BAB IV

HASIL DAN PEMBAHASAN

Pada bab ini, akan menjelaskan tentang proses penilaian risiko yang dilakukan terhadap sistem pembelajaran eLINA Universitas Narotama. Berdasarkan NIST SP 800 -30 Revisi 1 2012 terdapat 4 tahap yang di gunakan dalam proses penilaian adalah :

1. *Prepare for the assessment* (Persiapan Penilaian)
    i. *Identify Purpose* (Tujuan Identifikasi)
    ii. *Identify Scope* (Identifikasi Ruang Lingkup)
    iii. *Identify Assumptions and Contraints* (Identifikasi Asumsi)
    iv. *Identify Information Sources* (Identifikasi Sumber Informasi)
    v. *Identify Risk Model and Analytic Approach* (Identifikasi Model Risiko dan Pendekatan analitik)
2. *Conduct the assessment* (Melakukan Penilaian)
    i. *threat sources* (Identifikasi sumber ancaman)
    ii. *threat event* (Identifikasi peristiwa ancaman)
    iii. *vulnerabilities* (Kerentanan)
    iv. *likelihood* (Kemungkinan)
    v. *Impact* (Dampak)
    vi. *Risk Determination* (Menentukan RIsiko)

3. *Communicate and share risk assessment result* (Komunikasi dan Hasil Penilaian Risiko)
4. *Maintain the assessment* (Menjaga Penilaian)

4.1 Persiapan untuk Penilaian

Dalam proses penilaian risiko tahapan pertama yang akan dilakukan adalah mempersiapkan untuk penilaian yaitu :

4.1.1 Tujuan Identifikasi

Tujuan dari tahapan ini yaitu untuk menganalisis dan mengindentifikasi pengelompokan manajamen risiko yang berguna untuk perbaikan dan meminimalisir permasalahan.

4.1.2 Ruang Lingkup

Tahapan ini berfokus pada aset teknologi informasi dan pengelolahan sistem pembelajaran eLINA Universitas Narotama.

4.1.3 Asumsi Kendala

Asumsi kendala yang terjadi saat melakukan penilaian terhadap risiko pada sistem pembelajaran eLINA Universitas Narotama adalah kurangnya keamanan pada web sehingga bisa memicu permasalahan sehingga sistem tidak bisa berkerja secara optimal.

4.1.4 Sumber Informasi

Sumber informasi yang diperoleh untuk penilaian dapat dari wawancara dengan pimpinan departemen eLINA dan juga staf yang bekerja membantu proses

operasional eLINA tentang sistem dan aset TI serta masalah yang mungkin akan terjadi maupun yang terjadi.

4.1.5 Model Penilaian

Penilaian ini dilakukan dengan menggunakan pendekatan pemodelan kuantitatif melalui pengembangan model risiko seperti *Scoring* dan *Rating.* Dalam penelitian ini, tingkatan dari permasalahan yang di kategorikan *Very High*, *High*, *Moderate*, *Low*, *Very Low* merupakan dari tingkat kerentanan, tingkat dampak dan tingkat penentuan risiko yang diperoleh dari hasil wawancara dan pengamatan secara langsung terhadap Sistem Pembelajaran eLINA, dan studi kasus yang telah ditentukan dengan mempertimbangkan aspek-aspek *confidentality*, *integrity* dan *availability* dari oprasional pelayanan dan konsekuensinya terhadap reputasi organisasi[12].

Berikut adalah tingkatan permasalahan yang direkomendasikan oleh Departemen eLINA Universitas Narotama untuk penelitian ini di jelasakan pada Tabel 4.5 :

Tabel 4.5 Penilaian Ancaman[12]

No	Sumber Ancaman	Deskripsi
1.	*Very High*	Efek dari kesalahan, kecelakaan, atau tindakan alam menyapu, melibatkan hampir semua sumber daya yang mempengaruhi : struktur organisasi / tata kelola; proses misi / bisnis atau segmen EA, infrastruktur umum, atau layanan dukungan; sistem informasi.
2.	*High*	Efek dari kesalahan, kecelakaan, atau tindakan alam sangat luas, melibatkan sebagian besar sumber daya yang mempengaruhi : struktur organisasi / tata kelola (termasuk banyak sumber daya penting); proses misi / bisnis atau segmen EA, infrastruktur umum, atau layanan dukungan; sistem informasi.
3.	*Moderate*	Efek dari kesalahan, kecelakaan, atau tindakan alam luas, melibatkan sebagian besar sumber daya yang mempengaruhi : struktur organisasi / tata kelola, tetapi tidak melibatkan sumber daya kritis; proses misi / bisnis atau segmen EA, infrastruktur umum, atau layanan dukungan; sistem informasi.
4.	*Low*	Efek dari kesalahan, kecelakaan, atau tindakan alam terbatas, melibatkan beberapa sumber daya yang mempengaruhi : struktur organisasi / tata kelola, termasuk beberapa sumber daya penting; proses misi / bisnis atau segmen EA, infrastruktur umum, atau layanan dukungan; sistem informasi.
5.	*Very Low*	Efek dari kesalahan, kecelakaan, atau tindakan alam minimal, melibatkan sedikit jika ada sumber daya yang mempengaruhi : struktur organisasi / tata kelola, dan tidak melibatkan sumber daya kritis; proses misi / bisnis atau segmen EA, infrastruktur umum, atau layanan dukungan; sistem informasi.

Tabel 4.6 Penilaian Kerentanan[12]

No	Tingkat Kerentanan	Deskripsi
1.	*Very High*	Kerentanan diekspos dan dieksploitasi, dan eksploitasinya dapat mengakibatkan dampak yang parah. Kontrol keamanan yang relevan atau remediasi lainnya tidak diterapkan dan tidak direncanakan; atau tidak ada tindakan pengamanan yang dapat diidentifikasi untuk memulihkan kerentanan.
2.	*High*	Kerentanan sangat memprihatinkan, berdasarkan pada paparan kerentanan dan kemudahan eksploitasi dan / atau beratnya dampak yang dapat dihasilkan dari eksploitasi tersebut. Kontrol keamanan yang relevan atau perbaikan lainnya direncanakan tetapi tidak diimplementasikan; kontrol kompensasi sudah ada dan setidaknya secara efektif minimal
4.	*Moderate*	Kerentanan keprihatinan moderat, berdasarkan pada paparan kerentanan dan kemudahan eksploitasi dan / atau keparahan dampak yang dapat dihasilkan dari eksploitasi tersebut. Kontrol keamanan yang relevan atau perbaikan lainnya dilaksanakan sebagian dan agak efektif.
5.	*Low*	Kerentanan itu menjadi perhatian kecil, tetapi efektivitas perbaikan dapat ditingkatkan. Kontrol keamanan yang relevan atau perbaikan lainnya dilaksanakan sepenuhnya dan agak efektif.
6.	*Very Low*	Kerentanan tidak menjadi perhatian. Kontrol keamanan yang relevan atau perbaikan lainnya dilaksanakan, dinilai, dan efektif sepenuhnya.

Tabel 4.7 Penilaian Dampak[12]

No	Tingkat Dampak	Deskripsi
1.	*Very High*	Peristiwa ancaman dapat diharapkan memiliki beberapa efek buruk yang parah atau bencana pada operasi organisasi, aset organisasi, individu, organisasi lain.
2.	*High*	Peristiwa ancaman dapat diharapkan memiliki efek buruk yang parah atau bencana pada operasi organisasi, aset organisasi, individu, organisasi lain.
4.	*Moderate*	Peristiwa ancaman dapat diharapkan memiliki efek buruk yang serius pada operasi organisasi, aset organisasi, individu organisasi lain.
5.	*Low*	Peristiwa ancaman dapat diharapkan memiliki efek buruk terbatas pada operasi organisasi, aset organisasi, individu organisasi lain.
6.	*Very Low*	Peristiwa ancaman dapat diharapkan memiliki efek buruk yang dapat diabaikan pada operasi organisasi, aset organisasi, individu organisasi lain.

4.2 Melakukan Penilaian

Dalam proses penilaian risiko terhadap aset pendukung dari aplikasi sistem pembelajaran eLINA melakukan penilaian. Risiko keamanan yang dapat diprioritaskan oleh tingkat risiko dan digunakan untuk menginformasikan keputusan respons risiko.

4.2.1 Identifikasi Aset

Seorang pemilik aset harus di identifikasi untuk setiap aset, untuk memberikan tanggung jawab dan akuntabilitas untuk aset terssebut. Pemilik 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 lainya 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 4.8.

Tabel 4.8 Daftar 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

Sumber : Hasil Penelitian

4.2.2 Identifikasi Ancaman

Tahap ini melakukan indentifikasi ancaman pada setiap aset dan sistem aplikasi eLINA Universitas Narotama yang teridentifikasi akan terjadinya permasalahan tersebut. tabel berikut menjelaskan ancaman apa saja yang dapat teridentifikasi dalam penelitian ini dapat dilihat pada Tabel 4.9.

Tabel 4.9 Identifikasi Ancaman

No.	Identifikasi	Sumber Ancaman	In scope	Rentang Efek
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)	Salah pengoperasian sistem yang meyebabkan *sistem* terhenti.	Ya	*High*
		Pencurian (*password*) terhadap aplikasi *e - learning* yang dapat mengakses profil/data yang sifatnya pribadi.	Ya	*High*
		Terjadi kesalahan dalam pengelolahan data oleh staff atau dosen.	Ya	*Very High*
		Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Ya	*Moderate*
		Kesalahan dalam *deployment* aplikasi *e-learning*	Ya	*Low*
		Pemanfaatan celah keamanan aplikasi *e-learning* oleh pihak dalam/luar.	Ya	*Moderate*

Sumber: Hasil Penelitian

Tabel 4.9 Identifikasi Ancaman (Lanjutan)

No.	Identifikasi		Sumber Ancaman	In scope	Rentang Efek
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)		Kehilangan data yang sifatnya sensitif.	Ya	*Very High*
			Kesalahan operasional yang disebabkan oleh staff IT.	Ya	*Moderate*
2.	*Windows Server* (*Proxmox, VMWareESXI*)		Windows tidak berjalan semestinya.	Ya	*High*
3.	IBM 3850 M2 / x3950 M2 server	*Database Server*	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Ya	*Very High*
		Storage server	Menggunakan *Password* Lemah atau menggunakan *default password.*	Ya	*Very High*
		OS Server	Tidak berjalan semestinya (Bajakan).	Ya	*Moderate*
			Kerusakan pada aset yang sudah menua ataupun rusak.	Ya	*Moderate*

Sumber: Hasil Penelitian

Tabel 4.9 Identifikasi Ancaman (Lanjutan)

No.	Identifikasi	Sumber Ancaman	In scope	Rentang Efek
3.	IBM 3850 M2 / x3950 M2 server	Bencana alam (banjir, kebakaran, gempa bumi, bom) sehingga bisa terjadinya kerusakan pada server.	Ya	*Very High*
		Ruangan server yang temperatur suhunya tidak stabil.	Ya	*Moderate*
		Pencurian pada *server* sehingga bisa terjadinya permasalahan pada semua sistem.	Ya	*Moderate*
		Gangguan tegangan listrik	Tidak	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.9 Identifikasi Ancaman (Lanjutan)

No.	Identifikasi		Sumber Ancaman	In scope	Rentang Efek
4.	IBM System x3400 M3 Server	*Database Server*	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Ya	*Very High*
		Storage server	menggunakan *Password* Lemah atau menggunakan *default password.*	Ya	*Moderate*
		OS Server	*OS Server* yang tidak berjalan semestinya (Bajakan).	Ya	*Moderate*
			Kerusakan pada aset yang sudah menua ataupun rusak.	Ya	*Moderate*
			Ruangan server yang temperatur suhunya tidak stabil.	Ya	*Moderate*
			Pencurian pada *server* sehingga bisa terjadinya permasalahan pada semua sistem.	Ya	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.9 Identifikasi Ancaman (Lanjutan)

No.	Identifikasi	Sumber Ancaman	In scope	Rentang Efek
4.	IBM 3850 M2 / x3950 M2 server	Bencana alam (banjir, kebakaran, gempa bumi, bom) sehingga bisa terjadinya kerusakan pada server.	Ya	*Very High*
		Gangguan tegangan listrik.	Tidak	*Moderate*
5.	*Router Linksys E1200*	Password lemah / menggunakan default password.	Ya	*High*
		Gangguan tegangan listrik.	Ya	*Moderate*
		Bencana alam (banjir, kebakaran, gempa bumi, cuaca curam,bom).	Ya	*Very High*
		Gangguan jaringan yang disebabkan oleh penyedia layanan internet.	Tidak	*High*

Sumber : Hasil Penelitian

4.2.3 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. 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 , organisasi mempertimbangkan serangkaian peristiwa ancaman yang reprensentatif dapat berfungsi sebagai titik awal untuk mengidentifikasi peristiwa ancaman spesifik dalam penilaian risiko dan tingkat konfirmasi apa yang diperlukan agar perisitiwa 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 dapat dilihat pada Tabel 4.10 .

Tabel 4.10 Identifikasi Peristiwa Ancaman

No.	Identifikasi	Peristiwa Ancaman	Sumber Ancaman	Relevansi
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)	Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Salah pengoperasian sistem yang meyebabkan *sistem* terhenti.	Diantisipasi
		Melakukan pengintaian / pemindaian jaringan perimeter.	Pencurian (*password*) terhadap aplikasi *e - learning* yang dapat mengakses profil/data yang sifatnya pribadi.	Dikonfirmasi
		Pertengkaran komunikasi	Terjadi kesalahan dalam pengelolahan data oleh staff atau dosen.	Diantisipasi
		Memberikan malware yang ditargetkan untuk kontrol sistem internal dan pengelupasan data.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Mungkin
		Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Kesalahan dalam *deployment* aplikasi *e-learning*	Dikonfirmasi

Sumber: Hasil Penelitian

Tabel 4.10 Identifikasi Peristiwa Ancaman (Lanjutan)

No.	Identifikasi		Peristiwa Ancaman	Sumber Ancaman	Relevansi
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)		Melakukan mengendus jaringan dari jaringan yang terpapar.	Pemanfaatan celah keamanan aplikasi *e-learning* oleh pihak dalam/luar.	Diantisipasi
			Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Kehilangan data yang sifatnya sensitif.	Diantisipasi
			Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Kesalahan operasional yang disebabkan oleh staff IT.	Diantisipasi
2.	*Windows server (Proxmox, VMWareESXI)*		Pengaturan hak khusus yang salah.	Windows tidak berjalan semestinya.	Diantisipasi
3.	IBM 3850 M2 / x3950 M2 server	*Database Server*	Melakukan pengintaian / pemindaian jaringan perimeter.	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Dikonfirmasi
		Storage server	Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	*Storage Server* yang menggunakan *Password* Lemah atau menggunakan *default password.*	Diantisipasi

Sumber : Hasil Penelitian

Tabel 4.10 Identifikasi Peristiwa Ancaman (Lanjutan)

No.	Identifikasi		Peristiwa Ancaman	Sumber Ancaman	Relevansi
3.	IBM 3850 M2 / x3950 M2 server	OS Server	Pengenalan kerentanan ke dalam produk perangkat lunak.	*OS Server* yang tidak berjalan semestinya (Bajakan).	DiKonfirmasi
			Kesalahan disk	Kerusakan pada aset yang sudah menua ataupun rusak.	Diantisipasi
			Penipisan sumber daya.	Pencurian pada *server* sehingga bisa terjadinya permasalahan pada semua sistem.	Mungkin
			Gempa bumi di fasilitas utama, Kebakaran di fasilitas utama, Banjir difasilitas Utama.	Bencana alam (banjir, kebakaran, gempa bumi, bom) sehingga bisa terjadinya kerusakan pada server.	Diprediksi
			Kesalahan disk.	Ruangan server yang temperatur suhunya tidak stabil.	Dikonfirmasi

Sumber : Hasil Penelitian

Tabel 4.10 Identifikasi Peristiwa Ancaman (Lanjutan)

No.	Identifikasi		Peristiwa Ancaman	Sumber Ancaman	Relevansi
3.	IBM 3850 M2 / x3950 M2 server		Pertengkaran Komunikasi	Gangguan tegangan litrik.	Diantisipasi
4.	IBM System x3400 M3 Server	*Database Server*	Melakukan pengintaian / pemindaian jaringan perimeter.	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Dikonfirmasi
		Storage server	Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	*Storage Server* yang menggunakan *Password* Lemah atau menggunakan *default password.*	Diantisipasi
		OS Server	Pengenalan kerentanan ke dalam produk perangkat lunak.	*OS Server* yang tidak berjalan semestinya (Bajakan).	Dikonfirmasi
			Kesalahan disk	Kerusakan pada aset yang sudah menua ataupun rusak.	Diantisipasi
			Pengenalan kerentanan ke dalam produk perangkat lunak.	Aplikasi error saat digunakan (Bajakan).	Diantisipasi

Sumber : Hasil Penelitian

Tabel 4.10 Identifikasi Peristiwa Ancaman (Lanjutan)

No.	Identifikasi	Peristiwa Ancaman	Sumber Ancaman	Relevansi
4.	IBM System x3400 M3 Server	Penipisan sumber daya.	Pencurian pada *server* sehingga bisa terjadinya permasalahan pada semua sistem.	Mungkin
		Gempa bumi di fasilitas utama, Kebakaran di fasilitas utama, Banjir difasilitas Utama.	Bencana alam (banjir, kebakaran, gempa bumi,bom) sehingga bisa terjadinya kerusakan pada server.	Diprediksi
		Kesalahan disk.	Ruangan server yang temperatur suhunya tidak stabil.	Dikonfirmasi

Sumber : Hasil Penelitian

Tabel 4.10 Identifikasi Peristiwa Ancaman (Lanjutan)

No.	Identifikasi	Peristiwa Ancaman	Sumber Ancaman	Relevansi
5.	*Router Linksys E1200*	Pengaturan hak khusus yang salah.	*Password* lemah / menggunakan *default password.*	Dikonfirmasi
		Pertengkaran Komunikasi.	Gangguan tegangan listrik.	Diprediksi
		Gempa bumi di fasilitas utama, Kebakaran di fasilitas utama, Banjir difasilitas Utama.	Bencana alam (banjir, kebakaran, gempa bumi,bom)	Mungkin
		Pertengkaran Komunikasi	Gangguan jaringan yang disebabkan oleh penyedia layanan internet.	Dikonfirmasi

Sumber : Hasil Penelitian

4.2.4 Identifikasi Kerentanan

Pada tahapan ini menjelasakan organisasi menentukan jenis krentanan yang harus dipertimbangkan selama penilaian risiko dan tingkat perincian yang diberikan dalam deskripsi kerentanan. Organisasi membuat eksplisit proses yang digunakan untuk mengidentifikasi kerentanan dan asumsi apapun yang terkait dengan proses identifikasi kerentanan. Jika informasi tersebut diidentifikasi selama langkah pembingkaian risiko dan dimasukan sebagai bagian dari strategi manajemen risiko organisasi, informasi tersebut tidak perlu diulang dalam setiap penilaian risiko individu. Kerentanan dapat dikaitkan dengan sistem informasi organisasi misalnya perangkat keras, perangkat lunak, kontrol internal dan prosedur keamanan atau lingkungan dimana sistem tersebut beroperasi dapat dilihat pada Tabel 4.11.

Tabel 4.11 Identifikasi Kerentanan

No.	Identifikasi	Kerentanan	Vulnerability Severity
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)	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 pengelolahan informasi/materi.	*Very High*
		Pengguna menggunakan *password Default* sehingga akan mudah terjadinya pencurian *password.*	*High*
		Belum adanya *upgrade* untuk bahasa *pemrograman* yang digunakan maupun versi *database* yang digunakan sehingga kemanan kurang.	*High*

Sumber : Hasil Penelitian

Tabel 4.11 Identifikasi Kerentanan

No.	Identifikasi	Kerentanan	Vulnerability Severity
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)	Tidak ada sistem *backup* pada keamanan *database* sehingga bisa terjadinya kehilangan data yang sifatnya sensitif.	*Very High*
		Jumlah mahasiswa terlalu banyak dan keterbatasan sumber daya manusia menyebabkan kesalahan pengelolahan nilai mahasiswa.	*Very High*
2.	*Windows Server (ProxMox, VMWareESXI)*	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 pada server oleh pihak luar/dalam.	*Moderate*

Sumber : Hasil Penelitan

Tabel 4.11 Identifikasi Kerentanan

No.	Identifikasi	Kerentanan	Vulnerability Severity
3.	IBM 3850 M2 / x3950 M2 server	Ruangan server terletak di lantai 1 sehingga jika ada banjir memungkinkan server terendam.	*Very High*
		Tegangann listrik yang bisa secara tiba-tiba naik dan turun.	*Moderate*
4.	IBM System x3400 M3 Server	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	*Very High*
		Tidak adanya pengecekan secara rutin disetiap ruangan server.	*High*
		Tegangann listrik yang bisa secara tiba-tiba naik dan turun.	*Moderate*
5.	*Router Linksys E1200*	Jaringan yang terhubung dalam dalam perangkat tersebut mengalami gangguan.	*High*

Sumber: Hasil Penelitian

Tabel 4.12 Identifikasi Kecenderungan

No.	Identifikasi	Kondisi Kecenderungan	Tingkat Kondisi
1.	Aplikasi Sistem Pembelajaran eLINA (*e-Learning*)	Kehilangan data yang sifatnya sensitif pernah terjadi 1x.	*Very High*
		Jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam pengelolahan data oleh staff atau dosen pernah terjadi 10x.	*Very High*
		Gangguan tegangan listrik pernah terjadi 2x.	*Moderate*
		Kesalahan operasional yang disebabkan oleh staff IT terjadi pernah 16x.	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.12 Identifikasi Kecenderungan

No.	Identifikasi	Kondisi Kecenderungan	Tingkat Kondisi
2.	IBM 3850 M2 / x3950 M2 server	Kerusakan pada aset yang sudah menua ataupun rusak pernah terjadi 1x.	*Moderate*
		Ruangan server yang temperatur suhunya tidak sesuai standart pernah terjadi 5x.	*Moderate*
		Kesalahan dalam deployment aplikasi *e – learning* pernah terjadi 3x.	*Low*
3.	IBM System x3400 M3 Server	Kerusakan pada aset yang sudah menua ataupun rusak pernah terjadi 1x.	*Moderate*
4.	*Router Linksys E1200*	Kesalahan jaringan yang disebabkan oleh penyedia layanan internet pernah terjadi 2x.	*Moderate*

Sumber : Hasil Penelitian

4.2.5 Identifikasi Kemungkinan

Pada tahapan ini menjelaskan organisasi membuat eksplisit proses yang digunakan untuk melakukan penentuan kemungkinan atau asumsi yang terkait dengan proses penentuan kemungkinan. Jika informasi tersebut diidentifikasi selama langkah pembingkaian risiko dan dimasukan sebagai bagian dari strategi manajemen risiko organisasi, informasi tersebut tidak perlu diulang dalam setiap penilaian individu dapat dilihat pada Tabel 4.13.

Tabel 4.13 Identifikasi Kemungkinan

No.	Risiko	Kemungkinan peristiwa ancaman yang terjadi	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan
1.	Kehilangan data yang sifatnya sensitif.	*Low*	*Very High*	*Moderate*
2.	pengoperasian sistem yang meyebabkan *sistem* terhenti.	*Low*	*Very High*	*Moderate*
3.	Pencurian (*password*) terhadap aplikasi *e - Learning* yang dapat mengakses profil/data yang sifatnya pribadi.	*Low*	*Very High*	*Moderate*
4.	Terjadi kesalahan dalam penginputan data mahasiswa oleh staff atau dosen.	*Moderate*	*Very High*	*High*
5.	Gangguan tegangan listrik.	*Low*	*High*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.13 Identifikasi Kemungkinan

No.	Risiko	Kemungkinan peristiwa ancaman yang terjadi	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan
6.	Kesalahan operasional yang disebabkan oleh staff IT.	*Moderate*	*Moderate*	*Moderate*
7.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	*Low*	*Very High*	*Moderate*
8.	Kerusakan pada aset yang sudah menua ataupun rusak.	*Low*	*Moderate*	*Low*
9.	Kesalahan dalam *deployment* aplikasi *E – learning* .	*Low*	*High*	*Moderate*
10.	Pemanfaatan celah keamanan aplikasi *e-learning* oleh pihak dalam/luar.	*Low*	*Very High*	*Moderate*
11.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	*Very Low*	*Very High*	*Low*

Sumber: Hasil Penelitian

Tabel 4.13 Identifikasi Kemungkinan

No.	Risiko	Kemungkinan peristiwa ancaman yang terjadi	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan
12.	Bencana alam (banjir, kebakaran, gempa bumi,bom) sehingga bisa terjadinya kerusakan seluruh pada aset.	*Very Low*	*Very High*	*Low*
13.	Ruangan server yang temperatur suhunya tidak terlalu dingin.	*Low*	*High*	*Moderate*
14.	Gangguan Jaringan	*Low*	*Very High*	*Moderate*

Sumber : Hasil Penelitian

4.2.6 Identifikasi Dampak

Pada tahapan ini menentukan menentukan potensi dampak buruk dalam hal operasi organisasi misalnya, Misi, fungsi, citra, dan reputas, aset organisasi, individu, organisasi lain. Organisasi membuat eksplisit proses yang digunakan untuk melakukan penentuan dampak dan setiap asumsi yang terkait dengan proses penentuan dampak. Jika informasi tersebut diidentifikasi selama langkah pembingkaian risiko dan dimasukkan sebagai bagian dari strategi manajemen risiko organisasi, informasi tersebut tidak perlu diulang dalam setiap penilaian risiko individu. Organisasi mengatasi dampak pada tingkat detail yang mencakup, misalnya, misi spesifik/proses bisnis atau sumber daya informasi misalnya, Informasi, personel, peralatan, dana, dan teknologi informasi. Organisasi dapat memasukkan informasi dari Analisis Dampak Bisnis sehubungan dengan memberikan informasi dampak untuk penilaian risiko dapat dilihat pada Tabel 4.14.

Tabel 4.14 Identifikasi Dampak

No.	Jenis Dampak	Keterangan	Dampak Maksimal
1.	Kehilangan data yang sifatnya sensitif.	Dampaknya *very high* karena data yang didalamnya berupa data yang sensitif yang mempengaruhi akreditasi.	*Very High*
2.	pengoperasian sistem yang meyebabkan *sistem* terhenti.	Halaman *web* tidak dapat diakses dan juga proses layanan tidak jalan.	*High*
3.	Pencurian (*password*) terhadap aplikasi *e - Learning* yang dapat mengakses profil/data yang sifatnya pribadi.	Dampaknya *high* karena capain pembelajaran ada dilaksanakan melalui eLINA maka, akan terjadinya permasalahan pencurian kunci jawaban/data yang sifatnya pribadi.	*High*
4.	Jumlah data nilai mahasiswa yang banyak, terjadi kesalahan dalam penginputan data oleh staff atau dosen.	Dampak *very high* karena bisa mempengaruhi penilaian mahasiswa.	*Very High*
5.	Gangguan tegangan listrik	Dampaknya *moderate* karena bisa menyebabkan sistem bermasalah dan kemungkinan memory server error ketika dinyalakan kembali.	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.14 Identifikasi Dampak (Lanjutan)

No.	Jenis Dampak	Keterangan	Dampak Maksimal
6.	Kesalahan operasional yang disebabkan oleh staff IT.	Kesalahan setting pada aktivitas *e – learning*	*Moderate*
7.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Jika server terkena virus dampaknya *high* karena bisa meyebabkan *sistem* terhenti	*High*
8.	Kerusakan pada aset yang sudah menua ataupun rusak	Dampaknya *high* karena bisa terjadinya permasalahan pada server.	*High*
9.	Kesalahan dalam *deployment* aplikasi *E – learning.*	Beberapa fitur kemungkinan tidak berfungsi.	*Moderate*
10.	Pemanfaatan celah keamanan aplikasi *e-learning* oleh pihak dalam/luar.	Dampaknya *high* karena membutuhkan tim rekanan yang memperbaiki program.	*High*

Sumber : Hasil Penelitian

Tabel 4.14 Identifikasi Dampak (Lanjutan)

No.	Jenis Dampak	Keterangan	Dampak Maksimal
11.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	Bedampak *very high* pada sistem sehinggan sistem eLINA tidak bisa berjalan.	*Very High*
12.	Bencana alam (banjir, kebakaran, gempa bumi,bom) sehingga bisa terjadinya kerusakan pada aset.	Dampaknya *very high* karena bisa menyebabkan *sistem* mati total dan seluruh data yang sifatnya sensitif akan hilang.	*Very High*
13.	Ruangan server yang temperatur suhunya tidak terlalu dingin.	Dampaknya *moderate* karena bisa terjadinya permasalahan pada server.	*Moderate*
14.	Gangguan jaringan	Dampaknya *moderate* Jaringan internet akan mengalami kegagalan koneksi yang berdampak pada sistem eLINA.	*High*

Sumber : Hasil Penelitian

4.2.7 Identifikasi Penentuan Risiko

Pada tahapan ini menjelaskan menilai risiko dari peristiwa ancaman sebagai kombinasi kemungkinan dan dampak. Tingkat risiko yang terkait dengan peristiwa ancaman yang teridentifikasi mewakili penentuan sejauh mana organisasi terancam oleh peristiwa semacam itu. Organisasi membuat secara eksplisit ketidakpastian dalam penentuan risiko, termasuk, misalnya, asumsi organisasi dan penilaian/keputusan subyektif. Organisasi dapat menerapkan daftar peristiwa ancaman yang menjadi perhatian berdasarkan tingkat risiko yang ditentukan selama penilaian risiko-dengan perhatian terbesar diberikan pada peristiwa berisiko tinggi. Organisasi selanjutnya dapat memprioritaskan risiko pada tingkat yang sama atau dengan skor yang sama. Setiap risiko sesuai dengan peristiwa ancaman khusus dengan tingkat dampak jika peristiwa itu terjadi. ketika beberapa risiko muncul, bahkan jika setiap risiko berada pada tingkat sedang, serangkaian risiko tingkat sedang tersebut dapat teragregasi ke tingkat risiko yang lebih tinggi bagi organisasi. Untuk mengatasi situasi di mana bahaya terjadi berkali-kali, organisasi dapat mendefinisikan peristiwa ancaman sebagai kejadian berulang kali bahaya dan tingkat dampak yang terkait dengan tingkat kerusakan kumulatif. Efektivitas hasil penilaian risiko sebagian ditentukan oleh kemampuan pengambil keputusan untuk dapat menentukan keberlangsungan asumsi yang dibuat sebagai bagian dari penilaian. Informasi terkait dengan ketidakpastian disusun dan disajikan dengan cara yang siap mendukung keputusan manajemen risiko yang terinformasi dapat dilihat pada Tabel 4.15.

Tabel 4.15 Penentuan Risiko

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
1.	Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Kehilangan data yang sifatnya sensitif.	*Very High*	Dikonfirmasi	Permasalahan terjadi 1x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun.	Tidak ada sistem *backup* pada keamanan *database* sehingga bisa terjadinya kehilangan data yang sifatnyasensitif.	*Very High*	Peristiwa ancaman dimulai atau terjadi memiliki dampak yang sangat buruk.	*Moderate*	*Very High*	*High*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
2.	Pertengkaran komunikasi.	Terjadi kesalahan dalam pengelolahan data mahasiswa oleh staff atau dosen.	*Very High*	Dikonfirmasi	Permasalahan terjadi 10x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun.	Jumlah mahasiswa terlalu banyak dan keterbatasan sumber daya manusia.	*Very High*	Peristiwa ancaman dimulai atau terjadi memiliki dampak yang sangat buruk.	*High*	*Very High*	*Very High*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
3.	Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Kesalahan dalam *deployment* aplikasi *e – learning.*	*Low*	Dikonfirmasi	Permasalahan terjadi 3x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun.	Sumber daya terbatas sehingga meyebabkan kesalahan dalam *mendeployment* aplikasi	*Moderate*	Jika peristiwa ancaman dimulai atau terjadi, sangat mungkin memiliki dampak buruk.	*Moderate*	*Moderate*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
4.	Salah penanganan informasi kritis dan / atau sensitif oleh pengguna yang berwenang.	Kesalahan operasional yang disebabkan oleh staff IT	*Moderate*	Diantisipasi	Permasalahan terjadi 16x dalam jangka waktu 1 tahun/lebih.	Kurang teliti dan kurang berhati – hati disaat bekerja.	*Moderate*	Jika peristiwa ancaman dimulai atau terjadi, itu agaknya memiliki dampak buruk.	*Moderate*	*Moderate*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
5.	Pertengkaran Komunikasi	Gangguan tegangan listrik.	*Moderate*	Diantisipasi	Permasalahan terjadi 2x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun..	Cuaca curam yang bisa secara tiba-tiba menyabakan tegangan listrik naik dan turun.	*Moderate*	Jika peristiwa ancaman dimulai atau terjadi, itu agaknya memiliki dampak buruk	*Moderate*	*Moderate*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
6.	Kesalahan disk	Kerusakan pada aset yang sudah menua ataupun rusak.	*Moderate*	Diantisipasi	Permasalahan terjadi 1x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun.	Tidak adanya pengecekan secara rutin disetiap ruangan server.	*High*	Jika peristiwa ancaman dimulai atau terjadi, itu agaknya memiliki dampak buruk	*Low*	*High*	*Low*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
7.	Kesalahan Disk.	Ruangan server yang termpatur suhunya tidak sesuai standart.	*Moderate*	Dikonfirmasi	Permasalahan terjadi 5x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun..	Tidak adanya pengecekan secara rutin disetiap ruangan server.	*Moderate*	Jika peristiwa ancaman dimulai atau terjadi, sangat mungkin memiliki dampak buruk.	*Moderate*	*Moderate*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
8.	Salah penanganan informasi kritis dan/atau sensitif oleh pengguna yang berwenang	Salah pengoperasian sistem yang menyebabkan sistem terhenti.	*High*	Diantisipasi	Belum Pernah terjadi.	Pengendalian dokumen belum diterapkan dengan baik.	*High*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Moderate*	*High*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
9.	Melakukan pengintaian/ pemindaian jaringan internet.	Pencurian (*password*) terhadap aplikasi *e-learning* yang dapat mengakses profil/data yang sifatnya pribadi.	*High*	Diantisipasi	Belum pernah terjadi.	Pengguna masih menggunakan *password Default* sehingga akan mudah terjadinya pencurian *password*.	*High*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Moderate*	*High*	*Moderate*

Sumber: Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
10.	Memberikan *malware* yang ditargetkan untuk kontrol sistem internal dan pengelupasan data.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	*High*	Diantisipasi	Belum pernah terjadi.	Staff saat bekerja membawa laptop masing – masing.	*Moderate*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Moderate*	*High*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
11.	Melakukan mengendus jaringan dari jaringan yang terpapar	Pemanfaatan celah keamanan aplikasi *e-learning* oleh pihak dalam/luar.	*Moderate*	Diantisipasi	Belum pernah terjadi.	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	*Very High*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Moderate*	*High*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
12.	Penipisan sumber daya.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	*Moderate*	Diantisipasi	Belum pernah terjadi.	Ruangan server kurang adanya keamanan sehingga bisa terjadinya pencurian pada pada server oleh pihak luar/dalam.	*Moderate*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Moderate*	*Very High*	*High*

Sumber: Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
13.	Gempa bumi di fasilitas utama, Kebakaran di fasilitas utama, Banjir difasilitas Utama.	Bencana alam (banjir, kebakaran, gempa bumi,bom) sehingga bisa terjadinya kerusakan pada server.	*Very High*	Diprediksi	Belum pernah terjadi.	Ruangan server di universitas narotama terletak di lantai 1 sehingga jika ada banjir memungkinkan server terendam.	*Very High*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Low*	*Very High*	*Moderate*

Sumber : Hasil Penelitian

Tabel 4.15 Penentuan Risiko (Lanjutan)

No.	Perisitiwa ancaman	Ancaman	Rentang Efek	Relevansi	Kemungkinan peristiwa terjadi	Kerentanan	Kekerasan	Kemungkinan peristiwa ancaman yang menghasilkan dampak buruk	Keseluruhan Kemungkinan	Tingkatan dari dampak	Risiko
14.	Pertengkaran Komunikasi	Gangguan Jaringan	*High*	Dikonfirmasi	Permasalahan terjadi 2x dalam jangka waktu kurang dari setahun sekali/lebih dari sekali setiap 10 tahun.	*High*	*High*	Jika peristiwa ancaman dimulai atau terjadi, hampir pasti memiliki dampak buruk.	*Moderate*	*High*	*Moderate*

Sumber : Hasil Penelitian

4.3 Mengkomunikasikan hasil penelitian

4.3.1 Mengkomunikasikan Hasil Penilaian Risiko

Membagikan informasi terkait yang dihasilkan selama penilian risiko terhadap sistem pembelajaran *e – learning* Universitas Narotama kepada pimpinan departemen eLINA dan beberapa personil dan juga memberikan penilaian risiko termasuk sistem informasi yang menggambarkan seperti fungsi misi, Proses bisnis dan ketergantungan pada sistem lain, atau infrastruktur umum guna untuk mendukung respons risiko.

4.3.2 Informasi Terkait Dengan Risiko

Setelah melakukan identifikasi segala permasalahan dan menentukan penilaian pada aset maupun sistem pembelajaran *e – learning* Universitas Narotama tujuan ini dari penilaian risiko merupakan, untuk mengetahui tingkatan permasalahan dan menggambarkan keseluran tingkat risiko yang harus segera dimitigasi terhadap organisasi. Dan tahap selanjutnya melakukan informasi respon risiko terhadap organisasi yang akan dilakukan untuk mengkomunikasikan hasil dari penilaian tersebut dalam bentuk laporan penilaian guna untuk mendukung respons risiko.

4.4 Menjaga Penilaian

4.4.1 Faktor Risiko Monitor

Pada tahap ini dilakukan untuk memantau faktor risiko yang penting secara berkesinambungan untuk memastikan bahwa informasi yang diperlukan untuk membuat keputasan yang kredibel dan berbasis risiko tersedia seiring waktu. Pemantauan faktor risiko ini dilakukan dengan cara mengidentifikasi sumber ancaman, peristiwa ancaman, kerentanan, kondisi kecenderungan, kemungkinan, penargetan operasi organisasi, aset, atau individu yang dapat memberikan informasi penting tentang perubahan kondisi yang berpotensi mempengaruhi kemampuan organisasi untuk melakukan misi inti dan fungsi bisnis.

4.4.2 Penilain Risiko Pembaruan

Pada tahap ini dilakukan untuk menentukan frekuensi dan keadaan dimana penilaian risiko diperbarui. Penentuan tersebut dilakukan dengan mengidentifikasi tingkat risiko saat ini. Organisasi mengkomunikasikan hasil penilaian risiko kepada entitas disemua tingkatan manajemen risiko untuk memastikan bahwa pejabat organisasi yang bertanggung jawab memiliki akses informasi penting yang perlukan untuk membuat keputusan berbasis risiko yang berkelanjutan.

4.5 Rekomendasi

Setelah melakukan identifikasi risiko dan penilaian risiko terhadap sistem pembelajaran eLINA Universitas Narotama, maka pada tahap ini melakukan berupa rekomendasi dari tingkatan masalah yang terdiri mulai dari *Very High*, *High*, *Moderate*, *Low*, *Very Low* berguna untuk meminimalisir permasalahan atau mencegah permasalahan pada sistem pembelajaran eLINA agar untuk kedepannya proses operasional bisa terhindar dari risiko-risiko ataupun ancaman dapat dilihat pada Tabel 4.16.

Tabel 4.16 Rekomendasi

No.	Ancaman	Kerentananan	Dampak	Tingkat Risiko	Rekomendasi
1.	Kehilangan data yang sifatnya sensitif.	Tidak ada sistem *backup* pada keamanan *database* sehingga bisa terjadinya kehilangan data yang sifatnya sensitif.	data yang didalamnya berupa data yang sensitif yang mempengaruhi akreditasi.	*High*	Menambahkan *strorage* khusus untuk sistem *backup.*
2.	Terjadi kesalahan dalam pengelolahan data mahasiswa oleh staff atau dosen.	Jumlah mahasiswa terlalu banyak.	Dampaknya bisa mempengaruhi penilaian mahasiswa.	*Very High*	Melakukan pengecekan secara ulang terhadap penilaian mahasiswa.
3.	Kesalahan dalam *deployment* aplikasi *e – learning.*	Sumber daya terbatas sehingga meyebabkan kesalahan dalam *mendeployment* aplikasi.	Beberapa fitur kemungkinan tidak berfungsi.	*Moderate*	Dilakukan pengujian dan memperbarui layanan secara berkala.

Sumber : Hasil Penelitian

Tabel 4.16 Rekomendasi (Lanjutan)

No.	Ancaman	Kerentananan	Dampak	Tingkat Risiko	Rekomendasi
4.	Kesalahan operasional yang disebabkan oleh staff IT	Kurang teliti dan kurang berhati – hati disaat bekerja.	Kesalahan setting pada aktivitas *e – learning.*	*Moderate*	1. Melakukan pengecekan secara ulang. 2. Mentraining staff IT saat mengperasikan sistem.
5.	Ganggan tegangan listrik.	Cuaca curam yang bisa secara tiba-tiba menyabakan tegangan listrik naik dan turun.	bisa menyebabkan sistem bermasalah dan kemungkinan memory server error ketika dinyalakan kembali.	*Moderate*	Menetapkan beberapa ganset demi menjaga proses keberlangsungan sistem.
6.	Kerusakan pada aset yang sudah menua ataupun rusak.	Tidak adanya pengecekan secara rutin disetiap ruangan server.	bisa terjadinya permasalahan pada server.	*Low*	Melakukan pengecekan ruangan server secara rutin.

Sumber : Hasil Penelitian

Tabel 4.16 Rekomendasi (Lanjutan)

No.	Ancaman	Kerentananan	Dampak	Tingkat Risiko	Rekomendasi
7.	Ruangan server yang termpatur suhunya tidak sesuai standart.	Tidak adanya pengecekan secara rutin disetiap ruangan server dan penataan kabel belum diterapkan dengan baik.	bisa terjadinya permasalahan pada server.	*Moderate*	1. Melakukan pengecekan ruangan server secara rutin 2. melakukan penataan ulang terhadap kabel dari setiap perangkat jaringan yang terhubung.
8.	pengoperasian sistem yang menyebabkan sistem terhenti.	Pengendalian dokumen belum diterapkan dengan baik.	Halaman *web* tidak dapat diakses dan juga proses layanan tidak jalan.	*Moderate*	1. melalukan update virus secara rutin. 2. melakukan siklus update *noodle* secara rutin. 3. mengupgrade bahasa pemerograman PHP ke versi terbaru.

Sumber : Hasil Penelitian

Tabel 4.16 Rekomendasi (Lanjutan)

No.	Ancaman	Kerentananan	Dampak	Tingkat Risiko	Rekomendasi
9.	Pencurian (*password*) terhadap aplikasi *e – learning* yang dapat mengakses profil/data yang sifatnya pribadi.	Pengguna masih menggunakan *password Default* sehingga akan mudah terjadinya pencurian *password.*	Dampaknya capain pembelajaran ada dilaksanakan melalui eLINA maka, akan terjadinya permasalahan pencurian kunci jawaban/data yang sifatnya pribadi.	*Moderate*	Menerapkan konfigurasi dan manajemen password seperti contoh bagi pengguna harus wajib mengganti *password.*
10.	Adanya serangan malware atau virus yang disebabkan oleh pihak luar/dalam.	Staff saat bekerja membawa laptop masing – masing sehingga kemungkinan akan terjadinya pencurian informasi yang sifatnya pribadi ataupun memasukan malware pada sistem.	Jika server terkena virus bisa memeyebabkan *sistem* terhenti	*Moderate*	Menambahkan beberapa PC yang berkerja untuk mengoperasikan sistem tersebut.

Sumber: Hasil Penelitian

Tabel 4.16 Rekomendasi (Lanjutan)

No.	Ancaman	Kerentananan	Dampak	Tingkat Risiko	Rekomendasi
11.	Pemanfaatan celah keamanan aplikasi *e-learning* oleh pihak dalam/luar.	Server aplikasi dan database tidak ada konfigurasi standar keamanan.	Membutuhkan tim rekanan yang memperbaiki program.	*Moderate*	Menambahkan keamanan yang lebih pada *sistem.*
12.	Pencurian pada aset sehingga bisa terjadinya permasalahan pada semua sistem.	Tidak adanya keamanan disetiap ruang server.	Dampaknya bisa menyebabkan sistem bermasalah.	*High*	1. Menambahkan keamanan pada setiap ruangan server 2. menetapkan beberapa CCTV 3. Menambahkan sensor *finger print* dipintu masuk.
13.	Bencana alam (banjir, kebakaran, gempa bumi,bom) sehingga bisa terjadinya kerusakan pada server.	Ruangan server di universitas narotama terletak di lantai 1 sehingga jika ada banjir memungkinkan server terendam.	bisa menyebabkan *sistem* mati total dan seluruh data yang sifatnya sensitif akan hilang.	*Moderate*	Memindahkan ruangan server yang lebih aman.

Sumber : Hasil Penelitian

Tabel 4.16 Rekomendasi (Lanjutan)

No.	Ancaman	Kerentananan	Dampak	Tingkat Risiko	Rekomendasi
14.	Gangguan Jaringan	Jaringan yang terhubung dalam dalam perangkat tersebut mengalami gangguan.	Berdampak Jaringan internet akan mengalami kegagalan koneksi yang berdampak pada sistem eLINA.	*Moderate*	1. Melakukan review terhadap seluruh konfigurasi jaringan 2. Melakukan pengecekan dan perawatan secara rutin.

Sumber : Hasil Penelitian