Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1

A A Putro[1]*, A Ambarwati[2], E Setiawan[3]
Program Studi Sistem Informasi, Universitas Narotama
Jl. Arif Rahman Hakim No.51 Surabaya
andrewanggoroputro@gmail.com[1]*, ambarwati1578@yahoo.com[2],
eman.setiawan@narotama.ac.id[3]

diterima: 4 Agustus 2021
direvisi: 17 Agustus 2021
dipublikasi: 1 September 2021

Abstrak

EdLink merupakan produk *e-learning* yang mendukung pembelajaran *online* di perguruan tinggi. EdLink tersedia dalam *platform* android, IOS, dan *web browser*. Pada tahun 2020 pengguna EdLink tercatat 100 perguruan tinggi dan terjadi peningkatan sampai dengan 270 perguruan tinggi di seluruh Indonesia pada tahun 2021. Dengan adanya kebijakan pembelajaran daring akibat dampak *COVID*-19 dan kebutuhan pasar yang meningkat, maka peneliti melakukan analisis manajemen risiko EdLink dengan menggunakan metode NIST SP 800-30 Revisi 1. Metode NIST SP 800-30 Revisi 1 telah dibandingkan dengan metode lain dan dipilih karena sesuai dengan kebutuhan penelitian. Dengan menggunakan metode NIST SP 800-30 Revisi 1 akan diketahui risiko yang mungkin terjadi pada EdLink beserta dengan rekomendasi kontrol EdLink. Rekomendasi kontrol yang diberikan diharapkan dapat meminimalisir peluang munculnya risiko yang menyebabkan dampak buruk bagi aplikasi EdLink maupun perusahaan pengembang. Berdasarkan hasil penelitian yang telah dilakukan dapat diketahui terdapat tujuh risiko dengan rincian tiga tingkat *very high* dan empat tingkat *high*. Peneliti telah memberikan tujuh rekomendasi kontrol untuk risiko dengan tingkat *very high* dan *high*.
Kata kunci: EdLink; manajemen risiko; NIST SP 800-30 Revisi 1; rekomendasi kontrol

Abstract

EdLink is an e-learning product that supports online learning in universities. EdLink is available on android, IOS and web browser platforms. In 2020, EdLink users recorded 100 universities and there was an increase to 270 universities throughout Indonesia in 2021. Along with online learning policies due to the impact of COVID-19 and increasing market needs, the researchers conducted an EdLink risk management analysis using the NIST SP method. 800-30 Revision 1. The NIST SP 800-30 Revision 1 method has been compared with other methods and was chosen because it fits the needs of the study. In the NIST SP 800-30 Revision 1 method, the risks that may occur in EdLink will be known along with recommendations for EdLink control. The control recommendations given are expected to minimize the opportunity for the emergence of risks that cause adverse effects for the EdLink application and developer companies. Based on the results of the research that has been done, it can be seen that there are 7 risks with details of 3 very high levels and 4 high levels. Researchers have given 7 control recommendations for risk with very high and high levels.
***Keywords**: EdLink; risk management; NIST SP 800-30 Revision 1; control recommendations*

1. Pendahuluan

EdLink merupakan produk sistem *e-learning* yang dibuat untuk membantu mahasiswa dan dosen dalam kegiatan pembelajaran *online*. EdLink saat ini tersedia dalam *platform* android, IOS, dan *web browser*. Pengembang dari produk EdLink adalah PT SVU, perusahaan konsultan pengembang teknologi informasi yang berfokus pada dunia pendidikan dan berdiri pada tahun 2004. Efek dari pandemi *Covid* 19 menyebabkan terjadinya peningkatan jumlah pengguna EdLink yang sebelumnya pengguna EdLink hanya sekitar 100 perguruan tinggi saat ini digunakan lebih dari 270 perguruan tinggi yang tersebar

di seluruh Indonesia. Berdasarkan hasil wawancara penulis dengan *Product Manager* EdLink, belum pernah dilakukan analisa manajemen risiko pada EdLink.

Peningkatan pengguna yang signifikan tersebut perlu juga disertai dengan analisa manajemen risiko agar keberlangsungan proses bisnis tidak terganggu oleh kesalahan perangkat keras, kesalahan teknis, kesalahan sumber daya manusia, dan gangguan lainnya yang akan menyebabkan gangguan finansial, menurunnya reputasi perusahaan dan menurunnya tingkat kepuasan pelanggan. Ada banyak metode untuk melakukan analisa manajemen risiko yaitu *Mehari, Magerit*, NIST 800-30, dan *Microsoft's Security Management Guide*. Dari keempat metode tersebut NIST 800-30 lebih unggul karena bisa memberikan rekomendasi kontrol. Berdasarkan latar belakang tersebut maka akan dilakukan penelitian Analisa Manajemen Risiko *E-Learning* EdLink Menggunakan Metode NIST SP 800-30 Revisi 1.

Tujuan dilakukan penelitian ini adalah dapat mengetahui peristiwa ancaman yang dapat menimbulkan dampak yang buruk bagi EdLink. Contoh peristiwa ancaman dan dampak buruk yang sering muncul pada aplikasi pembelajaran *online* meliputi, menurunnya reputasi perusahaan yang disebabkan oleh aplikasi tidak dapat diakses, akses aplikasi dengan menggunakan kata sandi dengan tingkat keamanan rendah, menurunnya kepercayaan pengguna yang disebabkan oleh bocornya data pengguna ke publik, dan kehilangan jumlah pengguna aktif yang disebabkan oleh aplikasi yang sulit diakses. Selanjutnya adalah memberikan rekomendasi kontrol risiko kepada EdLink agar dapat mencegah potensi risiko yang akan muncul. Manfaat dari dilakukan penelitian ini adalah dapat mengurangi risiko yang kedepannya akan terjadi di EdLink dan dapat mempersiapkan tindakan pencegahan untuk menghadapi risiko yang akan terjadi.

2. Kajian Pustaka

Risiko yakni peluang yang dapat menimbulkan kerugian bagi organisasi atau perusahaan [1]. Disebutkan juga bahwa risiko merupakan hal yang memberikan dampak negatif atau ancaman terhadap nilai perusahaan [2]. Risiko dapat diidentifikasi dari internal mapun eksternal. Risiko yang disebabkan faktor internal seperti gangguan bencana alam, operasional, dan sebagainya [3].

Manajemen risiko adalah kegiatan mengidentifikasi risiko terhadap aset yang dimiliki. Manajemen risiko diperlukan dalam mengatur proses bisnis agar berjalan secara efektif sehingga memberi keuntungan bagi perusahaan dan meminimalisir dampak yang disebabkan risiko IT [4]. Terdapat tiga tahap manajemen risiko teknologi yakni *risk assesment, risk mitigation,* dan *evaluation and assesment* [5]. Tahap pertama *Risk assesment* adalah proses identifikasi risiko dan dampak risiko sehingga diketahui rekomendasi kontrol untuk meminimalisir risiko. Tahap kedua r*isk mitigation* adalah tahap dari memprioritaskan tingkat risiko, evaluasi penyebab dan dampak, dan mengimplementasikan rekomendasi yang telah dibuat. Tahap terakhir *evaluation and assesment* yakni proses berkelanjutan dari manajemen risiko yang telah dievaluasi sehingga seluruh tahapan telah berhasil dilakukan.

Ada beberapa contoh proses metode risiko yang bisa dilakukan, yaitu *Mehari, Magerit, NIST800-30, dan Microsoft's Security Management Guide.* Keempat manajemen risiko tersebut memiliki kelebihan dan kekurangan masing – masing. Dari keempat metode tersebut, NIST 800-30 lebih unggul karena bisa memberikan rekomendasi kontrol untuk objek yang sedang diteliti [6]

NIST SP 800-30 revisi 1 merupakan *framework* pengukuran risiko IT atau *risk assesment* [7]. Proses penilian risiko menurut NIST 800:30 revisi 1 terdiri dari identifikasi sumber ancaman, identifikasi peristiwa ancaman, identifikasi kerentanan, penentuan kemungkinan atau kecenderungan, analisa dampak, dan penentuan risiko [6].

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

Ada banyak kegiatan yang dilakukan pada UPT Perpustakaan Universitas Lampung seperti peminjaman buku, pengembalian, pencarian buku, dan unggah dokumen skripsi mahasiswa. Dari beberapa kegiatan yang dilakukan pada UPT Perpustakaan Universitas Lampung ditemukan masalah dan potensi risiko bagi sistem informasi perpustakaan. Untuk menghindari potensi permasalahan tersebut, maka dilakukan evaluasi potensi risiko dengan menggunakan metode NIST SP 800-30. Hasil evaluasi tersebut menemukan bahwa metode NIST SP 800-30, dapat mendeskripsikan profil risiko yang berpotensi mengancam keberlangsungan kegiatan pada UPT Perpustakaan Universitas Lampung [8].

E-Learning pada Universitas Narotama digunakan oleh semua mahasiswa dan dosen, dalam penggunaannya tersebut ditemukan potensi risiko yang mengancam berjalannya kegiatan belajar mengajar. Sehingga dilakukan proses penelitian untuk mengetahui potensi risiko apa yang mengancam *E-Learning* Universitas Narotama. Ditemukan bahwa metode NIST SP 800-30 dapat memberikan rekomendasi kontrol untuk mencegah potensi munculnya risiko yang mengancam sistem [9].

Dalam perjalanan proses kegiatan akademik STMIK Sumedang, masih ditemukan risiko yang mengancam proses kegiatan akademik. Untuk mengurangi potensi munculnya risiko maka dilakukan proses penelitian manajemen risiko menggunakan NIST SP 800-30 revisi 1. Ditemukan bahwa NIST SP 800-30 revisi 1 dapat menghasilkan tingkat potensi risiko yang akan terjadi pada STMIK Sumedang [10]

Masih ditemukan beberapa risiko yang mengancan proses berjalannya belajar mengajar pada aplikasi pembelajaran *Online* Universitas UPN Veteran Jakarta. Sehingga perlu dilakukan proses penilaian risiko dengan menggunakan metode Oktave Allegro. Hasil dari penilaian risiko tersebut dapat memberikan gambaran potensi risiko yang mengancam keberlangsungan proses belajar mengajar pada Universitas UPN Veteran jakarta. Sehingga UPN Veteran Jakarta dapat menghindari potensi risiko yang mungkin akan terjadi. [11]

3. Metode Penelitian

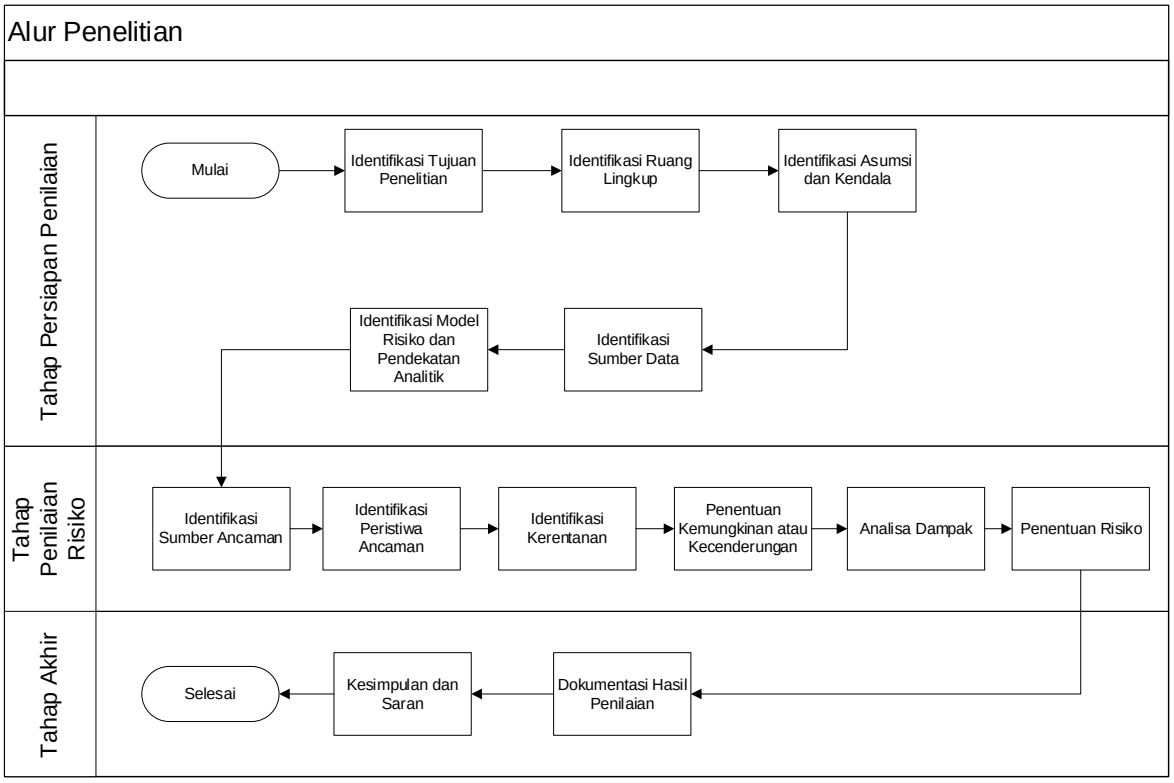
Pada tahap metode penelitian mengambarkan tahap-tahap penelitian yang dapat dilihat pada Gambar 1. Penelitian ini akan dibagi menjadi 3 tahapan yakni tahap persiapan penilaian, tahap penilaian risiko, dan tahap akhir. Tahap yang ada pada Gambar 1 diadopsi dari tahap yang ada pada NIST SP 800-30 revisi 1, dengan beberapa penyesuaian, pada tahapan tersebut penulis menambahkan tahap kesimpulan dan saran agar dapat mengetahui penyelesaian dari permasalah yang dapati.

Tahap pertama merupakan tahap persiapan penelitian. Tujuan utama dari tahap ini adalah untuk mengetahui tujuan dari dilakukannya analisis manajemen risiko pada EdLink. Identifikasi ruang lingkup dilakukan untuk menentukan apa yang akan dipertimbangkan dalam penilaian. Ruang lingkup penilaian risiko mempengaruhi kisaran informasi yang tersedia untuk membuat keputusan berbasis risiko dan ditentukan oleh peneliti. Identifikasi asumsi dan kendala perlu dilakukan untuk mengetahui secara spesifik area mana yang akan dilakukan proses penilaian risiko, agar penilaian risiko yang dilakukan dapat tepat sasaran. Wawancara dan pengisian kuesioner dilakukan kepada satu orang *product manager*, satu orang *product support*, dan dua *system engineer* EdLink dilakukan untuk memperoleh data. Selain individu yang akan diberikan kuesioner dan dilakukan proses wawancara, data selanjutnya yang dibutuhkan adalah data aset yang ada pada EdLink. Dari data yang sudah didapatkan selanjutnya perlu dilakukan identifikasi model risiko dan pendekatan analitik yang akan digunakan. Pada penelitian ini pendekatan analitik yang digunaakan adalah pendekatan analitik kualitatif.

Tahap kedua adalah penilaian risiko, yang dilakukan pertama adalah melakukan identifikasi sumber ancaman yang mengancam proses berjalannya kegiatan pada EdLink.

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

Dari sumber ancaman tersebut nantinya dapat diukur rentang efek dari setiap sumber ancaman yang ada pada setiap aset yang dimiliki EdLink. Identifikasi sumber ancaman perlu dilakukan untuk mengetahui apakah sumber ancaman yang ada masih relevan dengan EdLink. Setelah diketahui sumber ancaman dan peristiwa ancaman yang relevan terhadap Edlink proses selanjutnya adalah identifikasi kerentanan. Identifikasi kerentanan perlu dilakukan untuk mengetahui tingkat kerentanan aplikasi EdLink. Dari tingkat kerentanan yang sudah diidentifikasi selanjutnya dapat dilakukan identifikasi kemungkinan peristiwa ancaman muncul. Identifikasi kemungkinan dapat memberikan informasi seberapa sering peristiwa ancaman muncul dan seberapa mungkin peristiwa ancaman dapat memberikan dampak yang buruk kepada EdLink. Setelah diketahui kemungkinan peristiwa ancaman maka selanjutnya dapat dilakukan analisa dampak untuk mengetahui seberapa jauh dampak yang disebabkan oleh peristiwa ancaman. Setelah keempat data tersebut terkumpul selanjutnya adalah pentuan tingkat risiko dari setiap peristiwa ancaman yang disebabkan oleh sumber ancaman. Penentuan risiko dapat diketahui dari seberapa mungkin peristiwa ancaman muncul dan seberapa jauh dampak yang diberikan jika peristiwa ancaman tersebut terjadi pada EdLink.



Gambar 1. Metode Penelitian

Setelah diketahui tingkat risiko dari setiap peristiwa ancaman maka peneliti dapat memberikan rekomendasi kontrol untuk pengembang EdLink. Dari rekomendasi kontrol yang diberikan maka kesimpulan dan saran dapat diberikan kepada pengembang EdLink.

4. Hasil dan Pembahasan

4.1. Identifikasi Data

Pada tahap ini dilakukan identifikasi data yang akan digunakan dalam penelitian. Data yang akan digunakan dalam penelitian adalah data aset. Aset yang diidentifikasi disini adalah merupakan aset yang dimiliki oleh EdLink dan berdampak langsung kepada pengguna

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

Edlink. Aset yang tidak memiliki dampak secara langsung kepada pengguna EdLink seperti: laptop, monitor, mesin cetak, dan flashdisk tidak akan diidentifikasi.

Dari ketentuan diatas maka terdapat empat aset yang akan diidentifikasi risiko sumber ancamannya berdasarkan NIST SP 800-30 revisi 1. Aset yang dimiliki terletak di beberapa lokasi yang berbeda. Ada beberapa aset yang keberadaanya ada pada *Amazon Web Service (AWS)* yang merupakan pihak ketiga penyedia layanan komputasi awan. Informasi identifikasi aset dapat dilihat pada Tabel 1.

Tabel 1. Aset

No	Nama Aset	Jenis	Lokasi
1	Aplikasi EdLink	Perangkat lunak	PT. SVU
2	AWS Server	Perangkat keras	AWS
3	*Database* Server	Perangkat keras	AWS
4	Jaringan Server	Jaringan	PT. SVU

Sumber: Hasil Penelitian Diolah Kembali

4.2. Identifikasi Sumber Ancaman

Pada tahap ini peneliti melakukan identifikasi sumber ancaman yang ada pada EdLink, dengan menyebarkan kuesioner kepada Satu *Product Manager* EdLink dengan latar belakang pendidikan sarjana dan pengalaman Empat tahun menjadi *Product Manager*, Dua *Product Consultant* EdLink dengan latar belakang pendidikan sarjana dan pengalaman Dua tahun memberikan konsultasi terkait sistem pembelajaran *online*, dan Satu *System Engineer* EdLink dengan latar belakang pendidikan sarjana dan pengalaman Tiga tahun mengerjakan aplikasi pembelajaran *online*. Dari kuesioner yang sudah diisi ditemukan 32 sumber ancaman yang berkaitan dengan keempat aset yang dimiliki EdLink. Lalu dari sumber ancaman yang sudah diidentifikasi selanjutnya adalah menentukan rentang efek dari setiap sumber ancaman. Diketahui daru kuesioner yang sudah diberikan kepada responden terdapat 9 sumber ancaman dengan rentang efek *Very High* seperti yang tertera pada Tabel 2.

Tabel 2. Sumber Ancaman

No	Aset	Sumber ancaman	Rentang Efek
1	Aplikasi EdLink	Akses ke sistem dicuri menyebabkan data pribadi dapat diakses	*Very High*
2	Aplikasi EdLink	Terkena *malware* dan virus dari pihak dalam atau luar	*Very High*
3	Aplikasi EdLink	Celah sistem yang dimanfaatkan oleh pihak lain	*Very High*
4	Aplikasi EdLink	Data sensitif hilang	*Very High*
5	AWS Server	Konfigurasi Server yang tidak terstandarisasi keamanannya	*Very High*
6	AWS Server	*Password* dengan tingkat keamanan minimal	*Very High*
7	*Database* Server	Konfigurasi Server yang tidak terstandarisasi keamanannya	*Very High*
8	*Database* Server	Bencana alam menyebabkan server rusak	*Very High*
9	Jaringan Server	Konfigurasi Server yang tidak terstandarisasi keamanannya	*Very High*

Sumber: Hasil Penelitian Diolah Kembali

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

4.3. Identifikasi Peristiwa Ancaman

Pada tahap ini dilakukan identifikasi peristiwa ancaman yang didapatkan dari wawancara yang dilakukan kepada responden, untuk mengetahui apakah peristiwa ancaman yang ada masih relevan terhadap EdLink. Peneliti mengidentifikasi relevansi dari setiap peristiwa ancaman. Diketahui terdapat delapan peristiwa ancaman dengan status *confirmed* yang artinya adalah peristiwa ancaman tersebut pernah terjadi di EdLink dan diketahui oleh pengembang Edlink. Tiga peristiwa ancaman *expected* yang berarti peristiwa ancaman tersebut diketahui oleh tim pengembang EdLink namun belum pernah terjadi pada EdLink. Lima peristiwa ancaman *anticipated* yang artinya adalah kelima peristiwa ancaman tersebut pernah dilaporkan oleh sumber terpercaya dan belum pernah terjadi di EdLink. Enam peristiwa ancaman *predicted* yang artinya keenam peristiwa ancaman tersebut telah diprediksi oleh sumber yang terpercaya. Terakhir empat peristiwa ancaman *possible* yang berarti peristiwa ancaman telah dijelaskan oleh sumber yang tidak dapat dipercaya. Beberapa contoh identifikasi peristiwa ancaman dapat dilihat pada Tabel 3.

Tabel 3. Peristiwa Ancaman

No	Aset	Peristiwa Ancaman	Sumber ancaman	Relevansi
1	Aplikasi EdLink	Informasi penting dan konfigurasi ditangani dengan cara yang salah oleh personil	Sistem berhenti karena kesalahan operasional	*Confirmed*
2	Aplikasi EdLink	Upaya pengintaian atau pemindaian terhadap server	Akses ke sistem dicuri menyebabkan data pribadi dapat diakses	*Anticipated*
3	Aplikasi EdLink	Komunikasi yang tidak baik	Salah pengoperasian oleh staff pengguna	*Confirmed*
…				
30	Jaringan Server	Komunikasi yang tidak baik	Jaringan dari penyedia layanan internet bermasalah	*Confirmed*

Sumber: Hasil Penelitian Diolah Kembali

4.4. Identifikasi Kerentanan

Peneliti melakukan identifikasi kerentanan dari memberikan kuesioner kepada responden, untuk mengetahui sejauh mana kontrol yang telah dipersiapkan untuk melindungi aplikasi dari ancaman yang mungkin terjadi. Berdasarkan hasil penelitian terdapat 22 kerenanan. Serta diketahui satu tingkat *severity very high* untuk aset Aplikasi EdLink. Tiga rentang tingkat *severity high* diidentifikasi pada aset aplikasi EdLink dan *Database* Server. Hasil identifikasi dengan kerentanan tingkat *very high* dan *high* tertera pada Tabel 4.

Tabel 4. Kerentanan

No	Aset	Kerentanan	Tingkat keparahan
1	Aplikasi EdLink	Personil mengakses jaringan internal sistem menggunakan akses jaringan publik diluar kantor tanpa pengaman apapun menyebabkan sistem internal rentan terkena virus	*High*
2	Aplikasi EdLink	Menggunakan *password* standar menyebabkan sistem rentan terhadap pencurian *password*	*High*

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

3	Aplikasi EdLink	Jumlah pengguna melebihi kapasitas yang mampu dilayani server menyebabkan sistem rentan tidak dapat diakses	*Very High*
4	*Database* Server	Anti virus tidak terupdate secara berkala menyebabkan sistem rentan terhadap virus yang belum dikenali	*High*

Sumber: Hasil Penelitian diolah kembali

4.5. Identifikasi Kemungkinan

Peneliti melakukan identifikasi kemungkinan untuk mengetahui sejauh mana kecenderungan yang akan terjadi. Dari keusioner yang diisi oleh responden peneliti terlebih dahulu mengidentifikasi kemungkinan terjadinya peristiwa ancaman. Setelah itu peneliti mengidentifikasi tingkat kemungkinan peristiwa ancaman dan tingkat kemungkinan peristiwa ancaman dapat memberikan dampak buruk. Hasil kombinasi keduanya akan menghasilkan tingkat keseluruhan kemungkinan. Terdapat dua peristiwa ancaman tingkat keseluruhan kemungkinan *very high* yaitu upaya mengintai jaringan yang rentan akan celah,dan *database* tidak dapat diakses selanjutnya dua peristiwa ancaman dengan tingkat keseluruhan kemungkinan *high* yaitu upaya pengintaian atau pemindaian terhadap server dan konfigurasi yang tidak sesuai pada hak akses sistem. Hasil seluruh kemungkinan dengan status *very high* dan *high* tertera pada Tabel 5.

Tabel 5. Kemungkinan

No	Peristiwa Ancaman	Kemungkinan Terjadinya Peristiwa Ancaman	Kemungkinan Peristiwa Ancaman Memberikan Dampak Buruk	Tingkat Kemungkinan Seluruhnya
1	Upaya pengintaian atau pemindaian terhadap server	*High*	*Moderate*	*High*
2	Upaya mengintai jaringan yang rentan akan celah	*Moderate*	*Very High*	*Very High*
3	Konfigurasi yang tidak sesuai pada hak akses sistem	*High*	*Moderate*	*High*
4	*Database* tidak dapat diakses	*Very High*	*High*	*Very High*

Sumber: Hasil Penelitian diolah kembali

4.6. Analisa Dampak

Pada tahap ini peneliti memberikan kuesioner kepada responden dan meminta pendapat responden terkait rentang dampak maksimal yang bisa dihasilkan dari peristiwa ancaman. Hasil dari kuesioner menunjukan jika terdapat 11 peristiwa ancaman yang memiliki dampak. Dari 11 data tersebut enam diantaranya memiliki rentang dampak maksimal *Very High* yaitu: Upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data, Upaya mengintai jaringan yang rentan akan celah, Konfigurasi yang tidak sesuai pada hak akses sistem, *Database* tidak dapat diakses, Banjir, gempa bumi, kebakaran, angin puting beliung pada ruang utama, dan Pengungkapan informasi penting secara tidak sengaja. Seperti yang dijabarkan pada Tabel 6.

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

Tabel 6. Dampak Peristiwa Ancaman

No	Peristiwa Ancaman	Informasi Dampak	Rentang Maksimal Dampak
1	Upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data	Kendali penuh atas sistem hilang, dan data sensitif hilang	*Very High*
2	Upaya mengintai jaringan yang rentan akan celah	Kelemahan sistem dapat terbaca, sehingga sistem mudah untuk diserang oleh pihak lain	*Very High*
3	Konfigurasi yang tidak sesuai pada hak akses sistem	Sistem tidak bisa berjalan dengan semestinya dan bisa menyebabkan sistem terhenti	*Very High*
4	*Database* tidak dapat diakses	aplikasi berhenti berjalan dan tidak dapat digunakan	*Very High*
5	Banjir, gempa bumi, kebakaran, angin puting beliung pada ruang utama	kehilangan keseluruhan perangkat keras yang terdampak	*Very High*
6	Pengungkapan informasi penting secara tidak sengaja	Kepercayaan pengguna menurun dikarenakan memberikan informasi penting kepada pihak luar	*Very High*

Sumber: Hasil Penelitian Diolah Kembali

4.7. Penentuan Risiko

Pada tahap akhir ini dilakukan pengumpulan dari keseluruhan data yang sudah didapatkan. Maka peneliti menghasilkan informasi penentuan tingkat risiko berdasarkan sumber ancaman, keseluruhan kemungkinan, dan tingkatan dari dampak yang terjadi. Berdasarkan hasil penelitian diketahui 7 peristiwa ancaman yang akan menyebabkan risiko dengan tingkat *Very High* dan *High.* 3 risiko *very high* meliputi: konfigurasi server yang tidak terstandarisasi keamanannya menyebabkan *database* tidak dapat diakses, celah sistem yang dimanfaatkan oleh pihak lain menyebabkan adanya upaya mengintai jaringan yang rentan akan celah, dan *operating system* tidak berjalan dengan normal menyebabkan *database* tidak dapat diakses.

Empat risiko *high* meliputi akses ke sistem dicuri menyebabkan data pribadi dapat diakses, konfigurasi server yang tidak terstandarisasi keamanannya menyebabkan adanya upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data, *operating system* tidak berjalan dengan normal disebabkan oleh konfigurasi yang tidak sesuai pada hak akses sistem, dan upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data. Tabel 7 menunjukan hasil analisis risiko berdasarkan rentang efek, relevansi, kemungkinan keseluruhan, dan tingkat dampak dengan tingkat risiko *very high* dan *high*.

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

Tabel 7. Risiko

No	Peristiwa Ancaman	Sumber ancaman	Rentang Efek	Relevansi	Kemungkinan Keseluruhan	Tingkat Dampak	Risiko
1	Upaya pengintaian atau pemindaian terhadap server	Akses ke sistem dicuri menyebabkan data pribadi dapat diakses	*Very High*	*Anticipated*	*High*	*High*	*High*
2	*Database* tidak dapat diakses	Konfigurasi Server yang tidak terstandarisasi keamanannya	*Very High*	*Confirmed*	*Very High*	*Very High*	*Very High*
3	Upaya mengintai jaringan yang rentan akan celah	Celah sistem yang dimanfaatkan oleh pihak lain	*Very High*	*Anticipated*	*Very High*	*Very High*	*Very High*
4	Upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data	Konfigurasi Server yang tidak terstandarisasi keamanannya	*Very High*	*Expected*	*Moderate*	*Very High*	*High*
5	Konfigurasi yang tidak sesuai pada hak akses sistem	*Operating system* tidak berjalan dengan normal	*High*	*Anticipated*	*Moderate*	*Very High*	*High*
6	*Database* tidak dapat diakses	*Operating system* tidak berjalan dengan normal	*High*	*Confirmed*	*Very High*	*Very High*	*Very High*
7	Upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data	Terkena *malware* dan virus dari pihak dalam atau luar	*Very High*	*Expected*	*Moderate*	*Very High*	*High*

Sumber: Hasil Penelitian Diolah Kembali

Jurnal Teknologi dan Informasi (JATI)
Volume 11 Nomor 2 Edisi September 2021
P-ISSN 2088-2270, E-ISSN 2655-6839
DOI 10.34010/jati.v11i2

4.8. Penentuan Rekomendasi Kontrol

Pada tahap akhir ini peneliti akan memberikan rekomendasi kontrol peristiwa ancaman berdasarkan NIST SP 800-30 revisi 1. Peristiwa ancaman yang akan diberikan rekomendasi kontrol adalah peristiwa ancaman dengan tingkat risiko *Very High* dan *High.*

Pertama adalah konfigurasi server yang tidak terstandarisasi keamanannya menyebabkan *database* tidak dapat diakses dengan dampak pengguna tidak dapat mengakses aplikasi, aplikasi berhenti berjalan, dan operasional sistem terhenti. Tingkat risiko dari peristiwa ancaman ini yaitu *Very High.* Rekomendasi yang dapat diberikan peneliti terkait peristiwa ancaman ini untuk pengembang EdLink adalah membuat standar konfigurasi server, dengan mengacu kepada sertifikasi yang sudah disediakan oleh penyedia *cloud* server.

Kedua adalah celah sistem yang dimanfaatkan oleh pihak lain menyebabkan adanya upaya mengintai jaringan yang rentan akan celah. Dampak yang disebabkan oleh peristiwa ancaman ini adalah kelemahan sistem dapat terbaca, sehingga sistem mudah diserang oleh pihak yang tidak bertanggung jawab. Tingkat risiko dari peristiwa ini yaitu *Very High*. Rekomendasi yang bisa diberikan peneliti terkait peristiwa ancaman ini kepada pengembang EdLink adalah secara berkala melakukan update standar keamanan server, membuat standar pengamanan untuk celah-celah yang sering dimanfaatkan oleh *hacker*, seperti celah *injection,broken authentication,cross-site scripting,insecure direct object references, security misconfiguration, sensitive data exposure, missing function tingkat access control, cross-site request forgery, using known vulnerable component, unvalidated redirects and forward.*

Ketiga adalah *operating system* tidak berjalan dengan normal menyebabkan *database* tidak dapat diakses. Dampak dari peristiwa ancaman ini merupakan pengguna tidak dapat mengakses aplikasi, aplikasi berhenti berjalan, dan operasional sistem terhenti. Tingkat risiko dari peristiwa ancaman ini yaitu *Very High.* Rekomendasi yang bisa diberikan oleh peneliti terkait peristiwa ancaman ini untuk pengembang EdLink adalah membuat standar konfigurasi server, dengan mengacu kepada sertifikasi yang sudah disediakan oleh penyedia *cloud* server.

Keempat adalah upaya pengintaian atau pemindaian terhadap server yang menyebabkan akses ke sistem dicuri dan data pribadi dapat diakses. Dampak dari peristiwa ancaman ini merupakan data sensitif dapat digunakan oleh pihak yang tidak bertanggung jawab tanpa sepengetahuan tim EdLink. Tingkat risiko dari peristiwa ancaman ini yaitu *High.* Rekomendasi yang dapat diberikan peneliti terkait peristiwa ancaman ini adalah memberikan sosialisasi kepada pegawai terkait kerentanan sistem, dan tidak melakukan akses server utama menggunakan wifi umum agar terhindar dari infiltrasi *hacker*.

Kelima adalah konfigurasi server yang tidak terstandarisasi keamanannya menyebabkan adanya upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data sensitif. Dampak dari peristiwa ancaman ini merupakan kendali penuh atas sistem hilang, dan data sensitif dapat digunakan oleh pihak yang tidak bertanggung jawab. Tingkat risiko dari peristiwa ancaman ini yaitu *High.* Rekomendasi kontrol yang dapat diberikan oleh peneliti terkait peristiwa ancaman ini kepada pengembang EdLink adalah membuat standar konfigurasi server, dengan mengacu kepada sertifikasi yang sudah disediakan oleh penyedia *cloud* server.

Keenam adalah *operating system* tidak berjalan dengan normal yang disebabkan karena konfigurasi yang tidak sesuai pada hak akses sistem. Dampak dari peristiwa ancaman ini merupakan sistem tidak berjalan dengan semestinya dan rentan menyebabkan proses operasional terhenti. Tingkat risiko dari peristiwa ancaman ini yaitu *High.* Rekomendasi yang dapat diberikan peneliti terkait peristiwa ancaman ini yaitu membuat standar

konfigurasi server dengan mengacu kepada sertifikasi yang sudah disediakan oleh penyedia cloud server.

Ketujuh adalah upaya menginputkan *malware* dengan tujuan mengontrol keseluruhan sistem dan pengambilan data. Dampak dari peristiwa ancaman ini adalah kendali penuh atas sistem hilang, dan data sensitif dapat digunakan oleh pihak yang tidak bertanggung jawab. Tingkat risiko dari peristiwa ancaman ini yaitu *High.* Rekomendasi yang dapat diberikan oleh peneliti terkait peristiwa ancaman ini adalah menjalankan backup secara berkala, melakukan update sistem secara berkala, dan menggunakan *password* dengan tingkat keamanan tinggi.

5. Kesimpulan

Berdasarkan hasil penelitian dari empat aset yang dimiliki EdLink dapat diketahui terdapat tiga peristiwa ancaman dengan tingkat risiko *very high*, empat peristiwa ancaman dengan tingkat risiko *high*. Pada penelitian ini telah memberikan tujuh rekomendasi kontrol yang dapat digunakan oleh tim EdLink untuk meminimalisir peluang munculnya risiko yang dapat memberikan dampak *very high* maupun *high*. Saran dari peneliti untuk penelitian selanjutnya adalah dapat dilakukan analisis manajemen risiko dengan menggabungkan ISO 27005 untuk mengidentifikasi aset yang akan diteliti dan menggunakan NIST SP 800-30 revisi 1 untuk melakukan penilaian risiko, agar hasil dari penilaian risiko lebih komprehensif. Menggabungkan penilaian risiko NIST SP 800-30 revisi 1 dengan metode *Cost benefit analysis* (*CBA*) untuk menghitung nominal kerugian material/keuntungan dan manfaat dari penerapan rekomendasi kontrol risiko.

Daftar Pustaka

[1] Angraini and I. D. Pertiwi, "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan Iso 31000," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. Vol. 3, no. 2, pp. 70–76, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/RMSI/article/viewFile/4317/2652.

[2] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 : 2018 (Studi Kasus: Cv. Xy)," *Sebatik*, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.

[3] A. F. Rohman, A. Ambarwati, and E. Setiawan, "Analisis Manajemen Risiko IT Dan Keamanan Aset Menggunakan Metode OCTAVE-S," *J. Inf. Technol. Comput. Sci.*, vol. 3, no. 2, pp. 298–310, 2020, [Online]. Available: https://journal.ipm2kpe.or.id/index.php/INTECOM/article/view/1854.

[4] Y. Idah and R. Prima, "Analisis Manajemen Risiko Sistem Pembelajaran Online pada Perguruan Tinggi Menghadapi Pandemi COVID-19," *J. Rekayasa Inf.*, vol. 10, no. 1, pp. 50–56, 2021, [Online]. Available: https://ejournal.istn.ac.id/index.php/rekayasainformasi/article/view/833/682.

[5] R. D. A. Putra, A. Ambarwati, and E. Setiawan, "Evaluasi Manajemen Risiko Teknologi Informasi Berdasarkan Framework COBIT 5 Pada PT.BTM," *JSI J. Sist. Inf.*, vol. 11, no. 2, pp. 1754–1762, 2019, doi: 10.36706/jsi.v11i2.9103.

[6] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," in *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 2009, pp. 726–731, doi: 10.1109/ARES.2009.75.

[7] K. Harsanto and D. Hidayat, "Sistem Informasi Manajemen Risiko dengan Menggunakan Framework National Institute of Standards and Technology pada Lembaga Pendidikan," *J. Ipsikom*, vol. 6, no. 1, 2018, [Online]. Available:

https://ojs.ipem.ecampus.id/ojs_ipem/index.php/stmik-ipem/article/view/87.

[8] D. S. Valena, R. Prabowo, A. R. Irawati, and J. I. Komputer, "Analisis Manajemen Risiko Sistem Informasi Perpustakaan Universitas Lampung Menggunakan Metode NIST SP 80-30," *J. Komputasi*, vol. 7, no. 1, pp. 1–10, 2019, [Online]. Available: https://jurnal.fmipa.unila.ac.id/komputasi/article/view/2053.

[9] R. R. Putra *et al.*, "Analisis Manajemen Risiko TI Pada Keamanan Data E-Learning Dan Aset TI Menggunakan NIST SP," *J. Tek. Inform. dan Sist. Inf.*, vol. 6, no. 1, pp. 96–105, 2019, [Online]. Available: https://pdfs.semanticscholar.org/454f/332f8c22a1f1da3c2ea2a82537728d9a5f42.pdf.

[10] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," *J. Inform. Pengemb. IT*, vol. 02, no. 02, pp. 1–8, 2017, [Online]. Available: https://ejournal.poltektegal.ac.id/index.php/informatika/article/view/484/547.

[11] H. B. Seta and T. Rahayu, "Manajemen Risiko Aplikasi Pembelajaran Berbasis Online," *Semin. Nas. Teknol. Inf. dan Multimed. 2017*, vol. 5, no. 1, pp. 7–12, 2017, [Online]. Available: https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1815.