ANALISIS MANAJEMEN RISIKO MENGGUNAKAN FRAMEWORK NIST (STUDI KASUS: PT. BRI KC SURABAYA KUSUMA BANGSA)

RISK MANAGEMENT ANALYSIS USING THE NIST FRAMEWORK (CASE STUDY: PT. BRI KC SURABAYA KUSUMA BANGSA)

Amalia Rodhya Ulfa[1*], Eka Fahira Aprilia[1], Carisca Rizky Sanyoko[1], Tantrik Ulil Lusianti[1], Reisa Permatasari[1]
*E-mail: 21082010212@student.upnjatim.ac.id

[1]Sistem Informasi, Fakultas Ilmu Komputer, UPN "Veteran" Jawa Timur

Abstrak

Teknologi informasi adalah suatu bentuk sistem yang digunakan untuk mendukung proses bisnis dalam suatu organisasi. Perkembangan teknologi yang terus berlanjut menghasilkan solusi baru dan inovatif yang berperan dalam proses manajemen risiko, membantu organisasi menganalisis, mengelola, dan menindaklanjuti risiko yang terkait dengan aspek teknologi. Organisasi dapat menggunakan sistem untuk mendeteksi ancaman atau mengidentifikasi dan mengelola risiko kepatuhan dan privasi data. PT. BRI memiliki teknologi informasi sesuai standar internasional berbasis NIST *cyber security framework.* Penelitian terhadap keamanan PT. BRI dilakukan sesuai standar NIST *cyber security framework* 1.1 untuk mengetahui keamanan saat ini. NIST *cyber security framework* 1.1 terdiri dari tiga bagian (*framework core*, *framework tier*, dan *framework profile*). *Framework core* digunakan sebagai kerangka inti untuk melakukan penelitian ini. Hasil penelitian menunjukkan perbandingan antara keamanan perusahaan dengan standar berbasis fungsi dari *framework core* terdiri dari *identify*, *protect*, *detect*, *respond*, dan *recover*. Keamanan siber pada PT. BRI KC Surabaya Kusuma Bangsa sudah sesuai dengan NIST *cyber security framework* 1.1. Namun, masih ada satu fungsi yang butuh peningkatan. Semua fungsi diklasifikasikan pada level tinggi berdasarkan hasil perhitungan persentase.
Kata kunci: *Teknologi Informasi, Manajemen Risiko,* NIST *cyber security framework* 1.1, *Framework Core.*

Abstract

Information technology is a form of system used to support business processes within an organization. The continuous development of technology has resulted in new and innovative solutions that play a role in the risk management process, helping organizations to analyze, manage and act on risks related to technological aspects. Organizations can use the system to detect threats or identify and manage compliance and data privacy risks. PT. BRI has information technology according to international standards based on the NIST cyber security framework. Research on the safety of PT. BRI is carried out according to the NIST cyber security framework 1.1 standards to determine current security. NIST cyber security framework 1.1 consists of three parts (core framework, framework tier, and framework profile). The Core Framework is used as the core framework for conducting this research. The results of the study show a comparison between company security and function-based standards from the Core framework consisting of identity, protect, detect, respond, and recover. Cyber security at PT. BRI KC Surabaya Kusuma Bangsa is following the NIST cyber security framework 1.1. However, there is still one function that needs improvement. All functions are classified at a high level based on percentage calculation results.
***Keywords**: Information Technology, Risk Management, NIST cyber security framework 1.1, Framework Core.*

1. PENDAHULUAN

Teknologi informasi adalah suatu bentuk sistem yang digunakan untuk mendukung proses bisnis dalam suatu organisasi [1]. Seiring dengan perkembangan zaman, teknologi informasi tumbuh dengan pesat. Teknologi informasi memberikan kemajuan dalam bidang-bidang, seperti bisnis, kesehatan, dan pendidikan. Selain itu, teknologi informasi telah memberikan akses ke sumber daya dan informasi dari seluruh dunia. Selain itu, perkembangan teknologi yang terus berlanjut menghasilkan solusi baru dan inovatif yang berperan dalam proses manajemen risiko, membantu organisasi menganalisis, mengelola dan menindaklanjuti risiko yang terkait dengan aspek teknologi. Organisasi dapat menggunakan sistem untuk mendeteksi ancaman atau mengidentifikasi dan mengelola risiko kepatuhan dan privasi data.

Ada banyak sekali kelebihan yang ditawarkan oleh teknologi informasi, seperti menyediakan akses informasi yang bisa memungkinkan perusahaan untuk mudah mengakses informasi yang dibutuhkan dari mana dan kapan saja, asal terkoneksi dengan jaringan internet. Teknologi informasi juga dapat meningkatkan produktivitas karena pekerjaan menjadi lebih cepat dan efisien sehingga meningkatkan hasil kerja. Teknologi informasi dapat meningkatkan komunikasi secara *real-time* (jarak jauh) yang memungkinkan untuk tetap terhubung dengan rekan kerja meskipun berada di tempat yang jauh. Meskipun demikian, teknologi informasi juga memiliki kekurangan. Ada risiko keamanan yang dapat mempengaruhi keamanan data dan privasi, seperti *cyber crime* (kejahatan siber). Hal ini membuat perusahaan rentan terhadap kejahatan siber, seperti *hacking*, *phishing*, dan *malware* karena teknologi informasi memungkinkan perusahaan untuk menyimpan dan mengakses informasi secara digital.

Banyak perusahaan yang masih kurang berhati-hati dalam melindungi informasi secara digital. Faktanya, pelaku kejahatan siber dapat dengan mudah mencuri informasi penting seperti informasi keuangan, informasi pelanggan, dan rahasia dagang. Meskipun perangkat lunak keamanan dan enkripsi ada, bahkan *hacker* berpengalaman pun dapat memecahkannya. Kejahatan siber bisa menimbulkan kerugian finansial dan hilangnya data-data yang penting. Oleh sebab itu, dibutuhkan upaya yang lebih besar untuk meningkatkan keamanan data dan informasi, serta memperbaiki hukum untuk melawan kejahatan siber. Meskipun teknologi informasi mempunyai kekurangan tersebut, perusahaan tidak bisa menghindari kecuali dengan memahami risiko yang diterima dan mengambil tindakan pencegahan yang tepat, perusahaan bisa memanfaatkan teknologi informasi secara lebih aman dan efektif.

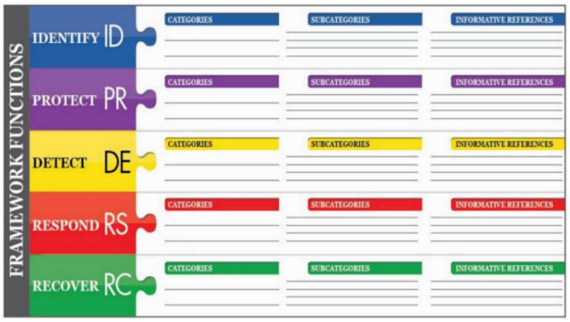
PT. BRI sebuah perusahaan yang menggunakan teknologi informasi. Setiap keamanan teknologi yang digunakan oleh PT. BRI harus menggunakan *framework* sesuai standar internasional. *Framework* dapat berfungsi sebagai model kerja sama internasional untuk memperkuat *cybersecurity* dalam infrastruktur kritis serta sektor dan komunitas lainnya [2]. Peluang kerentanan keamanan PT. BRI sangat tinggi karena ada banyak data nasabah yang dikelola dan disimpan. Pencegahan dapat dilakukan dengan mengembangkan tata kelola pengamanan atau teknologi keamanan informasi. PT. BRI memiliki teknologi informasi sesuai standar internasional berbasis NIST *cyber security framework* [6].

Perusahaan PT. BRI memiliki tujuan untuk memberikan pelayanan yang berfokus terhadap nasabah melalui teknologi informasi yang dapat dipercaya dan aman, dan jaringan kerja konvensional maupun digital yang produktif dengan menerapkan prinsip manajemen risiko [6]**.** Oleh karena itu, perlu dilakukan analisa keamanan sehingga dapat membantu PT. BRI untuk mengetahui keamanan saat ini. Apakah data nasabah sudah terjamin aman dari kebocoran data? Apakah keamanan dari PT. BRI sudah 100% sesuai dengan standar? Hal ini dapat diketahui melalui hasil. Analisa dilakukan menggunakan NIST *cyber security framework* 1.1 sebagai perbandingan dengan keamanan PT. BRI. Penelitian ini menggunakan *framework core* dengan memilih salah satu kategori pada fungsi.

2. METODOLOGI

2.1 NIST *Cyber Security Framework* 1.1

NIST *cyber security framework* 1.1 merupakan salah satu bagian dari NIST *framework*. Versi 1.1 bentuk penyempurnaan versi 1.0 yang dirilis oleh National Institute of Standards and Technology. *Framework* ini dapat meningkatkan manajemen risiko perusahaan. Selain itu, framework versi 1.1 dapat meminimalisir risiko kejahatan siber. NIST *cyber security framework* 1.1 terdiri dari tiga bagian (*framework core*, *framework tier*, dan *framework profile*). Penelitian ini menggunakan *framework core* sebagai kerangka inti untuk analisis keamanan siber. Ada lima fungsi yang mewakili aktivitas keamanan siber pada *framework core* terdiri dari identify, protect, detect, respond, dan recover. *Framework core* juga mengidentifikasi kategori dan sub kategori setiap fungsi. Sub kategori dicocokkan dengan referensi informatif seperti standar, pedoman, dan praktik.



Gambar 1. Kerangka Inti Framework Core

Pada Gambar 1 Fungsi *framework core* dapat membantu organisasi memahami risiko, melindungi sistem dan data, mendeteksi kejahatan keamanan siber, merespons kejahatan secara efektif, dan memperbaiki. Setiap fungsi dijelaskan di bawah ini.

- Identify

  Pemahaman pengelolaan risiko keamanan organisasi dalam kategori manajemen aset. Data, personel, dan perangkat sistem (*hardware* dan *software*) organisasi dianalisis oleh peneliti.
- Protect

  Perlindungan keamanan siber organisasi dianalisis untuk memastikan dapat membatasi dampak dari kejahatan keamanan siber. Penelitian menggunakan kategori keamanan data pada fungsi ini. Analisis dilakukan terhadap pengelolaan informasi dan data organisasi sudah sesuai dengan strategi risiko atau belum.
- Detect

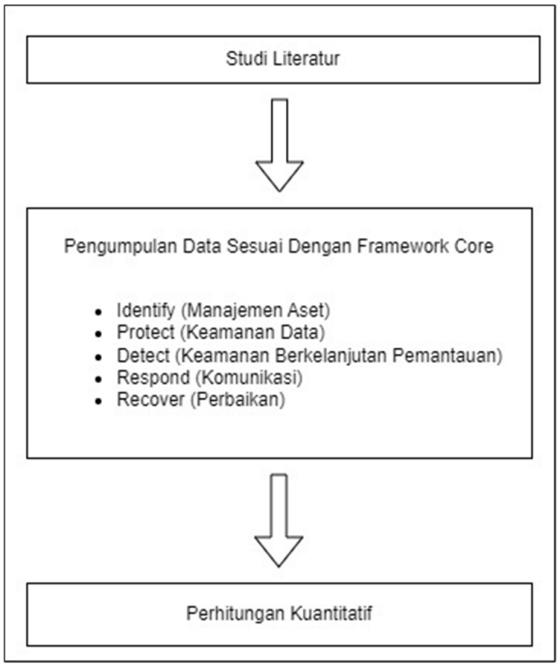
  Identifikasi terhadap pengembangan dan penerapan aktivitas organisasi yang sesuai untuk mengidentifikasi kejahatan keamanan siber. Kategori keamanan berkelanjutan pemantauan digunakan oleh peneliti. Kategori tersebut menganalisis apakah sistem informasi dan aset organisasi dipantau.
- Respond

  Peneliti mengidentifikasi pengambilan tindakan organisasi mengenai kejahatan keamanan siber yang sedang terjadi pada sistem. Pada fungsi ini peneliti menggunakan kategori komunikasi. Kategori digunakan untuk analisis kegiatan respons organisasi sudah dikoordinasikan dengan pemangku kepentingan internal dan eksternal atau belum.
- Recover

  Pemulihan organisasi terhadap kemampuan atau layanan yang terganggu akibat kejahatan keamanan siber diidentifikasi menggunakan kategori perbaikan. peneliti melakukan analisis

terhadap pemulihan organisasi, apakah pemulihan yang dilakukan berbasis pengalaman sebelumnya.

2.2 Metode Penelitian



Gambar 2. Model Metode Penelitian

2.2.1 Studi Literatur (Gambar 2)

Studi literatur merupakan tahap penyelesaian masalah dengan memilih sumber pustaka yang relevan, menelusuri sumber pustaka menggunakan kata kunci, membaca sumber pustaka, melakukan pencatatan, dan menyajikan kajian pustaka yang telah dikumpulkan.

2.2.2 Pengumpulan Data (Gambar 2)

Pengumpulan data pada PT. BRI dalam tahap ini adalah mengenai keadaan saat ini, yaitu target yang akan dicapai (tujuan) dan sistem manajemen risiko, apakah sesuai dengan standar atau tidak. Data penelitian akan dikumpulkan dengan dua cara, yaitu wawancara dan diskusi bersama narasumber. Melalui wawancara dapat mendapatkan perspektif langsung dari narasumber dan memperoleh informasi rinci tentang pendapat atau pengetahuan mereka terkait dengan subjek penelitian.

2.2.3 Perhitungan Kuantitatif (Gambar 2)

Metode selanjutnya yang digunakan dalam penelitian ini adalah penelitian dengan perhitungan kuantitatif. Data kuantitatif adalah suatu pendekatan penelitian yang didasarkan pada pandangan positivistik. Dalam metode ini, data yang dikumpulkan berupa angka-angka yang dapat diukur dan kemudian dianalisis menggunakan alat statistik. Tujuan utama dari penggunaan data kuantitatif adalah untuk menghubungkan data dengan masalah penelitian yang sedang diteliti, dengan harapan dapat mencapai suatu kesimpulan yang solid [7]. Penelitian kuantitatif adalah jenis penelitian yang sistematis, terencana, dan terstruktur [8]. Perhitungan ini dapat dilakukan dengan menggunakan metode statistika atau matematika yang sesuai dengan jenis data yang dianalisis. Pendekatan matematika berbasis persentase dapat digunakan untuk menghitung data. Perhitungan data dilakukan dengan rumus di bawah ini.

Persentase = (Jumlah Tanggapan Ya/Jumlah Pertanyaan) × 100

Hasil perhitungan persentase akan diklasifikasi menjadi level tinggi, sedang, dan rendah. Peneliti menetapkan ambang batas untuk masing-masing klasifikasi.

Tabel 1. Klasifikasi

Level	Ambang Batas
Rendah	0% - 29,99%
Sedang	30% - 69,99%
Tinggi	70% - 100%

3. HASIL DAN PEMBAHASAN

3.1 Pertanyaan Wawancara

Pada saat wawancara, peneliti memberikan beberapa pertanyaan ke narasumber. Pertanyaan dibuat berdasarkan *framework core* yang mempunyai lima fungsi. Setiap fungsi memiliki beberapa kategori. Peneliti memilih salah satu kategori untuk melakukan analisis. Pertanyaan wawancara dipaparkan pada Tabel 2.

Tabel 2. Pertanyaan Wawancara

Fungsi	Kategori	Pertanyaan	Kode
Identify	Manajemen Aset	Apakah KC BRI Surabaya Kusuma Bangsa menyusun daftar *hardware* milik kantor?	I1
		Apakah KC BRI Suarabaya Kusuma Bangsa menyusun daftar *platform* perangkat lunak dan aplikasi yang digunakan?	I2
		Apakah ada kebijakan dan prosedur yang diterapkan untuk melindungi keamanan dan kerahasiaan data yang dikirim dan diterima dalam komunikasi organisasi?	I3
		Apakah sistem informasi eksternal yang dikatalogkan telah dikelompokkan berdasarkan kategori atau tujuan penggunaannya?	I4
		Apakah sumber daya diprioritaskan berdasarkan klasifikasi, kekritisan, dan nilai bisnisnya?	I5
		Apakah peran dan tanggung jawab terkait keamanan siber telah ditetapkan secara jelas untuk seluruh tenaga kerja di organisasi dan pemangku kepentingan pihak ketiga?	I6
Protect	Keamanan Data	Apakah terdapat penggunaan sistem otentikasi atau otorisasi yang kuat untuk mengontrol akses ke *data-at-rest*?	P1
		Apakah terdapat mekanisme autentikasi yang kuat, seperti penggunaan sertifikat digital atau mekanisme otentikasi dua faktor, untuk memverifikasi identitas pihak yang berkomunikasi dalam *data-in-transit*?	P2
		Apakah terdapat kebijakan atau pedoman yang mengatur proses penghapusan, transfer, dan disposisi aset?	P3
		Apakah ada pemantauan dan pemeliharaan rutin terhadap perangkat keras dan perangkat lunak untuk memastikan ketersediaan dan kinerja yang optimal?	P4

		Apakah dilakukan evaluasi keamanan secara rutin untuk mengidentifikasi celah atau kerentanan yang dapat menyebabkan kebocoran data?	P5
		Apakah ada prosedur untuk mendeteksi dan mengatasi perubahan yang tidak sah pada perangkat lunak, *firmware*, atau integritas informasi?	P6
		Apakah ada mekanisme kontrol akses yang memastikan bahwa hanya lingkungan pengembangan dan pengujian yang dapat diakses oleh tim pengembang dan pengujian?	P7
		Apakah organisasi memiliki mekanisme pengujian atau sertifikasi untuk memastikan integritas perangkat keras sebelum digunakan?	P8
Detect	Pemantauan Berkelanjutan Keamanan	Apakah jaringan dipantau untuk mendeteksi potensi peristiwa keamanan siber?	D1
		Apakah ada sistem pengawasan yang memantau lingkungan fisik untuk mendeteksi ancaman keamanan siber?	D2
		Apakah ada proses pemantauan yang dilakukan untuk mengidentifikasi potensi ancaman keamanan siber yang berasal dari aktivitas personel?	D3
		Apakah ada alat atau perangkat yang digunakan untuk mendeteksi adanya kode berbahaya?	D4
		Apakah ada alat atau perangkat yang digunakan untuk mendeteksi adanya kode seluler yang tidak sah?	D5
		Apakah ada proses pemantauan yang dilakukan untuk mengidentifikasi potensi ancaman keamanan siber yang melibatkan penyedia layanan eksternal?	D6
		Apakah ada prosedur yang mengatur pemantauan terhadap personel, koneksi, perangkat, dan perangkat lunak yang tidak sah?	D7
		Apakah pemindaian kerentanan dilakukan untuk mengidentifikasi titik lemah dalam sistem?	D8
Respond	Komunikasi	Apakah Anda mampu berperan dengan tepat dan sesuai dengan urutan operasi yang ditetapkan?	RP1
		Apakah insiden dilaporkan sesuai dengan kriteria yang ditetapkan?	RP2
		Apakah Anda memastikan bahwa informasi yang disebarluaskan sesuai dengan rencana respons yang telah disusun?	RP3
		Apakah koordinasi dengan pemangku kepentingan terjadi sesuai dengan rencana respons?	RP4
		Apakah Anda yakin bahwa informasi yang dibagikan kepada pemangku kepentingan eksternal sesuai dengan kebijakan dan persyaratan yang telah ditetapkan?	RP5
Recover	Perbaikan	Apakah Anda telah mengevaluasi kegagalan dan kesuksesan sebelumnya untuk memperbarui rencana pemulihan Anda?	RC1
		Apakah Anda memperbarui strategi pemulihan secara teratur berdasarkan umpan balik dan evaluasi kinerja?	RC2

3.2 Hasil Wawancara

Tabel 3. Identify (Manajemen Aset)

Pertanyaan	Jawaban
I1, I2, I3, I4, I5, I6	Ya

Tabel 4. Protect (Keamanan Data)

Pertanyaan	Jawaban
P1, P2, P3, P4, P5, P6, P7, P8	Ya

Tabel 5. Detect (Pemantauan Berkelanjutan Keamanan)

Pertanyaan	Jawaban
D1, D2, D3, D6, D7, D8	Ya
D4, D5	Tidak

Tabel 6. Respond (Komunikasi)

Pertanyaan	Jawaban
RP1, RP2, RP3, RP4, RP5	Ya

Tabel 7. Recover (Perbaikan)

Pertanyaan	Jawaban
RC1, RC2	Ya

3.3 Pembahasan

Fungsi identify dengan kategori manajemen aset mendapatkan hasil 100% sehingga PT. BRI KC Surabaya Kusuma Bangsa sudah mengelola data, personel, dan perangkat sistem sesuai standar. PT. BRI KC Surabaya Kusuma Bangsa mengklasifikasi sistem informasi eksternal sesuai dengan penggunaan jenis aplikasi. Fungsi Protect dengan kategori keamanan data mendapatkan hasil 100%. Data pelanggan dan karyawan sudah terconnect dan terprotect oleh kantor pusat. Data hanya bisa diakses menggunakan jaringan internal. PT. BRI KC Surabaya Kusuma Bangsa menggunakan sertifikat digital SSL (*Secure Sockets Layer*) untuk membuka aplikasi web. perangkat keras yang digunakan sudah melalui uji standar keamanan dan sudah terverifikasi oleh BI/OJK. Fungsi detect dengan kategori pemantauan berkelanjutan keamanan mendapatkan hasil 75% sehingga perlu diperhatikan lagi.

Fungsi respond dengan kategori komunikasi mendapatkan hasil 100% . Semua insiden mengenai kejahatan keamanan siber dilaporkan sesuai dengan kriteria yang ditetapkan. PT. BRI KC Surabaya Kusuma Bangsa membentuk tim manajemen krisis untuk menyusun rencana respons (rencana tanggap darurat). Fungsi recover dengan kategori perbaikan mendapatkan hasil 100% sehingga pemulihan yang dilakukan oleh PT. BRI KC Surabaya Kusuma Bangsa berbasis pengalaman sebelumnya. Sistem pada kantor dikembangkan secara *up to date* sesuai dengan ketentuan dan kebijakan yang berlaku. PT. BRI KC Surabaya menerapkan strategi pemulihan berdasarkan *feedback* dari *user* ketika ada permasalahan yang muncul pada aplikasi yang digunakan.

4. KESIMPULAN DAN SARAN

Keamanan siber pada PT. BRI KC Surabaya Kusuma Bangsa sudah sesuai dengan NIST *cyber security framework* 1.1. Secara keseluruhan, PT. BRI KC Surabaya Kusuma Bangsa sudah menyesuaikan keamanan dengan *framework core*. Penelitian memiliki batasan dengan memilih salah satu kategori fungsi pada *framework core*. Namun, masih ada satu fungsi yang butuh peningkatan. Fungsi yang perlu ditingkatkan oleh PT. BRI KC Surabaya Kusuma Bangsa

merupakan fungsi detect. Keamanan siber perusahaan tidak menggunakan perangkat yang digunakan untuk mendeteksi adanya kode berbahaya dan kode seluler yang tidak sah sehingga fungsi detect tidak mendapatkan hasil 100%. Fungsi identify, detect, protect, respond, dan recover diklasifikasikan pada level tinggi berdasarkan hasil perhitungan persentase. Saran untuk penelitian selanjutnya dapat menggunakan kategori lain yang belum digunakan untuk analisis keamanan siber.

5. DAFTAR RUJUKAN

[1] K. C. Laudon and J. P. Laudon, "Management Information Systems: Managing the Digital Firm," Edisi 11, Upper Saddle River, NJ: Prentice Hall, 2008, hal. 21.
[2] National Institute of Standards and Technology, "NIST CYBERSECURITY FRAMEWORK," 2018. [Online].
[3] A. Calder, "NIST Cybersecurity Framework: A pocket guide," IT Governance Publishing Ltd., 2018.
[4] K. Stouffer, T. Zimmerman, C. Tang, M. Pease, J. Lubell, J. Cichonski, and J. McCarthy, "Cybersecurity framework version 1.1 manufacturing profile," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020.
[5] B. Krumay, E. W. Bernroider, and R. Walser, "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework," in Proceedings 23 of the Secure IT Systems: 23rd Nordic Conference, NordSec 2018, Oslo, Norway, November 28-30, 2018, pp. 369-384, Springer International Publishing, 2018.
[6] PT. Rakyat Indonesia (Persero) Tbk., "PT. Rakyat Indonesia (Persero) Tbk.," PT. Rakyat Indonesia (Persero) Tbk., [Online]. Available: https://bri.co.id/. [Diakses 17 Mei 2023].
[7] Sugiyono, "Metode Penelitian Kuantitatif, Kualitatif, dan R&D," Penerbit Alfabeta, 2018.
[8] U. Nugroho, "Metodologi Penelitian Kuantitatif Pendidikan Jasmani," Rajawali Pers, 2018.
[9] F. Panjaitan dan A. Aprilio, "ANALISIS MANAJEMEN RISIKO KEAMANAN JARINGAN MENGGUNAKAN FRAMEWORK NIST," Jurnal Ilmiah MATRIK, 2022.
[10] M. Z. Andriyansa dan F. Panjaitan, "ANALISIS SISTEM KEAMANAN JARINGANMENGGUNAKAN FRAMEWORK NIST," Bina Darma Conference on Computer Science.
[11] T. Tan dan B. Soewita, "MANAJEMEN RISIKO SERANGAN SIBER MENGGUNAKAN FRAMEWORK NIST CYBERSECURITY DI UNIVERSITAS ZXC," Journal of Information System, Applied, Management, Accounting and Research., 2022.
[12] T. S. Putri, N. Mutiah dan D. Prawira, "ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NISTCYBERSECURITY FRAMEWORK DAN ISO/IEC27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," Jurnal Komputer dan Aplikasi, 2022.
[13] R. B. Kusumadewa, S. Z. Sari dan E. A. Hakim, "Analisis Perbandingan Bukti Digial Forensik pada Instant Messaging Berbasis Smartphone Android menggunakan Framework NIST," 2022.
[14] W. S. Prabowo, W. N. A. S, M., H. Muslim dan Y. S. Utama, "MANAJEMEN RISIKO INFRASTRUKTUR CLOUD PEMERINTAH MENGGUNAKAN NIST FRAMEWORK STUDI KASUS LEMBAGA ILMU PENGETAHUAN INDONESIA (LIPI)," Jurnal Penelitian Pos dan Informatika, 2017.
[15] W. Syafitri, "Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)," Jurnal CoreIT, vol. 2, no. 2, pp. 8-13, 2016.