Peraturan dan Regulasi Keamanan Siber di Era Digital

Novera Kristianti¹, Ririn Kurniasi²

Universitas Palangka Raya¹, IAHN-Tampung Penyang Palangka Raya²

noverara@gmail.com¹, kurniasiririn@gmail.com²

Riwayat Jurnal

Artikel diterima: 15 Mei 2024

Artikel direvisi: 24 Mei 20224

Artikel disetujui: 27 Mei 2024

Abstrak

Perkembangan teknologi digital yang pesat telah membawa berbagai kemajuan dalam berbagai aspek kehidupan, namun juga menimbulkan tantangan baru dalam hal keamanan siber. Tujuan penelitian tentang peraturan dan regulasi keamanan siber di era digital ini, untuk menyoroti pentingnya kerangka hukum yang efektif untuk melindungi data dan sistem informasi dari ancaman siber. Penelitian ini mengkaji berbagai pendekatan yang telah diadopsi oleh negara-negara maju dan berkembang dalam mengatasi masalah keamanan siber, termasuk undang-undang, standar industri, dan kebijakan pemerintah. Selain itu, penelitian ini menganalisis peran kerjasama internasional dalam membangun ekosistem keamanan siber yang tangguh dan efektif. Temuan penelitian menunjukkan bahwa harmonisasi peraturan di tingkat global serta adaptasi kebijakan yang fleksibel dan dinamis sangat penting untuk mengantisipasi ancaman yang terus berkembang di dunia maya. Melalui pemahaman mendalam tentang regulasi keamanan siber, artikel ini memberikan rekomendasi strategis bagi pembuat kebijakan, penegak hukum, dan praktisi keamanan siber untuk meningkatkan perlindungan dan mitigasi risiko di era digital.

Kata kunci : *Keamanan Siber, Peraturan dan Regulasi, Era Digital.*

Abstract

The rapid development of digital technology has brought about various advancements in various aspects of life, but it also poses new challenges in terms of cybersecurity. This article examines cybersecurity rules and regulations in the digital age, highlighting the importance of an effective legal framework to protect data and information systems from cyber threats. It examines the various approaches that developed and developing countries have adopted in addressing cybersecurity issues, including laws, industry standards and government policies. In addition, the article analyzes the role of international cooperation in building a resilient and effective cybersecurity ecosystem. The research findings show that regulatory harmonization at the global level as well as flexible and dynamic policy adaptation are essential to anticipate evolving threats in cyberspace. Through an in-depth understanding of cybersecurity regulation, this article provides strategic recommendations for policymakers,

law enforcement, and cybersecurity practitioners to enhance protection and risk mitigation in the digital age.

Keywords: *Cyber Security, Rules and Regulations, Digital Era.*

Pendahuluan

Di era digital yang semakin maju ini, teknologi informasi dan komunikasi telah menjadi tulang punggung berbagai aspek kehidupan manusia. Dari sektor ekonomi, pendidikan, kesehatan, hingga pemerintahan, transformasi digital telah membawa berbagai kemudahan dan efisiensi. Namun, di balik semua kemajuan tersebut, ancaman keamanan siber juga meningkat dengan cepat, menciptakan tantangan baru yang kompleks dan dinamis. (Sujitparapitaya et al., 2012) (Bechara & Schuch, 2020)

Keamanan siber menjadi isu krusial mengingat meningkatnya frekuensi dan skala serangan siber yang dapat menyebabkan kerugian finansial, kehilangan data pribadi, dan ancaman terhadap keamanan nasional. Oleh karena itu, kebutuhan akan peraturan dan regulasi yang komprehensif dan efektif menjadi sangat mendesak untuk melindungi data dan sistem informasi dari berbagai ancaman siber. (Babajide Tolulope Familoni & Philip Olaseni Shoetan, 2024) (Syafrietal et al., 2020)

Keamanan siber menjadi semakin penting seiring dengan meningkatnya ketergantungan kita pada teknologi digital. Serangan siber dapat mengakibatkan kerugian finansial yang signifikan, reputasi yang rusak, dan bahkan ancaman terhadap keamanan nasional. Oleh karena itu, perlindungan terhadap infrastruktur digital dan data sensitif menjadi prioritas utama bagi banyak negara dan organisasi.

Keamanan siber menjadi semakin penting seiring dengan meningkatnya ketergantungan kita pada teknologi digital. Serangan siber dapat mengakibatkan kerugian finansial yang signifikan, reputasi yang rusak, dan bahkan ancaman terhadap keamanan nasional. Oleh karena itu, perlindungan terhadap infrastruktur digital dan data sensitif menjadi prioritas utama bagi banyak negara dan organisasi.

Meningkatnya frekuensi dan kompleksitas serangan siber memerlukan upaya yang lebih serius dalam hal pengembangan kebijakan dan regulasi keamanan siber. Serangan seperti pencurian data, ransomware, dan sabotase infrastruktur digital bisa berdampak luas dan merusak. Selain dampak langsung, serangan ini juga bisa menurunkan kepercayaan publik terhadap sistem digital dan menimbulkan ketidakstabilan ekonomi serta sosial. Negara dan organisasi harus bekerja sama dalam menciptakan dan menerapkan peraturan serta regulasi yang komprehensif untuk melindungi aset digital.

Untuk mengatasi ancaman siber, berbagai peraturan dan regulasi telah diterapkan oleh pemerintah di seluruh dunia. Peraturan ini bertujuan untuk melindungi data pribadi, memastikan integritas sistem informasi, dan menegakkan hukum terhadap pelaku kejahatan siber. Selain itu, regulasi keamanan siber juga mendorong penerapan praktik terbaik dalam manajemen risiko dan meningkatkan kesadaran tentang pentingnya keamanan informasi.

Negara-negara di seluruh dunia telah menyadari pentingnya mengembangkan kerangka hukum yang kuat untuk menghadapi tantangan ini. Berbagai pendekatan regulasi telah diimplementasikan, mulai dari undang-undang nasional, standar industri, hingga kebijakan pemerintah yang bertujuan untuk memperkuat keamanan siber. Namun, keberhasilan dari upaya ini sangat bergantung pada harmonisasi dan kerjasama internasional, mengingat sifat ancaman siber yang tidak mengenal batas geografis.(ORCA – *Online Research @ Cardiff Transnational Governance of Cybersecurity* :, n.d.)(Hui-Lin & Kuei-, 2014)

Artikel ini bertujuan untuk mengeksplorasi berbagai peraturan dan regulasi keamanan siber yang ada di era digital, mengidentifikasi praktik terbaik, dan menganalisis tantangan yang dihadapi dalam implementasinya. Dengan memahami dinamika regulasi keamanan siber, penelitian ini berharap dapat memberikan wawasan dan rekomendasi yang berguna bagi pembuat kebijakan, penegak hukum, dan praktisi keamanan siber.

Penelitian ini akan dimulai dengan tinjauan literatur mengenai konsep dan definisi keamanan siber, diikuti oleh analisis mendalam tentang berbagai kerangka regulasi yang telah diterapkan di berbagai negara. Selain itu, artikel ini juga akan membahas peran kerjasama internasional dalam membangun ekosistem keamanan siber yang efektif, serta mengidentifikasi tantangan utama dan peluang untuk peningkatan regulasi di masa depan. Melalui pendekatan ini, diharapkan dapat terbangun pemahaman yang komprehensif tentang pentingnya regulasi keamanan siber di era digital.

Hasil dari penelitian ini diharapkan dapat memberikan kontribusi yang signifikan terhadap pemahaman tentang peraturan dan regulasi keamanan siber. Selain itu, penelitian ini diharapkan dapat membantu pembuat kebijakan, praktisi keamanan siber, dan masyarakat luas dalam mengembangkan strategi yang lebih efektif untuk melindungi aset digital di era digital yang terus berkembang.

Metode

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus dan analisis komparatif untuk mengeksplorasi peraturan dan regulasi keamanan siber di era digital. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam tentang berbagai kebijakan dan kerangka hukum yang telah diterapkan di berbagai negara, serta untuk menganalisis efektivitas dan tantangan implementasinya.

Metode Pengumpulan Data

a) Studi Literatur

Penelitian ini dimulai dengan tinjauan literatur yang komprehensif untuk mengumpulkan informasi mengenai konsep dasar keamanan siber, perkembangan peraturan dan regulasi di berbagai negara, serta studi kasus yang relevan. Sumber

data meliputi jurnal ilmiah, buku, laporan resmi dari pemerintah dan organisasi internasional, serta artikel dari media terpercaya.

b) Analisis Dokumen

Analisis dokumen dilakukan terhadap undang-undang, regulasi, kebijakan pemerintah, dan standar industri terkait keamanan siber. Dokumen-dokumen ini diperoleh dari situs web resmi pemerintah, organisasi internasional, dan lembaga terkait lainnya.

c) Wawancara Mendalam

Wawancara mendalam dilakukan dengan ahli keamanan siber, pembuat kebijakan, dan praktisi di bidang keamanan siber. Wawancara ini bertujuan untuk memperoleh wawasan langsung tentang tantangan dan peluang dalam implementasi regulasi keamanan siber.

d) Studi Kasus

Studi kasus dipilih dari berbagai negara dengan tingkat perkembangan yang berbeda dalam regulasi keamanan siber. Analisis studi kasus ini akan membantu mengidentifikasi praktik terbaik dan memberikan gambaran tentang bagaimana regulasi diimplementasikan dalam konteks yang berbeda.

e) Analisis Data

Data yang diperoleh dari berbagai sumber tersebut dianalisis secara kualitatif dengan pendekatan analisis tematik. Proses analisis meliputi:

f) Koding Data

Data dari studi literatur, analisis dokumen, dan wawancara dikoding untuk mengidentifikasi tema-tema utama yang muncul.

g) Kategorisasi Tema

Tema-tema yang diidentifikasi kemudian dikategorikan berdasarkan relevansinya dengan tujuan penelitian, seperti efektivitas regulasi, tantangan implementasi, dan kerjasama internasional.

h) Komparasi Tematik

Analisis komparatif dilakukan antara berbagai kasus studi untuk mengidentifikasi perbedaan dan persamaan dalam pendekatan regulasi keamanan siber di berbagai negara.

i) Validitas dan Reliabilitas

Untuk memastikan validitas dan reliabilitas penelitian, triangulasi data dilakukan dengan membandingkan informasi dari berbagai sumber. Selain itu, verifikasi hasil wawancara dilakukan dengan responden untuk memastikan akurasi dan konsistensi data.

Dengan pendekatan metode ini, penelitian ini diharapkan dapat memberikan gambaran yang komprehensif tentang peraturan dan regulasi keamanan siber di era digital, serta memberikan rekomendasi yang berguna bagi pembuat kebijakan dan praktisi di bidang ini.

Pembahasan

Penelitian ini menyoroti beberapa temuan penting terkait peraturan dan regulasi keamanan siber di era digital, serta mengidentifikasi tantangan dan peluang dalam implementasinya. Berikut adalah pembahasan lebih lanjut berdasarkan hasil analisis data yang diperoleh dari studi literatur, analisis dokumen, wawancara mendalam, dan studi kasus.

Kerangka Regulasi Keamanan Siber

1. Variasi dalam Pendekatan Regulasi

Negara-negara menunjukkan variasi yang signifikan dalam pendekatan regulasi keamanan siber. Beberapa negara, seperti Amerika Serikat dan negara-negara anggota Uni Eropa, telah mengembangkan kerangka regulasi yang komprehensif dan spesifik, termasuk undang-undang yang mengatur perlindungan data pribadi (misalnya, GDPR di Uni Eropa) dan kewajiban pelaporan insiden siber.

Di negara-negara berkembang, regulasi seringkali masih dalam tahap awal, dengan fokus utama pada peningkatan kesadaran dan pengembangan kapasitas. Kurangnya sumber daya dan keahlian sering menjadi kendala utama dalam penerapan regulasi yang efektif.

2. Standar Industri dan Kepatuhan

Standar industri internasional, seperti ISO/IEC 27001 untuk sistem manajemen keamanan informasi, memainkan peran penting dalam membantu organisasi mencapai kepatuhan terhadap regulasi keamanan siber. Penelitian ini menemukan bahwa penerapan standar ini dapat meningkatkan kepercayaan antara perusahaan dan pelanggan serta mengurangi risiko insiden siber. Implementasi standar internasional menyediakan kerangka kerja yang sistematis untuk mengelola keamanan informasi, sehingga organisasi dapat lebih mudah memenuhi persyaratan regulasi lokal dan internasional. Selain itu, sertifikasi ISO/IEC 27001 menunjukkan komitmen organisasi terhadap keamanan informasi, yang dapat meningkatkan kepercayaan pelanggan dan mitra bisnis, serta memberikan keunggulan kompetitif di pasar.

Penerapan standar ini juga membantu organisasi mengidentifikasi, menilai, dan mengelola risiko dengan lebih efektif, mengurangi kerugian finansial, kerusakan reputasi, dan gangguan operasional akibat serangan siber. Lebih lanjut, penerapan standar dapat meningkatkan efisiensi operasional dengan mengembangkan proses yang lebih terstruktur dan responsif terhadap insiden. Namun, terdapat beberapa tantangan dalam penerapan standar internasional. Biaya implementasi yang signifikan, kompleksitas proses, dan kebutuhan akan pemeliharaan serta pembaruan berkelanjutan bisa menjadi hambatan, terutama bagi organisasi kecil dan menengah. Meskipun demikian, manfaat yang diperoleh dari peningkatan kepercayaan pelanggan, pengurangan risiko insiden siber, dan efisiensi operasional membuat penerapan standar ini menjadi investasi yang berharga.

Dengan adopsi yang luas dan dukungan dari pemerintah serta industri, standar seperti ISO/IEC 27001 dapat berkontribusi secara signifikan terhadap peningkatan keamanan siber di era digital. Upaya kolektif ini penting untuk memastikan perlindungan terhadap infrastruktur digital dan data sensitif, yang menjadi prioritas utama bagi banyak negara dan organisasi dalam menghadapi ancaman siber yang terus berkembang. (Kitsios et al., 2023)(Vitunskaitė et al., 2019)

3. Pemerintah dan Badan Regulasi

Pemerintah memiliki peran kunci dalam mengembangkan dan menegakkan regulasi keamanan siber. Badan regulasi yang kuat dan independen diperlukan untuk memastikan kepatuhan dan memberikan sanksi bagi pelanggaran. Namun, penelitian ini juga mengungkapkan bahwa di beberapa negara, tumpang tindih kewenangan dan kurangnya koordinasi antar lembaga dapat menghambat efektivitas regulasi.

Pemerintah harus memastikan bahwa badan regulasi memiliki otoritas yang jelas dan sumber daya yang memadai untuk melaksanakan tugasnya. Regulasi yang efektif memerlukan pengawasan yang ketat, penegakan hukum yang konsisten, dan kemampuan untuk beradaptasi dengan perkembangan teknologi dan ancaman siber yang terus berubah. Selain itu, kolaborasi antar lembaga pemerintah dan antara pemerintah dengan sektor swasta sangat penting untuk menciptakan pendekatan yang komprehensif terhadap keamanan siber.

Kurangnya koordinasi antar lembaga dapat mengakibatkan inefisiensi dan kebingungan dalam penegakan regulasi. Misalnya, tumpang tindih kewenangan antara badan yang berbeda dapat memperlambat respons terhadap insiden siber dan mengurangi efektivitas upaya mitigasi. Oleh karena itu, perlu ada mekanisme yang jelas untuk koordinasi dan komunikasi antara berbagai badan regulasi, serta pembagian tanggung jawab yang tegas untuk menghindari konflik dan redundansi.

Selain itu, pemerintah juga perlu mengedukasi dan meningkatkan kesadaran masyarakat serta organisasi tentang pentingnya keamanan siber. Kampanye edukasi

dan pelatihan keamanan siber dapat membantu mengurangi risiko yang disebabkan oleh human error dan meningkatkan kepatuhan terhadap regulasi. Dengan dukungan yang kuat dari pemerintah, sektor swasta, dan masyarakat, regulasi keamanan siber dapat lebih efektif dalam melindungi infrastruktur digital dan data sensitif dari berbagai ancaman..(Tanaka, n.d.)(Ngozi Samuel Uzougbo et al., 2024)(Larionova & Shelepov, 2021)

Tantangan dalam Implementasi

1. Evolusi Ancaman Siber

Ancaman siber terus berkembang dalam hal kompleksitas dan metode serangan. Regulasi seringkali tidak dapat mengikuti kecepatan perubahan ini, sehingga menciptakan kesenjangan antara kebijakan yang ada dan realitas ancaman yang dihadapi. Penelitian ini menekankan pentingnya regulasi yang dinamis dan fleksibel untuk menanggapi ancaman yang muncul.

2. Kekurangan Sumber Daya dan Keahlian

Banyak negara, terutama yang sedang berkembang, menghadapi kekurangan sumber daya manusia yang terampil dalam bidang keamanan siber. Pelatihan dan pengembangan keahlian menjadi prioritas untuk meningkatkan kapasitas lokal dalam menghadapi ancaman siber.

3. Kerjasama Internasional

Ancaman siber bersifat lintas batas, sehingga kerjasama internasional menjadi esensial. Penelitian ini menemukan bahwa meskipun sudah ada upaya untuk membangun kerjasama internasional, seperti melalui konvensi internasional dan forum regional, implementasinya seringkali terhambat oleh perbedaan kepentingan nasional dan kebijakan domestik.(Mohamed & Ali, 2020)(Hui-Lin & Kuei-, 2014)

Peluang untuk Peningkatan

1. Harmonisasi Regulasi Global

Harmonisasi regulasi di tingkat global dapat membantu mengurangi kesenjangan dalam keamanan siber antar negara. Inisiatif untuk menyelaraskan standar dan praktik terbaik dapat memperkuat pertahanan siber secara keseluruhan. Penelitian ini menunjukkan bahwa upaya kolaboratif internasional sangat penting dalam menghadapi ancaman siber yang bersifat lintas batas.

Dengan menyelaraskan regulasi dan standar keamanan siber, negara-negara dapat menciptakan kerangka kerja yang konsisten yang memudahkan kolaborasi dan pertukaran informasi. Hal ini juga dapat mengurangi beban kepatuhan bagi perusahaan yang beroperasi di berbagai yurisdiksi, karena mereka hanya perlu mengikuti satu set standar yang diakui secara internasional. Inisiatif seperti General Data Protection Regulation (GDPR) di Eropa telah menunjukkan bagaimana regulasi yang terharmonisasi dapat meningkatkan perlindungan data di berbagai negara.

Selain itu, harmonisasi regulasi dapat memperkuat kapasitas tanggap terhadap insiden siber. Dengan memiliki protokol yang seragam, negara-negara dapat lebih cepat dan efisien dalam merespons serangan siber, serta bekerja sama dalam investigasi dan penuntutan kejahatan siber. Kerja sama ini juga penting untuk menangani serangan yang menargetkan infrastruktur kritis dan dapat berdampak luas pada keamanan nasional.

Standar industri internasional seperti ISO/IEC 27001 dapat berfungsi sebagai dasar bagi harmonisasi regulasi. Dengan mengadopsi standar ini, negara-negara dapat memastikan bahwa praktik keamanan siber mereka selaras dengan praktik terbaik global. Selain itu, adopsi standar internasional dapat meningkatkan kepercayaan dan integritas dalam perdagangan dan transaksi digital di pasar global.

Namun, harmonisasi regulasi juga menghadapi tantangan. Perbedaan budaya, tingkat perkembangan teknologi, dan prioritas nasional dapat mempengaruhi bagaimana negara-negara menerapkan dan menafsirkan regulasi keamanan siber. Oleh karena itu, dialog yang berkelanjutan dan upaya kolaboratif

antar pemerintah, organisasi internasional, dan sektor swasta sangat diperlukan untuk mencapai keselarasan yang efektif.

2. Inovasi Teknologi dan Kebijakan Adaptif

Penggunaan teknologi inovatif seperti kecerdasan buatan (AI) dan analisis big data dapat membantu dalam mendeteksi dan merespons ancaman siber secara lebih efektif. Regulasi yang adaptif dan mendukung inovasi dapat meningkatkan ketahanan siber.

Kecerdasan buatan memiliki potensi besar dalam meningkatkan keamanan siber. AI dapat digunakan untuk menganalisis pola dan mendeteksi anomali dalam jaringan yang mungkin menunjukkan adanya ancaman siber. Dengan machine learning, sistem AI dapat belajar dari insiden sebelumnya dan mengidentifikasi serangan yang baru dan lebih kompleks. Selain itu, AI dapat membantu dalam otomatisasi respons terhadap insiden siber, mengurangi waktu yang dibutuhkan untuk merespons dan memitigasi ancaman.

Analisis big data juga memainkan peran penting dalam keamanan siber. Dengan kemampuan untuk mengumpulkan dan menganalisis data dalam jumlah besar, organisasi dapat mendapatkan wawasan yang lebih mendalam tentang aktivitas jaringan mereka. Analisis big data memungkinkan deteksi dini terhadap potensi ancaman dan kerentanan, serta membantu dalam pengambilan keputusan yang lebih tepat berdasarkan data yang akurat dan real-time.

3. Pendidikan dan Kesadaran Publik

Meningkatkan pendidikan dan kesadaran publik tentang keamanan siber adalah langkah penting untuk menciptakan budaya keamanan yang kuat. Program edukasi dan kampanye kesadaran dapat membantu masyarakat dan organisasi memahami pentingnya perlindungan data dan praktik keamanan yang baik.

Edukasi tentang keamanan siber harus dimulai sejak dini, termasuk dalam kurikulum pendidikan dasar dan menengah. Pengenalan konsep dasar keamanan siber kepada siswa dapat membentuk pemahaman yang kuat mengenai pentingnya

menjaga privasi dan keamanan data pribadi. Selain itu, program pelatihan khusus untuk guru dan staf sekolah dapat memastikan bahwa mereka memiliki pengetahuan yang diperlukan untuk mendidik siswa tentang keamanan siber. Di tingkat organisasi, pelatihan keamanan siber yang rutin dan menyeluruh bagi karyawan sangat penting. Program pelatihan ini harus mencakup berbagai aspek, seperti pengenalan ancaman siber, teknik pencegahan, dan prosedur respons insiden.

Simpulan

Penelitian ini mengeksplorasi peraturan dan regulasi keamanan siber di era digital, mengungkapkan berbagai pendekatan yang diambil oleh negara-negara di seluruh dunia serta menyoroti tantangan dan peluang dalam implementasinya. Dari analisis yang dilakukan, beberapa kesimpulan utama dapat diambil. Negara-negara memiliki pendekatan yang beragam dalam mengatur keamanan siber, mulai dari regulasi yang sangat komprehensif hingga kebijakan yang masih dalam tahap awal pengembangan. Negara-negara maju cenderung memiliki kerangka regulasi yang lebih kompleks dan spesifik, sementara negara-negara berkembang fokus pada peningkatan kesadaran dan pengembangan kapasitas. Standar industri internasional, seperti ISO/IEC 27001, sangat penting dalam membantu organisasi mencapai kepatuhan terhadap regulasi keamanan siber, yang tidak hanya meningkatkan keamanan informasi tetapi juga kepercayaan pelanggan dan mitra bisnis. Namun, ancaman siber terus berkembang dengan cepat, seringkali melebihi kemampuan regulasi untuk mengikuti perubahan ini, sehingga dibutuhkan regulasi yang dinamis dan fleksibel serta kebijakan adaptif yang dapat menanggapi ancaman yang muncul dengan cepat dan efektif.

Berdasarkan temuan penelitian ini, beberapa rekomendasi strategis dapat diberikan. Regulasi harus dirancang untuk dapat beradaptasi dengan cepat terhadap perkembangan ancaman siber. Diperlukan peningkatan kerjasama antar negara

dalam berbagi informasi, sumber daya, dan praktik terbaik untuk menghadapi ancaman siber yang bersifat global. Peningkatan pendidikan dan pelatihan di bidang keamanan siber sangat penting untuk mengatasi kekurangan sumber daya manusia dan meningkatkan kesadaran publik. Selain itu, regulasi harus mendukung adopsi teknologi inovatif yang dapat membantu mendeteksi dan merespon ancaman siber secara lebih efektif. Dengan mengimplementasikan rekomendasi-rekomendasi ini, diharapkan dapat tercipta lingkungan digital yang lebih aman dan terlindungi serta peningkatan ketahanan terhadap ancaman siber di era digital.

Daftar Pustaka

- Babajide Tolulope Familoni, & Philip Olaseni Shoetan. (2024). *Cybersecurity in the Financial Sector: a Comparative Analysis of the Usa and Nigeria*. Computer Science & IT Research Journal, 5(4), 850–877. <https://doi.org/10.51594/csitrj.v5i4.1046>
- Bechara, F. R., & Schuch, S. B. (2020). *Cybersecurity and global regulatory challenges*. Journal of Financial Crime, 28(2), 359–374. <https://doi.org/10.1108/JFC-07-2020-0149>
- Hui-Lin, H., & Kuei-, M. W. (2014). *The critical success factors assessment of ISO 27001 certification in computer organization by test-retest reliability*. African Journal of Business Management, 8(17), 705–716. <https://doi.org/10.5897/ajbm2014.7443>
- Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). *The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector*. Sustainability (Switzerland), 15(7). <https://doi.org/10.3390/su15075828>
- Larionova, M., & Shelepov, A. (2021). *Emerging Regulation for the Digital Economy: Challenges and Opportunities for Multilateral Global Governance*. International Organisations Research Journal, 16(1), 1–32. <https://doi.org/10.17323/1996-7845-2021-01-02>
- Mohamed, H., & Ali, H. (2020). *Finding solutions to cybersecurity challenges in the digital economy*. Fostering Innovation and Competitiveness With FinTech, RegTech,

and SupTech, April, 80–95. <https://doi.org/10.4018/978-1-7998-4390-0.ch005>

Ngozi Samuel Uzougbo, Chinonso Gladys Ikegwu, & Adefolake Olachi Adewusi. (2024). *Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations*. International Journal of Science and Research Archive, 12(1), 533–548. <https://doi.org/10.30574/ijsra.2024.12.1.0802>

ORCA – Online Research @ Cardiff Transnational Governance of Cybersecurity :
(n.d.).

Sujitparapitaya, S., Shirani, A., & Roldan, M. (2012). *Issues in Information Systems*. Issues in Information Systems, 13(2), 112–122.

Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). *Analysis of Cybersecurity Standard and Framework Components*. International Journal of Communication Networks and Information Security, 12(3), 417–432. <https://doi.org/10.17762/ijcnis.v12i3.4817>

Tanaka, H. (n.d.). *Adapting to Change : Analyzing Dynamic System Variations and Cyber Security in Smart Grids*.

Vitunskaitė, M., He, Y., Brandstetter, T., & Janicke, H. (2019). *Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership*. Computers and Security, 83, 313–331. <https://doi.org/10.1016/j.cose.2019.02.009>