Jurnal Infosecure Vol.4 No.1, Maret 2023
p-ISSN: 2087-1023
MTI-UNLA

Penilaian Risiko Keamanan Sistem Informasi Aplikasi Eco-System Menggunakan ISO 27005 di Sekolah Bisnis XYZ

Rulli Wibowo[1], Arif Zulianto[2], Wiwin Suwarningsih[3], Awan Setiawan[4]

Prodi Teknik Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3,4]

[1]rulli.wibowo@gmail.com

[2]madzul@gmail.com

[3]winak03@gmail.com

[4]awans@gmail.com

Abstrak— Sekolah Bisnis XYZ adalah sekolah tinggi negeri sebagai salah satu lembaga pendidikan tinggi di Indonesia memiliki beberapa aplikasi yang dibangun untuk menunjang sistem pendidikan, sistem administrasi perkuliahan dan operasional penyelenggaraan perkuliahan. Eco-System adalah sistem informasi pendukung operasional yang digunakan untuk pengajuan pengadaan barang dan jasa di lingkungan Sekolah Bisnis XYZ. Sistem informasi ini memiliki fungsi yang sangat penting bagi kelangsungan proses bisnis. Pada tahun 2023 Eco-System mengalami insiden serangan siber *web defacement*. *Web defacement* yang dialami berupa berubahnya tampilan situs menjadi tampilan judi online. Serangan *web defacement* umumnya disebabkan oleh langkah-langkah keamanan yang buruk, kurangnya pembaruan sistem secara berkala, dan langkah-langkah pertahanan keamanan yang tidak memadai. Tujuan penelitian ini adalah memberikan rekomendasi kontrol keamanan untuk meningkatkan keamanan sistem informasi di Sekolah Bisnis XYZ berdasarkan penilaian risiko ISO/IEC 27005:2022 dan kontrol keamanan sesuai standar ISO/IEC 27002:2022. Dari hasil penelitian terdapat terdapat 2 risiko tinggi, 3 risiko sedang, dan 5 risiko rendah. Dari risiko yang berhasil ditemukan diberikan 5 rekomendasi kontrol sesuai stnadar ISO/IEC 27002:2022.

Kata kunci— Penilaian Risiko, ISO/IEC 27005, Rekomendasi Kontrol ISO/IEC 27002

I. PENDAHULUAN

Sekolah Bisnis XYZ sebagai salah satu lembaga pendidikan tinggi di Indonesia memiliki beberapa aplikasi yang dibangun untuk menunjang sistem pendidikan, sistem pendukung administrasi perkuliahan dan operasional. Eco-System adalah sistem informasi pendukung operasional yang digunakan untuk pengajuan pengadaan barang dan jasa di lingkungan Sekolah Bisnis XYZ. Sistem informasi ini memiliki fungsi yang sangat penting bagi kelangsungan proses bisnis di Sekolah Bisnis XYZ. Pada tahun 2023 Eco-System mengalami insiden serangan siber *web defacement*. *Web defacement* yang dialami Sekolah Bisnis XYZ berupa berubahnya tampilan situs menjadi tampilan judi online. *Defacement* pada situs web dapat diartikan tindakan mengubah tampilan halaman situs yang tidak semestinya oleh orang yang tidak memiliki otoritas [4]. Website *defacement* didefinisikan sebagai serangan keamanan cyber yang mengubah tampilan halaman web tertentu dengan cara mengeksploitasi kerentanannya. Serangan *defacement* website umumnya disebabkan oleh langkah-langkah keamanan yang buruk, kurangnya pembaruan sistem secara berkala, dan langkah-langkah pertahanan keamanan yang tidak memadai [3].

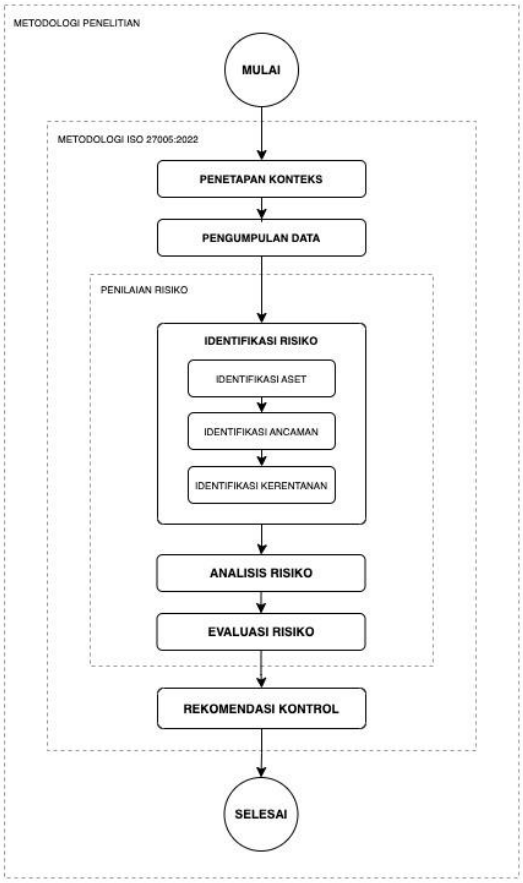
Dalam penelitian lain yang dilakukan untuk menilai risiko keamanan informasi, [5] menggunakan ISO/IEC 27005:2011 pada SIAK UMMI, tujuannya adalah agar dapat menentukan nilai aset, ancaman, kelemahan dan dampak yang mungkin terjadi sehingga dihasilkan daftar nilai risiko dari yang terendah ke yang tertinggi. Dafar risiko ini akan menjadi rekomendasi dalam penanganan risiko yang akan dilakukan oleh pengelolan SIAK UMMI. [6] memberikan rekomendasi dalam penelitiannya mencakup berbagai kontrol dan tindakan yang dapat diimplementasikan untuk mengurangi risiko keamanan informasi. Referensi rekomendasi yang diberikan berasal dari ISO/IEC 27002:2013, yang merupakan standar internasional untuk praktik manajemen keamanan informasi. Penelitian tersebut menjadi rujukan dalam melakukan penelitian penilaian risiko keamanan informasi menggunakan ISO 27005:2022 pada aplikasi Eco-System di Skolah Bisnis XYZ.

II. METODE

Tahapan penelitian yang dilakukan terdiri 6 tahap yaitu penetapan konteks, pengumpulan data, identifikasi risiko yang didalamnya terdapat identifikasi aset, identifikasi ancaman, dan identifikasi kerentanan. Kemudian tahap berikutnya adalah analisis risiko dan evaluasi risiko. Pada tahap terakhir diberikan rekomendasi kontrol dari standar ISO/IEC 27002:2022 yang sesuai dengan hasil evaluasi risiko. Tahapan penelitian dapat dilihat pada gambar 1.

Tahap pertama adalah penetapan konteks. Dalam penelitian ini penetapan konteks pada studi kasus aplikasi pengadaan barang dan jasa Eco-System yang akan dibahas adalah infrastruktur yang berkaitan dengan aplikasi Eco-System, yaitu berupa perangkat keras, perangkat lunak, informasi, dan data lainnya. Dalam penilaian risiko ditetapkan pula kriteria kemungkinan kejadian, kriteria dampak risiko, dan matriks penilaian risiko.

Tahap kedua adalah pengumpulan data. Pada penelitian ini karakteristik pendekatan yang digunakan adalah pendekatan secara kualitatif dan pengolahan data secara observasi dan wawancara. Penelitian yang dilakukan penulis menggunakan metode deskriptif kualitatif dari ISO/IEC 27005:2022. Data yang diperoleh berasal dari wawancara, observasi dan dari penelitian sebelumnya. Penelitian ini dilakukan dengan mengamati dan observasi secara langsung untuk mendapatkan dan menetukan aset dan batasan data yang akan diteliti.



Gambar. 1 Tahapan Penelitian

Tahap ketiga adalah identifikasi risiko. Identifikasi risiko adalah proses sistematis untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko-risiko yang terkait dengan keamanan informasi dalam suatu organisasi [1]. Dalam penilaian risiko terdiri dari tahapan Identifikasi Risiko, Analisis Risiko, dan Evaluasi Risiko. Sedangkan pada tahapan Identifikasi Risiko terdiri dari Identifikasi Aset, Identifikasi Ancaman, dan Identifikasi Kerentanan

Setelah risiko-risiko diidentifikasi, tahap keempat adalah menganalisis risiko-risiko tersebut. Analisis risiko melibatkan pemahaman mendalam tentang jenis risiko, penyebabnya, kemungkinan terjadinya, dan dampaknya terhadap organisasi. ISO 27005 menekankan pentingnya menilai konsekuensi potensial dari risiko dan kemungkinan terjadinya. Dilakukan penetapkan prioritas risiko berdasarkan tingkat keparahan dan kemungkinan terjadinya. Hal ini memungkinkan organisasi untuk fokus pada risiko-risiko yang memiliki dampak terbesar dan memerlukan tindakan perlakuan risiko yang lebih mendesak.

Tahap kelima adalah evaluasi risiko. Tahap evaluasi risiko dilakukan untuk membandingkan hasil analisis risiko dengan kriteria risiko yang telah ditetapkan. Tujuannya adalah untuk menentukan apakah risiko tersebut dapat diterima atau tidak, serta untuk memprioritaskan risiko-risiko yang perlu ditangani lebih lanjut. Evaluasi risiko juga melibatkan penentuan tingkat risiko yang dihasilkan dari kombinasi konsekuensi dan kemungkinan terjadinya.

Tahap keenam adalah rekomendasi kontrol. Setelah melakukan evaluasi risiko, akan diperoleh prioritas risiko dari risiko yang mempunyai nilai tertinggi hingga yang terendah. Risiko tinggi dan sedang diberikan rekomendasi untuk perbaikan sesuai dengan standar ISO 27002:2022.

III. HASIL DAN PEMBAHASAN

A. Identifikasi Risiko

Pada identifikasi risiko meliputi identifikasi aset, identifikasi kerentanan, dan identifikasi ancaman.

A.1. Identifikasi Aset

Eco-System memiliki aset yang dapat dikategorikan dalam perangkat lunak, perangkat keras, jaringan, dan sumber daya manusia. Adapun daftar aset disajikan pada Tabel I.

TABEL I
DAFTAR ASET

Nama Aset	Kategori	Detail Aset
Aplikasi Eco-System	Perangkat Lunak	PHP Versi 5.6
Basis Data MySQL	Perangkat Lunak	MySQL Versi 8.1
Server	Perangkat Keras	Dell Poweredge T40 Spesifikasi: Processor Intel® Xeon® E-2224G, Memori RAM 16, Power Supply 300 Watt
	Perangkat Lunak	Operating System: Ubuntu Server 20.04
	Perangkat Lunak	Web Server: Nginx versi 1.18
Koneksi internet	Network	Provider: Linknet & Bnet
Router	Network	Microtik
Pengembang web, pengelola aplikasi, dan pengguna.	Sumber Daya Manusia	- Web developer: 1 orang tenaga alih daya. - Admin pengelola: 1 orang staf tetap.

A.2. Identifikasi Ancaman

Tahap selanjutnya adalah mengidentitifikasi ancaman. Dengan mengidentifikasi ancaman-ancaman potensial ini, organisasi dapat mengidentifikasi area-area yang rentan dan mengambil langkah-langkah untuk mengurangi risiko serta meningkatkan keamanan informasi mereka. Hasil dari identifikasi ancaman pada layanan Eco-System disajikan pada Tabel II.

TABEL II
DAFTAR ANCAMAN

Sumber Ancaman	Ancaman
Peretas	Serangan *Distributed Denial of Service* (DDoS)
	Serangan *Malware*
	Serangan *Brute Force*
	Serangan *SQL Injection*
	Serangan *Cross-Site Scripting (XSS)*
	Serangan *Defacement*
	Akses aplikasi/data oleh orang yang tidak berhak
Faktor Teknis dan Lingkungan	Gangguan listrik
	Gangguan hubungan internet
	Kerusakan perangkat keras
	Kerusakan perangkat lunak
	Kesalahan konfigurasi alat / perangkat lunak
Orang dalam lingkungan organisasi	Memberikan akses login kepada orang yang tidak berhak

A.3. Identifikasi Kerentanan

Hasil identifikasi kerentanan yang terdapat di Sekolah Bisnis XYZ dapat dilihat pada tabel III. Dengan mengidentifikasi kerentanan-kerentanan ini organisasi dapat memahami di mana titik-titik lemah dalam sistem mereka dan mengambil langkah-langkah untuk mengurangi kerentanan tersebut serta meningkatkan keamanan informasi.

TABEL III
DAFTAR KERENTANAN

Aset	Kerentanan
Aplikasi Eco-System	Framework PHP yang digunakan versi 5.5, dimana PHP versi 5 tidak lagi mendapatkan dukungan update keamanan sejak 31 Desember 2018. Terdapat beberapa kerentanan pada PHP (Sumber: https://www.cvedetails.com/vendor/74/PHP.html) - *Buffer Overflow* - *Memory Corruption* - *Input Validation*
	Tidak tersedianya dokumentasi teknis aplikasi Eco-System.
	Tidak adanya pemantauan aplikasi secara rutin.
Database MySql	Terdapat beberapa kerentanan pada MySql Oracle (Sumber: https://www.cvedetails.com/vendor/93/Oracle.html) Ancaman tertinggi pada serangan *Denial of Service*.
Server	Tidak ada pencadangan sumber listrik baterai
	Terdapat kerentanan *Memory Corruption* pada Operating System Ubuntu sehingga rentan terhadap serangan *Denial of Service* (Sumber: https://www.cvedetails.com/version/579251/Canonical-Ubuntu-Linux-20.04.html)
Pengembang web, pengelola aplikasi, dan pengguna.	Tidak adanya prosedur pendaftaran dan penghapusan akun pengguna aplikasi.
	Personel pengembang aplikasi yang baru tidak menguasai alur code program aplikasi.
	Kurangnya kesadaran akan risiko keamanan informasi.
	Terbatasnya jumlah staf admin pengelola aplikasi (1orang). Jika staf pindah atau keluar kerja, staf baru membutuhkan waktu lagi untuk mempelajari teknis kode aplikasi.

B. Analisis Risiko

Hasil dari analisis risiko akan digunakan untuk menentukan penanganan risiko. Risiko-risiko yang diidentifikasi kemudian dianalisis untuk mengevaluasi kemungkinan terjadinya risiko dan dampak yang ditimbulkan jika risiko tersebut terjadi. Analisis risiko membantu dalam memahami tingkat risiko yang dihadapi oleh organisasi.

TABEL IV
HASIL PENILAIAN RISIKO

Aset	Kode Risiko	Ancaman	Tingkat Risiko
Aplikasi Eco-System	R1	Serangan *Web Defacement*	Tinggi
	R2	Waktu perbaikan aplikasi yang lama	Tinggi
	R3	Akses aplikasi oleh orang yang tidak berhak	Rendah
Basis Data MySQL	R4	Kerusakan Perangkat Lunak	Rendah
	R5	Akses data oleh pihak yang tidak berhak	Sedang
	R6	Serangan *Denial of Service* (DoS)	Rendah
	R7	Serangan *SQL Injection*	Rendah
Server	R8	Serangan *Denial of Service* (DoS)	Sedang
	R9	Gangguan listrik	Rendah
	R10	Kerusakan perangkat keras	Sedang

Dari hasil penilaian risiko terlihat 2 risiko dengan kategori Tinggi, 3 risiko dengan kategori Sedang, dan 5 risiko dengan kategori Rendah. Penilaian risiko tinggi ada pada ancaman serangan *web defacement* dan pada ancaman lamanya waktu perbaikan aplikasi Eco-System. Kerentanan pada versi framework PHP yang digunakan adalah versi yang sudah tidak mendapatkan dukungan pembaruan keamanan merupakan salah satu penyebab tingkat risiko pada aplikasi Eco-System menjadi tinggi. Kerentanan lainya yang menyebabkan waktu perbaikan aplikasi yang lama adalah tidak tersedianya dokumentasi teknis dari aplikasi Eco-System sehingga staf admin memerlukan waktu yang lama untuk melakukan penelusuran kode dan fungsi-fungsi pada aplikasi Eco-System.

Tahap berikutnya adalah melakukan pemetaan risiko berdasarkan level risiko dengan menggunakan matriks penilaian risiko. Matriks tersebut membantu dalam menganalisis risiko dengan menggambarkan hubungan antara kemungkinan terjadinya risiko (yaitu seberapa sering risiko terjadi) dan dampaknya (yaitu seberapa besar konsekuensi dari terjadinya risiko tersebut). Ini memungkinkan manajer risiko untuk fokus pada risiko-risiko yang memiliki dampak signifikan atau kemungkinan terjadinya tinggi. Matriks hasil pemetaan risiko dapat dilihat pada tabel V.

TABEL V
MATRIKS HASIL PEMETAAN RISIKO

Tingkat Kemungkinan		Tingkat Dampak				
		1	2	3	4	5
		Tidak Signifikan	Rendah	Sedang	Tinggi	Sangat Tinggi
	Sangat Tinggi (5)					
	Tinggi (4)					
	Sedang (3)		R8	R10	R1, R2	
	Rendah (2)	R9	R3	R5		
	Sangat Rendah (1)	R6	R7	R4		

C. Rekomendasi Kontrol

Dari hasil penilaian risiko terlihat 2 risiko dengan kategori Tinggi, 3 risiko dengan kategori Sedang, dan 5 risiko dengan kategori Rendah. Selanjutnya diberikan rekomendasi kontrol sesuai ISO 27002:2022 pada risiko yang sudah ditentukan. Rekomendasi yang diberikan fokus pada ancaman dengan tingkat risiko yang tinggi dan sedang. Pada tabel VI dapat dilihat rekomendasi kontrol dari ISO 27002.

TABEL VI
REKOMENDASI KONTROL

No.	Risiko	Rekomendasi Kontrol ISO 27002
1	Serangan Web Defacement	8.5 *Secure authentication* 8.25 *Secure development life cycle* 8.26 Persyaratan keamanan aplikasi 8.28 Pengkodean yang aman 8.29 Pengujian keamanan dalam pengembangan dan penerimaan
2	Waktu perbaikan aplikasi yang lama	5.26 Respons terhadap insiden keamanan informasi
3	Kerusakan Perangkat Keras	7.8 Penempatan dan perlindungan peralatan
4	Serangan *Denial of Service* (DoS)	8.16 Pemantauan Kegiatan
5	Akses data oleh pihak yang tidak berhak	5.15 Akses kontrol

IV. SIMPULAN

Dengan menggunakan ISO/IEC 27005:2022 untuk menjalankan penilaian risiko keamanan informasi pada aplikasi Eco-System di Sekolah Bisnis XYZ, kami menemukan ada 10 risiko yang harus ditangani. Berdasarkan penanganan risiko yang kami ajukan, dihasilkan peta penanganan risiko dengan penanganan risiko dan rekomendasi kontrol sesuai ISO/IEC 27002:2022. Kami berharap hasil evaluasi risiko dan rekomendasi kontrol bisa digunakan sebagai masukan dalam perancangan SOP pengoperasian aplikasi Eco-System sehingga proses bisnis di Sekolah Bisnis XYZ tidak terganggu.

REFERENSI

[1] International Standard ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO EIC.
[2] International Standard ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information Security Control. ISO EIC.
[3] Albalawi, Mariam. (2022). Website Defacement Detection and Monitoring Methods: A Review. Electronics 2022, 11, 3573.
[4] Romagna, M., & Hout, N. J. Van Den. (2017). Hacktivism and website defacement : Motivations, capabilities and potential threats. 27th Virus Bulletin International Conference, (October).
[5] Asriyanik & Prajoko. (2018). Penilaian Risiko Keamanan Informasi pada Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi menggunakan ISO 27005:2011.
[6] Syahindra, I P. S., Primasari, C.H. & Irianto, A.B.P. (2022). Evaluasi Risiko Keamanan Informasi DISKOMINFO Provinsi XYZ menggunakan Indeks KAMI dan ISO 27005 : 2011. JURNAL TEKNOINFO Volume 16, Nomor 2, Juli 2022, Page 165-182.
[7] Whitman, M.E. & Mattord, H.J. (2014). Management of Information Security (4th edition). Boston: Couse Technology
[8] R. Sarno & I. Iffano (2009). Sistem Manajemen Keamanan Informasi Berbasis ISO 27001, Surabaya: ITSPress, 2009.