TESIS

ANALISIS TINGKAT KESIAPAN PENERAPAN KEAMANAN SISTEM MANAJEMEN INFORMASI BERBASIS INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA UNIVERSITAS TEKNOLOGI MATARAM

(Studi Kasus: Kampus Universitas Teknologi Mataram)

Disusun oleh:

Nama	**: Zumratul Muahidin**
NIM	**: 19.51.1277**
Konsentrasi	**: Business Intelligence**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

TESIS

ANALISIS TINGKAT KESIAPAN PENERAPAN KEAMANAN SISTEM MANAJEMEN INFORMASI MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA UNIVERSITAS TEKNOLOGI MATARAM

(Studi Kasus: Kampus Universitas Teknologi Mataram)

ANALYSIS OF READINESS LEVEL OF INFORMATION SECURITY MANAGEMENT SYSTEM USING THE KAMI INDEX BASED ON ISO/IEC 27001:2013 STANDARD AT UNIVERSITAS TEKNOLOGI MATARAM

(Case Study: Campus Universitas Teknologi Mataram)

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama	**: Zumratul Muahidin**
NIM	**: 19.51.1277**
Konsentrasi	**: Business Intelligence**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2022

HALAMAN PENGESAHAN

ANALISIS TINGKAT KESIAPAN PENERAPAN KEAMANAN SISTEM MANAJEMEN INFORMASI MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA UNIVERSITAS TEKNOLOGI MATARAM

ANALYSIS OF READINESS LEVEL OF INFORMATION SECURITY MANAGEMENT SYSTEM USING THE KAMI INDEX BASED ON ISO/IEC 27001:2013 STANDARD AT UNIVERSITAS TEKNOLOGI MATARAM

Dipersiapkan dan Disusun oleh

Zumratul Muahidin

19.51.1277

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Rabu, 03 Agustus 2022

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 03 Agustus 2022
Rektor

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERSETUJUAN

ANALISIS TINGKAT KESIAPAN PENERAPAN KEAMANAN SISTEM MANAJEMEN INFORMASI MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001:2013 PADA UNIVERSITAS TEKNOLOGI MATARAM

ANALYSIS OF READINESS LEVEL OF INFORMATION SECURITY MANAGEMENT SYSTEM USING THE KAMI INDEX BASED ON ISO/IEC 27001:2013 STANDARD AT UNIVERSITAS TEKNOLOGI MATARAM

Dipersiapkan dan Disusun oleh

Zumratul Muahidin

19.51.1277

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Rabu, 03 Agustus 2022

Pembimbing Utama

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

Anggota Tim Penguji

Dr. Andi Sunyoto, M.Kom.
NIK. 190302052

Dhani Ariatmanto, M.Kom., Ph.D.
NIK. 190302197

Pembimbing Pendamping

Drs. Asro Nasiri, M.Kom.
NIK. 190302152

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 03 Agustus 2022
Direktur Program Pascasarjana

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini.

Nama mahasiswa : Zumratul Muahidin
NIM : 19.51.1277
Konsentrasi : Business Intelligence

Menyatakan bahwa Tesis dengan judul berikut:
Analisis Tingkat Kesiapan Penerapan Keamanan Sistem Manajemen Informasi Menggunakan Indeks Kami Berdasarkan Standar ISO/IEC 27001:2013 Pada Universitas Teknologi Mataram

Dosen Pembimbing Utama : Prof. Dr. Kusrini, M.Kom.
Dosen Pembimbing Pendamping : Drs. Asro Nasiri, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, 03 Agustus 2022
Yang Menyatakan,

Zumratul Muahidin

HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan kehadirat Allah SWT, atas segala rahmat, karunia dan hidayah-Nya yang telah diberikan sehingga penyusunan dan penulisan tesis ini dapat terselesaikan guna memenuhi salah satu syarat dalam menyelesaikan pendidikan program Magister Komputer pada Program Pascasarjana Universitas AMIKOM Yogyakarta. Tesis ini saya persembahkan untuk:

1. Kedua orang tua saya Alm. H. Paozan Azim dan Ibu Hj. Aisah serta seluruh keluarga atas doa, dorongan serta motivasi sehingga penulis dapat menyelesaikan penyusunan tesis ini.
2. Ibu Prof. Dr. Kusrini M. Kom dan Bapak Drs. Asro Nasiri, M. Kom yang telah memberikan bimbingan aktif selama pelaksanaan penelitian, semoga mendapatkan banyak keberkahan dan dilancarkan segala urusannya.
3. Rektor Universitas Teknologi Mataram Bapak H. Lalu Darmawan Bakti, M.Sc., M.Kom atas doa, dorongan serta motivasnya sehingga penulis dapat menyelesaikan penyusunan tesis ini.
4. Saudara-saudara saya Zulkifli, Rokyal Aini, Uji Burrahman, M. Patroni dan Nurul Wahyuni atas doa, dorongan serta motivasinya sehingga penulis dapat menyelesaikan penyusunan tesis ini.
5. Keluarga besar kelas MTI20-A yang selalu membantu dan memberi saran demi kelancaran pengerjaan tesis, semoga selalu semangat dan sukses.

HALAMAN MOTTO

"Allah tidak membebani seseorang melainkan sesuai kesanggupannya"

QS Al Baqarah 286.

"Terkadang orang dengan masa lalu paling kelam akan menciptakan masa depan paling cerah."

Umar bin Khattab

"Barang siapa keluar untuk mencari sebuah ilmu, maka ia akan berada di jalan Allah hingga ia kembali."

HR Tirmidzi

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur penulis panjatkan sehadirat Allah SWT karena atas segala karunia dan ridho-Nya, sehingga tesis yang berjudul "Analisis Tingkat Kesiapan Penerapan Keamanan Sistem Manajemen Informasi Menggunakan Indeks Kami Berdasarkan Standar ISO/IEC 27001:2013 Pada Universitas Teknologi Mataram" dapat diselesaikan dengan tepat waktu.

Tesis ini disusun untuk memenuhi salah satu syarat memperoleh gelar Magister Komputer pada program studi Magister Teknik Informatika Universitas Amikom Yogyakarta.

Penyelesaian tesis yang sangat berharga ini tidak lepas dari bantuan dan dukungan dari berbagai pihak. Pada kesempatan ini, penulis mengucapkan rasa syukur dan terima kasih kepada:

1. Orang tua Ibu Hj. Aisah serta seluruh keluarga atas doa, dorongan serta motivasi sehingga penulis dapat menyelesaikan penyusunan tesis ini.
2. Ibu Prof. Dr. Kusrini M. Kom selaku pembimbing utama yang telah membimbing, membantu, dan memotivasi dalam penulisan tesis ini sehingga dapat terselesaikan dengan baik.
3. Bapak Drs. Asro Nasiri, M. Kom selaku pembimbing pendamping yang telah membimbing, membantu, dan memotivasi dalam penulisan tesis ini sehingga dapat terselesaikan dengan baik.
4. Dosen Penguji yang telah memberikan saran yang baik demi kemajuan tesis ini.

5. Direktur Program Pascasarjana, jajarannya, staf dan rekan-rekan. Magister Teknik Informatika Universitas Amikom Yogyakarta.
6. Saudara-saudara saya Zulkifli, Rokyal Aini, Uji Burrahman, M. Patroni dan Nurul Wahyuni atas doa, dorongan serta motivasinya sehingga penulis dapat menyelesaikan penyusunan tesis ini

Demikian ucapan terima kasih ini penulis sampaikan, tentunya penulisan tesis ini masih belum sempurna. Penulis menyadari sepenuhnya sehingga saran dan masukan untuk menyempurnakan tesis ini sangat diharapkan. Semoga Allah SWT senantiasa membimbing dan menyertai langkah kita dalam mengembangkan keilmuan, aamiin.

Yogyakarta, 03 Agustus 2022

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Dengan diterbitkannya Peraturan Menteri Komunikasi dan Informatika (Kominfo) nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, maka setiap organisasi maupun perusahaan harus menerapkan standar ini untuk memastikan tingkat keamanan informasinya. Badan Pengelola Sistem Informasi (BPSI) Universitas Teknologi Mataram sebagai unit kerja yang bertanggung jawab terhadap keamanan informasi di Universitas memiliki tuntutan untuk segera mengimplementasikan standart ISO 27001:2013. penelitian ini bertujuan untuk menganalisis tingkat kesiapan penerapan keamanan sistem manajemen informasi pada kampus Universitas Teknologi Mataram berdasarkan standar ISO/IEC 27001:2013 dengan menggunakan indeks KAMI versi 4.1. Metode pengumpulan data dengan cara melakukan observasi langsung dan interview terhadap penanggung jawab sistem informasi.

Hasil penilaian dengan indeks KAMI didapatkan skor kategori elektronik adalah 23, untuk penilaian tata kelola keamanan informasi dengan skor 83, Pengelolaan Risiko Keamanan Informasi skornya 55, Kerangka Kerja Pengelolaan Keamanan Informasi skornya 61, Pengelolaan Aset Informasi dengan skor 124, Teknologi dan Keamanan Informasi skornya 93, tingkat kematangan keamanan informasi yaitu tingkat II dengan nilai sebesar 416, hasil yang didapatkan sampai Pemenuhan Kerangka Kerja Dasar.

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.

Kata kunci: Indeks KAMI, ISO/IEC 27001:2013, Keamanan Informasi.

ABSTRACT

With the issuance of Regulation of the Minister of Communication and Information (Kominfo) number 4 of 2016 concerning Information Security Management Systems, every organization and company must apply this standard to ensure the level of information security. The Information System Management Agency (BPSI) of the Mataram Technology University as a work unit responsible for information security at the University has demands to immediately implement the ISO 27001:2013 standard. This study aims to analyze the level of readiness for the application of information management system security on the Mataram Technology University campus based on the ISO/IEC 27001:2013 standard using the K.A.M.I index version 4.1. Methods of collecting data by conducting direct observations and interviews with the person in charge of the information system.

The results of the assessment with the K.A.M.I index obtained a score of 23 for the electronic category, for the assessment of information security governance with a score of 83, Information Security Risk Management with a score of 55, Information Security Management Framework with a score of 61, Management of Information Assets with a score of 124, Technology and Information Security with a score of 93 , the maturity level of information security is level II with a value of 416, the results obtained are up to the fulfillment of the Basic Framework.

From these results it can be concluded that the level of information security is still very low and it is necessary to improve the information security system by cooperating with information security developers from third parties.

Keyword: KAMI Index, ISO/IEC 27001:2013, Information Security.

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Perkembangan teknologi informasi yang terus berkembang pada saat ini, menuntut setiap organisasi maupun perusahaan harus dapat mengikuti perkembangan teknologi informasi, 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 salah satu aspek yang sangat penting saat ini, terutama bagi organisasi maupun perusahaan yang menggunakan teknologi informasi sebagai pendukung proses bisnisnya (Hambali et al., 2020). Dengan diterbitkannya Peraturan Menteri Komunikasi dan Informatika (Kominfo) nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, maka setiap organisasi maupun perusahaan harus menerapkan standar ini untuk memastikan tingkat keamanan informasinya.

Instansi pendidikan di indonesia juga perlu menerapkan standar ini untuk memastikan tingkat keamanan informasinya telah memenuhi standar ISO 27001: 2013, dimana penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sebagian besar sudah menjadi kebutuhan dan tuntutan untuk setiap organisasi penyelenggara pelayanan publik (Yustanti et al., 2018). Badan Pengelola Sistem Informasi (BPSI) Universitas Teknologi Mataram sebagai unit kerja yang bertanggung jawab terhadap keamanan informasi di Universitas memiliki tuntutan

untuk segera mengimplementasikan standart ISO 27001:2013. Dalam pengukuran tingkat kesiapan penerapan keamanan sistem manajemen informasi tersebut, pemerintah telah menyiapkan perangkat atau *tools* yang disebut sebagai Indeks Keamanan Informasi (KAMI) yang berisi pengukuran terhadap tingkat urgensitas peran TIK dalam upaya peningkatan kualitas layanan, yakni sebagai proses realisasi dari tata kelola yang baik (Yustanti et al., 2018). Dalam penyelenggaraan tata kelola, faktor keamanan informasi merupakan aspek yang sangat diperhatikan. Kinerja tata kelola akan terganggu apabila informasi yang merupakan salah satu obyek utama pada tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) (Juliharta, 2019).

ISO 27001 merupakan Standar Nasional Indonesia (SNI) dalam mengelola keamanan informasi untuk semua organisasi di Indonesia oleh Badan Standarisasi Nasional (BSN) yang mencakup seluruh tipe organisasi, seperti perusahaan komersil, pemerintahan dan organisasi non-profi (Hambali et al., 2020). ISO 27001 juga menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif sesuai dengan SNI. Hal ini termasuk kemampuan akses data secara berkelanjutan, kerahasiaan, dan integritas atas informasi yang dimiliki. Untuk mendapatkan ukuran terstandarisasi SNI ISO/IEC 27001:2013 Badan Siber dan Sandi Negara (BSSN) mengeluarkan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevaluasi tingkat kesiapan (kelengakapan dan kematangan) penerapan SNI ISO/IEC

27001:2013 yaitu Indeks KAMI (Keamanan Informasi). Indeks KAMI (Keamanan Informasi) tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai alat perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi. pada penelitian ini dilakukan evaluasi dengan menggunakan Indeks KAMI, *tools* ini merupakan alat bantu yang dikeluarkan pada Peraturan Menteri Komunikasi dan Informatika untuk menilai kondisi keamanan informasi (Arman et al., 2019).

Menjaga keamanan informasi berarti perlunya usaha dalam memperhatikan faktor-faktor keamanan dari seluruh piranti pendukung, jaringan, dan fasilitas lain yang terkait secara langsung maupun tidak langsung dalam proses pengolahan informasi. Instansi pendidikan di Indonesia juga perlu menerapkan keamanan informasi untuk menghindari adanya pencurian data dan hilangnya data secara sengaja maupun tidak sengaja. Hal ini juga perlu diterapkan dan diperhatikan di kampus Universitas Teknologi Mataram. Universitas Teknologi Mataram membangun sebuah badan pengelola sistem informasi (BPSI) untuk menangani permasalahan teknologi informasi dan sistem informasi yang dimiliki. Semua kegiatan teknologi informasi dan sistem informasi dipusatkan dan dikembangkan di BPSI. Data dari BPSI menyatakan bahwa ditemukannya beberapa celah keamanan sistem informasi dan jaringan yang cukup berbahaya. Gangguan keamanan informasi tersebut juga dirasakan oleh pihak civitas akademika Universitas Teknologi Mataram, seperti pembobolan data untuk SIAKAD dimana para mahasiswa tidak dapat login pada masing-masing akun yang dimiliki. Selain gangguan pada SIAKAD, hal serupa juga pernah terjadi untuk akun email

Universitas Teknologi Mataram yang dibobol dan harus dilakukan *reset password* untuk menangani masalah tersebut. Salah satu upaya yang dapat dilakukan oleh kementrian Kominfo untuk meningkatkan kualitas keamanan informasi pada suatu instansi adalah dengan membuat salah satu alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Indeks KAMI mengacu pada standar ISO/IEC 27001:2013 yang berisi tentang keamanan informasi.

Berbagai penelitian mengenai analisis keamanan sistem manajemen informasi menggunakan Indeks KAMI telah dilakukan, salah satunya adalah penelitian yang berjudul Analisa Tingkap Kesiapan Penerapan Keamanan Teknologi Informasi Dalam Pelaksanaan *E-Government* Berbasis Indeks Keamanan Informasi (KAMI) Studi Kasus Pemerintah Kota Kediri (Ferdiansyah, Subektiningsih, dan Indrayani, 2019). Penelitian tersebut melakukan evaluasi untuk mendapatkan informasi terkait tingkat kematangan dan kesiapan keamanan informasi pada UPTD XYZ. Hasil yang didapatkan dari evaluasi tersebut adalah 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. Perbedaan dari penelitian ini adalah lokasi penelitian dan alat ukur Indeks KAMI yang digunakan. Pada penelitian ini dilakukan di pemerintah Kota Kediri dan menggunakan Indeks KAMI versi 3.1, sedangkan penelitian saya dilakukan di Kampus Universitas Teknologi Mataram dan

menggunakan Indeks KAMI versi 4.1 dan perbedaan ini berada pada kuesionernya, alat ukur evaluasi ini terdapat 141 pertanyaan sedangkan Indeks KAMI versi 4.1 memiliki 194 pertanyaan dan penambahan area suplemen.

Penelitian yang dilakukan oleh Rahmat Hidayat, Mohammad Suyanto, dan Andi Sunyoto (2018) terkait dengan Indeks Penelitian Keamanan Informasi Untuk Mengukur Kematangan Manajemen Keamanan Layanan TI (Studi Kasus BPMP Kabupaten Gresik). Penelitian ini berisi hasil pengukuran kematangan Sistem Manajemen Keamanan Informasi (ISMS) di Kabupaten Gresik Hasil pengukuran kelengkapan dan kematangan ISMS di BPMP Kabupaten Gresik masih tergolong rendah, yaitu pada level I sampai II yang berarti tingkat kematangannya dinyatakan dalam kondisi awal hingga implementasi kerangka dasar, masih di bawah standar ISO 27001: 2009. Penyebab tingkat kematangan yang rendah dari SMKI termasuk tingkat kesadaran yang rendah dari kepemimpinan dan karyawan terkait SMKI, kurangnya dokumentasi kegiatan dan juga untuk pengembangan aplikasi dan infrastruktur yang ada reaktif. Peneliti menyarankan hal-hal yang perlu untuk meningkatkan kesadaran kepada para pemimpin dan karyawan tentang pentingnya ISMS, dan untuk mengembangkan Cetak Biru TIK yang memungkinkan pengembangan aplikasi BPMP dan infrastruktur harus dilakukan secara terencana dan komprehensif. Perbedaan dari penelitian ini adalah lokasi penelitian dan alat ukur Indeks KAMI yang digunakan. Pada penelitian ini dilakukan di BPMP Kabupaten Gresik dan menggunakan Indeks KAMI versi 3.1, sedangkan penelitian saya dilakukan di Kampus Universitas Teknologi Mataram dan menggunakan Indeks KAMI versi 4.1 dan perbedaan ini berada pada kuesionernya, alat ukur

evaluasi ini terdapat 141 pertanyaan sedangkan Indeks KAMI versi 4.1 memiliki 194 pertanyaan dan penambahan area suplemen.

Pada penelitian lain yang berjudul Analisis Tingkat Kesiapan dan Kematangan Implementasi ISO 27001:2013 Menggunakan Indeks Keamanan Informasi 3:2015 Pada UPT. PPTI Universitas Negeri Surabaya (Yustanti, Bisma, Qoiriah, dan Prihanto, 2018). tujuan dari penelitian ini adalah untuk memastikan bahwa tingkat keamanan informasi yang diterapkan telah memenuhi standar ISO 27001: 2013, dimana penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) sebagian besar sudah menjadi kebutuhan dan tuntutan untuk setiap organisasi penyelenggara pelayanan publik. Dari hasil analisa yang didapatkan bahwa pada sistem elektronik yang digunakan dalam kegiatan operasiona di Universitas Negeri Surabaya sudah termasuk dalam kategori strategis, namun pada pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi dan pengelolaan asset keamanan informasi. Ketiga area masih dalam kategori I sampai II yang artinya secara kelengkapan dan kematangan masih banyak yang harus diperbaiki.

Penelitian lain dengan judul *Information Security Readiness of Government Institution in Indonesia* (Kautsarina dan Gautama, 2014). Pada penelitian tersebut memperoleh gambaran status keamanan informasi di Indonesia, sektor pemerintah khususnya, dari tahun 2011 sampai tahun 2013 dan hasil penelitian tersebut menunjukkan bahwa di instansi pemerintah 3% yang mendekati untuk memenuhi standar sementara, dan yang lain masih membutuhkan banyak perbaikan. Berdasarkan hasil yang di temukan bahwa sebagian besar organisasi berfokus pada teknologi, tetapi mengabaikan manajemen risiko dan manajemen keamanan

layanan TI, Karena tata kelola organisasi yang baik telah menjadi kebutuhan untuk mereformasi institusi pemerintah. Salah satu upaya yang dilakukan adalah pembangunan pemerintah elektronik adalah untuk meningkatkan kualitas pelayanan publik. Dengan demikian, sumber informasi yang diperlukan untuk memastikan bahwa sumber daya ini dilindungi dengan baik dalam rangka memenuhi aspek keamanan informasi untuk memberikan informasi berkualitas tinggi. Tetapi pada kenyataannya, ada banyak kasus menunjukkan bahwa sumber daya pemerintah diserang dan tidak aman.

Berdasarkan pada permasalahan penelitian yang telah dilakukan dan permasalahan yang ditemukan di Kampus Universitas Teknologi Mataram, pada penelitian ini akan diukur tingkat kategori sistem elektronik yang digunakan di Universitas Teknologi Mataram serta lima area pengeloaan keamanan informasi dalam hal tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi serta penggunaan teknologi dalam keamanan informasi dalam hal mengukur tingkat kesiapan Universitas Teknologi Mataram dalam menerapkan ISO 27001:2013 yang merupakan standar internasional yang mengatur tentang manajemen keamanan informasi.

1.2. Rumusan Masalah

Dari uraian latar belakang diatas, dapat dirumuskan beberapa poin yang menjadi masalah-masalah, sehingga dilakukan penelitian ini:

a. Berapa tingkat kesiapan penerapan keamanan sistem manajemen informasi berbasis indeks keamanan informasi pada Universitas Teknologi Mataram?
b. Bagaimana merekomendasikan untuk meningkatkan manajemen keamanan sistem informasi yang ada di Universitas Teknologi Mataram?

1.3. Batasan Masalah

Dari masalah yang diangkat, penulis memberikan batasan masalah agar fokus penelitian tidak terlalu luas. Beberapa batasan masalahnya antara lain:

a. Mengukur tingkat kesiapan penerapan keamanan sistem manajemen informasi berbasis Indeks Keamanan Informasi pada Universitas Teknologi Mataram.
b. Menggunakan Indeks Keamanan Informasi (KAMI) versi 4.1.
c. Data yang digunakan adalah hasil wawancara dan analisis dokumen pada Badan Pengelola Sistem Informasi (BPSI) Universitas Teknologi Mataram.
d. Penilaian keamanan informasi meliputi tingkat kematangan dalam penerapan pengelolaan keamanan informasi.
e. Saran perbaikan area keamanan informasi mengacu pada standar ISO/IEC 27001:2013.

1.4. Tujuan Penelitian

Berdasarkan hasil rumusan masalah dan batasan masalah yang telah disebutkan sebelumnya, maka tujuan yang dicapai dari penelitian ini adalah sebagai berikut:

a. Mengetahui tingkat kesiapan Universitas Teknologi Mataram dalam menerapkan keamanan sistem manajemen informasi.
b. Mengetahui tingkat kategori Sistem Elektronik yang digunakan pada Universitas Teknologi Mataram.
c. Memberikan usulan perbaikan keamanan informasi kepada pihak Badan Pengelola Sistem Informasi (BPSI) Universitas Teknologi Mataram dalam Keamanan Informasi yang harus dijalankan.

1.5. Manfaat Penelitian

Adapun manfaat yang dapat dirasakan dalam melakukan kegiatan penelitian ini, antara lain:

a. Membantu pihak kampus untuk mengetahui kondisi saat ini terkait sistem manajemen keamanan informasi dan memberikan gambaran terkait tindak lanjut dalam meningkatkan keamanan pada sistem informasi yang dimiliki Universitas Teknologi Mataram.
b. Memberikan gambaran kepada kampus mengenai tata kelola teknologi informasi yang baik.
c. Membantu kampus dalam mengawasi manajemen keamanan sistem informasi yang sedang berjalan.
d. Bagi peneliti dapat menambah wawasan pengetahuan.

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

Beberapa hasil penelitian yang digunakan sebagai acuan untuk penelitian ini antara lain:

Penelitian dari Hambali & Musa (2020), yang melakukan penelitian tentang analisis keamanan sistem manajemen informasi menggunakan Indeks Keamanan Informasi (KAMI). Tujuan dari penelitian ini adalah mengukur tingkat kesiapan keamanan informasi yang memenuhi persyaratan standar ISO/IEC 27001:2013 di Unit X Instansi Pemerintah Pusat sehingga menghasilkan kesimpulan kondisi tingkat pengamanan sudah diterapkan walapun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif, dan Indeks KAMI yang digunakan masih versi 4.0.

Pada penelitian yang dilakukan oleh Juliharta (2018), dalam penelitian Analisa Tingkap Kesiapan Penerapan Keamanan Teknologi Informasi dalam Pelaksanaan E-Government Berbasis Indeks Keamanan Informasi (KAMI) di Pemerintah Kota Kediri dapat disimpulkan bahwa penerapan yang dilakukan oleh Pemerintah Kota Kediri masuk ke dalam katagori tidak layak, terutama di bidang pengelolaan resiko dengan nilai 18. Skor Maksimal dari Indeks KAMI adalah 588 dan Pemerintah Kota kediri berada di Skor 308, dengan tingkat penggunaan Sistem Elektronik yang berada di level Tinggi. Dapat dikatakan sistem Keamanan yang

digunakan di Pemerintah Kota Kediri tidak memadai. Kelemahan dari penelitian ini adalah masih menggunakan Indeks KAMI versi 3.1.

Pada penelitian yang dilakukan oleh (Ferdiansyah et al., 2019), mengenai Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.0 Pada Lembaga UPTD XYZ dengan tujuan penelitian untuk mendapatkan informasi terkait tingkat kematangan dan kesiapan keamanan informasi. Kesimpulan dari penelitian ini adalah bahwa tingkat keamanan informasi masih sangat rendah dan diperlukan perbaikan sistem keamanan informasi dengan bekerja sama dengan pengembang keamanan informasi dari pihak ketiga.

Penelitian lain yang dilakukan oleh (Firzah A Basyarahil et al., 2017), dalam penelitian tersebut didapatkan hasil bahwa keamanan informasi dari DPTSI ITS Surabaya berada dalam tidak layak, dimana peneliti memberikan rekomendasi berdasarkan ISO 27001 untuk dijadikan bahan pertimbangan dan evaluasi kepada pihak DPTSI untuk melakukan perbaikan dalam keamanan informasi.

Penelitian selanjutnya tentang Analisis Tingkat Kesiapan dan Kematangan Implementasi ISO 27001:2013 Menggunakan Indeks Keamanan Informasi 3:2015 Pada UPT. PPTI Universitas Negeri Surabaya (Yustanti et al., 2018), dari hasil analisa data yang dikumpulkan didapatkan bahwa sistem elektronik yang digunakan dalam kegiatan operasiona di Universitas Negeri Surabaya sudah termasuk dalam kategori strategis, artinya bahwa sebagian besar kegiatan layanan operasional akademik maupun non akademik bertumpu pada sistem elektronik. Berdasarkan ukuran dalam indeks KAMI disimpulkan bahwa area pengelolaan resiko, kerangka kerja keamanan dan pengelolaan asset keamanan informasi masih rendah yaitu pada

level I-II yang berarti masih perlu perbaikan untuk menuju kesiapan implementasi ISO 27001:2013.

Penelitian lainnya yang membahas keamanan informasi dilakukan oleh (Mahersmi et al., 2016) dengan melakukan identifikasi, menilai dan memitigasi risiko teknologi informasi yang dikelola oleh Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung menggunakan metode OCTAVE. Penelitian tersebut menghasilkan identifikasi risiko terhadap teknologi informasi dan memberikan rekomendasi mitigasi ISO 27001 kepada Dinas Perhubungan Komunikasi dan Informatika Kabupaten Tulungagung.

Dalam penelitian ini, kontribusi utama atau kontribusi keilmuannya menggunakan Indeks Keamanan Informasi (KAMI) versi 4.1 dimana pada versi ini terdapat penambahan area suplemen dimana pada area suplemen ini terdapat Tambahan pengukuran dilakukan untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (*Cloud Service*) dan Perlindungan Data Pribadi dan mengacu pada standar ISO/IEC 27001:2013.

Dalam penelitian ini juga digunakan beberapa penelitian terdahulu sebagai pedoman dan referensi dalam melaksanakan proses dalam penelitian, sebagai bahan tinjauan dalam penelitian ini akan dicantumkan beberapa hasil penelitian sebelumnya yang dilakukan oleh beberapa peneliti dan akan dicantumkan kontribusi utama dalam penelitian ini, seperti yang terdapat pada Tabel 2.1.

2.2. Keaslian Penelitian

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian
Analisis Tingkat Kesiapan Penerapan Keamanan Sistem Manajemen Informasi Menggunakan Indeks Kami Berdasarkan Standar ISO/IEC 27001:2013 Pada Universitas Teknologi Mataram (Studi Kasus: Kampus Universitas Teknologi Mataram)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Analysis of Governance Security Management Information System Using Indeks KAMI in Central Government Institution	Hambali, Purnawarman Musa, Jurnal Ilmiah Bidang Teknologi, Angkasa, 2020	Tujuan dari penelitian ini adalah untuk mengukur tingkat kesiapan keamanan informasi yang memenuhi persyaratan standar ISO/IEC 27001:2013 di unit kerja X Instansi Pemerintah Pusat	Kesimpulan dari penelitian ini adalah hasil skor pengukuran SE (Sistem Elektronik) pada Instansi Pemerintah Pusat adalah 30 dari total skor 50, yang artinya peran dan tingkat kepentingan TIK termasuk dalam kategori tinggi.	Pada penelitian berikutnya diharapkan adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif, dan Indeks KAMI yang digunakan masih versi 4.0, saran perbaikan pada area suplemen belum ada.	Pada penelitian Hambali dan Purnawarman Musa masih menggunakan metode Indeks KAMI versi 4.0 sedangkan pada penelitian yang akan dilakukan menggunakan metode Indeks KAMI versi 4.1. Penelitian dilakukan di instansi pendidikan secara menyeluruh bukan hanya pada divisi/ bagian tertentu. Metode penilaian yang digunakan berbeda, dimana pada penelitian selanjutnya akan dilakukan penilaian secara langsung oleh peneliti.

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
2	Analisis Tingkat Kesiapan Pengamanan Sistem Informasi (Studi Kasus UPN Veteran Jakarta)	Nurhafifah Matondang, Bayu Hananto, Catur Nugrahaeni, Jurnal Teknologi Informasi dan Pendidikan (JTIP), 2019	Tujuan dari penelitian ini adalah untuk melakukan pengukuran level tingkat pengamanan sistem informasi untuk melihat kematangan dari sebuah sistem informasi pada UPN Veteran Jakarta.	Kesimpulan dari penelitian ini adalah tingkat ketergantungan UPNVJ terhadap teknologi sangat tinggi tetapi masih perlu banyak pembenahan diberbagai bidang aspek.	Untuk penelitian berikutnya perlu meningkatkan pengamanan sistem terutama untuk mengurangi risiko yang akan terjadi.	Penelitian Nurhafifah Matondang, Bayu Hananto dan Catur Nugrahaeni masih menggunakan Indeks KAMI 3.1 dan pengukuran hanya masih di liga area saja belum dilakukan pengukuran di area suplemen sedangkan pada penelitian yang akan dilakukan dalam penelitian ini mencangkup disemua area yang terdiri dari Kategori SE, Tata Kelola, Pengelolaan Risiko Keamana Informasi, Kerangka Kerja, Pengelolaan Aset, Teknologi dan Keamanan Informasi, dan Suplemen.
3	Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus di PUSTIPD UIN Raden Fatah Palembang	Catur Eri Gunawan, Fenando, Jurnal Sistem Informasi (JUSIFO), 2018	Penelitian ini bertujuan untuk melakukan penilaian secara internal terhadap sistem manajemen keamanan informasi di PUSTIPD UIN Raden Fatah Palembang.	Hasil dari pengukuran tingkat penggunaan Sistem Elektronik yaitu: sebesar 25 (dua puluh lima) dari jumlah total keseluruhan sebesar 50 (lima puluh). Hal ini menunjukkan bahwa tingkat ketergantungan terhadap penggunaan	Pada penelitian berikutnya diharapkan seluruh area yang dinilai dalam Indeks Keamanan Informasi (KAMI) sudah terpenuhi dan sesuai dengan ISO/IEC 27001. Hasil yang diperoleh dari evaluasi ini menunjukkan bahwa	Perbedaan dari penelitian yang dilakukan oleh Catur Eri Gunawan dan Fenando adalah belum semua area dapat dilakukan atau terpenuhi penilain dalam Indeks Keamanan Informasi (KAMI) dan standar ISO yang digunakan masih 27001, sedangkan pada penelitian

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
				Sistem Elektronik di Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPD) Universitas Islam Negeri Raden Fatah Palembang termasuk dalam kategori Tinggi. Hal ini menjelaskan bahwa penggunaan Sistem Elektronik merupakan bagian yang sangat penting dan tidak dapat dipisahkan dengan proses kerja yang dijalankan.	penilaian hanya sampai pada kategori kerangka kerja dasar, dan sebagian area sudah pada kategori proses penerapan.	yang akan dilakukan saat ini akan mengevaluasi disemua area kategori Indeks Keamanan Informasi agar penilain terpenuhi dan standar yang digunakan sudah 27001:2013.
4	Analisa Tingkap Kesiapan Penerapan Keamanan Teknologi Informasi dalam Pelaksanaan E-Government Berbasis Indeks Keamanan Informasi (KAMI) Studi Kasus Pemerintah Kota Kediri	I Gede Putu Krisna Juliharta, Jurnal Teknologi Informasi dan Komputer, 2019.	Untuk menghasilkan tingkat kematangan keamanan informasi di Pemerintah Kota Kediri, yang nantinya akan dievaluasi dan digunakan sebagai referensi untuk meningkatkan	Penerapan atau tingkat kematangan keamanan sistem di Pemerintah Kota Kediri masuk ke dalam katagori tidak layak, terutama di bidang pengelolaan resiko dengan nilai 18. Skor Maksimal dari Indeks KAMI adalah 588 dan Pemerintah	Pemerintah Kota Kediri perlu meningkatkan pengelolaan sistem yang dimiliki.	Penelitian yang dilakukan Juliharta masih menggunakan metode Indeks KAMI versi 3.1 dan hanya mengevaluasi di lima area sedangkan pada penelitian yang akan dilakukan menggunakan metode Indeks KAMI versi 4.1.

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			tingkat keamanan informasi Pemerintah Kota Kediri.	Kota kediri berada di Skor 308. Dengan tingkat penggunaan Sistem Elektronik yang berada di level Tinggi. Dapat dikatakan sistem Keamanan yang digunakan di Pemerintah Kota Kediri tidak memadai.		
5	Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.0 Pada Lembaga UPTD XYZ	Pramudhita Ferdiansyah, Subektiningsih, Rini Indrayani, Jurnal Mobile and Forensics (MF), 2019.	untuk melakukan evaluasi kematangan keamanan informasi pada UPTD XYZ berdasarkan standar ISO/IEC 27001:2013 dengan menggunakan indeks keamanan informasi (KAMI) versi 4.	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.	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.	Penelitian yang dilakukan Pramudhita Ferdiansyah, Subektiningsih dan Rini Indrayani masih menggunakan metode Indeks KAMI versi 4.0 sedangkan pada penelitian yang akan dilakukan menggunakan metode Indeks KAMI versi 4.1
6	Evaluasi Keamanan Informasi pada Dinas Komunikasi dan	Nofry Arman, Widhy Hayuhardhika	Tujuan dari penelitian ini adalah untuk meningkatkan	Tingkat kelengkapan terhadapa keamanan	Hasil dari penelitian menunjukkan bahwa	perbedaan dari penelitian ini dan penelitian yang akan diangkat adalah penelitian

Tabel 2.1. Matriks Literatur Review dan Posisi Penelitian (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
	Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI)	Nugraha Putra, Aditya Rachmadi, Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2019.	kualitas keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo	informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo berada pada area berwarna kuning yang berarti masuk dalam kategori "Perlu Perbaikan" dengan skor sebesar 334, Dikarenakan masih terdapat syarat keamanan informasi yang belum diterapkan atau masih dalam status perencanaan. Sedangkan pada tingkat kematangan disetiap area keamanan informasi Dinas Komunikasi dan Informatika Kabupaten Sidoarjo berada pada level II	terdapat kontrol ISO 27001:2013 yang belum terpenuhi berdasarkan area pada Indeks KAMI.	saat ini akan melakukan evaluasi disemua area kategori Indeks KAMI.

2.3. Landasan Teori

2.3.1. Keamanan Informasi

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

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

a. *Physical security*, keamanan yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
b. *Personal security*, keamanan yang overlap dengan *physical security* dalam melindungi orang-orang dalam suatu organisasi.
c. *Operational security*, keamanan yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
d. *Communications security*, keamanan yang bertujuan untuk mengamankan media komunikasi, teknologi komunikasi beserta isinya, dan kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan sebuah organisasi.

e. *Network security*, keamanan yang memfokuskan pada pengamanan peralatan jaringan dan organisasi, jaringan dan isinya, beserta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi tersebut.

2.3.2. Sistem Manajemen Keamanan Informasi (SMKI)

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

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

Penerapan Sistem Manajemen Keamanan Informasi pada sebuah organisasi juga harus memiliki pedoman yang ditujukan pada pimpinan organisasi. Hal ini telah dinyatakan olehDirektorat Sistem Informasi pada tahun 2007 bahwa telah ditetapkan 10 pedoman terbaik untuk penerapan SMKI, namun tidak menutup

kemungkinan untuk terjadi perubahan pada pedoman-pedoman yang telah ada. Berikut ini adalah 10 pedoman yang disebutkan:

a. Pedoman 1 tentang manajemen umum.
b. Pedoman 2 tentang kebijakan keamanan yang memenuhi sasaran bisnis.
c. Pedoman 3 tentang manajemen risiko keamanan informasi yang mengidentifikasi aset kritis diantaranya sistem, jaringan, dan data.
d. Pedoman 4 tentang arsitektur & desain keamanan berdasar kebutuhan bisnis dan perlindungan aset informasi paling kritis.
e. Pedoman 5 tentang isu-isu pengguna yang meliputi akuntabilitas & pelatihan serta ekspertis yang memadai.
f. Pedoman 6 tentang manajemen sistem & jaringan yang meliputi kontrol akses untuk melindungi aset dalam jaringan, integritas *software*, konfigurasi aset, dan *backup* yang terjadwal.
g. Pedoman 7 tentang otentikasi & otorisasi bagi pengguna aset dan pihak ketiga (kontraktor & penyedia layanan).
h. Pedoman 8 tentang pengawasan & audit terhadap kondisi sistem dan jaringan yang ada.
i. Pedoman 9 tentang keamanan fisik aset informasi dan layanan serta sumber daya TI.
j. Pedoman 10 tentang rencana keberlanjutan bisnis & pemulihan bencana untuk aset kritis dan dilakukannya tes secara periodik dan pastikan berfungsi secara efektif.

2.3.3. Manajemen Risiko Teknologi Informasi

Manajemen risiko merupakan serangkaian aktivitas dalam menganalisis risiko. Risiko tersebut diidentifikasi, dinililai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi risiko tersebut (Stoneburner, 2002).

Tujuan utama dari dilaksanakannya manajemen risiko adalah memberikan pandangan terkait kemungkinan yang bisa terjadi sehingga perusahaan dapat menyusun langkah mitigasi dan evaluasi terkait risiko. Tahapan dalam manajemen risiko berdasarkan (Spremic, 2008) diantaranya:

a. Mengidentifikasi dan mengklarifikasi risiko.
b. Setiap risiko dinilai.
c. Menyusun langkah penaggulangan risiko.
d. Pendokumentasian dan pengimplementasian dari langkah menanggulangi risiko.
e. Pendekatan portfolio risiko TI.
f. Monitoring berkala terhadap tingkat risiko TI dan audit.

2.3.4. ISO/IEC 27001 sebagai Standar SMKI

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

SMKI merupakan sebuah pendekatan yang bersifat sistematis yang bertujuan untuk mengelola informasi penting maupun informasi perusahaan yang

bersifat sensitif agar tetap aman. SMKI ini juga memberikan panduan untuk mengelola unsur yang termasuk dalam melakukan pengelolaan informasi penting seperti manusia, proses dan sistem Teknologi Informasi dengan menerapkan proses manajemen risiko yang telah sesuai standar. ISO 27001 telah dirancang sedemikian rupa sehingga dapat disesuaikan dalam pengaplikasiannya pada organisasi kecil, menengah hingga organisasi besar di sektor apapun dalam rangka melindungi aset informasi penting organisasi tersebut.

2.3.5. Indeks Keamanan Informasi (KAMI)

Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Aspek Teknologi dengan suplemen Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi. Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi.

Alat evaluasi Indeks KAMI dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya. Evaluasi yang dilakukan dengan menggunakan indeks KAMI ini mencakup beberapa target area, yaitu: Kategori Sistem Elektronik, Tata Kelola Keamanan Informasi, Pengelolaan Risiko

Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi, dan Suplemen.

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 berikut (BSSN 2019).

Tabel 2.2. Kategori Sistem Elektronik

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

Pengelompokan data berikutnya dilakukan berdasarkan pada tingkat kematangan penanganan keamanan dengan kategorisasi yang mengacu pada tingkat kematangan yang digunakan oleh COBIT atau CMMI (BSSN 2019). Tingkat kematangan pada indeks KAMI versi 4.1 didefinisikan dalam 5 kategori, yaitu:

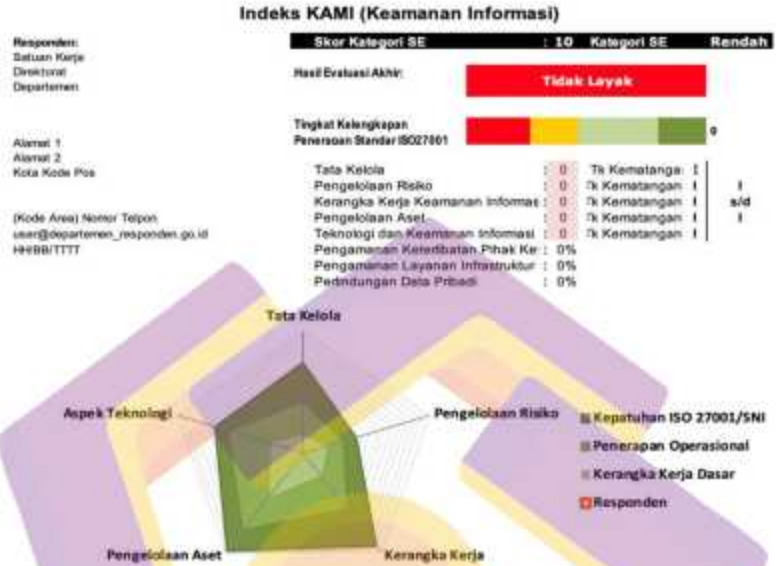
- Tingkat I – Kondisi Awal
- Tingkat II – Penerapan Kerangka Kerja Dasar
- Tingkat III – Terdefinisi dan Konsisten

- Tingkat IV – Terkelola dan Terukur
- Tingkat V – Optimal

Tingkat kematangan tersebut masih ditambah 4 kategori sebagai uraian yang lebih detail, yaitu tingkat I+, II+, III+, dan IV+, sehingga terdapat 9 tingkat kematangan. 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 2.1.

Gambar 2.1. Tingkat Kematangan Kesiapan Sertifikasi ISO 27001

Setelah mengklasifikasikan Peran Sistem Elektronik di instansi terkait, maka akan dilakukan penilaian terhadap kelima area yang ada di Indeks KAMI versi 4.1. Hasil penilaian menggunakan Indeks KAMI versi 4.1 akan digambarkan kedalam diagram yang berbentuk jaring laba-laba (spider chart) dengan 5 area utama. Dalam diagram jaring laba-laba tersebut juga akan dilihat tentang nilai Indeks KAMI dengan kepatuhan terhadap ISO/IEC 27001:2013. Hasil evaluasi menggunakan indeks KAMI versi 4.1 dapat dilihat melalui Gambar 2.2.



Gambar 2.2. Penilaian Indeks KAMI

Semakin tinggi ketergantungan sebuah instansi terhadap Peran SE, maka semakin banyak bentuk pengamanan yang diperlukan dan harus diterapkan sampai tahap tertinggi.

BAB III

METODE PENELITIAN

3.1. Jenis, Sifat, dan Pendekatan Penelitian

Pada penelitian ini menggunakan metode penelitian yang bersifat deskriftif kualitatif artinya laporan pelaksanaan penelitian disampaikan dalam bentuk deskriptif yang bersifat eksploratif artinya dilakukan dengan cara menggali informasi dari pihak pengelola informasi untuk mengetahui kematangan keamanan yang berlangsung di institusi tersebut.

3.2. Metode Pengumpulan Data

Pada tahap ini akan dilakukan pengumpulan data-data terkait dengan penilitian yang akan dikerjakan. Data yang didapat ini berasal dari Kampus Universitas Teknologi Mataram. Data akan didapatkan selama melakukan wawancara dan observasi secara langsung oleh peneliti. Data yang akan diperoleh adalah bukti pendukung berupa dokumen-dokumen yang dapat memperkuat pernyataan dari pihak yang diwawancara.

3.3. Metode Analisis Data

Dalam metode analisis data yang digunakan untuk melakukan penelitian penulis menggunakan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013.

3.4. Alur Penelitian

Tahapan penelitian dalam melakukan analisis kesiapan keamanan sistem dan teknologi informasi dengan menggunakan indeks keamanan informasi berdasarkan ISO/IEC 27001:2013 mengacu pada penelitian dari (Hambali, 2020). Penelitian diawali dengan melakukan identifikasi masalah dan studi literatur terkait dengan analisis kesiapan keamanan sistem dan keamanan informasi. Langkah berikutnya yaitu studi lapangan untuk pengumpulan data dengan melakukan interview kepada pengelola Sistem Informasi 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 usulan dan saran perbaikan sistem keamanan informasi pada Kampus Universitas Teknologi Mataram berdasarkan ISO/IEC 27001. Proses alur penelitian ditunjukkan gambar dibawah ini.

Gambar 3.1. Alur Penelitian

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Gambaran Sistem yang Dievaluasi

Dalam rangka menjalankan roda organisasi, Universitas Teknologi Mataram mempunyai BAAK yang bertugas untuk memberikan layanan teknis dan administrasi, dalam prosesnya membutuhkan sistem informasi akademik secara *online*/jaringan internet. Untuk memenuhi tugas tersebut BAAK bekerja sama dengan BPSI (Badan Pengelola Sistem Informasi) untuk Mengembangkan Teknologi Informasi SIAKAD. Teknologi informasi diaplikasikan dalam suatu organisasi/institusi akan mempengaruhi seberapa jauh organisasi/institusi tersebut telah mencapai visi dan misi ataupun tujuan strategisnya. Oleh karena itu Universitas Teknologi Mataram menggunakan SIAKAD untuk pengolah data akademik mahasiswa, data dosen dan pegawai serta keuangan. Untuk menjaga data dan informasi perguruan tinggi dengan baik terhadap ancaman dari berbagai lubang keamanan. Diharapkan hasil dari pengukuran dan evaluasi menggunakan indeks KAMI dapat digunakan Univeritas Teknologi Mataram sebagai media evaluasi dan perbaikan dalam hal keamanan sitem informasi dan jaringan.

4.2. Hasil Penilaian Penggunaan Sistem Elektronik Pada Kampus Universitas Teknologi Mataram

Proses klasifikasi dilakukan terhadap penggunaan Sistem Elektronik (SE) dalam instansi atau cakupan evaluasinya. Tujuan dari proses ini adalah untuk mengelompokkan instansi kedalam ukuran tertentu: Rendah, Tinggi, dan Strategis.

Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik penggunaan Sistem Elektronik yang spesifik. Hasil pengelompokan tadi didapat dari penjumlahan semua nilai kriteria yang didapat dari setiap pertanyaan yang disuguhkan terkait kategori Sistem Elektronik. Untuk mengetahui seberapa besar peran penggunaan Sistem Elektronik dalam instansi tersebut, maka akan diberikan 10 pertanyaan yang dapat menggambarkan hal tersebut. Setiap pertanyaan akan mempunyai 3 kriteria penilaian, berikut adalah tabel kriteria pertanyaan kategori Sistem Elektronik:

Tabel 4.1. Kriteria Pertanyaan Kategori Elektronik

Kriteria	Nilai
A	5
B	2
C	1

Berikut ini adalah hasil dari penilaian tingkat kepentingan penggunaan Sistem Elektronik pada Kampus Universitas Teknologi Mataram:

Tabel 4.2. Hasil Penilaian Penggunaan Sistem Elektronik Kampus Universitas Teknologi Mataram

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**	Skor
#	**Karakteristik Instansi/Perusahaan**		
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	C	1

Tabel 4.2. Hasil Penilaian Penggunaan Sistem Elektronik Kampus Universitas Teknologi Mataram (Lanjutan)

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**	Skor
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	B	2
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	B	2
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi	B	2
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	B	2
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	A	5
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	A	5

Tabel 4.2. Hasil Penilaian Penggunaan Sistem Elektronik Kampus Universitas Teknologi Mataram (Lanjutan)

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
	[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	**Status**	Skor
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	B	2
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	C	1
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	C	1
	Skor penetapan Kategori Sistem Elektronik	**23**	

Dari hasil penilaian tingkat kepentingan penggunaan Sistem Elektronik pada Kampus Universitas Teknologi Mataram telah didapatkan skor penetapan Kategori Sistem Elektronik sebesar 23, sehingga tingkat ketergantungan termasuk dalam kategori Tinggi sesuai dengan tabel tingkat kematangan Indeks KAMI versi 4.1 dimana kategori Tinggi berkisar antara skor 16 sampai dengan 34. Maksud dari kategori Tinggi disini yaitu kepentingan penggunaan Sistem Elektronik pada

Kampus Universitas Teknologi Mataram merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan. Penggunaan sistem elektronik ini mendapat nilai yang tinggi karena kewajiban kepatuhan terhadap Peraturan atau Standar Nasional, menggunakan teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri untuk keamanan informasi dalam Sistem Elektronik, pengguna sistem elektronik juga berkisar antara 1.000 sampai dengan 5.000 pengguna, keterhubungan data pribadi yang diolah terkait dengan data pribadi lainnya, tingkat klasifikasi atau kekritisan Data yang ada dalam Sistem Elektronik sangat rahasia dan dampak dari kegagalannya juga dapat berdampak secara tidak langsung dan potensi kerugiannya mengakibatkan gangguan operasional sementara.

4.3. Penilaian Kesiapan Area Keamanan Informasi Pada Kampus Universitas Teknologi Mataram

Proses penilaian dilakukan dengan 2 (dua) metode, yang pertama jumlah (kelengkapan) bentuk pengamanan dan yang kedua tingkat kematangan proses pengolahan pengamanan informasi. Metode pertama akan mengevaluasi sejauh mana Bidang Teknologi Informasi dan Sistem Informasi (TISI) sesuai dengan standar ISO 27001:2013 (Kominfo, 2011). Terdapat lima area keamanan informasi antara lain sebagai berikut:

I : Tata Kelola Keamanan Informasi

II : Pengelolaan Risiko Keamanan Informasi

III : Kerangka Kerja Keamanan Informasi

IV : Pengelolaan Aset Informasi

V : Teknologi dan Keamanan Informasi

Metode yang kedua merupakan perluasan dari evaluasi kelengkapan dan digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT (*Control Objective for Information and related Technology*) atau CMMI (*Capability Maturity Model for Integration*). Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi pada Kampus Universitas Teknologi Mataram. Setiap kategori pertanyaan pada area keamanan informasi meliki nilai skor yang berbeda-beda. Berikut adalah tabel pemetaan skor Indeks KAMI berdasarkan masing-masing kategori:

Tabel 4.3. Matriks Skor Pemetaan Pengamanan

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

(Sumber: Kominfo, 2017)

4.3.1. Hasil Penilaian Tata Kelola Keamanan Informasi

Penilaian Tata Kelola Keamanan Informasi yang ada pada Kampus Universitas Teknologi Mataram Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Tata Kelola Keamanan Informasi sebesar 83. Hasil lengkapnya dapat dilihat pada tabel 4.4 berikut ini.

Tabel 4.4. Hasil Penilaian Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Fungsi/Organisasi Keamanan Informasi**		
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian	2
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.4. Hasil Penilaian Tata Kelola Keamanan Informasi (Lanjutan)

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Penerapan / Diterapkan Sebagian	2
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Diterapkan Secara Menyeluruh	6
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan	Dalam Penerapan / Diterapkan Sebagian	4

Tabel 4.4. Hasil Penilaian Tata Kelola Keamanan Informasi (Lanjutan)

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
			pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?		
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Diterapkan Secara Menyeluruh	6
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian	4
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Diterapkan Secara Menyeluruh	6
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Diterapkan Secara Menyeluruh	9
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan	0
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0

Tabel 4.4. Hasil Penilaian Tata Kelola Keamanan Informasi (Lanjutan)

Bagian II: Tata Kelola Keamanan Informasi					
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Diterapkan Secara Menyeluruh	9
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian	6
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Tata Kelola	**83**	

Pada Tabel 4.5 akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 8 bernilai 19, sedangkan untuk pertanyaan tahap 2 dengan jumlah 8 bernilai 34 dari hasil yang diperoleh, maka jumlah nilai untuk tahap penerapan 1 dan 2 berjumlah 53.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal tahap penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Tata Kelola yaitu 48. Jumlah skor pada tahap penerapan 1 dan 2 adalah 53 sehingga

dapat disimpulkan bahwa skor melebihi dari tahapan penerapan 3, maka dari itu bagian Tata Kelola dapat disimpulkan Status Penilaian Tahap Penerapan 3 adalah Valid.

Tingkat Kelengkapan (Valid/Tidak Valid)	=	Jika (Total Skor Tahap Penerapan 1&2) >= (Batas Skor Min untuk Skor Tahap Penerapan 3)

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	53
Status Penilaian Tahapan Penerapan 3	Valid

Tabel 4.5. Tingkat Kelengkapan Tata Kelola Keamanan Informasi

Kategori (Tahapan)	Pertanyaan Tata Kelola	Nilai
1	8	19
2	8	34
3	6	30
Total	22	83

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan tata kelola keamanan informasi yang akan menentukan tingkat kematangan pada bagian tersebut. Semakin tinggi nilai tingkat kelengkapan tata kelola keamanan informasi, maka semakin tinggi pula tingkat kematangan tata kelola keamanan informasi. Tabel 4.6 berikut ini akan dijelaskan tingkat kematangan tata kelola keamanan informasi:

Tabel 4.6. Tingkat Kematangan Tata Kelola Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Tata Kelola	Nilai	Tingkat Validasi Kematangan
II	13	37	II
III	3	16	No
IV	6	30	No
Total	22	83	

Pada area tata kelola keamanan informasi, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+, namun hasil dari tabel tata kelola keamanan informasi hanya valid ditingkat kematangan II, yang artinya dalam kondisi tingkat Penerapan Kerangka Kerja Dasar (Aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

Area Tata kelola Keamanan Informasi ini mendapat point 83 dari 126 dimana poin ini terbilang lumayan baik karena kampus Universitas Teknologi Mataram hanya belum menerapkan:

a. Pengidentifikasian data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku
b. Pendefinisian metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporan
c. Program penilaian kinerja pengelolaan keamanan informasi bagi individu

4.3.2. Hasil Penilaian Pengelolaan Risiko Keamanan Informasi

Penilaian Pengelolaan Risiko Keamanan Informasi yang ada pada Kampus Universitas Teknologi Mataram Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Pengelolaan Risiko Keamanan Informasi sebesar 55. Hasil lengkapnya dapat dilihat pada tabel 4.7 berikut ini.

Tabel 4.7. Hasil Penilaian Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Kajian Risiko Keamanan Informasi**		
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian	2
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Dalam Penerapan / Diterapkan Sebagian	2
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian	2
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Diterapkan Secara Menyeluruh	3

Tabel 4.7. Hasil Penilaian Pengelolaan Risiko Keamanan Informasi (Lanjutan)

Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Kajian Risiko Keamanan Informasi**		
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Penerapan / Diterapkan Sebagian	2
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian	2
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Penerapan / Diterapkan Sebagian	2
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.7. Hasil Penilaian Pengelolaan Risiko Keamanan Informasi (Lanjutan)

Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Kajian Risiko Keamanan Informasi**		
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Penerapan / Diterapkan Sebagian	4
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Penerapan / Diterapkan Sebagian	4
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Dalam Penerapan / Diterapkan Sebagian	4
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Penerapan / Diterapkan Sebagian	4
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Diterapkan Secara Menyeluruh	9
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Diterapkan Secara Menyeluruh	9
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**55**	

Pada Tabel 4.8 akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 10 bernilai 21 sedangkan untuk pertanyaan tahap 2 dengan jumlah 4 bernilai 16 dari hasil yang diperoleh, maka jumlah nilai untuk tahap penerapan 1 dan 2 berjumlah 37. Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal tahap penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Pengelolaan Risiko Keamanan Informasi yaitu 36. Jumlah skor pada tahap penerapan 1 dan 2 adalah 37 sehingga dapat disimpulkan bahwa skor melebihi dari Tahapan Penerapan 3, maka dari itu status bagian Pengelolaan Risiko Peniliaian Tahap Penerapan 3 adalah Valid.

Tingkat Kelengkapan (Valid/Tidak Valid)	=	Jika (Total Skor Tahap Penerapan 1&2) >= (Batas Skor Min untuk Skor Tahap Penerapan 3)
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		37
Status Penilaian Tahapan Penerapan 3		Valid

Tabel 4.8. Tingkat Kelengkapan Pengelolaan Risiko Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Resiko	Nilai
1	10	21
2	4	16
3	2	18
Total	16	55

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan pengelolaan risiko keamanan informasi yang akan menentukan tingkat kematangan pada bagian tersebut. Semakin tinggi nilai tingkat kelengkapan pengelolaan risiko keamanan informasi, maka semakin tinggi pula tingkat kematangan pengelolaan risiko keamanan informasi. Tabel 4.9 berikut ini akan dijelaskan tingkat kematangan pengeloaan risiko keamanan informasi:

Tabel 4.9. Tingkat Kematangan Pengelolaan Risiko Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Pengelolaan Resiko	Nilai	Tingkat Validasi Kematangan
II	10	21	II
III	2	8	No
IV	2	8	No
V	2	18	No
Total	16	55	

Pada area Pengeloaan Risiko Keamanan informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi penerapan kerangka kerja dasar (aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

Area Pengelolaan Risiko Keamanan Informasi ini mendapat poin 55 dari 72 dimana poin ini terbilang baik karena pihak Kampus Universitas Teknologi Mataram sudah menerapakan semua aspek pada area Pengelolaan Risiko Keamanan Informasi, walaupun ada beberapa yang masih dalam penerapan atau diterapkan sebagian.

4.3.3. Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi yang ada pada Kampus Universitas Teknologi Mataram Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Kerangka Kerja Pengelolaan Keamanan Informasi sebesar 61. Hasil lengkapnya dapat dilihat pada tabel 4.10 berikut ini.

Tabel 4.10 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Dalam Penerapan / Diterapkan Sebagian	2
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Diterapkan Secara Menyeluruh	3
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Diterapkan Secara Menyeluruh	3

Tabel 4.10 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	2
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh	3
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Dalam Perencanaan	1
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Penerapan / Diterapkan Sebagian	4
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	Dalam Penerapan / Diterapkan Sebagian	4

Tabel 4.10 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

(Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Dalam Perencanaan	2
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Dalam Penerapan / Diterapkan Sebagian	4
4.12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Diterapkan Secara Menyeluruh	6
4.13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Dalam Penerapan / Diterapkan Sebagian	4
4.14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Dalam Perencanaan	2
4.15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Dalam Penerapan / Diterapkan Sebagian	4

Tabel 4.10 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

(Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Penerapan / Diterapkan Sebagian	0
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Penerapan / Diterapkan Sebagian	0
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Penerapan / Diterapkan Sebagian	0
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan / Diterapkan Sebagian	0
#	**Pengelolaan Strategi dan Program Keamanan Informasi**				
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian	2
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian	2
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Dalam Perencanaan	1

Tabel 4.10 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.2.3	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Dalam Perencanaan	1
4.2.4	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Dalam Perencanaan	1
4.2.5	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
4.2.6	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	4
4.2.7	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Perencanaan	0
4.2.8	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Dalam Perencanaan	0

Tabel 4.10 Hasil Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
4.29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan	0
			Total Nilai Evaluasi Kerangka Kerja	**61**	

Pada Tabel 4.11 akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 12 bernilai 23, sedangkan untuk pertanyaan tahap 2 dengan jumlah 10 bernilai 38. Dari hasil yang diperoleh, maka jumlah nilai untuk tahap penerapan 1 dan 2 berjumlah 61.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal tahap penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI bagian Pengelolaan Kerangka Kerja yaitu 64. Jumlah skor pada tahap penerapan 1 dan 2 adalah 61, sehingga dapat disimpulkan bahwa jumlah skor di bawah Tahapan Penerapan 3, maka dari itu status bagian Kelengkapan Pengelolaan Kerangka Kerja Peniliaian Tahap Penerapan 3 adalah Tidak Valid.

Tingkat Kelengkapan (Valid/Tidak Valid)	=	Jika (Total Skor Tahap Penerapan 1&2) >= (Batas Skor Min untuk Skor Tahap Penerapan 3)

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	61
Status Penilaian Tahapan Penerapan 3	Tidak Valid

Tabel 4.11. Tingkat Kelengkapan Pengelolaan Kerangka Kerja Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Kerangka Kerja	Nilai
1	12	23
2	10	38
3	7	0
Total	29	61

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan kerangka kerja pengelolaan keamanan informasi yang akan menentukan tingkat kematangan pada bagian tersebut. Semakin tinggi nilai tingkat kelengkapan kerangka kerja pengelolaan keamanan informasi, maka semakin tinggi pula tingkat kematangan kerangka kerja pengelolaan keamanan informasi. Tabel 4.12 berikut ini akan dijelaskan tingkat kematangan kerangka kerja pengelolaan keamanan informasi:

Tabel 4.12. Tingkat Kematangan Pengelolaan Kerangka Kerja Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Kerangka Kerja	Nilai	Tingkat Validasi Kematangan
II	11	28	II
III	13	33	No
IV	3	0	No
V	2	0	No
Total	29	55	

Pada area Kerangka Kerja Keamanan informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi tingkat Penerapan Kerangka Kerja Dasar (Aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

Area Kerangka Kerja Pengelolaan Keamanan Informasi ini mendapat point 61 dari 159 dimana point ini terbilang lumayan baik karena pihak Kampus Universitas Teknologi Mataram masih dalam tahap perancanaan pada:

a. Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga
b. Penerapan kebijakan dan prosedur operasional
c. Proses untuk menanggulangi risiko dan jadwal penyelesaiaannya
d. Strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja
e. Melaksanakan program audit internal yang dilakukan oleh pihak independen
f. Rencana dan program peningkatan keamanan informasi untuk jangka menengah atau panjang.

4.3.4. Hasil Penilaian Pengelolaan Aset Informasi

Penilaian Pengelolaan Aset Informasi yang ada pada Kampus Universitas Teknologi Mataram Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Pengelolaan Aset sebesar 129. Hasil lengkapnya dapat dilihat pada tabel 4.13 berikut ini:

Tabel 4.13. Hasil Penilaian Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara? (Termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	3
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Dalam Penerapan / Diterapkan Sebagian	2
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Dalam Penerapan / Diterapkan Sebagian	2
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	2
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	2
5.7	II	1	Apakah tersedia proses untuk menilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian	2
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		

Tabel 4.13. Hasil Penilaian Pengelolaan Aset Informasi (Lanjutan)

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
5.8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Diterapkan Secara Menyeluruh	3
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Diterapkan Secara Menyeluruh	3
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Diterapkan Secara Menyeluruh	3
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Diterapkan Secara Menyeluruh	3
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Diterapkan Secara Menyeluruh	3
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Diterapkan Secara Menyeluruh	3
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian	2
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Penerapan / Diterapkan Sebagian	2
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian	2
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian	2
5.18	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.13. Hasil Penilaian Pengelolaan Aset Informasi (Lanjutan)

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian	4
5.20	III	2	Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian	4
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Dalam Penerapan / Diterapkan Sebagian	4
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Penerapan / Diterapkan Sebagian	4
5.23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Dalam Penerapan / Diterapkan Sebagian	4
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Penerapan / Diterapkan Sebagian	4
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Diterapkan Secara Menyeluruh	9
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Dalam Penerapan / Diterapkan Sebagian	6
5.27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Dalam Penerapan / Diterapkan Sebagian	6

Tabel 4.13. Hasil Penilaian Pengelolaan Aset Informasi (Lanjutan)

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Fisik**		
5.28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Dalam Penerapan / Diterapkan Sebagian	2
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Dalam Penerapan / Diterapkan Sebagian	2
5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Dalam Penerapan / Diterapkan Sebagian	2
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Dalam Penerapan / Diterapkan Sebagian	2
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Penerapan / Diterapkan Sebagian	2
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Dalam Penerapan / Diterapkan Sebagian	2
5.34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Dalam Penerapan / Diterapkan Sebagian	4

Tabel 4.13. Hasil Penilaian Pengelolaan Aset Informasi (Lanjutan)

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Diterapkan Secara Menyeluruh	6
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	4
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (Misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Dalam Penerapan / Diterapkan Sebagian	4
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Pengelolaan Aset	**124**	

Pada Tabel 4.14 akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 24 bernilai 55 sedangkan untuk pertanyaan tahap 2 dengan pertanyaan yang berjumlah 10 bernilai 42 dari hasil yang diperoleh, maka jumlah nilai untuk tahap penerapan 1 dan 2 berjumlah 97.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian

Pengelolaan Aset yaitu 88. Jumlah skor pada tahap penerapan 1 dan 2 adalah 97 sehingga dapat disimpulkan bahwa jumlah skor melebihi Tahapan Penerapan 3, maka dari itu status bagian Pengelolaan Aset Peniliaian Tahap Penerapan 3 adalah Valid.

Tingkat Kelengkapan (Valid/Tidak Valid)	=	Jika (Total Skor Tahap Penerapan 1&2) >= (Batas Skor Min untuk Skor Tahap Penerapan 3)

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	97
Status Penilaian Tahapan Penerapan 3	Valid

Tabel 4.14. Tingkat Kelengkapan Pengelolaan Aset Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Pengelolaan Aset	Nilai
1	24	55
2	10	42
3	4	27
Total	29	124

Nilai tingkat kelengkapan pada masing-masing kategori kelengkapan pengelolaan aset informasi yang akan menentukan tingkat kematangan pada bagian tersebut, semakin tinggi nilai tingkat kelengkapan kelengkapan pengelolaan aset informasi, maka semakin tinggi pula tingkat kematangan kelengkapan pengelolaan aset informasi. Tabel 4.15 berikut ini akan dijelaskan tingkat kematangan kelengkapan pengelolaan aset informasi:

Tabel 4.15. Tingkat Kematangan Pengelolaan Aset Informasi

Kategori Tingkat Kematangan	Pertanyaan Pengelolaan Aset	Nilai	Tingkat Validasi Kematangan
II	29	77	II
III	9	47	No
Total	38	124	

Pada area Pengelolaan Aset informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi tingkat Penerapan Kerangka Kerja Dasar (Aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

Area Pengelolaan Aset Informasi ini mendapat poin 124 dari 168 dimana poin ini terbilang lumayan baik karena pihak Kampus Universitas Teknologi Mataram sebagian besar masih dalam penerapan / diterapkan sebagian.

4.3.5. Hasil Penilaian Teknologi dan Keamanan Informasi

Penilaian Teknologi dan Keamanan Informasi yang ada pada Kampus Universitas Teknologi Mataram Pusat Bidang Teknologi Informasi dan Sistem Informasi (TISI) yang mana didapatkan total nilai evaluasi Teknologi dan Keamanan Informasi sebesar 93. Hasil lengkapnya dapat dilihat pada tabel 4.16 berikut ini.

Tabel 4.16. Hasil Penilaian Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi		
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.		
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**	Skor
# **Pengamanan Teknologi**		

Tabel 4.16. Hasil Penilaian Teknologi dan Keamanan Informasi (Lanjutan)

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Diterapkan Secara Menyeluruh	3
6.3	II	1	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 Penerapan / Diterapkan Sebagian	2
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
6.5	II	1	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
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Diterapkan Secara Menyeluruh	3
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Dalam Penerapan / Diterapkan Sebagian	2
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.16. Hasil Penilaian Teknologi dan Keamanan Informasi (Lanjutan)

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian	2
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Penerapan / Diterapkan Sebagian	2
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Diterapkan Secara Menyeluruh	3
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Diterapkan Secara Menyeluruh	6
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Penerapan / Diterapkan Sebagian	4
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Diterapkan Secara Menyeluruh	6
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Dalam Penerapan / Diterapkan Sebagian	4
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*, dan penarikan akses?	Dalam Penerapan / Diterapkan Sebagian	4

Tabel 4.16. Hasil Penilaian Teknologi dan Keamanan Informasi (Lanjutan)

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Penerapan / Diterapkan Sebagian	4
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	2
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Diterapkan Secara Menyeluruh	3
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Diterapkan Secara Menyeluruh	6
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Penerapan / Diterapkan Sebagian	4
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Diterapkan Secara Menyeluruh	6
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Dalam Penerapan / Diterapkan Sebagian	4
6.25	III	3	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Dalam Penerapan / Diterapkan Sebagian	6

Tabel 4.16. Hasil Penilaian Teknologi dan Keamanan Informasi (Lanjutan)

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Penerapan / Diterapkan Sebagian	6
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**93**	

Pada Tabel 4.17 akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 14 bernilai 33 sedangkan untuk pertanyaan tahap 2 dengan jumlah 10 bernilai 48 dari hasil yang diperoleh, maka jumlah nilai untuk tahap penerapan 1 dan 2 berjumlah 81.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Teknologi dan Keamanan Informasi yaitu 68. Jumlah skor pada tahap penerapan 1 dan 2 adalah 81 sehingga dapat disimpulkan bahwa jumlah skor melebihi Tahapan Penerapan 3, maka dari itu status bagian Teknologi dan Keamanan Informasi Peniliaian Tahap Penerapan 3 adalah Valid.

Tingkat Kelengkapan (Valid/Tidak Valid)	=	Jika (Total Skor Tahap Penerapan 1&2) >= (Batas Skor Min untuk Skor Tahap Penerapan 3)

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	81
Status Penilaian Tahapan Penerapan 3	Valid

Tabel 4.17. Tingkat Kelengkapan Teknologi dan Keamanan Informasi

Kategori Kontrol (Tahapan)	Pertanyaan Teknologi dan Keamanan Informasi	Nilai
1	14	33
2	10	48
3	2	12
Total	26	93

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan teknologi dan keamanan informasi yang akan menentukan tingkat kematangan pada bagian tersebut. Semakin tinggi nilai tingkat kelengkapan teknologi dan keamanan informasi, maka semakin tinggi pula tingkat kematangan teknologi keamanan informasi. Tabel 4.18 berikut ini akan dijelaskan tingkat kematangan Teknologi dan Keamanan Informasi:

Tabel 4.18. Tingkat Kematangan Teknologi dan Keamanan Informasi

Kategori Tingkat Kematangan	Pertanyaan Pengelolaan Aset	Nilai	Tingkat Validasi Kematangan
II	14	33	II
III	11	54	No
IV	1	6	No
Total	38	93	

Pada area Teknologi dan Keamanan informasi hanya valid ditingkat kematangan II yang artinya dalam kondisi penerapan kerangka kerja dasar (Aktif), pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

Area Teknologi dan Keamanan Informasi ini mendapat poin 93 dari 120 dimana poin ini terbilang baik karena pihak Kampus Universitas Teknologi Mataram sudah menerapakan semua aspek pada area Teknologi dan Keamanan Informasi, walaupun ada beberapa yang masih dalam penerapan atau diterapkan sebagian.

4.4. Penilaian Area Modul Suplemen Pada Kampus Universitas Teknologi Mataram

Untuk menilai kesiapan instansi atau perusahaan dalam mengelola risiko di 3 (tiga) area baru ini, pada Indeks KAMI versi 4.1 terdapat modul suplemen yang membahas aspek kesiapan pengamanan untuk ketiga aspek tersebut. Modul suplemen digunakan untuk menilai kesiapan pada Kampus Universitas Teknologi Mataram dalam mengelola risiko di 3 (tiga) untuk evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan dan Perlindungan Data Pribadi digunakan sesuai konteks atau cakupan yang ada. Responden hanya perlu menjawab area evaluasi yang berlaku. Hasil penilaian evaluasi kesiapan Pengamanan ketiga area tersebut disampaikan dalam bentuk persentase (%) dengan obyektif sesuai sasaran pencapaian maksimal. Hasil lengkapnya dapat dilihat pada tabel 4.19 di bawah ini.

Tabel 4.19. Hasil Penilaian Area Modul Suplemen

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7,1			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**		1,89
7.1.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.5		1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.1.1.7		1	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.2			**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**		
7.1.2.1		1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.2.3		1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.3			**Pengelolaan Layanan dan Keamanan Pihak Ketiga**		
7.1.3.1		1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	Diterapkan Secara Menyeluruh	3
7.1.3			**Pengelolaan Layanan dan Keamanan Pihak Ketiga**		
7.1.3.2		1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.1.3.3		1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.3.4		1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.3.5		1	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.3.6		1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.3.7		1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.3.8		1	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.4			**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**		
7.1.4.1		1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.1.4.2		1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Dalam Perencanaan	1
7.1.5			**Penanganan Aset**		
7.1.5.1		1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.5.2		1	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	Dalam Perencanaan	1
7.1.6			**Pengelolaan Insiden oleh Pihak Ketiga**		
7.1.6.1		1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	Dalam Perencanaan	1
7.1.6.2		1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Dalam Perencanaan	1
7.1.7			**Rencana Kelangsungan Layanan Pihak Ketiga**		
7.1.7.1		1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.7.2		1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Dalam Penerapan / Diterapkan Sebagian	2
7.1.7.3		1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Dalam Penerapan / Diterapkan Sebagian	2
7,2			**Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**		2,00

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.2.1		1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.2		1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.3		1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.4		1	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.5		1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.6		1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.7		1	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7.2.8		1	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.9		1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?	Dalam Penerapan / Diterapkan Sebagian	2
7.2.10		1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Dalam Penerapan / Diterapkan Sebagian	2
7,3			**Perlindungan Data Pribadi**		2,13
7.3.1		1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Diterapkan Secara Menyeluruh	3
7.3.2		1	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.3		1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.4		1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen				
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	Skor
7.3.5	1	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	Diterapkan Secara Menyeluruh	3
7.3.6	1	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.7	1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.8	1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.9	1	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.10	1	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.11	1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.12	1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Dalam Penerapan /	2

Tabel 4.19. Hasil Penilaian Area Modul Suplemen (Lanjutan)

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
				Diterapkan Sebagian	
7.3.13		1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.14		1	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.15		1	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?	Dalam Penerapan / Diterapkan Sebagian	2
7.3.16		1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Dalam Penerapan / Diterapkan Sebagian	2

Pada Tabel 4.20 akan dijelaskan bahwa hasil dari penilaian modul suplemen untuk mengetahui kesiapan pengamanan pada Kampus Universitas Teknologi Mataram dalam mengelola risiko Keterlibatan Pihak Ketiga adalah skor 1,89, Pengamanan Layanan Infrastrukutur Awan adalah skor 2 dan Perlindungan Data Pribadi adalah skor 2,13.

Untuk mengetahui kesiapan pengamanan dalam bentuk persentase pada Kampus Universitas Teknologi Mataram dalam mengelola risiko di 3 (tiga) area

modul suplemen dapat dilihat pada tabel 4.20. Syarat pemenuhan kesiapan pengamanan pada modul suplemen adalah 100% semua area terpenuhi.

Tabel 4.20. Hasil Persentase Penilaian Area Modul Suplemen

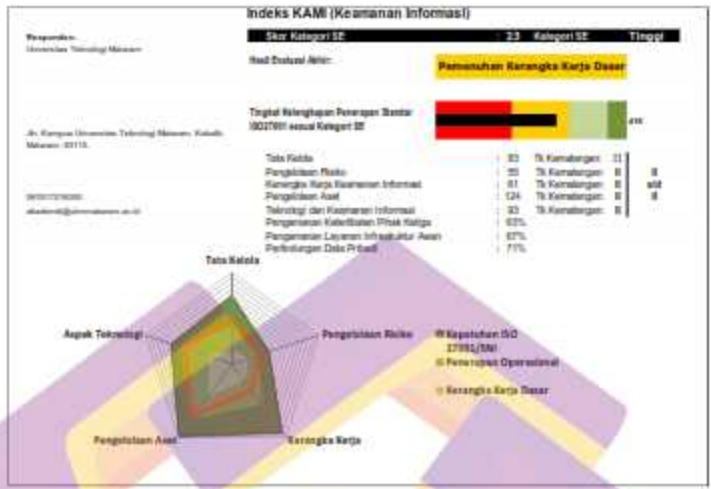
Area Modul Suplemen	Pertanyaan Area Modul Suplemen	Nilai	Persentase
Pengamanan Keterlibatan Pihak Ketiga	27	1,89	63%
Pengamanan Layanan Infrastrukutur Awan	10	2	67%
Perlindungan Data Pribadi	16	2,13	71%

Pada modul suplemen area Pengamanan Keterlibatan Pihak Ketiga dengan nilai 1.89, jika dipersentasikan menjadi 63%, area Pengamanan Layanan Infrastruktur Awan dengan nilai 2, jika dipersentasikan menjadi 67%, dan area Perlindungan Data Pribadi dengan nilai 2.13, jika dipersentasikan menjadi 71%, diantara ke 3 (tiga) area modul suplemen tidak ada yang mencapai 100%, sehingga dapat disimpulkan bahwa pada Kampus Universitas Teknologi Mataram belum memenuhi syarat kesiapan pengamanan pada modul suplemen karena nilai persentase masih berada di bawah 100%.

4.5. Pembahasan

4.5.1. Analisis Hasil Akhir Penilaian Indeks KAMI

Analisis hasil dari penilaian indeks KAMI pada Kampus Universitas Teknologi Mataram akan dijelaskan melalui tampilan dari *Dashboard* indeks KAMI, seperti pada gambar 4.1 berikut ini:



Gambar 4.1. Dashboard Hasil Penilaian Indeks KAMI Universitas Teknologi Mataram

Gambaran secara keseluruhan dari penilaian yang telah dilakukan dengan menggunakan indeks KAMI versi 4.1 dapat dilihat pada gambar 4.1 *dashboard*. Dapat dilihat pada radar *chart dashboard* bahwa hampir seluruh area yang dinilai dalam indeks KAMI belum terpenuhi dan belum sesuai dengan standar ISO 27001.

Gambar 4.2. Hasil Evaluasi Indeks KAMI Kampus Universitas Teknologi Mataram

Pada Gambar 4.2 menunjukkan hasil evaluasi akhir tingkat keamanan informasi pada Kampus Universitas Teknologi Mataram bahwa kepentingan penggunaan sistem elektronik yaitu mencapai tingkat Tinggi dengan nilai sebesar 23, dan tingkat kelengkapan penerapan sesuai kategori dengan nilai 416, serta kondisi Pemenuhan Kerangka Kerja Dasar.

Untuk tingkat kematangan setiap area yang telah dinilai dalam indeks KAMI versi 4.1 masih sangat kurang. Berikut ini adalah uraian dari tingkat kematangan kelima area yang telah dinilai sebelumnya:

Tabel 4.21. Tingkat Kematangan Kelima Area

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi
Tingkat Kematangan II					
Status	II	II	II	II	II
Tingkat Kematangan III					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Tingkat Kematangan IV					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Tingkat Kematanagan V					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	II	II	II	II	II

Urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Batasan minimal yang harus dicapai agar dapat melakukan sertifikasi ISO adalah III+, sedangkan untuk saat ini tingkat kematangan pada Kampus Universitas Teknologi Mataram hanya dibatas I-II. Tingkat kematangan ini menunjukkan posisi Kampus Universitas Teknologi Mataram sebagai berikut ini:

Tabel 4.22. Tingkatan Kondisi Kampus Universitas Teknologi Mataram

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

Hasil penilaian kelima area Indeks KAMI ini dibatasi sampai penilaian kualitas tanpa adanya penilaian kuantitas pada pertanyaan-pertanyaan tertentu. Ada beberapa pertanyaan dimasing-masing area yang juga membutuhkan penilaian terhadap kuantitas dan hal ini dapat mempengaruhi hasil penilaian pada instansi terkait.

Validasi terkait penilaian manajemen keamanan informasi yang ada pada Kampus Universitas Teknologi Mataram telah dilakukan guna memastikan bahwa penilaian yang dilakukan sudah benar dan sesuai dengan kondisi sesungguhnya yang ada di instansi terkait. Validasi dilakukan dengan pengecekan terhadap nilai-nilai yang masih kurang di masing-masing area dan disesuaikan dengan kondisi sesungguhnya di Kampus Universitas Teknologi Mataram. Selain itu juga dilakukan pengecekan apakah pihak yang dipilih sebagai narasumber sudah tepat atau belum dengan menandai pertanyaan-pertanyaan yang telah disesuaikan dengan keahlian dari masing-masing narasumber.

4.5.2. Saran Perbaikan Area Keamanan Informasi

Setelah melakukan penilaian dengan indeks KAMI versi 4.1 dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI versi 4.1, maka tahap selanjutnya adalah membuat saran perbaikan pada area keamanan informasi

setiap bagian yang memiliki hasil status penilaian masih kurang. Berikut ini adalah saran perbaikan yang dibuat masing-masing area yang ada dengan tabel berisikan pertanyaan, status, kontrol ISO, dan saran perbaikan:

a. Saran Perbaikan area tata kelola keamanan informasi

Rekomendasi saran perbaikan pada area tata kelola keamanan informasi, berisi saran perbaikan untuk 3 pertanyaan yang memiliki nilai 0 (nol) atau statusnya tidak dilakukan oleh pihak Kampus Universitas Teknologi Mataram. Rekomendasi saran perbaikan mengacu pada ISO/IEC 27001:2013.

Tabel 4.23. Saran Perbaikan Area Tata Kelola Keamanan Informasi

No	Pertanyaan	Status	Kontrol ISO
2.11	Apakah instansi/ perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	18.1.4
Saran Perbaikan: **Control 18.1.4** ***Privacy and protection of personally identifiable information*** BPSI sebagai pihak yang menanggani keamanan informasi diharapkan menerapkan pengamanan Privasi dan perlindungan informasi terkait data pribadi sebagaimana disyaratkan dalam undang-undang dan peraturan yang berlaku dengan relevan. Adapun cara melaksanakan keamanan data pribadi yang digunakan dalam proses kerja agar sesuai dengan dengan perundangan-undagan yang berlaku adalah dengan cara menyusun aturan internal perlindungan Data Pribadi sebagai bentuk tindakan pencegahan untuk menghindari terjadinya kegagalan dalam perlindungan Data Pribadi yang dikelola.			
2.18	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan	6.1.5

Tabel 4.23. Saran Perbaikan Area Tata Kelola Keamanan Informasi (Lanjutan)

No	Pertanyaan	Status	Kontrol ISO
Saran Perbaikan: **Control 6.1.5 *Information security in project management*** Pihak BPSI diharapkan menerapan program untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi yang dapat diterapkan/ diintegrasikan pada suatu manajemen proyek agar dapat memastikan bahwa risiko terkait keamanan informasi telah diidentifikasi dan ditangani sebagai bagian dari proyek. Penilaian risiko keamanan informasi dilakukan pada tahap awal untuk mengidentifikasi kendali yang diperlukan. Keamanan informasi harus ditangani dan ditinjau secara teratur dalam semua proyek. Tanggung jawabnya juga harus dialokasikan secara spesifik dalam manajemen proyek.			
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	7.2.1 7.2.3
Saran Perbaikan: **Control 7.2.1 *Management responsibilities*** **Control 7.2.3 *Disciplinary process*** Diterapkan program penilaian kinerja pengelolaan keamanan informasi bagi masing-masing individu terkait. Penilaian kinerja terhadap masing-masing individu dapat dilihat dari beberapa hal antara lain: - Kedisiplinan dalam menjalankan keamanan informasi sesuai dengan prosedur dimana instansi harus terlebih dahulu menerapkan proses kedisiplinan secara formal - Pelanggaran yang pernah dilakukan terkait keamanan informasi organisasi - Motivasi dalam memenuhi kebijakan keamanan informasi yang ada - Kepatuhan terhadap syarat dan kondisi kerja, termasuk kebijakan keamanan informasi organisasi - Memiliki keterampilan dan kualifikasi yang sesuai dengan persyaratan yang telah ditentukan sebelumnya			

b. Saran Perbaikan Area Pengelolaan Risiko Keamanan Informasi

Rekomendasi saran perbaikan pada area pengelolaan risiko keamanan informasi, berisi saran perbaikan kepada pihak Kampus Universitas Teknoogi

Mataram untuk pertanyaan yang statusnya Dalam Penerapan / Diterapkan Sebagian. Rekomendasi saran perbaikan mengacu pada ISO/IEC 27001:2013.

Tabel 4.24. Saran Perbaikan Area Pengelolaan Risiko Keamanan Informasi

No	Pertanyaan	Status	Kontrol ISO
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan/ Diterapkan Sebagian.	16.1.6
Saran Perbaikan: **Control 16.1.6** ***Learning from information security incidents*** Harus ada mekanisme yang dilakukan untuk mengukur dan memonitor biaya dan tipe insiden keamanan informasi. Informasi yang diperoleh dari evaluasi insiden keamanan informasi harus digunakan untuk mengidentifikasi dampak dari insiden yang terjadi. Evaluasi insiden keamanan informasi dapat mengindikasikan peningkatan kebutuhan kontrol untuk membatasi kerusakan yang terjadi dimasa mendatang dan agar diperhitungkan dalam proses peninjauan kebijakan keamanan informasi.			
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Dalam Penerapan/ Diterapkan Sebagian.	16.1.7
Saran Perbaikan: **Control 16.1.7** ***Collection of evidence*** Dilakukan penentuan dan penetapan prosedur untuk identifikasi, pengumpulan, dan akuisisi informasi yang dapat berfungsi sebagai bukti. Setelah melakukan mitigasi terhadap insiden yang terjadi maka dapat diukur apakah langkah tersebut berjalan dengan baik dan efektif untuk menanggulangi insiden yang terjadi. Ketika insiden keamanan informasi terdeteksi pertama kali, mungkin sulit untuk menentukan tindakan penyelesaiannya. Oleh karena itu setiap bukti yang diperlukan harus dijaga atau tidak boleh dihancurkan sebelum langkah mitigasi insiden direalisasikan.			

c. Saran Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi

Rekomendasi saran perbaikan pada area kerangka kerja pengelolaan keamanan informasi, berisi saran perbaikan untuk 7 pertanyaan yang memiliki nilai 0 (nol). Rekomendasi saran perbaikan mengacu pada ISO/IEC 27001:2013.

Tabel 4.25. Saran Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi

No	Pertanyaan	Status	Kontrol ISO
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Penerapan/Di terapkan Sebagian.	17.1.2
Saran Perbaikan: **Control 17.1.2 *Implementing information security continuity*** Pihak Kampus Universitas Teknologi Mataram harus mendefinisikan peran tanggung jawab dan harus memastikan: - Adanya struktur manajemen yang berwenang, berpengalaman, dan berkompetensi untuk mempersiapkan, memitigasi, dan menanggapi suatu peristiwa yang mengganggu - Pihak terkait harus memiliki kewenangan, tanggung jawab, dan kompetensi dalam mengelola insiden dan menjaga keamanan informasi - Mengembangkan dan menyetujui dokumentasi rencana, respon, dan pemulihan prosedur secara rinci sebagaimana organisasi akan mengelola suatu peristiwa yang mengganggu dan akan menjaga keamanan informasi untuk tingkat yang telah ditentukan, berdasarkan pada tujuan kelangsungan keamanan informasi manajemen yang disetujui.			
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	Dalam Penerapan/Di terapkan Sebagian.	17.1.2

Tabel 4.25. Saran Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)

No	Pertanyaan	Status	Kontrol ISO
Saran Perbaikan: **Control 17.1.2** ***Implementing information security continuity*** Setelah menentukan kebijakan dan prosedur terkait BCP dan DRP, pihak Kampus Universitas Teknologi Mataram harus melakukan uji coba terhadap dokumen tersebut yang dilakukan sesuai dengan tanggung jawab dan jadwal yang sudah direncanakan.			
4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Dalam Penerapan/Di terapkan Sebagian.	17.1.3
Saran Perbaikan: **Control 17.1.3** ***Verify, review, and evaluate information security continuity*** Setelah melakukan uji coba terhadap dokumen, pihak Kampus Universitas Teknologi Mataram juga dapat melakukan evaluasi langkah perbaikan. Kampus Universitas Teknologi Mataram harus memverifikasi keberlangsungan manajemen keamanan informasinya dengan cara: - Menguji fungsi dari proses kesinambungan keamanan informasi, prosedur dan kontrol untuk memastikan bahwa mereka sudah konsisten dengan tujuan kelangsungan keamanan informasi - Meninjau validitas dan efektivitas informasi terkait langkah-langkah penilaian keberlangsungan keamanan informasi, proses keamanan informasi, prosedur dan kontrol manajemen kelangsungan bisnis atau manajemen pemulihan bencana			
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan/Di terapkan Sebagian.	5.1.2
Saran Perbaikan: **Control 5.1.2** ***Review of the policies for information security*** Target dan sasaran keamanan informasi terdapat dalam kebijakan keamanan informasi yang mana harus dilakukan peninjauan secara rutin untuk memastikan kesesuaian,			

Tabel 4.25. Saran Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)

No	Pertanyaan	Status	Kontrol ISO
kecukupan, dan efektivitasnya secara terus menerus. Tinjauan tersebut harus mencakup penilaian peluang perbaikan kebijakan organisasi dan pendekatan untuk mengelola keamanan informasi dalam menanggapi perubahan lingkungan organisasi, situasi bisnis, kondisi hukum atau lingkungan teknis. Jika terjadi revisi saat melakukan review kebijakan ini maka harus mendapatkan persetujuan dari manajemen terkait.			
4.27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Perencanaan	5.1.2
Saran Perbaikan: **Control 5.1.2** ***Review of the policies for information security*** Dalam melakukan review kebijakan dan prosedur terkait keamanan informasi, pihak Kampus Universitas Teknologi Mataram juga harus memperhitungkan aspek finansial terkait perubahan infrastruktur dan proses perubahannya.			
4.28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Dalam Perencanaan	17.2.1
Saran Perbaikan: **Control 17.2.1** ***Availability of information processing facilities*** Pihak Kampus Universitas Teknologi Mataram harus melakukan identifikasi kebutuhan bisnis untuk ketersediaan sistem informasi dimana ketersediaan tidak bisa dijamin dengan menggunakan arsitektur sistem yang ada.			

Tabel 4.25. Saran Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)

No	Pertanyaan	Status	Kontrol ISO
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan	17.2.1
Saran Perbaikan: **Control 17.2.1** ***Availability of information processing facilities*** Untuk rencana kedepannya terkait peningkatan keamanan informasi harus direncanakan dalam membentuk strategi organisasi yang memperhatikan pentingnya keamanan informasi didalam instansi.			

d. Saran Perbaikan Area Pengelolaan Aset Informasi

Rekomendasi saran perbaikan pada area pengelolaan aset informasi, berisi saran perbaikan kepada pihak kampus Universitas Teknologi Mataram untuk beberapa pertanyaan yang statusnya Dalam Penerapan/Diterapkan Sebagian. Rekomendasi saran perbaikan mengacu pada ISO/IEC 27001:2013.

Tabel 4.26. Saran Perbaikan Area Pengelolaan Aset Informasi

No	Pertanyaan	Status	Kontrol ISO
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Dalam Penerapan/Diterapkan Sebagian.	8.2.1

Tabel 4.26. Saran Perbaikan Area Pengelolaan Aset Informasi (Lanjutan)

No	Pertanyaan	Status	Kontrol ISO
Saran Perbaikan: **Control 8.2.1 *Classification of information*** Informasi harus diklasifikasikan sesuai persyaratan hukum, nilai, kekritisan, dan kepekaan terhadap penggunaan/modifikasi yang tidak sah. Untuk mengurangi/menghindari pelanggran tersebut, maka dapat dilakukan klasifikasi aset informasi. Selain itu juga harus diidentifikasikan terkait kepemilikan aset informasi terkait masing-masing klasifikasi. Dibuat skema klasifikasi aset dengan tingkatan tertentu dan nama yang masuk akal. Skema ini harus diterapkan secara konsisten di seluruh organisasi sehingga setiap orang akan mengklasifikasikan informasi dan aset terkait dengan cara yang sama dan menerapkan perlindungan yang tepat. Hasil klasifikasi harus menunjukkan sensitivitas dan kekritisan nilai aset untuk organisasi. Contoh skema klasifikasi kerahasiaan aset informasi dapat didasarkan pada 4 tingkatan sebagai berikut: - Tidak menyebabkan kerugian - Menyebabkan kerugian ringan dan gangguan kecil pada operasional - Dampak jangka pendek yang signifikan pada operasional dan tujuan taktis - Dampak serius pada tujuan strategis jangka panjang atau berisiko pada kelangsungan hidup organisasi.			
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan/Di terapkan Sebagian.	13.2.4
Saran Perbaikan: **Control 13.2.4 *Confidentiality or non-disclosure agreements*** Pihak Kampus Universitas Teknologi Mataram dapat melakukan pencatatan terhadap penyelesaian insiden yang dilakukan terkait kegagalan keamanan informasi yang terjadi. Hal ini dapat membantu Pihak Kampus untuk melakukan investigasi lebih lanjut terkait kesesuaian tindakan penyelesaian insiden yang dilakukan.			
5.18	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	Dalam Penerapan/Di terapkan Sebagian.	12.3.1

Tabel 4.26. Saran Perbaikan Area Pengelolaan Aset Informasi (Lanjutan)

No	Pertanyaan	Status	Kontrol ISO
Saran Perbaikan: **Control 12.3.1 *Information backup*** Pihak Kampus harus membuat sebuah kebijakan yang menentukan persyaratan organisasi dalam melakukan *backup* informasi, perangkat lunak, dan sistem. Kebijakan *backup* harus menentukan retensi dan perlindungan persyaratan. Fasilitas *backup* yang memadai harus disediakan untuk memastikan bahwa semua informasi penting dan *software* dapat dipulihkan setelah kegagalan bencana atau media.			
5.23	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Dalam Penerapan/Di terapkan Sebagian.	9.2.3
Saran Perbaikan: **Control 9.2.3 *Management of privileged access rights*** Pembuatan prosedur yang membahas alokasi hak akses yang dikontrol melalui proses otorisasi resmi. Hal yang harus dipertimbangkan adalah: - Identifikasi hak akses istimewa yang terkait dengan setiap sistem operasi, database, dan aplikasi - Keistimewaan hak akses tidak boleh diberikan sampai proses otorisasi selesai - Persyaratan untuk berakhirnya hak akses istimewa harus didefinisikan - Kompetensi pengguna dengan hak akses istimewa harus ditinjau secara teratur untuk memverifikasi apakah mereka sejalan dengan tugas mereka.			

Dari hasil penelitian yang telah dilakukan terhadap analisis tingkat kesiapan keamanan sistem manajemen informasi dengan menggunakan indeks KAMI berdasarkan standar ISO/IEC 27001:2013 yang ada di kampus Universitas Teknologi Mataram bahwa Nilai hasil tingkat kelengkapan penerapan Standar ISO 27001 sesuai Kategori SE sebesar 416, dimana hasil akhir evaluasinya berada pada level Pemenuhan Kerangka Kerja Dasar, sehingga Kampus Universitas Teknologi Mataram tidak layak atau belum layak untuk melakukan sertifikasi keamanan

sesuai dengan standar ISO/IEC 27001:2013 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 maka dari itu diperlukan perbaikan pada semua aspek yang ada yaitu pada tata kelola keamanan infromasi, pengelolaan risiko keamanan, kerangka kerja keamanan informasi, pengelolaan aset, teknologi dan keamanan informasi. Disarankan juga agar pihak Kampus Universitas Teknologi Mataram perlu melakukan peningkatan pengamanan informasi baik dengan pihak internal maupun dengan pihak ketiga dan melakukan evaluasi dan pemantauan keamanan secara berkala.

Setelah dilakukannya penelitian terkait dengan analisis kemanan sistem manajemen informasi menggunakan Indeks KAMI berdasarkan Standar ISO/IEC 27001:2013, memberikan pemahaman bahwa dimasing-masing area yang dievaluasi menjadi penting untuk diperhatikan karena akan berdampak pada hasil akhir untuk mengetahui sejauh mana peningkatannya terutama dalam hal keamanan sistem manajemen informasi yang telah dilakukan, apakah semakin meningkat atau menurun.

BAB V

PENUTUP

5.1. Kesimpulan

Kesimpulan yang dapat diperoleh dari penelitian ini terkait penilaian manajemenen keamanan informasi pada Kampus Universitas Teknologi Mataram menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

a. Hasil dari penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 23 dari jumlah total keseluruhan sebesar 50. Hal ini menunjukkan bahwa Kampus Universitas Teknologi Mataram sudah tinggi dalam kebutuhan penggunaan sistem elektronik yang artinya penggunaan sistem elektronik adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan.

b. Hasil keseluruhan dari penilaian kelima area dalam Indeks KAMI adalah sebesar 416 dari jumlah total keseluruhan sebesar 645 dan berada pada level II-II dimana level ini berada dikondisi tingkat Pemenuhan Tingkat Kerja Dasar, yang artinya kondisi tingkat pengamanan sudah diterapkan walaupun sebagian masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.

c. Rincian area indeks KAMI sebagai berikut, Tata Kelola dengan status Tk Kematangan II dan skor 83, Pengelolaan Risiko dengan status Tk Kematangan II dan skor 55, Kerangka Kerja Keamanan Informasi dengan status Tk Kematangan II dan skor 61, Pengelolaan Aset dengan status Tk Kematangan II dan skor 124, dan Teknologi dan Keamanan Informasi

dengan status Tk Kematangan II dan skor 93. Hasil skor area modul suplemen pada 3 area yaitu Pengamanan Keterlibatan Pihak Ketiga dengan nilai persentase 63%, Pengamanan Layanan Infrastruktur Awan dengan nilai persentase 67%, dan Perlindungan Data Pribadi dengan nilai persentase 71%, diantara ke 3 area modul suplemen tidak ada yang mencapai 100%, sehingga dapat disimpulkan bahwa Kampus Universitas Teknologi Mataram belum memenuhi syarat kesiapan pengamanan pada modul suplemen.

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, berikut ini merupakan saran secara singkat yang diberikan untuk meningkatkan kelima area pengamanan Indeks Keamanan Informasi (KAMI):

a. Untuk penelitian selanjutnya sebaiknya peneliti menggunakan standar penilaian Indeks Keamanan Informasi (KAMI) versi terbaru dari Kementerian Kominfo agar dapat menyesuaikan dengan perkembangan kebutuhan, relevansi serta teknologi terbaru.

b. Diperlukan adanya petunjuk teknis secara detail mengenai proses penilaian pada Indeks KAMI guna memahami perolehan skor yang didapat maupun untuk perbaikan serta pengembangan proses penilaian untuk kedepannya.

c. Perlunya pendokumentasian terhadap kerangka kerja keamanan informasi serta melakukan uji coba dan monitoring kerangka kerja secara berkelanjutan.

d. Perhatikan cara pengujian pada pertanyaan yang membutuhkan jenis penilaian lebih dari satu, maka lakukan pengujian terhadap kualitas dan juga kuantitas pada item yang dinilai agar nilai yang diberikan pada pertanyaan tersebut benar-benar valid.

DAFTAR PUSTAKA

PUSTAKA MAJALAH, JURNAL ILMIAH ATAU PROSIDING

Hambali., Musa, P., 2020, Analysis of Governance Security Management Information System Using Indeks KAMI in Central Government Institution, Jurnal Ilmiah Bidang Teknologi (ANGKASA), Vol. XII, No. 1, Mei 2020.

Yustanti, W., Bisma, R., Qoiriah, A., Prihanto, A., 2018, Analisis Tingkat Kesiapan dan Kematangan Implementasi ISO 27001:2013 Menggunakan Indeks Keamanan Informasi 3:2015 pada UPT. PPTI Universitas Negeri Surabaya, Prosiding Semnas PPM, Vol. 1, No. 1, Desember 2018.

Juliharta, I. G. P. K., 2019, Analisa Tingkap Kesiapan Penerapan Keamanan Teknologi Informasi dalam Pelaksanaan E-Government Berbasis Indeks Keamanan Informasi (KAMI) Studi Kasus Pemerintah Kota Kediri, Jurnal Teknologi Informasi dan Komputer, Vol. 5, No. 1, Januari 2019.

Matondang, N., Hananto, B., Nugrahaeni, C., 2019, Analisis Tingkat Kesiapan Pengamanan Sistem Informasi, Jurnal Teknologi Informasi dan Pendidikan (JTIP), Vol. 12, No. 1, Maret 2019.

Ferdiansyah, P., Subektiningsih., Indrayani, R., 2019, Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.0 pada Lembaga UPTD XYZ, Jurnal Mobile and Forensics (MF), Vol. 1, No. 2, September 2019.

Arman, N., Putra, W. H. N., Rachmadi. A., Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo menggunakan Indeks Keamanan Informasi (KAMI), Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, Vol. 3, No. 6, Juni 2019.

Riswaya, A. R., Sasongko, A., Maulana. A., 2020, Evaluasi Tata Kelola Keamanan Teknologi Menggunakan Indeks KAMI untuk Persiapan Standar SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia), Jurnal Computech & Bisnis, Vol. 14, No. 1, Juni 2020.

Gala, R. A. P. P., Sengkey. R., Punusingo. C., 2020, Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI, Jurnal Teknik Informatika, Vol. 15, No. 3 Juli-September 2020.

Gunawan, C. E., Fenando., 2018, Pengukuran Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Studi Kasus di PUSTIPD UIN Raden Fatah Palembang, Jurnal Sistem Informasi (JUSIFO), Vol. 4, No. 2, Desember 2018

PUSTAKA LAPORAN PENELITIAN

Basyarahil, F. A., 2017, Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 20071:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya, Tugas Akhir, Jurusan Sistem Informasi, Institut Teknologi Sepuluh November, Surabaya.