ISO/IEC 27001:2022 to design governance policies and management of cybersecurity operations infrastructure. This policy framework includes organizational objectives, a description of infrastructure management and safeguard activities, details of activities, provisions for implementation, monitoring, evaluation, internal audit, management review, continuous improvement, and impacts and sanctions if policies are not implemented properly. This research aims to enable organizations to be more effective in dealing with cyber threats and ensure that cybersecurity operations services run optimally.

Keywords: *Cyber Security Operations, Information Security Policy*, ISO/IEC 27001:2022, NIST CSF 2.0, *Cyber Security Governance*.

1. PENDAHULUAN

Seiring dengan berkembangnya zaman, penggunaan akan teknologi informasi untuk mendukung proses bisnis yang dimiliki oleh organisasi baik pemerintahan maupun swasta. Hal tersebut menyebabkan adanya peningkatan terhadap ancaman yang mengintai terhadap aset teknologi informasi [1], [2]. Oleh karena itu, dilakukan serangkaian kegiatan operasi keamanan siber dengan tujuan mengamankan aset yang dimiliki organisasi dari serangan siber [3]–[9].

Pelaksanaan kegiatan operasi keamanan siber harus dilakukan secara cermat, teratur, dan cepat untuk memastikan aset yang dimiliki terlindungi dan insiden siber dapat ditangani dengan baik [10]. Menurut NIST pada dokumen NIST CSF 2.0, operasi keamanan siber terbagi atas enam kategori kegiatan [11], yaitu: (1) *Govern*/Tata Kelola; (2) *Identify*/Identifikasi; (3) *Detect*/Deteksi; (4) *Protect*/Proteksi; (5) *Respond*/Penanggulangan; dan (6) *Recover*/Pemulihan. Serangkaian kegiatan tersebut dapat dilakukan secara independen namun harus tetap saling terhubung antara satu kegiatan dengan kegiatan lain. Ilustrasi rangkaian kegiatan tersebut ditampilkan pada Gambar 1.

Gambar 1. Kegiatan operasi keamanan siber [11]

Dari enam kegiatan yang dilakukan pada operasi keamanan siber, kegiatan *Govern* merupakan serangkaian kegiatan yang meliputi perencanaan, pengelolaan, dan pengaturan terhadap operasi

keamanan siber yang mendukung proses bisnis utama yang dimiliki oleh suatu organisasi atau instansi. Adapun *output* dari kegiatan *Govern* berupa rencana strategis dan kebijakan teknis tentang operasi keamanan siber memiliki peran penting pada organisasi atau instansi [11], [12].

Dalam pelaksanaannya, kegiatan operasi keamanan siber memerlukan serangkaian infrastruktur yang digunakan baik untuk kegiatan Identifikasi, Deteksi, Proteksi, Penanggulangan, dan Pemulihan [13], [14]. Infrastruktur tersebut dapat berupa perangkat keras seperti komputer, *server*, dan perangkat jaringan lainnya, dan perangkat lunak seperti aplikasi, sensor, dan sistem informasi [15], [16]. Perangkat-perangkat tersebut perlu pengelolaan dan pengamanan sehingga dapat digunakan secara optimal untuk kegiatan operasi keamanan siber [17]–[20]. Oleh karena itu, perlu diterapkan suatu standar untuk mengelola dan mengamankan infrastruktur pendukung operasi keamanan siber.

Salah satu standar yang dapat diterapkan guna mengelola dan mengamankan infrastruktur operasi keamanan siber adalah ISO/IEC 27001:2022 [12]. Standar tersebut mengatur mengenai persyaratan Sistem Manajemen Keamanan Informasi untuk Perlindungan Keamanan Informasi, Keamanan Siber dan Privasi. Pada standar tersebut, terdapat klausul-klausul yang mencakup penjelasan konteks organisasi hingga perbaikan [12], [21]–[24]. Klausul-klausul tersebut bertujuan untuk mewujudkan tata kelola dan pengamanan terhadap infrastruktur teknologi informasi, yang mana salah satu bentuk infrastruktur teknologi informasi adalah infrastruktur operasi keamanan siber.

Konsep mengenai pengelolaan dan pengamanan infrastruktur operasi keamanan siber juga selaras dengan Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (SKSN MKS) [25], di mana pada peraturan tersebut terdapat fokus area SKSN yaitu Tata Kelola. Fokus area Tata Kelola meliputi penguatan ekosistem keamanan siber yang mencakup sumber daya manusia (*people*), proses (*process*), dan teknologi (*technology*).

Terdapat penelitian yang berkaitan dengan gagasan yang disampaikan oleh penulis pada tulisan ini. Penelitian yang dilakukan oleh Saadat et al menjelaskan bahwa ISO/IEC 27001 dapat dijadikan referensi dalam perumusan kebijakan tentang keamanan informasi [26]. Kobayashi et al melakukan penelitian mengenai *agreement method* terhadap kebijakan keamanan informasi berbasis *assurance case* dan ISO/IEC 27001 [27]. Penelitian yang dilakukan oleh Amiruddin et al menunjukkan bahwa NIST CSF dapat digunakan sebagai dasar penyusunan kebijakan operasional keamanan siber dan manajemen risiko siber pada organisasi [28].

Berdasarkan latar belakang tersebut, pada dokumen ini dijelaskan mengenai peluang untuk pengembangan kebijakan yang dapat diterapkan oleh organisasi/instansi mengenai tata kelola dan manajemen infrastruktur operasi keamanan siber menggunakan NIST CSF 2.0 dan ISO/IEC 27001:2022. Kebijakan ini bertujuan untuk menjadi landasan pelaksanaan kegiatan pengelolaan dan pengamanan terhadap infrastruktur operasi keamanan siber. Dengan adanya kebijakan tersebut, diharapkan bahwa pengelolaan dan pengamanan infrastruktur operasi keamanan siber dapat diterapkan dengan baik guna mendukung kegiatan operasi keamanan siber secara keseluruhan.

2. LANDASAN TEORI

2.1 NIST CSF 2.0 Sebagai Kerangka Kerja Operasi Keamanan Siber

NIST CSF 2.0 merupakan dokumen dari *National Institute of Standards and Technology* (NIST) yang berisi panduan untuk mengurangi risiko keamanan siber dengan cara membantu organisasi atau instansi untuk memahami, menilai, menentukan prioritas dan mengkomunikasikan risiko keamanan siber beserta kendali yang dapat diterapkan untuk memitigasi risiko tersebut. Pada kerangka kerja tersebut, terdapat enam kegiatan yang dinamakan *framework core*. Kegiatan-kegiatan tersebut beserta penjelasannya dirangkum pada Tabel 1.

Tabel 1. Kegiatan/Framework Core pada NIST CSF 2.0 [11]

Kode	Kegiatan (*Framework Core*)	Penjelasan
GV	*Govern* (Tata Kelola)	Menerapkan dan memantau strategi, ekspektasi, dan kebijakan manajemen risiko pada organisasi.
ID	*Identify* (Identifikasi)	Menentukan risiko keamanan siber yang saat ini ada pada organisasi.
PR	*Protect* (Proteksi)	Menerapkan pengamanan untuk mencegah atau memitigasi risiko keamanan siber.
DE	*Detect* (Deteksi)	Menemukan dan menganalisis kemungkinan serangan keamanan siber.
RS	*Respond* (Penanggulangan)	Mengambil tindakan terhadap insiden keamanan siber yang terjadi atau terdeteksi.
RC	*Recover* (Pemulihan)	Memulihkan aset dan operasional yang terdampak oleh serangan keamanan siber.

2.2 ISO/IEC 27001:2022 Sebagai Kerangka Kerja Sistem Manajemen Keamanan Informasi (SMKI)

Untuk mendukung kegiatan operasi keamanan siber, diperlukan adanya infrastruktur berupa perangkat keras, perangkat lunak, dan infrastruktur lainnya (ruangan, infrastruktur jaringan dan lain-lain). Dalam hal operasionalnya, infrastruktur tersebut harus terpenuhi perlindungan terhadap aspek berupa kerahasiaan (*confidentiality*), keutuhan (*integrity*),

dan ketersediaan (*availability*) [12].

Untuk memenuhi perlindungan terhadap ketiga aspek tersebut, perlu diterapkan serangkaian aksi yang dapat memastikan perlindungan terhadap ketiga aspek tersebut terpenuhi. Salah satu standar yang dapat diterapkan untuk memenuhi perlindungan kerahasiaan, keutuhan, dan ketersediaan dari infrastruktur operasi keamanan siber adalah ISO/IEC 27001:2022. Standar tersebut memiliki beberapa klausul yang mengatur mulai dari konteks organisasi hingga perbaikan. Klausul-klausul tersebut dirangkum pada Tabel 2.

Tabel 2. Klausul Pada ISO/IEC 27001 [12]

Klausul	Judul	Penjelasan
Klausul 4	Konteks Organisasi	Klausul ini mengatur mengenai pemahaman/identifikasi dasar dan tujuan organisasi, kebutuhan dan ekspektasi pemangku kepentingan, serta sistem manajemen keamanan informasi dan cakupannya.
Klausul 5	Kepemimpinan	Klausul ini mengatur mengenai kepemimpinan dan komitmen pimpinan, kebijakan, peran, tanggung jawab dan wewenang dalam organisasi.
Klausul 6	Perencanaan	Klausul ini mengatur mengenai tindakan terhadap risiko dan peluang serta tujuan dari keamanan informasi dan rencana untuk mencapainya.
Klausul 7	Dukungan	Klausul ini mengatur mengenai dukungan sumber daya, kompetensi, kesadaran keamanan informasi, komunikasi, dan informasi terdokumentasi.
Klausul 8	Operasi	Klausul ini mengatur mengenai perencanaan dan kendali operasi, penilaian risiko keamanan informasi, dan penanganan terhadap risiko keamanan informasi.
Klausul 9	Evaluasi Performa	Klausul ini mengatur mengenai pemantauan, pengukuran, analisis dan evaluasi performa, audit internal, dan ulasan manajemen.
Klausul 10	Perbaikan	Klausul ini mengatur mengenai perbaikan berkelanjutan terhadap sistem manajemen keamanan informasi.

2.3 Komponen Kebijakan Publik

Menurut Charles O. Jones, kebijakan publik memiliki lima komponen, yaitu: (1) *Goal* atau tujuan yang ingin dicapai dari adanya kebijakan; (2) *Plans* atau Proposal, yaitu pengertian yang spesifik untuk mencapai tujuan; (3) *Program*, yaitu upaya yang berwenang dalam mencapai tujuan; (4) *Decision* atau keputusan, yaitu tindakan-tindakan untuk menentukan tujuan, membuat rencana, melaksanakan, dan mengevaluasi program; dan (5) Efek, yaitu dampak dari penerapan program [29].

3. METODE PENELITIAN

Pada penelitian ini, digunakan metode studi literatur serta pendekatan konseptual terhadap penyusunan kebijakan pengamanan dan pengelolaan infrastruktur operasi keamanan siber. Pada penelitian ini dilakukan analisis konseptual dan pengembangan kebijakan berdasarkan pemahaman yang mendalam tentang kerangka kerja dan standar yang relevan dalam keamanan siber. Metode ini digunakan untuk merumuskan panduan dan rekomendasi kebijakan yang dapat diterapkan oleh organisasi/instansi dalam mengelola dan mengamankan infrastruktur operasi keamanan siber.

3.1 Pendekatan Analisis Konseptual

Pendekatan analisis konseptual bertujuan untuk memahami dan menganalisis konsep, gagasan, atau teori yang berkaitan dengan tata kelola dan pengamanan terhadap infrastruktur teknologi informasi, khususnya pada infrastruktur operasi keamanan siber. Metode analisis konseptual melibatkan komponen pemahaman desain, skema perancangan analitis, pemetaan pola pikir desain, metode pendekatan desain, dan diakhiri dengan perumusan konsep desain [30]. Pendekatan analisis konseptual dilakukan dengan cara menggabungkan konsep-konsep praktis yang dapat diterapkan untuk menjadi penyelesaian atas suatu permasalahan.

4. HASIL PENELITIAN

4.1 Integrasi Konsep Govern pada NIST CSF dengan SMKI ISO/IEC 27001:2022

Pada kegiatan *framework core* Govern dari NIST CSF 2.0, terdapat 5 (lima) kategori yang dimiliki, yaitu: (1) Konteks Organisasi; (2) Manajemen Rantai Pasok Keamanan Siber; (3) Peran dan Tanggung Jawab; (4) Kebijakan, Proses, dan Prosedur; dan (5) *Oversight*. Penjelasan masing-masing kategori pada konsep *Govern* dirangkum pada Tabel 3.

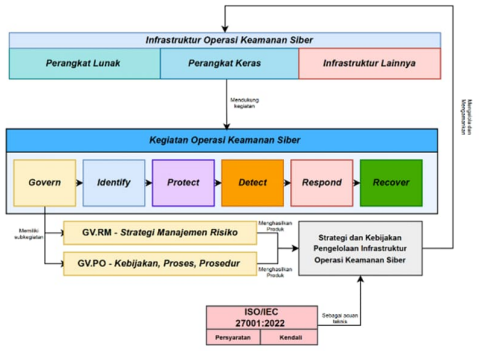
Dari enam kategori tersebut, terdapat dua kategori utama yang berkaitan erat dengan implementasi pengelolaan dan pengamanan infrastruktur operasi keamanan siber. Kategori pertama adalah kategori Kebijakan, Proses, dan Prosedur (kode GV.PO) yang memiliki peran untuk penetapan, komunikasi dan penerapan kebijakan, proses dan prosedur keamanan siber pada organisasi. Kategori kedua adalah Strategi Manajemen Risiko (kode GV.RM) yang memiliki peran untuk mengidentifikasi, menyusun prioritas, dan menyusun rencana penanganan terhadap risiko.

Untuk mengimplementasikan kedua kategori tersebut dibutuhkan standar lain yang mengatur mengenai teknis pengelolaan dan pengamanan infrastruktur operasi keamanan siber yaitu ISO/IEC 27001:2022. Berdasarkan kebutuhan tersebut, dapat dirumuskan suatu kebijakan untuk pengelolaan dan pengamanan infrastruktur operasi keamanan siber dengan mengintegrasikan antara NIST CSF 2.0 dengan ISO/IEC 27001:2022. Kerangka konseptual bagaimana hasil integrasi antara NIST CSF dengan ISO/IEC 27001:2022 untuk pengelolaan dan

pengamanan infrastruktur operasi keamanan siber diilustrasikan pada Gambar 2.

Tabel 3. Kategori pada kegiatan *Govern* [11]

Kode	Kategori	Penjelasan
GV.OC	Konteks Organisasi	Organisasi dapat memahami kondisi, misi, ekspektasi pemangku kepentingan, *risk tolerance*, *risk appetite*, dan asumsi-asumsi lainnya untuk mendukung dalam hal pengambilan keputusan risiko operasional.
GV.RM	Strategi Manajemen Risiko	Organisasi dapat menetapkan dan mengkomunikasikan prioritas, *constraints*, toleransi dan selera risiko untuk mendukung keputusan terhadap risiko operasional.
GV.SC	Manajemen Rantai Pasok Keamanan Siber	Proses manajemen rantai pasok keamanan siber pada organisasi diidentifikasi, ditetapkan, dikelola, dipantau, dan diperbarui oleh pemangku kepentingan.
GV.RR	Peran, Tanggung Jawab, dan Wewenang	Penetapan peran, tanggung jawab, dan wewenang dalam operasi keamanan siber untuk mendukung adanya akuntabilitas, penilaian kinerja, dan perbaikan.
GV.PO	Kebijakan, Proses, dan Prosedur	Penetapan, komunikasi dan penerapan terhadap kebijakan, proses dan prosedur keamanan siber pada organisasi.
GV.OV	*Oversight*	Hasil dari performa strategi manajemen risiko organisasi digunakan untuk memperbaharui dan menyesuaikan strategi manajemen risiko.



Gambar 2. Kerangka konseptual integrasi NIST CSF 2.0 dengan ISO/IEC 27001

4.2 Kerangka Kebijakan Pengelolaan dan Pengamanan Infrastruktur Operasi Keamanan Siber

Kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber perlu dituangkan dalam suatu kebijakan yang mengikat agar penerapannya dapat dikendalikan dan dapat dilakukan penilaian terhadap hasil penerapannya. Oleh karena itu, berdasarkan gagasan pada subbab sebelumnya, dapat dilakukan perumusan kebijakan dengan 5 (lima) komponen penyusun berdasarkan teori kebijakan publik Charles O. Jones. Komponen penyusun kebijakan, konsep substansi kebijakan pengelolaan infrastruktur Kegiatan operasi keamanan siber, serta kaitannya terhadap klausul ISO/IEC 27001:2022 dirangkum pada Tabel 4.

Berdasarkan dari rancangan kerangka kebijakan pada Tabel 4, diketahui terdapat 5 (lima) bab dengan total 17 subbab yang mengatur mengenai pelaksanaan dari kebijakan pengelolaan dan pengamanan infrastruktur operasi keamanan siber. Rancangan kebijakan tersebut dapat disesuaikan substansinya sesuai dengan kondisi organisasi masing-masing dan tujuan yang akan dicapai dari kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber.

5. KESIMPULAN

Penelitian ini membahas mengenai rancangan kebijakan pengelolaan dan pengamanan infrastruktur operasi keamanan siber untuk mendukung kegiatan operasi keamanan siber. Rancangan kebijakan ini melibatkan komponen-komponen seperti tujuan organisasi, penjelasan kegiatan pengelolaan dan pengamanan infrastruktur, rincian kegiatan, ketentuan penerapan, pemantauan, evaluasi, audit internal, ulasan manajemen, perbaikan berkelanjutan, serta dampak dan sanksi jika kebijakan tidak dilaksanakan dengan baik.

Hal tersebut bertujuan agar pengelolaan dan pengamanan infrastruktur operasi keamanan siber untuk melindungi aset teknologi informasi organisasi dapat dilaksanakan dengan baik. Dengan merumuskan dan menerapkan kebijakan yang terstruktur, organisasi dapat lebih efektif dalam menghadapi ancaman siber dan memastikan layanan operasi keamanan siber berjalan optimal.

6. SARAN

Penelitian ini memiliki keterbatasan berupa pelaksanaan pengujian untuk mengukur efisiensi dan efektivitas dari kebijakan yang dapat menjadi peluang penelitian selanjutnya.

Tabel 4. Rancangan Kerangka Kebijakan

No.	Komponen	Konsep Substansi	Konsep Bab	Konsep Subbab	Klausul ISO/IEC 27001
1	*Goals* atau Tujuan	Tujuan dari penerapan pengelolaan dan pengamanan infrastruktur Kegiatan operasi keamanan siber yang berisi penjabaran dari sasaran/tujuan strategis organisasi terhadap pengamanan ekosistem siber baik terhadap pemangku kepentingan internal maupun eksternal.	Bab I	Subbab I.1 Dasar dan tujuan	Klausul 4
				Subbab I.2 Identifikasi peran organisasi terhadap internal dan eksternal	Klausul 5
				Subbab I.3 Identifikasi pemangku kepentingan internal dan eksternal	Klausul 4
2	*Plans* atau *proposals*	Penjelasan umum mengenai kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber yang bertujuan untuk mencegah dan/atau meminimalisir dampak serangan siber terhadap infrastruktur terkait sehingga layanan operasi keamanan siber dapat diberikan dengan baik oleh organisasi kepada pemangku kepentingan.	Bab II	Subbab II.1 Penjelasan umum kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber	Klausul 6
				Subbab II.2 Cakupan kegiatan-kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber	
				Subbab II.3 Hasil yang diharapkan dari kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber	
3	*Program*	Penjelasan rinci mengenai kegiatan-kegiatan yang dilakukan dalam rangka pengelolaan dan pengamanan infrastruktur operasi keamanan siber beserta sumber daya yang digunakan atau dibutuhkan dalam pelaksanaannya	Bab III	Subbab III.1 Penjelasan umum risiko terhadap infrastruktur operasi keamanan siber	Klausul 8
				Subbab III.2 Penilaian risiko terhadap infrastruktur operasi keamanan siber	
				Subbab III.3 Penanganan terhadap risiko infrastruktur operasi keamanan siber	
				Subbab III.4 Penerapan kendali terhadap operasional infrastruktur operasi keamanan siber	
				Subbab III.5 Dukungan terhadap sumber daya yang diperlukan dalam kegiatan pengelolaan dan pengamanan infrastruktur operasi keamanan siber	Klausul 7
4	*Decisions*	Penjelasan tentang ketentuan penerapan dari kebijakan ini serta bentuk pemantauan, evaluasi, penilaian, audit internal	Bab IV	Subbab IV.1 Pemantauan, Evaluasi dan Penilaian terhadap keluaran (*output*) dari pengelolaan dan pengamanan infrastruktur operasi keamanan siber	Klausul 9
				Subbab IV.2 Audit internal terhadap penerapan pengelolaan dan pengamanan	

No.	Komponen	Konsep Substansi	Konsep Bab	Konsep Subbab	Klausul ISO/IEC 27001
				infrastruktur operasi keamanan siber	
				Subbab IV.3 Ulasan manajemen berkelanjutan terhadap pengelolaan dan pengamanan infrastruktur operasi keamanan siber	
				Subbab IV.4 Perbaikan berkelanjutan terhadap pengelolaan dan pengamanan infrastruktur operasi keamanan siber	Klausul 10
5	*Effect*	Penjelasan mengenai dampak dan/atau sanksi yang dapat dijatuhkan oleh organisasi apabila kebijakan ini tidak dilaksanakan dengan baik	Bab V	Subbab V.1 Dampak apabila pengelolaan dan pengamanan infrastruktur operasi keamanan siber tidak dilakukan dengan baik	Klausul 4
				Subbab V.2 Sanksi yang dapat dijatuhkan apabila pengelolaan dan pengamanan infrastruktur operasi keamanan siber tidak dilakukan dengan baik	

REFERENSI

[1] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "Challenges and Performance Metrics for Security Operations Center Analysts: A Systematic Review," *Journal of Cyber Security Technology*, vol. 4, no. 3, pp. 125–152, Jul. 2020, doi: 10.1080/23742917.2019.1698178.

[2] Badan Siber dan Sandi Negara, "LANSKAP KEAMANAN SIBER INDONESIA 2022," Jakarta, 2023.

[3] National Institute of Standards and Technology, "Security and privacy controls for federal information systems and organizations," *NIST Special Publication 800-53*, 2020.

[4] A. Wirth, "The Economics of Cybersecurity," *Biomed Instrum Technol* , vol. 51, no. s6, pp. 52–59, 2017, doi: https://doi.org/10.2345/0899-8205-51.s6.52.

[5] A. Yuswanto and B. Wibowo, "Pembangunan Pusat Pengendalian Operasional Keamanan Informasi (Pusdalops Kami) guna Meningkatkan Pelayanan E-Gov dari Ancaman Kejahatan Siber." [Online]. Available: https://sijaki.jakarta.go.id

[6] B. Fachriandi and T. Dirgahayu, "Kepedulian Keamanan Informasi di Pemerintahan: Praktik Manajemen dan Dampaknya," *Jurnal Manajemen Informatika (JAMIKA)* , vol. 11, no. 1, pp. 72–87, 2021, doi: 10.34010/jamika.v11i1.

[7] H. Jauhary, G. Eldisa Pratiwi, A. Zamzami Salim, P. Studi Teknik Informatika, and U. Jakarta, "Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi : Literatur Review," *Media Jurnal Informatika*, vol. 14, no. 1, 2022, doi: 10.35194/mji.v%vi%i.1581.

[8] W. Wu, K. Shi, C.-H. Wu, and J. Liu, "Research on the Impact of Information Security Certification and Concealment on Financial Performance," *Journal of Global Information Management*, vol. 30, no. 3, pp. 1–16, Sep. 2021, doi: 10.4018/jgim.20220701.oa2.

[9] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *Journal of Cybersecurity and Privacy*, vol. 1, no. 2, pp. 219–238, Apr. 2021, doi: 10.3390/jcp1020012.

[10] A. Chodakowska, S. Kańduła, and J. Przybylska, "Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done," *Lex Localis*, vol. 20, no. 1, pp. 161–192, Jan. 2022, doi: 10.4335/20.1.161-192(2022).

[11] NIST, *The NIST Cybersecurity Framework 2.0*. 2023. doi: https://doi.org/10.6028/NIST.CSWP.29.ipd.

[12] Iso, "Information security, cybersecurity and privacy protection-Information security management systems-Requirements," 2022.

[13] "Security and Privacy Controls for Information Systems and Organizations," Gaithersburg, MD, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[14] V. J. R. Winkler, *Securing the Cloud: Cloud computer Security techniques and tactics*. Elsevier, 2011.

[15] P. Tubío Figueira, C. López Bravo, and J. L. Rivas López, "Improving information security risk analysis by including threat-occurrence predictive models," *Comput Secur*, vol. 88, Jan. 2020, doi: 10.1016/j.cose.2019.101609.

[16] E. Yunizal, J. Santoso, and K. Surendro, "A Method of Simplifying the Asset Dependency Cycle in Security Risk Analysis," *IOP Conf Ser Mater Sci Eng*, vol. 1077, no. 1, p. 012002, Feb. 2021, doi: 10.1088/1757-899x/1077/1/012002.

[17] D. G. S. Barani, W. Hayuhardhika, N. Putra, and B. S. Prakoso, "Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus : Dinas Komunikasi dan Informatika Provinsi Jawa Timur)," 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[18] E. Rizky Pratama, "EVALUASI TATA KELOLA SISTEM KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN INDEKS KAMI DAN ISO 27001 (STUDI KASUS KOMINFO PROVINSI JAWA TIMUR)."

[19] P. Sundari, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, vol. 12, no. 1, p. 35, 2021.

[20] W. Yeoh, S. Wang, A. Popovič, and N. H. Chowdhury, "A systematic synthesis of critical success factors for cybersecurity," *Comput Secur*, vol. 118, Jul. 2022, doi: 10.1016/j.cose.2022.102724.

[21] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *TQM Journal*, vol. 33, no. 7. Emerald Group Holdings Ltd., pp. 76–105, Mar. 16, 2021. doi: 10.1108/TQM-09-2020-0202.

[22] M. Bouziani, M. Merbah, M. Tiskar, A. Et-tahir, and A. Chaouch, "When can we talk about implementing an Information Security Management System, according to ISO 27001?," 2022.

[23] A. Calder and S. G. Watkins, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," in *Information Security Risk Management for ISO 27001/ISO 27002, third edition*, IT Governance Publishing, Sep. 2019, pp. 87–93. doi: 10.2307/j.ctvndv9kx.11.

[24] M. Waruwu and A. Indrati, "IDN Media Information Security Management System Maturity Measurement Analysis Using ISO 27001:2013 and KAMI Index Version 4.0," *International Research Journal of Advanced Engineering and Science*, vol. 6, no. 3, pp. 36–40, 2021.

[25] Presiden RI, *PERATURAN PRESIDEN REPUBLIK INDONESIA NOMOR 47 TAHUN 2023 TENTANG STRATEGI KEAMANAN SIBER NASIONAL DAN MANAJEMEN KRISIS SIBER*. 2023.

[26] M. Saadat and M. U. Abbasi, "Information Security Policy Development: the Mechanism to Ensure Security Over Information Technology Systems," *Global International Relations Review*, vol. IV, no. IV, pp. 32–42, Dec. 2021, doi: 10.31703/girr.2021(iv-iv).04.

[27] N. Kobayashi, A. Nakamoto, M. Kawase, M. Ioki, and S. Shirasaka, "A Proposal of Information Security Policy Agreement Method for Merger and Acquisition Using Assurance Case and ISO 27001," in *Proceedings - 2019 8th International Congress on Advanced Applied Informatics, IIAI-AAI 2019*, Institute of Electrical and Electronics Engineers Inc., Jul. 2019, pp. 727–733. doi: 10.1109/IIAI-AAI.2019.00150.

[28] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho, "Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8," in *2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS*, Jakarta: IEEE, Oct. 2021.

[29] A. Tahir, *Kebijakan Publik dan Good Governancy*. 2018.

[30] "Pendekatan Konseptual Dalam Proses Perancangan Interior (Adi Santosa)." [Online]. Available: http://puslit.petra.ac.id/journals/interior/