KOMPUTASI (Jurnal Ilmiah Ilmu Komputer dan Matematika)
Vol.16, No.1, Januari 2019, Hal. 203 – 212
P-ISSN: 1693-7554, E-ISSN: 2654-3990
https://journal.unpak.ac.id/index.php/komputasi

SISTEM PEMERIKSA KEAMANAN INFORMASI MENGGUNAKAN *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST) CYBERSECURITY FRAMEWORK

Victor Ilyas Sugara[1)], Hadi Syahrial[2)], Muhammad Syafrullah[3)]
[1)]Program Studi Ilmu Komputer, FMIPA, Universitas Pakuan, Bogor, Indoensia
[2,3)]Program Studi Magister Ilmu Komputer, Program Pascasarjana, Universitas Budi Luhur, Jakarta, Indonesia

Corresponding Author: victor.ilyas@unpak.ac.id

***Article history**: received 4 September 2018; revised 21 September 2018; accepted 5 Desember 2018*

ABSTRAK

Masalah kemanan informasi dapat mempengaruhi operasional di suatu perusahaan/organisasi. Resiko yang timbul dapat berakibat proses bisnis tidak optimal, kerugian finansial, berkurangnya kepercayaan pelanggan, menurunnya reputasi dan yang paling buruk adalah hancurnya bisnis perusahaan. 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 organisasi/perusahaan 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 16.67%, Melindungi (Protect) sebesar 32.86%, Mendeteksi (Detect) sebesar 25%, Menanggapi (Respond) sebesar 23.33% dan Memulihkan (Recover) sebesar 58.33%. Namun untuk keseluruhan nilai NIST Security Framework yang didapat hanya 27.55%.

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

ABSTRACT

Security issues can affect operations in a company / organization. Risks that arise can result in business process is not optimal, financial losses, reduced customer confidence, decreased reputation and the worst is the collapse of the company's business. For that we need a way to monitor the information security in this company periodically. The best practice method is National Institute of Standards and Technology (NIST) Cybersecurity Framework. This framework provides an assessment mechanism that enables organizations / companies to determine their current cybersecurity capabilities, set individual goals, and create plans to improve and maintain cybersecurity programs. From this research got the test result for Identify function equal to 16.67%, Protect (Protect) equal to 32.86%, Detect (Detect) 25%, Responds 23.33% and Recover (58.33%). But for the overall value of NIST Security Framework obtained only 27.55%.

***Keywords:** security, information, NIST, cybersecurity, framework*

1. Pendahuluan

Perusahaan-perusahaan 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 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*) [1].

Masalah kemanan informasi dapat mempengaruhi operasional di suatu perusahaan/organisasi. Sebagai contoh kasus, masalah keamanan informasi juga terjadi di PT NPI sehingga menyebabkan operasional perusahaan menjadi terhambat. Oleh karena itu diperlukan suatu sistem untuk memeriksa secara periodik keamanan informasi bagi perusahaan. Sistem ini berguna untuk memonitor kerentanan-kerentanan pada keamanan informasi di PT NPI. Metode atau *framework* yang bisa dijadikan sebagai *best practice* dalam penerapan sistem ini adalah *National Institute of Standards and Technology* (NIST) *Cybersecurity Framework.* Namun penerapan *cybersecurity framework* tersebut tidak akan selalu sama untuk setiap perusahaan. Karena perbedaan karakteristik bisnis yang dijalankan.

Berdasarkan latar belakang penelitian yang telah diuraikan, maka dapat diidentifikasi permasalahan yang adaalah kurangnya pengawasan terhadap resiko keamanan informasi di PT NPI dan belum adanya acuan *cybersecurity framework* standar yang bisa digunakan sebagai penerapan keamanan informasi di PT NPI.

Penulis memiliki beberapa sumber sebagai dasar ilmu dalam melakukan analisis dengan menggunakan *cybersecurity framework*. Berikut ini adalah beberapa literatur yang telah dilakukan penelitian tentang *cybersecurity framework* :

a. Penelitian yang dilakukan oleh Hadi Syahrial, dipublikasikan pada Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011 (Semantik 2011) dengan judul PENGEMBANGAN SISTEM MANAJEMEN KELEMAHAN KEAMANAN INFORMASI (SMKKI) MENGGUNAKAN LOTUS NOTES. Penelitian ini bertujuan untuk mengembangkan sebuah *prototype* sistem yang diberi nama Sistem Manajemen Kelemahan Keamanan Informasi (SMKKI) yang berbasis Lotus Notes dan yang disesuaikan dengan kebutuhan akan manajemen kelemahan keamanan informasi. Sistem ini nantinya dapat digunakan oleh petugas keamanan informasi (*Information Security Officer*) untuk menganalisa, mencatat dan mengirim notifikasi kepada staf departemen yang terkait dengan keamanan informasi seperti departemen Teknologi Informasi. Sistem ini juga dapat digunakan untuk memonitor status kelemahan keamanan informasi yang terdeteksi oleh alat pemindai kelemahan, sehingga dapat diketahui sudah berapa lama kelemahan-kelemahan tersebut terdapat pada sistem operasi maupun aplikasi.[2]
b. Penelitian yang dilakukan oleh Margo Utomo, Ahmad Holil Noor Ali, Irsal Affandi, dipublikasikan pada Jurnal Teknik ITS Vol. 1, No. 1, Sept. 2012 dengan judul PEMBUATAN TATA KELOLA KEAMANAN INFORMASI KONTROL AKSES BERBASIS ISO/IEC 27001:2005 PADA KANTOR PELAYANAN PERBENDAHARAAN SURABAYA I. Penelitian ini bertujuan untuk untuk mengelola teknologi informasi berbasis resiko yang dituangkan dalam tata kelola untuk mengelola ancaman atau kelemahan yang muncul menggunakan ISO/IEC 27001:2005. Tata kelola sistem informasi ini menitikberatkan pada kontrol akses yang merupakan salah satu kontrol keamanan dari ISO/IEC 27991:2005[3]
c. Penelitian yang dilakukan oleh Muhammad Mahreza Maulana dan Suhono Harso Supangkat dengan judul PEMODELAN FRAMEWORK MANAJEMEN RESIKO TEKNOLOGI INFORMASI UNTUK PERUSAHAAN DI NEGARA BERKEMBANG. Penelitian ini bertujuan untuk Penelitian ini memodelkan framework manajemen resiko dalam penerapan TI di dalam organisasi ataupun perusahaan. Tujuan dari penelitian ini adalah untuk memberikan gambaran yang lebih sederhana dan mudah dalam menerapkan framework-framework manajemen resiko yang telah ada. Framework-framework manajemen resiko yang menjadi bahan dalam penelitian ini adalah COBIT (*Control Objectives for Information and Related Technology*), NIST *Special Publication* 800-30 dan OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*).[4]
d. Penelitian yang dilakukan oleh Mohamed Ghazouani,Sophia Faris, Hicham Medromi dan Adil Sayouti, dipublikasikan pada International Journal of Computer Applications (0975 – 8887) Volume 103 – No.8, October 2014, dengan judul INFORMATION SECURITY RISK ASSESSMENT - A PRACTICAL APPROACH WITH A MATHEMATICAL FORMULATION OF RISK. Penelitian ini bertujuan untuk mengusulkan rumusan risiko matematika dengan menggunakan tingkat granularitas elemen yang lebih rendah: ancaman, probabilitas, kriteria yang digunakan untuk menentukan nilai aset, eksposur, frekuensi dan ukuran

perlindungan yang ada.[5]

e. Penelitian yang dilakukan oleh Karin Huijben, Tesis 2014, dengan judul A LIGHTWEIGHT, FLEXIBLE EVALUATION FRAMEWORK TO MEASURE THE ISO 27002 INFORMATION SECURITY CONTROLS. Penelitian ini bertujuan untuk membuat framework evaluasi ISO 27002 yang fleksibel dan ringan untuk mengukur keamanan informasi.[6]

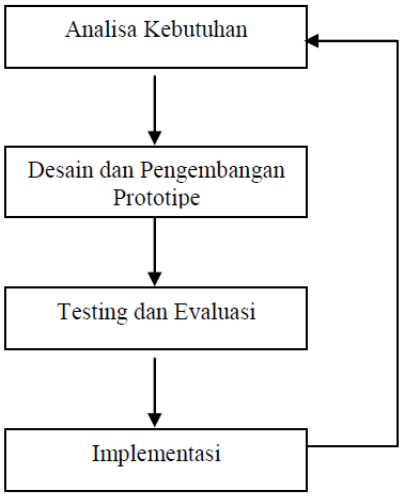
Pada penelitian ini penulis menggunakan NIST *Cybersecurity Framework* sebagai alat untuk memeriksa keamanan di PT NPI, UML sebagai alat untuk pengembangan sistem berupa *prototype*. Diharapkan *prototype* ini dapat menjadi sebuah sistem yang dapat digunakan untuk memeriksa keamanan informasi di PT NPI dan dapat digunakan juga minimal oleh staff IT di PT NPI.

2. Metode Penelitian

Penelitian ini menggunakan NIST *Cybersecurity Framework* dan model *prototype* dengan tahapan-tahapan sebagai berikut yaitu: tahap analisa kebutuhan, tahap desain dan pengembangan *prototype*, tahap testing dan evaluasi, dan tahap implementasi [6]. Tahapan-tahapan pengembangan Sistem adalah:

a. Analisa Kebutuhan
   Tujuan dari analisa ini adalah untuk mengetahui kebutuhan yang diinginkan agar dapat diaplikasikan dalam bentuk sebuah sistem. Metodologi pengumpulan data dilakukan studi lapangan dengan mempelajari dan mengamati
b. Desain dan Pengembangan Sistem
   Tujuan dari desain prototype adalah untuk mendapat gambaran tentang sistem pemeriksa keamanan informasi yang akan dikembangkan
c. Testing dan Evaluasi
   Sebelum sistem diimplementasi, perlu dilakukan pengujian dan evaluasi apakah sistem bekerja dengan baik dan sesuai dengan kebutuhan.
d. Implementasi
   Setelah sistem diuji dan dievaluasi, maka sistem sudah siap untuk diimplementasi. Untuk mengimplementasi harus diperhatikan kebutuhan perangkat keras dan perangkat lunak

Alur dari analisa kebutuhan pada pembuatan *prototype* sistem ini dapat dilihat pada Gambar 1



Gambar 1. Tahap-tahap pengembangan Sistem

3. Hasil dan Pembahasan

3.1. Pengumpulan Data

Proses pengumpulan data dilakukan dengan cara observasi, diskusi non formal, mengulas sistem yang berjalan saat ini melalui kuisioner dan mempelajari dokumen-dokumen kegiatan IT 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. Kategori paling sederhana yang diambil dari framework core ini adalah Fungsi dan Kategori seperti pada Tabel 1 [7]. Perancangan *Framework Core* di PT NPI 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.

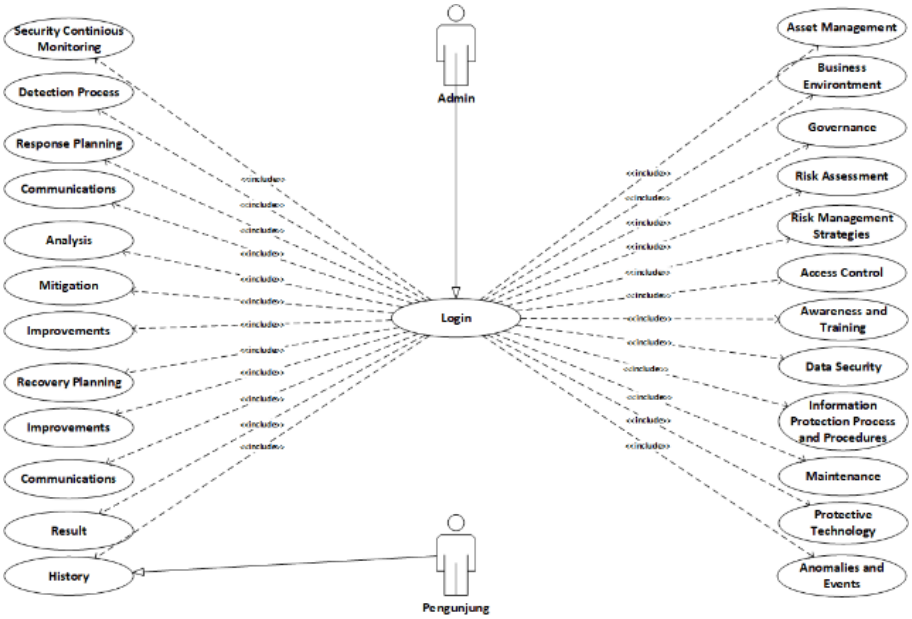
Tabel 1. Framework Core

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 [8]. Kontrol yang dipilih dapat diuraikan lebih detail menjadi sub-kategori yang sesuai dan memberikan pengenal *(Identifier)* pada setiap kontrol yang dibuat. Tahap selanjutnya ada menentukan sub-kategori dari masing-masing kontrol yang digunakan pada NIST *Cybersecurity Framework* di PT NPI berdasarkan data dan dokumen yang ada.

3.3. Desain sistem

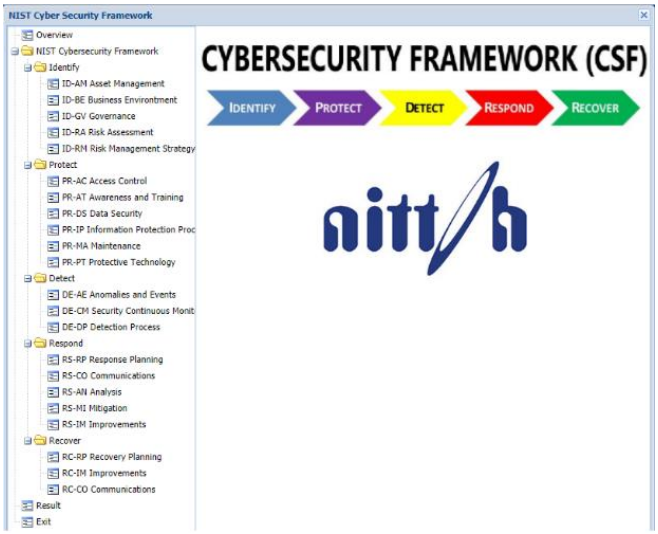
Use case diagram yang berlaku untuk sistem ini adalah seperti ditunjukkan pada gambar 2 di bawah ini.



Gambar 2. *Use case diagram*

Pengguna biasa bisa memasukkan nilai pada kontrol yang telah disediakan, sedangkan Admin memiliki hak yang sama dengan pengguna biasa ditambah dengan kemampuan untuk menghapus data

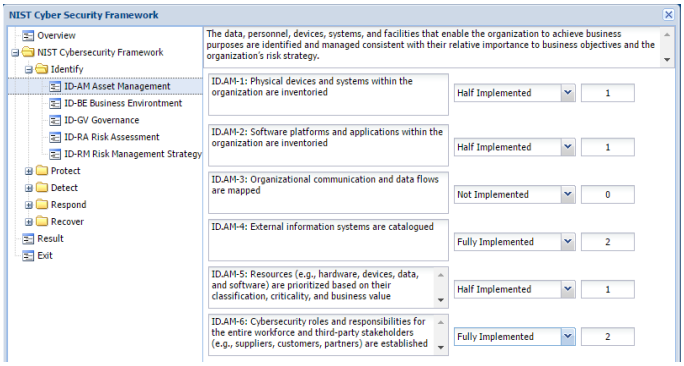
Tampilan antarmuka pada aplikasi ini pada Gambar 3 terdiri dari beberapa fitur yang diimplementasikan sesuai dengan kebutuhan pengguna



Gambar 3. Tampilan Menu

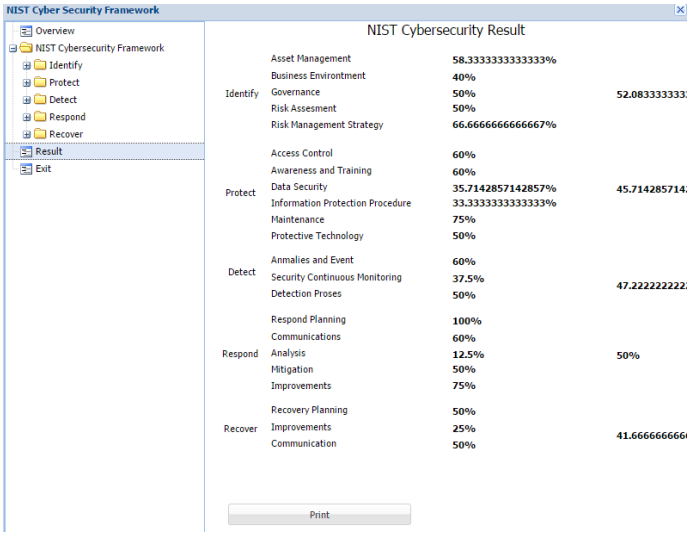
Contoh penggunaan aplikasi ini adalah menggunakan Menu ID-AM *Asset Management* pada Gambar 4 yang terdiri dari 6 pertanyaan yang harus dijawab. Pertanyaan yang harus dijawab merupakan sub-kategori dari *Asset Management* yaitu ID-AM-1 sampai ID-AM-6 yang dapat berisi nilai :

0 : *Not Implemented*
1 : *Partial Implemented*
2 : *Full Implemented*



Gambar 4. Menu ID-AM *Asset Management*

Sedangkan contoh hasil perhitungan dapat dilihat pada Menu Results pada gambar 5 yang menampilkan persentase *security level* pada tiap-tiap kontrol *framework*.



Gambar 5. Hasil Perhitungan

3.4. Penilaian Jawaban

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

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

Sedangkan penilaian yang dilakukan terhadap jawaban yang didapat dapat dilihat pada Tabel 2 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

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

3.5. Ujicoba Sistem

3.5.1 Ujicoba terhadap Fungsi Mengenali *(Identify)*

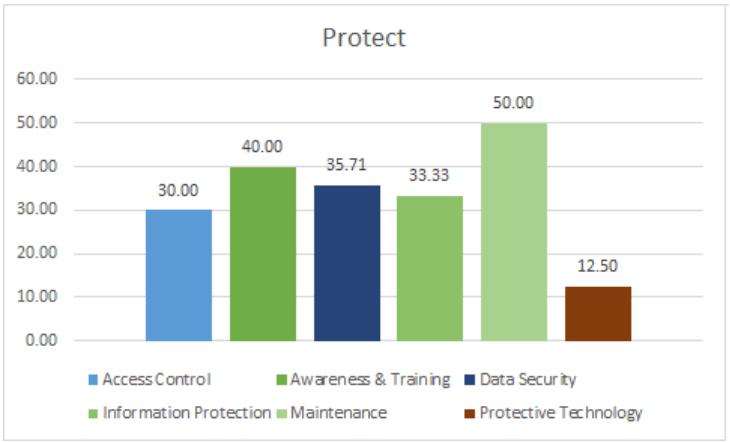
Hasil ujicoba terhadap fungsi ini dapat dilihat pada Gambar 6

Gambar 6. Hasil Ujicoba Fungsi Mengenali *(Identify)*

Dari hasil ujicoba tersebut terlihat bahwa dari 24 kontrol (sub-kategori) terdapat 2 kontrol yang sudah diimplementasikan secara penuh dan 4 kontrol yang sudah diimplementasikan sebagian dan sisanya belum diimplementasikan sama sekali.

3.5.2 Ujicoba terhadap Fungsi Melindungi *(Protect)*

Hasil ujicoba terhadap funsi ini dapat dilihat pada Gambar 7



Gambar 7. Hasil Ujicoba Fungsi Melindungi *(Protect)*

Dari hasil ujicoba tersebut terlihat bahwa dari 35 kontrol (sub-kategori) terdapat 5 kontrol yang sudah diimplementasikan secara penuh dan 13 kontrol yang sudah diimplementasikan sebagian dan sisanya belum diimplementasikan sama sekali.

3.5.3 Ujicoba terhadap Fungsi Mendeteksi *(Detect)*

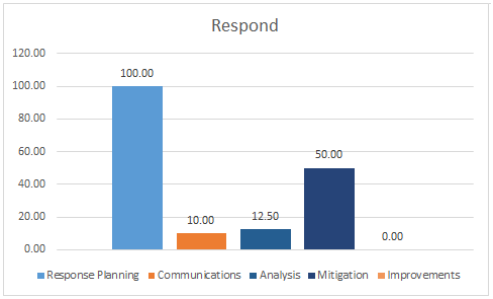
Hasil ujicoba terhadap funsi ini dapat dilihat pada Gambar 8

Gambar 8. Hasil Ujicoba Fungsi Mendeteksi *(Detect)*

Dari hasil ujicoba tersebut terlihat bahwa dari 18 kontrol (sub-kategori) terdapat 1 kontrol yang sudah diimplementasikan secara penuh dan 7 kontrol yang sudah diimplementasikan sebagian dan sisanya belum diimplementasikan sama sekali.

3.5.4 Ujicoba terhadap Fungsi Menanggapi (*Respond*)

Hasil ujicoba terhadap funsi ini dapat dilihat pada Gambar 9

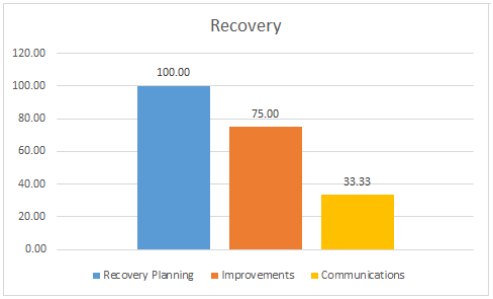


Gambar 9. Hasil Ujicoba Fungsi Menanggapi *(Respond)*

Dari hasil ujicoba tersebut terlihat bahwa dari 15 kontrol (sub-kategori) terdapat 2 kontrol yang sudah diimplementasikan secara penuh dan 3 kontrol yang sudah diimplementasikan sebagian dan sisanya belum diimplementasikan sama sekali.

3.5.6 Ujicoba terhadap Fungsi Memulihkan *(Recover)*

Hasil ujicoba terhadap funsi ini dapat dilihat pada Gambar 10

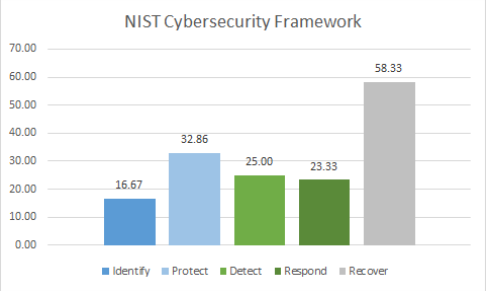


Gambar 10. Hasil Ujicoba Fungsi Memulihkan *(Recover)*

Dari hasil ujicoba tersebut terlihat bahwa dari 6 kontrol (sub-kategori) terdapat 2 kontrol yang sudah diimplementasikan secara penuh dan 3 kontrol yang sudah diimplementasikan sebagian dan sisanya belum diimplementasikan sama sekali.

3.5.7 Penilaian Keseluruhan

Dari semua hasil ujicoba yang telah dipaparkan sebelumnya, hasil penilaian dapat dilihat secara umum pada Gambar 11



Gambar 11. Hasil Penilaian NIST *Cybersecurity Framework*

Dari hasil pengujian terlihat bahwa fungsi Memulihkan memiliki persentase yang paling besar yaitu sebesar 58.33%, dan yang peling kecil adalah fungsi Mengenali yaitu sebesar 16.67%. Namun secara keseluruhan nilai NIST *Cybersecurity Framework* yang diperoleh adalah **27.55%**

3.6. Tindak Lanjut

Tindakan selanjutnya yang dapat dilakukan dari penelitian ini adalah

a. 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
b. Menambahkan beberapa fasilitas di sistem seperti *history/log* pemeriksaan sebelumnya sehingga dapat diketahui perubahan-perubahan yang telah dilakukan terhadap keamanan informasi

4. Kesimpulan

Kesimpulan yang didapat dari penelitian ini didapatkan hasil pengujian untuk fungsi Mengenali (*Identify*) sebesar 16.67%, Melindungi (*Protect*) sebesar 32.86%, Mendeteksi (*Detect*) sebesar 25%, Menanggapi (*Respond*) sebesar 23.33% dan Memulihkan (*Recover*) sebesar 58.33%. Namun untuk keseluruhan nilai NIST *Security Framework* yang didapat hanya 27.55%. Ini membuktikan bahwa keamanan informasi yang dimiliki PT NPI masih sangat rendah. Hal ini disebabkan karena banyaknya fungsi pada NIST Cybersecurity Framework yang belum diimplementasi sepenuhnya sehingga menimbulkan kerentanan terhadap keamanan informasi di PT NPI.

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.

Referensi

[1] Utomo, M., Ali, A. H. N. and Affandi, I.2005. Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO / IEC 27001: Pada Kantor Pelayanan
[2] Syahrial, Hadi. 2011.Pengembangan Sistem Manajemen Kelemahan Keamanan Informasi (SMKKI) Menggunakan Lotus Notes', *Seminar Nasional Teknologi Informasi & Komunikasi Terapan.*
[3] Utomo, M., Ali, A. H. N. and Affandi, I. 2012. Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO / IEC 27001: 2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I. *Jurnal Teknik ITS*, 1(1): 288–293.
[4] 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.* 121–126.

[5] Ghazouani, Mohamed., Faris, Sophia., Medromi, Hicham., dan Sayouti, Adil. 2014. Information Security Risk Assessment - A Practical Approach With A Mathematical Formulation Of Risk. *International Journal of Computer Applications*; 103 (8).
[6] Huijben, K. A. 2006. lightweight, flexible evaluation framework to measure the ISO 27002 information security controls. 86(2):1–3, doi: 10.4172/2168-9695.1000e118.
[7] NIST. 2014. 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.
[8] Jazri, H. and Jat, S. D. A. 2016. Quick Cybersecurity Wellness Evaluation Framework for Critical Organizations.