CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 5, No. 1, Mei 2022, hlm. 32-45

OPTIMASI KEAMANAN INFORMASI MENGGUNAKAN MANAJEMEN INDEKS KEAMANAN INFORMASI (KAMI) STUDI KASUS: IBISA PURWOREJO

Eko Jhony Pranata[1], Muhammad Taufiq Nuruzzaman [2]

[12] Universitas Islam Negeri Sunan Kalijaga Yogyakarta
Email: [1]ekojhonypranata@gmail.com, [2]m.taufiq@uin-suka.ac.id

Abstrak

Serangan yang terjadi pada jaringan sudah sangatlah umum untuk saat ini, dengan semakin banyaknya cara untuk mengakses data dan tentu saja semakin banyak teknologi yang digunakan untuk meningkatkan ancaman terhadap keamanan jaringan. Optimasi terhadap Keamanan Informasi dengan menggunakan Indeks Keamanan Informasi (KAMI) pada jaringan IBISA Purworejo mendapatkan Hasil indeks yaitu 235, sehingga dapat dikatakan belum optimal dan masih banyak perbaikan. Oleh karena itu yang menjadi dasar perlunya implementasi Open Source SIEM menggunakan Manageengine OpManager ke dalam Indeks Keamanan Informasi (KAMI). Penelitian ini dilakukan sebagai bentuk optimasi untuk mendukung Proses keamanan informasi agar bekerja sesuai dengan standar yang ada pada Indeks KAMI. Metode penelitian yang dilakukan meliputi studi literatur, kemudian melakukan Pra-Assessment indeks KAMI, setelah itu melakukan implementasi infrastruktur ManageEngine OpManager, kemudian melakukan monitoring terhadap Indeks Keamanan Informasi menggunakan teknologi pada ManageEngine OpManager, dan melakukan Post-Assessment Indeks KAMI, selanjutnya tahap akhir ini adalah melakukan Analisis terhadap hasil monitoring dan melakukan perbandingan dari hasil monitoring bagaimana Kondisi jaringan sebelum dan sesudah dilakukannya implementasi ManageEngine OpManager. Skor dari perbandingan untuk hasil penelitian yang terkait dengan indeks KAMI Menunjukkan bahwa skor penilaian pasca diimplementasikan ManageEngine OpManager telah meningkat sebesar 57 lebih baik dari sebelumnya tanpa di diimplementasikan ManageEngine OpManager yang semula didapat nilai 235 menjadi 292. Keuntungan dalam indeks KAMI yaitu membantu menambah nilai pada aspek tata kelola, pengelolaan aset, dan Teknologi dan Keamanan Informasi, akan tetapi Kelayakan keamanan informasi masih pada level I sampai dengan II keamanan informasi pada jaringan berstatus tidak layak dan masih butuh perbaikan.

Kata kunci: *Indeks KAMI, Keamanan Informasi, ManageEngine OpManager*

OPTIMIZATION OF INFORMATION SECURITY USING MANAGEMENT OF INFORMATION SECURITY INDEKS (KAMI) CASE STUDY: IBISA PURWOREJO

Abstract

Attacks that occur on networks are very common nowadays, with more and more ways to access data and of course more and more technologies are used to increase threats to network security. Optimization of Information Security by using the Information Security Index (KAMI) on the Purworejo IBISA network obtained an index result of 235, so it can be said that it is not optimal and there are still many improvements. Therefore, that is the basis for the need to implement Open Source SIEM using Manageengine OpManager into the Information Security Index (KAMI). This research was conducted as a form of optimization to support the information security process so that it works in accordance with the standards in the KAMI Index. The research method carried out includes a literature study, then conducting a Pre-Assessment of the KAMI index, after that implementing the ManageEngine OpManager infrastructure, then monitoring the Information Security Index using technology on the ManageEngine OpManager, and conducting a Post-Assessment of the KAMI Index, then this final stage is Analyze the monitoring results and compare the results of monitoring the network conditions before and after the implementation of ManageEngine OpManager. The score from the comparison for research results related to the KAMI index Shows that the assessment score after the implementation of ManageEngine OpManager has increased by 57, better than before without the implementation of ManageEngine OpManager which originally got a value of 235 to 292. The advantage in the KAMI index is that it helps add value to aspects of governance, asset management, and Information Technology and Security, but the feasibility of information security is still at level I to II information security on the network status is not feasible and still needs improvement.

Keywords*: Indeks KAMI, Information Security, ManageEngine OpManage*

1. PENDAHULUAN

Banyaknya pengguna layanan serta pengaruh internet maka akan semakin banyak pula informasi yang didapatkan dari internet. Di seluruh dunia terdapat sekitar 650 *terabyte* data dan 205 juta *email* di kirim melalui internet setiap menit nya. Perencanaan, desain dan implementasi topologi jaringan, dalam hal ini jaringan komputer nirkabel, tidak dapat diandalkan seperti itu. Perluasan jaringan komputer akan berdampak besar pada kualitas layanan koneksi internet dan kondisi pertukaran data yang ada. Kualitas dari layanan internet maupun koneksi pertukaran data setelah adanya perluasan jaringan maka tentu akan sangat penting untuk merubah performa dari jaringan komputer itu sendiri.

Sesuai dengan Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Standar Sistem Manajemen Keamanan Informasi, setiap instansi pemerintah wajib mematuhi SMKI dan memiliki nilai CIA (Confidentiality, Availability and Integrity) untuk aset informasi. institusi mereka. Menurut penelitian yang dilakukan oleh tim Iccs india, yang menjelaskan bahwa kerugian kejahatan dunia maya diperkirakan mencapai 6 triliun dan 60 juta catatan dikompromikan karena cloud tidak dikonfigurasi sesuai dengan keamanan siber. Pelanggaran keamanan terjadi di bisnis kecil, dengan total 43% serangan. 56% pelanggaran data membutuhkan waktu lebih dari sebulan untuk menemukan penanganan nya. Itu kemudian dikuatkan oleh data tentang serangan ransomware paling umum yang ditemui pada tahun 2019, tetapi WannaCry terus memakan korban di seluruh dunia, dan laporan baru menunjukkan itu tetap menjadi infeksi ransomware nomor satu tahun lalu.

2. TINJAUAN PUSTAKA

WannaCry ditangkap di lebih dari 23,5 persen perangkat yang akhirnya menjadi sasaran ransomware, dan email spam dan phishing tetap menjadi sumber infeksi paling umum tahun lalu, kata Precise Security. Tidak kurang dari 67% infeksi ransomware dikirim melalui email, dan kurangnya pelatihan keamanan siber serta kata sandi yang lemah dan manajemen akses adalah alasan berikutnya mengapa komputer akhirnya dienkripsi setelah serangan. Hanya 16% serangan ransomware yang didukung oleh situs web jahat dan iklan online. "Jumlah serangan ransomware yang menargetkan lembaga pemerintah, organisasi di sektor kesehatan, energi, dan pendidikan terus meningkat.

Sementara beberapa ransomware sederhana dapat mengunci sistem dengan cara yang tidak sulit bagi orang yang berpengetahuan untuk membalikkannya, malware yang lebih canggih mengeksploitasi a teknik yang disebut crypto-virus ransomware. (Dewantara and Sugiantoro, 2021)

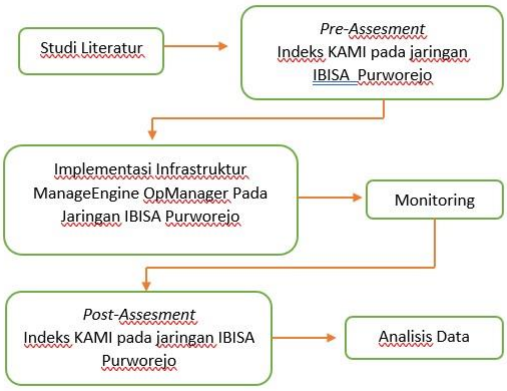
Institut Teknologi Bisnis Dan Kesehatan Bhakti Putra Bangsa Indonesia (IBISA) adalah salah satu perguruan tinggi atau kampus yang berada di Purworejo Jawa Tengah. IBISA memiliki Pusat Pangkalan Data dan Informasi (PUSDATIN) Kampus IBISA memiliki juga memiliki layanan sistem informasi yaitu: Pendaftaran mahasiswa baru IBISA melalui sistem online, Layanan sistem informasi akademik untuk mahasiswa, dosen dan akademik, Data alumni dan Tracer Studi, Sistem layanan ujian online, eLearning terintegrasi dengan sistem akademik, Sistem persuratan terintegrasi dan Sistem Pengelolaan kepegawaian terintegrasi.

Dengan kebutuhan untuk lembaga pemerintah untuk dapat menerapkan standar manajemen keamanan informasi sesuai dengan SMKI dan kebutuhan untuk melacak ke masyarakat adalah pilihan absolut sehingga petugas perlindungan dapat dengan jelas melihat apa yang terjadi dengan jaringannya. Pertanyaannya adalah apakah penggunaan Ossim dapat mendeteksi semua serangan pada jaringan dan secara efektif mengamankan jaringan dari serangan yang ada. Terutama dalam hal pemantauan server dan jaringan, tentu saja, administrator tidak dapat bekerja 24 jam di depan komputernya sehingga selalu tahu jika ada gangguan pada server dan jaringan. (Angga Juansyah, Bagus Pratama, 2018), oleh karena itu fasilitas pendukung diperlukan oleh sistem perdagangan administrator dapat memonitor server dan jaringan meskipun mereka tidak berada di depan komputer secara langsung, sehingga sistem pelacakan diperlukan yang dapat memonitor server mereka dan Jaringan selama 24 jam dan dapatkan pemberitahuan langsung ke admin.

Sebelum standar keamanan informasi diterapkan, evaluasi perangkat keamanan informasi di jaringan IBISA Indonesia diperlukan untuk mendapatkan gambaran tentang kondisi kesiapan dan kematangan manajemen keamanan informasi. Berdasarkan hal ini, penelitian ini akan mengukur tingkat kematangan manajemen keamanan informasi pada jaringan IBISA Indonesia menggunakan versi yang disiapkan oleh komunikasi Indonesia pada tahun 2019, yaitu *Indeks* kami. *Indeks* kami dibuat dengan ISO 27001: 2018 Referensi yang berisi keamanan informasi ISO 27001 adalah bentuk kerangka kerja standar internasional yang berisi standar di wilayah keamanan informasi, ruang lingkup penggunaan teknologi dan manajemen aset yang membantu organisasi memastikan bahwa keamanan informasi telah berjalan dengan efektif.

3. METODE PENELITIAN

Tahap yang akan dilakukan pada penelitian ini terkait dengan evaluasi Keaamanan Informasi (KAMI) menggunakan ManageEngine OpManager pada jaringan IBISA Purworejo dapat dilihat pada gambar berikut.



Gambar 1 Alur Penelitian

3.A. Studi literatur

Adapun tahap pertama dalam penelitian ini adalah Sudi Literatur guna mencari referensi serta landasan teori yang nantinya dapat digunakan sebagai acuan ataupun dasar pada penelitian ini. Studi Literatur dilakukan dengan melakukan *review* terhadap *paper* ataupun jurnal yeng berkaitan dengan tema penelitian ini, membaca dan mengkaji berbagai sumber pustaka yang terkait sebagai justifikasi awal untuk melihat apakan ada perbedaan jika ManageEngine OpManager dan tanpa implementasi ManageEngine OpManager.

3.B. Pre-Assessment Indeks KAMI Pada Jaringan IBISA Purworejo

Sebelum melakukan simulasi terhadap implementasi serangan dapat dilihat hasil dari *Network forensic* yang dilakukan pemaparan mengenai hasil dari simulasi tersebut yang kemudian dilanjutkan dengan pengisian kuesioner *Pre-Assesment* Indeks KAMI kepada responden yang dalam hal ini adalah Kepala Devisi Teknologi Informasi dan Pangkalan data (PUSDATIN) IBISA Purworejo. Adapun hasil dari kuesioner kemudian dilakukan perhitungan yang sesuai dengan format yang ada pada aplikasi dari Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia.

3.C. Implementasi Infrastruktur OpManager Pada Jaringan IBISA Purworejo

Pada tahap ini dilakukan implementasi infrastruktur ManageEngine OpManager pada suatu *server* dan *agent* yang akan ditempatkan pada jaringan IBISA Purworejo dengan ruang lingkup jaringan yang akan dipantau dan dibatasi pada jaringan komputer yang berada di IBISA Purworejo.

3.D. Monitoring

Pada tahap ini dilakukan untuk memantau jaringan dan mendeteksi adanya upaya penyusupan, melakukan proses *filtering*, dan mendeteksi *installation* pada *bandwidth* yang terdeteksi tidak wajar pada jaringan sebagai akibat dari serangan maupun ancaman terhadap keamanan jaringan baik dari *internal* maupun *eksternal.*

3.E. Post-Assessment Indeks KAMI Pada Jaringan IBISA Purworejo

Setelah dilakukannya pemaparan hasil dari monitoring, maka akan dilakukan kembali pengukuran mengenai *Indeks* KAMI terhadap responden dalam hal ini adalah kepada Staff Ahli Analisis Sistem Informasi di kantor PUSDATIN pada lingkungan lingkungan jaringan IBISA Purworejo dengan memberikan *Post-Assesment Indeks* Keamanan Informasi (KAMI) untuk mengukur kembali nilai dari *Indeks* Keamanan Informasi (KAMI) setelah dilakukan monitoring dengan *ManageEngine OpMananager* . Kemudian hasil dari kuesioner akan dihitung kembali sesuai dengan format aplikasi yang dimiliki oleh Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika Indonesia. Kemudian hasil dari perhitungan tersebut akan dibandingkan dengan hasil dari *Pre-Assesment* yang telah dilakukan sebelumnya apakah terdapat perbedaan atau tidak, perbedaan dapat berupa penurunan ataupun peningkatan dalam *Indeks* KAMI terhadap jaringan yang ada di IBISA Purworejo.

3.F. Analisis Data

Adapun tahap akhir pada penelitian ini adalah dengan menganalisis hasil dari monitoring untuk dapat mengetahui perbandingan terhadap jaringan baik sebelum dan setelah dilakukannya implementasi dan instalasi *ManageEngine OpMananager* pada jaringan IBISA Purworejo. Kemudian Hasil dari analisis akan didapatkan kesimpulan untuk menjadi bahan masukan dalam melakukan manajemen keamanan jaringan ke depannya.

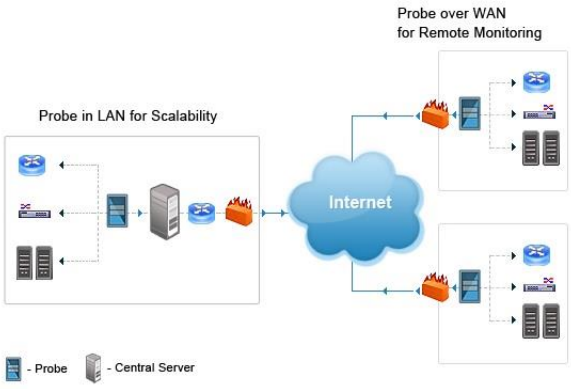
4. HASIL DAN PEMBAHASAN

4.A. Arsitektur OpManager

Arsitektur dari ManageEngine OpManager adalah sebagai berikut:

a. *Central Server*
   Central Server bertindak sebagai konsol terpadu yang menyinkronkan data dengan beberapa server Probe. *Central Server* dirancang untuk memberikan visibilitas jaringan di seluruh lokasi, mengkonsolidasikan, dan melaporkan kesehatan beberapa jaringan jarak jauh.

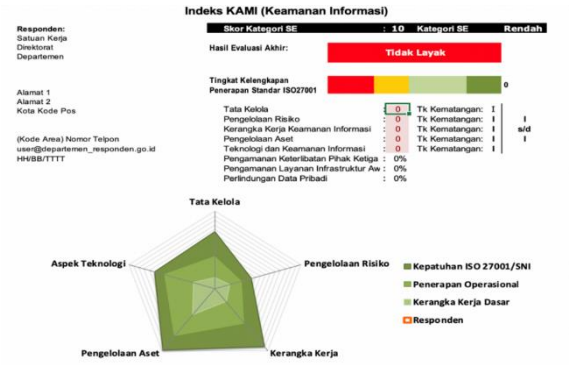
b. *Probe Server*
   Probe Server bertindak sebagai mesin *polling*. Ini memonitor router, switch, firewall, server, dan perangkat jaringan lainnya untuk kesalahan dan kinerja. Ini menghasilkan availability, health, dan performance report. Server Probe secara berkala menyinkronkan data dengan *Central Server*.



Gambar 2 Arsitektur OpManager

4.B. Evaluasi Indeks KAMI

Evaluasi Indeks KAMI direkomendasikan untuk dilakukan oleh staff yang berwewenang dan bertanggung jawab terhadap seluruh pengelolaan keamanan informasi pada instansi.



Gambar 3 Grafik Indeks KAMI

Berdasarkan gambar diatas grafik Indeks KAMI tentang evaluasi yang dilakukan menggunakan Indeks Keamanan Informasi (KAMI) yaitu mencakup 5 aspek diantaranya adalah:

1. Tata kelola keamanan informasi

Bagian ini mengevaluasi bentuk tata kelola keamanan informasi dan organisasi/fungsi, serta kesiapan tanggung jawab dan tanggung jawab Manajer yang bertanggung jawab atas keamanan informasi. Kontrol yang diperlukan adalah untuk mendefinisikan peran, tanggung jawab, Kewenangan pengelolaan keamanan informasi dari penanggung jawab unit kerja hingga pelaksana operasi. Ini termasuk perencanaan kerja berkelanjutan, alokasi anggaran, evaluasi rencana, dan strategi untuk meningkatkan kinerja tata kelola keamanan informasi

2. Pengelolaan Risiko Keamanan Informasi

Pada bagian ini, kesiapan penerapan manajemen risiko keamanan informasi dievaluasi sebagai dasar penerapan strategi informasi keamanan. Pengendalian yang diterapkan adalah adanya kerangka manajemen risiko dan didefinisikan secara jelas terkait dengan ambang batas penerimaan risiko, rencana manajemen risiko dan langkah-langkah mitigasi Tinjau keefektifan nya secara berkala

3. Kerangka kerja Keamanan Informasi

Bagian ini menilai kelengkapan dan kesiapan kerangka manajemen keamanan informasi (kebijakan dan prosedur) Dan strategi implementasi. Pengendalian yang diperlukan adalah sejumlah kebijakan dan prosedur operasi, termasuk strategi implementasi, pengukuran efektivitas pengendalian, dan tindakan korektif.

4. Pengelolaan Aset Informasi

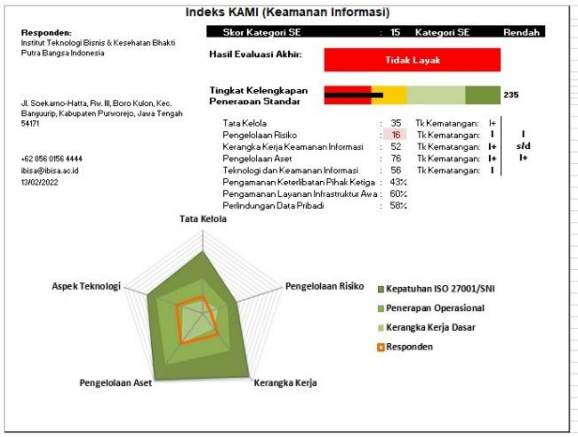
Bagian ini menilai keamanan dan integritas aset informasi, termasuk seluruh siklus hidup aset tersebut. Kontrol yang diperlukan adalah bentuk keamanan terkait keberadaan aset informasi dan seluruh proses teknologi Dan siklus hidup aset yang dikelola.

5. Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi integritas, konsistensi, dan efektivitas penggunaan teknologi untuk melindungi aset informasi. Pengendalian yang digunakan adalah strategi yang berkaitan dengan tingkat risiko dan tidak secara eksplisit menyebutkan teknologi atau merek tertentu. Di antara lima aspek keamanan informasi berdasarkan *Indeks* Keamanan Informasi (KAMI), peran IT dalam melindungi informasi dapat diukur dan digunakan sebagai input. manajer layanan IT.

4.C. Hasil Indeks KAMI

Pada tahap ini membahas tentang hasil dari penilaian secara keseluruhan pada ke-5 area keamanan informasi pada jaringan IBISA Purworejo. Berikut merupakan *dashboard* hasil dari penilaian ke-5 area keamanan informasi jaringan IBISA Purworejo.



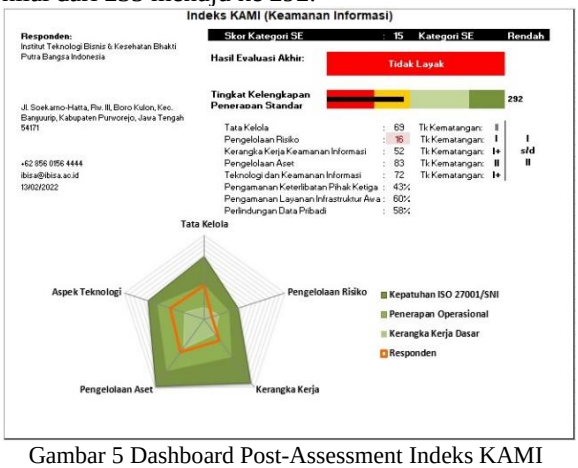
Gambar 4 Dashboard Pre-Assesment Indeks KAMI

Pada gambar diatas 3 menunjukkan bahwa kategori sistem elektronik pada jaringan kampus IBISA Purworejo tergolong kategori **Rendah**, dengan skor 15. Suatu sistem elektronik yang kinerja atau keberlangsungan aliran jaringan IBISA

Purworejo belum sepenuhnya terwujud. Pada saat yang sama, tingkat integritas penerapan ISO 27001 berada pada tingkat "**Tidak Layak**", dengan level skor 235, menunjukkan bahwa ketergantungan tinggi lembaga pada sistem elektronik tidak didukung oleh keamanan informasi yang memadai dari lembaga. Hasil akhir ini juga menunjukkan bahwa jaringan IBISA Purworejo masih membutuhkan banyak perbaikan. Hal ini terlihat dari tingkat kematangan, dengan rata-rata I dan I+ dapat dikatakan kesiapan sertifikasi keamanan informasi masih belum layak untuk sertifikasi keamanan informasi. dikarenakan untuk mencapai batas minimum kesiapan sertifikasi keamanan informasi harus berada pada tingkat III.

Setelah dilakukan analisis dan simulasi, dilakukan pemaparan terhadap hasil analisis forensic pada jaringan IBISA Purworejo dan melakukan kuesioner ulang sebagai bentuk perbandingan, apa yang terjaadi setelah *ManageEngine OpMananager* di diimplementasikan di dalam infrastruktur jaringan IBISA Purworejo. Penelitian melakukan Post-assessment terhadap jaringan IBISA Purworejo dengan kuesioner Indeks Keamanan Informasi (KAMI) untuk dapat mengukur nilai Indeks Keamanan Informasi (KAMI) yang dimiliki instansi tersebut.

Dengan adanya peran penting IT yang begitu tinggi, dan dari hasil analisis serangan dan korelasi nya dengan *ManageEngine OpMananager* yang dilakukan. Seperti gambar 4.6 nilai dari monitoring jaringan IBISA Purworejo adalah 292, hal ini menunjukkan bahwa tingkat kematangan informasi mengalami perubahan atau kenaikan yang sebelumnya ketika *Pre-assessment* berada pada level I s/d I+ kini berada pada level I s/d II ketika *Post-assessment* dilakukan, adapun kenaikan nilai pada aspek Tata Kelola, Pengelolaan Aset dan Teknologi dan Keamanan Informasi sehingga total kenaikan nilai dari 235 menuju ke 292.



Gambar 5 Dashboard Post-Assessment Indeks KAMI

Detail pada setiap aspek yang ada telah diukur dalam indeks dapat dilihat pada grafik Gambar 5, dapat dilihat bahwa tidak ada perubahan pada aspek Pengelolaan Risiko, kerangka kerja keamanan informasi, terjadi perubahan pada aspek Tata kelola, Pengelolaan asset Informasi dan Teknologi dan Keamanan Informasi yang menunjukkan adanya kenaikan secara berturut-turut yaitu 34, 10 dan 16 pion.

4.D. Tata kelola Keamanan Informasi

Tabel 1 Nilai kematangan Area Tata Kelola Keamanan Informasi (i)

Keterangan	Skor
Jumlah pertanyaan Tahap 1	8
Jumlah pertanyaan Tahap 2	8
Jumlah pertanyaan Tahap 3	6
Batas Skor Min untuk Skor Tahap Penerapan 3	48
Total Skor Tahap Penerapan 1 & 2	35
Status Penilaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	27
Skor Minimum Tingkat Kematangan II	*12*
Skor Pencapaian Tingkat Kematangan II	*36*
Status	I+
Skor Tingkat Kematangan III	8
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	8
Skor Pencapaian Tingkat Kematangan III	14
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	24
Skor Pencapaian Tingkat Kematangan IV	54
Status	No

Tabel 2 Nilai Kematangan Area Tata Kelola Keamanan Informasi (ii)

Status Penerapan	Tingkat Kematangan				Total
	II	II I	I V	V	
Tidak Dilakukan	1	0	6	0	7
Dalam Perencanaan	4	2	0	0	6
Dalam Penerapan/Diterapkan Sebagian	8	1	0	0	9
Diterapkan Secara Menyeluruh	0	0	0	0	0
Total	13	3	6	0	22

Skor kelengkapan yang telah didapatkan dari kematangan tata kelola keamanan informasi adalah 35. Berdasarkan tabel 1 dapat di ketahui bahwa jumlah pertanyaan pada tahap 1,2 dan 3 secara berturut-turut adalah 8, 8 dan 6 dengan batas skor terhadap penerapan 3 yaitu 48 dan dengan total tahap

1 & 2 yaitu 35, sehingga status penilaian tahap penerapan 3 berstatus "Tidak Valid". Untuk skor kematangan II yatu bernilai 27 dengan skor minimum yaitu 12 serta skor pencapaian bernilai 36, sehingga didapatilah status "I+". selanjutnya untuk skor tingkat kematangan III bernilai 8 dengan validitas "No" beserta skor minimum bernilai 8 dan skor pencapaian dengan nilai 14, sehingga didapatkan status "No". kemudian untuk skor tingkat kematangan IV bernilai 0 dengan validitas "No" serta skor minimum adalah 24 dan skor pencapaian bernilai 54 sehingga didapatilah status "No".

Berdasarkan Tabel 2 terdapat 7 pertanyaan pada tingkat kematangan II dan IV yang tidak terdapat direspon atau dalam hal ini "Tidak dilakukan". Kemudian terdapat 6 buah pertanyaan yang masing-masing pada tingkat kematangan II dan III yang telaah direspon "Dalam Perencanaan". Selanjutnya pada status penerapan "Dalam penerapan/Diterapkan Sebagian" yang terdapat pada 9 pertanyaan yang telah direspon masing-masing terdapat pada tingkat kematangan II dan III yaitu berturut-turut 8 dan 1. Berdasarkan hasil yang diperoleh diketahui bahwa pada area tata kelola keamanan informasi saat ini pemahaman tentang keamanan informasi Masih belum seperti yang diharapkan dalam instansi, banyak terdapat poin yang tidak atau belum dilakukan.

2.1 Pengelolaan Risiko Keamanan Informasi

Tabel 3 Skor kematangan area Pengelolaan Risiko Keamanan Informasi(i)

Keterangan	Skor
Jumlah pertanyaan Tahap 1	10
Jumlah pertanyaan Tahap 2	4
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	36
Total Skor Tahap Penerapan 1 & 2	16
Status Penilaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	8
Skor Minimum Tingkat Kematangan II	14
Skor Pencapaian Tingkat Kematangan II	*20*
Status	No
Skor Tingkat Kematangan III	4
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	4
Skor Pencapaian Tingkat Kematangan III	8
Status	No
Skor Tingkat Kematangan IV	4
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	8
Skor Pencapaian Tingkat Kematangan IV	12
Status	No
Skor Tingkat Kematangan V	0
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18

Tabel 4 Skor kematangan area Pengelolaan Risiko Keamanan Informasi(ii)

Status Penerapan	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	2	0	0	1	3
Dalam Perencanaan	8	2	2	1	13
Dalam Penerapan/Diterapkan Sebagian	0	0	0	0	0
Diterapkan Secara Menyeluruh	0	0	0	0	0
Total	10	2	2	2	16

Skor yang telah didapatkan pada pengelolaan risiko keamanan informasi adalah 16, berdasarkan tabel 3 dapat diketahui bahwa jumlah pertanyaan pada tahap 1, 2 dan 3 berturut-turut adalah 10, 4 dan 2 dengan batas skor minimal untuk skor tahap penerapan 3 yaitu 36 dan dengan total skor tahap 1 & 2 yaitu 16, sehingga status penilaian tahap penerapan 3 berstatus "Tidak Valid". untuk skor tingkat kematangan II terdapat nilai 8 dengan skor minimum yaitu 14 beserta skor pencapaian yaitu 20 sehingga didapatkan ststus "No". kemudian untuk skor tingkat kematangan III terdapat nilai 4 dengan validitas "No" serta skor minimumnya bernilai 4 dan skor pencapaian bernilai 8 sehingga didapat status "No". Selanjutnya untuk skor tingkat kematangan IV bernilai 4 dengan validitas "No" dengan skor minimum yaitu 8 dan dengan skor pencapaian bernilai 12 dengan status "No". Selanjutnya untuk skor tingkat kematangan V yang bernilai 0 dengan validitas "No" dengan skor minimum yaitu 12 dan skor pencapaian bernilai 18 sehingga mendapat status "No".

Menurut tabel 4 terdapat 3 pertanyaan pada tingkat II dan V yang tidak direspon atau "Tidak Dilakukan" dengan 2 pertanyaan pada tingkat II dan 1 pertanyaan pada tingkat V. kemudian pada tahap "Dalam Perencanaan" terdapat 13 pertanyaan yang masing-masing telah direspon pada tingkat II, III, IV, dan V secara berturut-turut adalah 8 pertanyaan untuk tingkat II, 2 pertanyaan pada tingkat III, 2 pertanyaan pada tingkat IV dan 1 pertanyaan pada tingkat ke V. Untuk tingkat kematangan pada status penerapan "Dalam Penerapan/Diterapkan Sebagian" dan pada tingkat kematangan status penerapan "Diterapkan Secara Menyeluruh" tidak terdapat pertanyaan yang direspon. Berdasarkan hasil yang telah didapatkan dapat diketahui bahwa kondisi pada area Pengelolaan Risiko Keamanan Informasi saat ini yaitu sebagian besar pada Pengelolaan Risiko Keamanan Informasi masih pada tahap perencanaan, meski ada beberapa yang tidak di terapkan.

4.E. Kerangka Kerja Pengelolaan Keamanan Informasi

Tabel 5 Skor kematangan area Kerangka kerja Keamanan Informasi (i)

Keterangan	Skor
Jumlah pertanyaan Tahap 1	12
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	7
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	52
Status Penilaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	20
Skor Minimum Tingkat Kematangan II	15
Skor Pencapaian Tingkat Kematangan II	*24*
Status	I+
Skor Tingkat Kematangan III	32
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	45
Skor Pencapaian Tingkat Kematangan III	62
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	15
Skor Pencapaian Tingkat Kematangan IV	27
Status	No
Skor Tingkat Kematangan V	0
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18
Status	No

Tabel 6 Skor kematangan area Kerangka kerja Keamanan Informasi (ii)

Status Penerapan	**Tingkat Kematangan**				**Total**
	II	**III**	**IV**	**V**	
Tidak Dilakukan	0	2	0	0	2
Dalam Perencanaan	8	5	2	1	16
Dalam Penerapan/Diterapkan Sebagian	2	4	1	1	8
Diterapkan Secara Menyeluruh	1	2	0	0	3
Total	11	13	3	2	29

Skor kelangkapan yang didapatkan pada kerangka kerja keamanan informasi adalah 52. Dapat dilihat dari Tabel 5 bahwa Soal 12, 10 dan 7 masing-masing untuk tahap 1, 2 dan 3 Batas skor minimum untuk skor penerapan 3 adalah 64 poin dari total 64 Implementasi tahap 1 dan 2 adalah 52, sehingga status penilaian pada tahap penerapan 3 berstatus "Tidak Valid". Kemudian Skor Kematangan II memiliki nilai 20 dengan Skor minimum adalah 15 dan skor pencapaian adalah 24, jadi Dapatkan status "I+". Skor Tingkat Kematangan Selanjutnya yaitu III dengan nilai 32, dengan validitas “No”, serta Skor Minimum bernilai 45, dan Skor pencapaian nya adalah 62, sehingga didapatkan status "No". Berikutnya Peringkat Kematangan IV bernilai 0, dengan Validitas “No”, dan dengan Skor minimal yaitu 15 dan skor pencapaian 27dengan statusnya "No". Kemudian untuk tingkat kematangan V terdapat skor 0 dengan Validitas "No", skor minimum bernilai 12 dengan nilai pencapaian skor 18 sehingga didapatkan status "No".

Berdasarkan tabel 6 terdapat 2 pertanyaan pada tingkat kematangan III yang tidak direspon atau “Tidak Dilakukan”. Pada tahap status penerapan “Dalam Perencanaan” terdapat 16 pertanyaan yang masing-masing 8 pertanyaan pada tingkat kematangan II, 5 pertanyaan pada tingkat kematangan III, 2 pertanyaan pada tingkat kematangan IV dan 1 pertanyaan pada tingkat kematangan V. sedangkan pada tahap status penerapan “Dalam Penerapan/Diterapkan Sebagian” terdapat 8 pertanyaan dengan 2 pertanyaan pada tingkat kematangan II, 4 pertanyaan pada tingkat kematangan III dan masing-masing 1 pertanyaan untuk tingkat kematangan IV dan V. pada status penerapan “Diterapkan Secara Menyeluruh” terdapat 1 pertanyaan pada tingkat kematangan II dan 2 pertanyaan pada tingkat kematangan III. Dari hasil tersebut dapat diketahui bahwa pada Area Kerangka Kerja Keamanan Informasi saat ini sebagian besar dokumen kebijakan dan prosedur dalam keamanan informasi berapa pada tahap perancanaan, belum terdapat konsekuensi serta proses tindak lanjut terhadap pelanggaran, Tidak ada proses pengembangan sistem yang diterapkan di dalam institusi Keamanan (SDLC Security).

4.F. Pengelolaan Aset Keamanan Informasi

Tabel 7 Skor kematangan area Pengelolaan Aset Informasi (i)

Keterangan	Skor
Jumlah pertanyaan Tahap 1	24
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	4
Batas Skor Min untuk Skor Tahap Penerapan 3	88
Total Skor Tahap Penerapan 1 & 2	72
Status Penilaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	60
Skor Minimum Tingkat Kematangan II	25
Skor Pencapaian Tingkat Kematangan II	*62*
Status	I+
Skor Tingkat Kematangan III	16
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	35
Skor Pencapaian Tingkat Kematangan III	50
Status	No

Tabel 8 Skor kematangan area Pengelolaan Aset Informasi (ii)

Status Penerapan	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	4	3	0	0	7
Dalam Perencanaan	7	1	0	0	8
Dalam Penerapan/Diterapkan Sebagian	7	2	0	0	9
Diterapkan Secara Menyeluruh	9	3	0	0	12
Total	27	9	0	0	36

Skor kelengkapan yang didapatkan pada pengelolaan aset informasi adalah 76. Berdasarkan tabel 7 jumlah pertanyaan pada tahap 1 adalah 24, kemudian pertanyaan pada tahap 2 adalah 10 dan 4 pertanyaan pada tahap ke 3 dengan batas skor minimal untuk tahap penerapan 3 yaitu 88 dan total skor yang didapat pada tahap 1 & 2 adalah 72, sehingga status pada penerapan 3 berstatus "Tidak Valid". skor kematangan tingkat II bernilai 60 dengan skor minimum yaitu 25 dan skor pencapaian bernilai 62 sehingga berada pada status kematangan "I+". Selanjutnya untuk skor tingkat kematangan III bernilai 16 dengan nilai validitas "No" dan skor minimum bernilai 35 dan skor pencapaian bernilai 50 sehingga didapatkan status "No".

Berdasarkan tabel 8 terdapat 7 pertanyaan pada tingkat kematangan II dan III yang tidak direspon atau "Tidak Dilakukan" masing-masing 4 pertanyaan pada tingkat kematangan II dan 3 pertanyaan pada tingkat kematangan III. Pada tahap status penerapan "Dalam Perencanaan" terdapat 8 pertanyaan yang masing-masing 7 pertanyaan pada tingkat kematangan II, 1 pertanyaan pada tingkat kematangan III. sedangkan pada tahap status penerapan "Dalam Penerapan/Diterapkan Sebagian" terdapat 9 pertanyaan dengan 7 pertanyaan pada tingkat kematangan II, 2 pertanyaan pada tingkat kematangan III. pada status penerapan "Diterapkan Secara Menyeluruh" terdapat 9 pertanyaan pada tingkat kematangan II dan 3 pertanyaan pada tingkat kematangan III. Berdasarkan hasil tersebut dapat diketahui kondisi pengelolaan aset informasi saat ini pada jaringan IBISA Purworejo meskipun ada beberapa poin yang tidak dilakukan secara umum telah melakukan pengelolaan aset teknologi informasi dengan cukup baik.

4.G. Teknologi Keamanan Informasi

Tabel 9 Skor area kerangka Teknologi dan Keamanan Informasi (i)

Keterangan	Skor
Jumlah pertanyaan Tahap 1	14
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	68
Total Skor Tahap Penerapan 1 & 2	56
Status Penilaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	16
Skor Minimum Tingkat Kematangan II	18
Skor Pencapaian Tingkat Kematangan II	*28*
Status	No
Skor Tingkat Kematangan III	40
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	40
Skor Pencapaian Tingkat Kematangan III	62
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	6
Skor Pencapaian Tingkat Kematangan IV	9
Status	No

Tabel 10 Skor area kerangka Teknologi dan Keamanan Informasi (ii)

Status Penerapan	Tingkat Kematangan				Total
	II	III	IV	V	
Tidak Dilakukan	5	1	0	0	6
Dalam Perencanaan	3	4	1	0	8
Dalam Penerapan/Diterapkan Sebagian	5	2	0	0	6
Diterapkan Secara Menyeluruh	1	4	0	0	6
Total	14	11	1	0	26

Skor kelengkapan yang didapatkan dari teknologi dan keamanan informasi adalah 56. Berdasarkan tabel 9 dapat diketahui jumlah pertanyaan pada tahap 1 adalah 14, kemudian pertanyaan pada tahap 2 adalah 10 dan 2 pertanyaan pada tahap ke 3 dengan batas skor minimal untuk tahap penerapan 3 yaitu 68 dan total skor yang didapat pada tahap 1 & 2 adalah 56, sehingga status pada penerapan 3 berstatus "Tidak Valid". skor kematangan tingkat II bernilai 16 dengan skor minimum yaitu 18 dan skor pencapaian bernilai 28 sehingga terdapat status kematangan "No". Untuk skor tingkat kematangan III bernilai 40 dengan nilai validitas "No" dan skor minimum bernilai 40 dan skor pencapaian bernilai 62 sehingga didapatkan status "No". Selanjutnya skor Kematangan IV bernilai 0, dengan Validitas "No", dan dengan Skor minimal yaitu 6 dan skor pencapaian 9 dengan statusnya "No".

Berdasarkan tabel 10 terdapat 6 pertanyaan pada tingkat kematangan II dan III yang tidak direspon atau "Tidak Dilakukan" masing-masing 5 pertanyaan pada tingkat kematangan II dan 1 pertanyaan pada tingkat kematangan III. Pada tahap status penerapan "Dalam Perencanaan" terdapat 8 pertanyaan yang masing-masing 3 pertanyaan pada tingkat kematangan II, 4 pertanyaan pada tingkat kematangan III dan 1 pertanyaan pada tingkat kematangan IV. sedangkan pada tahap status penerapan "Dalam

Penerapan/Diterapkan Sebagian" terdapat 6 pertanyaan dengan 4 pertanyaan pada tingkat kematangan II, 2 pertanyaan pada tingkat kematangan III. pada status penerapan "Diterapkan Secara Menyeluruh" terdapat 6 pertanyaan, 2 pertanyaan pada tingkat kematangan II dan 4 pertanyaan pada tingkat kematangan III. Berdasarkan dari hasi tersebut dapat diketahui bahwa kondisi pada area teknologi dan keamanan informasi saat ini layanan TIK yang menggunakan internet pada instansi belum dilindungi secara berlapis atau masih dalam tahap perencanaan, belum tersedianya konfigurasi standar untuk keamanan sistem, instansi juga tidak memiliki rekaman analisa yang mengkonfirmasi bahwa antivirus/*malware* telah dimutakhirkan dan juga beberapa masalah terkait keamanan informasi lainnya.

Berikut merupakan tingkat kelayakan untuk ke-5 aspek berdasarkan tingkat validitas nilai.

Tabel 11 tingkat kelayakan untuk ke-5 aspek berdasarkan tingkat validitas nilai.

	Tata Kelola	**Pengelolaan Risiko**	**Kerangka Kerja**	**Pengelolaan Aset**	**Aspek Teknologi**
Tingkat II					
Status Tingkat III	I+	No	I+	I+	No
Validitas	No	No	No	No	No
Status Tingkat IV	No	No	No	No	No
Validitas	No	No	No	No	No
Status Tingkat V	No	No	No	No	No
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	**I+**	**I**	**I+**	**I+**	**I**
	2	**1**	**2**	**2**	**1**

Berdasarkan Tabel 11 dapat di ketahui bahwa status kematangan pada lima area Keamanan Informasi dapat dilihat bahwa untuk aspek tata kelola dan kerangka kerja berada pada tingkat II dengan nilai "I+", pada pengelolaan risiko dan Aspek teknologi pada tingkat II dengan status nilai "No", kemudian pada aspek pengelolaan aset status pada tingkat II bernilai "I+". Pada tingkat kematangan III, IV dan V pada keseluruhan aspek mulai dari Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset dan Aspek Teknologi memiliki validitas "No". Dalam hal ini dapat dilihat bahwa dari ke-lima aspek belum ada yang mencapai ambang batas minimum level kematangan sedangkan ambang batas minimum kesiapan sertifikasi adalah berada pada tingkat "III+".

Tabel 12 Trafik jaringan IBISA

Tgl Pengujian	**Jam kerja**			**Bukan jam Kerja**		
	Min	**Max**	**Avg**	**Min**	**Max**	**Avg**
7/04/2022	86,0	801.0	278.82	76.0	1351.0	286.11
8/04/2022	90,0	3217.0	392.77	80.0	1181.0	250.62
9/04/2022	84.0	1242.0	288.93	80.0	1901.0	282.77
10/04/2022	87.0	1247.0	288.01	67.0	2412.0	275.3
11/04/2022	66.0	830.0	275.16	76.0	1222.0	219.3
12/04/2022	79.0	689.0	220.63	75.0	6139.0	335.44
13/04/2022	67.0	6055.0	734.07	87.0	3337.0	296.66

Pembangunan jaringan dari sistem pendeteksi ini dimulai dengan Pemodelan kondisi normal dan jaringan yang diamati, Kemudian lanjutkan sebagai pengecualian. Kelebihan dari sistem deteksi berbasis anomali adalah tidak memerlukan pengetahuan *malware* yang mendalam dan dapat mendeteksi serangan dalam bentuk *malware* baru. Sedangkan kekurangan dari sistem deteksi berbasis anomali adalah tidak dapat mengetahui tipe serangan apa yang menyerang pada jaringan dan tingginya tingkat *false positive.*

ManageEngine OpManager memiliki kemampuan untuk melakukan pengamatan trafik jaringan. Pada penelitian ini langkah yang akan dilakukan selanjutnya adalah melakukan monitoring dan pengambilan data pada sistem jaringan IBISA Purworejo. Monitor serta pengambilan data pada jaringan IBISA Purworejo dilakukan selama satu minggu dimulai dari tanggal 7 April 2022 sampai 13 April 2022, pengamatan dilakukan pada jam kerja pada pukul 07.00 WIB sampai 17.00 WIB dan pada non jam kerja pada pukul 17.00 WIB sampai 07.00 WIB.

Adapun tujuan dari pengambilan data yaitu untuk menganalisa kondisi keamanan dan jaringan, dengan cara memonitoring perubahan trafik pada jaringan. Dari data pengamatan telah didapatkan bahwa kondisi trafik jaringan pada saat jam kerja lebih besar dibandingkan dengan non jam kerja.

Gambar 6 Perbandingan Indeks KAMI Pre-Assesment dan Post-Assesment jaringan IBISA Purworejo

Berdasarkan pada gambar 6 dapat diketahui bahwa kenaikan dari nilai Indeks Keamanan Informasi (KAMI) terdapat pada beberapa aspek diantaranya : aspek tata kelola, pengelolaan aset informasi dan teknologi keananan informasi yang dapat ditunjukkan pada tabel dibawah ini.

Tabel 13 Pre-Aseesment Aspek "Tata Kelola Keamanan Informasi"

No	Evaluasi Tata Kelola Keamanan Informasi	Status	Poin
1	Apakah Jaringan IBISA Purworejo sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhan nya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2	Apakah Jaringan IBISA Purworejo menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Perencanaan	2
3	Apakah Jaringan IBISA Purworejo sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Tidak Dilakukan	0
4	Apakah kondisi dan permasalahan keamanan informasi di IBISA Purworejo menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan Anda?	Dalam perencanaan	2
5	Apakah Jaringan IBISA Purworejo anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauan nya dan eskalasi pelaporan nya?	Tidak Dilakukan	0
6	Apakah Jaringan IBISA Purworejo Anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0
7	Apakah IBISA Purworejo sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaian nya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Tidak Dilakukan	0

Tabel 14 Post-Aseesment Aspek "Tata Kelola Keamanan Informasi"

No	Evaluasi Tata Kelola Keamanan Informasi	Status	Poin
1	Apakah Jaringan IBISA Purworejo sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhan nya bagi semua pihak yang terkait?	Diterapkan Secara Menyeluruh	3
2	Apakah Jaringan IBISA Purworejo menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	6
3	Apakah Jaringan IBISA Purworejo sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Diterapkan Secara Menyeluruh	6
4	Apakah kondisi dan permasalahan keamanan informasi di IBISA Purworejo menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Dalam Penerapan/Diterapkan sebagian	4
5	Apakah Jaringan IBISA Purworejo anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauan nya dan eskalasi pelaporan nya?	Dalam Penerapan/Diterapkan sebagian	6
6	Apakah Jaringan IBISA Purworejo Anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Diterapkan Secara Menyeluruh	9
7	Apakah IBISA Purworejo sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaian nya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Dalam Penerapan/Diterapkan sebagian	6

Tabel 15 Pre-Aseesment Aspek "Pengelolaan Aset Informasi"

No	Evaluasi Pengelolaan Aset Informasi	Status	Poin
1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di IBISA Purworejo	Dalam Penerapan / Diterapkan Sebagian	2

2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Tidak Dilakukan	0
3	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Perencanaan	2
4	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	4

Tabel 16 Post-Aseesment Aspek "Pengelolaan Aset Informasi"

No	Evaluasi Pengelolaan Aset Informasi	Status	Poin
1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di IBISA Purworejo	Diterapkan Secara Menyeluruh	3
2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Perencanaan	2
3	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian	4
4	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Diterapkan Secara Menyeluruh	6

Tabel 17 Pre-Assessment Aspek "Teknologi dan Keamanan Informasi"

No	Evaluasi Teknologi dan Keamanan Informasi	Status	Poin
1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
2	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Tidak Dilakukan	0
3	Apakah IBISA Purworejo secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Tidak Dilakukan	0
4	Apakah jaringan komunikasi di segmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Tidak Dilakukan	0
5	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Tidak Dilakukan	0
6	Apakah Jaringan IBISA Purworejo menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar *platform* teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	Tidak Dilakukan	0
7	Apakah Jaringan IBISA Purworejo melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Perencanaan	2
8	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Perencanaan	2

9	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Perencanaan	2

Tabel 18 Post-Assessment Aspek "Teknologi dan Keamanan Informasi"

No	Evaluasi Teknologi dan Keamanan Informasi	Status	Poin
1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	3
2	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2
3	Apakah IBISA Purworejo secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Perencanaan	1
4	Apakah jaringan komunikasi di segmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Dalam Perencanaan	1
5	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dalam Perencanaan	1
6	Apakah Jaringan IBISA Purworejo menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar *platform* teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	Tidak Dilakukan	6
7	Apakah Jaringan IBISA Purworejo melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Perencanaan	6
8	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Perencanaan	4
9	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	4

Hasil dari perbandingan diatas menunjukkan bahwa *ManageEngine OpMananager* dapat membantu menaikkan nilai atau poin untuk aspek Teknologi yang ada pada Indeks Keamanan Informasi (KAMI) akan tetapi tidak berpengaruh pada aspek-aspek lainnya. Terlihat bahwa nilai dari Indeks Kami jaringan IBISA Purworejo adalah 292 dari yang sebelumnya yaitu 235 poin, hal tersebut menunjukkan bahwa tingkat kematangan Keamanan informasi yang sebelumnya ketika *Pre-assessment* berada pada level I s/d I+ kini berada pada level I s/d II ketika *Post-assessment* dilakukan. Akan tetapi dari aspek Tata kelola menunjukkan adanya perubahan nilai dari 35 menjadi 69, Pengelolaan Aset Informasi menunjukkan adanya perubahan nilai dari 76 menjadi 86 dan Aspek Teknologi Keamanan Informasi menunjukkan adanya perubahan nilai dari 56 menjadi 72. Hal tersebut juga dijelaskan pada Gambar 6 dengan memonitor kondisi jaringan IBISA Purworejo bahwasanya dapat diperoleh tujuan penelitian ini, yaitu memonitoring dan mengetahui lebih detail permasalahan yang ada pada jaringan IBISA Purworejo sehingga dapat diketahui pola solusi yang dapat digunakan sehingga dapat memaksimalkan kinerja jaringan komputer yang ada dengan lebih efektif dan efesien sebagaimana fungsinya.

5. KESIMPULAN DAN SARAN

Tingkat Kematangan dan integritas keamanan informasi jaringan IBISA Purworejo masih rendah. alasan rendah Integritas dan tingkat kematangan keamanan informasi ini adalah Jaringan IBISA Purworejo belum sepenuhnya melaksanakan Persyaratan keamanan informasi atau masih dalam perencanaan. pada penggunaan teknologi *ManageEngine OpMananager* terbukti dapat

meningkatkan nilai dari Indeks Keamanan Informasi (KAMI) pada jaringan IBISA Purworejo pada berbagai aspek. Peningkatan nilai-nilai pada berbagai aspek tidak lepas dari peranan penggunaan teknologi *ManageEngine OpMananager* dalam menganalisa yang menjadi kelemahan dan perubahan konfigurasi aset informasi pada jaringan IBISA Purworejo. *ManageEngine OpMananager* juga dapat melakukan monitoring serta melakukan proses Analisa terhadap aset dan jaringan IBISA Purworejo secara sistematis. Hal ini mengartikan bahwa keamanan informasi pada jaringan IBISA Purworejo tidak layak dan perlu banyak perbaikan. Sedangkan tingkat kematangan untuk setiap area keamanan informasi berada pada level I sampai dengan II. Kemudian sebagai kebijakan standar ISO/IEC 27001:2018, Tanggal kedaluwarsa yang diharapkan untuk ambang batas minimum Kesiapan sertifikasi adalah berada pada Level atau tingkat kematangan III+.

Rekomendasi ataupun saran untuk penelitian selanjutnya adalah Membangun kesadaran di antara staf PUSDATIN IBISA Purworejo berkaitan dengan keamanan informasi. staf terlebih dahulu menyadari pentingnya perlindungan keamanan informasi dari Semua aspek yang terkait dengan keamanan informasi dalam Mendukung kinerja jaringan. indeks KAMI paling tidak digunakan satu tahun sekali sebagai alat Tinjauan terhadap kesiapan keamanan informasi serta Mengevaluasi keberhasilan perbaikan yang telah dilaksanakan dengan mencapai tingkat kelengkapan atau kematangan tertentu.

DAFTAR PUSTAKA

ADI REYNALDO, SENGKEY RIZAL, P. (2020) ‘Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI’, *Jurnal Teknik …*, pp. 189–198. Available at: https://ejournal.unsrat.ac.id/index.php/informatika/article/view/31597.

ANGGA JUANSYAH, BAGUS PRATAMA, I. D. (2018) ‘Analisis dan implementasi open source security information managament (ossim) pada keamanan jaringan komputer pt. satria antaran prima palembang’. Available at: http://library.palcomtech.com/pdf/5621.pdf.

ARFANUDIN, C. *ET AL.* (2019) ‘Analisis Serangan Router Dengan Security Information and Event Management (Siem) Dan Implikasinya Pada Indeks Analysis of Router Attack With Security Information and Event Management and Implications (Siem) in Information Security’, 2(1), pp. 1–7.

DARWIS, D. AND SOLEHAH, N. Y. (2021) ‘PENERAPAN FRAMEWORK COBIT 5 UNTUK AUDIT TATA KELOLA KEAMANAN INFORMASI PADA KANTOR WILAYAH KEMENTERIAN’, 1(2), pp. 38–45.

DEWANTARA, R. AND SUGIANTORO, B. (2021) ‘Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)’, *Jurnal Teknologi Informasi dan Ilmu Komputer*, 8(6), p. 1137. doi: 10.25126/jtiik.2021863123.

HERMAWAN, W. (2019) ‘Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE)’, *Jurnal Telekomunikasi dan Komputer*, 9(2), p. 129. doi: 10.22441/incomtech.v9i2.6474.

KAMAL, M. R. AND SETIAWAN, M. A. (2021) ‘Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII’, *Automata*, (4).

KORNELIA, A. AND IRAWAN, D. (2021) ‘Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1’, *Jurnal Pengembangan Sistem Informasi dan Informatika*, 2(2), pp. 78–86. doi: 10.47747/jpsii.v2i2.548.

KRISTANTO, T. *ET AL.* (2019) ‘Analisis Manajemen Keamanan Informasi Menggunakan Standard ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ’, *JISA(Jurnal Informatika dan Sains)*, 2(2), pp. 30–33. doi: 10.31326/jisa.v2i2.497.

LENAWATI, M., WINARNO, W. W. AND AMBOROWATI, A. (2017) ‘Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5’, *Sentra Penelitian Engineering dan Edukasi*, 9(1), pp. 44–49. Available at: http://speed.web.id/jurnal/index.php/speed/article/view/220.

NOFRY ARMAN, WIDHY HAYUHARDHIKA NUGRAHA PUTRA, A. R. (2019) ‘3. Tampilan Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI).pdf’.

PAMUNGKAS, W. C. AND SAPUTRA, F. T. (2020) ‘Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013’, *Jurnal Sistem Komputer dan Informatika (JSON)*, 1(2), p. 101. doi: 10.30865/json.v1i2.1924.

WIJATMOKO, T. E. (2020) ‘Evaluasi Keamanan

Informasi Menggunakan Indeks Keamanan Informasi (Kami) Pada Kantor Wilayah Kementerian Hukum Dan Ham Diy', *Cyber Security dan Forensik Digital*, 3(1), pp. 1–6. doi: 10.14421/csecurity.2020.3.1.1951.

WIJAYA, Y. D. (2021) 'Evaluasi Kemananan Sistem Informasi Pasdeal Berdasarkan Indeks Keamanan Informasi (Kami) Iso/Iec 27001:2013', *Jurnal Sistem Informasi dan Informatika (Simika)*, 4(2), pp. 115–130. doi: 10.47080/simika.v4i2.1178.

YAUMA DZIKRI IMANY, WIDHY HAYUHARDIKA NUGRAHA PUTRA, ADMAJA D. H. (2019) 'Tampilan Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia).pdf'.

YUNELLA, DWI HERLAMBANG, NUGRAHA PUTRA, M. (2019) 'Tampilan Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI.pdf'.