

Analisis Manajemen Risiko TI Pada Keamanan Data E-Learning Dan Aset TI Menggunakan NIST SP 800-30 Revisi 1

Riszullah Ramadhan Putra^{*1}, Eman Setiawan², Awalludiyah Ambarwati³

^{1,2}Universitas Narotama; Jl. Arif Rahman Hakim No.51 Surabaya, Telp: (031) 5946404

³Progam Studi Sistem Informasi, Universitas Narotama Surabaya

e-mail: *riszulahramadhan@gmail.com, eman.setiawan@narotama.ac.id,
ambarwati1578@yahoo.com

Abstrak

Keamanan Informasi merupakan hal yang sangat penting bagi pihak perusahaan maupun perguruan tinggi. Banyak dampak negatif yang ditimbulkan bagi perguruan tinggi jika keamanan informasi tidak dijaga dengan baik. Penelitian ini menganalisis bagaimana administrator universitas dapat mengidentifikasi faktor risiko operasional yang terlibat dengan operasi e-Learning. Empat jenis risiko operasional utama yang terlibat ialah risiko keamanan data, keamanan password, risiko proses, serta risiko serangan dari hacker. eLINA (E-Learning Universitas Narotama) belum pernah melakukan penilaian manajemen risiko pada web pembelajaran berbasis online. Untuk melindungi web tersebut, serta menjaga keberlangsungan proses bisnis, maka penelitian ini akan menggunakan metode NIST SP 800-30 Revisi 1, yang terdiri dari empat proses yaitu persiapan untuk melakukan penilaian, melakukan penilaian, komunikasikan hasil, dan mempertahankan penilaian. Hasil akhir dari penilaian ini berupa rekomendasi pendekatan mitigasi untuk perlindungan sistem pembelajaran online Universitas Narotama.

Kata kunci: Manajemen Risiko, NIST SP 800-30 Revisi 1, Keamanan Informasi, e – learning, Penilaian Risiko.

Abstract

Information security is very important for companies and universities. Many negative impacts have been caused by universities if information security is not properly maintained. This study analyzes how university administrators can identify operational risk factors involved with e-Learning operations. The four main types of operational risks involved are data security risk, password security, process risk, and the risk of attacks from hackers. eLINA (E-Learning Narotama University) has never conducted a risk management assessment on an online-based learning web. To protect the web, as well as maintain the continuity of business processes, this study will use the NIST SP 800-30 Revision 1 method, which consists of four processes, namely preparation for assessment, assessment, communicating results, and maintaining assessment. The final result of this assessment is a recommendation for a mitigation approach for the protection of the online learning system of Narotama University.

Keywords: Risk Management, NIST SP 800-30 Revision 1, Information Security, E – Learning, Risk Assesment.



1. PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif [2]. Dalam penelitian ini menggunakan sistem pembelajaran *E-Learning* Universitas Narotama sebagai studi kasusnya, yang mana seringkali terjadi kendala pada server dan juga sistem keamanannya.

(*e-Learning Universitas Narotama*) merupakan suatu *web* pembelajaran *online* yang diciptakan khusus untuk mahasiswa Universitas Narotama agar mereka dapat memanfaatkan teknologi informasi dan komunikasi pada masa kini. Untuk dapat mengakses sistem pembelajaran ini diperlukan perangkat komputer, laptop atau *smartphone* yang telah terhubung dengan koneksi internet. Penggunaan eLINA memberikan banyak keuntungan, maka dari itu kehadirannya dinilai sangat penting karena memiliki manfaat dalam efisiensi waktu dan biaya. Selain itu, pembelajaran online ini dapat dilakukan dimanapun dan kapanpun tanpa menghabiskan waktu untuk belajar di dalam ruangan. Sekian banyaknya keuntungan yang diperoleh dari eLINA, tapi tak dapat dipungkiri adanya kemungkinan yang mengancam dan berisiko. Penelitian ini berperan penting karena menganalisis berbagai risiko hal tersebut menjadi suatu acuan bagi manajemen dalam melakukan pencegahan, penanganan, serta perbaikan terhadap berbagai kemungkinan risiko tersebut. Maka dari itu, proses analisis ini akan menerapkan sebuah metode NIST SP 800-30 Rev 1 guna sebagai membantu keamanan pada *web* dan menganalisa permasalahan tersebut.

Penelitian terdahulu ini akan dicantumkan oleh Fathoni Mahardika 2017 [3] Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800 – 30 Revisi 1. Hasil kesimpulan bahwa metode NIST SP 800 – 30 Revisi 1 merupakan metode yang berfokus pada sistem keamanan pada suatu sistem dan memiliki hasil berupa rekomendasi sebagai meminimalisir permasalahan sistem yang di kelompokkan dengan penilaian dilakukan berdasarkan kondisi masalah organisasi tersebut. Persamaan dari Penelitian Terdahulu ini penelitian dilakukan menggunakan metode NIST SP 800 – 30 Revisi 1 yang membahas tentang keamanan sistem. Sedangkan perbedaan yang terdapat pada penelitian ini dengan Penelitian Terdahulu yang di atas membahas tentang sistem keamanan *web* pembelajaran *online* yang ada di Universitas Narotama beserta aset TI (Teknologi Informasi).

2. METODE PENELITIAN

2.1 Tahapan Penelitian



Gambar 1. Tahapan Penelitian

2.2 Pengumpulan Data

2.2.1 Wawancara

Memperoleh data – data permasalahan yang ada sistem pembelajaran eLINA dan memperoleh data – data sebuah ancaman dan risiko yang telah terjadi sehingga bisa mempengaruhi proses yang sedang berlangsung, untuk tujuan penelitian ini dengan cara tanya jawab dan sambil bertatap muka secara langsung antara pimpinan departemen eLINA dan personil yang membantu mengelola sistem tersebut.

2.2.2 *Studi Literatur*

Data yang diperoleh seperti buku, jurnal, dan informasi dari internet yang berhubungan dengan manajemen resiko sistem informasi menggunakan metode NIST 800-30 Revisi 1, dan standar penerapan manajemen resiko.

2.3 *Analisis*

NIST (*National Institute of Standard and Technology*) merupakan organisasi pemerintah di Amerika Serikat dengan misi mengembangkan dan mempromosikan penilaian, serta standar dan teknologi untuk meningkatkan fasilitas dan kualitas kehidupan [1]. Kegunaan utamanya adalah meneliti berbagai ilmu untuk mempromosikan dan meningkatkan infrastruktur teknologi. NIST mengeluarkan rekomendasi melalui publikasi khusus 800-30 *Revisi 1* tentang *Guide for Conducting Risk Assessments*

2.3.1 *Conduct The Assessment (Melakukan Penilaian)*

2.3.1.1 *Threat Sources (Identifikasi Sumber Ancaman)*

Mengidentifikasi dan menggambarkan sumber ancaman yang terjadi pada sistem pembelajaran eLINA sebagai karakteristik penargetan untuk ancaman permusuhan dan berbagai efek untuk ancaman non-permusuhan [4].

2.3.2 *Threat event (Identifikasi Peristiwa Ancaman)*

Mengidentifikasi Peristiwa ancaman didapat dari hasil wawancara dan observasi. Setelah melakukan wawancara dan observasi di departemen eLINA, maka akan didapatkan sekumpulan peristiwa risiko yang mungkin terjadi.

2.3.4 *Vulnerabilities (Kerentanan)*

Dalam tahap ini merupakan berbagai kelemahan atau kekurangan dari sistem pembelajaran eLINA yang memungkinkan terjadi ancaman terhadap sistem [5]. Input dari serangan yang pernah terjadi, dari hasil pengecekan/pengetesan sistem, serta dari proses yang dihasilkan *list vulnerability* atau kerentanan yang memungkinkan diserang oleh risiko.

2.3.5 *Likelihood (Kemungkinan)*

Digunakan untuk memperoleh nilai kecenderungan yang mungkin terjadi, tingkat kemungkinan terbagi menjadi 5 *Very High, High, Moderate, Low, Very Low*

2.3.6 *Impact (Dampak)*

Pada tahap analisis dampak akan menjelaskan bagaimana risiko akan berpengaruh pada misi sistem dan data yang diolah pada sistem pembelajaran ELINA akan menghasilkan berupa definisi dampak dari risiko-risiko tersebut.

2.3.7 *Risk Determination (Menentukan Risiko)*

Penentuan risiko ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan pada metode NIST SP 800-30 Revisi 1

3. HASIL DAN PEMBAHASAN

3.1 Identifikasi Aset

Seorang pemilik aset harus diidentifikasi untuk setiap aset, untuk memberikan tanggung jawab dan akuntabilitas untuk aset tersebut. aset tersebut tidak memiliki hak atas aset, tetapi memiliki tanggung jawab untuk pembuatan, pengembangan, pemeliharaan, penggunaan dan keamanan yang sesuai. Pemilik aset seringkali adalah orang yang paling cocok untuk menentukan nilai aset terhadap organisasi. Aset utama meliputi -proses dan informasi inti dari kegiatan dalam lingkup. Aset utama lainnya seperti proses organisasi juga dapat diperhitungkan, yang akan lebih tepat untuk menyusun kebijakan keamanan informasi atau rencana kelangsungan proses pelayanan. Berikut adalah beberapa aset pada aplikasi eLINA (*e - Learning*) Universitas Narotama seperti pada Tabel 1

Tabel 1. Aset eLINA

Aset	Jenis Aset	Penanggung Jawab	Spesifikasi	Lokasi Aset
IBM 3850 M2 / x3950 M2 server	Aset Pendukung	Ka. Teknis	8x Intel (R) CPU E5620 @ 2.40 Ghz (1 socket) RAM 20GiB HD 1 TB	Gedung E103 Universitas Narotama
IBM System x3400 M3 Server	Aset Pendukung	Ka. Teknis	8x Intel (R) CPU E7420 @ 2.13 Ghz (2 socket) RAM 50 GiB HD 300 GiB	Radnet (Intiland Tower) Lt 6
Router Linksys E1200	Aset Pendukung	Ka. Teknis	10/100 Mbps Wireless Speed, 2.4 Ghz WPA, WPA2	Departemen eLINA Universitas Narotama

3.2 Threat Sources (Identifikasi Sumber Ancaman)

Mengidentifikasi dan menggambarkan sumber ancaman yang terjadi pada sistem pembelajaran ELINA sebagai karakteristik penargetan untuk ancaman permusuhan dan berbagai efek untuk ancaman non-permusuhan. Tabel 2 berikut ini:

Tabel 2. Identifikasi Ancaman

No.	Identifikasi	Sumber Ancaman	Rentang Efek	
1.	Aplikasi Sistem Pembelajaran eLINA (<i>e-Learning</i>)	Salah pengoperasian sistem yang meyebabkan <i>sistem</i> terhenti.	High	
		Pencurian (<i>password</i>) terhadap aplikasi <i>e-learning</i> yang dapat mengakses profil/data yang sifatnya pribadi.	High	
		Terjadi kesalahan dalam pengolahan data oleh staff atau dosen.	Very High	
		Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Moderate	
		Pemanfaatan celah keamanan aplikasi <i>e-learning</i> oleh pihak dalam/luar.	Moderate	
		Kehilangan data yang sifatnya sensitif.	Very High	
		Kesalahan operasional yang disebabkan oleh staff IT.	Moderate	
2.	Windows Server (<i>Proxmox</i>)	Windows tidak berjalan semestinya.	High	
3.	IBM 3850 M2 / x3950 M2 server	Database Server	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Very High
		Storage server	Menggunakan <i>Password</i> Lemah atau menggunakan <i>default password</i> .	Moderate
		OS Server	Tidak berjalan semestinya (Bajakan).	Moderate
4.	IBM System x3400 M3 Server	Database Server	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Very High
		Storage server	Menggunakan <i>Password</i> Lemah atau menggunakan <i>default password</i> .	Moderate
		OS Server	Tidak berjalan semestinya (Bajakan).	Moderate
5.	Router Linksys E1200	Gangguan jaringan yang disebabkan oleh penyedia layanan internet.	High	
		Password lemah / menggunakan default password.	High	

3.3 Threat Event (Identifikasi Peristiwa Ancaman)

Pada tahapan ini menjelaskan organisasi menentukan peristiwa ancaman yang harus dipertimbangkan selama penilaian risiko dan tingkat perincian yang diperlukan untuk menggambarkan peristiwa tersebut [6]. Deskripsi peristiwa ancaman dapat diekpresikan dalam istilah yang sangat umum misalnya, Phising, Distribusi penolakan layanan, dalam istilah lebih deskriptif menggunakan taktik, teknik dan prosedur atau dengan istilah yang sangat spesifik. Selain itu [9], organisasi mempertimbangkan serangkaian peristiwa ancaman yang representatif dapat berfungsi sebagai titik awal untuk mengidentifikasi peristiwa ancaman spesifik dalam penilaian risiko dan tingkat konfirmasi apa yang diperlukan agar peristiwa ancaman dianggap relevan untuk tujuan penilaian risiko. Organisasi dapat mempertimbangkan peristiwa ancaman yang telah diamati baik secara internal atau oleh organisasi yang merupakan rekan / mitra atau semua peristiwa ancaman yang mungkin terjadi.

3.4 Vulnerabilities (Kerentanan)

Dalam tahap ini merupakan berbagai kelemahan atau kekurangan dari sistem pembelajaran eLINA yang memungkinkan terjadi ancaman terhadap sistem. Input dari serangan yang pernah terjadi, dari hasil pengecekan/pengetesan sistem, serta dari proses yang dihasilkan *list vulnerability* atau kerentanan yang memungkinkan diserang oleh risiko. Pada Tabel berikut 3 ini:

Tabel 3. Kerentanan

No.	Identifikasi	Kerentanan	Tingkatan
1.	Aplikasi Sistem Pembelajaran eLINA (<i>e-Learning</i>)	Keterlambatan dalam melakukan Update Virus sehingga memungkinkan malware/virus masuk ke dalam sistem.	Moderate
		Staff saat bekerja membawa laptop masing – masing sehingga kemungkinan akan terjadinya pencurian informasi yang sifatnya pribadi ataupun memasukan malware pada sistem.	Moderate
		Kelalaian/keterlambatan staff dalam pengolahan informasi/materi.	Very High
		Pengguna menggunakan <i>password Default</i> sehingga akan mudah terjadinya pencurian <i>password</i> .	High
		Belum adanya <i>upgrade</i> untuk bahasa pemrograman yang digunakan maupun versi <i>database</i> yang digunakan sehingga keamanan kurang.	High
		Tidak ada sistem <i>backup</i> pada keamanan <i>database</i> sehingga bisa terjadinya kehilangan data yang sifatnya sensitif.	Very High
		Jumlah mahasiswa terlalu banyak dan keterbatasan sumber daya manusia menyebabkan kesalahan pengolahan nilai mahasiswa.	Very High
2.	Windows Server (<i>Proxmox</i>)	Antivirus tidak terupdate pada laptop atau OS bajakan.	High
3.	IBM 3850 M2 / x3950 M2 server	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Very High
		Suhu ruangan server yang tidak stabil.	Moderate
		Ruangan server kurang adanya keamanan sehingga bisa terjadinya pencurian pada server oleh pihak luar/dalam.	Moderate
4.	IBM System x3400 M3 Server	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Very High
5.	Router Linksys E1200	Jaringan yang terhubung dalam perangkat tersebut mengalami gangguan.	High

3.5 Likelihood (Kemungkinan)

Digunakan untuk memperoleh nilai kecenderungan yang mungkin terjadi, tingkat kemungkinan terbagi menjadi tiga kategori, yaitu [7]:

- i. Tinggi, sumber ancaman yang memiliki motivasi tinggi dapat merugikan organisasi, hal ini terjadi karena pengendalian untuk mencegah kerentanan dilakukan tidak efektif.
- ii. Sedang, sumber ancaman memiliki motivasi yang mampu merugikan organisasi, namun organisasi masih dapat melakukan kontrol yang mana mampu menghambat keberhasilan dari kerentanan yang ada.
- iii. Rendah, sumber ancaman yang memiliki motivasi kurang atau rendah, kontrol digunakan untuk mencegah atau mengurangi suatu kerentanan yang akan terjadi pada organisasi. Pada Tabel 4 berikut ini:

Tabel 4. Identifikasi Kemungkinan

No.	Risiko	Kemungkinan peristiwa ancaman yang terjadi	menghasilkan dampak buruk	Keseluruhan Kemungkinan
1.	Kehilangan data yang sifatnya sensitif.	<i>Low</i>	<i>Very High</i>	<i>Moderate</i>
2.	pengoperasian sistem yang meyebabkan sistem terhenti.	<i>Low</i>	<i>Very High</i>	<i>Moderate</i>
3.	Pencurian (<i>password</i>) terhadap aplikasi <i>e - Learning</i> yang dapat mengakses profil/data yang sifatnya pribadi.	<i>Low</i>	<i>Very High</i>	<i>Moderate</i>
4.	Terjadi kesalahan dalam penginputan data mahasiswa oleh staff atau dosen.	<i>Moderate</i>	<i>Very High</i>	<i>High</i>
5.	Gangguan tegangan listrik.	<i>Low</i>	<i>High</i>	<i>Moderate</i>
6.	Kesalahan operasional yang disebabkan oleh staff IT.	<i>Moderate</i>	<i>Moderate</i>	<i>Moderate</i>
7.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	<i>Low</i>	<i>Very High</i>	<i>Moderate</i>
8.	Kerusakan pada aset yang sudah menua ataupun rusak.	<i>Low</i>	<i>Moderate</i>	<i>Low</i>
9.	Kesalahan dalam <i>deployment</i> aplikasi <i>E - learning</i> .	<i>Low</i>	<i>High</i>	<i>Moderate</i>
10.	Pemanfaatan celah keamanan aplikasi <i>e-learning</i> oleh pihak dalam/luar.	<i>Low</i>	<i>Very High</i>	<i>Moderate</i>
11.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	<i>Very Low</i>	<i>Very High</i>	<i>Low</i>
12.	Bencana alam (banjir, kebakaran, gempa bumi dll) sehingga bisa terjadinya kerusakan seluruh pada aset.	<i>Very Low</i>	<i>Very High</i>	<i>Low</i>
13.	Ruangan server yang temperatur suhunya tidak terlalu dingin.	<i>Low</i>	<i>High</i>	<i>Moderate</i>
14.	Gangguan Jaringan	<i>Low</i>	<i>Very High</i>	<i>Moderate</i>

3.6 *Impact* (Dampak)

Pada tahap analisis dampak akan menjelaskan bagaimana risiko akan berpengaruh pada misi sistem dan data yang diolah pada sistem pembelajaran eLINA akan menghasilkan berupa definisi dampak dari risiko-risiko tersebut [8]. Tabel 5 berikut ini:

Tabel 5. Identifikasi Dampak

No.	Jenis Dampak	Keterangan	Dampak Maksimal
1.	Kehilangan data yang sifatnya sensitif.	Dampaknya <i>very high</i> karena data yang didalamnya berupa data yang sensitif yang mempengaruhi akreditasi.	<i>Very High</i>
2.	pengoperasian sistem yang meyebabkan <i>sistem</i> terhenti.	Halaman <i>web</i> tidak dapat diakses dan juga proses layanan tidak jalan.	<i>High</i>
3.	Pencurian (<i>password</i>) terhadap aplikasi <i>e - Learning</i> yang dapat mengakses profil/data yang sifatnya pribadi.	Dampaknya <i>high</i> karena capain pembelajaran ada dilaksanakan melalui eLINA maka, akan terjadinya permasalahan pencurian kunci jawaban/data yang sifatnya pribadi.	<i>High</i>
4.	Jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam penginputan data oleh staff atau dosen.	Dampak <i>very high</i> karena bisa mempengaruhi penilaian mahasiswa.	<i>Very High</i>
5.	Gangguan tegangan listrik	Dampaknya <i>moderate</i> karena bisa menyebabkan sistem bermasalah dan kemungkinan memory server error ketika dinyalakan kembali.	<i>Moderate</i>
6.	Kesalahan operasional yang disebabkan oleh staff IT.	Kesalahan setting pada aktivitas <i>e - learning</i>	<i>Moderate</i>
7.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Jika server terkena virus dampaknya <i>high</i> karena bisa meyebabkan <i>sistem</i> terhenti	<i>High</i>
8.	Kerusakan pada aset yang sudah menua ataupun rusak	Dampaknya <i>high</i> karena bisa terjadinya permasalahan pada server.	<i>High</i>
9.	Kesalahan dalam <i>deployment</i> aplikasi <i>E - learning</i> .	Beberapa fitur kemungkinan tidak berfungsi.	<i>Moderate</i>
10.	Pemanfaatan celah keamanan aplikasi <i>e-learning</i> oleh pihak dalam/luar.	Dampaknya <i>high</i> karena membutuhkan tim rekaman yang memperbaiki program.	<i>High</i>
11.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	Bedampak <i>very high</i> pada sistem sehingga sistem eLINA tidak bisa berjalan.	<i>Very High</i>
12.	Bencana alam (banjir, kebakaran, gempa bumi dll) sehingga bisa terjadinya kerusakan pada aset.	Dampaknya <i>very high</i> karena bisa menyebabkan <i>sistem</i> mati total dan seluruh data yang sifatnya sensitif akan hilang.	<i>Very High</i>
13.	Ruangan server yang temperatur suhunya tidak stabil.	Dampaknya <i>moderate</i> karena bisa terjadinya permasalahan pada server.	<i>Moderate</i>
14.	Gangguan jaringan	Dampaknya <i>moderate</i> Jaringan internet akan mengalami kegagalan koneksi yang berdampak pada sistem eLINA.	<i>High</i>

3.7 Risk Determination (Menentukan Risiko)

Penentuan risiko ini bertujuan untuk menilai tingkat risiko terhadap sistem, untuk menilai tingkat risiko ini mengacu kepada kemungkinan risiko dan dampak risiko yang sudah ditentukan pada metode NIST SP 800-30 .[10]. Masing-masing memiliki skor sebagai berikut:

- i. Dampak yang akan dihasilkan dari peristiwa tersebut
- ii. Kemungkinan terjadinya peristiwa.

Tabel 6. Penentuan Risiko

No.	Ancaman	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
1.	Kehilangan data yang sifatnya sensitif.	Moderate	Very High	High
2.	Terjadi kesalahan dalam pengolahan data mahasiswa oleh staff atau dosen	High	Very High	Very High
3.	Kesalahan dalam <i>deployment</i> aplikasi <i>e-learning</i> .	Moderate	Moderate	Moderate
4.	Kesalahan operasional yang disebabkan oleh staff IT.	Moderate	Moderate	Moderate
5.	Gangguan tegangan listrik.	Moderate	Moderate	Moderate
6.	Kerusakan pada aset yang sudah menua ataupun rusak.	Low	High	Low
7.	Ruangan server yang terpapar suhunya tidak sesuai standart.	Moderate	Moderate	Moderate
8.	Salah pengoperasian sistem yang menyebabkan sistem terhenti.	Moderate	High	Moderate
9.	Pencurian (<i>password</i>) terhadap aplikasi <i>e-learning</i> yang dapat mengakses profil/data yang sifatnya pribadi.	Moderate	High	Moderate
10.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Moderate	High	Moderate
11.	Pemanfaatan celah keamanan aplikasi <i>e-learning</i> oleh pihak dalam/luar.	Moderate	High	Moderate
12.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	Moderate	Very High	High
13.	Bencana alam (banjir, kebakaran, gempa bumi dll) sehingga bisa terjadinya kerusakan pada server.	Low	Very High	Moderate
14.	Gangguan Jaringan	Moderate	High	Moderate

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan melalui wawancara dan observasi pada sistem pembelajaran eLINA (*e-learning*) Universitas Narotama mengenai risiko – risiko yang ada pada sistem tersebut peneliti menggunakan metode NIST SP 800-30 Revisi 1 guna untuk identifikasi risiko yang dilakukan untuk mengetahui permasalahan atau ancaman sehingga dapat dilakukan tindakan pengamanan yang bersifat pencegahan, deteksi maupun koreksi.

5. SARAN

Berdasarkan kesimpulan dari penelitian tersebut, maka penulis merekomendasikan berupa saran – saran sebagai berikut.

Aplikasi sistem pembelajaran eLINA (*e-learning*) merupakan aplikasi yang sangat penting bagi mahasiswa maupun dosen tetapi departemen eLINA belum menerapkan keamanan penuh pada sistem tersebut sehingga banyak ancaman atau permasalahan yang berulang – ulang yang selalu terjadi, maka diharapkan untuk kedepannya departemen eLINA dapat melakukan penilaian risiko, peringanan risiko dan evaluasi risiko agar terhindar dari risiko – risiko yang mempengaruhi operasional, Dan juga program eLINA dibuat menggunakan PHP (bahasa pemrograman) versi 3.7 sedangkan siklus update PHP sudah 7.0 maka diperlukan update PHP (bahasa pemrograman) agar untuk kedepannya keamanan bisa lebih meningkat.

Perawatan terhadap aset – aset TI dan sistem keamanan perlu ditingkatkan lagi yang diharapkan untuk kedepannya, departemen eLINA mengecek secara rutin terhadap aset – aset

TI karena hal tersebut masih rentan akan terjadinya ancaman yang dapat menghasilkan dampak buruk atau risiko – risiko yang dapat mempengaruhi sistem, aset – aset TI sangat memiliki peran penting dalam proses aplikasi sistem pembelajaran eLINA (*e-learning*) Univeritas Narotama.

DAFTAR PUSTAKA

- [1] A. Elanda dan D. Tjahjadi 2018, *Analisis Manajemen Risiko Sistem Keamanan Ids(Intrusion Detection System) Dengan Framework Nist (National Institute of Standards And Technology) Sp 800-30*. (Studi Kasus: DISINFOLAHTAAU Mabes TNI AU), Vol. 12, No. 1, hal. 1–13, Diakses dari ejournal.stmik-sumedang.ac.id
- [2] H. B. Seta dan T. Rahayu. 2017, *Manajemen Risiko Aplikasi Pembelajaran Berbasis Online*, hal. 7–12, Diakses dari <https://ojs.amikom.ac.id>
- [3] S. Kasus dan S. Sumedang. 2017, *Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1*, Vol. 02, No. 02, hal. 1–8, Diakses dari <https://ejournal.poltektegal.ac.id>
- [4] S. Patomviriyavong, B. Samphanwattanachai, dan T. Suwannoi. 2006, *eLearning Operational Risk Assessment and Management: A Case Study of The M . Sc . in Management Program*, hal. 1–5. Diakses dari www.ijcim.th.org
- [5] M. P. Dr. Mamduh M. Hanafi, *Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management*, hal. 1–40, 2018, repository.ut.ac.id.
- [6] J. W. Meritt. 1999, *A Method for Quantative Risk Analysis, Proc. 22nd Natl. Inf. Syst. Secur. Conf.* Diakses dari <https://csrc.nist.gov>
- [7] M. Mahfouz dan A. Adjei-quaye. 2017, *Information Security in an Organization*, Diakses dari <https://www.researchgate.net>
- [8] E. Llc, 2014, *e-learning Concepts, Trends, Applications*. <https://www.talentlms.com>
- [9] J. Task dan F. Transformation. 2012, *Guide for Conducting Risk Assessments*, Diakses dari <https://www.govinfo.gov>
- [10] D. A. Jakaria dan J. T. Informatika, 2013, *Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro*, hal. 37–42, Diakses dari <https://journal.uii.ac.id>