# Manajemen Risiko Keamanan Informasi Menggunakan ISO 27005:2011 pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)

http://dx.doi.org/10.28932/jutisi.v4i2.792

Asriyanik[#1], Prajoko[*2]

[#]*Program Studi Teknik Informatika Universitas Muhammadiyah Sukabumi*
*Jl. R. Syamsudin, S.H. No. 50 Kota Sukabumi*
[1]asriyanik@gmail.com

[*]*Program Studi Teknik Informatika Universitas Muhammadiyah Sukabumi*
*Jl. R. Syamsudin, S.H. No. 50 Kota Sukabumi*
[2]pradjoko@yahoo.com

*Abstract* — **Information security is an important part of an academic information system, including Muhammadiyah University of Sukabumi (UMMI). Information security is conducted to protect UMMI assets, especially data and information. Data and information have become an important asset in an organization because it relates to the image of the organization. At this time academic information system at UMMI is built online, causing various threats that may occur. Threats can arise inside or outside. If the threat occurs then the information security aspect will be disrupted and enable the disruption of business process on academic information system of UMMI. The likelihood of this threat is called risk. To minimize losses from risks, risk management should be done well. The risk management method used in risk management in the academic information system of UMMI is ISO 27005. The selection of this method to facilitate the development in the next stage of information security management system on UMMI Academic Information System uses ISO 27000 series. Data collection is done by interview and discussion. The risk management process under ISO 27005 includes four main steps: scope determination, risk assessment, risk treatment and risk acceptance. The result of the risk assessment found 73 possible threat scenarios divided into 3 risk levels, which were 2 low risks, 64 medium risks and 7 high risks. Out of 73 threat scenarios, 47 were made to risk treatment planning. Results of the risk treatment plan, 19 modified risks, 1 risk transferred and 27 risks could be avoided. This risk treatment plan is a recommendation for the leadership of UMMI to conduct risk management.**

*Keywords*— **risk management, information security, ISO 27005, information academic system.**

## I. PENDAHULUAN

Pada saat ini penerapan TIK di perguruan tinggi hampir semua terhubung ke jaringan luas (*internet*) termasuk di Universitas Muhammadiyah Sukabumi (UMMI). Salah satu sistem yang terhubung ke jaringan luas di UMMI adalah sistem informasi akademik (SIAK). Dengan terhubungnya SIAK ke jaringan luas maka proses bisnis bidang akademik di UMMI menjadi lebih cepat dan mudah. Namun memunculkan hal lain juga, yaitu mendatangkan peluang terjadinya ancaman pada SIAK UMMI. Kemungkinan terjadinya ancaman ini merupakan risiko yang harus ditanggung oleh UMMI ataupun perguruan tinggi lain saat menghubungkan sistem yang dibangun ke jaringan luas. Hal ini telah terbukti dengan banyaknya laporan terjadinya serangan siber dan upaya *hacking* terhadap sistem informasi di perguruan tinggi [1]. Jika terjadi serangan pada sistem informasi akademik maka akan mengganggu proses berjalannya sistem yang ada, terutama aspek keamanan informasi. Aspek keamanan informasi yang akan terganggu adalah aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) data atau informasi [2].

Sistem Informasi Akademik (SIAK) di Universitas Muhammadiyah Sukabumi (UMMI) terdiri dari beberapa komponen yaitu perangkat keras dan jaringan komputer, perangkat lunak yang terdiri dari aplikasi dan basis data SIAK, serta pengguna SIAK UMMI. Ketiga komponen tersebut merupakan aset yang penting dalam keberlangsungan proses akademik di UMMI. Pada tahun 2015 telah dilakukan penelitian di UMMI dalam upaya menerapkan tata kelola teknologi informasi yang baik dalam mengelola teknologi informasi di Universitas

Muhammadiyah Sukabumi (UMMI) dengan menggunakan standar COBIT 5 [3]. Namun pelaksanaan tata kelola teknologi informasi di UMMI masih bersifat umum karena komponen yang dibangun baru pada tahap kebijakan pengelolaan teknologi informasi. Untuk mengelola keamanan informasi pada sistem informasi akademik secara khusus harus dilakukan sistem manajemen keamanan informasi [4], dan salah satu bagiannya yaitu melakukan manajemen risiko keamanan informasi.

Metode-metode yang dapat digunakan dalam melakukan manajemen risiko keamanan informasi di antaranya yaitu FAIR, OCTAVE, ISO 27005, NIST 800-30 dan yang lainnya [5]. emilihan metode dapat disesuaikan dengan kondisi organisasi atau kebutuhan organisasi. Untuk pengimplementasian tata kelola teknologi informasi dan pengembangan manajeman keamanan informasi bagi penyelenggaran publik di Indoensia dihimbau untuk menggunakan standar dari ISO 27000 [6]. Salah satu seri dari ISO 27000 yaitu ISO 27005 yang merupakan panduan untuk melakukan manajemen risiko keamanan informasi. Pemilihan ISO 27005 sebagai standar yang digunakan selain dari himbauan pemerintah juga untuk memudahkan pengelolaan kemananan informasi SIAK UMMI pada tahap selanjutnya yaitu dalam pengembangan dan audit keamanan informasi di UMMI.

Maka berdasarkan uraian di atas, permasalahan yang akan diangkat adalah bagaimana melakukan manajemen risiko pada sistem informasi akademik UMMI dengan menggunakan standar ISO 27005. Tujuan dari penelitian ini adalah menghasilkan rekomendasi penanganan risiko pada sistem informasi akademik UMMI sesuai dengan prioritas risiko yang ada. Hasil dari penelitian ini diharapkan dapat menjadi masukan bagi UMMI melakukan tindakan penanganan risiko pada SIAK menjadi lebih terencana dan tepat sasaran sesuai dengan tingkat risiko yang ada.

Data yang digunakan dalam penelitian ini didapatkan dari hasil wawancara dan kesimpulan dari forum diskusi dengan bagian pengelola sistem informasi akademik di UMMI, perwakilan pengguna SIAK UMMI seperti dosen, administrator SIAK UMMI, mahasiswa, perwakilan fakultas dan juga beberapa orang yang paham dalam bidang ini.

Untuk membatasi lingkup penelitian maka penelitian ini dibatasi pada beberapa hal yaitu: data aset yang akan digunakan adalah data aset secara umum, tidak melingkupi isi data dan informasi secara detail, seri ISO 27005 yang digunakan adalah ISO 27005:2011, dan proses yang dilakukan dalam manajemen risiko sampai pada tahap penanganan risiko (*risk treatment)* dari sistem informasi akademik Universitas Muhammadiyah Sukabumi (UMMI)

## II. TINJAUAN PUSTAKA

Beberapa kepustakaan yang digunakan sebagai rujukan dalam penelitian ini adalah sebagai berikut.

### *A. Manajemen Risiko Keamanan Informasi (MRKI)*

Risiko merupakan peluang terjadinya ancaman atau serangan sehingga memberikan akibat atau dampak terganggunya proses bisnis pada suatu organisasi atau instansi atau bahkan menyebabkan gagalnya tujuan organisasi. Manajemen risiko merupakan proses yang terdiri dari kegiatan mengindentifikasi, menganalisis dan melakukan penanganan dengan tujuan mengurangi dampak risiko pada proses bisnis organisasi [7].

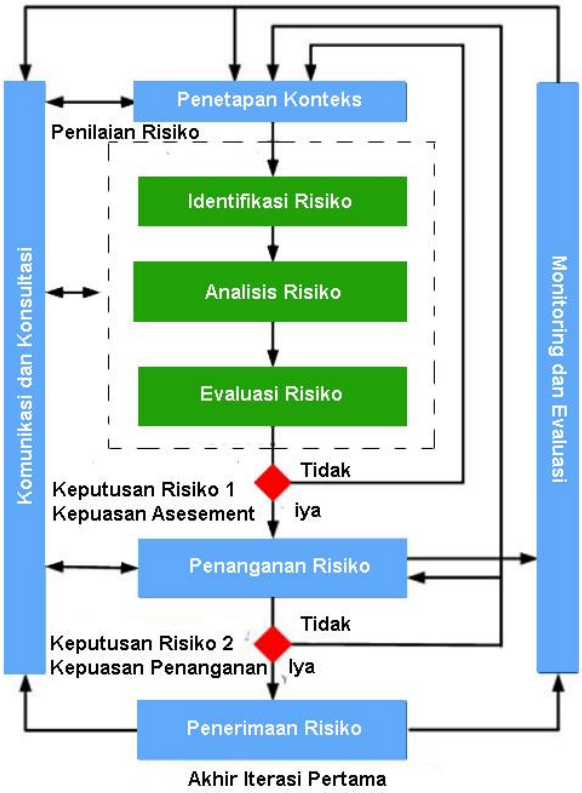
Keamanan informasi adalah proses terjaganya aspek keamanan informasi yang meliputi aspek kerahasiaan, keutuhan dan ketersediaan data dan informasi [6]. Tujuan dari dilakukan manajemen keamanan informasi adalah untuk meminimalisasi terjadinya risiko, menjamin keberlangsungan roses bisnis dan mempercepat tujuan suatu organisasi atau instansi. Tujuan lebih detailnya yaitu untuk melindungi dari berbagai bahaya seperti virus, pencurian data, serangan *hackers* yang dapat mengancam keamanan infomasi [8]. Data dan informasi harus dilindungi karena merupakan salah satu sumber daya yang dapat meningkatkan nilai atau citra suatu organisasi [9].

Dari uraian di atas dapat disimpulkan bahwa manajemen risiko keamanan informasi adalah rangkaian proses yang dilakukan dalam mengelola risiko mulai dari proses identifikasi sampai penanganan risiko dengan tujuan untuk menjaga keamanan informasi agar tujuan organisasi dapat berjalan dengan baik.

### *B. Standar ISO 27005:2011*

Pada tahun 2005, ISO (*International Organization for Standarization*) bekerja sama dengan IEC (*International Electronichal Comission*) mengeluarkan standarisasi untuk *Informatioan System Managemen Security* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) yang dikelompokkan dalam seri ISO/IEC 27000. Bagian dari ISO /IEC27000 adalah ISO/IEC 27000: ISMS *Overview and Vocabulary*, ISO/IEC 27001: ISMS *Requirements*, ISO/IEC 27002: *Code practise for* ISMS, ISO/IEC 27003: *Implementation and guidance of* ISMS, ISO/IEC 27004: ISMS *Measurments*, ISO/IEC 27005: *Information Security Risk Management* (ISRM), ISO/IEC 27006: *Sertification Body Requirements of* ISMS, ISO/IEC 27007: *Guidelines for* ISMS *auditing.* [10][11]

ISO/IEC 27005 adalah seri SMKI yang digunakan sebagai acuan dalam melakukan manajemen risiko keamanan informasi. Proses umum pada manajemen risiko keamanan informasi berdasar ISO 27005:2011 digambarkan pada Gambar 1 berikut [12].




Gambar. 1 Alur Manajemen Keamanan Informasi dengan ISO 27005:2011

Uraian dari langkah-langkah di atas adalah:

*1) Penetapan konteks manajemen risiko keamanan informasi*: pada tahap ini dilakukan penggambaran konteks manajemen risiko keamanan informasi untuk sistem informasi akademik yang meliputi: pertimbangan umum, kriteria dasar, ruang lingkup dan batasan, organisasi manajemen keamanan informasi.

*2) Penilaian risiko keamanan informasi*: Secara umum proses ini meliputi: identifikasi risiko, analisis risiko dan evaluasi risiko. Identifikasi risiko diuraikan lagi menjadi beberapa proses yaitu identifikasi aset, ancaman, identifikasi kerentanan, identifikasi dampak terjadinya ancaman atau ancaman. Proses analisis risiko meliputi penentuan kategori dampak risiko yang mungkin terjadi berdasar pada ancaman yang ada, penentuan kemungkinan terjadinya ancaman (*likelyhood*), serta menentukan level risiko yang mungkin terjadi dari setiap ancaman terhadap aset yang ada. [7] Untuk membuat kategori dampak risiko dan kemungkinan terjadinya ancaman dapat dilakukan berdasar dari keputusan pihak pengelola sesuai dengan hasil analisis. Jadi pengkategorian ini tidak bersifat baku untuk setiap organisasi atau instansi. Kategori dampak dan kemungkinan terjadinya ancaman (*likelyhood*) yang akan digunakan pada penelitian ini digambarkan pada Tabel I dan Tabel II di bawah ini.

TABEL I
KATEGORI KEMUNGKINAN (*LIKELYHOOD*) DARI ANCAMAN

| **Ketegori *Likelyhood*/ Kemungkinan Ancaman** | **Keterangan** |
|---|---|
| *Very unlikely (1)* | Ancaman hampir tidak pernah terjadi |
| *Unlikely (2)* | Frekuensi kejadian ancaman jarang (1 – 5 kali/semester) |
| *Possible (3)* | Frekuensi kejadian ancaman cukup sering (6-10 kali/ semester) |
| *Likely (4)* | Frekuensi kejadian ancaman sering (10-20 kali/semester) |
| *Frequent (5)* | Frekuensi kejadian ancaman sangat sering (>20 kali/semester) |

TABEL II
KATEGORI DAMPAK TERJADINYA RISIKO

| **Kategori Dampak** | **Keterangan** |
|---|---|
| *Very Low (1)* | Dampak tidak signifikan. Artinya tidak menimbulkan gangguan aktivitas yang berarti. Untuk masalah ini toleransi penyelesaian sampai 7 hari. |
| *Low (2)* | Dampak gangguan kecil pada layanan SIAK UMMI bukan pada program utama. Toleransi penyelesaian masalah 1-2 hari |
| *Medium (3)* | Dampak gangguan sedang, yaitu ada gangguan kegiatan pada layanan pendukung SIAK UMMI. Masalah harus diselesaikan paling lama 1 hari. |
| *High (4)* | Dampak gangguan besar, artinya menimbulkan gangguan pada kegiatan layanan utama SIAK UMMI. Masalah harus diselesaikan <12 jam |
| *Very High (5)* | Dampak sangat krusial. Artinya menimbulkan gangguan pada kegiatan layanan utama dan pendukung SIAK UMMI secara kritis. Masalah ini harus diselesaikan < 1 jam |

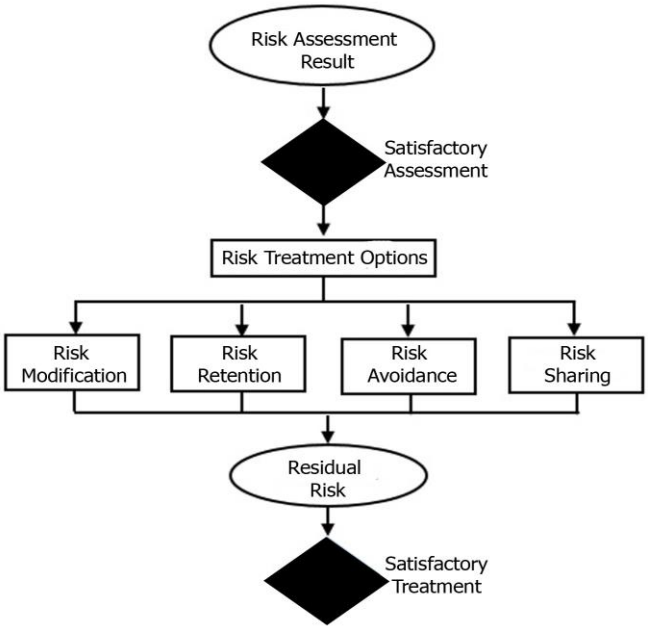
Bagian dari analisis risiko adalah membuat kategori penilaian risiko. Proses penilaian risiko ini dapat dilakukan secara kualitatif dan kuantitatif. [10] Pada dasarnya untuk nilai risiko dihitung dengan cara mengalikan nilai dampak dan nilai kemungkinan terjadinya ancaman. Kategori penilaian risiko yang akan digunakan dalam manajemen risiko keamanan informasi pada penelitian ini dibagi menjadi tiga kategori yaitu: Risiko rendah (*Low Risk*), risiko sedang (*Medium Risk*), risiko tinggi (*High Risk*). Untuk lebih jelasnya kategori risiko disajikan pada Tabel III berikut.

TABEL IIIII
MATRIKS KATEGORI PENILAIAN RISIKO

| | | **Kemungkinan Terjadinya Ancaman (*Likelyhood*)** | | | | |
|---|---|---|---|---|---|---|
| | | *Very un likely (1)* | *Un likely (2)* | *Possible (3)* | *Likel y (4)* | *Frequent (5)* |
| **Dampak** | *Very Low (1)* | 1 / L | 2/ L | 3/L | 4/M | 5/M |
| | *Low (2)* | 2/ L | 4/L | 6/M | 8/M | 10/M |
| | *Medium (3)* | 3/ L | 6/M | 9/M | 12/ M | 15/H |
| | *High (4)* | 4/ M | 8/M | 12/M | 16/ H | 20/H |
| | *Very High (5)* | 5/ M | 10/ M | 15/H | 20/ H | 25/H |

Tahap terakhir dari penilaian risiko adalah evaluasi risiko, yaitu mengevaluasi risiko yang telah didapatkan pada tahap sebelumnya dan dibuat daftar prioritas risiko sesuai dengan nilai risiko.

*3) Penanganan Risiko*: Proses penanganan risiko didasarkan pada hasil penilaian risiko. Proses penanganan risiko meliputi pemilihan penanganan risiko, perencanaan penanganan risiko dan evaluasi sisa risiko. Langkah tersebut berulang sampai ditemukan penganganan risiko yang terbaik. Ada empat opsi dalam penanganan risiko yaitu modifikasi risiko, mempertahankan risiko, menghindari risiko dan membagi risiko. Adapun lebih jelasnya langkah-langkah pada penanganan risiko digambarkan pada Gambar 2 berikut.




Gambar. 2 Alur Penanganan Risiko dengan ISO 27005:2011

Dalam pemilihan penanganan risiko perlu diperhatikan beberapa hal, yaitu nilai risiko, biaya pemulihan dan biaya transfer risiko [10]. Untuk menentukan hal ini maka dibuat matriks keterhubungan antara ketiganya yang dapat sajikan pada Tabel IV berikut.

TABEL IVV
MATRIKS PEMILIHAN PENANGANAN RISIKO

| **Nilai Risiko** | **Biaya Pemulihan** | | |
|---|---|---|---|
| | ***Low*** | ***Medium*** | ***High*** |
| ***Low*** | *Risk Retention* | *Risk Modification* | *Risk Sharing/Avoid ance* |
| ***Medium*** | *Risk Modification* | *Risk Modification* | *Risk Sharing/ Avoidance* |
| ***High*** | *Risk Avoidance* | *Risk Avoidance* | *Risk Sharing/ Avoidance* |
| | ***High*** | ***Medium*** | ***Low*** |
| | **Biaya Transfer** | | |

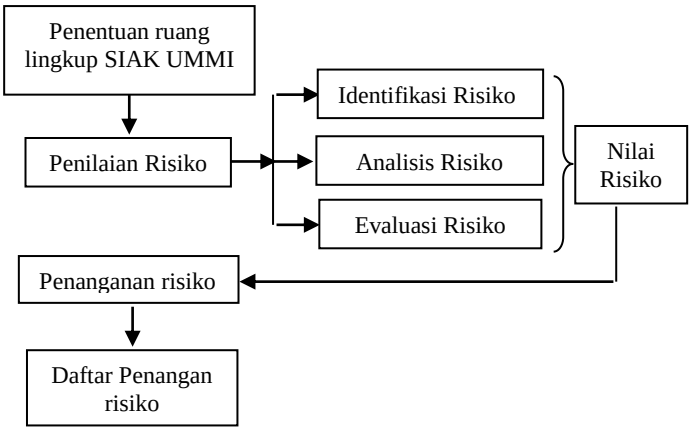
*4) Penerimaan Risiko*: Proses penerimaan risiko dilakukan jika hasil dari perencanaan penanganan risiko telah ada. Pada tahap ini dilakukan keputusan oleh pengambil kebijakan atau pihak yang bertanggung jawab untuk penentuan keputusan penerimaan risiko.

*5) Konsultasi dan Komunikasi*: kegiatan untuk mencapai kesepakatan pengelolaan risiko dengan bertukar dan atau berbagi informasi tentang risiko antara pengambil keputusan dan pemangku kepentingan lainnya.

*6) Review dan Monitoring*: Risiko bersifat dinamis, oleh karena itu harus selalu dilakukan *review* dan *monitoring* terhadap peluang, ancaman dan serangan yang mungkin terjadi [10].

## III. METODE PENELITIAN

Proses manajemen risiko keamanan informasi pada SIAK UMMI dilakukan dengan menggunakan standar ISO 27005:2011. Data yang digunakan dalam penelitian ini adalah data kualitatif [13]. Data kualitatif ini didapatkan berdasarkan hasil wawancaran dan diskusi dengan pengelola SIAK UMMI, pengguna SIAK UMMI, dan pemegang kebijakan di UMMI dalam bidang sistem informasi. Juga studi dokumentasi terhadap dokumen-dokumen yang berkaitan dengan SIAK UMMI, seperti cetak biru SIAK UMMI, buku panduan penggunaan SIAK UMMI, dan lainnya. Langkah penelitian yang dilakukan disajikan pada Gambar 3 berikut.




Gambar. 3 Langkah penelitian pada Manajemen Risiko Keamanan Informasi SIAK UMMI

## IV. PEMBAHASAN

### *A. Gambaran Umum Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI)*

Universitas Muhammadiyah Sukabumi (UMMI) mulai membangun Sistem Informasi Akademik (SIAK) pada tahun 2012, dan mulai implementasi SIAK pada awal tahun 2013. Pengembangan SIAK ini dimulai dari pengambangan perangkat lunak yang mendukung kegiatan akademik di UMMI, disertai penyediaan perangkat keras pendukung diantaranya penyediaan komputer *server*, komputer klien serta instalasi jaringan komputer baik jaringan komputer lokal dan jaringan komputer luas di lingkungan UMMI. Selain itu juga dilakukan pelatihan terhadap calon pengguna SIAK UMMI mulai dari mahasiswa, dosen, dan pengelola.

Perangkat lunak SIAK UMMI dibangun dengan berbasis *web*, beberapa aplikasi yang ada pada SIAK UMMI disajikan pada Tabel V berikut.

TABEL V
PEMBAGIAN APLIKASI PADA SIAK UMMI

| No | Modul Aplikasi | Proses |
|---|---|---|
| 1 | Modul Mahasiswa | - Mengisi Kontrak kuliah<br>- Mencetak KRS<br>- Mencetak hasil studi per semester<br>- Mencetak transkrip nilai<br>- Mencetak kartu ujian<br>- Melihat data pembayaran<br>- Melihat informasi dan jadwal |
| 2 | Modul Fakultas | - Pengelolaan data master mahasiswa, mata kuliah, dosen<br>- Pengelolaan data pengumuman, pelepasan mahasiswa, nilai<br>- Pengelolaan data pembayaran mahasiswa |
| 3 | Modul Dosen | - Pembimbingan mahasiswa (DPA)<br>- Memasukkan data nilai<br>- Pembimbingan skripsi mahasiswa |
| 4 | Modul Ketua Program Studi | - Melihat data mahasiswa, dosen, nilai dan mata kuliah |

Pengembangan SIAK UMMI terus berlanjut setiap tahun, baik itu yang bersifat perbaikan ataupun penambahan modul aplikasi. Selain dari pengembangan aplikasi, juga dibangun infrastruktur pendukung agar SIAK UMMI dapat berjalan dengan baik yaitu penginstalasian komputer dan jaringan komputer di UMMI. UMMI pada saat ini memiliki 5 komputer server, 213 komputer klien yang ditempatkan di setiap ruang perkantoran, 90 printer, 51 scanner, 48 pheriperal jaringan. Setiap komputer di UMMI dihubungkan melalui jaringan lokal menggunakan kabel, dan masing-masing jaringan lokal dihubungkan dengan menggunakan akses poin ke jaringan luas. Pada saat ini terdapat 15 akses poin untuk kegiatan sivitas akademik UMMI dan 20 MB *Bandwidth.*

Selain pengembangan aplikasi dan perangkat keras, juga dilakukan pelatihan kepada para pengguna SIAK di UMMI. Pelatihan ini dilakukan terutama kepada staf administrasi di setiap fakultas di UMMI dan kepada mahasiswa baru. Selain pelatihan juga dilakukan sosialisasi setiap ada penambahan modul baru pada SIAK UMMI.

### *B. Penilaian Risiko Keamanan Informasi pada SIAK UMMI*

Proses penilain risiko keamanann informasi pada Sistem informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi dilakukan melalui tiga langkah, yaitu identifikasi risiko, analisis risiko dan evaluasi risiko.

*1) Identifikasi Risiko*: Pada tahap ini dilakukan pengindentifikasin risiko yang mungkin ada pada SIAK UMMI. Hasil akhir dari identifikasi risiko pada SIAK UMMI adalah daftar prioritas risiko keamanan informasi mulai dari yang terkecil sampai yang terbesar atau sebaliknya. Proses identifikasi risiko pada SIAK UMMI dibagi menjadi lima langkah yaitu identifikasi aset, identifikasi ancaman, identifikasi kendali yang ada, identifikasi kerentanan, identifikasi dampak saat risiko terjadi.

Hasil dari identifikasi aset yang akan dijadikan objek penelitian untuk manajemen risiko keamanan informasi pada SIAK UMMI disajikan pada Tabel VI berikut.

TABEL VI
DAFTAR ASET SISTEM INFORMASI AKADEMIK UNIVERSITAS MUHAMMADIYAH SUKABUMI

| No | Kode Aset | Nama Aset |
|---|---|---|
| A: Aset Perangkat Keras dan Jaringan pada SIAK UMMI | | |
| 1 | A-001 | Komputer server SIAK UMMI |
| 2 | A-002 | Komputer klien (Di perkantoran UMMI) |
| 3 | A-003 | Perangkat keras jaringan komputer: Mikrotik atau router, Modem, Akses poin, Switch atau hub, Fiber Optik, Kabel UTP |
| B: Aset Perangkat Lunak pada SIAK UMMI | | |
| 4 | B-001 | Sistem operasi |
| 5 | B-002 | Aplikasi SIAK UMMI |
| 6 | B-003 | MySql (*Database management* |

| No | Kode Aset | Nama Aset |
|---|---|---|
| | | *system*) |
| 7 | B-004 | Web browser |
| 8 | B-005 | Aplikasi Email UMMI |
| C: Aset Sumber Daya Manusia pada SIAK UMMI | | |
| 9 | C-001 | Pengelola SIAK UMMI |
| 10 | C-002 | Pengguna Akhir SIAK UMMI |
| D: Aset Data dan Informasi yang berhubungan dengan SIAK UMMI | | |
| 11 | D-001 | Data akademik UMMI yang tercetak |
| 12 | D-002 | Data akademik UMMI yang bersifat elektronik dan tersimpan di media penyimpanan komputer klien |
| 13 | D-003 | Data akademik UMMI yang tersimpan pada basis data SIAK |

Hasil identifikasi ancaman dan ancaman yang mungkin terjadi pada SIAK UMMI disajikan pada Tabel VII berikut.

TABEL VII
DAFTAR ANCAMAN PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS MUHAMMADIYAH SUKABUMI

| No | Kode Ancaman | Penjelasan Ancaman |
|---|---|---|
| 1 | E-001 | Penyadapan |
| 2 | E-002 | Akses data oleh pihak yang tidak berhak (sniffing) |
| 3 | E-003 | Adware, malware, spyware |
| 4 | E-004 | Trojan , virus, worm |
| 5 | E-005 | Bruteforce login |
| 6 | E-006 | Menebak password |
| 7 | E-007 | Dokumen Hilang |
| 8 | E-008 | Penyebaran informasi atau data rahasia dan penting |
| 9 | E-009 | Pencurian berkas dokumen yang akan dibuang |
| 10 | E-010 | Korupsi data |
| 11 | E-011 | Pencurian data penting dari komputer |
| 12 | E-012 | Pengolahan data ilegal |
| 13 | E-013 | Memberitahukan akses login ke pihak yang tidak berwenang |
| 14 | E-014 | Aplikasi basis data error |
| 15 | E-015 | Kesalahan penggunaan perangkat lunak |
| 16 | E-016 | Penyalahgunaan hak akses |
| 17 | E-017 | Aplikasi SIAK UMMI Error |
| 18 | E-018 | SQL Injection |
| 19 | E-019 | Session Hijacking |
| 20 | E-020 | Spam |
| 21 | E-021 | Backdoor |
| 22 | E-022 | Error Koneksi basis data dan aplikasi |
| 23 | E-023 | Mallicious Software |
| 24 | E-024 | Cookie Injection |
| 25 | E-025 | Registri error |
| 26 | E-026 | DdoS |
| 27 | E-027 | Kesalahan penggunaan perangkat TI |
| 28 | E-028 | Gangguan listrik |
| 29 | E-029 | Gangguan koneksi internet |
| 30 | E-030 | Kebakaran |
| 31 | E-031 | Bencana Alam |
| 32 | E-032 | IP Scan |
| 33 | E-033 | Pencurian hardware |
| 34 | E-034 | Gangguan sinyal |
| 35 | E-035 | Kerusakan perangkat keras |
| 36 | E-036 | Cross Site Scripting |

Hasil dari identifikasi kerentanan pada SIAK UMMI disajikan pada Tabel VIII berikut.

TABEL VIII
DAFTAR KERENTANAN PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS MUHAMMADIYAH SUKABUMI

| Kode Aset | Kode Ancaman | Uraian Kerentanan | No. Skenario Ancaman |
|---|---|---|---|
| A-001 | E-030 | Tidak hati-hati dalam penggunaan api di lingkungan UMMI | 1 |
| | E-028 | Sumber atau aliran listrik di UMMI tidak stabil | 2 |
| | E-029 | Koneksi internet di UMMI tidak stabil | 3 |
| | E-033 | Kurang pengawasan dan keamanan pada penyimpanan perangkat keras di UMMI | 4 |
| | E-027 | Kurangnya pelatihan terhadap pengguna SIAK UMMI | 5 |
| | E-031 | Penempatan perangkat ditempat yang rawan bencana | 6 |
| A-002 | E-030 | Tidak hati-hati dalam penggunaan api di lingkungan UMMI | 7 |
| | E-028 | Sumber atau aliran listrik di UMMI tidak stabil | 8 |
| | E-029 | Koneksi internet di UMMI tidak stabil | 9 |
| | E-033 | Kurang pengawasan dan keamanan pada penyimpanan perangkat keras di UMMI | 10 |
| | E-027 | Kurangnya pelatihan terhadap pengguna SIAK UMMI | 11 |
| | E-031 | Penempatan perangkat ditempat yang rawan bencana | 12 |
| A-003 | E-006 | Password untuk akses point terlalu mudah atau disebar sembarangan | 13 |
| | E-034 | Akses poin disimpan terlalu jauh atau dekat dengan sumber gangguan sinyal | 14 |
| | E-033 | Perangkat keras jaringan komputer di UMMI | 15 |

| Kode Aset | Kode Ancaman | Uraian Kerentanan | No. Skenario Ancaman |
|---|---|---|---|
| | | kurang pengamanan | |
| | E-016 | Tidak ada pengawasan terhadap log aktivitas pengguna SIAK UMMI | 16 |
| | E-005 | Belum ada ketentuan batasan jika pengguna gagal login untuk akses internet | 17 |
| | E-026 | Sistem pengamanan perangkat lunak tidak dipebarui secara berkala, port yang tidak digunakan masih aktif, | 18 |
| | E-035 | Kurangnya pemeliharaan atau batas usia perangkat keras jaringan komputer di UMMI telah mencapai batas akhir | 19 |
| B-001 | E-025 | Kurangnya pemeliharaan sistem operasi pada komputer klien dan server di lingkungan UMMI secara berkala | 20 |
| | E-003 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 21 |
| | E-004 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 22 |
| | E-021 | Sistem operasi yang digunakan di komputer server dan klien UMMI tidak diperbarui | 23 |
| | E-011 | Data atau informasi yang dibagi di folder dalam jaringan UMMI tidak dilindungi dengan kata kunci | 24 |
| B-002 | E-005 | Belum ada ketentuan batasan jika pengguna gagal login pada aplikasi SIAK UMMI | 25 |
| | E-036 | Kurang lengkapnya pengujian terhadap aplikasi terutama yang berkaitan dengan tipe data yang dimasukkan | 26 |
| | E-006 | Password untuk masuk ke SIAK UMMI terlalu mudah | 27 |
| | E-027 | Kurangnya pahamnya pengguna dalam menggunakan SIAK UMMI, tidak ada panduan penggunaan, tampilan aplikasi tidak mudah digunakan, | 28 |
| | E-016 | Tidak adanya pencatatan log dari pengguna SIAK di UMMI | 29 |
| | E-017 | Kurangnya pengujian pada perangkat aplikasi SIAK UMMI | 30 |
| | E-018 | Kurangnya pemeriksaan terhadap tipe input data pada SIAK UMMI ketika selesai dibangun, kurangnya pemeliharaan SIAK UMMI | 31 |
| | E-019 | Kurangnya pemahaman pengguna SIAK UMMI terhadap file temporary | 32 |
| B-003 | E-014 | Aplikasi basis data yang digunakan untuk SIAK UMMI tidak diperbarui | 33 |
| | E-001 | Pengamanan data pada basis data SIAK UMMI tidak terlalu baik | 34 |
| | E-016 | Pengguna tidak melakukan logout setelah menggunakan SIAK UMMI, Tidak adanya pencatatan log dari pengguna | 35 |
| | E-022 | Pemeliharaan terhadap basis data dan aplikasi 23SIAK UMMI kurang dilakukan secara berkala | 36 |
| B-004 | E-003 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 37 |
| | E-004 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 38 |
| | E-023 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 39 |
| | E-024 | Kurang pahamnya pengguna SIAK UMMI untuk melakukan pembersihan terhadap | 40 |

| Kode Aset | Kode Ancaman | Uraian Kerentanan | No. Skenario Ancaman |
|---|---|---|---|
| | | temporary file setelah melakukan browsing | |
| B-005 | E-020 | Belum diterapkan filtering terhadap aplikasi Email UMMI | 41 |
| | E-021 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan terhadap email server UMMI | 42 |
| | E-003 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan terhadap email server UMMI | 43 |
| | E-004 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan terhadap email server UMMI | 44 |
| | E-016 | Belum ada kebijakan tentang penggunaan hak akses email UMMI | 45 |
| | E-005 | Belum ada kebijakan atau ketentuan batasan login pada email UMMI | 46 |
| | E-006 | Kata kunci untuk Email UMMI terlalu mudah | 47 |
| C-001 | E-015 | Kurangnya pelatihan dalam penggunaan aplikasi SIAK UMMI | 48 |
| | E-016 | Belum adanya kebjiakan dalam penggunaan hak akses terhadap SIAKUMMI | 49 |
| | E-011 | Kurangnya pengawasan terhadap data SIAK UMMI | 50 |
| | E-012 | Belum adanya kebijakan dalam pengolahan data SIAK UMMI | 51 |
| | E-008 | Kurangnya pemahaman pengelola atas kerahaasiaan data SIAK UMMI | 52 |
| | E-013 | Kurangnya pemahaman pengelola tentang pembagian hak akses SIAK UMMI | 53 |
| | E-027 | Proses rekrutment pegawai yang tidak sesuai dengan kebutuhan | 54 |
| C-002 | E-008 | Belum adanya kebjiakan tentang kerahasiaan data SIAK UMMI | 55 |
| | E-011 | Kurangnya pengawasan terhadap data SIAK UMMI | 56 |
| | E-009 | Belum adanya kebijakan tentang penghapusan dokumen-dokumen SIAK UMMI | 57 |
| | E-013 | Kurangnya sosialisasi tentang pentingnya akun pribadi SIAK UMMI | 58 |
| | E-015 | Kurangnya pemahaman pengguna akhir terhadap SIAK UMMI | 59 |
| | E-016 | Belum adanya kebijakan hak akses dalam penggunaan SIAK UMMI | 60 |
| D-001 | E-007 | Kebijakan penyimpanan dokumen tidak dilaksanakan dengan benar | 61 |
| | E-008 | Belum adanya kebijakan tentang kerahasiaan data | 62 |
| | E-009 | Belum adanya kebijakan dalam penghapusan data SIAK | 63 |
| | E-031 | Kebijakan penggunaan api yang tidak dipatuhi | 64 |
| D-002 | E-010 | Tidak adanya perlindungan terhadap file SIAK UMMI yang tesimpan di komputer | 65 |
| | E-011 | Tidak adanya perlindungan terhadap file SIAK UMMI yang tesimpan di komputer | 66 |
| | E-003 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 67 |
| | E-004 | Tidak terinstalasi atau tidak diperbaruinya aplikasi pengamanan komputer di komputer server dan klien di lingkungan UMMI | 68 |
| | E-012 | Tidak adanya mekanisme terhadap penggunaan komputer di lingkungan UMMI | 69 |
| D-003 | E-013 | Belum adanya kebijakan tentang pentingnya hak akses login ke SIAK UMMI | 70 |
| | E-012 | Tidak adanya pemeriksaan dari kebenaran data yang masuk ke SIAK UMMI | 71 |
| | E-001 | Tidak adanya perlindungan terhadap basis data SIAK UMMI | 72 |

| Kode Aset | Kode Ancaman | Uraian Kerentanan | No. Skenario Ancaman |
|---|---|---|---|
| | E-014 | Tidak adanya pemeliharaan secara berkala terhadap basis data SIAK UMMI | 73 |

Identifikasi dampak dari kemungkinan terjadinya risiko akan disajikan bersama dengan kriteria penilaian risiko.

*2) Analisis Risiko*: Pada tahapan ini akan dilakukan penilaian kemungkinan ancaman, penilaian konsekuensi atau dampak dan penilaian tingkat risiko yang mungkin terjadi pada SIAK UMMI. Hasil penilaian kemungkinan ancaman disajikan pada Tabel IX berikut.

TABEL IX
HASIL PENILAIAN KEMUNGKINAN ANCAMAN PADA SIAK UMMI

| Kriteria Kemungkinan Ancaman | No. Skrenario Ancaman |
|---|---|
| *Very unlikely (1)* | 32, 40, 46, 47, 54, 64, 70 |
| *Unlikely (2)* | 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 18, 23, 26, 28, 30, 31, 33, 36, 37, 38, 39, 42, 50, 51, 52, 53, 57, 63, 65, 72, 73 |
| *Possible (3)* | 2, 8, 14, 15, 16, 17, 19, 20, 24, 25, 34, 49, 55, 56, 58, 61, 62, 66, 67, 69, 71 |
| *Likely (4)* | 27, 29, 35, 43, 44, 45, 48, 59, 60, 68 |
| *Frequent (5)* | 21, 22, 41, |

Adapun hasil dari penilaian kemungkinan dampak risiko yang mungkin terjadi pada SAIK UMMI disajikan pada Tabel X berikut.

TABEL X
HASIL PENILAIAN DAMPAK DARI RISIKO YANG MUNGKIN TERJADI

| Kategori Dampak | No. Skrenario Ancaman |
|---|---|
| *Very Low (1)* | |
| *Low (2)* | |
| *Medium (3)* | 2, 3, 5, 8, 11, 12, 16, 19, 20, 21, 22, 23, 24, 27, 29, 36, 37, 39, 40, 45, 48, 50, 51, 52, 53, 55, 56, 57, 58, 59, 60, 62, 65, 70, |
| *High (4)* | 6, 12, 10, 13, 14, 15, 17, 18, 25, 26, 28, 31, 32, 34, 35, 38, 41, 43, 44, 46, 47, 49, 54, 61, 63, 66, 67, 68, 69, 71, 72 |
| *Very High (5)* | 1, 7, 4, 9, 30, 33, 42, 64, 73 |

Berdasarkan hasil penilaian kemungkinan ancaman dan dampak, maka dapat dilakukan penilaian risiko yang ada pada SIAK UMMI. Penilaian risiko dilakukan dengan mengalikan nilai *likelyhood* dengan nilai risiko yang didapat dari hasil identifikasi risiko. Adapun hasil dari penilaian risiko keamanan informasi pada SIAK UMMI disajikan pada Tabel XI.

TABEL XI
HASIL PENILAIAN TINGKAT RISIKO KEAMANAN INFORMASI PADA SIAK UMMI

| No. Skenario Ancaman | Nilai *Likelyhood* | Nilai Dampak | Nilai Risiko | Level Risiko |
|---|---|---|---|---|
| 1 | 2 | 5 | 10 | M |
| 2 | 3 | 3 | 9 | M |
| 3 | 2 | 3 | 6 | M |
| 4 | 2 | 5 | 10 | M |
| 5 | 2 | 3 | 6 | M |
| 6 | 2 | 4 | 8 | M |
| 7 | 2 | 5 | 10 | M |
| 8 | 2 | 3 | 6 | M |
| 9 | 2 | 5 | 10 | M |
| 10 | 2 | 4 | 8 | M |
| 11 | 2 | 3 | 6 | M |
| 12 | 2 | 3 | 6 | M |
| 13 | 2 | 4 | 8 | M |
| 14 | 3 | 4 | 12 | M |
| 15 | 3 | 4 | 12 | M |
| 16 | 3 | 3 | 9 | M |
| 17 | 3 | 4 | 12 | M |
| 18 | 2 | 4 | 8 | M |
| 19 | 3 | 3 | 9 | M |
| 20 | 3 | 3 | 9 | M |
| 21 | 5 | 3 | 15 | H |
| 22 | 5 | 3 | 15 | H |
| 23 | 2 | 3 | 6 | M |
| 24 | 3 | 3 | 9 | M |
| 25 | 3 | 4 | 12 | M |
| 26 | 2 | 4 | 8 | M |
| 27 | 4 | 3 | 12 | M |
| 28 | 2 | 4 | 8 | M |
| 29 | 4 | 3 | 12 | M |
| 30 | 2 | 5 | 10 | M |
| 31 | 2 | 4 | 8 | M |
| 32 | 1 | 4 | 4 | M |
| 33 | 2 | 5 | 10 | M |
| 34 | 3 | 4 | 12 | M |
| 35 | 4 | 4 | 16 | H |
| 36 | 2 | 3 | 6 | M |
| 37 | 2 | 3 | 6 | M |
| 38 | 2 | 4 | 8 | M |
| 39 | 2 | 3 | 6 | M |
| 40 | 1 | 3 | 3 | L |
| 41 | 5 | 4 | 20 | H |
| 42 | 2 | 5 | 10 | M |
| 43 | 4 | 4 | 16 | H |
| 44 | 4 | 4 | 16 | H |
| 45 | 4 | 3 | 12 | M |
| 46 | 1 | 4 | 4 | M |
| 47 | 1 | 4 | 4 | M |
| 48 | 3 | 4 | 12 | M |
| 49 | 3 | 4 | 12 | M |
| 50 | 2 | 3 | 6 | M |
| 51 | 2 | 3 | 6 | M |
| 52 | 2 | 3 | 6 | M |
| 53 | 2 | 3 | 6 | M |
| 54 | 1 | 4 | 4 | M |

| No. Skenario Ancaman | Nilai *Likelyhood* | Nilai Dampak | Nilai Risiko | Level Risiko |
|---|---|---|---|---|
| 55 | 3 | 3 | 9 | M |
| 56 | 3 | 3 | 9 | M |
| 57 | 2 | 3 | 6 | M |
| 58 | 3 | 3 | 9 | M |
| 59 | 4 | 3 | 12 | M |
| 60 | 4 | 3 | 12 | M |
| 61 | 3 | 4 | 12 | M |
| 62 | 3 | 3 | 9 | M |
| 63 | 2 | 4 | 8 | M |
| 64 | 1 | 5 | 5 | M |
| 65 | 2 | 3 | 6 | M |
| 66 | 3 | 3 | 9 | M |
| 67 | 3 | 4 | 12 | M |
| 68 | 4 | 4 | 16 | H |
| 69 | 3 | 4 | 12 | M |
| 70 | 1 | 3 | 3 | L |
| 71 | 3 | 4 | 12 | M |
| 72 | 2 | 4 | 8 | M |
| 73 | 2 | 5 | 10 | M |

*7) Evaluasi Risiko*: Pada tahap ini akan dilakukan proses inventaris kembali profil risiko yang ada pada SIAK UMMI berdasarkan pada keterhubungan antara frekuensi terjadinya ancaman dan nilai dampak. Selain itu juga akan diurutkan level risiko dari yang tertinggi ke yang terendah. Hasil kedua data tersebut disajikan pada Tabe XII dan Tabel XIII.

TABEL XII
DAFTAR SKENARIO ANCAMAN SIAK UMMI BERDASAR PADA NILAI *LIKELYHOOD* DAN NILAI DAMPAK

| | | **Kemungkinan Terjadinya Ancaman (*Likelyhood*)** | | | | |
|---|---|---|---|---|---|---|
| | | *1* | *2* | *3* | *4* | *5* |
| **Dampak** | *5* | 64, | 1,4,7,9, 30, 33, 42, 73 | | | |
| | *4* | 32, 46, 47, 54, | 6,10,13,18 ,26, 28, 31, 38, 63, 72 | 14,15, 17, 25, 34, 48, 49, 61, 67, 69, 71, | 35, 43, 44, 68, | 41 |
| | *3* | 40, 70 | 3,5,8,11,1 2,23, 36, 37, 39, 50, 51, 52, 53, 57, 65, | 2,16,19,20 , 24, 55, 56, 58, 62, 66, | 27,29, 45, 59, 60, | 21, 22 |
| | *2* | | | | | |
| | *1* | | | | | |

Adapun level risiko yang mungkin terjadi ada pada SIAK UMMI berdasarkan skenario ancaman disajikan pada Tabel XIII berikut.

TABEL XIII
DAFTAR LEVEL RISIKO YANG MUNGKIN TERJADI PADA SIAK UMMI

| Level Risiko | Nomor Skenario Ancaman |
|---|---|
| Low (L) | 40, 70 |
| Medium (M) | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 42, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 69, 71, 72, 73 |
| High (H) | 21, 22, 35, 41, 43, 44, 68 |

*C. Penanganan Risiko*

Pada proses ini akan dilakukan pemilihan tindakan yang akan diambil terhadap risiko yang telah diidentifikasi sebelumnya. Hasilnya akan menjadi rencana penanganan risiko. Proses penanganan risiko yang mungkin ada pada SIAK UMMI dilakukan berdasarkan hasil penilaian risiko dan kriteria penanganan risiko dengan memperhitungkan biaya pemulihan, level dan biaya transfer risiko. Kriterianya pemilihan model penanganan risiko telah disebutkan pada Tabel IV. Adapun rencana penanganan risiko disajikan pada Tabel XIV. Rencana penanganan risiko yang ditampilkan pada Tabel XIV hanya dilakukan pada skenario ancaman yang tidak bisa diselesaikan oleh pengendalian yang telah dilakukan oleh UMMI pada masa sekarang.

TABEL XIV
RENCANA PENANGANAN RISIKO PADA SIAK UMMI

| No Skenario Ancaman | Level Risiko | Biaya Pemulihan | Penanganan Risiko |
|---|---|---|---|
| 13 | M | L | RM |
| 17 | M | H | RA |
| 18 | M | H | RA |
| 19 | M | H | RS |
| 20 | M | L | RM |
| 21 | H | L | RA |
| 22 | H | L | RA |
| 23 | M | L | RM |
| 24 | M | M | RA |
| 25 | M | H | RA |
| 26 | M | H | RA |
| 27 | M | H | RA |
| 28 | M | M | RM |
| 30 | M | M | RM |
| 31 | M | H | RA |
| 32 | M | H | RA |
| 33 | M | H | RA |
| 35 | H | M | RA |
| 36 | M | M | RM |
| 37 | M | M | RM |
| 38 | M | H | RA |
| 39 | M | M | RM |
| 40 | L | M | RM |
| 45 | M | H | RA |
| 46 | M | H | RA |
| 47 | M | H | RA |
| 48 | M | L | RM |
| 49 | M | H | RA |
| 50 | M | H | RA |
| 52 | M | M | RM |
| 53 | M | H | RA |
| 54 | M | M | RM |

| No Skenario Ancaman | Level Risiko | Biaya Pemulihan | Penanganan Risiko |
|---|---|---|---|
| 13 | M | L | RM |
| 17 | M | H | RA |
| 18 | M | H | RA |
| 19 | M | H | RS |
| 20 | M | L | RM |
| 21 | H | L | RA |
| 22 | H | L | RA |
| 23 | M | L | RM |
| 24 | M | M | RA |
| 55 | M | M | RM |
| 56 | M | H | RA |
| 57 | M | H | RA |
| 58 | M | M | RM |
| 59 | M | M | RM |
| 60 | M | M | RM |
| 62 | M | M | RM |
| 63 | M | M | RM |
| 66 | M | H | RA |
| 67 | M | H | RA |
| 68 | H | M | RA |
| 69 | M | H | RA |
| 70 | L | M | RM |
| 73 | M | H | RA |

Keterangan:
RM = *Risk Modification* RA = *Risk Avoidance*
RS = *Risk Sharing*

Dari 73 skenario ancaman yang mungkin terjadi, 26 skenario ancaman dapat diselesaikan dengan model keamanan yang telah dilakukan oleh UMMI pada saat ini dan 47 skenario ancaman lainnya dilakukan rencana penanganan seperti pada Tabel XIV di atas. Daftar rencana penanganan ini menjadi rekomendasi untuk pihak pengambil kebijakan dalam menangani risiko pada Sistem Informasi Akademik UMMI.

### *D. Penerimaan Risiko*

Penerimaan risiko keamanan pada Sistem Informasi akademik (SIAK ) Universitas Muhammadiyah Sukabumi (UMM) merupakan langkah dalam penentuan keputusan penerimaan dari rencana penanganan yang telah dibuat. Tahapan ini dilakukan melalui proses diskusi dengan pihak pengelola dan pengambil kebijakan SIAK UMMI.

## V. KESIMPULAN

Hasil dari pengelolaan risiko pada Sistem Informasi Akademik (SIAK) Universitas Muhammadiyah Sukabumi (UMMI) dapat diketahui bahwa aset SIAK UMMI terbagi menjadi empat aset utama, yaitu perangkat keras dan jaringan, perangkat lunak aplikasi dan pendukung SIAK UMMI, sumber daya manusia dan data serta informasi yang ada pada SIAK UMMI. Berdasarkan proses penilaian risiko, terdapat 73 skenario ancaman yang mungkin terjadi dengan kategori level risiko rendah sampai tinggi, yaitu 2 risiko level rendah (*low*), 7 risiko level tinggi (*high*) dan 64 risiko level sedang (*medium*).

Rencana penanganan risiko dibuat berdasarkan analisis level risiko dan pengendalian yang telah dilakukan oleh pihak pengelola SIAK UMMI. Untuk itu, didapatkan 47 skenario ancaman yang harus ditangani karena belum bisa diselesaikan oleh pengendalian yang telah ada. Hasil dari pemilihan perlakuan terhadap risiko yaitu 19 akan dilakukan modifikasi, 1 risiko ditransfer, dan 27 risiko dihindari. Adanya rencana penganangan risiko ini menjadi rekomendasi bagi pihak SIAK UMMI dalam pengelolaan risiko pada SIAK UMMI sehingga proses penangan risiko sesuai dengan yang seharusnya.

## UCAPAN TERIMA KASIH

Pada kesempatan ini saya ingin mengucapkan terima kasih kepada pihak Kementrian Riset dan Teknologi Republik Indonesia atas hibah yang telah diberikan untuk SKIM PDP untuk Tahun Anggaran 2018, Universitas Muhammadiyah Sukabumi (UMMI) sebagai tempat penelitian dan Program Studi Teknik Informatika UMMI. Semoga ke depannya dapat melakukan penelitian dengan lebih baik.

## DAFTAR PUSTAKA

[1] H. Zaskuri, (2013) Headlines News homepage on CISO. [Online]. Tersedia: http://www.ciso.co.id/2013/10/cyber-security-awareness-perguruan-tinggi-dan-ancaman-digital/.

[2] C. Chazar, “Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/IEC 27001:2005,” *Jurnal Informasi*, vol. VII, no. 2, pp. 48-57, 2015.

[3] Asriyanik and M. Hendayun, "Tata Kelola Teknologi Informasi Menggunakan COBIT 5," *Jurnal Teknik Informatika dan Sistem Informasi (JuTISI)*, vol. III, no. 1, pp. 206-216, 2017.

[4] N. A. N. Dewi and I. G. P. H. Yudana, "Analisa Manajemen Risiko pada Sistem Akademik di STMIK STIKOM Bali," *Seminar Nasional Teknologi Informasi dan Multimedia*, 2016, paper 1.5, p. 7

[5] S. Ritchie, Security Risk Management, Atlanta, Atlanta: HA&W, 2013.

[6] Kementrian Komunikasi dan Informatika RI, Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, Jakarta: Kemkominfo RI, 2016.

[7] R. Sarno and I. Iffano, Sistem Manajemen Keamanan Informasi Berbasis ISO 27001, Surabaya: ITSPress, 2009.

[8] W. Syafitri, "Penilaian Risiko Keamanan Informasi menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)," *Jurnal CorelIT*, vol. II, no. 2, pp. 8-13, 2016.

[9] M. P. Mokodompit and Nurlaela, "Evaluasi Keamanan Sistem Informasi Akademik Menggunakan ISO 17799:2000," *Jurnal Sistem Informasi Bisnis*, vol. II, no. 2, pp. 94-104, 2016.

[10] Badan Standarisasi Nasional, Manajemen Risiko Keamanan Informasi (ISO/ IEC 27005:2011), Jakarta: BSN, 2013.

[11] Tim Direktorat Keamanan Informasi, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, Jakarta, Jakarta: Kementrian Komunikasi dan Informatika RI, 2011.

[12] A. Saut and K. Surendro, "Perancangan Model Penilaian Kapabilitas Proses Manajemen Resiko Keamanan Informasi Menggunakan ISO 27005 Dan ISO 33020 Studi Kasus: Pusat Komunikasi Kementerian Luar Negeri," *Seminar Nasional Teknologi Informasi*, 2016, paper B.6, p. 26.

[13] Sugiyono, Metode Penelitian Pendekatan Kuantitatif, Kualitatif dan R&D, Bandung: Alfa Beta, 2014.