CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol.3, No. 1, Mei 2020, hlm. 1-6

EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA KANTOR WILAYAH KEMENTERIAN HUKUM DAN HAM DIY

Taufiq Effendy Wijatmoko

Jurusan Magister Informatika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga Yogyakarta
Email: taufiq.ew@gmail.ac.id

Abstrak

Kantor Wilayah Kementerian Hukum dan HAM DIY merupakan instansi vertikal Kementerian Hukum dan HAM Republik Indonesia yang berkedudukan di provinsi yang melaksanakan tugas dan fungsi dalam hal layanan Hukum dan HAM, Kemigrasian, Pemasyarakatan dan Administrasi. Dalam pelaksanaannya dibantu dengan Teknologi Informasi dalam bingkai *e-government* berdasarkan suatu tata kelola pemerintahan yang baik (*Good Corporate Governance*). Pengelolaan informasi merupakan salah satu aspek dalam *Good Corporate Governance*, termasuk kualitas dan keamanan pengelolaan informasi. Penggunaan Indeks KAMI untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi dan diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Hasil dari penggunaan Indeks KAMI versi 4.1 di Kantor Wilayah Kementerian Hukum dan HAM DIY ini adalah tingkat ketergantungan penggunaan sistem pemerintahan berbasis elektronik (*e-government*) sebesar 32 dari total skor 50 dan masuk kedalam kategori Tinggi dimana sistem pemerintahan berbasis elektronik (*e-government*) adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 314 dari 645 dan berada pada kategori pemenuhan kerangka kerja dasar. Rekomendasi dari penelitian ini dapat dijadikan sebagai bahan pertimbangan dan evaluasi bagi instansi dalam melakukan perbaikan yang berkaitan dengan mitigasi atau pencegahan kerentanan keamanan informasi, serta memastikan regulasi dapat dicapai dengan baik dan kebijakan keamanan institusi di masa yang akan datang.

Kata kunci: *Indeks KAMI, ISO 27001:2013, Keamanan Informasi, e-government.*

INFORMATION SECURITY EVALUATION USING INFORMATION SECURITY INDEX (KAMI) IN THE MINISTRY OF LAW AND HAM DIY

Abstract

Ministry of Law and Human Rights DIY is a vertical agency of the Ministry of Law and Human Rights Republic of Indonesia domiciled in the provinces carry out their duties and functions in terms of Law and Human Rights, Migration, Correctional and Administration services. In its implementation, it is assisted by Information Technology in the e-government framework based on a good corporate governance. Information management is one aspect of Good Corporate Governance, including the quality and security of information management. The use of the KAMI Index to measure the level of maturity and completeness in information security is followed by the adoption of ISO 27001 as an international security standard that can help an organization ensure that the security of information applied is effective. The results of the use of the KAMI 4.1 index in the Ministry of Law and Human Rights DIY is the level of dependence of the use of electronic systems by 32 of the total score of 50 and into the High category where the electronic system is an inseparable part of the running work process. The results of the assessment of the five areas that have been carried out amounted to 314 of 645 and are in the category of meeting the basic framework. Recommendations from this research can be used as material for consideration and evaluation for the institution to make improvements relating to mitigation or prevention of information security vulnerabilities, as well as ensuring regulations can be achieved properly and institutional security policies in the future.

Keywords: *KAMI Index, ISO 27001: 2013, Information Security, e-government.*

1. PENDAHULUAN

Indonesia yang tergolong sebagai negara berkembang satu dasawarsa ini menunjukkan peningkatan pesat dalam penggunaan internet. Walaupun belum menyamai negara-negara maju lainnya, tetapi hal ini sudah dapat menggambarkan bahwa Indonesia sudah siap untuk beralih menuju pada penerapan *e-government*. Implementasi *e-government* merupakan suatu bentuk perubahan baru yang diharapkan dari sebuah negara yang berkembang. Karena semakin berkembangnya informasi dan semakin pesatnya kemajuan TIK, perubahan untuk menjadi *good government* sangat diharapkan masyarakat. Masyarakat sangat optimis dengan adanya *e-government* yang nantinya diharapkan menimbulkan dampak perubahan ke arah yang lebih baik bagi pelayanan dalam pemerintahan (Heeks, 2006).

Internet merupakan sebuah media pertukaran informasi dan data yang terbuka, artinya internet dapat diakses oleh siapa saja, kapan saja dan darimana saja. Dengan berbagai kecanggihan sarana komunikasi modern tersebut, internet sangat rentan terhadap serangan sistem informasi. Tanpa adanya sistem keamanan terhadap informasi membuat sistem informasi yang dimiliki individu,organisasi bahkan instansi pemerintahan menjadi sangat rentan terhadap adanya upaya-upaya penyerangan sistem informasi (Al-jaghoub, Al-yaseen and Al-hourani, 2010).

Saat ini, penggunaan TIK di lingkungan pemerintah sebagai penyelenggara pelayanan publik terus mengalami pertumbuhan, sejalan dengan kebutuhan penyediaan pelayanan publik yang cepat, andal dan aman. Penggunaan TIK yang makin kompleks dapat menyebabkan kerawanan dan ancaman Keamanan Informasi,yang meliputi aspek kerahasiaan, keutuhan, dan ketersediaan layanan, sehingga dapat mengganggu kinerja penyelenggara pelayanan publik. Peran sumber daya informasi dan TIK semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi tata kelola pemerintahan yang baik (*Good Corporate Governence*) (Carbonel, 2008).

Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah berupa gangguan dan ancaman yang menyangkut aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

Adanya ancaman terhadap sumber daya informasi tersebut membutuhkan adanya sebuah tata kelola keamanan informasi di setiap organisasi/ instansi tidak terkecuali instansi penyelenggara pelayanan publik milik pemerintah. Dengan demikian perlu ditingkatkan kesiapan dan kewaspadaan terhadap ancaman serangan keamanan informasi pada instansi pemerintah terutama pada infrastrutur kritis milik pemerintah.

Salah satu upaya yang dapat dilakukan oleh kementrian Kominfo untuk meningkatkan kualitas keamanan informasi pada suatu instansi adalah dengan membuat salah satu alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Indeks KAMI mengacu pada ISO 27001 yang berisi tentang keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif.

Dalam menerapkan tata kelola keamanan informasi di lingkungan instansi pemerintah dibutuhkan kesiapan baik yang mencakup beberapa aspek, di antaranya: infrastruktur, perencanaan, dana/finansial dan kesiapan sumber daya manusia. Dengan demikian, kajian ini ditujukan untuk menggali dan mengevaluasi sejauh mana kesiapan instansi pemerintah dalam hal ini Kantor Wilayah Kementerian Hukum dan HAM Daerah Istimewa Yogyakarta untuk menerapkan tata kelola keamanan informasi. Beberapa sistem informasi utama yang diterapkan, diantaranya adalah website yang mencakup layanan hukum dan HAM, layanan Keimigrasian, dan layanan Pemasyarakatan secara online, Sistem Informasi Surat Masuk dan Keluar (SISUMAKER), Sistem Informasi Manajemen Kepegawaian (SIMPEG), serta Sistem Informasi Kehadiran Apel (SIKAP).

2. TINJAUAN PUSTAKA

2.A. Keamanan Informasi

Keamanan informasi merupakan suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin akan timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, dan mengoptimalkan pengembalian investasi. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharingkan maka semakin besar pula resiko terjadi kerusakan, kehilangan atau terekseposnya data ke pihak eksternal yang tidak diinginkan (Sarno & Iffano, 2009).

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam sebuah organisasi. Jenis keamanan informasi dapat dibagi menjadi beberapa bagian berikut (Whitman & Mattord, 2013) :

- *Physical security*
- *Personal security*
- *Operational security*
- *Communications security*

- *Network security*

2.B. Aspek Keamanan Informasi

Informasi merupakan salah satu aset penting dari perusahaan. Perusahaan melakukan pengolahan terhadap informasi, kemudian hasilnya disimpan dan dibagikan. Keamanan sistem informasi terdiri dari perlindungan terhadap aspek-aspek berikut ini:

a) *Confidentiality* (Kerahasiaan) Aspek yang menjamin kerahasian data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasian data yang dikirim, diterima dan disimpan.
b) *Integrity* (Integritas) Aspek yang menjamin bahwa data tidak diubah tanpa ada ijin pihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
c) *Availability* (Ketersediaan) Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (Harliana, Perdana, & Prasetyo, 2015).

Sumber lain menyebutkan bahwa aspek keamanan sistem informasi melingkupi 4 aspek. Grafinkel mengemukakan bahwa keamanan komputer melingkupi 4 aspek, yaitu *privacy*, *integrity*, *authentication* dan *availability*. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non-repudiation* (Juliharta, 2015).

Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi, Pasal 1 Butir 6 berbunyi, “Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.”

Prinsip keamanan sistem informasi dapat diilustrasikan sebagai berikut :

Gambar 1. CIA Triangle

Ketiga parameter ini adalah sebuah parameter umum yang digunakan untuk menilai baik atau buruknya sebuah keamanan pada suatu jaringan, yang ditinjau dari tiga aspek, yaitu : *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan) suatu informasi. Parameter ini sering dikenal dengan istilah CIA.

2.C. Sistem Manajemen Keamanan Informasi

Sebuah organisasi harus menerapkan Sistem Manajemen Keamanan Informasi untuk menjamin keamanan aset teknologi informasi dan komunikasi (TIK). Sistem Manajemen Keamanan Informasi adalah kumpulan dari kebijakan dan prosedur untuk mengatur data sensitif milik organisasi secara sistematis. Tujuan dari SMKI sendiri adalah untuk meminimalisir risiko dan menjamin kelangsungan bisnis secara proaktif untuk membatasi dampak dari pelanggaran keamanan.

Sistem Manajemen Keamanan Informasi juga harus mengacu pada standar nasional atau internasional yang ada agar kualitas pengamanan yang diberikan tinggi dan mampu menanggulangi adanya masalah. Standar internasional yang telah direkomendasikan untuk penerapan SMKI adalah ISO/IEC 27001. Standar ini telah berjalan berbasis risiko sehingga mampu mengurangi ancaman dan menanggulangi masalah dengan cepat dan tepat.

2.D. ISO 27001 sebagai Standar SMKI

ISO 27001:2013 ini merupakan sebuah standar yang dikeluarkan oleh *International Organization for Standardization*. ISO 27001 ini merupakan standar yang ditujukan dapat membantu perusahaan dalam melindungi keamanan aset perusahaan dan untuk melindungi sistem manajemen keamanan informasi (SMKI).

SMKI merupakan sebuah pendekatan yang bersifat sistematis yang bertujuan untuk mengelola informasi penting maupun informasi perusahaan yang bersifat sensitif agar tetap aman. SMKI ini juga memberikan panduan untuk mengelola unsur yang termasuk dalam melakukan pengelolaan informasi penting seperti manusia, proses dan sistem Teknologi Informasi dengan menerapkan proses manajemen risiko yang telah sesuai standar.

2.E. Indeks Keamanan Informasi (KAMI) versi 4.1 sebagai Tools SMKI

Indeks KAMI versi 4.1 adalah sebuah tools yang digunakan untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan ISO 27001:2013 dan gambaran tata kelola keamanan informasi di sebuah organisasi. Indeks KAMI ini dibuat oleh pihak Kementrian Kominfo. Alat evaluasi ini tidak digunakan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat yang untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pemimpin instansi.

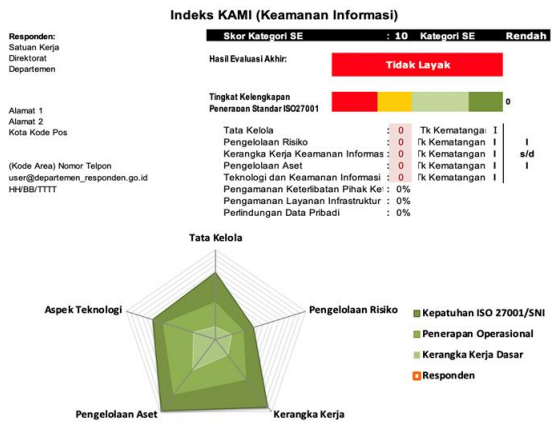
Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Evaluasi yang dilakukan dengan menggunakan indeks KAMI ini mencakup 5 target area, yaitu tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi & keamanan informasi.

Sebelum dilakukan proses penilaian secara kuantitatif, maka dilakukan proses klasifikasi terlebih dahulu terhadap kategori sistem pemerintahan berbasis elektronik (*e-government*). Responden diminta untuk mendeskripsikan Sistem Elektronik yang ada dalam satuan kerjanya secara singkat. Tujuan dari penilaian kategori Sistem Elektronik ini adalah untuk mengelompokkan instansi kedalam ukuran tertentu yang akan ditampilkan dalam gambar berikut :

Rendah	
10	15
Tinggi	
16	34
Strategis	
35	50

Gambar 2. Nilai Kategori Sistem Elektronik

Setelah menklasifikasikan Peran SE di instansi terkait, maka akan dilakukan penilaian terhadap kelima area yang ada di Indeks KAMI versi 4.1. Hasil penilaian menggunakan Indeks KAMI versi 4.1 akan digambarkan kedalam diagram yang berbentuk jaring laba-laba (*spider chart*) dengan 5 area utama. Dalam jaring laba-laba tersebut juga akan dilihat tentang nilai Indeks KAMI dengan kepatuhan terhadap ISO/IEC 27001:2013 [8]. Hasil evaluasi menggunakan indeks KAMI versi 4.1 dapat dilihat melalui gambar berikut :



Gambar 3. Dashboard Penilaian Indeks KAMI 4.1

Semakin tinggi ketergantungan sebuah instansi terhadap Peran SE, maka semakin banyak bentuk pengamanan yang diperlukan dan harus diterapkan sampai tahap tertinggi. Pada Gambar 4 dibawah ini akan menunjukkan skor akhir yang akan disesuaikan dengan status kesiapan instansi terkait mengenai keamanan informasinya

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Gambar 4. Matriks Kategori SE dan Status Kesiapan Indeks KAMI 4.1

3. METODOLOGI PENELITIAN

Penelitian ini adalah penelitian evaluatif mengenai kesiapan penerapan tata kelola keamanan informasi dengan metode penelitian kualitatif. Tujuan penelitian ini adalah untuk menghasilkan sebuah rekomendasi terkait dengan keamanan informasi pada Kantor Wilayah kementerian Hukum dan HAM DIY.

Adapun penjelasan masing-masing tahapan penelitian secara sistematis dijelaskan pada penjelasan berikut:

- Tahap 1, pendefinisian masalah dan tinjauan literatur. Pada tahap ini dilakukan untuk mempelajari berbagai teori yang relevan mencakup teori untuk mengkaji kesiapan keamanan informasi instansi Kantor Wilayah Kementerian Hukum dan HAM DIY.
- Tahap 2, pengumpulan dan analisis data. Setelah diperoleh model pengkajian yang cocok, dilakukan pengumpulan data berikut analisis data untuk mengetahui kondisi kesiapan keamanan informasi pada instansi pemerintah.
- Tahap 3, rekomendasi strategi peningkatan kesiapan keamanan informasi pada instansi pemerintah. Berdasarkan data kondisi tersebut dilakukan *gap analysis* dengan kondisi ideal, selanjutnya akan disusun strategi dan alternatif kebijakan peningkatan kesiapan keamanan informasi pemerintah.

Dalam melakukan penelitian ini, data dikumpulkan dengan cara:

- Studi Literatur.
  Studi literatur dilakukan untuk mempelajari berbagai dokumen/ referensi yang terkait dengan tema penelitian untuk dijadikan acuan.
- Wawancara pejabat pengelola dan document review.
  Proses ini dilakukan untuk mendapatkan gambaran terkini/kondisi mengenai objek

penelitian. Dalam penelitian ini, proses ini dilakukan juga untuk mengetahui visimisi, strategi serta tujuan jangka panjang keamanan informasi pemerintah.

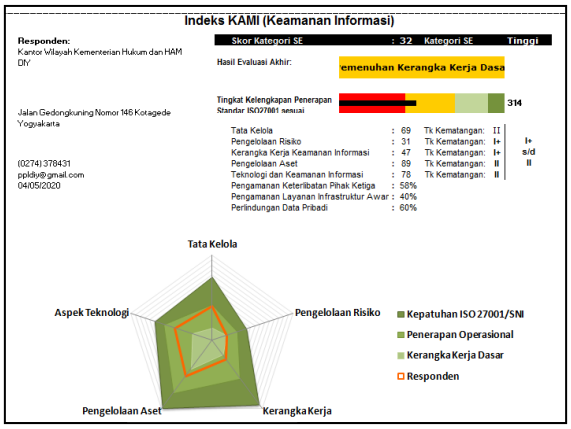
- Wawancara mendalam dengan pakar.
  Wawancara dengan pakar bertujuan untuk mendapatkan pandangan dari pakar secara teknis mengenai kondisi kesiapan keamanan informasi.

Analisis dan interpretasi data menggunakan metode analisis kualitatif. Teknik analisis ini dilakukan menggunakan pendekatan logika induktif, di mana penarikan kesimpulan dibangun berdasarkan pada hal-hal khusus atau data di lapangan yang bermuara pada kesimpulan-kesimpulan umum. Analisis data kualitatif adalah upaya yang dilakukan dengan cara mengorganisasikan data dengan memilah-milahnya menjadi satuan yang dapat dikelola kemudian mensintesanya (Bogdan & Biklen, 1982). Kemudian berdasarkan proses tersebut, ditemukan apa yang penting dan apa yang dapat dipelajari untuk menunjang keputusan. Penelitian ini dilakukan di Kantor Wilayah Kementerian Hukum dan HAM D.I. Yogyakarta.

4. HASIL DAN PEMBAHASAN

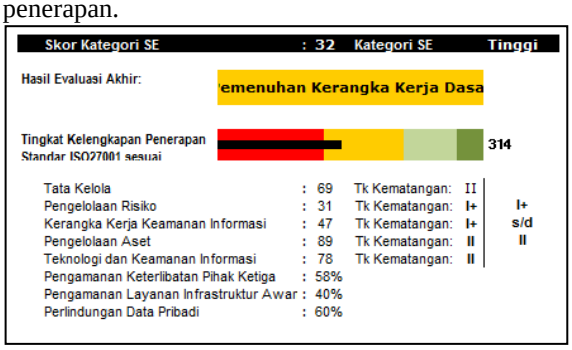
4.A. Analisis Hasil Penilaian Indeks KAMI

Berikut ini adalah tampilan dari dashboard penilaian menggunakan indeks KAMI pada Kantor Wilayah Kementerian Hukum dan HAM DIY:



Gambar 5. Hasil dashboard Indeks KAMI 4.1 Kantor Wilayah Kementerian Hukum dan HAM DIY

Dashboard diatas merupakan gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan indeks KAMI versi 4.1. Dari dashboard diatas, dapat dilihat bahwa tingkat kematangan keamanan informasi di Kantor Wilayah kementerian Hukum dan HAM DIY masih berada pada tingkat II dengan nilai sebesar 314. Dapat dilihat pada radar chart dashboard tersebut bahwa hampir seluruh area yang dinilai dalam indeks KAMI belum terpenuhi dan sesuai dengan ISO 27001. Jika dilihat dibagian radar chart dashboard, hasil yang didapat sampai kategori proses penerapan.



Gambar 6. Hasil Indeks KAMI 4.1 Kantor Wilayah Kementerian Hukum dan HAM DIY

Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI versi 4.1 masih masih berada pada kategori I+ dan II. Berikut ini adalah uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

Tabel 1. Tingkat Kematangan Kelima Area

	Tata kelola	Pengelola-an resiko	Kerangka kerja	Pengelola-an aset	Tekno-logi
Tingkat Kematangan II					
Status	II	I+	I+	II	II
Tingkat Kematangan III					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Tingkat Kematangan IV					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Tingkat Kematangan V					
Status	No	No	No	No	No
Validitas	No	No	No	No	No
Status Akhir	II	I+	I+	II	II

Urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III+, sedangkan untuk saat ini tingkat kematangan dari Kantor Wilayah Kementerian Hukum dan HAM DIY berada pada tingkat I - II. Tingkat kematangan ini menunjukkan posisi Kantor Wilayah Kementerian Hukum dan HAM DIY sebagai berikut ini:

Tabel 2. Tingkatan kondisi Kantor Wilayah Kementerian Hukum dan HAM DIY

Tingkatan	Kondisi
I	Kondisi Awal
II	Penerapan Kerangka Kerja Dasar
III	Terdefinisi dan Konsisten
IV	Terkelola dan Terukur
V	Optimal

5. KESIMPULAN DAN SARAN

5.A. Kesimpulan

Kesimpulan yang dapat diperoleh dari penelitian ini terkait penilaian manajemen keamanan

informasi di Kantor Wilayah kementerian Hukum dan HAM DIY dengan menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

a) Hasil dari penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 32 dari jumlah total keseluruhan sebesar 50. Hal ini menunjukkan bahwa Kantor Wilayah kementerian Hukum dan HAM DIY sudah tinggi dalam kebutuhan penggunaan sistem pemerintahan berbasis elektronik (*e-government*). Hal ini menunjukkan bahwa pemanfaatan Teknologi Informasi dalam bentuk sistem pemerintahan berbasis elektronik (website, Sistem Informasi Manajemen Kepegawaian, Sistem Informasi Surat Masuk dan Keluar, dll) adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan.
b) Hasil keseluruhan dari penilaian kelima area dalam Indeks KAMI adalah sebesar 314 dari jumlah total keseluruhan sebesar 645 dan berada pada level I-II dimana level ini berada pada kondisi awal penerapan keamanan informasi dan kondisi penerapan kerangka kerja dasar penerapan keamanan informasi.
c) Tingkat kematangan per-area akan dijabarkan sebagai berikut: Area Tata Kelola Keamanan Informasi berada pada tingkat II, area Pengelolaan Risiko Keamanan Informasi pada tingkat I+, area Kerangka kerja Pengelolaan Keamanan Informasi pada tingkat I+, area Pengelolaan Aset Informasi pada tingkat II, dan area Teknologi & Keamanan Informasi pada tingkat II.
d) Hasil penilaian kelima area yang menunjukkan nilai sebesar 314, dengan hasil nilai tingkat penggunaan sistem pemerintahan berbasis elektronik (*e-government*) sebesar 32 maka Kantor Wilayah kementerian Hukum dan HAM DIY belum dapat dikatakan matang dan sesuai dengan standar ISO 27001:2013 karena belum mencapai level III+ dimana penerapan keamanan informasi telah terdefinisi dan konsisten.

5.B. Saran Perbaikan Keamanan Informasi

Kantor Wilayah Kementerian Hukum dan HAM sudah menerapkan Tata Kelola TIK, dengan kapasitas sesuai dengan kondisi SDM, dukungan pimpinan, dan pendanaan. Untuk mengoptimalkan peningkatan keamanan informasi perlu didukung dengan peningkatan kapasitas SDM, penguatan komitmen pimpinan serta dukungan pendanaan.

Peran IT harus ditingkatkan baik secara struktur maupun kebijakan. Hal ini diperlukan agar kebijakan yang dikeluarkan dalam bidang TIK khususnya keamanan informasi dapat dijadikan landasan hukum yang kuat bagi instansi dalam menerapkan tata kelola TI dan tata kelola keamanan informasi.

Hal terpenting dalam kaitan penerapan kemanan informasi adalah membangun kesadaran akan keamanan informasi. Selanjutnya adalah membuat prosedur dan kebijakan yang terkait dengan pengelolaan keamanan informasi. Setelah itu membuat kelembagaan keamanan informasi untuk dapat menerapkan tata kelola keamanan informasi.

Pada Kantor Wilayah Kementerian Hukum dan HAM DIY perlu dibentuk penanggung jawab dalam hal tata kelola TIK, seperti CIO (*Chief Information Officer*) dan juga penanggung jawab yang khusus di bidang keamanan informasi, seperti CISO (*Chief Information Security Officer*). Instansi juga perlu membentuk struktur kelembagaan tim respon insiden seperti CERT *(Computer Emergency Response Team)* khusus untuk menangani adanya insiden keamanan informasi.

DAFTAR PUSTAKA

AL-JAGHOUB, S., AL-YASEEN, H. AND AL-HOURANI, M. (2010) 'Evaluation of Awareness and Acceptability of Using e-Government Services in Developing Countries : the Case of Jordan', 13(1), pp. 1–8.

BOGDAN, R.C. & BIKLEN K.S., 1982. Qualitative Research for Education: An Introduction to Theory and Methods. Allyn and Bacon, Inc.: Boston London

CARBONEL, J.-C., 2008. Assessing IT security governance through a maturity model and the definition of a governance profile.Information System Control Journal, Vol.2, ISACA , 4.

HARLIANA P., PERDANA A., PRASETYO R.M.K., 2015. Sniffing dan Spoofing Pada Aspek Keamanan Komputer. https://www.academia.edu/5088063/Jurnal Keamanan-Komputer,

HEEKS, R. 2006. Implementing and Managing e-Government : An International Text. London: SAGE Publications Ltd.

JULIHARTA, I. G. P. K. (2015) 'Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing', *Jurnal Sistem Dan Informatika*, 10(1), pp. 149–158.

SARNO, R,. & IFFANO, I., 2009. Sistem Manajemen Keamanan Informasi, Surabaya: ITS Press.

WITMAN, M.E., MATTORD, H.J, 2014. Principles of Information Security Fifth Edition, Boston: Cengage Learning.