ANALISIS MANAJEMEN RISIKO IT PADA IKEST MUHAMMADIYAH PALEMBANG MENGGUNAKAN METODE OCTAVE – S

Dedy Syamsuar [1)], **Ahmad Firdaus** [2*)], **Paray Theo Lonando** [3)]

[1)] *Teknik Informatik Universias Bina Darma*
[2), 3)] *Sistem Informasi Institut Ilmu Kesehatan dan Teknologi Muhammadiyah Palembang*
email : dedy_syamsuar@binadarma.ac.id [1)], eche.chow@gmail.com [2))], theo.blue89@gmail.com [3)]

Abstraksi

Perkembangan teknologi yang semakin pesat menjadikan suatu perhatian khususnya penggunaan teknologi dibidang pendidikan dalam upaya pemanfaatan dan pemanfaatan teknologi informasi. Permasalahan ancaman yang terindentifiakasi dari perkembangan teknologi informasi dapat mengganggu kerugian baik dari operasional sampai dengan aset. Penguatan fungsi dan keamanan teknologi informasi dengan menerapkan manajemen resiko dalam penggunaan teknologi informasi sangatlah penting. Aset teknologi informasi merupakan aset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Indentifikasi resiko ancaman dan kelemahan infrastukrur teknologi informasi menjadi prioritas utama dalam proses pengembangan kedepan sehingga diperlukan manajemen risiko.

Dalam melakukan pembangunan manajemen risiko perlu didasari dengan teori – teori pendukung baik sesuai dengan syarat kebutuhan maupun dari standar yang diperlukan sehingga penulis menggunakan motode *octave – s* yang merupakan framework yang tepat didasari oleh jumlah sumber daya manusia dan infrastruktur di institusi tersebut. Dengan menggunakn meotede *octave – s* penulis dapat mengindentifikasi kelemahan dan ancaman dalam pemanfaatan teknologi informasi sehingga institusi dapat melakukan pembenahan dan strategi dalam melakukan pengembangan teknologi.

***Kata Kunci* :**
Octave –s , Manajemen Risiko, Keamanan

Abstract

The rapid development of technology makes it a concern, especially the use of technology in the field of education in the effort to utilize and utilize information technology. Identified threat problems from developments in information technology can disrupt losses both from operations to assets. Strengthening the function and security of information technology by implementing risk management in the use of information technology is very important. Information technology assets are important assets for an organization that need to be protected from security risks both from outsiders and within the organization. Identification of risks, threats and weaknesses in information technology infrastructure is a top priority in the future development process so that risk management is required.

In carrying out the development of risk management, it is necessary to be based on supporting theories both in accordance with the requirements and the required standards so that the authors use the octave – s method, which is an appropriate framework based on the number of human resources and infrastructure in the institution. By using the octave – s method the author can identify weaknesses and threats in the use of information technology so that institutions can make improvements and strategies in developing technology.

***Keywords* :**
Octave - s, Risk Management, Security

Pendahuluan

Perkembangan teknologi informasi sangat pesat mempengaruhi sistem dalam melakukan aktivitas keseharian, baik fungsi dan tugas selalu berkembang mengikuti kemajuan ilmu pengetahuan. Perkembangan teknologi informasi dimulai pada pertengahan tahun 1960-an ketika komputasi menyebar ke negara-negara industri jasa dengan ditandai sebagai munculnya fenomena masyarakat informasi. Era perkembangan komputerisasi terus belanjut pada tahun 1990-an sehingga melahirkan teknologi internet [1].Berkembangnya teknologi informasi sampai saat ini yang semakin pesat membuat setiap perusahaan maupun organisasi bergerak mengikutinya sebagai atribut yang sangat penting dalam mendukung proses bisnis sehingga penggunaan komputer dan internet sangat mendominasi pekerjaaan manusia hampir disegala bidang baik industri maupun bidang pendidikan.

Bagi dunia pendidikan kebutuhan akan teknologi informasi merupakan sebuah aset dan kebutuhan dalam melakukan operasinya. Hal ini dilakukan untuk memudahkan pekerjaan seperti pelayanan pembelajaran, pelayanan administrasi maupun

penyebaran informasi publik. Sebagian besar aktivitas dilakukan memanfaatkan teknologi informasi Akibatnya, semakin banyak pengguna infrastuktur teknologi informasi sehingga dampak resiko semakin meningkat. Resiko terjadi baik berhubungan dengan infrastruktur, hardware, software, internet maupun brainware.

Selanjutnya, Perguruan Tinggi seperti Universitas, Institut dan lainnya yang menerapkan komputerisasi disemua aktivitas baik belajar secara online maupun pengurusan administrasi mata kuliah dan nilai sehingga perlu pengawasan dalam mengetahui status keamanan diantaranya adalah hilangnya data, redundancy, data rusak, infeksi data oleh malware dan virus, personil yang menyalah gunakan hak akses yang dimiliki. Hal tersebut menghambat proses bisnis dan merugikan baik itu dari segi waktu maupun biaya bagi pihak perguruan tinggi dan mahasiswa [2].

Peruruan tinggi juga diwajibkan oleh pihak regulator (pemerintah) untuk dapat memanfaatkan IT. Sebagai contoh, pelaporan data akademik yang meliputi peserta didik, dosen dan hasil proses akademik dilaporkan berkala melalui sistem yang terstruktur sehingga mengharuskan penggunaan teknologi informasi dalam menunjang proses kerja baik internal maupun untuk eksternal. Penguatan keamanan jaringan dan sistem dalam pembangunan manajemen resiko harus diterapkan bagi Perguruan Tinggi. Sebagai penunjang aktivitas pengolahan data pada bidang teknologi informasi seperti Institut Ilmu Kesehatan dan Teknologi Muhammadiyah Palembang (IKesT MP). Oleh karenanya, peningkatan resiko ini menuntut strategi manajemen yang memadai untuk mencegah resiko buruk terhadap operasional Perguruan Tinggi tersebut.

(IKesT MP) adalah perubahan bentuk Sekolah Tinggi Ilmu Kesehatan Muhamamdiyah Palembang yang bergerak dibidang pelayanan pendidikan kesehatan yang kemudian pada tanggal 05 Agustus 2020 STIKes Muhammadiyah Palembang berubah bentuk menjadi Institut Ilmu Kesehatan dan Teknologi Muhammadiyah Palembang dengan menambah pelayanan pendidikan dibidang teknologi yang juga merupakan brand baru institusi. Perubahan bentuk berdampak pada penambahan struktur organisasi, adminsirtasi dan SDM sehingga penggunaan teknologi informasi semakin bertambah. Seiring proses perubahan bentuk dan proses perkembangan infrastruktur di IKesT MP belum adanya manajemen risiko dalam penilaian analisis risiko yang jelas berkaitan dengan ancaman, kelemahan dan keamanan TI. Untuk mengetahui sampai sejauh mana kesiapan untuk menghadapi ancaman-ancaman yang ada. Tindakan untuk meminimalisir kemungkinan terjadinya risiko aset TI pada IKesT MP, yaitu dengan analisis manajamen risiko TI dan penyusunan dokumen operasioanl kebijakan dalam infrastruktur TI. Banyak framework yang telah disediakan untuk menghadapi risiko-risiko ancaman yang kemungkinan terjadi. Salah satunya yaitu *Octave – s.*

Risk assessment memegang peranan penting dalam penerapan sistem manajemen keamanan informasi. Ada banyak metode yang dapat digunakan untuk melaksanakan risk assessment, karena banyaknya konsultan keamanan informasi yang mengembangkan berbagai pendekatan untuk melakukannya. Banyak framework manajemen risiko dapat digunakan dalam membangun *risk manaagmen*t baik dari fungsi maupun struktur dokumen yang sesuai dengan kebutuhan dan misi dari penelitian. Satu yang terkenal diantaranya adalah metode *octave* yang dikembangkan oleh Carnegie Mellon Software Engineering Institute, Pittsburg.

Valuation (*octave*) merupakan metode yang dapat digunakan untuk mengidentifikasi ancaman yang dapat menimbulkan risiko TI. Dalam praktiknya *octave - s* juga dapat membantu dalam melakukan evaluasi risiko, identifikasi aset TI yang penting sesuai organisasi, juga melakukan identifikasi kerentanan dan ancaman terhadap aset TI tersebut serta melakukan evaluasi potensi jika ancaman tersebut terjadi [3].

Indentifikasi resiko ancaman dan kelemahan infrastukrur menjadi prioritas, mengetahui apa saja ancaman yang akan terjadi untuk dapat menerapkan standar operasional dalam menjaga keamanan data. Sehingga pentingnya membangun manajemen risiko sebagai proses pengembangan kedepan sebagai strategi untuk menghindari kesalahan – kesalahan di bidang infrastuktur TI di IKesT Muhammadiyah Palembang

Tinjauan Pustaka

Ada beberapa framework dalam membangun manajemen risiko (Octave, COBIT, ISO 31000:2009) dengan kelebihan dan keurangan yang dirangkum. Dalam pemilihan framework harus disesuaikan dengan rancangan dan tujuan sebuah organisasi sehingga dapat membantu secara efektif sesuai dengan tujuan.

Dalam melakukan pembangunan manajemen risiko TI penulis menggunakan metode octave – s. Dimana octave –s merupakan salah satu teknik dan metode yang digunakan untuk strategi dan perencanaan risiko keamanan teknologi informasi sesuai dengan kelebihan dan kekurangan. dan menurut penelitian sebelumnya keuntungan metode octave adalah self-directed dengan berkerjasama langsung pada Divisi IT yang berkaitan langsung tentang keamanan organisasi, flexible dan evolved menjalankan teknologi yang bersifat bisnis. Penelitian juga dilakukan oleh Bambang Suprandono [4].

Dengan beberapa framework dapat simpulkan bahwa dalam melakukan analisa risiko digunakan berberapa dokumen dan kerangka kerja sesuai dengan standar yang telah ditetapkan sehingga dapat menghasilkan status risiko dan profil risiko. Metode yang digunakan dalam membangun analisi risiko ini

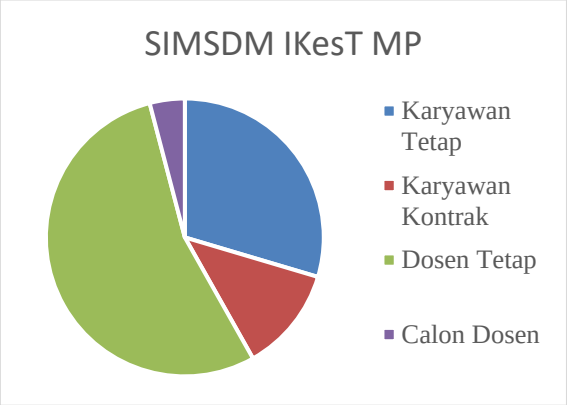
bersifat kualitatif dengan penerapan dan kelebihan yang berbeda. Berikut rangkuman pemetaan kelebihan dan kekurangan dari jenis framework

Tabel 1. Kelebihan dan Kekurangan Framework Manajemen Risiko

No	Jenis Framework	Kelebihan	Kelemahan	Sumber
1	*Octave*	Metode yang terstandar (prosedur, bimbingan, lembar kerja, katalog informasi) dan pelatihan	Belum lengkap seperti octave – s	[5] , [6]
2	*Octave s*	1.Untuk Organisasi 100 orang atau kurang 2. Memiliki 3 Fase Tepat 3. Dilakukan dengan Tim yang terkait	1.Memakan waktu cukup lama, karena pengukuran risiko TI 2. dilakukan secara keseluruhan.	[6] , [7] , [8]
3	*Octave Allergo*	1. Lebih pada proses (simpan dan proses) 2. Buku Pedoman dan Standar Kuieioner tanpa harus ahli dibidangnya	Analisa Pengguaan saja	[6] , [7]
4	COBIT	1. Dikembangkan oleh ISACA .2. Plan and Organise (PO), 3. Acquire and Implement (AI), 4. Deliver and Support (DS) 5. Monitor and Evaluate (ME)	1. bersifat flexible tidak dapat menyesuaikan dengan kemajuan zaman 2. Dijadikan Proses Bisnis 3. Harus Sertifikasi 4. tidak adanya desain faktor terlebih dahulu	[9] , [10]
6	ITIL	1. Service Strategy 2. Service design 3. Service Transition 4. Service Operation 5. Continual Service	1. Pedoman ITIL yang sulit dijangkau untuk non komersial 2. Memerlukan Biaya dan Pelatihan Khusus 3. Harus Bersertifikasi 4. ITIL mendapat kritikan dari beberapa professional ICT mengenai sifatnya yang subjektif dan emotional degradation	[11] , [12]
6	ISO 31000:2009	1. Berkomunikasi dan berkonsultasi 2. Menetapkan konteks Penilaian risiko 3. Evaluasi Analisis Identifikasi 4. Perawatan risiko	Biaya dan Wajib berkelanjutan	[13] , [14]

Dari pemetaan diatas disimpulkan penggunaan metode *octave- s* sangat tepat dalam melakukan analisa risiko di IKesT MP yang bersifat organisasi yang lebih lengkap dalam mengukur aspek

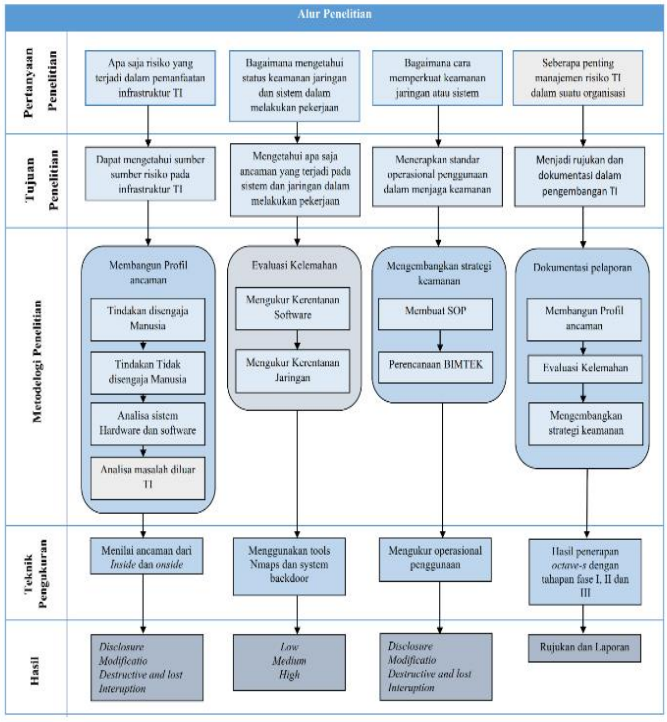
kelemahan dan risiko pada infrastruktur yang dilakukan pada bagian yang terkait dengan organisasi berbasis manufaktur kecil secara khusus dirancang untuk organisasi dari sekitar 100 orang atau kurang hal ini merajuk pada jumlah karyawan dan dosen baik tetap maupun kontrak yang terdaftar pada sistem informasi sumberdaya manusia berjumlah 98 orang.



Gambar. 1 Presentasi Data Pegawai (Sumber SIM SDM)

Metode Penelitian

Adapun alur kerangka kerja penelitian yang digunakan dalam membangun manajemen risiko TI terdapat pada gambar dibawah ini :



Gambar. 2 Alur Metode Penelitian

Ada beberapa tahapan dalam pengumpulan dan persiapan penelitian dengan Pengelolahan data, pembuatan laporan dan melakukan wawancara kebagian unit yang berhubungan langsung dengan teknologi informasi maupun yang bertanggung jawab atas keputusan dan kebijakan penerapan teknologi informasi. Sebagai bahan penelitian membangun kerangka pertanyaan yang berfokus pada teknologi informasi menggunakan framework octave –s, dan nmelakukan pendokumentasian infrastruktur aset di IKesT Muhammadiyah Palembang dengan melakukan pendekatan ke bagian unit PUSDATIN

Penelitian ini menggunakan penelitian kualitatif dan menggunakan teknik analisis deksriptif yang melampirkan hasil berupa uraian dari data hasil dari dua aktivitas yaitu wawancara dan observasi yang telah dilakukan kepada yang betanggung jawab dalam infrastruktur teknologi informasi. Dalam proses pengumpulan data dilakukam proses persiapan seperti menyusun Jadwal, membentuk tim analisis , meminta dokumen dan menyiapkan logistic data yang dibutuhkan dalam evaluasi risiko keamanan menggunakan *octave-s* yang terdiri dari data primer dan skunder . Data primer yang dibutuhkan merupakan data-data yang dibutuhkan merupakan data –data terkait standard operasi, strategi keamanan dan aset-aset yang digunaan di teknologi informasi sedangkan data skunder merupakan data seperti pengunaan layanan , jumlah pengguna dan sebagainya.

HASIL PENELITIAN

Observasi

Dalam melakukan observasi peneliti melakukan pengamatan langsung untuk mendokumentasikan yang dilakukan secara sistematik dengan membuat lembar kerja pada sarana prasarana, pengguna dan standar operasional teknologi informasi.berikut tabel langkah dalam observasi sebelum melakukan langkah kerja *octave – s*

Tabel 2. Langkah Kerja Observasi

Step	**Proses**
Step 1	Memulai lembar kerja Informasi Aset Kritis untuk setiap aset penting. Mencatat nama aset .
Step 2	Mencatat alasan dalam memilih setiap aset penting
Step 3	mencatat deskripsi untuk setiap aset penting yang terkait.
Step 4	Mencatat Aset yang terkait dengan aset penting siapa saja yang menggunakan dan bertanggung jawab
Step 5	Mencatat persyaratan keamanan untuk setiap aset

Wawancara

Wawancara dilakukan kepada yang betanggung jawab dalam infrastruktur teknologi informasi seperti keputusan kebijakan sampai pada pengguna yang bertanggung jawab dalam teknologi informasi di IKesT MP. Dari hasil wawancara yang terdiri beberapa informan dapat ditarik kesimpulan bahwa P01 perannya sebagai pengambil dan penentu

kebijakan keputusan perkembangan di bidang TI selanjutya informan P02 mempunyai peranan dalam merancang, membangun dan menganalisa kebutuhan TI untuk dilaporkan kepada P01 dan informan P03 sebagai pelaksana tugas dengan berkoordinasi bersama informan P02. sehingga didapatlah data informan sebagai berikut:

Tabel. 3. Data Informan

Narasumber	**Jabatan**	**Tanggung Jawab**
P01	Pimpinan	Pegambil Keputusan dan Kebijakan
P02	Kepala Pusdatin	Merancang, Membangun dan Menganalisa Kebutuhan TI
P03	Staf IT	Pelaksana

Hasil dan Pembahasan

Membangun Profil Aset Berbasis Ancaman yaitu mendefiniskan kriteria dampak evaluasi yg akan digunakan untuk mengevaluasi risiko , mengidentifikasi aset penting dan mengevaluasi praktek keamanan yang sedang berlanngsung. Dari hasil yang didapat faktor pelaku baik dari internal maupun eksternal yang kurang menyadari pentingnya pengunaan data akun dan pencurian data informasi merupakan ancaman yang sangat kritis dengan motif yang disengaja untuk yang tidak disengaja kelalaian kesalahan konfigurasi dari penyedia web hosting dapat menyebabkan kerusakan dan pencurian data. Untuk sistem yang bermasalah ialah kurannya dalam pemeliharaan update baik hardware dan software penggunaan yang tidak wajar seperti membuka game , live streaming di media social yang menyebabkan kerja Komputer meningkat ini juga dikarenakan kurangnya kontrol berkala dari staf IT dikarenakan kurangnya SDM IT pada perguruan tinggi. Sedangkan untuk sistem jaringan jarak jaringan yang terlalu jauh dari router menyebabkan internet menjadi lambat dan juga meningkatkan kinerja dari router. Untuk ancaman dari masalah lain fakor listrik dengan tegangan tingga sehingga diperlukan stabilizer dalam mengatur tegangan dan UPS yang dapat membantu hardware dalam mengurangi gangguan saat listrik mati tiba-tiba dan faktor alam seperti gempa bumi , banjir dll dapat merusak hardware dan software

Indentifikasi Kelemahan Infrastruktur (*Indentify* Infrastruktur *Vulnerabilities*) Setelah dilakukan ujicoba melakukan tools maka selanjutnya Memeriksa Infrasturktur yang berhubungan dengan aset sistem yang merupakan aset penting bagi perguruan tinggi dihubungkan langsung dengan database server yang ada di ruang server maupun web hosting, komponen-komponen yang berkaitan dengan database server terdiri dari server, internal network dan external network merupakan saranan yang digunakan untuk mengirimkan informasi dari database sistem. Pegawai atau operator mengakses database melalui komputer masing-masing atau menggunakan laptop pribadi yang terhubung dengan jaringan wireless. Dalam penyimanan data menggunakan storage device dan cloud.

Mengembangkan Strategi Keamanan dan Perencanaannya (*Develop Security Strategy and Plans*) dengan menentukan status stoplight dengan ketentuan tinggi (*red*), sedang (*yellow*) dan rendah (*green*) dan menghitung probabilitas terkait unsur dan kompenen dalam pelaksanaan aktivvitas dengan nilai 1 (Tidak Terjadi nilai probabilitas < 20%) , 2 – 3 (Jarang nilai probabilitas 20% - 80 %) dan 4 – 5 (terjadi nilai probabilitas >80%) .dari hasil perhitungan tersebut maka dihasilkan status dari manajemen risiko di IKesT MP seperti kabel dibawah ini :

Tabel. 5. Status Keamanan

No	Praktik Keamanan	Red	ellow	Green
1	Kesadaran Keamanan dan Pelatihan			√
2	Strategi Keamanan			√
3	Manajemen Keamanan			√
4	Kebijakan Keamanan dan Peraturan		√	
5	Manajemen Keamanan Kolaboratif		√	
6	Perencanaan Contgency	√		
7	Pengendalian Aset Fisik		√	
8	Pemantauan dan Audit Keamanan Fisik		√	
9	Sistem dan Manajemen Jaringan		√	
10	Pemantauan dan Audit Keamanan TI		√	
11	Pengesahan dan Otoritas			√
12	Manajemen Kerentanan		√	
13	Enskripsi			√
14	Desain dan Arsitektur Keamanan			√
15	Manajemen Insiden		√	

Dari hasil tabel diatas dapat disimpulkan sebagai berikut :

1. Keamanan dan Pelatihan

   Untuk pelatihan keamanan sudah dilakukan tetapi dalam perguruan ini pegawai belun menyadari tanggung jawab keamanan akun tetapi mereka untuk tidak membocorkan informasi penting ke perguruan tinggi lainnya serta memiliki kemampuan yang

cukup dalam penggunaan komputer. Status *spotlight green*.

2. Strategi Keamanan
   Perguruan tinggi belum secara rutin memasukan pertimbangan keamanan tetapi perguruan tinggi sudah melakukan strategi keamanan dan telah didokumentasikan. Status *spotlight green*.
3. Manajemen Keamanan
   Perguruan tinggi mengelokasikan dana yang cukup dalam menunjang aktivitas keamanan, mempunyai akun yang berbeda setiap bagian, ada prosedur keamanan yang berwenang dan mengawasi unit bagian dan IT telah memberikan arahan dan penjelasan mengenai peran dan tanggung jawab keamanan. Status *spotlight green*.
4. Kebijakan Keamanan dan Peraturan
   Perguruan tinggi mempunyai kebjakan keamanan tetapi tidak melakukan secara berkala, memeiliki SOP terkait keamanan tetapi tidak ada peraturan undang-undang secara resmi. Status *spotlight yellow*.
5. Manajemen Keamanan Kolaboratif
   Tertuang dalam lembar perjanjian kerjasama pada pihak ketiga dalam menjaga kepercayaan tapi belum melakukan verifikasi keamanan secara valid. Status *spotlight yellow*.
6. Rencana Contigency
   Belum adanya rencana penanggulangan bencana dan hal-hal yang tidak terduga secara resmi. Status *spotlight red*.
7. Pengendalian Aset Fisik
   Perguruan tinggi telah melakukan rencana dan prosedur keamanan fasilitas dan telah diuji, mempunyai SOP pengendalian akses fisik, belum adanya kebijakan dan dokumnetasi bagi pengujung, dalam pengendalian aset fisik bagi pihak external tleah dilakukan komunikasi dan menverifikasi penyedia layanan dalam memenuhi control terhadap aset fisik. Status *spotlight yellow*.
8. Pemantuan dan Audit Keamanan
   Perguruan tinggi telah melakukan pengendalian fisik untuk dapat dipertanggung jawabkan, untuk dokumentasi perbaikan dan modifikasi masih jarang dilakukan, belum adanya audit tentang pemantauan dan keamanan fisik. Untuk pihak external persyaratan untuk memantau keamanan telah dikomunikasikan tetapi belum melakukan verifikasi dalam mememnuhi persyaratan keamanan. Status *spotlight yellow*.
9. Sistem Manajemen Jaringan
   Perguruan tinggi telah melakukan perlingdungan data informasi penting, melakukan backup data secara montly dan saat perubahan data informasi penting, menggunakan password kombinasi, melakukan update firewall untuk sistem keamanan jaringan sesuai notifikasi perangkat. Perguruan tinggi juga melakukan persyaratan keamanan bagi pihak external tetapi belum melakukan verifikasi keamanan. Status *spotlight yellow*.
10. Pemantauan dan Audit Keamanan TI
    Perguruan tinggi telah melakukan update firelwall berkala untuk keamanan tetapi jarang sekali melakukan pemantauan, belum tersedianya alat dan sistem dalam pemantauan sistem dan jaringan. Untuk pihak external belum adanya dokumentasi resmi sebagai persyaratan keamanan dan verifikasi persyaratan keamanan. Status *spotlight yellow*.
11. Pengesahan Otoritas
    Perguruan tinggi telah melakukan control akses dan otoritas , terdapat SOP pengguna setiap akses, melakukan update otoritas sesui kebutuhhan akses. Untuk pihak external telah melakukan kontrol akses terhadap penyedia layanan serta memverifikasi akses dan otoritas. Status *spotlight green*.
12. Manajemen Kerentanan
    Perguruan tinggi jarang melakukan manajemen kerentanan, manajemen kerentenan dilakukan saat terindentifikasi masalah. Untuk pihak external telah melakukan komnukasi tentang kerentanan yang tedokumentasi secara resmi. Status *spotlight yellow*.
13. Enskripsi
    Perguruan tinggi telah menyesuaikan keamanan enskripsi baik pada sistem aplikasi maupun pada perangkat jaringan. Untuk pihak ketiga telah dikomunikasikan dan menjamin keamanan hal ini juga sudah diverifikasi. status *spotlight green*.
14. Desain dan Arsitektur Keamanan
    Perguruan tinggi memeiliki standar keamanan jaringan dan melakukan startegi kebijakan dan update design sistem keamanan sedangkan untuk pihak external tleah menerapkan keamanan dan arsitekur keamanan jaringan sesuai standar perusahaan. Status *spotlight green*.
15. Manajemen Insiden
    Belum adanya dokumen insiden insternal dan strategi insiden yang terdokumentasi. Untuk pihak esternal telah tertuang manajemen insiden pada perjanjian kontrak kerja. Status *spotlight yellow*.

KESIMPULAN DAN SARAN

Kesimpulan

Hasil analisis risiko di IKesT MP adalah Pemanfaatan IT di IKesT MP masih pada posisi medium dimana faktor risiko internal yang paling berbahaya adalah kesadaran pengguna dalam penggunaan akun. Dan juga tidak menutup kemungkinan gangguan dari luar oleh orang yang tidak bertanggung jawab. Perlunya penambahan dokumentasi resmi. penguatan manajemen kebijakan, tanggung jawab dan SOP

Saran

Pada perguruan tinggi IKesT MP harus membuat kebijakan , mekanisme dan prosedur terkait aset TI dengan pengawasan dan pengembangan pada strategi keamanan

Daftar Pustaka

[1] daryanto Setiawan, "Dampak Perkembangan Teknologi Informasi dan Komunikasi Terhadap Budaya Impact of Information Technology Development and Communication on," *J. Pendidik.*, vol. X, no. 2, pp. 195–211, 2017.

[2] L. J. Fahri Husaini, Awalludiyah Ambarwati, "Analisis Risiko Aset TI Menggunakan Metode OCTAVE Pada SWD Resto," *Semin. Nas. Sist. Inf.*, vol. 3, no. 1, pp. 1940–1946, 2019, [Online]. Available: https://jurnalfti.unmer.ac.id/index.php/senasif/article/view/258

[3] A. Mathematics, "済無No Title No Title No Title," vol. 3, pp. 1–23, 2016.

[4] B. Supradono, "Manajemen risiko keamanan informasi dengan menggunakan metode octave (operationally critical threat, asset, and vulnerability evaluation)," *Media Elektr.*, vol. 2, no. 1, pp. 4–8, 2009.

[5] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," *Pittsburgh, PA, Carnegie Mellon Univ.*, no. August, 2003.

[6] S. Supatmi, "4. konsep Pengukuran Saat Resiko Terjadi (at Risk)," 2020.

[7] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2003.

[8] P. E. Rahman, "ANALISIS MANAJEMEN RISIKO KEAMANAN SISTEM INFORMASI STATISTIK RUTIN MENGGUNAKAN METODE OCTAVE-S." Universitas Islam Negeri Sultan Syarif Kasim Riau, 2016.

[9] A. Pasquini and E. Galiè, "COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process," *Proc. FIKUSZ*, vol. 13, pp. 67–76, 2013.

[10] A. M. Syuhada, "Kajian Perbandingan Cobit 5 dengan Cobit 2019 sebagai Framework Audit Tata Kelola Teknologi Informasi," *Syntax Lit. J. Ilm. Indones.*, vol. 6, no. 1, pp. 30–39, 2021.

[11] J. Joyto, "Analisis Perbandingan Framework COBIT 5.0 Dengan ITIL Dalam Mengaudit Sistem Informasi," *J. Ilm. Ilmu Terap. Univ. Jambi| JIITUJ|*, vol. 5, no. 1, pp. 76–85, 2021.

[12] L. Sembilla, U. Fu'aida, M. Y. Randy, and R. N. Supangat, "Keterkaitan 5 Fokus Area Tata Kelola Teknologi Informasi Dengan Framework Cobit 5, Coso, Itil Dan Iso 38500," *J. Sist. Inf. Dan Bisnis Cerdas Vol*, vol. 11, no. 1, 2018.

[13] D. Gjerdrum and M. Peter, "The new international standard on the practice of risk management–A comparison of ISO 31000: 2009 and the COSO ERM framework," *Risk Manag.*, vol. 31, no. 21, pp. 8–12, 2011.

[14] E. Erniyani, N. Wisudawati, and N. E. Pratiwi, "Analisis Penerapan Manajemen Risiko Berdasarkan ISO 31000: 2009 (Studi Kasus: Jasmini Laundry)," *Integr. J. Ilm. Tek. Ind.*, vol. 5, no. 1, pp. 34–41, 2020.