**Jurnal Mobile and Forensics (MF)**
Vol. 1, No. 2, September 2019, pp. 53-62
P-ISSN: 2656-6257, E-ISSN: 2714-6685, DOI: https://doi.org/10.12928/mf.v1i2.1001

# EVALUASI TINGKAT KESIAPAN KEAMANAN INFORMASI PADA LEMBAGA PENDIDIKAN MENGGUNAKAN INDEKS KAMI 4.0

**[1,*]Pramudhita Ferdiansyah, [2]Subektiningsih, [3]Rini Indrayani**
[1,2,3]Teknik Komputer, Universitas Amikom Yogyakarta, Jalan Ringroad Utara, Yogyakarta, Indonesia
e-mail: ferdian@amikom.ac.id, subektiningsih@amikom.ac.id, rini.i@amikom.ac.id
[*)] corresponding author

**Abstrak**

Evaluasi keamanan sistem informasi sangat diperlukan bagi sebuah organisasi, instansi, maupun perusahaan guna mencegah kebocoran data ataupun kerusakan sistem informasi. Penelitian ini dilakukan di sektor pendidikan pada lembaga UPTD XYZ di bawah kuasa Dinas Pendidikan Provinsi Daerah Istimewa Yogyakarta. Evaluasi kematangan dan tata kelola keamanan informasi diterapkan berdasarkan standar ISO/IEC 27001:2017 dengan menggunakan indeks keamanan informasi KAMI versi 4.0. Metode pengumpulan data dilakukan dengan cara observasi langsung dan interview terhadap penanggungjawab sistem informasi. Hasil yang didapatkan dari evaluasi untuk kebutuhan sistem elektronik sebesar 20, sedangkan tingkat kelengkapan informasi mendapatkan skor 245. Dari hasil tersebut dapat disimpulkan bahwa tingkat keamanan informasi masih sangat rendah dan diperlukan perbaikan sistem keamanan informasi dengan bekerja sama dengan pengembang keamanan informasi dari pihak ketiga.

*Information system security evaluation is indispensable for an organization, agency, or company to prevent data leakage or damage to information systems. This research was conducted in the education sector at the UPTD XYZ institution under the authority of the Yogyakarta Provincial Education Office. Information security maturity and governance evaluation is implemented based on ISO / IEC 27001: 2017 standard by using the WE information security index version 4.0. The data collection method is done by direct observation and interviews with the person in charge of the information system. The results obtained from the evaluation for electronic system requirements were 20, while the level of completeness of information got a score of 245. From these results it can be concluded that the level of information security is still very low and it is necessary to improve information security systems in collaboration with information security developers from third parties.*

**Kata Kunci:** ISO/IEC 27001:2013, Indeks KAMI, Evaluasi Keamanan, Teknologi Informasi

## PENDAHULUAN

Pengelolaan teknologi informasi dan komunikasi yang terstruktur sudah menjadi kebutuhan setiap penyelenggara layanan publik berbasis internet maupun intranet secara online dan offline. Dalam perkembangan teknologi informasi yang semakin pesat sebanding dengan tingkat resiko terhadap teknologi informasi. Sehingga pengelolaan teknologi informasi dan komunikasi diharapkan memiliki tingkat keamanan yang baik terhadap sistem informasi. Keamanan informasi merupakan mekanisme yang berkaitan dengan kerahasiaan, integritas, keutuhan data, dan ketersediaan aset informasi berupa pengolahan, penyimpanan, dan transmisi [1]. Keamanan informasi merupakan aspek yang penting didalam tata kelola teknologi informasi demi terbebasnya dari aktivitas dari pihak yang tidak memiliki kewenangan terhadap sistem. Aktivitas tersebut dapat berupa pencurian data, perubahan data,

*Received December 9, 2018; Revised January 3, 2019; Accepted February 17, 2019*

bahkan penghapusan data dari sistem tanpa diketahui oleh pihak yang berwenang. Untuk itu perlu adanya audit sistem keamanan sistem yang terstruktur.

Audit keamanan sistem informasi merupakan strategi yang diterapkan untuk mengurangi potensi resiko kerentanan suatu sistem informasi terhadap pihak yang tidak bertanggung jawab. Standar yang digunakan untuk melakukan audit keamanan sistem yaitu dengan menggunakan indeks keamanan sistem (KAMI) berdasarkan ISO/IEC 27001:2013, dimana dalam indeks tersebut dapat digunakan untuk melakukan analisa dan evaluasi tingkat kesiapan atau kematangan sistem informasi pada sebuah instansi maupun organisasi dengan kriteria SNI ISO/IEC 27001:2013 [2]. Indeks KAMI berdasarkan ISO/IEC 27001:2013 merupakan alat atau aplikasi yang fleksibel digunakan untuk menganalisa tingkat kematangan suatu organisasi, instansi bahkan perusahaan besar berupa gambaran kondisi kesiapan kelengkapan kerangka kerja keamanan teknologi informasi yang dapat diusulkan kepada pimpinan instansi, organisasi, dan atau perusahaan [3]. Ruang lingkup evaluasi indeks keamanan informasi KAMI meliputi tata kelola, pengelolaan resiko, kerangka kerja, pengelolaan aset, dan aspek teknologi [4].

ISO 27001 merupakan standar keamanan sistem informasi yang dipublikasikan dan diterbitkan oleh *The International Organization for Standardizilation* dan *The Electrotehnical Commission* ditujukan untuk membantu suatu organisasi, institusi, dan perusahaan dalam mengamankan informasi yang menjabarkan prasyarat bagi penerapan, penetapan, pelaksanaan, pemeliharaan, pemantauan, serta peninjauan ulang sistem manajemen keamanan informasi atau SMKI [5].

Berbagai penelitian mengenai keamanan informasi telah dilakukan, salah satunya penelitian dengan berjudul Perencanaan dan Implementasi *Information Security Management System* Menggunakan *Framework* ISO/IEC 27001 [6]. Penelitian tersebut melakukan analisis deskriptif kuantitatif dimana peneliti melakukan analisis dengan mendeskripsikan tingkat kematangan keamanan informasi pada PT. Bank Pembangunan Daerah Sumatera Barat. Tujuan penelitian tersebut adalah melakukan evaluasi keaman informasi untuk tindak lanjut perencanaan dan implementasi sistem manajemen keamanan informasi menggunakan *framefork* ISO 27001.

Penelitian lainnya yang membahas keamanan informasi dilakukan oleh [7] dengan melakukan identifikasi, menilai dan memitigasi resiko teknologi informasi yang dikelola oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung menggunakan metode OCTAVE. Penelitian tersebut menghasilkan identifikasi resiko terhadap teknologi informasi dan memberikan rekomendasi mitigasi ISO 27001 kepada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

Penelitian [8] melakukan analisa manajemen resiko pada salah satu Kantor Pelayanan Pajak Pratama. Kantor Pelayanan Pajak Pratama merupakan salah satu lembaga pemerintahan yang bergerak di bidang keuangan sehingga memiliki banyak data elektronik, sehingga membutuhkan pengamanan untuk mencegah pencurian data. Metode yang dilakukan adalah pengumpulan data melalui identifikasi aset, ancaman, dan dampak ancaman terhadap aset. Hasil dari penelitian tersebut adalah seubah rekomendasi pengamanan aset berdasarkan tingkat prioritas tertinggi.

Berdasarkan hasil tinjauan pustaka, penelitian mengenai evaluasi keamanan informasi menggunakan indeks KAMI versi 4.0 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN) masih terbatas jumlahnya. Indeks KAMI versi 4.0 merupakan penyempurnaan dari versi sebelumnya. Versi terbaru ini memuat evaluasi keamann informasi dengan berbagai kategori dengan tambahan berupa suplemen sebagai

penunjang keamanan informasi terkait pihak ketiga [9]. Oleh karena itu penelitian ini menggunakan indeks KAMI versi 4.0 untuk evaluasi keaman informasi pada lembaga pemerintahan UPTD XYZ. Tujuan penelitan ini adalah untuk mendapatkan informasi terkait tingkat kematangan dan kesiapan keamanan informasi.

UPTD XYZ merupakan instansi milik pemerintah provinsi Daerah Istimewa Yogyakarta yang bergerak dibidang pelayanan teknis atau Unit Pelayanan Teknis Daerah (UPTD). Pelayanan yang diberikan berupa diklat atau pelatihan dengan ditunjang fasilitas meliputi bengkel, laboratorium komputer, asrama serta sarana olahraga. Diklat tersebut dapat diikuti oleh siswa sekolah kejuruan (SMK), mahasiswa, guru, dan kepala bengkel atau kepala laboratorium. Dalam pengelolaan diklat pada UPTD XYZ langsung diatur dan dilindungi oleh peraturan mentri ketenagakerjaan Republik Indonesia. Dengan banyaknya data informasi yang terdapat pada UPTD XYZ dalam menangani pelayanan publik, maka diperlukan evaluasi keamanan informasi untuk mengukur tingkat kesiapan kematangan dan kelengkapan keamanan informasi pada UPTD XYZ. Informasi yang terdapat pada UPTD XYZ dapat berupa *soft file,* website, email dan berbagai bentuk lain yang bersifat informatif. Hasil dari evaluasi yang dilakukan berupa data yang dapat memberikan usulan perbaikan keamanan sistem informasi kepada kepala UPTD XYZ.

## METODE PENELITIAN

Tahapan penelitian dalam melakukan evaluasi keamanan sistem dan teknologi informasi dengan menggunakan indeks keamanan informasi berdasarkan ISO/IEC 27001:2013. Penelitian diawali dengan melakukan identifikasi masalahdan studi literature terkait dengan evaluasi keamanan sistem dan keamanan informasi. Langkah berikutnya yaitu studi lapangan untuk pengumpulan data dengan melakukan *interview* kepada penanggung jawab *IT* pada objek penelitian serta mengobservasi dan *review* dokumen. Dokumen-dokumen hasil *review* tersebut dapat diproses untuk diberikan penilaian sesuai dengan indeks kemanan informasi KAMI berdasarkan ISO/IEC 27001:2013. Hasil dari penilaian melalui indeks kemanan informasi tersebut dapat dianalisa dan dikaji sehingga dapat dijadikan dasar atau dasar usulan dan saran perbaikan sistem keamanan informasi pada UPTD XYZ berdasarkan ISO/IEC 27001. Proses alur penelitian ditunjukkan pada Gambar 1.

### Pengumpulan Data

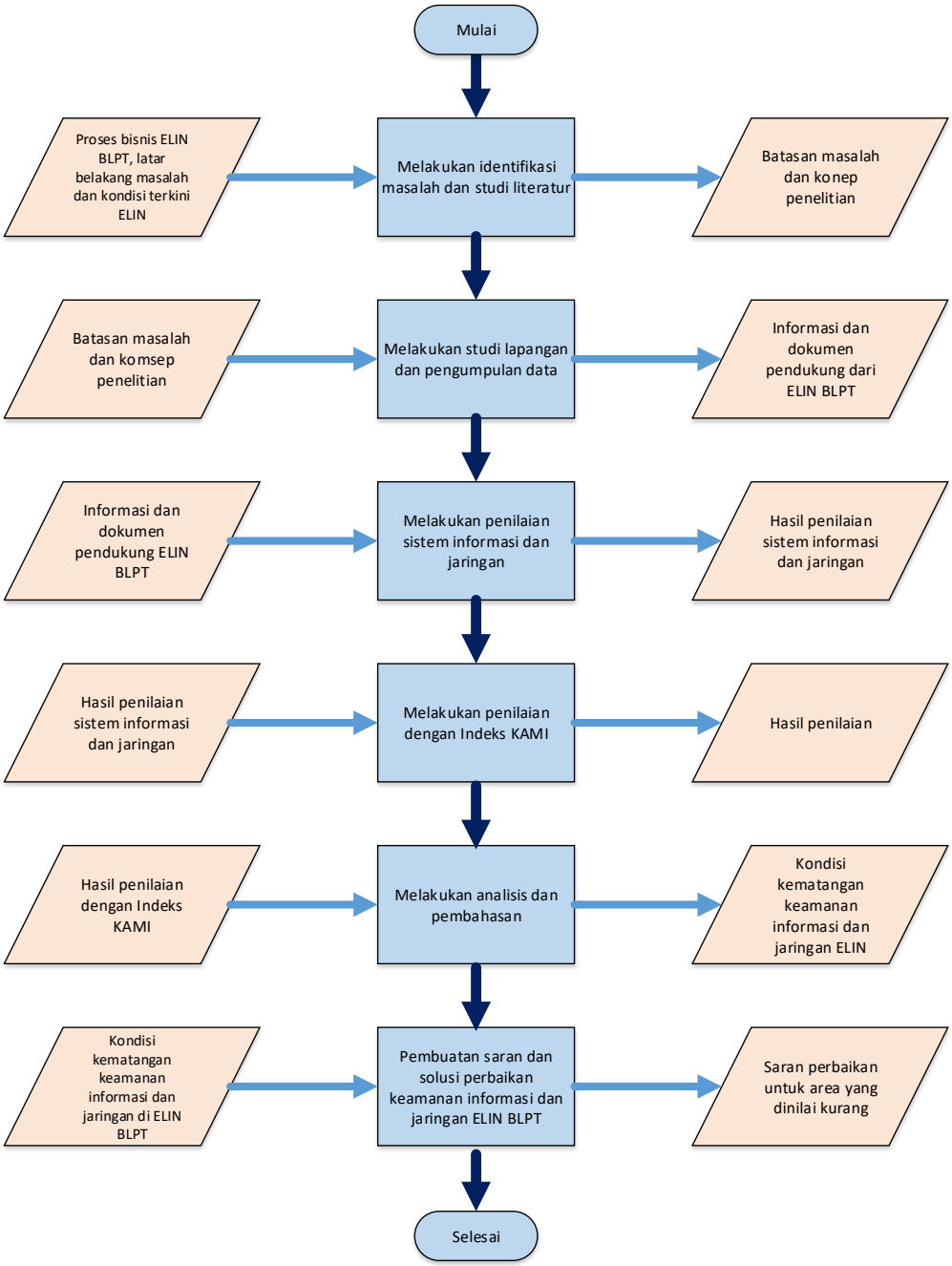
Teknik pengumpulan data yang digunakan pada penelitia ini yaitu dengan pendekatan kuantitatif, yaitu :

1. Metode observasi
   Meninjau langsung ke pusat layanan informasi pada UPTD XYZ untuk melakukan pengamatan, pencatatan teknologi informasi yang sudah ada.
2. Metode wawancara

Melakukan *interview* terhadap penanggung jawab layanan informasi elektronik di UPTD XYZ dengan mengajukan pertanyaan sesuai dengan indeks keamanan informasi KAMI.

### Analisis data

Sebelum melakukan proses penilaian, perlu dilakukan klasifikasi data elektronik dengan tujuan untuk mengelompokkan kedalam ukuran tertentu. Korelasi kategori sistem elektronik dengan status kesiapan yang mengacu pada indeks keamanan informasi KAMI didefinisikan melalui Tabel 1 [9].




Gambar 1. Skema metode penelitian

Tabel 1. Tabel kategori sistem elektronik

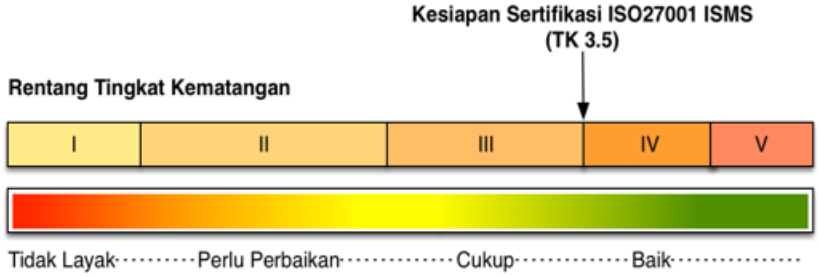
| Rendah | | Skor akhir | | Status kesiapan |
|---|---|---|---|---|
| 10 | 15 | 0 | 174 | Tidak layak |
| | | 175 | 312 | Pemenuhan Kerangka Kerja Dasar |
| | | 313 | 535 | Cukup Baik |
| | | 536 | 645 | Baik |
| Tinggi | | Skor akhir | | Status Kesiapan |
| 16 | 34 | 0 | 272 | Tidak Layak |
| | | 273 | 455 | Pemenuhan Keranka Kerja Dasar |

| | | | | |
|---|---|---|---|---|
| | | 456 | 583 | Cukup Baik |
| | | 584 | 645 | Baik |
| Strategis | | Skor Akhir | | Status Kesiapan |
| 35 | 50 | 0 | 333 | Tidak Layak |
| | | 334 | 535 | Pemenuhan Keranka Kerja Dasar |
| | | 536 | 609 | Cukup Baik |
| | | 610 | 645 | Baik |

Pengelompokan data berikutnya didasarkan pada tingkat kematangan penanganan keamanan dengan kategorisasi yang mengacu pada tingkat kematangan yang digunakan oleh COBIT atau CMMI [9]. Tingkat kematangan pada indeks KAMI versi 4 didefinisikan dalam 5 kategori, yaitu :

- Tingkat I - Kondisi awal
- Tingkat II - Penerapan kerangka kerja dasar
- Tingkat III - Terdefinisi dan Konsisten
- Tingkat IV - Terkelola dan Terukur
- Tingkat V - Optimal

Tingkat kematangan tersebut masih ditambah 4 kategori sebagiai uraian yang lebih detail, yaitu tingkat I+, II+, III+, dan IV+. Standarisasi keamanan informasi yang mengacu pada ISO/IEC 27001:2013 batas minimum tingkat kematangan kesiapan sertifikasi terletak pada Tingkat III+. Evaluasi dengan menggunakan indeks keamanan informasi KAMI versi 4 menghasilkan tingkat kematangan yang ditunjukkan melalui Gambar 2 :




Gambar 2. Tingkat kematangan kesiapan sertifikasi ISO 27001

Untuk mendapatan tingkat kematangan, responden diberikan pertanyaan-pertanyaan yang terbagi menjadi tujuh kelompok. Setiap status pengamanan memiliki skor sesuai dengan tingkat kematangan. Tabel 2 berikut merupakan rangkuman jawaban penilaian dengan membentuk matriks antara status pengamanan dan kategori.

Tabel 2. Skor tingkat kematangan [9]

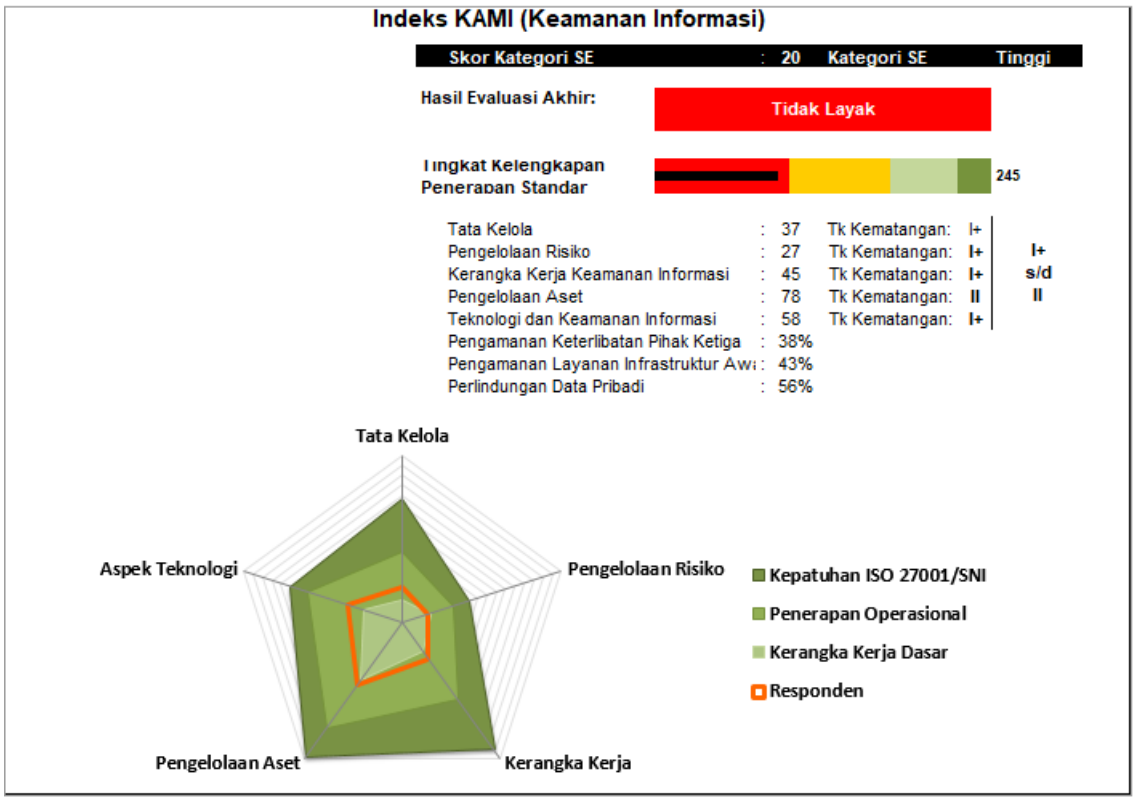
| Status pengamanan | Tingkat kematangan | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Tidak dilakukan | 0 | 0 | 0 |
| Dalam perencanaan | 1 | 2 | 3 |
| Dalam penerapan atau diterapkan sebagian | 2 | 4 | 6 |
| Diterapkan secara menyuluruh | 3 | 6 | 9 |

Pengisian pertanyaan pada kategori “3” di tingkat kematangan dapat memberikan hasil skor apabila semua pertanyaan pada kategori “1” dan “2” terisi dengan status minimal dalam penerapan atau diterapkan sebagian.

Dengan semakin tingginya tingkat ketergantungan sebuah instansi terhadap peran sistem elektronik, maka akan mengakibatkan bertambah banyak bentuk penerapan pengamanan informasi [10].

## HASIL DAN PEMBAHASAN

Hasil evaluasi tingkat kematangan keamanan informasi pada UPTD XYZ dikelompokkan menjadi 7 kategori sesuai dengan indeks keamanan informasi KAMI versi 4 [4] ditunjukkan pada Gambar 3.




Gambar 3. *Dashboard* evaluasi indeks KAMI versi 4

### 1. Kategori sistem elektronik

Kategori sistem elektronik merupakan kategori pertama pada dokumen evaluasi indeks KAMI 4.0. Kategori ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan. Terdapat tiga kategori hasil evaluasi yaitu rendah, tinggi, dan strategis. Pada kategori ini UPTD XYZ mendapat skor 20 predikat tinggi**.** Hasil ini didapatkan dari 10 pertanyaan indikator dengan nilai maksimum 50. Pada kategori ini hanya poin bagian dampak dari kegagalan sistem elektronik yang memiliki nilai tertinggi.

Hasil evaluasi pada sistem elektronik dengan predikat tinggi yaitu penggunaan sistem elektronik di UPTD XYZ memiliki kecenderungan kebutuhan yang tinggi terhadap sistem elektronik.

### 2. Tata Kelola Keamanan Informasi

Pada kategori ini merupakan evaluasi tata kelola keamanan informasi yang dapat mempengaruhi data di UPTD XYZ. Maka dari itu evaluasi pada kategori ini lebih menekankan pada rencana yang dipersiapkan untuk menanggulangi resiko terhadap ancaman keamanan informasi. Batas skor maskismum kategori tata kelola keamanan

informasi pada indeks KAMI yaitu 126. Hasil evaluasi pada kategori informasi yang ditunjukkan pada Tabel 3 didapatkan skor 37, sehingga pada kategori ini termasuk dalam tingkat kematangan I+.

Tabel 3. Hasil evaluasi tata kelola keamanan informasi

| Status pengamanan | Tingkat kematangan | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | Skor | 2 | Skor | 3 | Skor | Total |
| Tidak dilakukan | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Dalam perencanaan | 1 | 0 | 2 | 12 | 3 | 0 | 12 |
| Dalam penerapan atau diterapkan sebagian | 2 | 14 | 4 | 8 | 6 | 0 | 22 |
| Diterapkan secara menyuluruh | 3 | 3 | 6 | 0 | 9 | 0 | 3 |
| Total nilai evaluasi tata kelola keamanan informasi | | | | | | | 37 |

### 3. Pengelolaan Resiko Keamanan Informasi

Pada tahap ketiga dilakukan evaluasi terhadap pengelolaan resiko keamanan informasi yang mencakup berbagai resiko yang dapat tejadi dan berpengaruh terhadap data informasi pada UPTD XYZ. Terdapat 4 kategori dalam evaluasi ini, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan/ penerapan sebagian, dan diterapkan secara menyulurh. Masing-masing kategori tersebut memilki skor 0, 1, 2, 3 , 4, 6 yang terbagi sesuai dengan tingkat kematangan yang telah ditentukan oleh indeks kemanan informasi KAMI [4]. Hasil evaluasi pada UPTD XYZ mendapatkan skor total 27, sehingga tergolong dalam tingkat kematangan I+. Hasil pengukuran evaluasi pengelolaan resiko keamanan informasi ditampilkan pada Tabel 4.

Tabel 4. Pengukuran evaluasi resiko keamanan informasi

| Status pengamanan | Tingkat kematangan | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | Skor | 2 | Skor | 3 | Skor | Total |
| Tidak dilakukan | 0 | 0 | 0 | 0 | 0 | 0 | |
| Dalam perencanaan | 1 | 3 | 2 | 6 | 3 | 0 | 9 |
| Dalam penerapan atau diterapkan sebagian | 2 | 14 | 4 | 4 | 6 | 0 | 18 |
| Diterapkan secara menyuluruh | 3 | 0 | 6 | 0 | 9 | 0 | 0 |
| Total nilai evaluasi tata kelola keamanan informasi | | | | | | | 27 |

### 4. Kerangka Kerja Pengelolaan Keamanan Informasi

Tahapan berikutnya yaitu evaluasi terhadap kerangkan pengelolaan keamanan informasi yang menekankan pada persiapan dan kelengkapan kerangka kerja. Pada tahapan ini merupakan tahapan realisasi dan evaluasi dari tahap sebelumnya. Terdapat 29 pertanyaan yang memiliki empat kompnen penilaian, yaitu tidak dilakukan, dalam perencanaan, dalam penerapan atau diterapkan sebagian, dan diterapkan secara menyeluruh dan bagi menjadi IV kategori kesiapan dan skor tertinggi sebesar 159. Pengukuran kerangka kerja pengelolaan keamanan informasi ditunjukkan oleh Table 5.

Tabel 5. Evaluasi kerangka kerja

| Status pengamanan | Tingkat kematangan | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | Skor | 2 | Skor | 3 | Skor | Total |
| Tidak dilakukan | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Dalam perencanaan | 1 | 7 | 2 | 12 | 3 | 0 | 19 |
| Dalam penerapan atau diterapkan sebagian | 2 | 10 | 4 | 16 | 6 | 0 | 26 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Diterapkan secara menyuluruh | 3 | 0 | 6 | 0 | 9 | 0 | 0 |
| Total nilai evaluasi tata kelola keamanan informasi | | | | | | | 45 |

Hasil dari evaluasi pada UPTD XYZ pada tahapan ini mendapatkan skor 45 yang tergolong dalam tingkat kematangan I+ menurut indeks kemanan informasi KAMI versi 4 [9]. Skor tersebut didapatkan karena pada evaluasi tahap ini masih banyak komponen yang memiliki status dalam perencanaan.

**5. Pengelolaan Aset Informasi**

Pada tahap ini dilakukan evaluasi kelengkapan pengamanan aset informasi, ermasuk keseluruhan siklus penggunaan aset yang digunakan tersebut [9]. Evaluasi pengelolaan aset informasi beberapa bagian memiliki pertanyaan mengenai aset inventaris yang telah dilaksanakan oleh UPTD XYZ, dimana aset tersebut langsung dibawah kendali dari Pemerintah Daerah. Pada Tabel 6 dapat dilihat hasil evaluasi di tahap ini diperoleh skor sebesar 78 dari total skor sebesar 168 sehingga masuk dalam kategori tingkat kematangan II yang masih tergolong rendah [9].

Tabel 6. Evaluasi pengelolaan aset informasi

| Status pengamanan | Tingkat kematangan | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | Skor | 2 | Skor | 3 | Skor | Total |
| Tidak dilakukan | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Dalam perencanaan | 1 | 5 | 2 | 14 | 3 | 0 | 19 |
| Dalam penerapan atau diterapkan sebagian | 2 | 26 | 4 | 12 | 6 | 0 | 38 |
| Diterapkan secara menyuluruh | 3 | 15 | 6 | 6 | 9 | 0 | 21 |
| Total nilai evaluasi tata kelola keamanan informasi | | | | | | | 78 |

**6. Teknologi dan Keamanan Informasi**

Evaluasi terhadap teknologi dan keamanan informasi menekankan kepada bagian kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi [9]. Beberapa elemen yang dievaluasi meliputi keamanan data pengguna informasi, jenis pengamanan, jenis sistem operasi yang digunakan pada instansi UPTD XYZ, keamanan jaringan komputer dan lain-lain yang terkait dengan mobilisasi data. Tabel 7 menunjukkan hasil evaluasi untuk teknologi dan keamanan informasi.

Tabel 7. Evaluasi teknologi dan keamanan informasi

| Status pengamanan | Tingkat kematangan | | | | | | |
|---|---|---|---|---|---|---|---|
| | 1 | Skor | 2 | Skor | 3 | Skor | Total |
| Tidak dilakukan | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Dalam perencanaan | 1 | 8 | 2 | 12 | 3 | 3 | 23 |
| Dalam penerapan atau diterapkan sebagian | 2 | 10 | 4 | 4 | 6 | 0 | 14 |
| Diterapkan secara menyuluruh | 3 | 3 | 6 | 18 | 9 | 0 | 21 |
| Total nilai evaluasi tata kelola keamanan informasi | | | | | | | 58 |

Hasil evaluasi pada tahap teknologi dan keamanan informasi pada UPTD XYZ diperoleh skor sebesar 58 dan tergolong dalam kategori I+ atau masih rendah. Skor tersebut diperoleh dari sedikitnya implementasi keamanan yang sudah diterapkan oleh UPTD XYZ.

### 7. Suplemen

Suplemen merupakan tahap tambahan yang dikembangkan oleh BSSN, yaitu dengan melibatkan pihak ketiga dalam *supply chain* layanan suatu instansi atau perusahaan menimbulkan resiko terkait keberadaan pihak ketiga tersebut [9]. Salah satu diantaranya adalah layanan infrastruktur berbasis *cloud* yang memeberikan peluang efisiensi peningkatan kinerja yang signifikan bagai instansi/ perusahaan. Pada tahap ini terdapat tiga golongan aspek pendukung penilaian, yaitu evaluasi kesiapan pengamanan pihak ketiga, pengamanan layanan infrastruktur awan, dan perlindungan data pribadi yang dinotasikan dalam persentase.

Hasil evaluasi pada tahapan suplemen diperoleh tingkat kematangan untuk pengamanan keterlebitan pihak ketiga sebesar 38%. Kemudian untuk pengamanan layanan infrastruktur awan sebesar 43% dan yang terakhir yaitu perlindungan data pribadi sebesar 56%.

## KESIMPULAN

Berdasarkan hasil evaluasi yang dilakukan terhadap tingkat kematangan keamanan informasi dengan menggunakan indeks keamanan informasi KAMI dapat disimpulkan bahwa tingkat kebutuhan dan kelengkapan perangkat elektronik mendapatkan skor hasil evaluasi sebesar 20 yang tergolong tinggi sesuai dengan model indeks KAMI dan masih berada pada level I sampai dengan level II. Sedangkan nilai hasil evaluasi tingkat kesiapan sebesar 245, sehingga UPTD XYZ tidak layak atau belum layak untuk melakukan sertifikasi keamanan sesuai dengan standar ISO/IEC 27001 karena antara penggunaan perangkat elektronik yang berkaitan dengan teknologi informasi tidak sebanding dengan tingkat keamanan yang diterapkan.

Untuk mendapatkan tingkat kelayakan dalam pemenuhan standar keamanan ISO/IEC 27001:2013 disarankan agar UPTD XYZ melakukan peningkatan pengamanan informasi baik dengan pihak internal maupun dengan pihak ketiga dan melakukan evaluasi dan pemantauan keamanan secara berkala.

## DAFTAR PUSTAKA

[1] E. Supristiowadi and Y. G. Sucahyo, "Manajemen Resiko Keamanan Informasi pada Sistem Aplikasi Keuangan Tingkat Instansi (SAKTI) Kementerian Keuangan," *Indones. Treas. Rev. J. Perbendaharaan Keuang. Negara Dan Kebijak. Publik*, vol. 3, no. 1, pp. 23–33, 2018, doi: 10.33105/itrev.v3i1.20.

[2] D. D. Prasetyowati, I. Gamayanto, S. Wibowo, and Suharnawi, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO / IEC 27001 : 2013 pada Politeknik Ilmu Pelayaran Semarang," *J. Inf. Syst.*, vol. 4, no. 1, pp. 65–75, 2019.

[3] R. Hidayat, M. Suyanto, and A. Sunyoto, "JURNAL INFORMATIKA DAN TEKNOLOGI INFORMASI P ROGRAM S TUDI T EKNIK I NFORMATIKA – F AKULTAS T EKNIK - U NIVERSITAS J ANABADRA," *J. Inf. Interaktif*, vol. 3, no. 1, pp. 27–34, 2018.

[4] BSSN, "Indeks KAMI," 2018. https://bssn.go.id/indeks-kami/.

[5] B. S. Darmawan and A. Tarigan, "INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI," *METIK J.*, vol. 2, no. 1, pp. 53–64, 2018.

[6] A. A. Putra, O. D. Nurhayati, and I. P. Windasari, "Perencanaan dan Implementasi Information Security Management System Menggunakan

Framework ISO/IEC 20071," *J. Teknol. Dan Sist. Komput.*, vol. 4, no. 1, p. 60, 2016, doi: 10.14710/jtsiskom.4.1.2016.60-66.
[7] B. Mahersmi, F. Muqtadiroh, and B. Hidayanto, "Analisis Resiko Keamanan Informasi Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001," no. November, 2016.
[8] I. Santosa and D. Kuswanto, "Analisa Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Pratama XYZ," *Rekayasa*, vol. 9, no. 2, p. 108, 2016, doi: 10.21107/rekayasa.v9i2.3347.
[9] BSSN, "Indeks KAMI Versi 4." 2019.
[10] F. A. Basyarahil, H. M. Astuti, and B. C. Hidayanto, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya," *J. Tek. ITS*, vol. 6, no. 1, pp. 116–121, 2017, doi: 10.12962/j23373539.v6i1.21211.