Jurnal ICT : Information Communication & Technology
Vol. 23, N0.1, Juli 2023, pp. 117-123
p-ISSN: 2302-0261, e-ISSN: 2303-3363

Sistem Manajemen Keamanan Informasi Perlindungan Nilai Matakuliah berbasis ISO 27001

Tuti Hartati[1*], Gema Parasti Mindara[2], Citra Lestari Mindara[3]
[1]Program Studi Teknik Informatika, Universitas Wanita Internasional, Indonesia
[2]Program Studi Teknologi Rekayasa Komputer, Sekolah Vokasi IPB, Indonesia
[3] Program Studi Teknik Informatika, Universitas Langlangbuana, Indonesia
Email: [1]toohart2013@gmail.com, [2]gemaparasti@apps.ipb.ac.id, [3]citramindara@gmail.com

INFORMASI ARTIKEL

Histori artikel:

Naskah masuk, 22 Juli 2023
Direvisi, 28 Juli 2023
Diiterima, 31 Juli 2023

Kata Kunci:

SMKI, ISO 27001, Nilai Mata Kuliah
.

ABSTRAK

Abstract- *Information Security Management System (ISMS) has become increasingly crucial in the field of higher education. ISMS focuses on safeguarding sensitive data and critical information from security threats that may exist in the academic environment. This includes personal student data, course grades, financial information, and others. The aim of ISMS is to maintain the confidentiality, integrity, and availability of academic data, thus ensuring the accuracy and reliability of academic information that impacts assessment and decision-making processes. ISMS is implemented to prevent data manipulation, grade changes, and unauthorized access that could harm students, faculty, and academic staff. The implementation of ISMS involves steps such as security risk assessment, development of security policies and procedures, as well as training and awareness for all members of the academic community. In an increasingly digitally connected environment, security risks are on the rise. Therefore, it is essential to properly implement ISMS, ensuring that the technological infrastructure and information systems have adequate security layers and providing limited and controlled access to authorized personnel. This research utilizes a qualitative descriptive method. The outcome of this study is a set of procedures and policies for monitoring and evaluating the protection of course grades.*

Abstrak- Sistem Manajemen Keamanan Informasi (SMKI) menjadi semakin krusial dalam bidang pendidikan tinggi. SMKI berfokus pada perlindungan data yang sensitif dan informasi penting dari ancaman keamanan yang mungkin ada di lingkungan akademik. Seperti halnya data pribadi mahasiswa, nilai matakuliah, keuangan dan lain-lain. Tujuan dari SMKI ini adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data akademik, sehingga dapat memastikan kebenaran dan keandalan informasi akademik yang berdampak pada penilaian dan pengambilan keputusan. SMKI diterapkan untuk mencegah manipulasi data, perubahan nilai, dan akses tidak sah yang dapat merugikan mahasiswa, dosen, dan staf akademik. Penerapan SMKI melibatkan langkah-langkah seperti penilaian risiko keamanan, pengembangan kebijakan dan prosedur keamanan, serta pelatihan dan kesadaran bagi seluruh anggota komunitas akademik. Dalam lingkungan yang semakin terhubung secara digital, risiko keamanan semakin meningkat. Oleh karena itu, penting untuk menerapkan SMKI dengan tepat, memastikan bahwa infrastruktur teknologi dan sistem informasi memiliki lapisan keamanan yang memadai, serta menyediakan akses yang terbatas dan terkontrol bagi pihak yang berwenang. Penelitian ini menggunakan metode deskriptif kualitatif. Luaran dari penelitian ini adalah sebuah prosedur dan kebijakan dalam *monitoring* dan evaluasi untuk perlindungan nilai mata kuliah.

Penulis Korespondensi*:*

Tuti Hartati
Program Studi Teknik Informatika,
Univeristas Wanita Internasional
Jl. Pasirkaliki No. 179 Bandung, Jawa Barat, Indonesia
Email: toohart2013@gmail.com

Jurnal ICT : Information Communication & Technology
Vol. 23, N0.1, Juli 2023, pp. 117-123
p-ISSN: 2302-0261, e-ISSN: 2303-3363

1. Pendahuluan

Perguruan Tinggi adalah sebuah lembaga yang akan menghasilkan generasi muda harapan bangsa serta membanggakan keluarga dan negara. Untuk itu perguruan tinggi harus memegang teguh kepercayaan masyarakat yang menitipkan putra dan putrinya untuk dididik dengan baik. Dengan kepercayaan masyarakat tersebut maka perguruan tinggi akan menjaga amanah itu dengan baik. Hal ini di buktikan melalui prosedur - prosedur yang jelas serta peraturan dan kebijakan terstruktur dengan baik yang harus ditaati dan dilaksanakan oleh semua unsur sivitas akademik.

Dalam kehidupan sehari-hari tidak bisa dipungkiri peluang dari ketidak jujuran sering terjadi di lingkungan perguruan tinggi, hal ini terjadi karena ada peluang dan kurang pengawasan (*monitoring*) serta evaluasi dalam sistem kerja yang sedang berlangsung terutama dalam masalah keamanan dan keaslian nilai mata kuliah yang di berikan oleh dosen pengampu mata kuliah. Dampak semua itu menimbulkan peluang terjadi perubahan nilai mata kuliah oleh pihak internal yang tidak diketahui oleh dosen pengampu mata kuliah maupun pimpinan perguruan tinggi. Apabila hal ini dibiarkan terus, maka akan berdampak kepada nama baik perguruan tinggi di kemudian hari.

Dengan mengkaji latar belakang di atas, maka dapat di identifikasi masalah yang terjadi adalah minimnya pengawasan (*monitoring*) dalam sistem kerja, sehingga peluang melakukan kecurangan oleh staf bisa terjadi, belum sempurnanya pengawasan dalam standar operasional prosedur (SOP) yang terkait dengan sistem alur keamanan nilai mata kuliah dari dosen pengampu mata kuliah.
Serta belum ada kebijakan yang tegas terkait dengan etos kerja dan kejujuran dari pimpinan kepada seluruh staf dan pimpinan akademik.

Peneliti akan membuat rumusan masalah berdasarkan identifikasi diatas, yaitu bagaimana meningkatkan *monitoring* dan evaluasi dengan baik berdasarkan struktur organisasi yang diterapkan kepada staf dan pimpinan akademik, bagaimana penyempurnaan SOP yang berhubungan dengan proses pengumpulan nilai dari dosen pengampu mata kuliah sampai pengumuman nilai kepada mahasiswa dibawah pengawasan tim penjaminan mutu serta membuat kebijakan yang tertuang dalam peraturan secara jelas dan tegas untuk semua staf dan pimpinan akademik agar dapat menjaga amanah dengan baik.

Dalam penelitian ini maka penulis bermaksud membuat Sistem Manajemen Keamanan Informasi (SMKI) menggunakan standar ISO 27001 untuk melindungi data nilai mata kuliah agar terjaga sesuai dengan yang diberikan oleh dosen pengampu mata kuliah tersebut.

Tujuan penelitian ini untuk menjaga keamanan dan keaslian data nilai mata kuliah yang disampaikan oleh dosen pengampu mata kuliah tersebut serta menjaga kepercayaan dari mahasiswa, dosen, pimpinan pada khususnya dan masyarakat pada umumnya terhadap kredibilitas yang baik dan berkualitas pada perguruan tinggi tersebut.

Dalam penelitian ini,penulis akan mengadopsi dari beberapa penelitian sebelumnya sebagai acuan atau referensi pada penelitian ini. Adapun beberapa kajian dari peneliti sebelumnya adalah [1] “Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013”, yang menerangkan bagaimana sebuah organisasi harus menjaga aset informasi dan pentingnya pengidentifikasi ancaman baik dari internal maupun dari ekternal serta membuat perancangan dalan kontrol keamanan untuk menjaga aset informasi. Peneliti ke 2 [2] “Analisis dan Penerapan Sistem Majemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001” pada penelitian ini menerangkan bagaimana pentingnya sebuah pengawasan yang dapat dilihat dari beberapa sudut pandang untuk menjaga aspek keamanan dan ketahanan dari sebuah aplikasi. Penelitian yang ke 3 sebagai rujukan adalah
[3] ”Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) pada Fakultas Teknik UIKA-BOGOR”, pada penelitian ini menerangkan pengelolaan sebuah informasi yang sangat sensitif terhadap institusi untuk menjaga agar tetap aman.

Dalam penelitian ini penulis akan mengkaji kepada bagaimana prosedur sistem manajemen keamanan informasi lebih terinci pada proses monitoring dan evaluasi nilai mata kuliah di perguruan tinggi agar tetap terjaga dalam kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*availability*)

2. Dasar Teori

2.1. *Sistem*

Definisi sistem menurut (Jogiyanto) dalam bukunya yang judul “*Sistem Teknologi Infomasi* ”, menyatakan bahwa : “ Sistem adalah suatu jaringan kerja dari prosedur -prosedur yang saling berhubungan, berkumpul bersama -sama untuk melakukan suatu kegiatan atau untuk menyelesaikan suatu sasaran yang tertentu[4].

2.2. *Informasi*

Secara etimologis istilah “informasi” berasal dari bahasa Latin, yaitu “*Informatinem*” yang artinya ide, kode, atau garis besar. Menurut (Gordon B.Davis) dalam bukunya berjudul “*Management Information System*” , Informasi adalah data yang sudah diproses menjadi bentuk lain yg berguna bagi pemakai dan mempunyai nilai pikir yang nyata bagi pembuatan keputusan pada saat sedang berjalan atau prospek masa depan [5].

2.3. *Keamanan Informasi*

Keamanan informasi terdiri dari empat bidang yaitu : organisasi, orang, proses, dan teknologi. Menurut (Whitman dan Mattord, 2010) keamanan informasi merupakan suatu bentuk perlindungan terhadap informasi dan unsur-unsur penting yang ada didalamnya seperti kerahasiaan, integritas, dan ketersediaan tidak terkecuali sistem dan hardware untuk menyimpan dan mengirim informasi tersebut. Tiga unsur penting dari keamanan informasi yaitu :

1) Kerahasiaan (*Confidentiality*)
   Kerahasiaan merupakan unsur untuk memastikan suatu informasi tersebut hanya bisa diakses oleh pihak yang memiliki wewenang atas akses ke informasi tertentu.
2) Integritas (*Integrity*)
   Integritas merupakan unsur yang memastikan bahwa kualitas, keutuhan, dan kelengkapan data terjaga sesuai dengan keaslian data.
3) Ketersediaan (*Availability*)
   Kerahasiaan merupakan unsur yang memastikan bahwa pihak yang memiliki hak akses ke suatu informasi dapat mengakses informasi tersebut dalam bentuk yang dibutuhkan tanpa gangguan atau hambatan.[6]

2.4. *Manajemen Keamanan Informasi*

Dalam melihat aspek dari manajemen keamanan informasi mempunyai 4 fase yaitu :

1) Identifikasi Ancaman,
   Ancaman bisa datang dari *internal* atau dari *ekternal* , yang dapat menyerang aset institusi baik itu aset informasi ataupun aset lain.
2) Identifikasi Risiko
   Tindakan ilegal yang menyebabkan resiko dapat digolongkan ke dalam empat jenis: a. Pencurian; b. Penyalahgunaan hak akses ; c. Pengrusakan dan d. Modifikasi yang ilegal.
3) Penetapan Kebijakan Keamanan Informasi
   Organisasi harus membuat sebuah kebijakan untuk menjaga keamanan informasi dan diterangkan berlaku untuk semua.
4) Penerapan pengawasan untuk mengatasi risiko.
   Penerapan pengawasan ini sangat penting untuk menghindari atau meminimalisir tingkat risiko yang lebih besar sebagai dampaknya.

2.5. *ISO - 27001*

ISO 27001 adalah suatu standar internasional untuk *Information Security Manajemen System* (ISMS). ISO 27001 berlaku untuk semua bisnis. keamanan informasi yang dimiliki dalam bentuk apapun, bukan hanya berupa data elektronik.

Gambar 1. Lingkup ISO
(Sumber : ISO 27001 Compliance-2023 COMPLETE GUIDE)[7]

Ada dua versi ISO 27001 yaitu 27001: 2013 dan 27001: 2005. Adapun perbedaannya adalah :

1) ISO 27001: 2013 memiliki 114 kendali (kontrol) dalam 14 kelompok domain,
2) ISO 27001: 2005 memiliki 133 kendali (kontrol) dalam 11 kelompok domain.

Beberapa perubahan sebagai perkembangan dari ISO 27001:2013 dibandingkan dengan ISO 27001: 2005 dikarenakan perkembangan dari teknologi yang mana berubahnya paradigma suatu kegiatan yang beralih menggunakan media digital sehingga mengakibatkan banyak hal kejadian di media digital ini yang memerlukan pengawasam dan pengendalian yang berhubungan dengan peluang tingkat kejahatan semakin marak melalui media sosial ini.

Tabel. 1. *Perbedaan ISO/IEC 27001: 2005 dengan ISO/IEC 27013[6]*

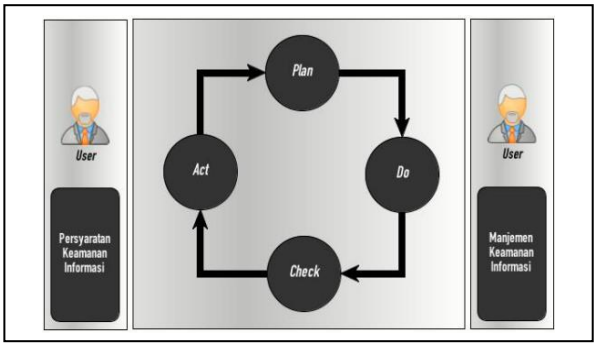
Summary Of Changes	
ISO/IEC 27001 : 2005	**ISO/IEC 27001 : 2005**
132 Shall Steatment section 4 to 8	125 Shall Steatment section 4 to 11
Annexure A	Annexure A
11 clauses	14 clauses
39 categories	35 categories
133 controls	114 controls

2) *Organization of Information Security*
3) *Human Resources Security*
4) *Asset Management*
5) *Access Control*
6) *Cryptography*
7) *Physical and Environmental Security*
8) *Operational Security*
9) *Communications Security*
10) *System Acquisition, Development, and Maintenance*
11) *Supplier Relationships*
12) *Information Security Incident Management*
13) *Compliance*
14) *Information Security Aspects of Business Continuity Management* [7]

2.6. *Sistem Manajemen Keamanan Informasi (SMKI)*

Sistem Manajemen Keamanan Informasi (SMKI) adalah kerangka kerja atau pendekatan yang digunakan oleh organisasi untuk memastikan keamanan informasi

yang efektif. SMKI melibatkan proses merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitoring dan meninjau (*Check*), serta memelihara dan meningkatkan atau mengembangkan *(Act)* terhadap keamanan informasi organisasi/perusahaan/perguruan tinggi. Proses dari *Plan*, *Do*, *Check* dan *Act* biasa di sebut dengan sistem PDCA.



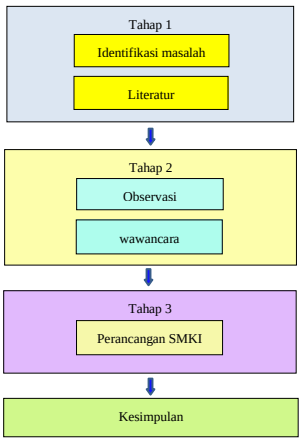
Gambar 2. *Siklus PDCA dalam Aplikasi SMKI (Sarno dan Iffano, 2009)*

Sistem Manajemen Keamanan Informasi memberikan perlindungan informasi dan penghitungan aset. Terdapat tiga komponen kunci dalam menyediakan jaminan layanan keamanan informasi, diantaranya :

1) *Confidentiality*/Kerahasiaan. Data hanya boleh diakses oleh yang berwenang.
2) *Integrity*/Integritas.Informasi tidak boleh berubah (tampered, altered, modifield) oleh pihak yang tidak berhak.
3) *Availability*/Ketersediaan. Informasi harus tersedia ketika dibutuhkan.

3. Metode Penelitian

Pada penelitian ini dilakukan dengan menggunakan deskriptif kualitatif dengan cara pengumpulan data melalui observasi dan wawancara dengan yang terlibat langsung kepada pelaksana kegiatan akademik.



Gambar 3. *Tahapan Penelitian*

Metode Penelitian merupakan rancangan pelaksanaan penelitian secara sistematis mengarah pada hasil yang dituliskan secara jelas dengan memuat teknik pengambilan data dan analisis yang digunakan untuk memperoleh hasil, selain itu dapat memuat jumlah responden yang digunakan dalam penelitian. Penulisan

4. *Hasil dan Analisa*

4.1. *Sistem Manajemen Keamanan Informasi Nilai Mata Kuliah.*

Sistem Manajemen Keamanan Informasi (SMKI) di bidang akademik adalah kerangka kerja yang digunakan perguruan tinggi untuk menjaga keamanan informasi dengan tujuan melindungi data dan informasi yang sensitif, termasuk data mahasiswa, nilai mata kuliah, informasi penelitian, informasi administratif, dan lainnya, dari ancaman yang dapat menimbulkan suatu risiko yang mungkin bisa terjadi.

Dalam bidang akademik, keamanan informasi menjadi hal yang sangat penting karena perguruan tinggi akan mengelola dan menyimpan berbagai jenis data sensitif yang melibatkan banyak pihak, termasuk mahasiswa, dosen, staf, dan pihak eksternal.

Tabel 2. Keterangn PDCA

No		Keterangan
1	*Plan*	Tahapan perencanaan dimulai dengan sebuah identifikasi masalah. Plan terdiri dari 5 W yaitu *what, who, whe, where,* dan *why* .
2	*Do*	Tahapan melaksanakan apa yang telah direncanakan sebelumnya, apabila ada kendala maka segera mencari solusi untuk mengatasi masalah tersebut.
3	*Check*	Pada tahapan ini dilakukan pengecekan, pengawasan serta audit untuk mengetahui apakah semua sudah sesuai dengan rencana sebelumnya ? apabila ada kendala maka harus segera dilakukan evaluasi dan memperbaiki kesalahan yang terjadi.
4	*Act*	Tahapan terakhir sebagai implementasi setelah memperbaiki semua kelemahan pada proses *DO* dan *Check*. Pada tahap ini akan menjadi role model PDCA yang akan di jalankan. PDCA adalah proses secara siklus bertujuan untuk selalu monitoring, evaluasi dan melakukan pengembangan-pengembangan.

Beberapa tujuan utama dari SMKI di bidang akademik yang terkait dengan keamanan nilai mata

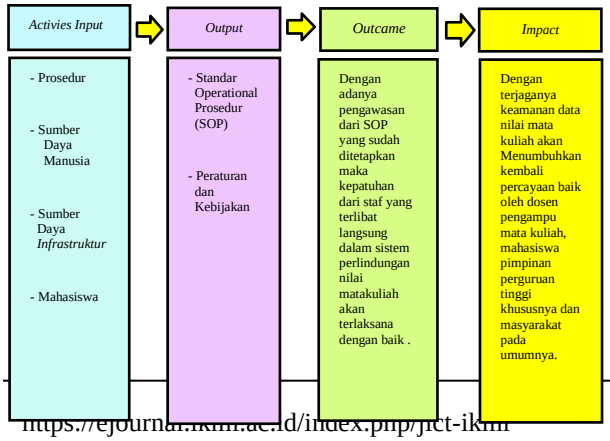
kuliah adalah 1) Melindungi Kerahasiaan, memastikan data sensitif seperti informasi pribadi mahasiswa, nilai mata kuliah, atau informasi keuangan, hanya dapat diakses oleh pihak yang berwenang 2)Menjaga Integritas Data: mencegah perubahan atau manipulasi yang tidak sah pada data dan informasi akademik yang dapat mempengaruhi kebenaran dan keandalan informasi, 3) Memastikan Ketersediaan, menjamin ketersediaan sistem dan layanan akademik sehingga mahasiswa, dosen, dan staf dapat mengakses data dan informasi yang mereka butuhkan dengan cepat dan tanpa gangguan. 4) Mengelola Risiko Keamanan, Melakukan identifikasi dan evaluasi risiko keamanan yang mungkin ada dalam lingkungan akademik dan mengimplementasikan tindakan pengendalian apabila ada prosedur yang di langgar oleh mahasiswa, dosen dan staff, 5) Menjaga Kepercayaan, membangun dan mempertahankan kepercayaan dari mahasiswa, dosen, dan pihak lainnya dengan melindungi data mereka dengan baik dan menghargai privasi mereka.

SMKI di bidang akademik terutama dalam kaitan dengan perlindungan data untuk nilai mata kuliah semakin penting, karena data harus terlindungi dengan baik mengingat banyak faktor peluang untuk terjadi ketidakamanan data seperti prosedur yang lemah, pengawasan terhadap kinerja staf yang melemah dan pertumbuhan teknologi informasi serta ketergantungan yang pada sistem komputer yang berhubungan dengan keamanan jaringannya. Perlindungan data dan informasi menjadi suatu prioritas yang sangat penting untuk menjaga reputasi perguruan tinggi dan menjaga kepercayaan seluruh anggota sivitas akademik dan kepercayaan masyarakat terhadap perguruan tinggi tersebut..

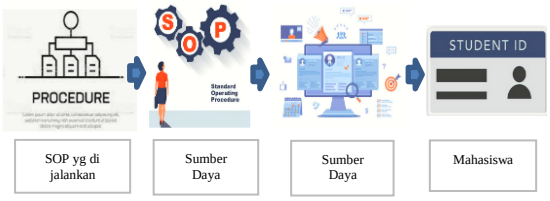
Pada penelitian ini penulis mengambil beberapa *Clause* dari ISO 27001 yaitu : *Information Security Policies , Organization of Information Security, Human Resources Security , Asset Management, Access Control, Operational Security , Compliance*

4.2. *Framework SMKI Perlindungan Nilai Mata Kuliah.*

Untuk membuat *Framework* SMKI Perlindungan Nilai Matakuliah dapat di lihat pada gambar 4. di bawah ini :



Gambar 4: Framework SMKI Perlindungan Nilai Mata Kuliah



Gambar 5 : *Activitas Input*

D.3. Lingkup Penelitian dan Analisa masalah

Lingkup penelitian terhadap keamanan nilai mata kuliah yang di lakukan oleh penulis melibatkan beberapa unsur yaitu : Prosedur, Sumber Daya Manusia, Sistem Informasi, Mahasiswa dan Pemangku Kebijakan.

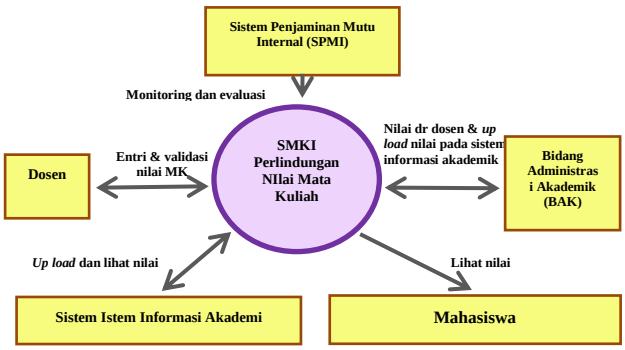
1. Prosedur, menerangkan bagaimana proses yang harus di
   lakukan para dosen pengampu mata kuliah untuk menyerahkan daftar nilai kepada Bidang Administrasi Akademik (BAK).
2. BAK, akan menerima daftar nilai mata kuliah dan akan memasukkannya kepada sistem akademik untuk dapat di lihat hasilnya oleh para mahasiswa
3. Sistem informasi bidang akademik, akan menampilkan daftar nilai yang sudah di up load sehingga dapat di lihat nilainya oleh mahasiswa.
4. Mahasiswa, akan memperoleh informasi nilai mata kuliah melalui sistem informasi yang di sediakan oleh kampus baik melalui Hp atau melalui Laptop.

Menganalisa dari prosedur di atas, maka dapat di lihat peluang-peluang untuk terjadi ketidakamanan dalam menjaga keaslian nilai matakuliah. Adapun peluang tersebut bisa di lakukan karena :

a. Lemahnya *monitoring* dan evaluasi dalam pelaksanaan prosedur *up load* nilai mata kuliah yang dapat di lakukan oleh internal,
b. Ketidak jujuran dari personal baik admin maupun personal lain yang mempunyai hak akses dalam entri nilai matakuliah tersebut,
c. Tidak ada proses validasi nilai oleh dosen pengampu terhadap nilai yang sudah di upload oleh admin, sehingga dosen pengampu mata kuliah tidak mengetahui apa nilai yang sudah di berikan itu masih asli atau sudah terjadi perubahan nilai tidak sesuai dengan aslinya.

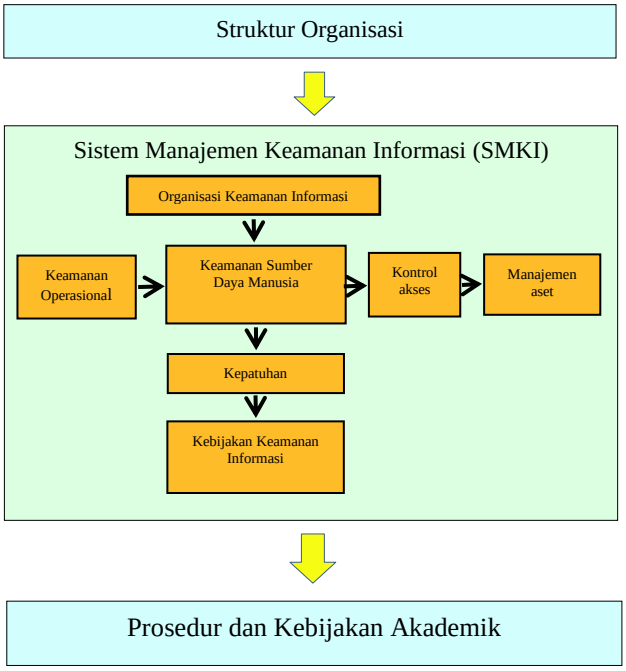
Untuk mengatasi masalah tersebut maka dalam perancangan Sistem Manajemen Keamanan Informasi (SMKI) untuk perlindungan nilai mata kuliah kontek

diagramnya di terangkan pada gambar 6 sebagai berikut ini :



Gambar 6. *Data Flow Diagram Nilai Mata Kuliah (MK)*

Peranan penjaminan mutu dalam struktur organisasi sangat memegang peranan penting untuk melakukan monitoring dan evaluasi terhadap implementasi dari SMKI, yang dapat di gambarkan seperti gambar 7 di bawah



Gambar 7 : *Monitoring SMKI*

Struktur organisasi merupakan hal yang paling penting dalam menjalankan kegiatan di perguruan tinggi, sebagai bentuk koordinasi antar satu bagian dengan bagian lain. Struktur organisasi akan berjalan dengan baik apabila masing-masing bagian mengerjakan tugas sesuai dengan tugasnya dan menjalankan amanah yang di berikan oleh pimpinan. Salah satu hal yang harus diperhatikan yaitu bagaimana struktur organisasi dapat merencanakan dan menjalankan semua proses dengan mengacu kepada sistem manajemen keamanan informasi (SMKI). Hal ini sangat penting untuk menjaga keamanan informasi yang di kelola karena menyangkut data-data sensitif terutama dibidang akademik seperti perlindungan data nilai matakuliah dari ancaman internal dan ekternal. Dalam struktur organisasi ini ada bagian penjaminan mutu yang dapat melakukan monitoring dan evaluasi setiap kegiatan. Dengan adanya monitoring ini maka dapat meminimalisir peluang-peluang ketidak amanan yang di timbukan baik dari internal maupun dari ekternal melalui melalui proses SMKI ini. Seorang pimpinan yang baik harus dapat memastikan bahwa SMKI telah diimplementasikan dengan baik serta semua anggota sivitas akademik mempunyai kesadaran tinggi, bagaimana mereka harus selalu menjaga keamanan informasi.

Kesimpulan dan Saran

Sistem Manajemen Keamanan Informasi merupakan hal yang sangat penting untuk diterapkan pada perguruan tinggi , pemerintahan, industri dan lainnya karena merupakan salah satu proses untuk menjaga keamanan informasi.

Dengan diterapkan sistem manajemen keamanan informasi melalui peraturan dan kebijakan perguruan tinggi serta adanya monitoring dan evaluasi oleh penjaminan mutu akan meminimalisir peluang kecurangan dan kejahatan yang dilakukan oleh pihak internal ataupun serangan dari ekternal. Dengan demikian nilai akan tetap terjaga keasliannya karena sudah tervalidasi oleh dosen pengampu mata kuliah tersebut. Peningkatan monitoring dan evaluasi merupakan proses yang sangat baik untuk menjaga keamanan sistem informasi di bidang akademik tetap aman Hal ini menumbuhkan kepercayaan kembali baik dari dosen, mahasiswa, pimpinan dan masyarakat pada umumnya.

Keamanan sistem informasi merupakan hal yang sanat penting pada saat ini, untuk itu penulis memberikan saran bagi peneliti berikutnya yaitu bagiamana membuat penelitian sistem kemanan informasi ini pada *flatform* sistem *softwarenya*, sehingga akan memperkuat pendukung dari sistem keamanan informasi yang berdasarkan prosedur dan kebijakan yang di buat oleh perguruan tinggi.

Daftar Pustaka

[1] Tuti Hartati, “Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013”, KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer, Vol. 01, No. 02, Juni 2017, pp. 63-70.

[2] Muhammad Bakri [1)], Nia Irmayana [2)], Jurnal TEKNOKOMPAK, Vol. 11, No. 2, 2017, 41-44. ISSN 1412-9663 (print

[3] Ritzkal[1)], Arief Goeritno[2)],A.Hendrawan [3)], ”Implementasi ISO/IEC 27001:2013 Untuk Sistem Manajemen Keamanan Informasi (SMKI) pada Fakultas Teknik UIKA-BOGOR”, PROSIDING Seminar Nasional Sains dan Teknologi, Fakultas Teknik Universitas Muhammadiyah Jakarta, 8 November 2016, p-ISSN:2407- 1846, e-ISSN : 2460-8416

[4] Hartono, Jogiyanto. (2005) . *Sistem Teknologi Informasi*. Yogyakarta: Andi Yogyakarta

[5] Gordon B.Davis, *Management Information System*,
[6] Catur Daya Solusi, "Upgrading ISO 27001:2005 ke ISO 27001:2013," 9 Maret 2015. [Online]. Available: http://caturdayasolusi.com/upgrading-iso-270012005-ke-iso- 270012013/.
[7] ISO 27001 Compliance-2023 COMPLETE GUIDE