Penilaian Resiko Keamanan Siber Kampus Menggunakan NIST Cybersecurity Framework 1.1 Dengan Peringkat PEGI

Eko Handoyo[1*], Mala Rosa Aprillya[2]
[1]Teknik Komputer, Fakultas Sains Teknologi dan Pendidikan, Universitas Muhammadiyah Lamongan
[2] Teknik Komputer, Fakultas Sains Teknologi dan Pendidikan, Universitas Muhammadiyah Lamongan
Email: [1]ekokurro17@gmail.com, [2] rosaprillya@gmail.com@email.com

Abstract. *The development of information technology is currently progressing rapidly. The threat of information technology that occurs makes many agencies and companies suffered losses. Information security aims to make the information that is guaranteed confidentiality, integrity and its availability. The many threats of information security that have a major impact on institutions need to be carried out by cyber security risk assessment. The campus is one of the implementation of cyber implementation in the scope of education with the amount of data and information that needs to be saved. This study uses the standard Nist Cybersecurity Framework 1.1. is a framework for directing organizations to cyber security activities and security risk assessments. Whereas PEGI is an assessment method used as a solution to analyze e-government where the assessment is 4 lavel, which is very good, good, less and very less. The results of this study obtained the value of the security of the Cyber campus security place the institution at a value of 2.08 with the conclusions that the campus cyber security system is still in less level so it needs to be improved to provide good Cyber Cyber security and data security and information security.*

Keywords: *Campus; Cyber security; NIST; PEGI; Risk*
Abstrak. *Perkembangan teknonogi informasi saat ini maju dengan pesat. Ancaman teknlogi informasi yang terjadi membuat banyak instansi dan perusahaan yang mengalami kerugian. Keamanan informasi bertujuan agar informasi yang dimiliki terjamin kerahasiaannya (confidentiality), keutuhannya (integrity) dan ketersediaannya (availability). Banyaknya ancaman keamanan informasi yang berdampak besar pada institusi perlu dilakukanan penilaian resiko keamanan siber. Kampus yang menjadi salah satu penimplementasian siber dalam ruang lingkup pendidikan dengan banyaknya data dan informasi yang perlu dipastikan keamananya. Penelitian ini menggunakan standar NIST Cybersecurity Framework 1.1. merupakan kerangka kerja untuk mengarahkan organisasi pada aktivitas keamanan siber dan asesemen resiko keamanan. Sedangkan PEGI adalah metode penilaian yang digunakan sebagai solusi untuk menanalisis E-Government dimana penilaian terdapat 4 lavel yaitu sangat baik, baik, kurang dan sangat kurang. Hasil dari penelitian ini didapatkan nilai Resiko keamanan siber kampus menempatkan intitusi pada nilai 2,08 dengan kesimpualan bahwa sistem keamanan siber kampus masih dalam level kurang sehingga perlu ditingkatkan untuk memberikan keamanan siber kampus yang baik dan mejanga keamanan data dan informasi.*
Kata Kunci: *Cybersecurity; Kampus; NIST; PEGI; Resiko*

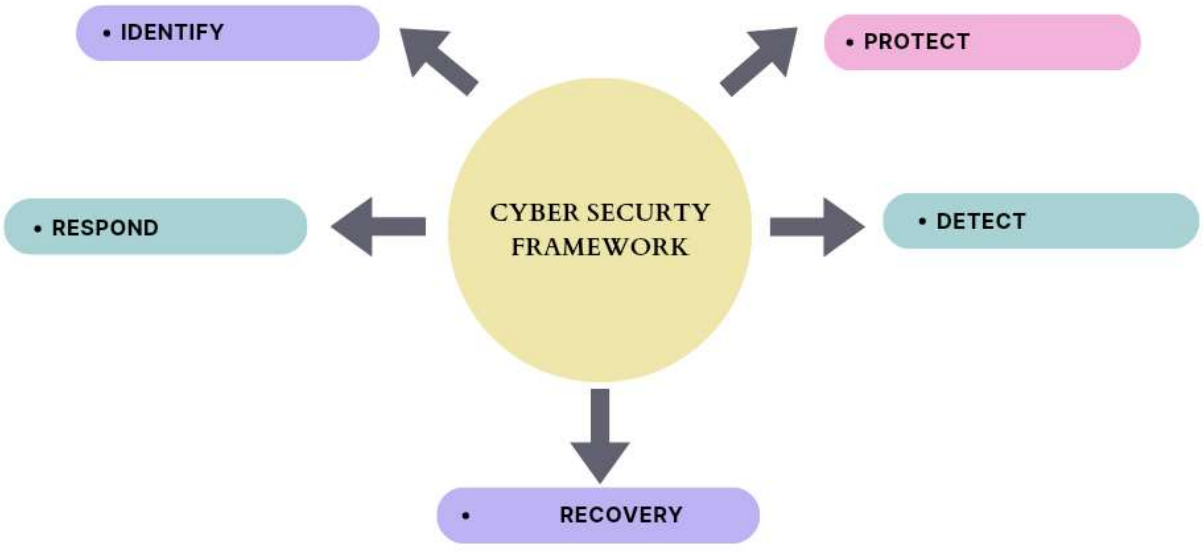
1. Pendahuluan

Perkembangan teknonogi informasi saat ini maju dengan pesat, perkembangan teknologi juga mulai mengeksodus hampir seluruh kehidupan manusia. pesatnya kemajuan teknologi memunculkan ancaman baru dalam bidang tersebut. Dampak ancaman yang terjadi membuat banyak instansi dan perusahaan yang mengalami kerugian. Salah satu aspek TI yang perlu diperhatikan adalah Keamanan Informasi. Dukungan keamanan informasi bertujuan agar informasi yang dimiliki terjamin kerahasiaannya (confidentiality), keutuhannya (integrity) dan ketersediaannya (availability) (Umar *et al*., 2017)seperti pada Gambar.1

 ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Gambar 1. Aspek keamanan TI

Banyaknya ancaman keamanan informasi yang berdampak besar pada institusi perlu dilakukanan penilaian resiko keamanan siber. Penilaian keamanan siber ini mengunakan NIST Cybersecurity Framework 1.1. merupakan kerangka kerja yang dapat digunakan untuk mengarahkan organisasi pada aktivitas keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses manajemennya. Kerangka kerja ini memberikan panduan dan tahapan dalam meningkatkan keamanan siber melalui analisis risiko keamanan siber. Framework core terdiri dari 5 fungsi, yaitu identifikasi *(identify);* perlindungan *(protect);* deteksi *(detect);* respon *(respond);* dan pemulihan *(recovery),* 22 kategori dan 100 subkategori yang cocok dengan contoh referensi informatifnya,(Handoyo, 2020)seperti pada Gambar.2



Gambar 2. *Cybersecurity framework.*

Istilah Perguruan Tinggi yang digunakan untuk lapisan ke-2, identik dengan istilah Perguruan Tinggi yang disebut dalam Peraturan Pemerintah No.30 th 1990, yaitu organisasi satuan pendidikan, yang menyelenggarakan pendidikan di jenjang pendidikan tinggi, penelitian dan pengabdian kepada masyarakat. Sistem ini bertujuan untuk mendukung penyelenggaraan pendidikan, sehingga kampus

dapat menyediakan layanan informasi yang lebih baik dan efektif kepada civitas akademika, baik didalam maupun diluar kampus melalui internet(Bianto and Aprillya, 2022).

PEGI adalah model yang dibuat oleh Direktorat E-Government, Direktorat Jenderal Aplikasi dan Telematika, Kementerian Komunikasi dan Informasi (Kementerian Kominfo) Yang Dapat Dapat Digunakan Sebagai Solusi untukK Menanalisis E-Government. PEGI memiliki lima dimensi penilaian, yaitu setiap kebijakan, kelembagaan, infrastruktur, aplikasi dan perencanaan. Setiap dimensi memiliki bobot yang sama dalam penilaian karena semuanya penting, saling terkait dan saling mendukung.

Tujuan penelitian ini menghasilkan penilaian Risiko keamanan siber kampus dengan menggunakan NIST *cybersecurity framework* 1.1 sebagai acuan standar. Studi kasus dilaksanakan di universitas Muhammadiyah lamongan, analisa resiko dihasilkan dari penggolahan data responden yang didasarkan atas Peringkat E-Government Indonesia (PEGI). Hasil penelitian keseluruhan yaitu menghasilkan adalah pemeringkatan (level) penilaian resiko siber kampus.

2. Tinjauan Pustaka

Berikut ini daftar publikasi jurnal dan prosiding yang digunakan sebagai penelitian yang paling relevan : Penelitian yang berjudul " Cyber security analysis of academic services based on domain delivery services and support using indonesian e-government ratings (PEGI)"penelitian ini mempunyai tujuan untuk melakukan analisis keamanan SIA dengan standar COBIT 5 pada domain Delivery service dan support menggunakan penilaian PEGI dengan hasil bahwa sistem kemanan yang diterapakan sangat handal dan efektif (Riadi, Riyadi Yanto and Handoyo, 2020)

Penelitian yang berjudul "Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad" penelitian ini menpunyai tujuan untuk mengalasisa kemanan data website dengan metode CIA Traid dengan hasil telah memenuhi 3 indikator utama keamanan informasi yang terdiri atas confidentiality, integrity dan *availability*(Hermawan *et al.*, 2022).

Penilitian yang berjudul "Manajemen risiko serangan siber Menggunakan framework NIST Cybersecurity di universitas ZXY" penelitan ini bertujuan untuk menganaslisa menajemn seriko sernagan siber mengunakan standar NIST cyberscurity dengan hasil bahawa kampus telah melakukan majamen kemanan dengan baik sesuai dengan standar yang ada(Tan and Soewito, 2022).

Penelitian yang berjudul "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST SP 800 – 55" Penelitinan ini bertujuan untuk menganalisa tingkat keamanan informasi dengan megkomparasikan metode COBIT 5 dengan NIST SP 800-55 dengan hasil bahwa standar NIST lebih komplesitas dan detail di bandingkan dengan standar COBIT 5 DSS05(Handoyo, 2020).

Penelitian yang berjudul "Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI" Penelitian ini bertujuan menganalisa keamanan SIA dengan standar COBIT 5 menggunakan CMMI. Penelitian ini dengan hasil memberikan anlisis yang baik terhadap keamanan SIA dengan hasil yang optimal(Riadi, Yanto and Handoyo, 2020).

3. Metode Penelitian

Penelitian ini diperlukan data dan informasi yang lengkap guna mendukung tahapan pengujian yang akan dilakukan. Metode pengumpulan data yang digunakan adalah seperti pada gambar pada Gambar. 3

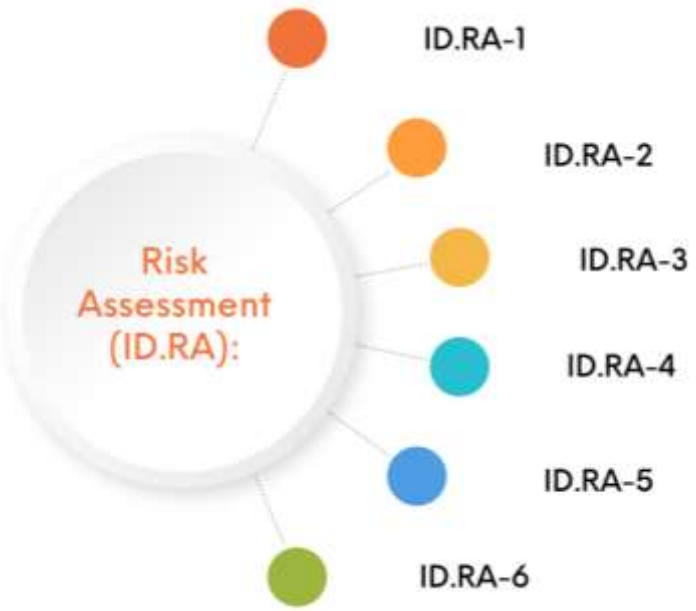
 ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Gambar 3. *Flowchart* penelitian

1. Studi Literarur: proses penegumpulan data dan informasi baik artikel, buku, jurnal dan juga prosiding untuk mendukung objek penelitian yang akan dilakukan.
2. Mapping standar NIST: proses terkait merancang terkait daftar tilik yang akan di laukakan dengan metode stanadar yang sudah disediakan oleh NIST.
3. Penentuan Nilai PEGI: proses perhitungan dan pengolahan data dan fakta dari hasil audit, menentukan hasil audit sehingga akan terlihat temuan-temuan yang harus dipertahankan dan yang harus diperbaiki.
4. Pengolahan data: proses dari perhitnungan dari data yang telah didaptkan dari daftar tilik yang dilakukan. Proses ini untuk mendapatkan nilai hasil dari penelitian.
5. Analisis hasil: Analisa hasil yang telah dilakukan dilakuakn penyusunan rekomendasi untuk perbaikan keamanan siber kedepnya dari institusi.

3.1 Standar NIST Cybersecurity *Framework* 1.1

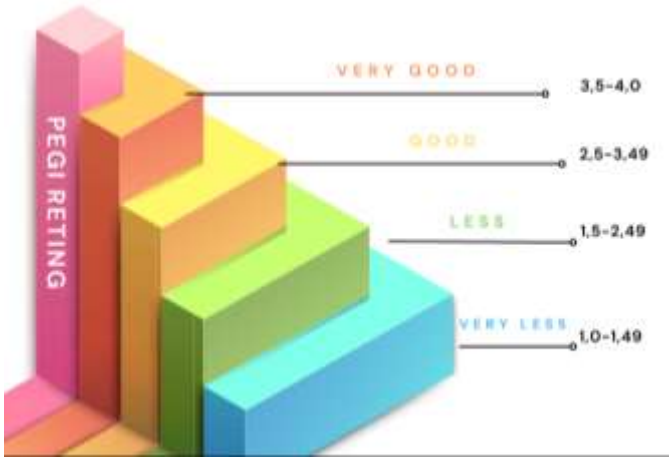
Standar NIST Cybersecurity Framework 1.1 dalam penalian resiko keamanan berada pada fungsi identifikasi dan katagori *Risk Assessment* yang memiliki 6 subkatagori(Ghazouani, Faris and Medromi, 2014),sebagaimana pada Gambar.4.



Gambar 4. ***Risk assessment***

3.2 Metode PEGI

Metode PEGI Secara umum, penilaian pemerintahan e-government Indonesia ditunjukkan memiliki 4 tigkatan peniliaian dari tingkatan sangat baik, baik, kurang dan sangat kurang(Riadi, Riyadi Yanto and Handoyo, 2020), seperti pada Gambar.5



Gambar 5. Pemeringkatan penilaian PEGI

4. Hasil dan Pembahasan

Pembahasan dan hasil dalam penelitian ini sebagai berikut :

4.1 Mapping Standar Cyaberscurity Framework 1.1

Berisi Proses penelitian dimulai dengan studi literiasi terkait penliaian resiko keamanan siber kampus menggunakan NIST cyberscurity framework 1.1 dengan metode PEGI. Proses berikutnya adalah melakukan mapping standar cyberscurity framework 1.1 dimulai dengan memilih standar yg berkaitan dengan penliaian resiko, didapati bahawa berada pada fungsi identifikasi dan katagori Risk assessment seperti pada Gambar. 6.

ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Gambar 6. ***Identify***

Setelah bisa mentukan fungsi maka berikutnya kita mentukan katagori risk assesment yang berisikan 6 subkatagori sepeti pada Gambar.4. Proses berikutnya adalah melakukan singkronisasi subkatagori dengan NIST SP 800 – 55 Rev.4 sepeti pada Tabel 1.

Tabel 1. Singkronisasi ID.RA dengan nsit sp 800-53

Category	***Subcategory***	***NIST SP 800-53 Rev. 4 Control Identifier***
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	*ID.RA-1: Asset vulnerabilities are identified and documented*	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	SI-5, PM-15, PM-16
	ID.RA-3: Threats, both internal and external, are identified and documented	RA-3, SI-5, PM-12, PM-16
	ID.RA-4: Potential business impacts and likelihoods are identified	RA-2, RA-3, SA-14, PM-9, PM-11
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	RA-2, RA-3, PM-16
	ID.RA-6: Risk responses are identified and prioritized	PM-4, PM-9

Proses berikutnya adalah membuat daftar tilik asesmen berdasarkan kontrol indentifikasi NIST SP 800-53 Rev. 4 yang berisikan daftar diskusi asesmen, seperti pada Tabel 2. daftar tilik asesmen ini terdiri dari 96 komponen yang akan diasesemen pada pemangku kepentingan.

Tabel 2. Daftar tilik asesmen

Control Identifier	Control Name	Discussion
PM-16	Program Kesadaran Ancaman	Menerapkan program kesadaran ancaman yang mencakup kemampuan berbagi informasi silang untuk intelijen ancaman.
PM-16(1)	Program Kesadaran Ancaman | Sarana otomatis untuk berbagi intelijen ancaman	Mempekerjakan mekanisme otomatis untuk memaksimalkan efektivitas berbagi informasi intelijen ancaman.
SI-5(1)	Peringatan, Penasihat, dan Arahan Keamanan | Peringatan dan nasihat otomatis	Peringatan Keamanan dan Informasi Penasihat Keamanan di seluruh organisasi menggunakan [penugasan: mekanisme otomatis yang ditentukan organisasi].

4.2 Penilaian Peringkat E-Government Indonesia (PEGI)

Proses ini merupakan proses penyusunan penilian dengan metode PEGI. Daftar tilik asesmen yang sudah dibuat akan dikombinasikan dengan pemeringaktan dari metode PEGI. Secara umum, penilaian pemerintahan e-government Indonesia ditunjukkan pada Gambar.4 dan dijelaskan :

1. **Nilai 1.0-1.49 (sangat kurang):** Indikator tidak ada sama sekali atau sangat kurang dalam hal kuantitas dan kualitas.
2. **Nilai 1.5-2.49 (Kurang):** Indikator sudah ada, tetapi masih perlu ditambahkan dalam hal kuantitas dan peningkatan kualitas.
3. **Nilai 2,5-3,49 (Baik):** Indikator jumlah dan kualitas cukup baik dan dapat dilihat memiliki dampak positif pada penggunaan e-government, tetapi perbaikan diperlukan untuk mempertahankan kesinambungan implementasi dalam masa depan.
4. **Nilai 3.5-4.0 (sangat baik):** Indikator baik dalam hal kuantitas dan kualitas yang sangat baik. Dampak penerapan e-government sangat nyata. Kesiapan untuk terus dikembangkan di masa depan terlihat jelas[12].

Proses penilaian daftar tilik asesmen dengan penilanan PEGI didapatkan hasil sebagaimana pada Tabel 3. Berisi hasil pembahasan dan bisa perbandingan dari hasil penelitian sebelumnya.

Tabel 3. Hasil Penilaian Daftar Tilik Asesemen Dengan PEGI

Subcategory	*Control Identifier*	*Control Name*	Hasil Asesmen	Nilai
CA-2	CA-2(1)	*Independent Assessors*	sangat kurang	1
	CA-2(2)	*Specialized Assessments*	sangat kurang	1
	CA-2(3)	*Leveraging Results from External Organizations*	kurang	2
Nilai Rata-rata	**CA-2**	***Control Assessments***		**1,33**

4.3 Pengolahan Data dan Hasil

Peroses Pengolahan data dimulai dari mengumpulkan seluruh nilai rata-rata dari setiap Control Identifier. Terdapat 26 Control Identifier yang sudah dilakukan penilaian dengan metode PEGI, seperti terdapat pada Tabel 4.

ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Tabel 4. Hasil Penilaian Control Identifiter

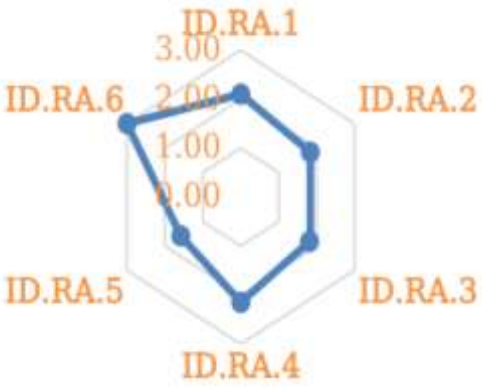
Subcategory	*Control Identifier*	Nilai PEGI	rata-rata Nilai
ID.RA.1	CA-2	1.33	2.10
	CA-7	2.67	
	CA-8	2.33	
	RA-3	1.75	
	RA-5	2.64	
	SA-5	1.60	
	SA-11	2.22	
	SI-4	1.88	
	SI-5	2.50	
ID.RA.2	SI-5	2.50	1.83
	PM-15	2.00	
	PM-16	1.00	
ID.RA.3	RA-3	1.75	1.81
	SI-5	2.50	
ID.RA.4	PM-12	2.00	2.15
	PM-16	1.00	
	RA-2	2.00	
	RA-3	1.75	
	SA-14	2.00	
	PM-9	3.00	
	PM-11	2.00	
ID.RA.5	RA-2	2.00	1.58
	RA-3	1.75	
	PM-16	1.00	
ID.RA.6	PM-4	3.00	3.00
	PM-9	3.00	

Berdasarkan hasil penilaian control *identifiter* maka bisa meghitung keseluruhan nilai dari *subcategory* pada proses *Risk Assessment* (ID.RA), seperti pada Tabel 5.

Tabel 5. Penilaian subcategory

Subcategory	Nilai
ID.RA.1	2.10
ID.RA.2	1.83
ID.RA.3	1.81
ID.RA.4	2.15
ID.RA.5	1.58
ID.RA.6	3.00
Rata-rata *Subcategory*	**2.08**

Berdasarkan hasil Penilaian subcatagory yang sudah dilakukan dapat dibuat diagram pemosisian penilain resiko keamanan siber kampsu bisa dilihat pada Gambar.7



Gambar 6. Pemosisian *Risk Assessment* (ID.RA)

Berdasarkan perhitungan metode penilaian Peringkat E-Government Indonesia (PEGI) didapati bahwa penilaian resiko keamanan siber dengan menggunakan standar NIST *Cybersecurity Framework* 1.1 memperoleh nilai 2,08 sehingga menempatkan instistusi kampus berada pada kondisi keamanan siber kurang dan perlu ditingkatkan.

5. Kesimpulan

Kesimpulan dari penelitian ini adalah :

1. Standar NIST Cybersecurity Framework 1.1 mampu menjawab kebutahan akan standar penilaian resiko keamanan siber yang kompleks.
2. Metode penilaian Peringkat E-Government Indonesia (PEGI) mampu memberikan tingkat penilaian yang baik dengan sekala minumum 1 dan maksimal 4.
3. Resiko keamanan siber kampus menempatkan intitusi pada nilai 2,08 dengan kesimpualan bahwa sistem keamanan siber kampus masih dalam level kurang sehingga perlu ditingkatkan.

Saran untuk peneliti selanjutnya adalah mampu mengkombinasikan standar NIST Cybersecurity Framework 1.1 dengan metode penilaian yang lain sehingga didapatkan hasil yang berbeda untuk dilakukan komparasi.

Ucapan Terimakasih

Ucapan terima kasih penulis kepada universitas Muhammadiyah Lamonagn membatu dalam pembiayayan riset melalu sekema Peneltian dosen pemuala yang saya terima, terima kasih pula kepada Universitas Muhammadiyah Lamoangan yang telah menfasiltasi kegitan penelitian dengan baik.

Referensi

Bianto, A. and Aprillya, M.R. (2022) *Sistem Pendukung Keputusan Identifikasi Daerah Potensi Banjir Dengan Metode Multi Attribute Utility Theory (Studi Kasus: Kabupaten Lamongan) 116 Sistem Pendukung Keputusan Identifikasi Daerah Potensi Banjir Dengan Metode Multi Attribute Utility Theory (Studi Kasus: Kabupaten Lamongan)*.

Ghazouani, M., Faris, S. and Medromi, H. (2014) *Information Security Risk Assessment-A Practical Approach with a Mathematical Formulation of Risk, International Journal of Computer Applications*. Available at: http://www.risicare.fr.

Handoyo, E. (2020) 'Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55', *Jurnal CoSciTech (Computer Science and Information Technology)*, 1(2), pp. 76–83. Available at: https://doi.org/10.37859/coscitech.v1i2.2199.

Hermawan, A. *et al.* (2022) 'Analisa Keamanan Data melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad', 7(3), pp. 125–130.

Riadi, I., Riyadi Yanto, I.T. and Handoyo, E. (2020) 'Cyber Security Analysis of Academic Services based on Domain Delivery Services and Support using Indonesian E-Government Ratings (PEGI)', *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, pp. 263–270. Available at: https://doi.org/10.22219/kinetik.v5i4.1083.

Riadi, I., Yanto, I.T.R. and Handoyo, E. (2020) 'Analysis of academic service cybersecurity in university based on framework COBIT 5 using CMMI', in *IOP Conference Series: Materials Science and Engineering*. Institute of Physics Publishing. Available at: https://doi.org/10.1088/1757-899X/821/1/012003.

Tan, T. and Soewito, B. (2022) 'Manajemen Risiko Serangan Siber Menggunakan Framework Nist Cybersecurity Di Universitas Zxc', *Journal of Information System, Applied, Management, Accounting and Research*, 6(2), pp. 411–422. Available at: https://doi.org/10.52362/jisamar.v6i2.781.

ISSN: 2579-566X (Online)
ISSN: 2477-5274 (Print)

Umar, R. *et al*. (2017) *ANALISIS TATA KELOLA TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 PADA DOMAIN DELIVERY, SERVICE, AND SUPPORT (DSS), Seminar Nasional Teknologi Informasi dan Komunikasi-SEMANTIKOM*.