JURNAL ILMIAH ELEKTRONIKA DAN KOMPUTER, Vol.14, No.1,Desember 2021, pp.141-151
p-ISSN : 1907-0012 (print)
e-ISSN : 2714-5417 (online)
http://journal.stekom.ac.id/index.php/elkom

Analisis Manajemen Risiko Infrastruktur Dengan Metode NIST (National Institute of Standards and Technology) SP 800-30 (Studi Kasus : STMIK Rosma)

Anggi Elanda[1], Robby Lintang Buana[2]
[1]STMIK Rosma
Jl. Kertabumi No. 62 Karawang, 0267-405312, e-mail: anggi@rosma.ac.id
[2]STMIK Rosma
Jl. Kertabumi No. 62 Karawang, 0267-405312, e-mail: robby.buana@mhs.rosma.ac.id

ARTICLE INFO

Article history:

Received 3 Juni 2021
Received in revised form 9 july 2021
Accepted 9 july 2021
Available online july 2020

ABSTRACT

Infrastructure is an important thing in an organization/company that is used to support activities carried out within the organization. Infrastructure that includes STMIK Rosma, including hardware, software, data, and information, and human resources that support information systems. Hardware resources include PCs that are used for clients with application program software. Windows 10 professional 32 and 64 bit as the operating system. While the software on the server uses Linux OS and PHP programming language. Data and information include infrastructure data, device data, server data and data on staff, students and lecturers at STMIK Rosma. So the need for the sustainability of this system is increasingly important. Problems that have existed in the STMIK Rosma infrastructure, such as those related to information security vulnerabilities. If this problem cannot be fixed in a sustainable manner, it will have an impact or risk on the sustainability of this infrastructure, especially the academic community. This study uses NIST SP 800-30 as the method used to solve these problems.

Keywords: Information Security, NIST SP 800-30, Infrastructure, Risk Assessment

Abstrak

Infrastruktur merupakan hal penting dalam sebuah organisasi/perusahaan yang digunakan untuk penunjang aktivitas yang dilakukan dalam organisasi tersebut. Infrastruktur yang meliputi STMIK Rosma, diantaranya perangkat keras, perangkat lunak, data, dan informasi, dan sumber daya manusia yang mendukung sistem informasi. Sumber daya perangkat keras meliputi PC yang digunakan untuk client dengan perangkat lunak program aplikasi. Windows 10 profesional 32 dan 64 bit sebagai sistem operasinya. Sedangkan perangkat lunak pada server menggunakan OS Linux dan Bahasa pemrograman PHP. Data dan informasi meliputi data infrastruktur, data device, data server serta data staff, mahasiswa maupun dosen yang berada di STMIK Rosma. Sehingga kebutuhan akan keberlangsungan sistem ini

Received Juni 3 , 2021; Revised july 9, 2021; Accepted july 9 , 2021

p-ISSN: 1907-0012 e-ISSN : 2714-5417

semakin penting. Permasalahan yang pernah ada di infrastruktur STMIK Rosma seperti berkaitan dengan celah kerawanan keamanan informasi. Jika permasalahan ini tidak dapat diperbaiki secara berkelanjutan, alhasil akan memberikan dampak ataupun risiko kepada keberlangsungan infrastruktur ini, khususnya civitas akademika. Penelitian ini menggunakan NIST SP 800-30 sebagai metode yang digunakan untuk menyelesaikan permasalahan tersebut.
Kata Kunci : Keamanan Informasi, NIST SP 800-30, Infrastruktur, Penilaian Resiko

1. PENDAHULUAN

Dalam organisasi perguruan tinggi sangat dituntut tata kelola manajemen yang baik dan dapat meningkatkan kegiatan pelayanan Pendidikan perguruan tinggi bagi masyarakat dan bangsa. Dengan demikian informasi-informasi dapat dikelola dan bermanfaat bagi pengambilan keputusan manajemen perguruan tinggi tersebut, dan disamping itu pengelolaan manajemen juga dapat memberikaan manfaat bagi stakeholder/sivitas akademika. Dalam kegiatan analisa resiko (Risk Assesment) khususnya teknologi informasi harus dapat mengevaluasi resiko yang kemungkinan timbul dalam tata kelola sistem informasi dan keberlangsungan operasional perguruan tinggi.

Permasalahan yang pernah ada di Infrastruktur STMIK Rosma seperti berkaitan dengan celah kerawanan keamanan informasi. Jika permasalahan ini tidak dapat diperbaiki secara berkelanjutan, alhasil akan memberikan dampak ataupun risiko kepada keberlangsungan infrastruktur ini, khusunya civitas akademika. Berbagai upaya telah dilakukan pihak STMIK ROSMA untuk melibatkan civitas akademika berpartisipasi demi kemajuan Infrastruktur. Misalnya membuat grup untuk sosialisasi infrastuktur. Hal ini tentu saja masih kurang efektif demi menyelesaikan permasalahan diatas [1]. Menurut [2], [3] dan [4], COBIT framework sebagai audit sistem informasi dan teknologi informasi masih bersifat umum seperti mengukur kematangan implementasi teknologi informasi. Sedangkan menurut [5], [6],[7], [8], [9] dan [10] manajemen risiko keamanan informasi dapat diterapkan sebagai pelindung teknologi informasi dari bahaya keamanan informasi, seperti virus, hacker ataupun pencurian data, menimbulkan ancaman besar terhadap asset dan reputasi perusahaan ataupun organisasi. Berdasarkan rekomendasi beberapa penelitian diatas untuk menyelesaikan permasalahan infrastruktur STMIK Rosma dibutuhkan manajemen risiko keamanan informasi. Ada banyak metode yang dapat digunakan untuk melakukan manajemen risiko keamanan informasi seperti Octave, NIST SP 800-30 dan ISO 27001. Metode OCTAVE terdapat beberapa langkah pengerjaan yaitu persiapan, Identifikasi Aset (Berdasarkan identifikasi ancaman), identifikasi kerawanan infrastruktur dan membuat strategi dan perencanaan keamanan [8]. NIST SP-800-30 Memiliki 9 langkah untuk melakukan analisa risiko yaitu karakterisasi sistem, identifikasi ancaman, identifikasi kerawanan, analisa kontrol, analisa kecenderungan, analisa dampak, penentuan risiko, rekomendasi kontrol dan dokumentasi [10]. metode iso 27001 terdiri dari 4 langkah utama serta bersifat umum yaitu Plan, Do, Check dan Act [5]. Metode Octave hanya digunakan bagi organisasi (evaluasi organisasi) sedangkan ISO 27001 lebih cenderung mengarahkan kepada manajemen level tingkat atas. NIST SP 800-30 telah terbukti memberikan kontribusi yang lebih seperti: memberikan wawasan keamanan informasi yang sifatnya konsisten dan komprehensif bagi pengambil kebijakan, pemodelan sumber daya yang terstruktur, wawasan keamanan informasi dapat diterima oleh berbagai pengambil resiko, penentuan ancaman dapat diidentifikasi dengan mudah, pengambil keputusan tidak ragu-ragu untuk mengambil resiko karena setiap resiko telah diselidiki dengan baik [10]. NIST SP 800-30 terbaik dari 3 metode untuk analisa resiko yaitu Mehari, Magerit dan Microsoft's Security Management Guide terutama pada saat melakukan analisa resiko, NIST SP 800-30 memberikan rekomendasi kontrol.

Penelitian ini akan menggunakan metode NIST SP 800-30 sebagai metode yang akan menyelesaikan permasalahan yang telah dibahas pada paragraf pertama. Maka, dipilih penilaian risiko infrastruktur jaringan menggunakan metode NIST SP 800-30 (Studi Kasus: STMIK Rosma).

2. TINJAUAN PUSTAKA

2.1. Infrastruktur

Infrastruktur merupakan sebuah kumpulan sistem komputer yang saling berhubungan, dihubungkan oleh berbagai macam bagian dari sebuah arsitektur telekomunikasi. Secara khusus, infrastruktur ini mengacu pada organisasi dan berbagai bagian konfigurasi mereka dari jaringan komputer individu sampai pada router, kabel, wireless access point, switch, backbone, network protocol, dan network access methodologies. Infrastruktur dapat berupa (open) atau tertutup (close). Contoh infrastruktur terbuka adalah internet, sedangkan contoh dari infrastruktur tertutup adalah private internet. Mereka dapat beroperasi melalui koneksi jaringan wireless, atau kombinasi antara keduanya. Bentuk paling sederhana dari

p-ISSN: 1907-0012 e-ISSN : 2714-5417

infrastruktur jaringan biasanya terdiri dari satu atau lebih komputer, sebuah jaringan atau koneksi internet, sebuah hub yang menghubungkan computer yang satu dengan yang lainnya sampai dengan sistem jaringan yang terhubung dengan sistem jaringan lainnya.

2.1.1. NIST SP 800-30

NIST (National Institute of Standard and Technology) Special Publication (SP) 800-30 adalah panduan manajemen risiko untuk sistem teknologi informasi yang terstandarisasi oleh Pemerintah Pusat Amerika Serikat. Metodologi ini dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisis keamanan yang cukup sesuai dengan keinginan pemilik sistem dan ahli teknis untuk benarbenar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem TI. Proses ini sangat komprehensif, meliputi segala sesuatu dari ancaman sampai dengan sumber identifikasi untuk evaluasi berkelanjutan dan penilaian. (Elky, Steve 2007). Sumber identifikasi ancaman dapat berasal dari salah satu atau beberapa disaster diantaranya natural disaster, environment/technology disaster, dan human disaster. Disaster yang sering terjadi pada sistem berbasis web adalah human disaster. Human disaster dapat berupa kesalahan input data dan peretasan. Kesalahan input data biasanya dilakukan oleh pegawai baru yang belum menguasai operasional sistem. Sedangkan peretasan biasanya dilakukan oleh hacker/cracker dengan memanfaatkan celah – celah keamanan website yang masih terbuka. Masalah yang timbul pada sistem dapat dikategorikan sebagai risiko. Risiko yang terjadi pada sistem akan menghambat proses bisnis. Dengan demikian, manajemen risiko dibutuhkan agar risiko-risiko yang mungkin timbul bisa tertata dan terkelola dengan baik. Berdasarkan uraian diatas, maka peneliti berencana membuat "Penilaian infrastruktur dengan metode NIST (National Institute of standards and Technology) SP 800-300 (Studi Kasus: STMIK Rosma)". Penelitian ini diharapkan mempermudah kepada auditor untuk keamanan internet dalam melakukan audit pada IDS (Intrusion Detection System) sehingga akan banyak pengembangan kedepannya. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko. Tahapan penilaian risiko berdasarkan NIST 800-30 yaitu (Syalim, Hori, dan Sakurai, 2009):

1. System Characterization
   Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.
2. Threat Identification
   Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada.
3. Vulnerability Identification
   Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya.
4. Control Analysis
   Analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinan kemungkinan pengembangan dari ancaman.
5. Likelihood Determination
   Proses rangking terhadap potensi dari kerawanan dapat dilaksanakan dalam lingkungan dari kerawanan tersebut. Faktor yang menjadi pertimbangan adalah ancaman (sumber dan kemampuan), sifat dari kerawanan serta keberadaan dan efektifitas kontrol jika diterapkan.
6. Impact Analysis
   Tahapan ini digunakan untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan.
7. Risk Determination
   Penilaian tingkat risiko pada sistem IT dilakukan pada langkah ini.
8. Control Recommendations
   Tahapan ini menilai kontrol yang mana dapat mengurangi atau menghilangkan risiko yang

p-ISSN: 1907-0012 e-ISSN : 2714-5417

telah teridentifikasi. kontrol yang direkomendasikan sebaiknya harus dapat mengurangi tingkat risiko pada sistem IT dan data, kepada tingkat risiko yang dapat diterima.

9. Results Documentation

Pada tahap ini, dilakukan pengembangan laporan hasil penilaian risiko (sumber ancaman, kerawanan, risiko yang dinilai dan kontrol yang direkomendasikan).

3. METODOLOGI PENELITIAN

3.1. System Characterization

Karakteristik infrastruktur yang meliputi STMIK Rosma, diantaranya perangkat keras, perangkat lunak, data, dan informasi, dan sumber daya manusia yang mendukung sistem informasi. Sumber daya perangkat keras meliputi PC yang digunakan untuk client dengan perangkat lunak program aplikasi. Windows 10 profesional 32 dan 64 bit sebagai sistem operasinya. Sedangkan perangkat lunak pada server menggunakan OS Linux dan Bahasa pemrograman PHP. Data dan informasi meliputi data infrastruktur, data device, data server serta data staff, mahasiswa maupun dosen yang berada di STMIK Rosma.

4. HASIL DAN PEMBAHASAN

4.1. Threat Identification

Identifikasi terhadap ancaman pada Infrastruktur STMIK Rosma dapat dilihat pada Tabel 1.

Tabel 1. Identifikasi ancaman pada STMIK Rosma

Asal ancaman	Motivasi	Kemungkinan konsekuensi
Hacker, cracker	1. Tantangan 2. Ego 3. Pemberontakan 4. Status 5. Uang	1. *Hacking* 2. *Social engineering* 3. Gangguan sistem, penyusupan 4. Akses yang tidak sah ke sistem
Kriminal komputer	1. Perusakan informasi Penyingkapan informasi 2. ilegal 3. Keuntungan moneter Perubahan data yang tidak sah	1. Kejahatan komputer (seperti *cyber stalking*) 2. Tindakan penipuan (mis. *replay*, peniruan, intersepsi) 3. Informasi suap 4. *Spoofing* 5. Intrusi Sistem
Teroris	1. Pemerasan 2. Perusakan 3. Eksploitasi 4. Balas dendam 5. Keuntungan politik 6. Liputan media	1. Bom/terorime 2. Informasi perang 3. Serangan sistem (seperti *denial of service* yang disebar) 4. Penetrasi sistem 5. Gangguan sistem
Spionase industri (kecerdasan, perusahaan, pemerintah asing, kepentingan pemerintah lainnya)	1. Keuntungan kompetititf 2. Spionase ekonomi	1. Keuntungan pertahanan 2. Keuntungan politik 3. Eksploitasi ekonomi 4. Pencurian informasi 5. Gangguan pada privasi pribadi 6. *Social engineering* 7. Penetrasi sistem

p-ISSN: 1907-0012 e-ISSN : 2714-5417

Asal ancaman	Motivasi	Kemungkinan konsekuensi
		8. Sistem akses yang tidak sah (akses pada sesuatu yang diklasifikasikan eksklusif, dan/atau informasi terkait teknologi)
Orang dalam (karyawan yang kurang terlatih, tidak puas, berbahaya, lalai, tidak jujur, atau dipecat)	1. Keuntungan moneter 2. Balas dendam 3. Kesalahan dan kelalaian yang tidak disengaja (seperti kesalahan entri data, kesalahan pemrograman)	1. Penyalahgunaan komputer 2. Kecurangan dan pencurian 3. Penyuapan informasi 4. Input dipalsukan, data yang rusak 5. Penangkapan 6. Kode berbahaya 7. (misalnya virus, *logic bomb*, *Trojan horse*) 8. Penjualan informasi pribadi 9. *Bug* sistem 10. Intrusi sistem 11. Sabotase sistem 12. Sistem akses yang tidak sah

4.2 Vulnerability Identification

Tabel berikut memberikan contoh kerentanan dalam berbagai area keamanan, termasuk contoh ancaman yang mungkin mengeksploitasi kerentanan itu. Daftar ini dapat memberikan bantuan selama penilaian ancaman dan kerentanan, untuk menentukan skenario insiden yang relevan. Ditekankan juga bahwa dalam beberapa kasus ancaman lain dapat mengeksploitasi kerentanan ini.

Tabel 2. *Vulnerability Identification*

Jenis	Contoh kerentanan	Contoh ancaman
Perangkat keras	Kurangnya pemeliharaan/kesalahan instalasi media penyimpanan	Pelanggaran pemeliharaan sistem informasi
	Kurangnya skema pergantian berkala	Perusakan peralatan atau media
	Kerentanan terhadap kelembaban, debu, kotoran	Debu, korosi, pendinginan
	Kurangnya kontrol perubahan konfigurasi yang efisien	Kesalahan penggunaan
	Kerentanan terhadap voltase yang bervariasi	Hilangnya pasokan listrik
	Kerentanan terhadap suhu yang bervariasi	Fenomena meteorologis
	Penyimpanan yang tidak dilindungi	Pencurian media atau dokumen
	Kurangnya perawatan di pembuangan	Pencurian media atau dokumen

p-ISSN: 1907-0012 e-ISSN : 2714-5417

Jenis	Contoh kerentanan	Contoh ancaman
	Penyalinan yang tidak terkendali	Pencurian media atau dokumen
Perangkat Lunak	Tidak ada atau tidak cukup pengujian perangkat lunak	Penyalahgunaan hak
	Kekurangan yang telah diketahui pada perangkat lunak	Penyalahgunaan hak
	Tidak '*logout*' ketika meninggalkan komputer	Penyalahgunaan hak
	Pembuangan atau pemakaian ulang media penyimpanan tanpa penghapusan yang tepat	Penyalahgunaan hak
	Kurangnya *audit trail*	Penyalahgunaan hak
	Kesalahan penempatan hak akses	Penyalahgunaan hak
	Perangkat lunak yang didistribusikan secara luas	Korupsi data
	Menerapkan program aplikasi untuk data yang salah dalam hal waktu	Korupsi data
	Antar muka yang rumit	Kesalahan penggunaan
	Kurangnya dokumentasi	Kesalahan penggunaan
	Kesalahan pengaturan parameter	Kesalahan penggunaan
	Kesalahan tanggal	Kesalahan penggunaan
	Kurangnya mekanisme identifikasi dan otentikasi seperti otentikasi pengguna	Pemalsuan hak
	Tabel *password* yang tidak dilindungi	Pemalsuan hak
	Manajemen *password* yang buruk	Pemalsuan hak
	Layanan yang tidak perlu diaktifkan	Pengolahan data ilegal
	Perangkat lunak baru atau belum matang	Kegagalan perangkat lunak
	Spesifikasi pengembangan yang tidak jelas atau tidak lengkap	Kegagalan perangkat lunak
	Kurangnya kontrol perubahan yang efektif	Kegagalan perangkat lunak
	Pengunduhan dan penggunaan perangkat lunak yang tidak terkontrol	Perusakan dengan perangkat lunak
	Kurangnya salinan *back-up*	Perusakan dengan perangkat lunak
	Kurangnya perlindungan fisik pada gedung, pintu, dan jendela	Pencurian media atau dokumen
	Kesalahan pembuatan laporan manajemen	Penggunaan peralatan yang tidak sah
Jaringan	Kurangnya bukti pengiriman dan penerimaan pesan	Penyangkalan atas tindakan
	Jalur komunikasi yang tidak dilindungi	Menguping

p-ISSN: 1907-0012 e-ISSN : 2714-5417

Jenis	Contoh kerentanan	Contoh ancaman
	Lalu lintas sensitif yang tidak dilindungi	Menguping
	Sambungan kabel yang buruk	Kesalahan peralatan komunikasi
	Titik tunggal kegagalan	Kesalahan peralatan komunikasi
	Kurangnya identifikasi dan otentikasi pada pengirim dan penerima	Pemalsuan hak
	Arsitektur jaringan yang tidak aman	*Remote spying*
	Transfer *password* dengan jelas	*Remote spying*
	Manajemen jaringan yang tidak cukup (ketahanan *routing)*	Kejenuhan sistem informasi
	Koneksi jaringan publik yang tidak dilindungi	Penggunaan peralatan yang tidak sah
Personel	Ketidakhadiran personel	Pelanggaran ketersediaan personel
	Prosedur rekrutmen yang tidak cukup	Perusakan peralatan atau media
	Pelatihan keamanan yang tidak cukup	Kesalahan penggunaan
	Kesalahan penggunaan atas perangkat lunak dan perangkat keras	Kesalahan penggunaan
	Kurangnya kesadaran akan keamanan	Kesalahan penggunaan
	Kurangnya mekanisme pemantauan	Pengolahan data ilegal
	Bekerja tanpa pengawasan oleh orang luar atau karyawan pembersih	Pencurian media atau dokumen
	Kurangnya kebijakan untuk penggunaan yang benar atas media telekomunikasi dan pesan	Penggunaan peralatan yang tidak sah
Situs	Penggunaan yang tidak memadai atau ceroboh atas kontrol akses fisik ke bangunan dan ruangan-ruangan	Perusakan peralatan atau media
	Lokasi pada daerah yang rentan banjir	Banjir
	Jaringan listrik yang tidak stabil	Hilangnya pasokan listrik
	Kurangnya perlindungan fisik terhadap gedung, pintu, dan jendela	Pencurian peralatan
Organisasi	Kurangnya prosedur formal untuk pendaftaran dan penghapusan pengguna	Penyalahgunaan hak
	Kurangnya proses formal untuk meninjau hak akses (pengawasan)	Penyalahgunaan hak
	Kurangnya ketentuan yang memadai (mengenai keamanan) dalam kontrak dengan pelanggan dan/atau pihak ketiga	Penyalahgunaan hak
	Kurangnya prosedur pemantauan fasilitas pengolah informasi	Penyalahgunaan hak

p-ISSN: 1907-0012 e-ISSN : 2714-5417

Jenis	Contoh kerentanan	Contoh ancaman
	Kurangnya audit berkala (pengawasan)	Penyalahgunaan hak
	Kurangnya prosedur identifikasi dan penilaian risiko	Penyalahgunaan hak
	Kurangnya laporan kesalahan yang tercatat dalam administrator dan pengelola log	Penyalahgunaan hak
	Respon pemeliharaan layanan yang tidak memadai	Menerobos pertahanan sistem informasi
	Kurang atau tidak cukup *Service Level Agreement*	Menerobos pertahanan sistem informasi
	Kurangnya prosedur kontrol perubahan	Menerobos pertahanan sistem informasi
	Kurangnya prosedur formal untuk pengendalian dokumen SMKI	Korupsi data
	Kurangnya prosedur formal untuk rekaman pengawasan SMKI	Korupsi data
	Kurangnya proses formal untuk otorisasi informasi yang tersedia untuk publik	Data dari sumber yang tidak terpercaya
	Kurangnya alokasi yang tepat atas tanggung jawab keamanan informasi	Tindakan penyangkalan
	Kurangnya rencana berkesinambungan	Kerusakan peralatan
	Kurangnya kebijakan penggunaan surat elektronik	Kesalahan penggunaan
	Kurangnya prosedur untuk memperkenalkan perangkat lunak ke dalam sistem operasional	Kesalahan penggunaan
	Kurangnya catatan di administrator dan pengelola log	Kesalahan penggunaan
	Kurangnya prosedur untuk menangani informasi rahasia	Kesalahan penggunaan
	Kurangnya tanggung jawab keamanan informasi dalam deskripsi pekerjaan	Kesalahan penggunaan
	Kurangnya atau tidak memadainya ketentuan (mengenai keamanan informasi) dalam kontrak dengan karyawan	Pengolahan data ilegal
	Kurangnya proses disipliner yang ditetapkan dalam kasus insiden keamanan informasi	Pencurian peralatan
	Kurangnya kebijakan formal pada penggunaan ponsel	Pencurian peralatan
	Kurangnya penguasaan aset lokal	Pencurian peralatan
	Kurangnya atau tidak cukup kebijakan 'meja bersih dan layar bersih'	Pencurian media atau dokumen

p-ISSN: 1907-0012 e-ISSN : 2714-5417

Jenis	Contoh kerentanan	Contoh ancaman
	Kurangnya otorisasi fasilitas pengolahan informasi	Pencurian media atau dokumen
	Kurangnya mekanisme pemantauan yang ditetapkan untuk pelanggaran keamanan	Pencurian media atau dokumen
	Kurangnya tinjauan manajemen rutin	Penggunaan peralatan yang tidak sah
	Kurangnya prosedur pelaporan kelemahan keamanan	Penggunaan peralatan yang tidak sah
	Kurangnya prosedur ketentuan sesuai dengan hak intelektual	Penggunaan perangkat lunak palsu atau salinan

4.3 Control Analysis

Pada tahapan ini, infrastruktur STMIK Rosma memiliki *control analysis* yang dieksekusi oleh pihak ketiga atau vendor. Sehingga akses ke sistem informasi akademik lebih terbatas.

4.4 Likelihood Determination

Penentuan likelihood pada penelitian ini dapat dilihat pada Tabel 3.

Tabel 3. Tingkat Likelihood

Tingkat Kemungkinan	Definisi Kemungkinan
High	Tingkat/Motivasi Ancaman sangat tinggi dimana pengendalian terhadap kemungkinan kelemahan sistem tidak dapat diatasi/tidak efektif
Medium	Tingkat/Motivasi Ancaman cukup tinggi, pengendalian terhadap beberapa kelemahan sistem masih belum dapat diatasi
Low	Tingkat ancaman sangat rendah, dimana pengendalian kelemahan sistem secara umum dapat diatasi.

4.5 Impact Analysis

Penentuan Impact pada penelitian ini dapat dilihat pada Tabel 4.

Tabel 4. Tingkat Impact

Tingkat Dampak	Definisi Dampak
High	1. Dapat mengakibatkan kerugian yang sangat mahal dari banyak aset berwujud 2. Dapat menganggu misi dan reputasi organisasi 3. Dapat mengakibatkan kematian manusia atau luka berat
Medium	1. Dapat mengakibatkan kerugian dari banyak aset berwujud 2. Dapat menganggu misi dan reputasi organisasi 3. Dapat mengakibatkan luka ringan
Low	Dapat mengakibatkan kerugian dari beberapa asset berwujud

p-ISSN: 1907-0012 e-ISSN : 2714-5417

4.6 Risk Determination

Penetuan Resiko pada penelitian ini dapat dilihat pada Tabel 5.

Tabel 5. Risk Determination

Threat Likelihood	***Impact***		
	Low (10)	***Medium* (50)**	***High* (100)**
High (1.0)	*Low* 10 x 1.0 = 10	*Medium* 50 x 1.0 = 50	*High*100 x 1.0=100
Medium (0.5)	*Low* 10 x 0.5 = 5	*Medium* 50 x 0.5 = 25	*Medium* 100 x 0.5 = 50
Low (0.1)	*Low* 10 x 0.1 = 1	*Low* 50 x 0.1 = 5	*Low* 100 x 0.1 = 10

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil penilaian risiko berbasis keamanan informasi, Infrastruktur STMIK Rosma memiliki 1 tingkat resiko tinggi, 5 tingkat risiko sedang dan 52 tingkat risiko rendah.

5.2. Saran

Diperlukan penelitian lebih lanjut dalam penilaian risiko menggunakan COBIT framework sebagai audit sistem informasi dan teknologi informasi.

DAFTAR PUSTAKA

[1] [1] D. S. och M. P. Halilintar, “Analisis Gangguan Sambaran Petir Terhadap Kerusakan Perangkat IT Pusat Komputer Universitas Lancang Kuning Menggunakan Metode Collection Volume,” 2015.

[2] T. I. och I. Hermadi, “Audit Proses Perencanaan dan Implementasi Sistem Informasi PT Bank XYZ, Tbk dengan Menggunakan Cobit Framework,” *J. Apl. Manaj.*, vol. 12, n, 2014.

[3] A. Setiawan, “EVALUASI PENERAPAN TEKNOLOGI INFORMASI DI PERGURUAN TINGGI SWASTA YOGYAKARTA DENGAN MENGGUNAKAN MODEL COBIT FRAMEWORK,” *Semin. Nas. Apl. Teknol. Inf.*, vol. pp. A15-A2, 2018.

[4] D. F. och Y. G. Sucahyo, “AUDIT SISTEM INFORMASI/TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI DI UNIVERSITAS XYZ,” *J. Sist. Inf. MTI-UI*, vol. 4, nr, 2015.

[5] A. H. N. A. och I. A. M. Utomo, “Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I,” *J. Tek. ITS*, vol. 1, nr, 2014.

[6] T. N. och M. Pehn, “Workshop-based Security Safeguard Selection with AURUM,” *Int. J. Adv. Secur.*, vol. 3, nr, 2017.

[7] B. Karabacak och I. Sogukpinar, “ISRAM: information security risk analysis method,” *Comput. Secur.*, vol. 24, n, 2017.

[8] B. Supradono, “MANAJEMEN RISIKO KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION),” *Media Elektr.*, vol. 2, nr, 2018.

[9] K. J. S. Hoo, “HOW MUCH IS ENOUGH? A RISK MANAGEMENT APPROACH TO COMPUTER SECURITY,” 2018.

[10] S. F. och T. N. A. Ekelhart, “AURUM: A Framework for Information Security Risk Management,” *Hawaii Int. Conf. Syst. Sci. Hawaii*, 2015.