

ANALISIS TINGKAT KESIAPAN PENGAMANAN SISTEM INFORMASI (Studi Kasus UPN Veteran Jakarta)

Nurhafifah Matondang¹⁾, Bayu Hananto²⁾, Catur Nugrahaeni³⁾

^{1,2,3}Prodi Sistem Informasi, UPN Veteran Jakarta

e-mail : nurhafifahmatondang@yahoo.com, bayu.hananto86@gmail.com, catur.nugrahaeni@gmail.com

ABSTRACT

The University has a number of data relating to Academic and Higher Education Governance. The large amount of data that requires security, especially in terms of readiness to secure information systems. Maintaining information system security in the university environment aims to maintain confidentiality, fulfill the availability of the system for those who have authority for those who use it and the integrity of the system. The University of National Development "Veteran" Jakarta has work units such as the Faculty, UPT and Bureau where each has the task and function to manage data. The problem is the need to measure the level of information system security to see the maturity of an information system at UPN Veteran Jakarta. OUR Index stands for Information Security Index which is used as a tool to analyze and measure and evaluate the maturity level of information security with the application of SNI ISO / IEC 27001: 2009 standards that can be applied within government agencies. As for the KAMi index version used, namely version 3.1. The method used to solve the problems in OUR index is through six stages, namely the first stage of electronic systems, both information security governance, third information security risk management, the four information security management frameworks, the five asset information management and the six information security technologies. The results obtained after taking measurements using the US Index need improvement in system security in managing information security risks and governance.

Keywords: *Our Index, Security, University*

INTISARI

Universitas memiliki sejumlah data yang berhubungan dengan Akademik dan Tata kelola Perguruan Tinggi. Banyaknya jumlah data sehingga memerlukan keamanan terutama dalam hal kesiapan pengamanan sistem informasi. Menjaga keamanan sistem informasi di lingkungan universitas bertujuan untuk menjaga kerahasiaan, memenuhi ketersediaan sistem bagi pihak yang memiliki otoritas bagi yang menggunakannya dan keutuhan sistem. Universitas Pembangunan Nasional "Veteran" Jakarta memiliki unit kerja seperti Fakultas, UPT dan Biro dimana masing-masing memiliki tugas dan fungsi untuk mengelola data. Permasalahannya adalah perlunya dilakukan pengukuran level tingkat pengamanan sistem informasi untuk melihat kematangan dari sebuah sistem informasi pada UPN Veteran Jakarta. Indeks KAMI merupakan singkatan dari Indeks Keamanan Informasi yang digunakan sebagai alat bantu menganalisa dan mengukur serta mengevaluasi tingkat kematangan keamanan informasi dengan penerapan standar SNI ISO/IEC 27001:2009 dapat diterapkan dilingkungan instansi pemerintah. adapun versi indeks KAMI yang digunakan yaitu versi 3.1. Metode yang digunakan untuk menyelesaikan permasalahan dalam indeks KAMI yaitu melalui enam tahapan yaitu tahap pertama sistem elektronik, kedua tata kelola keamanan informasi, ketiga pengelolaan risiko keamanan informasi, keempat kerangka kerja pengelolaan keamanan informasi, kelima pengelolaan asset informasi dan keenam teknologi keamanan informasi. Hasil yang diharapkan setelah melakukan pengukuran dengan menggunakan Indeks KAMI perlunya perbaikan terhadap keamanan sistem untuk mengurangi risiko keamanan informasi dan tata kelola sistem universitas.

Kata Kunci : Indeks Kami, Keamanan, Universitas

PENDAHULUAN

Keamanan merupakan hal penting dalam pengelolaan sebuah Teknologi Informasi, konsep keamanan bidang komputer saat ini berkembang dengan pesat. Hal ini disebabkan oleh adanya perkembangannya teknologi baik *hardware* maupun *software* yang signifikan. Pemerintah saat ini sedang gencar – gencarnya menggalakkan Standar Nasional Indonesia (SNI) untuk keamanan dalam bidang komputer, hal ini disebabkan oleh maraknya *malware*. *Malware* tersebut diciptakan bertujuan untuk merusak dokumen atau *file* di dalam komputer. Hal tersebut terjadi karena lemahnya monitoring terhadap keamanan di sebuah instansi.

Kementerian Komunikasi dan Informatika (KOMINFO), membangun sebuah perangkat/tools digunakan untuk menganalisa, mengukur dan mengevaluasi kesiapan keamanan dari sebuah instansi. Penilaian kesiapan keamanan sebuah instansi dapat dibagi kedalam beberapa kategori. Kategori yang dinilai adalah Peran TIK, Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi.

UPN “Veteran” Jakarta merupakan Perguruan Tinggi Negeri Baru (PTNB) yang disahkan pada tahun 2014 sudah menerapkan perlindungan teknologi informasi salah satu diantaranya anti virus, *firewall*, dan lain sebagainya. Namun keamanan system informasi di UPN “Veteran” Jakarta seperti informasi yang telah ditampilkan melalui website masih kurang dari segi keamanan yang menyebabkan terjadi beberapa kali kehilangan data karena diserang oleh *hacker* hal inilah yang menjadi dasar untuk dilaksanakannya penelitian ini. Untuk memastikan bahwa semua aspek keamanan telah terpenuhi maka tim peneliti akan melakukan analisis kesiapan keamanan dari UPN “Veteran” Jakarta dalam menghadapi perkembangan teknologi Informasi saat ini.

Hasil yang diperoleh dari penelitian Tedi Agoan, Hans F. Wowor dan Stanley Karouw (2017) dengan judul Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS). Alat ukur yang digunakan dalam penelitian ini yaitu COBIT 5 untuk mendapatkan rekomendasi kematangan sistem informasi

Hasil yang diperoleh dari penelitian Mufti Rizal and Yudho Giri Sucahyo (2013) dengan judul A Study on the Preparedness of Information Security Framework Area based on the Assessment of Information Security Index in Ministry of XYZ. Metode untuk mengukur kematangan sistem pada penelitian ini menggunakan alat ukur yaitu COBIT 4.1.

Hasil yang diperoleh dari penelitian Edit Prima, Yudho G. Sucahyo, and Zainal A. Hasibuan (2013) dengan judul *Mapping the Certification Authority for e-Government Procurement System into eGovAMAN Framework*. Tujuan penelitian ini menjelaskan tentang kerangka kerja untuk melakukan audit pada keamanan informasi di pemerintahan Indonesia.

PENDEKATAN PEMECAHAN MASALAH Indeks KAMI

Indeks KAMI merupakan singkatan dari Indeks Keamanan Informasi yang digunakan sebagai alat/tools bantu menganalisa dan mengukur serta mengevaluasi tingkat kematangan keamanan informasi dengan penerapan standar SNI ISO/IEC 27001:2009 dapat diterapkan di lingkungan instansi pemerintah sebagai gambaran institusi terhadap kesiapan keamanan sistem saat ini untuk analisa lebih lanjut dimasa yang akan datang.

Tahapan evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001:2009. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di instansi pemerintah.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh Instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan snapshot indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembandingan dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian dapat digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (stakeholders).

Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di Instansi pemerintah. Pertukaran informasi dan diskusi

dengan Instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari lesson learned yang sudah

Metode Penelitian ini bersifat deskriptif kualitatif artinya laporan pelaksanaan penelitian disampaikan dalam bentuk deskriptif yang bersifat eksploratif artinya dilakukan dengan cara menggali informasi dari pihak pengelola informasi untuk mengetahui kematangan keamanan yang berlangsung di institusi tersebut.

Tahapan Penelitian

1. Studi awal

Pada langkah ini peneliti menggali penggunaan teknologi informasi dalam institusi, menyiapkan kuesioner dan studi literatur yang berhubungan dengan penelitian ini.

2. Pengumpulan Data

Pada tahap ini peneliti mengumpulkan data yang diperoleh dengan cara melakukan wawancara dan menyebarkan kuesioner.

3. Pengolahan Data

Penulis melakukan pengolahan data dari hasil pengisian kuesioner yang telah diisi oleh responden dengan Indeks KAMI. Hasil yang diperoleh yaitu tingkat kesiapan dengan maturity dan hasil pengolahan data dengan Ms. Excel.

4. Analisis Data

Pada tahap ini, peneliti melakukan analisis terhadap tingkat maturity.

5. Simpulan dan Saran

Pemberian saran dan simpulan terhadap hasil penelitian dan institusi yang menjadi objek peneliti.

HASIL DAN PEMBAHASAN

Pengukuran adalah hal yang mutlak untuk dilakukan guna mendapatkan peningkatan kualitas. Untuk mengetahui tingkat keamanan penggunaan sistem informasi pada Universitas Pembangunan Nasional Veteran Jakarta, pada penelitian ini menggunakan perangkat/tools indeks KAMI. Dalam melakukan penilaian terdapat 141 pertanyaan yang akan dijawab oleh responden.

Tahap penilaian pertama : Kategori sistem elektronik

Bagian ini mengevaluasi kategori sistem elektronik yang digunakan. Jumlah pertanyaan sebanyak 10 sehingga menghasilkan jumlah skor penetapan kategori sistem elektronik dengan total 28 dan tingkat ketergantungan termasuk tinggi.

Tahap penilaian kedua : Tata kelola keamanan informasi

Pada tahapan ini tindakan yang dilakukan mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi, fungsi dan tugas tanggung jawab pengelola keamanan informasi dilingkungan UPNVJ. Sejumlah 22 pertanyaan diajukan ke responden.

Tahap penilaian ketiga : Pengelolaan risiko keamanan informasi

Tahapan ini melakukan evaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Pertanyaan yang di ajukan ke responden sejumlah 16 pertanyaan.

Tahap penilaian ke empat : Kerangka Kerja Pengelolaan Keamanan Informasi

Tahapan ini melakukan evaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Pertanyaan yang diberikan ke responden sejumlah 29 pertanyaan tujuannya adalah untuk mengetahui apakah pada tahapan ini penilaian tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian dana tau diterapkan secara menyeluruh.

Tahap penilaian ke lima : Pengelolaan Aset Informasi

Tahapan ini melakukan evaluasi kelengkapan pengamanan asset informasi, termasuk keseluruhan siklus penggunaan asset tersebut. Sejumlah 38 pertanyaan di ajukan ke responden untuk mengetahui apakah pada tahapan ini penilaian tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian dana tau diterapkan secara menyeluruh.

Tahap penilaian ke enam : Teknologi dan keamanan informasi

Tahapan ini merupakan tahapan terakhir yang bertujuan untuk mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan asset informasi. Sebanyak 26 pertanyaan di ajukan kepada responden untuk mengetahui apakah pada tahapan ini penilaian tidak dilakukan, dalam perencanaan, dalam penerapan

atau diterapkan sebagian dana tau diterapkan secara menyeluruh.

Hasil rekapitulasi pengolahan data observasi dimuat dalam table sebagai berikut :

Tabel : Skor Area Pada UPN Veteran Jakarta

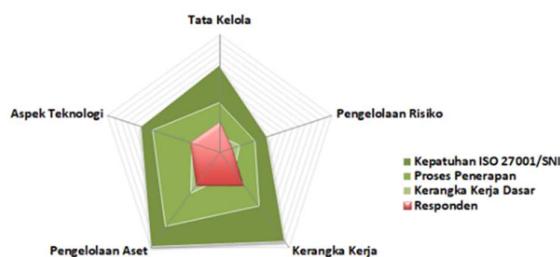
Area	Skor
Kategori Sistem Elektronik	28
Tata Kelola Keamanan Informasi	44
Pengelolaan Risiko Keamanan Informasi	18
Kerangka Kerja Keamanan Informasi	57
Pengelolaan Aset	59
Teknologi dan Keamaan Informasi	45

Berdasarkan informasi yang ditampilkan dalam table, disimpulkan bahwa :

1. Peran sistem elektronik pada UPN Veteran Jakarta setelah dilakukan pengujian terletak pada level tinggi dengan nilai 28
2. Penerapan kelengkapan TKPS UPN Veteran Jakarta dari hasil pengukuran berada pada level “Tidak Layak”, area “Merah” dengan total nilai 223, berkaitan dengan jumlah rata-rata seluruh nilai pertanyaan pada worksheet Keamanan Sistem Informasi yang di evaluasi.



Gambar 2. Hasil evaluasi keamanan dengan Penilaian Indeks KAMI



Gambar 3 : Diagram radar hasil penilaian Indeks KAMI

Untuk melihat kelengkapan penerapan hasil penilaian maka pada bagian tengah diagram terdapat warna merah muda yaitu menunjukkan kondisi Sistem Keamanan UPN Veteran Jakarta

saat penelitian ini dilakukan sehingga hasil pengisian kuesioner yang disebar kepada responden. Dijelaskan sebagai berikut:

1. Terdapat lima area keamanan informasi yang diperoleh, tampak bahwa UPN Veteran Jakarta pada aspek penilaian risiko dan kerangka kerja mengalami perhatian yang kurang oleh pimpinan dan oleh pihak pengelola sistem sehingga sangat perlu dilakukan perbaikan untuk keamanan sistem.
2. Pada Area Pengelolaan asset, Tata kelola dan Aspek teknologi terlihat bahwa proses penerapan sudah mulai direncanakan dan dilaksanakan secara keseluruhan.

KESIMPULAN

Penelitian ini telah memenuhi tujuannya yakni dapat menguji dapat kesiapan keamanan sistem informasi dilindungi institusi peneliti, sehingga hasil yang diperoleh penulis menarik kesimpulan bahwa tingkat ketergantungan UPNVJ terhadap teknologi sangat tinggi tetapi masih perlu banyak pembenahan diberbagai bidang aspek. Universities juga perlu meningkatkan pengamanan system terutama untuk mengurangi risiko yang akan terjadi.

DAFTAR PUSTAKA

- [1] S.M. Arief, “Kajian Keamanan Teknologi dan Sistem Informasi Dengan Menggunakan Metode Indeks KAMI: Studi Kasus Pada Perusahaan XYZ”, *Faktor Exacta*, vol. 8, no. 2, pp. 169-180, 2015.
- [2] D.K. Putri, “Pengukuran Kesiapan Manajemen Keamanan Informasi Direktorat Sistem Informasi Universitas Telkom Menggunakan ISO/IEC 20000 Dan COBIT 5”, *e-Proceeding of Engineering*, vol.2, No.3 Desember 2015|Page 7854.ISSN: 2355-9365.
- [3] M.R. Ridho. “Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya”, *Jurnal Teknik Pomits*, vol. 1, no. 1, 2012. 1-6.
- [4] T. Agoan, H.F. Wowor dan S. Karouw, “Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan Framework COBIT 5 Domain Evaluate,

- Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS)”, *E-Journal Teknik Informatika*, vol. 10, no. 1 (2017).ISSN: 2301-8364.
- [5] Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika, *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*, Jakarta, Indonesia, 2011.
- [6] M. Rizal, dan Y.G. Sucahyo, *A Study on the Preparedness of Information Security Framework Area based on the Assessment of Information Security Index in Ministry of XYZ*, Conference: 2013 Internasional Conference on Advanced Computer Science and Information Systems (ICACSIS), September 2013, DOI:101109/ICACSIS.2013.6761552.
- [7] E. Prima, Y.G. Sucahyo, dan Z.A. Hasibuan, *Mapping the Certification Authority for e-Government Procurement System into eGovAMAN Framework*, 2013 5th International Conference on Advanced Computer Science and Information Systems, ICACSIS 2013 - Bali, Indonesia, 2013.
- [8] C. Chazar, “Model Perencanaan Keamanan Sistem Informasi Menggunakan Pendekatan Metode Octave dan ISO 27001:2005”, *Seminar Nasional Telekomunikasi dan Informatika (Selisik 2016)*, Bandung, Mei 28, 2016. ISSN:2503-2844.
- [9] KOMINFO, *Indeks Keamanan Informasi (KAMI)*, 2013, Website: [https://kominfo.go.id/index.php/content/detail/3326/Indeks+Keamanan+Informasi+\(KAMI\)/0/keamanan_informasi](https://kominfo.go.id/index.php/content/detail/3326/Indeks+Keamanan+Informasi+(KAMI)/0/keamanan_informasi), diakses tanggal 2 Februari 2018.
- [10] KOMINFO, *Audisi Pertama "Born to Protect", Jaring Bakat Cyber Security Indonesia*, 2017, Website: https://kominfo.go.id/content/detail/10363/audisi-pertama-born-to-protect-jaring-bakat-cyber-security-indonesia/0/berita_satker,