# Pengukuran Tingkat Keamanan Informasi Perguruan Tinggi XYZ Menggunakan Indeks Keamanan Informasi (KAMI) Berbasis ISO/IEC-27001:2013

*Information Security Measurementsat University of XYZ using KAMI Index Based On ISO/IEC-27001:201*

**Febryan Hari Purwanto*[1], Miftahul Huda[2]**
[1]Akademi Farmasi Al-Fatah Bengkulu
[2]Magister Teknik Informatika, Universitas Amikom Yogyakarta
e-mail: ***[1]fharipurwanto@gmail.com**, [2]miftahulh2@gmail.com

***Abstrak***

*Keamanan informasi pada perguruan tinggi merupakan hal penting yang harus dilindungi karena perguruan tinggi adalah salah satu penyelenggara sistem elektronik dimana sistem elektronik tersebut dapat berisi data-data pribadi dan informasi penting bagi banyak orang terutama bagi dosen, mahasiswa dan sivitas akademika. Perguruan Tinggi XYZ adalah salah satu perguruan tinggi yang sudah menerapkan sistem elektronik dalam kegiatan operasionalnya yang termasuk dalam kategori rendah sehingga Perguruan Tinggi XYZ harus menerapkan pedoman Indeks KAMI seperti yang dinyatakan dalam Peraturan Menteri Komunikasi dan Informasi Republik Indonesia Nomor 4 Tahun 2016 Bab III Pasal 7 bahwa penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik rendah harus menerapkan pedoman Indeks Keamanan Informasi (KAMI). Pada penelitian ini kami melakukan pengukuran tingkat kesiapan keamanan informasi pada Perguruan Tinggi XYZ dengan menggunakan Indeks KAMI versi 3.1. Alat evaluasi indeks KAMI pada versi 3.1. telah mengacu pada kerangka kerja ISO/IEC 27001:2013. Berdasarkan hasil penilaian tingkat keamanan informasi di Perguruan Tinggi XYZ diperoleh hasil bahwa Sistem Elektronik di Perguruan Tinggi XYZ masuk pada kategori Sistem Elektronik Rendah dan hasil penilaian pada ke 5 area keamanan informasi pada Perguruan Tinggi XYZ seluruhnya berada pada Tingkat kematangan I+ atau pada Tingkat Kondisi Awal dengan tingkat penerapan standar ISO/IEC 27001:2013 berada pada nilai 179 atau pada status Perlu Perbaikan. Keamanan informasi pada Perguruan Tinggi XYZ sudah cukup baik pada area tata kelola, namun masih perlu perbaikan pada ke 5 area untuk dapat memenuhi tingkat kerangka kerja dasar. Selain itu Perguruan Tinggi XYZ juga dapat menerapkan pedoman Indeks Keamanan Informasi (KAMI) pada tingkat III dan seterusnya agar dapat mencapai kesiapan sertifikasi ISO/IEC 27001..*

***Kata kunci***—Tingkat Keamanan Informasi, Indeks Keamanan Informasi, Indeks KAMI, ISO/IEC-27001:2013.

***Abstract***

*Information security at universities is an important thing that must be protected because university is one of the organizers of electronic systems where the electronic system can contain personal data and important information for many people, especially for lecturers, students and academicians. University of XYZ is one of the universities that have implemented electronic system in its operational activities which are included in low category so that University of XYZ must apply KAMI Index guideline as stated in Regulation of Minister of Communication and Information of Republic of Indonesia Number 4 Year 2016 Chapter III Article 7 that the*

*organizers of electronic systems that administer low electronics systems must implement the Information Security Index guidelines (KAMI). In this study we measured the level of information security preparedness at University of XYZ by using KAMI Index version 3.1. KAMI Index evaluation tool in version 3.1. has referred to the ISO / IEC 27001: 2013 framework. Based on the results of the assessment of information security level in University of XYZ obtained the result that the Electronic System in University of XYZ entered in the category of Low Electronic System and the assessment result in the 5 information security areas at University of XYZ are all at maturity level I+ or at initial condition level with the level of implementation of ISO / IEC 27001: 2013 standards is at 179 or on the Need Repair status. Information security at University of XYZ is good enough in the area of governance, but still needs improvement in the 5 areas to meet the basic framework level. In addition University of XYZ may also apply the Information Security Index (KAMI) guidelines at level III and beyond in order to achieve ISO / IEC 27001 certification readiness.*

***Keywords***—Measurement of Information Security,Information Security, KAMI Index,ISO/IEC-27001:2013

## 1. PENDAHULUAN

Keamanan informasi pada perguruan tinggi merupakan hal penting yang harus dilindungi karena perguruan tinggi adalah salah satu penyelenggara sistem elektronik dimana sistem elektronik tersebut dapat berisi data-data pribadi dan informasi penting bagi banyak orang terutama bagi dosen, mahasiswa dan sivitas akademika. Keamanan informasi juga sangat dibutuhkan untuk menjamin kepercayaan dari masyarakat terhadap suatu perguruan tinggi dan mencegah pemanfaatan informasi oleh pihak yang tidak bertanggungjawab. Keamanan Informasi adalah terjaganya kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) informasi [1].

Salah satu upaya pemerintah dalam meningkatkan kematangan keamanan informasi pada instansi di Indonesia adalah dengan menerbitkan peraturan menteri tentang keamanan informasi. Dalam Peraturan Menteri Komunikasi dan Informasi Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi disebutkan bahwa setiap penyelenggara sistem elektronik harus menerapkan standar SNI ISO/IEC 27001 dalam melakukan pengamanan informasi[1]. Disamping itu Departemen Komunikasi dan Informasi Republik Indonesia juga telah mengembangkan alat bantu evaluasi keamanan informasi yaitu Indeks Keamanan Informasi (KAMI) yang merujuk pada standar SNI-SNI/IEC 27001[2]. Alat evaluasi ini digunakan untuk memberikan gambaran kondisi kesiapan yaitu kelengkapan dan kematangan kerangka kerja keamanan informasi dalam suatu organisasi.

Perguruan Tinggi XYZ adalah salah satu perguruan tinggi yang sudah menerapkan sistem elektronik dalam kegiatan operasionalnya yang termasuk dalam kategori rendah sehingga Perguruan Tinggi XYZ harus menerapkan pedoman Indeks KAMI seperti yang dinyatakan dalam Peraturan Menteri Komunikasi dan Informasi Republik Indonesia Nomor 4 Tahun 2016 Bab III Pasal 7 bahwa penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik rendah harus menerapkan pedoman Indeks Keamanan Informasi (KAMI). Selain itu belum pernah dilakukan evaluasi terhadap keamanan informasi di Perguruan Tinggi XYZ.

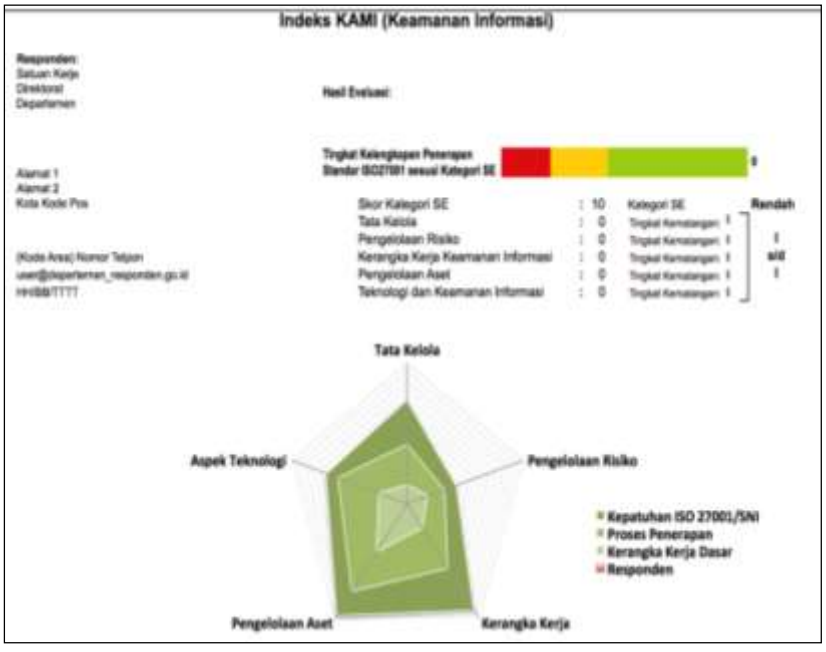
Beberapa penelitian sebelumnya pernah melakukan pengukuran tingkat keamanan informasi menggunakan Indeks KAMI di instansi pendidikan pada tingkat sekolah menengah atas [3] dan tingkat perguruan tinggi [2,4,5,6,7]. Namun pada penelitian [2,3,4,5,6] evaluasi keamanan informasi dilakukan menggunakan Indeks Keamanan Informasi (KAMI) yang masih mengacu pada kerangka kerja SNI ISO/IEC 27001:2009 dimana evaluasi yang dilakukan mencakup peran TIK di dalam instansi, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi[2].

Pada penelitian ini kami melakukan pengukuran tingkat kesiapan keamanan informasi pada Perguruan Tinggi XYZ dengan menggunakan Indeks KAMI versi 3.1. Alat evaluasi indeks KAMI pada versi 3.1. telah mengacu pada kerangka kerja ISO/IEC 27001:2013 dimana peran TIK di dalam instansi pada indeks kami versi sebelumnya telah diganti dengan kategori sistem elektronik yang digunakan instansi[7]. Sehingga evaluasi yang dilakukan pada indeks KAMI versi 3.1. meliputi:

1. Kategori sistem elektronik yang digunakan instansi,
2. Tata kelola keamanan informasi,
3. Pengelolaan risiko keamanan informasi,
4. Kerangka kerja keamanan informasi,
5. Pengelolaan aset informasi, dan
6. Teknologi dan keamanan informasi.

Indeks KAMI versi 3.1 adalah sebuah tools yang dikembangkan oleh Kominfo yang digunakan untuk mengevaluasi tingkat kematangan dan kelengkapan tata kelola keamanan informasi pada sebuah organisasi berdasarkan ISO/IEC 27001:2013. Alat evaluasi ini digunakan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pemimpin instansi namun tidak dapat digunakan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada [7].

Evaluasi yang dilakukan menggunakan indeks KAMI versi 3.1 mencakup 5 target area, yaitu [8]: tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan
Informasi. Sebelum dilakukan proses penilaian secara kuantitatif, maka dilakukan proses klasifikasi terlebih dahulu terhadap kategori Sistem Elektronik. Responden diminta untuk mendeskripsikan Sistem Elektronik yang ada dalam satuan kerjanya [8]. Setelah melakukan klasifikasi pada Peran Sistem Elektronik pada organisasi, kemudian dilakukan penilaian terhadap kelima area yang ada di Indeks KAMI versi 3.1. Hasil penilaian akan digambarkan kedalam grafik radar yang menunjukkan tingkat kepatuhan organisasi pada 5 area utama terhadap ISO/IEC 27001:2013[8]. Seperti ditunjukkan pada gambar 1.




**Gambar 1.**Dashboard Indeks KAMI versi 3.1

Setelah semua pertanyaan pada masing-masing area diisi maka diperoleh skor akhir evaluasi. Kemudian skor akhir ini dipetakan sesuai kategori sistem elektronik yang sudah ditentukan sebelumnya. sehingga skor akhir dapat digunakan untuk menentukan tingkat kesiapan keamanan informasi suatu organisasi seperti ditunjukkan pada Tabel 1.

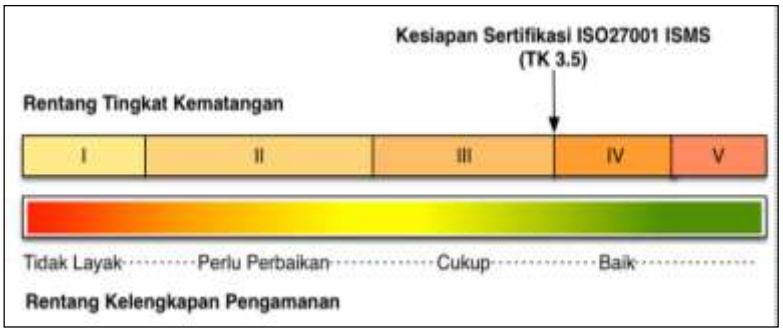
**Tabel1.**Tabel Skor Penilaian Indeks KAMI versi 3.1

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

Selanjutnya dilakukan pengelompokan berdasarkan tingkat kematangan dengan kategori yang mengacu pada tingkat kematangan yang digunakan oleh COBIT atau CMMI yang didefinisikan menjadi[8] :

Tingkat I/I+ : Kondisi Awal
Tingkat II/II+ : Penerapan Kerangka Kerja Dasar
Tingkat III/III+ : Terdefinisi dan Konsisten
Tingkat IV/IV+ : Terkelola dan Terukur
Tingkat V : Optimal

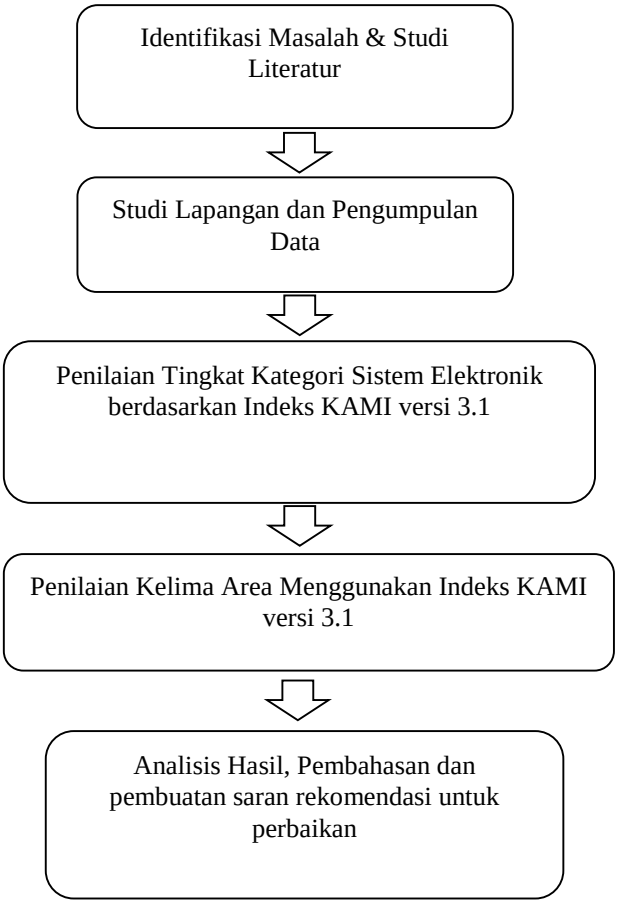
Pada tahap awal reponden diberi nilai tingkat kematangan I, nilai akan diperoleh setelah responden mengisi seluruh pertanyaan yang diminta. Untuk dapat mengikuti sertifikasi ISO 27001:2013 maka tingkat kematangan yang dibutuhkan untuk ambang batas minimum adalah Tingkat III+ seperti ditunjukkan pada gambar 3.




**Gambar 3.**Tingkat Kematangan Kesiapan Sertifikasi ISO27001 ISMS

## 2. METODE PENELITIAN

Penelitian ini dilakukan dalam 5 Langkah seperti ditunjukkan pada gambar 4 antara lain : Identifikasi Masalah dan Studi Literatur, Studi Lapangan dan Pengumpulan Data, Penilaian Tingkat Kategori Sistem Elektronik, Penilaian Kelima Area dengan Indeks KAMI serta Melakukan Analisis dan Pembahasan serta Pembuatan Saran Rekomendasi.




**Gambar 4.**Alur Peneltian

Pada tahap Identifikasi Masalah dan Studi Literatur penulis melakukan identifikasi masalah dimana diketahui bahwa Perguruan Tinggi XYZ adalah salah satu perguruan tinggi yang sudah menerapkan sistem elektronik dalam kegiatan operasionalnya yang termasuk dalam kategori rendah namun Perguruan Tinggi XYZ belum pernah menerapkan evaluasi terhadap keamanan informasi. Kemudian penulis melakukan studi literatur yang berkaitan pedoman Indeks KAMI.

Tahap Studi Lapangan dan Pengumpulan Data dilakukan dengan melakukan studi lapangan dan mengumpulkan data di Perguruan Tinggy XYZ dengan menggunakan alat evaluasi Index KAMI yang diisi oleh responden yaitu bagian ICT Center Perguruan Tinggi XYZ. Pada tahap ini juga dilakukan Penilaian Tingkat Kategori Sistem Elektronik untuk mengetahui kategori sistem elektronik yang ada di Perguruan Tinggi XYZ.

Selanjutnya dilakukan Penilaian Kelima Area dengan Indeks KAMI dengan melakukan penilaian pada 5 area kesiapan keamanan informasi antara lain : tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi. Setelah dilakukan penilaian selanjutnya

dilakukan Analisis dan Pembahasan serta Pembuatan Saran Rekomendasi yang dibutuhkan bagi pengembangan sistem elektronik dan peningkatan tingkat keamanan informasi pada Perguruan Tinggi XYZ.

## 3. HASIL DAN PEMBAHASAN

### *3.1. Hasil Penilaian Kategori Sistem Elektronik di Perguruan Tinggi XYZ*

Pada proses penilaian kategori sistem elektronik yang digunakan pada Perguruan Tinggi XYZ diperoleh hasil skor penetapan kategori sistem elektronik sebesar 13. Hal ini menunjukkan bahwa sistem elektronik masih berada pada kategori rendah sesuai dengan ketentuan pada penentuan kategori sistem elektronik[8] seperti ditunjukkan pada tabel 2.

**Tabel2.**Tabel Kategori Sistem Elektronik

| **Kategori Sistem Elektronik** | **Nilai Skor** |
|---|---|
| Rendah | 10-15 |
| Tinggi | 16-34 |
| Strategis | 35-50 |

### *3.2. Hasil Penilaian 5 Area Kesiapan Keamanan Informasi di Perguruan Tinggi XYZ*

Setelah diketahui bahwa sistem elektronik di Perguruan Tinggi XYZ berada pada kategori rendah, maka selanjutnya dilakukan penilaian pada 5 area kesiapan keamanan informasi antara lain : tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi.

Penilaian dilakukan pada ke 5 area dan diperoleh bahwa evaluasi pada area pengelolaan resiko keamanan informasi memperoleh nilai paling rendah yaitu 20 poin dan nilai tertinggi diperoleh pada hasil evaluasi pengelolaan aset informasi yaitu sebesar 62 poin, sedangkan nilai pada tiga area lainnya adalah 28 poin untuk nilai evaluasi pada area tata kelola keamanan informasi, 34 poin untuk nilai evaluasi pada area kerangka kerja pengelolaan keamanan informasi dan 35 poin untuk evaluasi area teknologi dan keamanan informasi. Keseluruhan nilai secara detil ditunjukkan pada tabel 3.

**Tabel3.**Tabel Hasil Penilaian pada 5 Area Kemananan Informasi di Perguruan Tinggi XYZ

| **No** | **Area Keamanan Informasi** | **Total Nilai** |
|---|---|---|
| 1 | Tata Kelola Keamanan Informasi | 28 |
| 2 | Pengelolaan Resiko Keamanan Informasi | 20 |
| 3 | Kerangka Kerja Pengelolaan Keamanan Informasi | 34 |
| 4 | Pengelolaan Aset Informasi | 62 |
| 5 | Teknologi dan Keamanan Informasi | 35 |

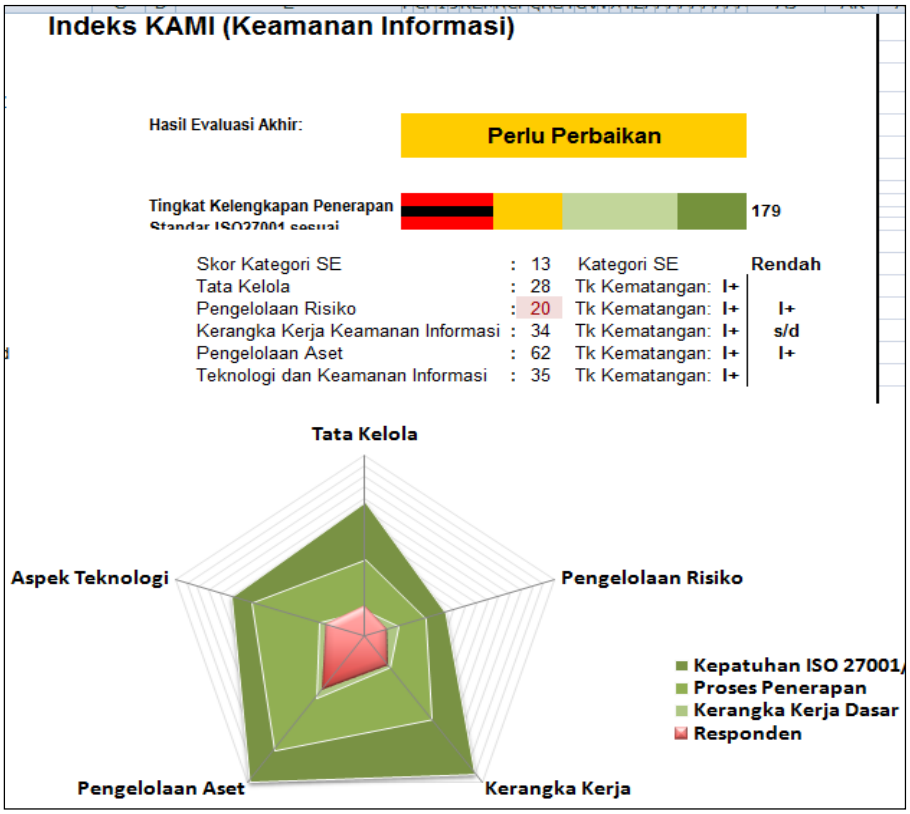
*3.3. Hasil Akhir Penilaian Indeks KAMI*

Setelah dilakukan penilaian pada ke 5 area keamanan informasi maka diperoleh hasil akhir penilaian tingkat kelengkapan dan kematangan keamanan informasi pada Perguruan Tinggi XYZ berdasarkan Indeks KAMI berbasis ISO/IEC 27001:2013 kemudian total nilai akan menentukan tingkat kesiapan keamanan informasi di Perguruan Tinggi XYZ sesuai dengan ketentuan skor status kesiapan keamanan informasi yang ditunjukkan pada tabel 4.

**Tabel4.**Tabel Skor Status Kesiapan Keamanan Informasi Sistem Elektronik Kategori Rendah

| **Skor Akhir** | | **Status Kesiapan** |
|---|---|---|
| 0 | 174 | Tidak Layak |
| 175 | 312 | Perlu perbaikan |
| 313 | 535 | Cukup |
| 536 | 645 | Baik |

Hasil akhir penilaian ke 5 area kemananan informasi dan hasil akhir tingkat kesiapan keamanan informasi pada Perguruan Tinggi XYZ ditunjukkan secara detil pada Dasbord Indeks KAMI seperti pada gambar 5 dimana untuk kategori Sistem Elektronik Rendah diperoleh hasil bahwa seluruh area keamanan informasi pada Perguruan Tinggi XYZ berada pada Tingkat kematangan I+ atau pada Kondisi Awal seperti ditunjukkan pada tabel 5 dengan tingkat penerapan standar ISO/IEC 27001:2013 berdasarkan kategori Sistem Elektronik berada pada nilai 179 yang artinya status kesiapan penerapan keamanan informasi pada Perguruan Tinggi XYZ masih Perlu Perbaikan.




**Gambar 5.**Hasil dasbor Indeks KAMI versi 3.1 pada penilaian kesiapan keamanan informasi pada Perguruan Tinggi XYZ

**Tabel5.**Tabel Tingkat Kematangan Ke 5 Area

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

*3.4. Saran Perbaikan pada 5 Area Keamanan Informasi di Perguruan Tinggi XYZ*

Setelah diperoleh hasil penilaian pada setiap area seperti ditunjukkan oleh grafik radar pada gambar 5, diketahui bahwa pada tingkat kerangka kerja dasar, keamanan informasi pada Perguruan Tinggi XYZ sudah cukup baik pada area tata kelola, namun perlu perbaikan pada ke 5 area untuk dapat memenuhi tingkat kerangka kerja dasar. Adapun perbaikan yang perlu dilakukan oleh Perguruan Tinggi XYZ antara lain :

1. Penanggung jawab pelaksanaan pengamanan informasi harus diberikan alokasi sumber daya untuk mengelola dan menjamin kepatuhan program keamanan informasi
2. Standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi harus didefinisikan dan sesuai dengan kebutuhan.
3. Instansi perlu melakukan peningkatan kompetensi dan keahlian yang memadai sesuai standar yang berlaku
4. Instansi harus mempunyai kerangka kerja pengelolaan resiko keamanan informasi yang terdokumentasi dan digunakan secara resmi
5. Instansi perlu menyusun langkah mitigasi dan penanggulangan risiko yang ada
6. Perlu adanya proses untuk mengkomunikasikan kebijakan keamanan informasi ke semua pihak terkait serta proses untuk mengidentifikasikan kondisi yang membahayakan keamanan informasi agar dapat ditindaklanjuti sesuai prosedur yang diberlakukan.
7. Instansi harus menetapkan dan memberlakukan konsekwensi pelanggaran kebijakan keamanan informasi.
8. Perlu adanya klasifikasi aset informasi sesuai dengan perundang-undangan yang berlaku, dan harus dilakukan evaluasi terhadap aset sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya.
9. Perlu dibuat tata tertib pengamanan dan penggunaan aset instansi terkait HAKI
10. Perlu dibuat peraturan terkait instalasi perangkat lunak di aset TI milik instansi
11. Perlu dibuat ketetapan terkait waktu penyimpanan, klasifikasi data, penghancuran data, serta ketetapan pertukaran data dengan pihak eksternal dan pengamanannya.
12. Instansi harus secara rutin melakukan analisa kepatuhan penerapan konfigurasi standar yang ada

13. Instansi harus memiliki infrastruktur jaringan yang secara keseluruhan dapat memastikan ketersediaan
14. Perlu dilakukan analisa secara berkala pada semua log untuk memastikan akurasi, validitas dan kelengkapan isi untuk kepentingan jejak dan forensic
15. Instansi dapat menerapkan enkripsi dalam melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.

Selain rekomendasi perbaikan di atas Perguruan Tinggi XYZ juga dapat menerapkan pedoman Indeks Keamanan Informasi (KAMI) pada tingkat III dan seterusnya agar dapat mencapai kesiapan sertifikasi ISO/IEC 27001.

## 4. KESIMPULAN

Berdasarkan hasil penilaian tingkat keamanan informasi di Perguruan Tinggi XYZ seperti ditunjukkan pada tabel 3, tabel 5 dan gambar 5 diperoleh hasil bahwa Sistem Elektronik di Perguruan Tinggi XYZ masuk pada kategori Sistem Elektronik Rendah dan hasil penilaian pada ke 5 area keamanan informasi pada Perguruan Tinggi XYZ seluruhnya berada pada Tingkat kematangan I+ atau pada Tingkat Kondisi Awal dengan tingkat penerapan standar ISO/IEC 27001:2013 berdasarkan kategori Sistem Elektronik Rendah berada pada nilai 179 atau berada pada status kesiapan penerapan keamanan informasi yang masih Perlu Perbaikan. Keamanan informasi pada Perguruan Tinggi XYZ sudah cukup baik pada area tata kelola, namun masih perlu perbaikan pada ke 5 area untuk dapat memenuhi tingkat kerangka kerja dasar. Selain itu Perguruan Tinggi XYZ juga dapat menerapkan pedoman Indeks Keamanan Informasi (KAMI) pada tingkat III dan seterusnya agar dapat mencapai kesiapan sertifikasi ISO/IEC 27001.

## UCAPAN TERIMA KASIH

Terimakasih kepada seluruh pihak yang telah membantu dalam menyelesaikan penelitian ini, sehingga dapat dipublikasikan.

## DAFTAR PUSTAKA

[1] Kementrian Komunikasi dan Informatika, “Peraturan Menteri Komunikasi Dan Informatika Republik Indonesia Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi”, *Kementrian Komunikasi dan Informatika*, 2016

[2] I. Afrianto, T. Suryana, Sufa’atin, “Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009”, ULTIMA InfoSys,Vol.VI, No.1, Juni 2015,pp.43-49

[3] D. Saputra, O. Gilang H, “Evaluasi Keamanan Informasi Pada Sma Islam Al-Azhar (SMAIA) 4 Kemang Pratama Berdasarkan Indeks Keamanan Informasi (KAMI) SNI ISO/IEC 27001:2009”,Jurnal Khatulistiwa Informatika, Vol. 4, No. 1, Juni 2016,pp.22-29

[4] M. I. Rosadi, L. Hakim, “Pengukuran Dan Evaluasi Keamanan Siakad Universitas Yudharta Menggunakan Indeks KAMI”, Explore IT - Volume 7, Nomor 1, Juni 2015, pp.33-42

[5] Zulkifli, “Mengukur Indeks Keamanan Informasi dengan Metode Octave berstandar ISO 27001pada Universitas Al Muslim-Bireuen”, Jurnal Penelitian Teknik Informatika (TECHSI), 2016, pp.157-166.

[6] M. F. Husin, H. F. Wowor, S.D.S. Karouw, “Implementasi Indeks KAMI di Universitas Sam Ratulangi”, E-Journal Teknik Informatika Vol 12, No.1, 2017.

[7] F. A. Basyarahil, H. M. Astuti, 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", Jurnal Teknik ITS Vol. 6, No. 1, 2017, pp.A.122-A.128.

[8] Kementrian Komunikasi dan Informatika, "Indeks Keamanan Informasi (KAMI) Versi 3.1", *Kementrian Komunikasi dan Informatika*, 15 April 2015.