Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity NIST 1.1

Eko handoyo, Izza eka nigrum
Email: ekokurro17@gmail.com, izzaeka@gmail.com

Teknik komputer, Fakultas sains teknologi dan pendidikan, Universitas muahammdiyah lamongan
Fisika, Fakultas sains teknologi dan pendidikan, Universitas muahammdiyah lamongan

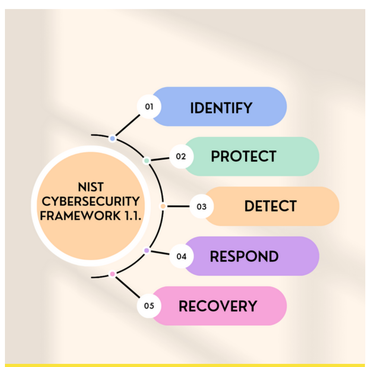
Abstrak

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.NIST Cybersecurity Framework 1.1 merupakan standar yang digunakan untuk mengarahkan organisasi pada aktivitas keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian dari proses manajemennya.Tujuan penelitian ini menghasilkan penilaian 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 institstusi 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

Pembahasan dan Hasil

1. Fugsi yang dipilih dalam penelitian terkait penilaian resiko keamanan siber ada dalam identify dan pada category risk assessment.
2. Mentukan category risk assesment yang berisikan 6 subkatagori.
3. Penilaian Jawaban

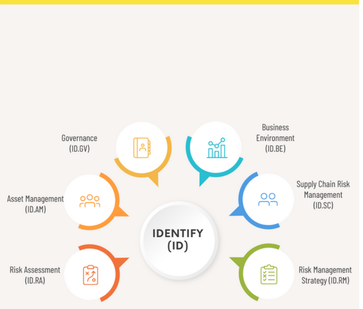
- Full Implemented, jika melaksanakan kontrol pada framework secara menyeluruh, rutin dan terdokumentasi.
- Partial Implemented, jika melaksanakan kontrol pada framework seperlunya saja dan belum terdokumentasi.
- Not Implemented, jika belum melaksanakan sama sekali kontrol pada framework



Cybersecurity Framework 1.1

No	Jawaban	Nilai
1	Full Implemente	2
2	Partial Implemented	1
3	Not Implemented	0

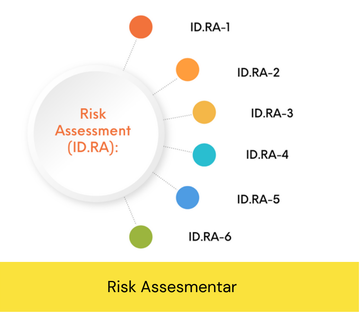
Rumus : $$Level\ control = \frac{total\ value}{lots\ of\ control\ X2}$$



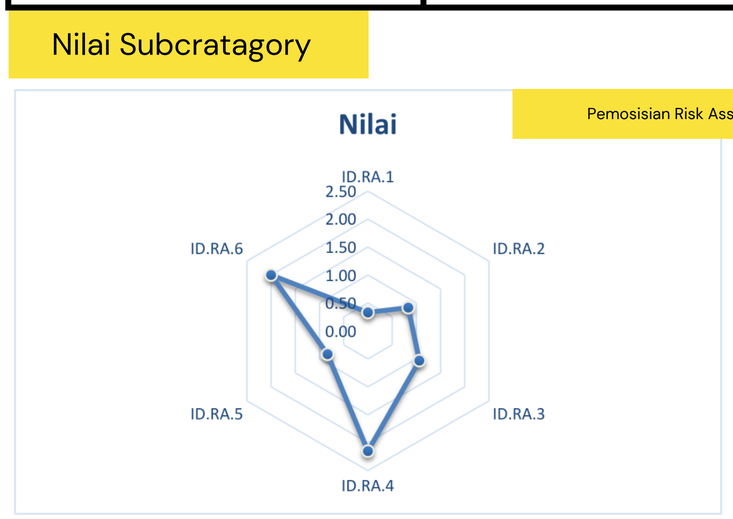
Identify

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

Nilai Subcratagory



Risk Assesmentar



Pemosisian Risk Assesmen

Pendahuluan

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. Tujuan penelitian ini menghasilkan penilaian 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

Metodologi

1. Studi Literarur : Mencari data dan mengumpulkan data, sumber informasi dari buku, literatur dan artikel yang terkait dengan objek penelitian[11].
2. Pengumpulan data: Mencari data didapat dari observasi langsung dan wawancara kepada pihak yang kompeten.
3. Pelaksanaan Audit: Melakukan audit check list terhadap sistem yang sedang berjalan berdasarkan NIST CyberSecurity Framework.
4. Penentuan Hasil Audit: Menentukan hasil dari Audit Check List dan juga hasil observasi yang telah dilakukan sehingga akan terlihat temuan-temuan yang harus diperthaankan dan yang harus diperbaiki.
5. Penyusunan rekomendasi: Berdasarkan hasil analisis data dan penjelasan kondisi sistem informasi yang sedang berjalan ini makan disusun rekomendasi untuk keamanan sistem informasi yang menjadi objek penelitian[12].

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 institstusi 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

Penelitian ini didanai oleh Kementerian Riset dan Teknologi – BRIN dalam Program Penelitian Kompetitif Nasional Penelitian Dosen Pemula sesuai 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