Jurnal ICT : Information Communication & Technology
Vol. 20, No.2, Desember 2021, pp. 291-297
p-ISSN: 2302-0261, e-ISSN: 2303-3363, DOI:

Pencegahan Serangan Siber Pada Sistem Informasi Manajemen Sekolah Di SMK Wahidin Kota Cirebon Berbasis Indeks Kami dan ISO 27001

Asep Suherman [1], Tedi Susanto [2], Djohar Syamsi[3], I Putu Robin Sunjaya[4], Muhammad Nasir[5]
[1,2,3,4,5]Program Magister Sistem Informasi, STMIK LIKMI Bandung, Indonesia
Email: [1]asepsuherman3@gmail.com, [2]tedi.susanto1984@gmail.com, [3]djohar09@gmail.com,
[4]iputurobins@gmail.com, [5]siap86.nsr@gmail.com

INFORMASI ARTIKEL

Histori artikel:

Naskah masuk: 15 Agustus 2021
Direvisi: 24 Agustus 2021
Diterima: 25 Agustus 2021

Kata Kunci:

cyber crime, hacking, keamanan sistem, sistem informasi manajemen sekolah, TIK

ABSTRAK

Abstract - *Wahidin Vocational School in Cirebon City is one of the vocational high schools that has used Information and Communication Technology (ICT) in managing school activities. Along with the development of digital-based school management, the potential for system security disturbances is also getting bigger. The problem of security disturbances related to cyber crime is currently included in the Top Ten Global Risk, meaning that it has a very detrimental impact. Forms of cyber crime include data theft, hacking, and breaches of network security. The purpose of this study is to find the right pattern in measuring the security feasibility of an ICT system, as well as to find a standardized management model of the ICT system, so that the ICT system built is protected from cyber attacks. The method used in this study is qualitative with primary data sources derived from the results of the assessment and evaluation of the ICT system at Wahidin Vocational School by using the Information Security Index (KAMI). While the stages of activities carried out include evaluation of ICT management methods, as well as methods of measuring the level of ICT security. The result of this activity is a method of preventing cyber attacks that can be used as a reference in building a reliable and accurate ICT system. The conclusion of this research activity is that cyber attacks can be prevented if ICT managers implement system management based on the cyber risk management framework from ISO27001 and continuously conduct security feasibility assessments based on SNI ISO/IEC 27001 criteria.*

Abstrak **–** SMK Wahidin di Kota Cirebon merupakan salah satu sekolah menengah kejuruan yang telah mempergunakan Teknologi Informasi dan Komunikasi (TIK) dalam mengelola kegiatan sekolah. Seiring dengan perkembangan manajemen sekolah berbasis digital, maka potensi gangguan keamanan sistem juga semakin besar. Permasalahan gangguan keamanan yang terkait dengan *cyber crime* pada saat ini telah masuk dalam *Top Ten Global Risk*, artinya memberikan dampak yang sangat merugikan. Bentuk *cyber crime* antara lain pencurian data, *hacking*, dan pelanggaran terhadap keamanan jaringan. Tujuan penelitian ini adalah mencari pola yang tepat dalam mengukur kelayakan keamanan sebuah sistem TIK, serta mencari model pengelolaan yang terstandarisasi dari sistem TIK, sehingga sistem TIK yang dibangun terhindar dari serangan siber. Metode yang digunakan pada penelitian ini adalah kualitatif dengan sumber data primer berasal dari hasil assessment dan evaluasi terhadap sistem TIK di SMK Wahidin dengan mempergunakan alat bantu Indeks Keamanan Informasi (KAMI). Sedangkan tahapan kegiatan yang dilakukan meliputi evaluasi terhadap metode pengelolaan TIK, serta metode pengukuran tingkat keamanan TIK. Hasil dari kegiatan ini adalah suatu metode pencegahan terhadap serangan siber yang dapat dijadikan acuan dalam membangun sistem TIK yang handal dan akurat. Kesimpulan dari kegiatan penelitian ini adalah serangan siber dapat dicegah jika pengelola TIK menerapkan pengelolaan sistem berdasarkan *cyber risk management framework* dari ISO27001 serta secara kontinyu selalu melakukan assessment kelayakan keamanan berdasarkan kriteria SNI ISO/IEC 27001.

Jurnal ICT : Information Communication & Technology p-ISSN: 2302-0261
Vol. 20, No.2, Desember 2021, pp. 291-297 e-ISSN: 2303-3363

***Penulis Korespondensi**:*

Asep Suherman
Program Magister Sistem Informasi, STMIK LIKMI –
Jln. Insinyur Juanda, Bandung
Email: asepsuherman3@gmail.com

1. Pendahuluan

Pengembangan dan penggunaan Teknologi Informasi dan Komunikasi (TIK) dalam bidang pendidikan dapat mendorong reformasi untuk melaksanakan manajemen sekolah yang lebih baik [2]. Berbagai layanan terkait proses belajar mengajar para siswa, pengolahan data akademik dan data kepegawaian, serta data pendukung lainnya telah menggunakan TIK. Sistem *physical distancing* dan *social distancing* yang telah diterapkan sebagai akibat pandemi Covid-19 telah mendorong meningkatnya penggunaan TIK untuk mendukung proses belajar mengajar dari rumah serta kegiatan manajemen sekolah [9][10]. Agar sistem TIK yang dibangun mampu memberikan layanan yang maksimal, maka diperlukan pengelolaan yang memenuhi standart-standart yang sudah baku terhadap sistem TIK tersebut.

Dalam penyelenggaran tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek tata kelola TIK mengalami gangguan. Beberapa hal yang menjadi masalah keamanan informasi antara lain yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) [7].

Kajian ini akan membahas dua permasalahan utama didalam mengelola sistem TIK untuk manajemen sekolah kejuruan, yaitu langkah-langkah yang seharusnya dilakukan untuk pencegahan dan mengurangi dampak buruk terhadap serangan siber, serta cara mengukur tingkat keamanan sistem TIK yang dibangun. Pada paper ini, sebagai studi kasus adalah SMK Wahidin di kota Cirebon. SMK Wahidin, merupakan salah satu sekolah menengah kejuruan yang telah membangun dan mempergunakan TIK untuk berbagai layanan digital kepada para siswa dan guru, serta mitra kerjasama.

Semakin meningkatnya pemanfaatan TIK untuk mengelola kegiatan di sekolah, maka kebutuhan terhadap keamanan sistem, database, dan sistem jaringan juga semakin meningkat, begitu pula dengan resiko terhadap serangan siber [6]. Ruang siber dapat diartikan sebagai Lingkungan dimana data digital dibentuk, disimpan, dan dibagi [12], sedangkan serangan siber merupakan suatu upaya untuk mengganggu sistem TIK atau pencurian data-data.

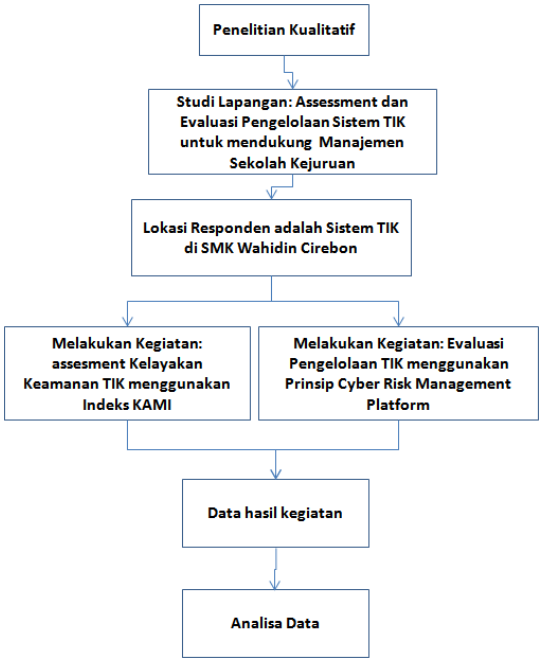
Resiko yang muncul dari serangan siber adalah kerusakan sistem, pencurian informasi, dan manipulasi informasi [5]. Oleh karena itu untuk mencegah serangan siber dan meminimalkan dampak yang terjadi, maka pada sistem TIK untuk manajemen sekolah memerlukan pengelolaan yang baik, yaitu dengan menerapkan *cyber-risk management* [8].

Kontribusi yang dapat diberikan dari kajian ini adalah terwujudnya acuan dalam membangun TIK untuk mendukung manajemen sekolah, khususnya di sekolah menengah kejuruan. Acuan tersebut berisi tahapan-tahapan yang harus dilakukan untuk mengelola sistem TIK guna mencegah serangan siber, serta metode untuk melakukan audit teknologi guna mengetahui tingkat keamanan dari sistem TIK yang dibangun.

2. Metode

Metode yang dipergunakan pada kajian ini adalah Kualitatif yaitu berdasarkan studi kasus terkait pengelolaan sistem TIK untuk mendukung manajemen sekolah di SMK Wahidin Kota Cirebon. Sebagaimana blok diagram dibawah ini yang menggambarkan tahapan kegiatan dari kajian ini yang meliputi :

a) Studi Pustaka;
b) Studi lapangan yang dilakukan di SMK Wahidin Kota Cirebon;
c) Pengumpulan data primer yang dilakukan dengan cara assessment menggunakan Indeks Keamanan Informasi (KAMI) dan evaluasi pengelolaan sistem TIK berbasis *cyber risk management framework* dari ISO 27001;
d) Selanjutnya data-data hasil *assessment* dan data hasil evaluasi akan dianalisa untuk mendapatkan kesimpulan;



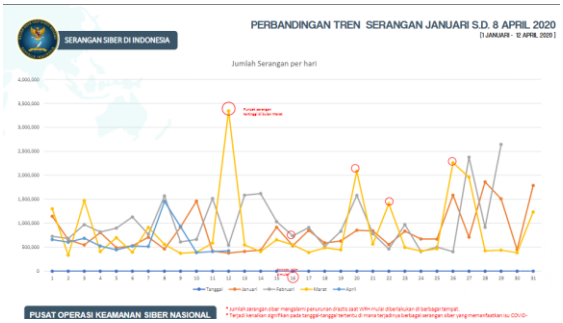
Gambar 1. Blok diagram dari metode penelitian.

2.1 Isu Global Serangan Siber

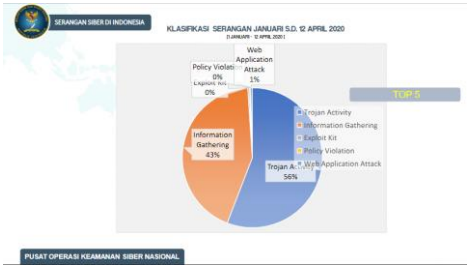
Menurut Aon's 2015 *Global Risk Management Survey*, *cyber risk* saat ini masuk dalam *Top Ten Global Risk*, yang berarti bukan lagi sebagai risiko dengan probabilitas dampak yang kecil [4].

Data dari *The Need for a New IT Security Architecture: Global Study*, menyatakan bahwa 71% perusahaan yang diteliti mengatakan bahwa risiko ini muncul akibat dari ketidakmampuan organisasi dalam mengontrol gadget beserta aplikasi para karyawannya, dan 74% merupakan akibat dari sistem IT yang ketinggalan zaman. Studi ini juga menggambarkan bahwa kunci untuk menekan terjadinya *cyber risk* dalam beberapa tahun ke depan adalah dengan manajemen database (73%), manajemen konfigurasi sistem (76%), dan manajemen aplikasi (72%). Studi ini menjadi penting untuk perusahaan yang saat ini benar-benar peduli akan keamanan informasi dan data rahasia internal [4].

Berikut ini adalah data-data yang terkait serangan siber pada bulan Januari - April tahun 2020 yang terekam oleh Badan Siber Dan Sandi Negara.



Gambar 2. Data Serangan Siber bulan Januari-April 2020.
Sumber (Rekapitulasi Insiden Web Defacement- Badan Siber Dan Sandi Negara.)



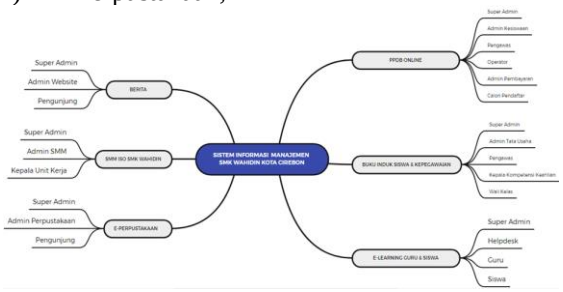
Gambar 3. Klasifikasi Serangan Siber Januari-April 2020.

Gambar diatas memperlihatkan aksi serangan siber di Indonesia, untuk itu diperlukan sosialisasi kepada para pengguna TIK dan acuan terkait upaya untuk pencegahan terhadap serangan siber.

2.2 Disain Sistem Informasi Manajemen Sekolah

Gambar dibawah menunjukkan blok diagram dari Sistem Informasi Manajemen Sekolah di SMK Wahidin. Pada dasarnya sistem Informasi Manajemen yang dibangun mempunyai beberapa fitur, antara lain :

a) PPDB *On-Line*.
b) Buku Induk Siswa dan Kepegawaian;
c) *E-Learning* Guru dan Siswa;
d) Berita;
e) SMM ISO SMK Wahidin;
f) E-Perpustakaan;



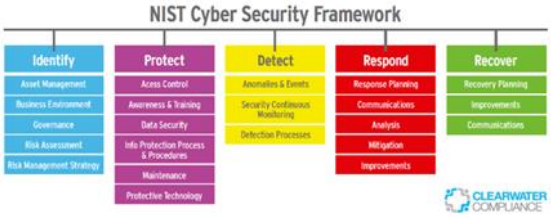
Gambar 4. Blok Diagram Sistem Informasi Manajemen Sekolah.

Dari gambar diatas terlihat bahwa fitur-fitur yang tersedia sebagai basis layanan terhadap para siswa, guru dan kegiatan di sekolah sudah cukup memadai. Untuk mengetahui apakah sistem TIK yang dibangun oleh SMK Wahidin mempunyai kelayakan dari sisi tingkat keamanannya, maka akan dilakukan pengujian dengan menggunakan Indeks Keamanan Informasi (KAMI).

2.3 Metode Pencegahan Serangan Siber Berdasarkan ISO 27001

Agar pembangunan TIK dapat memberikan manfaat yang maksimal dalam mendukung manajemen sekolah, maka pihak pengelola TIK perlu menerapkan standart prosedur dalam mengelola sistem TIK. Berdasarkan ISO 27001 dan *NIST Cyber Security Framework*, terdapat lima komponen kunci dalam cyber risk management framework [4], yaitu :

a) *Protect Valuable Data:* merupakan tindakan dari pihak pengelola TIK untuk mengidentifikasi data dan informasi yang dianggap berharga serta di mana data dan informasi tersebut disimpan dan siapa saja yang berhak mengaksesnya.
b) *Monitor for cyber risk* : merupakan himbauan kepada pengelola TIK untuk mengembangkan sistem intelijen yang dapat langsung memberikan sinyal alarm, jika terjadi serangan siber.
c) *Understand your cyber perimeter*: merupakan kewajiban dari pengelola TIK untuk mengetahui seluas apa jangkauan keamanan yang perlu dijaga. Bukan hanya pada area gedung/ kantor, tapi juga area dimana *stakeholders* memiliki akses terhadap jaringan internal perusahaan. Sistem TIK yang memadai dan kedisiplinan karyawan menjadi tiang-tiang penopang keberhasilan *cyber risk management.*
d) *Improve cyber intelligence*: merupakan kewajiban bagi pengelola TIK untuk mengembangkan sistem inteligen yang berkaitan dengan *cyber risk.* Fungsinya untuk mengatasi kesenjangan antara sistem-sistem yang dimiliki oleh pengelola, baik itu sistem keuangan, sumber daya manusia, dan lainnya. Dengan *cyber intelligence*, perusahaan juga dapat menganalisis secara lebih mendalam mengenai kemungkinan-kemungkinan lain yang dapat merugikan. Penelitian dan perkembangan seputar *cyber intelligence* juga menjadi relevan untuk terus diperkaya secara berkesinambungan.
e) *Report and Take action*: merupakan peringatan bagi pengelola TIK untuk mempunyai tim yang solid dalam membangun *cyber security* yang efektif, yaitu segenap pihak yang memiliki pengetahuan, keahlian, dan pengaruh yang kuat yang dapat memastikan sistem kontrol *cyber risk management* berjalan dalam koridor optimal. Sehingga pihak pengelola bisa segera mengambil keputusan yang cepat dan tepat atas laporan yang akurat.



Sumber : Article from clearwatercompliance.com

Gambar 5. Model Cyber Security Framework

Gambar diatas menjelaskan model tindakan yang harus dilakukan secara terus menerus terkait keamanan sistem informasi, untuk mencegah serangan *cyber*. Lima langkah diatas merupakan tindakan yang disarankan oleh ISO 27001 dan *NIST Cyber Security Framework*, untuk pencegahan dari serangan siber.

2.4 Indeks Keamanan Informasi

Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001 [1][11]. Indeks Keamanan Informasi (KAMI) merupakan sebuah perangkat audit teknologi untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan sistem informasi.

KAMI merupakan perangkat evaluasi untuk menganalisa tingkat kesiapan pengamanan sistem informasi. Perangkat ukur ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan sistem informasi [3].

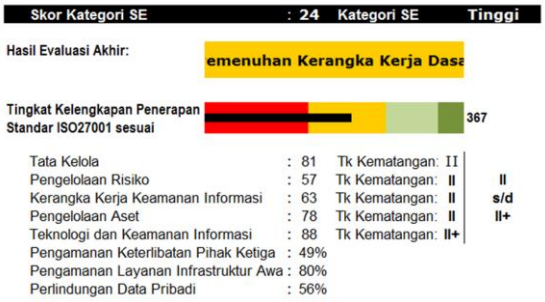
Pada dasarnya KAMI merupakan sebuah perangkat evaluasi untuk melihat gambaran dari sebuah sistem informasi yang telah dibangun. Didalam KAMI terdapat 7 tabel yang harus diisi oleh pengguna, Tabel tersebut berisi beberapa pertanyaan yang terkait dengan bagaimana sistem TIK yang dibangun dikelola. Tujuh tabel tersebut terdiri dari :

1. Tabel ke-satu terdiri dari bagian Kategori Sistem Elektronik, yaitu mengevaluasi tingkat atau kategori sistem elektronik yang digunakan;
2. Tabel ke-dua terdiri dari bagian Tata Kelola Keamanan Informasi, yaitu mengevaluasi tata kelola keamanan informasi beserta

instansi/perusahaan/fungsi, tugas dan tanggungjawab pengelola keamanan sistem informasi;

3. Tabel ke-tiga terdiri dari Pengelolaan Resiko Keamanan Sistem Informasi, yaitu mengevaluasi kesiapan penerapan pengelolaan resiko keamanan sistem informasi sebagai dasar penerapan strategi keamanan sistem informasi;
4. Tabel ke-empat terdiri dari Kerangka Kerja Pengelolaan Keamanan Sistem Informasi, yaitu mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan sistem informasi dan strategi penerapannya;
5. Tabel ke-lima terdiri dari Pengelolaan Aset Informasi, yaitu mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut;
6. Tabel ke-enam terdiri dari Teknologi dan Keamanan Informasi, yaitu mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi;
7. Tabel ke-tujuh terdiri dari Suplemen, yaitu mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi;

Selanjutnya secara otomatis perangkat ukur KAMI akan menyajikan hasil dari pengisian questioner sebagaimana hasil dari evaluasi dari sistem TIK yang dibangun oleh SMK Wahidin. Gambar dibawah menunjukkan hasil evaluasi KAMI terhadap sistem TIK di SMK Wahidin.



Gambar 6. Hasil pengisian questioner KAMI SMK Wahidin

Gambar diatas memperlihatkan bahwa sistem TIK yang dibangun oleh SMK Wahidin untuk manajemen sekolah berada diposisi kuning, artinya secara kerangka dasar telah memenuhi persyaratan kemananan.

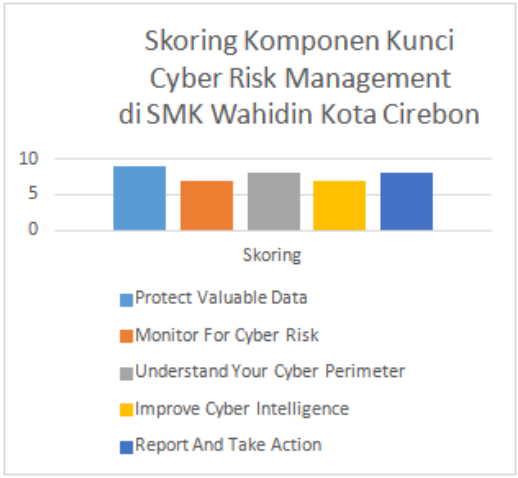
3. Hasil dan Pembahasan

Hasil dari Assessment menggunakan Indeks KAMI dan hasil evaluasi menggunakan lima parameter *Cyber Risk Management Framework* terhadap pengelolaan TIK di SMK Wahidin setelah dilakukan analisa dan diskusi didapat hasil sebagai berikut :

a) Pengelolaan TIK untuk mendukung kegiatan manajemen sekolah di SMK Wahidin telah menggambarkan upaya untuk meningkatkan layanan sesuai dengan prinsip-prinsip didalam proses bisnis yang modern yaitu terkait dengan efektifitas dan effisiensi.
b) Lima hal yang disarankan oleh ISO 27001 dan *NIST Cyber Security Framework* yang terkait dengan *cyber risk management framework*, telah dilaksanakan oleh SMK Wahidin, meskipun belum semuanya dapat diwujudkan oleh pengelola sistem TIK di SMK Wahidin Kota Cirebon. Gambar dibawah ini merupakan hasil penilaian terhadap pelaksanaan pengelolaan TIK menggunakan parameter Cyber Security Framework dari ISO 27001.

Tabel 1. penilaian parameter manajemen TIK

Komponen Kunci	Skoring
Protect Valuabel Data	9
Monitor For Cyber Risk	7
Understand Your Cyber Primeter	8
Improve Cyber Intellgence	7
Report and Take Action	8



Gambar 7. Grafik penilaian manajemen TIK.

c) Untuk mencegah serangan siber, dapat dilakukan dengan meningkatkan kualitas sistem TIK dengan mempergunakan metode yang sudah baku dan teruji efektifitasnya, yaitu dari ISO 27001 dan *NIST Cyber Security Framework.*
d) Dari hasil essessment dengan mempergunakan pengisian kuesioner dari Indeks KAMI, didapat hasil: bahwa sistem TIK yang dibangun oleh SMK Wahidin untuk mendukung kegiatan manajemen sekolah, secara umum dapat dikatakan telah memenuhi kerangka dasar

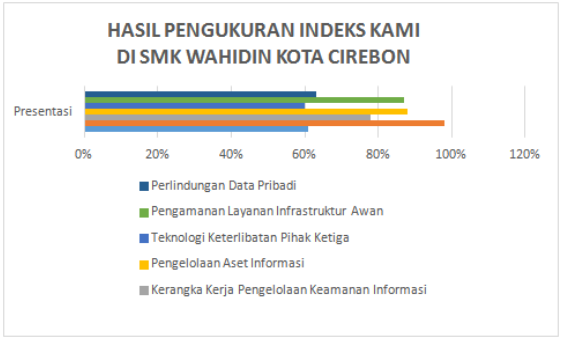
keamanan, sebagaimana hasil *assessment* dibawah ini.

Presentasi hasil pengukuran menggunakan indeks KAMI di SMK Wahidin Kota Cirebon

Tabel 2. Hasil *Assessment* Indeks KAMI.

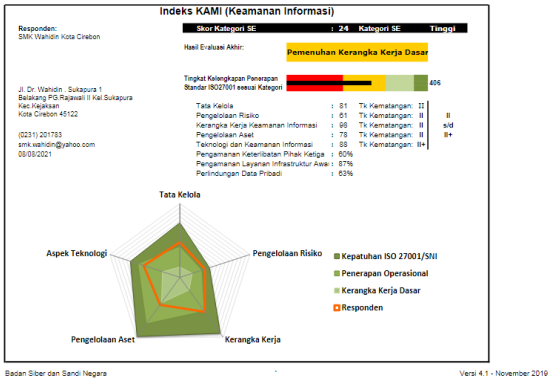
Kategori Sistem Elektronik	**24**
Instrumen KAMI Versi 4.1	**Presentasi**
Tata Kelola Keamanan Sistem Informasi	61%
Pengelolaan Resiko Keamanan Sistem Informasi	98%
Kerangka Kerja Pengelolaan Keamanan Informasi	78%
Pengelolaan Aset Informasi	88%
Teknologi Keterlibatan Pihak Ketiga	60%
Pengamanan Layanan Infrastruktur Awan	87%
Perlindungan Data Pribadi	63%

Gambar 9 diatas menunjukkan hasil keseluruhan assessment terhadap sistem TIK di SMK Wahidin.



Gambar 8. Hasil pengisian Tabel KAMI

Gambar 8 juga memperlihatkan hasil pengukuran dari tiap komponen assessment.



Gambar 9. Hasil keseluruhan dari *assessment*.

Gambar 9 memperlihatkan hasil keseluruhan dari assessment di SMK Wahidin.

4. Bagian Kesimpulan

Bahwa pembangunan sistem TIK untuk mendukung manajemen sekolah, seharusnya di disain dan di kelola dengan mengacu pada standart-standart yang sudah diakui (ISO 27001 dan *NIST Cyber Security Framework)* dan audit teknologi dengan mempergunakan perangkat KAMI perlu dilakukan secara kontinyu untuk mengetahui tingkat keamanan sistem secara keseluruhan.

Saran : Audit teknologi perlu dilakukan juga pada komponen *software*/perangkat lunak, serta selalu meningkatkan pengetahuan SDM pengelola sistem TIK. Perkembangan teknologi IT akan semakin berkembang pada era Industri 4.0, untuk itu untuk mendukung pengembangan sistem TIK diperlukan pula kegiatan riset pada lingkup pengelola sistem TIK.

Daftar Pustaka

[1] Badan Sisber dan Sandi Negara; Assesment Indeks KAMI; https://bssn.go.id/indeks-kami/

[2] Budiana, H.R., Sjafirah, N.A. dan Bakti, I., Pemanfaatan Teknologi Informasi Dan Komunikasi Dalam Pembelajaran Bagi Para Guru Smpn 2 Kawali Desa Citeureup Kabupaten Ciamis, Jurnal Aplikasi Ipteks untuk Masyarakat, ISSN 1410 – 5675, Vol. 4, No. 1, Mei 2015: 59 – 62.

[3] Fanny Wahyu Kurniawan; Pengukuran Indeks Keamanan Sistem Informasi Berdasarkan Standar ISO 27001: (Studi Kasus Instansi Badan Nasional Penempatan dan Perlindungan Tenaga Kerja Indonesia) ; Makalah Program Studi : Magister Teknik Elektro, Universitas Mercubuana, 2015.

[4] I Gede Christian Adiputra, M.M. – Trainer & Consultant PPM Manajemen *Tulisan ini dimuat di SWA Online (https://dev.ppm-manajemen.ac.id/id_ID/blog/artikel-manajemen-18/post/ancaman-cyber-risk-1352)

[5] I. Rahmawati, "Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense," J. Pertahanan dan Bela Negara, vol. 7, no. 2, pp. 51–66, 2017.

[6] M. J. Hutchins, R. Bhinge, M. K. Micali, S. L. Robinson, J. W. Sutherland, and D. Dornfeld, "Framework for Identifying Cybersecurity Risks in Manufacturing," Procedia Manuf., vol. 1, pp. 47–63, 2015.

[7] Muhammad Ikhsan, Eko Darwiyanto, Dawam Dwi Jatmiko Suwawi," Audit Keamanan Sistem Informasi Akademik Sekolah Tinggi Farmasi Bandung Berbasis Risiko dengan Menggunakan Standar ISO 27001," e-Proceeding of Engineering : Vol.3, No.3 December 2016 | Page 5221, ISSN : 2355-9365.

[8] Obrina Candra Briliyant, Rizqi Aulia Ashari, Rencana Penerapan Cyber-Risk Management

Menggunakan NIST CSF dan COBIT 5, Jurnal Sistem Informasi (Journal of Information System), Volume 14, Issue 2, October 2018.

[9] Reni Kurniawati Pertiwi, Sutama, Membudayakan Kelas Digital Untuk Membimbing Siswa Dalam Pembelajaran Di Tengah Pandemi Covid-19, Jurnal Kajian Teknologi Pendidikan, e-ISSN 2615-8787, Vol 3 No (4) November (2020): 350-365.

[10] Ratih, Anjelina Tanti Kusumaningrum," Analisis Pemanfaatan Teknologi Informasi Dan Komunikasi Pada Pembelajaran Daring Di Tengah Pemdemi Covid-19," Edustream: Jurnal Pendidikan Dasar, Volume IV, Nomor 2, November 2020, E-ISSN: 2614-4417.

[11] Sutara, "Pengukuran Keamanan Informasi PDAM Titra Medal Menggunakan Indeks KAMI Untuk Analisis Tingkat Kematangan Keamanan Informasi," JICT - STMIK IKMI Cirebon – Vol.17, No.2 – Desember 2018, p-ISSN: 2302-0261, e-ISSN: 2303-3363.

[12] Wisnu Handi Prabowo, Satriya Wibawa, Fuad Azmi," Perlindungan Data Personal Siber di Indonesia," Padjadjaran Journal of International Relations (PADJIR), e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (218-239) doi: 10.24198/padjir.v1i3.26194.