PENILAIAN RESIKO KEAMANAN INFORMASI MENGGUNAKAN *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST) *CYBERSECURITY FRAMEWORK* DI PUSAT TEKNOLOGI DAN KOMUNIKASI (PUTIK) UNIVERSITAS PAKUAN

Victor Ilyas Sugara[1] ,Aries Maesya[2]

Program Studi Ilmu Komputer, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Pakuan

victor.ilyas@unpak.ac.id , a.maesya@unpak.ac.id

ABSTRAK

Masalah kemanan informasi dapat mempengaruhi operasional di suatu perusahaan/perguruan tinggi. Resiko yang timbul dapat berakibat proses bisnis tidak optimal, kerugian finansial, berkurangnya kepercayaan pelanggan, menurunnya reputasi dan yang paling buruk adalah hancurnya bisnis. Untuk itu diperlukan suatu cara untuk memonitor keamanan informasi di perusahaan ini secara periodik. Metode yang bisa digunakan sebagai best practise *adalah National Institute of Standards and Technology* (NIST) *Cybersecurity Framework*. *Framework* ini menyediakan mekanisme penilaian yang memungkinkan perusahaan/perguruan tinggi menentukan kemampuan *cybersecurity* saat ini, menetapkan sasaran individual, dan membuat rencana untuk memperbaiki dan memelihara program *cybersecurity*. Dari penelitian ini didapatkan hasil pengujian untuk fungsi Mengenali (*Identify*) sebesar 68,75%, Melindungi (*Protect*) sebesar 41,43%, Mendeteksi (*Detect*) sebesar 22,22%, Menanggapi (*Respond*) sebesar 23.33% dan Memulihkan (*Recover*) sebesar 16,67%. Namun untuk keseluruhan nilai NIST *Security Framework* yang didapat hanya 40,31%.

Kata Kunci : keamanan, informasi, NIST, cybersecurity, framework

1. Pendahuluan

Perusahaan dan perguruan tinggi saat ini sudah menggunakan Teknologi Informasi (TI) sebagai basis layanan yang berkualitas dan juga sebagai optimalisasi dalam proses bisnisnya. Penerapan TI ini memerlukan perencanaan yang strategis agar selaras dengan tujuan bisnis perusahaan dan perguruan tinggi tersebut. Jika tidak, maka akan menimbulkan resiko yang dapat berakibat proses bisnis tidak optimal, kerugian finansial, berkurangnya kepercayaan pelanggan, menurunnya reputasi dan yang paling buruk adalah hancurnya bisnis perusahaan. 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)* (Utomo dkk., 2012).

Oleh karena itu diperlukan suatu penilaian resiko untuk memeriksa secara periodik keamanan informasi bagi perusahaan dan perguruan tinggi. Penilaian resiko ini berguna untuk memonitor kerentanan-kerentanan pada keamanan informasi di Pusat Teknologi Informasi dan Komunikasi Universitas Pakuan (PUTIK UNPAK). Metode atau *framework* yang bisa dijadikan sebagai *best practice* dalam penerapan ini adalah *National Institute of Standards and Technology* (NIST) *Cybersecurity Framework.*

Berdasarkan latar belakang penelitian yang telah diuraikan, maka dapat diidentifikasi belum adanya acuan *cybersecurity framework* standar yang bisa digunakan sebagai penerapan keamanan informasi di PUTIK UNPAK.

2. Metodologi dan Rancangan Penelitian

Pada penelitian ini dilakukan beberapa tahapan, yaitu :

a. Studi Kepustakaan dan Penentuan Ruang Lingkup
   Mencari data dan mengumpulkan data, sumber informasi dari buku, literatur dan artikel yang terkait dengan objek penelitian.
b. Pengumpulan Data
   Pengumpulan data didapat dari observasi langsung dan wawancara kepada pihak yang kompeten
c. Pelaksanaan Audit
   Melakukan audit *check list* terhadap sistem yang sedang berjalan berdasarkan NIST *CyberSecurity Framework*
d. 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
e. Penyusunan rekomendasi (Ermana dkk, 2012)
   Berdasarkan hasil analisis data dan penjelasan kondisi sistem informasi yang sedang berjalan ini

makan disusun rekomendasi untuk keamanan sistem informasi yang menjadi objek penelitian

3. Pembahasan Hasil Penelitian

3.1. Pengumpulan Data

Proses pengumpulan data dilakukan dengan cara observasi, diskusi non formal, mengulas sistem yang berjalan saat ini melalui wawancara dan mempelajari dokumen-dokumen yang berkaitan dengan penelitian ini.

3.2. Pembuatan *Framework Core*

Dalam penelitian ini, penulis mengusulkan agar kerangka kerja ini diadopsi dalam bentuk yang paling sederhana dengan tujuan eksekusi yang cepat dan mudah untuk menilai risiko organisasi terkait dengan ancaman dan kerentanan dinamis. Kategori paling sederhana yang diambil dari *framework core* ini adalah Fungsi dan Kategori seperti pada tabel 1. Perancangan *Framework Core* di PUTIK UNPAK dilihat berdasarkan kebutuhan yang paling dasar dan juga sarana, peralatan yang tersedia serta aktifitas rutin yang dilakukan saat ini. Perancangan juga harus tidak mengganggu bisnis proses yang sedang berjalan.

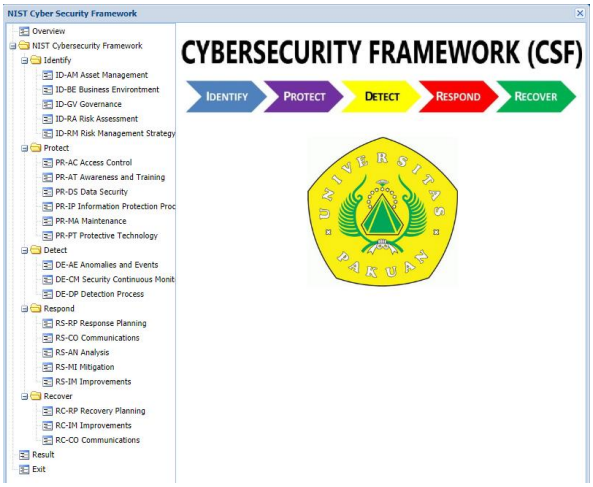
Tabel 1. *Framework Core*

Function	***Category***
Identify	*Asset Management*
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	*Access Control*
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	*Anomalies and Events*
	Security Continuous Monitoring
	Detection Processes
Respond	*Response Planning*
	Communications
	Analysis
	Mitigation
	Improvements
Recover	*Recovery Planning*
	Improvements
	Communications

Di bawah Fungsi, ruang lingkup selanjutnya dibagi menjadi 5 sub-area yaitu *Identify, Protect, Detect, Respond, Recover*. Di bawah kategori, terdapat 22 kontrol yang dapat dipilih dan disesuaikan sesuai kebutuhan (Jazri, H. and Jat, S. D, 2016). Kontrol yang dipilih dapat diuraikan lebih detail menjadi sub-kategori yang sesuai dan memberikan pengenal *(Identifier)* pada setiap kontrol yang dibuat

3.3. Antarmuka

Tampilan antarmuka pada aplikasi ini pada gambar 1 terdiri dari beberapa fitur yang diimplementasikan sesuai dengan kebutuhan pengguna



Gambar 1. Tampilan Menu

3.4. Penilaian Jawaban

Pemberian jawaban untuk masing-masing kontrol *framework* dibagi menjadi 3 bagian yaitu

- *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*

Sedangkan penilaian yang dilakukan terhadap jawaban yang didapat dapat dilihat pada tabel IV-12 berikut

Tabel 2. Penilaian Jawaban

No.	**Jawaban**	**Nilai**
1.	Full Implemented	2
2.	Half Implemented/Partial Implemented	1
3.	Not Implemented	0

Sehingga untuk masing-masing level kontrol pada *framework*, nilai presentasinya bisa didapat dari persamaan berikut

$$Level\ Kontrol = \frac{Total\ Nilai}{Banyaknya\ Kontrol * 2} * 100\%$$

3.5. Ujicoba Program

Ujicoba terhadap Fungsi Mengenali *(Identify)*

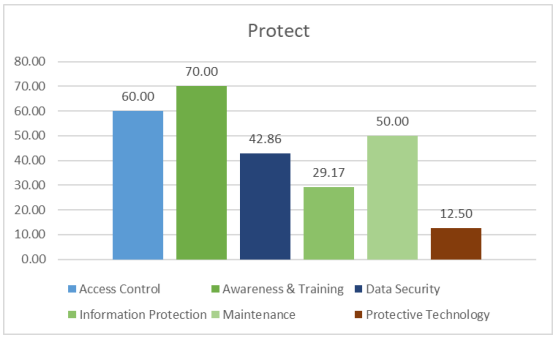
Hasil ujicoba terhadap fungsi ini dapat dilihat gambar 3 dibawah ini

Gambar 3. Hasil Ujicoba Fungsi Mengenali *(Identify)*

Dari hasil ujicoba tersebut terlihat bahwa dari 24 kontrol (sub-kategori) terdapat 9 kontrol yang sudah diimplementasikan secara penuh dan 15 kontrol yang sudah diimplementasikan sebagian.

Ujicoba terhadap Fungsi Melindungi *(Protect)*

Hasil ujicoba terhadap funsi ini dapat dilihat pada gambar 4 dibawah ini

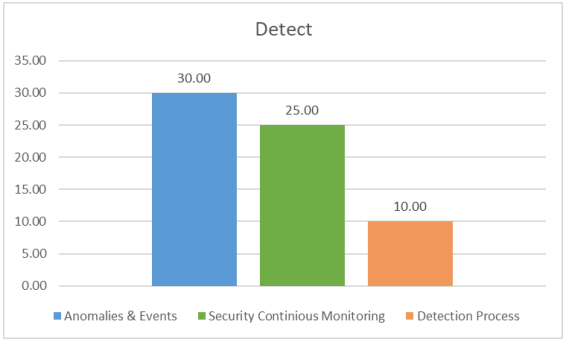


Gambar 4. Hasil Ujicoba Fungsi Melindungi *(Protect)*

Dari hasil ujicoba tersebut terlihat bahwa dari 35 kontrol (sub-kategori) terdapat 4 kontrol yang sudah diimplementasikan secara penuh dan 21 kontrol yang sudah diimplementasikan sebagian dan 10 kontrol belum diimplementasikan sama sekali. Secara lebih detail hasilnya dapat dilihat pada Lampiran 2.

Ujicoba terhadap Fungsi Mendeteksi *(Detect)*

Hasil ujicoba terhadap funsi ini dapat dilihat pada gambar 5 dibawah ini

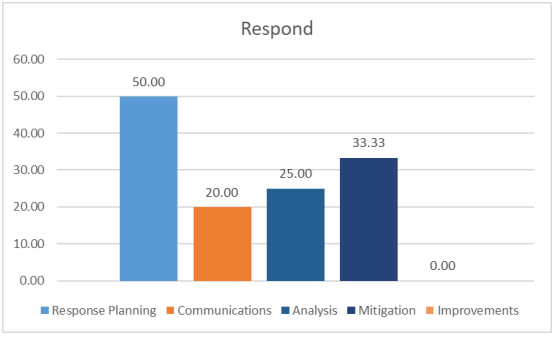


Gambar 5. Hasil Ujicoba Fungsi Mendeteksi *(Detect)*

Dari hasil ujicoba tersebut terlihat bahwa dari 18 kontrol (sub-kategori) terdapat 0 kontrol yang sudah diimplementasikan secara penuh dan 8 kontrol yang sudah diimplementasikan sebagian dan 10 kontrol belum diimplementasikan sama sekali.

Ujicoba terhadap Fungsi Menanggapi (*Respond*)

Hasil ujicoba terhadap funsi ini dapat dilihat pada gambar 6 dibawah ini

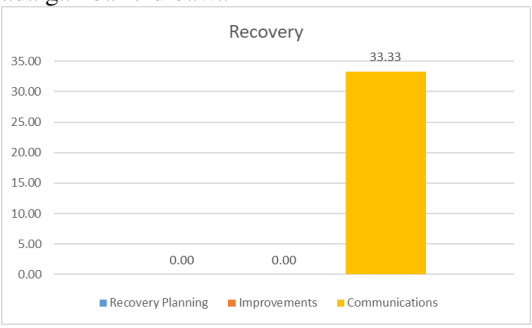


Gambar 6. Hasil Ujicoba Fungsi Menanggapi *(Respond)*

Dari hasil ujicoba tersebut terlihat bahwa dari 15 kontrol (sub-kategori) terdapat 1 kontrol yang sudah diimplementasikan secara penuh dan 5 kontrol yang sudah diimplementasikan sebagian dan 9 kontrol yang belum diimplementasikan sama sekali.

Ujicoba terhadap Fungsi Memulihkan *(Recover)*

Hasil ujicoba terhadap funsi ini dapat dilihat pada gambar 7 dibawah ini

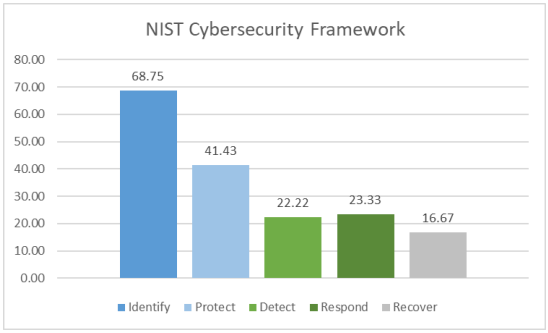


Gambar 7. Hasil Ujicoba Fungsi Memulihkan *(Recover)*

Dari hasil ujicoba tersebut terlihat bahwa dari 6 kontrol (sub-kategori) terdapat 0 kontrol yang sudah diimplementasikan secara penuh dan 2 kontrol yang sudah diimplementasikan sebagian dan 4 kontrol yang belum diimplementasikan sama sekali.

Penilaian Keseluruhan

Dari semua hasil ujicoba yang telah dipaparkan sebelumnya, hasil penilaian dapat dilihat secara umum pada gambar 8



Gambar 8. Hasil Penilaian NIST *Cybersecurity Framework*

Dari hasil pengujian terlihat bahwa fungsi Mengenali *(Identify)* memiliki persentase yang paling besar yaitu sebesar 68.75%, dan yang peling kecil adalah fungsi Memulihkan *(Recover)* yaitu sebesar 16.67%., secara keseluruhan nilai NIST *Cybersecurity Framework* yang diperoleh oleh PUTIK UNPAK adalah **40.31%**

3.6. Tindak Lanjut

Tindakan selanjutnya yang dapat dilakukan dari penelitian ini adalah

1. Mempertahankan kinerja fungsi pada NIST *Cybersecurity Framework* yang bernilai 2, meningkatkan kinerja pada fungsi yang bernilai 1 dan melakukan tindakan-tindakan yang dianggap perlu untuk menjalankan fungsi yang bernilai 0
2. Melakukan perbaikan pada fungsi yang mendapatkan nilai terendah yaitu Memulihkan *(Recover)* dengan cara memperbaiki dokumentasi yang sudah ada dan mengikuti pelatihan-pelatihan bagi pegawai PUTIK UNPAK serta mengaplikasikan di tempat kerja
3. Menambahkan beberapa fasilitas di program seperti *history/log* pemeriksaan sebelumnya sehingga dapat diketahui perubahan-perubahan keamanan informasi di PUTIK UNPAK

4. Kesimpulan

Kesimpulan yang didapat dari penelitian ini adalah sebagai berikut :

1. Dari penelitian ini didapatkan hasil pengujian untuk fungsi Mengenali (*Identify*) sebesar 68,75%, Melindungi (*Protect*) sebesar 41,43%, Mendeteksi (*Detect*) sebesar 22,22%, Menanggapi (*Respond*) sebesar 23.33% dan Memulihkan (*Recover*) sebesar 16,67%. Namun untuk keseluruhan nilai NIST *Security Framework* yang didapat hanya 40,31%. Ini membuktikan bahwa keamanan informasi yang dimiliki PUTIK UNPAK masih perlu dilakukan perbaikan. Hal ini disebabkan karena banyaknya fungsi pada NIST *Cybersecurity Framework* yang belum diimplementasi sepenuhnya sehingga menimbulkan kerentanan terhadap keamanan informasi di PUTIK UNPAK
2. Dalam mengimplementasikan NIST *cybersecurity framework* perlu dilakukan secara bertahap dan dilakukan evaluasi secara berkala dan dilakukan perbaikan-perbaikan terhadap kerentanan keamanan informasi yang ada. Serta melakukan dokumentasi terhadap perubahan-perubahan yang sudah dibuat dan tindakan-tindakan yang dijalankan secara rutin.

Daftar Pustaka

Committee on National Security Systems. ‘Committee on National Security Systems (CNSS) Glossary’, (4009), p. 160. 2015

Darmawan, Deni. “Desain dan Pemrograman Website”. Mediakom, 2015.

Davis, Fred D., “Technology Acceptance Model for Empirically Testing New End-User Information System Theory and Results”,. Massachusetts Institute of Technology (MIT). 1986.

Davis, Fred D., “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology”., *MIS Quarterly Vol.13, No.3, p.319-340*. September 1989.

Davis, Fred D., ‘User Acceptance of Computer Technology: A Comparison of Two Theoritical Models’, *Management Science*, *35 (8), p.982-1002,* 1989.

Ghazouani, Mohamed., Faris, Sophia., Medromi, Hicham., dan Sayouti, Adil. ‘Information Security Risk Assessment - A Practical Approach With A Mathematical Formulation Of Risk’, *International Journal of Computer Applications*, Vol 103 – No.8, October 2014.

Huijben, K. (2006) ‘A lightweight, flexible evaluation framework to measure the ISO 27002 information security controls’, 86(2), pp. 1–3. doi: 10.4172/2168-9695.1000e118.

Jazri, H. and Jat, S. D. 'A Quick Cybersecurity Wellness Evaluation Framework for Critical Organizations', 2016

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P. and Jones, K. 'A survey of cyber security management in industrial control systems', *International Journal of Critical Infrastructure Protection*. Elsevier, 9, pp. 52–80. doi: 10.1016/j.ijcip.2015.02.002. 2015

Maulana, M. M. and Supangkat, S. H. (2006) 'Pemodelan Framework Manajemen Resiko Teknologi Informasi untuk Perusahaan di Negara Berkembang', *Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, pp. 121–126.

McLeod, Raymond, and George, P., Schell. 'Management Information System', Salemba. Jakarta. 2009.

NIST. 'Guide for conducting risk assessments', (September), p. 95. doi: 10.6028/NIST.SP.800-30r1. 2012

NIST. 'Security and Privacy Controls for Federal Information Systems and Organizations Security and Privacy Controls for Federal Information Systems and Organizations', Sp-800-53Ar4, p. 400+. doi: 10.6028/NIST.SP.800-53Ar4. 2014

NIST. 'Guide for conducting risk assessments', (September), p. 95. doi: 10.6028/NIST.SP.800-30r1. 2012

NIST. 'Framework for Improving Critical Infrastructure Cybersecurity', National Institute of S, pp. 1–41. doi: 10.1109/JPROC.2011.2165269. 2014

NIST. 'An Introduction to Computer Security : The NIST Handbook', National Institute of Standards and Technology Technology Administration U.S. Department of Commerce An, SP800(12), pp. 1–278. doi: 10.1002/wics.106. 1995

NIST. 'Cybersecurity Framework Manufacturing Profile'. 2017

Paulsen, C. Toth, P. 'Small Business Information Security: The Fundamentals Small Business', National Institute of Standards and Technology Interagency Report, 7621, p. 20. doi: 10.6028/NIST.IR.7621r1. 2016

Syahrial, Hadi. 'Pengembangan Sistem Manajemen Kelemahan Keamanan Informasi (SMKKI) Menggunakan Lotus Notes', *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*. 2011.

USC. 'Sec 3552, Public Printing and Documents / Coordination of Federal Information Policy / Information Security / Definitions', p. 3553. 2014

Utomo, M., Ali, A. H. N. and Affandi, I. 'Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO / IEC 27001 : 2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I', *Jurnal Teknik ITS*, 1(1), pp. 288–293. 2012