Vol. 4, No. 3, Desember 2023, hal. 677-685

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity NIST 1.1

Eko Handoyo*[1], Izza Eka Nigrum[2]
Email: [1]ekokurro17@gmail.com, [2]izzaeka@gmail.com

[1]Teknik komputer, Fakultas Sains Teknologi dan Pendidikan, Universitas Muhammdiyah Lamongan
[2]Fisika, Fakultas Sains Teknologi dan Pendidikan, Universitas Muhammdiyah Lamongan

Diterima: 25 Agustus 2023 | Direvisi: 27 Agustus 2023 | Disetujui: 1 Januari 2024

Abstrak

Revulusi Industri 4.0 memaksa institusi dan perusahanan untuk mulai berbenaha dalam impelmentasi teknologi informasi untuk mampu bersaing dengan baik. Kampus menjadi salah satu sektor yang paling masif dalam pengembangan dan implentasi teknologi informasi. Karena banyak sekali layanan dan proses bisnis yang ada dalam sistem kampus.Sistem bisnis kampus yang komples dan memiliki banyak data di informasi tentu menimbulkan ancaman dalam sektor keamanan teknolgi infomasi. Keamanan teknolgi tentu harus menjamin kerahasiaannya, keutuhannya dan ketersediaannya.Penaggulangan terkait ancaman *cyberscurity* dapat dengan melakukan penilaian resiko *cyberscurity.* Standar untuk melakakukan penilaian *cyberscurity* sepeti *COBIT 5, NIST, dan ISO 20071.* Setiap standar memiliki modul-modul audit yang bertujuan untuk membuat instusi menjadi *good gaverment*. Standar *NIST Cybersecurity Framework 1.1* bertujuan untuk memanajemen institusi pada aktivitas keamanan siber dengan mempertimbangkan risiko keamanan siber sebagai bagian utama dari proses manajemennya. Tujuan penelitian menghasilkan nilai risiko keamanan siber kampus dengan menggunakan *NIST cybersecurity framework 1.1* sebagai acuan standar. Hasil penelitian keseluruhan yaitu menghasilkan adalah pemeringkatan (level) penilaian resiko siber kampus. Penilaian resiko keamanan siber kampus ini didapatkan hasil nilai 1,20 sehingga menempatkan instistusi kampus berada pada kondisi keamanan siber "*Partial Implemented*" dimana kampus melaksanakan kontrol pada f*ramework* seperlunya saja dan belum terdokumentasidan sehingga perlu ditingkatkan terkait kontrol dan pendokumntasian dengan baik untuk mengkatkan keamanan siber yang lebih baik..

Kata kunci: *Cybersecurity, Framework,* Kampus, *NIST,* Risiko

Cyber campus safety risk assessment using NIST cybersecurity framework 1.1

Abstract

The Industrial Revolution 4.0 forced institutions and companies to start improving the implementation of information technology to be able to compete well.The campus is one of the most massive sectors in the development and implementation of information technology.Because there are so many services and business processes that exist in the campus system.Campus business systems that are complex and have a lot of data in the information certainly pose a threat in the information technology security sector.Technological security must of course guarantee its confidentiality, integrity and availability. Countermeasures related to cybersecurity threats can be carried out by conducting a cyber security risk assessment.Standards for conducting cyber security assessments include COBIT 5, NIST, and ISO 20071. Each standard has audit modules that aim to make the institution a good government.NIST Cybersecurity Framework 1.1 is a standard used to direct organizations to cybersecurity activities and consider cybersecurity risks as part of their management process. The purpose of this study is to produce an assessment of campus cybersecurity risks using the NIST cybersecurity framework 1.1 as a standard reference.The overall result of the research, which is to produce, is the ranking of campus cyber risk assessments.The assessment of campus cyber security risks resulted in a value of 1.20, placing the campus institution in a "Partially Implemented" cybersecurity condition.Where campuses

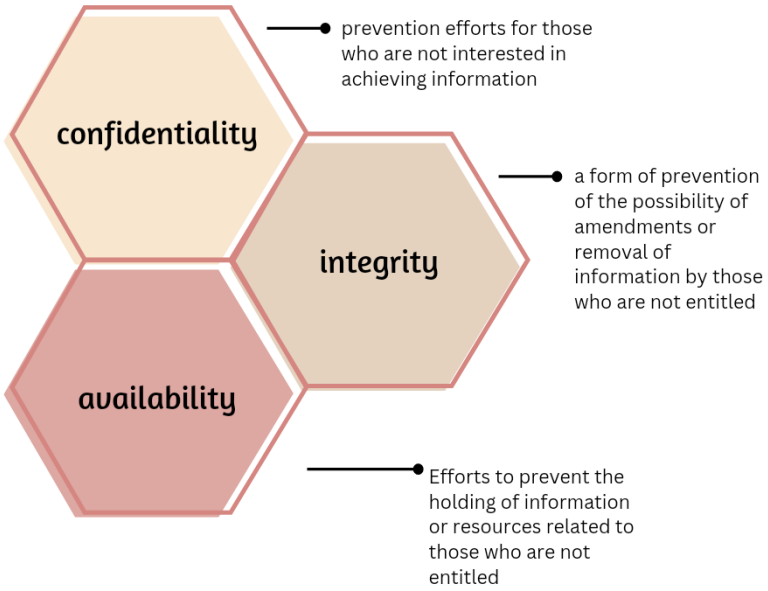
only carry out control on the framework as necessary and have not been documented, and so it needs to be improved regarding proper control and documentation to improve better cyber security.

Keywords: *Campus, Cybersecurity, Framework, NIST, Risk*

1. PENDAHULUAN

Revulusi Industri 4.0 memaksa institusi dan perusahanan untuk mulai berbenaha dalam impelmentasi teknologi informasi untuk mampu bersaing dengan baik. Penggunan teknologi informasi juga meramba dalam bidang pendidikan tidak terkeculai kampus. Kampus menjadi salah satu sektor yang paling masif dalam pengembangan dan implentasi teknologi informasi. Karena banyak sekali layanan dan proses bisnis yang ada dalam sistem kampus. Implentasi teknologi sepeti Sistem Infromasi akademik, Keuangan, Aset bahkan sistem seklsi penerimaan mahasiswa baru[1].

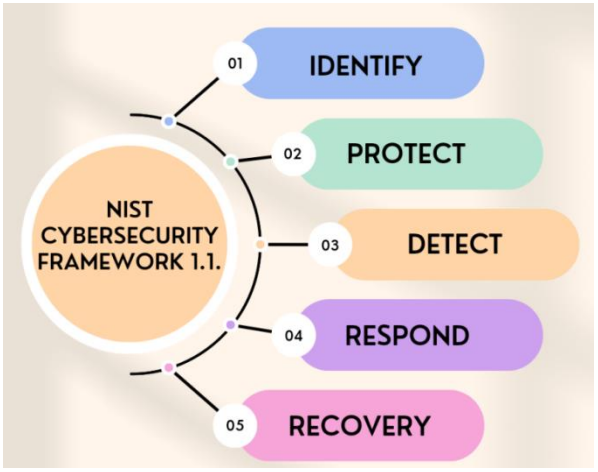
Sistem bisnis kampus yang komples dan memiliki banyak data di informasi tentu menimbulkan ancaman dalam sektor keamanan teknolgi infomasi. Timbulnya ancanaman tentu institusi harus melakukan upaya metigasi detaksi dini terkait peluang terjadinya ancaman keamanan. Keamanan teknolgi tentu harus menjamin kerahasiaannya, keutuhannya dan ketersediaannya seperti pada[2] Gambar 1.



Gambar 1. Aspek keamanan IT

Luang lingkup sistem teknologi kampus yang saat ini berbasis online dengan media internet tentu memudahkan akses pengunanya, disisi lain menimbulkan ancaman yang lebih besar disektor cyberscurity. Penaggulangan terkait ancaman cyberscurity dapat dengan melakukan penilaian resiko cyberscurity. Standar untuk melakakukan penilaian cyberscurity sepeti COBIT 5, NIST, dan ISO 20071. Setiap standar memiliki modul-modul audit yang bertujuan untuk membuat instusi menjadi *good gaverment*[3].

NIST Cybersecurity Framework 1.1 merupakan sebuah standar untuk melakukan manajemen terkait keamanan sisber kampus dengan mengarahkan institusi pada aktivitas mempertimbangkan risiko keamanan siber sebagai bagian utama prosesnya. Kerangka kerja ini memberikan panduan dan tahapan dalam meningkatkan keamanan siber melalui analisis risiko keamanan siber. NIST Cybersecurity Framework 1.1 terdiri dari 5 fungsi, yaitu *identify; protect*; *detect*; *respond*; dan *recovery* yang tepat dengan contoh referensi informatifnya [4], [5]seperti pada gambar 2.



Gambar 2. NIST Cybersecurity Framework 1.1

Penelitian ini memiliki sumber ilmu dasar untuk menganalisis menggunakan *NIST cybersecurity framework* 1.1. dibawah ini merupakakan literatur yang menjadi acuan penelitian tentang *cybersecurity framework*:

a. Penelitian oleh Victor Ilyas Sugara pada Jurnal KOMPUTASI dengan judul "SISTEM PEMERIKSA KEAMANAN INFORMASI MENGGUNAKAN NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK" penelitian dengan standar NIST Cybersecurity Framework digunakan untuk menganalisis keamanan PT NPI, UML unutk pemgembangan prototaipe sistem keamanan, hasil yang di dapatkan adalah recoveri (58.33%), Respon (23.33%), identifikasi (25%), dan perlindungan (32.86%), dengan nilai keseluruhan 27.55%[6].

b. Penelitian yang dilakukan oleh Imam Riadi dipublikasi pada jurnal Kinetik dengan judul "*Cyber security analysis of academic services based on domain delivery services and support using indonesian e-government ratings (PEGI)"* pada 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[7].

c. Penelitian yang dilakukan oleh Tony Tan dipublikasi pada jurnal JISAMAR dengan judul "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[8].

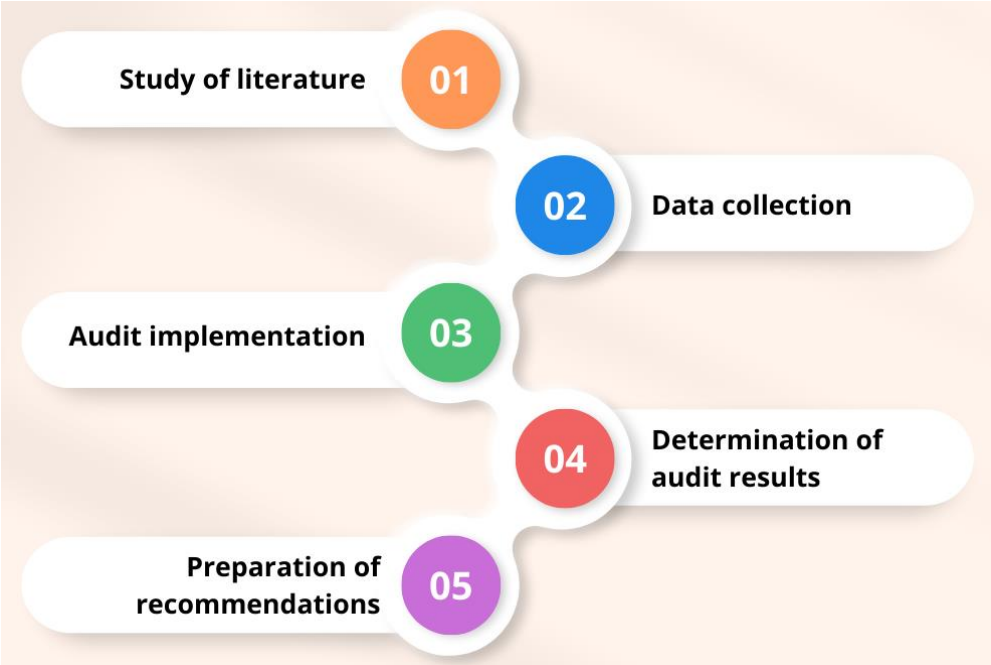
d. Penelitian yang dilakukan oleh Risma Anggraini dipublikasi pada jurnal Jurnal Teknologi dan Manajemen dengan judul "analisis keamanan *private cloud* berbasis *framework NISTCS* di PT. XYZ" penelitian ini memberikan hasil analisis keamanan sistem informasi dan mengetahui kelemahannya, menyususn rekomendasi terkait keamanan siber sistem informasi private cloud di instansi menggunakan standar *framework NIST Cybersecurity*. Hasil Analisa didapatkan rencana tindakan dari pengolahan SDM dan teknologi bebas dari ancaman dan serangan, memberikan sistem yang efisien dan mendetesi acaman dini dalam proses *privat cloud*. data dan informasi dapat dijaga kerahasiaannya[9].

e. Penelitian yang dilakukan oleh Tasha Safira Putri dipublikasi pada jurnal Coding : Jurnal Komputer dan Aplikasi dengan judul "analisis manajemen risiko keamanan informasi menggunakan nistcybersecurity framework DAN ISO/IEC27001:2013" penelitian ini bertujuan memberikan nilai terkait resiko keamanan sistem informasi dengan standar NIST Cybersecurity Framework Dan ISO/IEC 27001:2013 untuk pengamanan kesenjangan aset informasi. analisis yang di daptkan adalah gap keamanan informasi, didominasi oleh kemenan data, mitigasi, penilian resiko dan pemulihan di daptkan nilai yang redah dengan 36 ancaman. merekomendasikan untuk memberikan implentasi keamanan yang semakn baik pada proses tersebut.[10].

Tujuan penelitian adalah mendapatkan nilai Risiko keamanan siber kampus dengan menggunakan NIST *cybersecurity framework 1.1* sebagai acuan standar. Hasil penelitian keseluruhan yaitu menghasilkan adalah pemeringkatan (level) penilaian resiko siber kampus.

2. METODE PENELITIAN

Pada penelitian ini dilakukan beberapa tahapan, sepeti pada gambar 3.



Gambar 3. Metode penelitian

1. Studi Literarur : proses penegumpulan data dan informasi baik artikel, buku, jurnal dan juga prosiding untuk mendukung objek penelitian yang akan dilakukan[11].

2. Pengumpulan data pendukung : proses menemukan fakta dari data dan informasi secara langsung ke pemangku kepetingan dan pihak-pihak yang kompeten dalam bidang keamaman teknolgi siber kampus.

3. Pelaksanaan Audit isntitusi: proes observasi dan wawancara langsung dengan mengunakan daftar tilik audit dengan standar *NIST CyberSecurity Framework.*

4. Penentuan Nilai dan Hasil Audit: 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.

5. Penyusunan rekomendasi untuk institusi : dari hasil Analisa hasil yang telah dilakukan dilakuakn penyusunan rekomendasi untuk perbaikan keamanan siber kedepnya dari institusi [12].

3. HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan ini dijelaskan secara lengkap tahapan penelitian yang dilakukan. Seperti pada bagian sebelumnya, penelitian ini memiliki empat tahap. Pada bagian ini akan dibahas hasil yang diperoleh pada setiap tahapan.

3.1. Pengumpulan data pendukung

Proses pengumpulan data pendukung adalah menemukan fakta dari data dan informasi secara langsung ke pemangku kepetingan dan pihak-pihak yang kompeten dalam bidang keamaman teknolgi siber kampus dilakukan dengan cara observasi, diskusi, mengulas sistem yang berjalan saat ini melalui wawancara dan mempelajari dokumen-dokumen pendukung penelitian.

3.2. Pembuatan Daftar Tilik Asesmen

Proses ini adalah kita mulai memetakan terkait standar NIST *framework core* ini adalah Fungsi dan Kategori seperti pada table 1. *Framework Core* di kampus dilihat pada system keamana yang digunakan untuk menilai fungsi dan katagori mana yang akan dibuat.

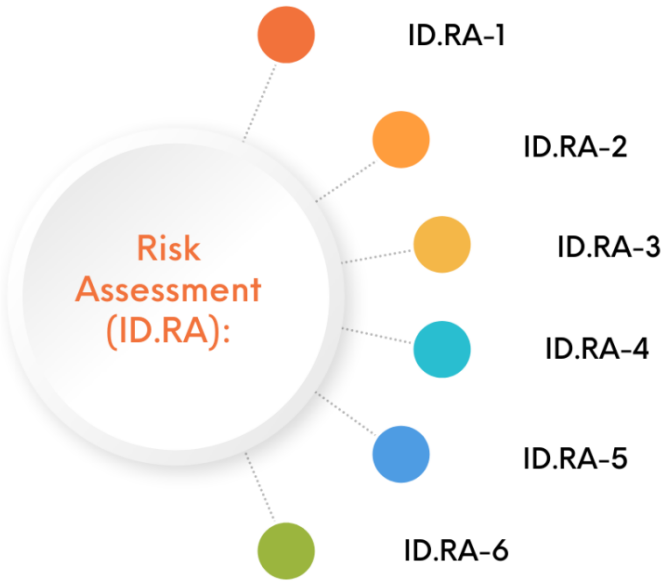
Tabel 1. *Framework Core NIST*

Fungsi	Katagori
Identifikasi	Asset Management
	Lingkungan bisnis
	Tata Kelola
	Tugas beresiko
	Strategi Manajemen Risiko
Melindungi	Kontrol akses
	Kesadaran dan Pelatihan
	Keamanan data
	Proses dan Prosedur Perlindungan Informasi
	Pemeliharaan
Deteksi	Teknologi Pelindung
	Anomali dan Peristiwa
	Pemantauan Keamanan Berkelanjutan
	Proses Deteksi
Menanggapi	Perencanaan Respons
	Komunikasi
	Analisis
	Mitigasi
	Perbaikan
Pulihan	Perencanaan Pemulihan
	Perbaikan
	Komunikasi

Fugsi yang dipilih dalam penelitian terkait penilaian resiko keamanan siber ada dalam *identify* dan pada *category risk assesment*, seperti pada Gambar 4.

Gambar 4. Identifikasi

Setelah kita mentukan *category risk assesment* yang berisikan 6 subkatagori sepeti pada Gambar 5. Proses berikutnya adalah melakukan singkronisasi subkatagori dengan NIST SP 800 – 55 Rev.4 sepeti pada Tabel 2.



Gambar 5. *Risk Assesment*

Tabel 2. *Singkronisasi ID.RA dengan NIST SP- 800-53*

Subcategory	**NIST SP 800-53 Rev. 4 Control Identifier**
ID.RA-1: Kerentanan aset diidentifikasi dan didokumentasikan	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Intelijen ancaman dunia maya diterima dari forum dan sumber berbagi informasi	SI-5, PM-15, PM-16
ID.RA-3: Ancaman, baik internal maupun eksternal, diidentifikasi dan didokumentasikan	RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potensi dampak dan kemungkinan bisnis diidentifikasi	RA-2, RA-3, SA-14, PM-9, PM-11
ID.RA-5: Ancaman, kerentanan, kemungkinan, dan dampak digunakan untuk menentukan risiko	RA-2, RA-3, PM-16
ID.RA-6: Respons risiko diidentifikasi dan diprioritaskan	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 3. daftar tilik asesmen ini terdiri dari 96 komponen yang akan diasesemen pada pemangku kepentingan.

Tabel 3. *Daftar Tilik Assesmen*

Control Identifier	***Control Name***	***Control Text***
RA-2	*Security Categorization*	A. Mengkategorikan sistem dan informasi yang diproses, disimpan, dan dikirimkan; B. Dokumentasikan hasil kategorisasi keamanan, termasuk alasan pendukung, dalam rencana keamanan sistem; Dan C. Verifikasi bahwa pejabat yang memberi wewenang atau perwakilan resmi yang ditunjuk meninjau dan menyetujui keputusan kategorisasi keamanan.
RA-2(1)	*Impact-level Prioritization*	Melakukan prioritas tingkat dampak sistem organisasi untuk mendapatkan rincian tambahan pada tingkat dampak sistem.
RA-3	*Risk Assessment*	A. Melakukan penilaian risiko, termasuk: 1. Mengidentifikasi ancaman dan kerentanan pada sistem; 2. Menentukan kemungkinan dan besarnya kerugian akibat akses, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran sistem yang tidak sah, informasi yang diproses, disimpan, atau dikirimkan, dan informasi terkait lainnya; Dan 3. Menentukan kemungkinan dan dampak dampak buruk pada individu yang timbul dari pemrosesan informasi identitas pribadi;

		B. Mengintegrasikan hasil penilaian risiko dan keputusan manajemen risiko dari perspektif organisasi dan misi atau proses bisnis dengan penilaian risiko tingkat sistem; C. Dokumentasikan hasil penilaian risiko di [Pilihan: rencana keamanan dan privasi; laporan penilaian risiko; [Tugas: dokumen yang ditentukan organisasi]]; D. Tinjau hasil penilaian risiko [Penugasan: frekuensi yang ditentukan organisasi]; e. Menyebarkan hasil penilaian risiko ke [Penugasan: personel atau peran yang ditentukan organisasi]; Dan F. Perbarui penilaian risiko [Penugasan: frekuensi yang ditentukan organisasi] atau ketika ada perubahan signifikan pada sistem, lingkungan operasinya, atau kondisi lain yang dapat memengaruhi status keamanan atau privasi sistem.

3.3. Penilaian

Penilaian jawaban dari masing-masing kontrol *framework* dibagi dalam 3 bagian penilaian yaitu[6] :

- **Diimplementasikan Penuh**, institusi melaksanakan seluruh kontrol secara menyeluruh, rutin dan terdokumentasi.
- **Diimplementasikan Sebagian**, institusi melaksanakan sebgian kontrol seperlunya saja dan biasanya dan belum terdokumentasi.
- **Tidak Diimplementasikan**, institusi tidak melaksanakan semua kontrol standar.

Penilaian yang dilakukan terhadap jawaban yang didapat dapat dilihat pada tabel 4 berikut:

Tabel 4. Penilaian Jawaban

No	Jawaban	Nilai
1	*Diimplementasikan Penuh*	2
2	*Partial Implemented*	1
3	*Not Implemented*	0

Rumus perhitungan framwork dengan nilai presentasinya persamaan berikut:

$$Level\ control = \frac{total\ value}{lots\ of\ control\ \text{X2}} \qquad (1)$$

3.4 Hasil dan Rekomndasi

Peroses Pengolahan data dimulai dari mengumpulkan seluruh nilai rata-rata dari setiap Control Identifier. Terdapat 26 Control Identifier yang sudah dilakukan penilaian, seperti terdapat pada Tabel 5.

Tabel 5. Penilaian Jawaban

Subcategory	***Control Identifier***	**Nilai**
ID.RA.1	CA-2	1.00
	CA-7	1.00
	CA-8	0.75
	RA-3	1.75
	RA-5	1.00
	SA-5	0.89
	SA-11	0.89
	SI-4	0.71
	SI-5	1.00
ID.RA.2	SI-5	1.00
	PM-15	1.00
	PM-16	0.50
ID.RA.3	RA-3	1.75
	SI-5	1.00
	PM-12	1.00

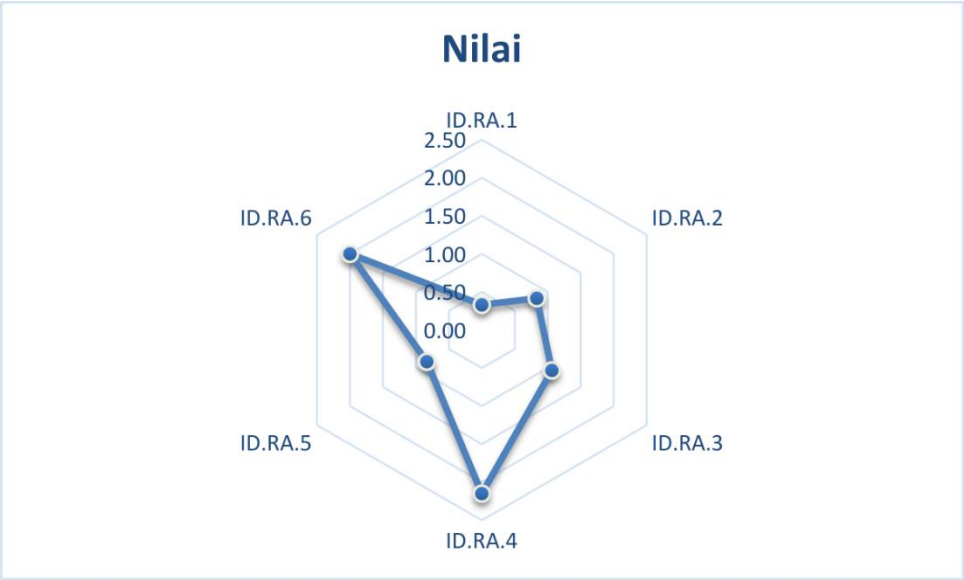
	PM-16	0.50
ID.RA.4	RA-2	1.00
	RA-3	0.50
	SA-14	1.00
	PM-9	2.00
	PM-11	1.00
ID.RA.5	RA-2	1.00
	RA-3	0.50
	PM-16	1.00
ID.RA.6	PM-4	2.00
	PM-9	2.00

Berdasarkan hasil penilaian control identifiter maka bisa meghitung keseluruhan nilai dari *subcatagory* pada proses *Risk Assessment* (ID.RA), seperti pada Tabel 6

Tabel 6. Nilai *Subcratagory*

Subcategory	**Nilai**
ID.RA.1	0.33
ID.RA.2	0.83
ID.RA.3	1.06
ID.RA.4	2.15
ID.RA.5	0.83
ID.RA.6	2.00

Berdasarkan hasil Penilaian subcatagory yang sudah dilakukan dapat dibuat diagram pemosisian penilain resiko keamanan siber kampsu bisa dilihat pada Gambar 6.



Gambar 5. Pemosisian *Risk Assesmen*

Berdasarkan perhitungan bahwa penilaian resiko keamanan siber dengan menggunakan standar *NIST Cybersecurity Framework 1.1* memperoleh nilai 1,20 sehingga menempatkan institusi kampus berada pada kondisi keamanan siber *"Partial Implemented"* dimana kampus melaksanakan kontrol pada *framework* seperlunya saja dan belum terdokumentasidan sehingga perlu ditingkatkan terkait kontrol dan pendokumntasian dengan baik untuk mengkatkan keamanan siber yang lebih baik.

4. KESIMPULAN

Standar *NIST Cybersecurity Framework 1.1* mampu menjawab kebutahan akan standar penilaian resiko keamanan siber yang kompleks dengan menyuguhkan fugsi yang bisa disesiuakan dengan kebutuhan audit. Penilaian resiko keamanan siber kampus

ini didapatkan hasil nilai 1,20 sehingga menempatkan institusi kampus berada pada kondisi keamanan siber ***"Partial Implemented"*** dimana kampus melaksanakan kontrol pada *framework* seperlunya saja dan belum terdokumentasidan sehingga perlu ditingkatkan terkait kontrol dan pendokumntasian dengan baik untuk mengkatkan keamanan siber yang lebih baik.

Ucapan Terimakasih

Kami ucapkan terimakasih atas pendanan yang diberikan oleh Kementerian Riset dan Teknologi – BRIN dalam Program Penelitian Kompetitif Nasional Penelitian Dosen Pemula. Kontrak Induk pada tanggal 19 Juli 2023, Nomor Kontrak Induk: 183/E5/PG.02.00.PL/2023

DAFTAR PUSTAKA

[1] R. Umar, I. Riadi, and E. Handoyo, "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," *JURNAL SISTEM INFORMASI BISNIS*, vol. 9, no. 1, p. 47, May 2019, doi: 10.21456/vol9iss1pp47-54.

[2] I. Riadi, S. Sunardi, and E. Handoyo, "Security Analysis of Grr Rapid Response Network using COBIT 5 Framework," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, p. 29, May 2019, doi: 10.24843/lkjiti.2019.v10.i01.p04.

[3] R. Umar, I. Riadi, and E. Handoyo, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)," *Scientific Journal of Informatics*, vol. 6, no. 2, pp. 2407–7658, 2019, [Online]. Available: http://journal.unnes.ac.id/nju/index.php/sji

[4] M. Ghazouani, S. Faris, and H. Medromi, "Information Security Risk Assessment-A Practical Approach with a Mathematical Formulation of Risk," 2014. [Online]. Available: http://www.risicare.fr

[5] E. Handoyo, "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)*, vol. 1, no. 2, pp. 76–83, Oct. 2020, doi: 10.37859/coscitech.v1i2.2199.

[6] V. I. Sugara, H. Syahrial, and M. Syafrullah, "Sistem Pemeriksa Keamanan Informasi Menggunakan National Institute Of Standards And Technology (Nist) Cybersecurity Framework," *Jurnal Ilmiah Ilmu Komputer dan Matematika)*, vol. 16, no. 1, pp. 203–212, 2019, [Online]. Available: https://journal.unpak.ac.id/index.php/komputasi

[7] I. Riadi, I. T. Riyadi Yanto, and E. Handoyo, "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, Nov. 2020, doi: 10.22219/kinetik.v5i4.1083.

[8] T. Tan and B. Soewito, "Manajemen Risiko Serangan Siber Menggunakan Framework Nist Cybersecurity Di Universitas Zxc," *Journal of Information System, Applied, Management, Accounting and Research*, vol. 6, no. 2, pp. 411–422, 2022, doi: 10.52362/jisamar.v6i2.781.

[9] R. Anggraini, "ANALISIS KEAMANAN PRIVATE CLOUD BERBASIS FRAMEWORK NISTCY DI PT XYZ," *Jurnal Teknologi dan Manajemen*, vol. 19, no. 1, pp. 41–46, Apr. 2021, doi: 10.52330/jtm.v19i1.11.

[10] T. S. Putri, N. Mutiah, and D. Prawira, "Analisis Manajemen Risiko Keamananinformasi Menggunakan Nistcybersecurity Framework Dan ISO/IEC27001:2013(Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," *Coding : Jurnal Komputer dan Aplikasi* , vol. 10, no. 02, pp. 237–248, 2022.

[11] B. P. Zen, A. Zafia, I. Nofi, and Y. Putro, "JURNAL RESTI Network Security Analysis Simulation at the GCS in the UCAV to support the Indonesian Defense Area," vol. 5, no. 158, pp. 824–831, 2022.

[12] H. Ernita, Y. Ruldeviyani, D. N. Maftuhah, and R. Mulyadi, "Strategy to Improve Employee Security Awareness at Information," vol. 5, no. 158, pp. 577–584, 2022.