JUSIFO JURNAL SISTEM INFORMASI

p-ISSN: 2460-092X, e-ISSN: 2623-1662
Vol. 7, No. 1, Juni 2021
Hal. 10 - 20

Penilaian Risiko Keamanan Informasi Menggunakan *Octave Allegro*: Studi Kasus pada Perguruan Tinggi

Prihatini Ramjanati*, Freddy Kurnia Wijaya, Muhamad Son Muarie
ramjanatip@gmail.com*
*Penulis korespondensi

Universitas Islam Negeri Raden Fatah Palembang - Indonesia

Diterima: 30 Mei 2020 | Direvisi: 08 Juni - 04 Sept 2020
Disetujui: 28 Juni 2021 | Dipublikasi: 30 Juni 2021
Program Studi Sistem Informasi, Fakultas Sains dan Teknologi,
Universitas Islam Negeri Raden Fatah Palembang, Indonesia

ABSTRACT

Currently the need for the use of information systems has become important for institution and organizations. The use of information systems has also expanded to various fields, namely educational institutions. However, on the other hand information can be an important security gap. The important information that falls to other parties can result in loss to the owner of the information. This study aims to conduct an internal assessment of information security risks from the use of information systems, so that it can be seen what risks are very high and need to be mitigated. In this study, the Octave Allegro framework was used to conduct an internal assessment. The steps taken in conducting an information security risk assessment consist of 8 steps. Each step produces an output that is used as the basis for evaluating the next step. There are 2 areas that need attention and become the focus of improvement. Information security risk management needs to be carried out and monitored closely and regularly against risks that are determined to be important and have a high risk probability.
Keywords: *Risk assessment, Octave Allegro, College*

ABSTRAK

Saat ini kebutuhan akan penggunaan sistem informasi sudah menjadi hal yang penting bagi instansi dan organisasi. Penggunaan sistem informasi juga telah meluas ke berbagai bidang, salah satunya adalah instansi pendidikan. Namun, di sisi lain informasi yang dihasilkan dapat menjadi celah keamanan yang penting untuk dijaga. Informasi penting yang jatuh ke pihak lain dapat mengakibatkan kerugian bagi pemilik informasi. Penelitian ini bertujuan melakukan penilaian secara internal risiko keamanan informasi dari penggunaan sistem informasi, sehingga dapat diketahui risiko apa yang sangat tinggi dan perlu untuk dilakukan mitigasi. Di dalam penelitian ini digunakan kerangka kerja Octave Allegro untuk melakukan penilaian secara internal. Langkah-langkah yang dilakukan dalam melakukan penilaian risiko keamanan informasi terdiri dari 8 (delapan) langkah. Masing-masing langkah menghasilkan keluaran yang digunakan sebagai dasar penilaian langkah setelahnya. Terdapat 2 (dua) area yang perlu diperhatikan dan menjadi fokus perbaikan. Manajemen risiko keamanan informasi perlu dilakukan dan dipantau secara ketat dan rutin terhadap risiko yang ditentukan penting dan memiliki probabilitas risiko yang tinggi.
Kata Kunci: *Penilaian risiko, Octave Allegro, Perguruan tinggi*

PENDAHULUAN

Saat ini kebutuhan akan penggunaan sistem informasi sudah menjadi hal yang penting bagi instansi dan organisasi. Dengan adanya sistem informasi, dapat digunakan untuk mendukung strategi bisnis, memperbaiki kualitas layanan, dan proses bisnis

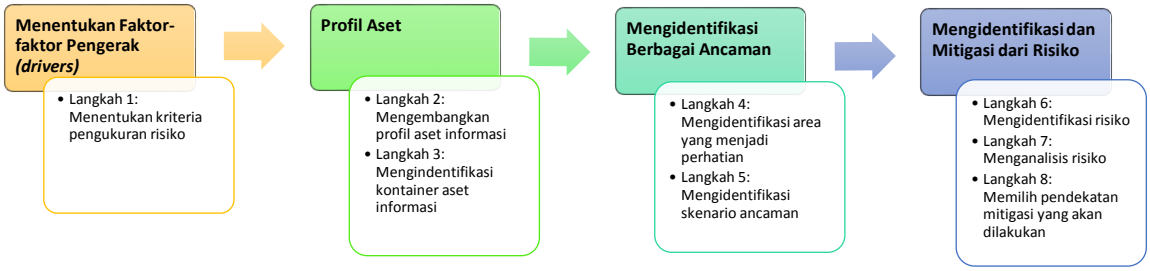
(Suroso & Fakhrozi, 2018). Penggunaan sistem informasi juga telah meluas ke berbagai bidang, salah satunya adalah instansi pendidikan. Namun, di sisi lain informasi yang dihasilkan dapat menjadi celah keamanan yang penting untuk dijaga. Informasi penting yang jatuh ke pihak lain dapat mengakibatkan kerugian bagi pemilik informasi (Rahardjo, 2005). Dalam upaya untuk mengendalikan dan mengurangi kerugian yang terjadi, dibutuhkan manajemen risiko terhadap keamanan informasi yang telah dihasilkan. Sasaran utama dari penerapan manajemen risiko yaitu dapat melindungi instansi terkait dari kerugian besar yang mungkin akan muncul dan juga dapat membantu dalam menghadapi berbagai keadaan merugikan yang tidak dapat diprediksi sebelumnya (Arifudin et al., 2020).

Perguruan Tinggi X sudah menerapkan manajemen risiko di dalam penggunaan sistem informasi untuk mendukung layanan yang mereka berikan. Layanan yang sudah tersedia dengan memanfaatkan penggunaan sistem informasi, antara lain: Sistem Informasi Akademik yang digunakan untuk layanan mahasiswa, Sistem Informasi Keuangan yang memudahkan proses pengelolaan data keuangan perguruan tinggi, Sistem Informasi *Tracer* Alumni untuk memudahkan dalam menelusuri alumni. Berdasarkan wawancara yang telah dilakukan bahwa pernah terjadi beberapa kerugian seperti cacat pada perangkat lunak *(software defect)*, kerusakan sistem. Selain itu, belum pernah dilakukan penilaian terhadap risiko keamanan informasi yang dihasilkan. Oleh karena itu, pada penelitian ini perlu untuk mengkaji sejauh mana risiko keamanan yang mungkin terjadi. Di dalam penelitian ini digunakan kerangka kerja *Octave Allegro* untuk melakukan penilaian risiko keamanan informasi dari penggunaan sistem informasi di perguruan tinggi X. Beberapa penelitian yang pernah dilakukan terkait penggunaan kerangka kerja *Octave Allegro*, antara lain: (Hamzah et al., 2020; Idris et al., 2020; Matondang et al., 2018; Rachmaniah & Mustafa, 2015; Ramadhintia & Bisma, 2021; Rijayanti, 2018; Sanjaya, 2020; Saputra et al., 2019; Seta et al., 2017; Tobing & Puspa, 2015; Zulfia et al., 2021)

Tujuan dari penelitian ini adalah melakukan penilaian secara internal risiko keamanan informasi dari penggunaan sistem informasi, sehingga dapat diketahui risiko apa yang sangat tinggi dan perlu untuk dilakukan mitigasi.

METODOLOGI PENELITIAN

Di dalam penelitian ini untuk melakukan penilaian secara internal risiko keamanan informasi digunakan 8 (delapan) langkah yang terdapat pada (Caralli et al., 2007), secara ringkas dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Dari langkah-langkah yang dilakukan dapat dijelaskan sebagai berikut:

Langkah 1: Menentukan kriteria pengukuran risiko

Terdapat 2 aktivitas yang dilakukan. Pada aktivitas ke 1, menentukan sekumpulan penilaian kualitatif (kriteria pengukuran risiko) yang dapat digunakan untuk

mengevaluasi dampak risiko terhadap misi dan tujuan organisasi. Setidaknya, pertimbangkan area dampak seperti: reputasi/kepercayaan pengguna, keuangan, produktivitas, kesehatan dan keamanan, denda/sanksi hukum, area dampak lainnya yang ditentukan pengguna. Pada aktivitas ke 2, prioritaskan area dampak mulai dari yang paling penting hingga yang tidak begitu penting menggunakan *Impact Area Ranking Worksheet*.

Langkah 2: Mengembangkan profil aset informasi

Terdapat 8 aktivitas yang dilakukan. Pada aktivitas ke 1, mengidentifikasi sekumpulan aset informasi yang dapat dilakukan penilaian. Penilaian tersebut menyajikan yang paling bermanfaat yang fokus pada aset informasi yang paling penting bagi organisasi (aset yang paling bernilai bagi organisasi, aset yang digunakan sehari-hari, pertimbangan jika aset tersebut hilang berdampak bagi organisasi, aset lainnya yang sangat berhubungan dengan aset tersebut). Pada aktivitas ke 2, berfokus pada beberapa hal yang paling penting. Hal ini sesuai dengan daftar yang dibuat pada aktivitas ke 1, beberapa pertimbangan yang lebih mendalam seperti, jika: aset diketahui orang yang tidak berwenang, aset dimodifikasi tanpa otorisasi yang sah, aset hilang/hancur, akses ke aset atau aset diretas oleh orang lain. Pada aktivitas ke 3, memasukkan dan mengumpulkan informasi mengenai aset informasi menggunakan *Critical Information Asset Profile*. Pada aktivitas ke 4, berdasarkan informasi yang telah dimasukkan ke dalam *Critical Information Asset Profile* dengan mempertimbangkan mengapa aset ini penting bagi organisasi, apakah aset informasi tersebut tunduk pada persyaratan peraturan? (kolom 2). Pada aktivitas ke 5, tambahkan deskripsi pada aset informasi tersebut (kolom 3). Pada aktivitas 6, identifikasi penanggungjawab aset informasi tersebut (kolom 4). Pada aktivitas ke 7, tambahkan persyaratan keamanan dalam mengakses aset informasi tersebut yang berkaitan dengan kerahasiaan, integritas, ketersediaan (kolom 5). Pada aktivitas ke 8, identifikasi persyaratan keamanan yang paling penting untuk mengakses aset informasi (kolom 6).

Langkah 3: Mengindentifikasi kontainer aset informasi

Kata "kontainer" mengarahkan pada dimana aset informasi tersebut disimpan, ditransfer, dan diproses. Terdapat 1 aktivitas yang dilakukan, mengidentifikasi dan mendokumentasikan kontainer (tempat penampung) dimana aset informasi tersebut disimpan, ditransfer, dan diproses.

Langkah 4: Mengidentifikasi area yang menjadi perhatian

Terdapat 1 aktivitas yang dilakukan, dalam hal ini memasukkan pernyataan deskriptif yang merincikan kondisi sebenarnya atau situasi yang berdampak/merusak aset informasi di organisasi.

Langkah 5: Mengidentifikasi skenario ancaman

Terdapat 3 aktivitas yang dilakukan. Pada aktivitas ke 1, mengidentifikasi skenario ancaman tambahan yang belum disebutkan pada area yang menjadi perhatian. Pada aktivitas ke 2, melengkapi *Information Asset Risk Worksheets* yang telah diidentifikasi pada kuesioner. Pada aktivitas ke 3, aktivitas ini bersifat opsional yaitu menambahkan pada *Information Asset Risk Worksheets* kemungkinan yang mungkin saja terjadi.

Langkah 6: Mengidentifikasi risiko

Terdapat 1 aktivitas yang dilakukan, menentukan bagaimana skenario ancaman yang telah dicatat pada *Information Asset Risk Worksheets* berdampak pada organisasi.

Langkah 7: Menganalisis risiko

Terdapat 2 aktivitas yang dilakukan. Pada aktivitas ke 1, menentukan dampak dari setiap risiko (tinggi, menengah, rendah). Pada aktivitas ke 2, melakukan perhitungan

terhadap penilaian risiko relatif kemudian catat hasilnya (tinggi = 3, menengah = 2, rendah = 1).

Langkah 8: Memilih pendekatan mitigasi yang akan dilakukan

Terdapat 3 aktivitas yang dilakukan. Pada aktivitas ke 1, mengelompokkan setiap risiko yang telah diidentifikasi berdasarkan skor risikonya (sesuai matriks risiko relatif). Pada aktivitas ke 2, tetapkan pendekatan mitigasi untuk setiap risiko yang ada (mitigasi, menunda, menerima). Pada aktivitas ke 3, seluruh risiko yang telah ditentukan untuk dilakukan mitigasi, maka diharuskan untuk mengembangkan strategi mitigasinya.

HASIL DAN PEMBAHASAN

Langkah 1: Menentukan kriteria pengukuran risiko

Pada aktivitas ke 1, didefinisikan area dampak serta ukuran kualitatifnya dengan menentukan bagaimana kualitasnya di masing-masing area dampak sesuai risikonya (rendah-menengah-tinggi). Area dampak yang ditentukan kualitasnya yaitu: reputasi/kepercayaan pengguna, keuangan, produktivitas, kesehatan dan keamanan, denda/sanksi hukum. Masing-masing kriteria pengukuran risiko ditentukan pada aktivitas ke 1 ini, sebagai contoh untuk area reputasi dan kepercayaan pengguna dapat dilihat pada Tabel 1.

Tabel 1. Kriteria Pengukuran Risiko Reputasi dan Kepercayaan Pengguna

Area Dampak	Rendah	Menengah	Tinggi
Reputasi	Reputasi tidak banyak terpengaruh jika terjadi gangguan sistem informasi kurang dari 1 hari.	Reputasi sedikit terpengaruh jika terjadi gangguan sistem informasi antara 1 sampai 3 hari.	Reputasi sangat terpengaruh jika terjadi gangguan sistem informasi lebih dari 3 hari.
Kepercayaan pengguna (*stakeholder*, mahasiswa, staff, dosen)	Hanya sebagian kecil pengguna yang terganggu.	Sebagian pengguna merasa terganggu.	Banyak pengguna yang merasa tidak nyaman terhadap layanan.
…	…	…	…

Selanjutnya pada aktivitas ke 2, seluruh area dampak yang telah ditentukan pada aktivitas ke 1 dikumpulkan dan dicatat. Jumlah area dampak pada penelitian ini adalah 5 (lima) area dampak. Selanjutnya, prioritas yang paling penting akan diberi nilai 5 (lima) dan seterusnya hingga urutan terendah. Penentuan prioritas area dampak ini nantinya akan digunakan untuk membuat skor risiko relatif, dapat dilihat pada Tabel 2.

Tabel 2. Penentuan Prioritas Area Dampak

Prioritas	Area Dampak
5	Reputasi dan kepercayaan pengguna
4	Produktifitas
3	Keuangan
2	Keamanan dan kesehatan
1	Denda dan hukum

Langkah 2: Mengembangkan profil aset informasi

Pada langkah ini akan berfokus untuk mengidentifikasi sekumpulan aset informasi yang akan dilakukan penilaian secara internal. Hal ini akan membantu dalam mengidentifikasi semua poin dimana aset informasi mungkin rentan terhadap akses terbuka oleh orang yang tidak sah, modifikasi, kehilangan/kerusakan, ataupun gangguan. Secara lengkap dapat dilihat pada Tabel 3.

Tabel 3. Profil Aset Informasi Kritis

Profil Aset Informasi Kritis		
(1) Aset kritis Aset informasi apa yang paling penting (kritis)?	**(2) Alasan pemilihan** Mengapa aset informasi tersebut penting bagi organisasi?	**(3) Deskripsi** Jelaskan dekripsi yang telah disepakati dari aset informasi tersebut?
Aset informasi akademik.	Hilangnya aset informasi ini akan berdampak sangat buruk. Penyalahgunaan aset informasi ini dapat mengganggu kelancaran administrasi akademik di perguruan tinggi.	Aset informasi terdapat beberapa data penting, yaitu: data mahasiswa yang terdiri dari data personal mahasiswa, KRS, KHS, jadwal perkuliahan, data nilai perkuliahan dari dosen.
(4) Pemilik aset informasi Siapa pemilik aset informasi?		
Yayasan, Staff TI, Dosen, Mahasiswa.		
(5) Persyaratan keamanan Apa persyaratan keamanan yang dibutuhkan untuk aset informasi ini?		
Kerahasiaan	Data penilaian mahasiswa perkelas hanya dapat diakses oleh dosen yang bersangkutan; Mahasiswa dapat mengakses prestasi milik mereka sesuai dengan hak akses mereka masing-masing.	
Integritas	Setiap dosen hanya dapat mengubah penilaian mahasiswa sesuai dengan kelasnya dan penilaian tidak bisa diubah lagi ketika sudah dikunci secara sistem; Mahasiswa tidak dapat mengubah nilai yang telah diterimanya	
Ketersediaan	Seluruh akses ke sistem informasi tersedia 24 jam selama 7 hari/minggu.	
(6) Persyaratan keamanan yang paling penting Persyaratan keamanan apa yang paling penting dari aset informasi tersebut?		
Terkait dengan **Integritas**		

Langkah 3 - Mengindentifikasi kontainer aset informasi

Pada langkah ini berfokus pada tempat penampungan dari aset informasi. Selain itu juga dijelaskan pihak internal dan pihak eksternal yang terlibat terhadap aset informasi. Selanjutnya, dilibatkan juga pembahasannya dari aspek teknis, aspek fisik, dan pengguna. Secara lengkap dapat dilihat pada Tabel 4, Tabel 5, dan Tabel 6.

Tabel 4. Peta Lingkup Risiko Aset Informasi (Teknis)

Internal	
Deskripsi Tempat Penampung	**Pemilik**
Database yang digunakan sebagai tempat penyimpanan sistem informasi yang digunakan. Sistem operasi yang digunakan *(Windows Server 2012).*	Yayasan, Staff IT
Eksternal	
Deskripsi Tempat Penampung	**Pemilik**
Infrastruktur jaringan *internet* yang digunakan di lingkungan perguruan tinggi	pihak ketiga (Telkom, *My Republic*)

Tabel 5. Peta Lingkup Risiko Aset Informasi (Fisik)

Internal	
Deskripsi Tempat Penampung	**Pemilik**
Harddisk Eksternal yang digunakan sebagai *backup* data mahasiswa.	Staff IT
Folder file yang digunakan sebagai penyimpanan berkas mahasiswa, dosen, dan keuangan	Bagian Keuangan
Eksternal	
Tidak ada	

Tabel 6. Peta Lingkup Risiko Aset Informasi (Pengguna)

Personil Internal	
Deskripsi Peran dan Tanggungjawab	**Departemen/Unit**
Administrator TI yang menjaga dan memelihara sistem informasi di lingkungan perguruan tinggi	Pusat Teknologi dan Data
Dosen sebagai pengajar di lingkungan perguruan tinggi.	Masing-masing Fakultas
Kepala bagian keuangan yang memahami pengelolaan keuangan perguruan tinggi	Bagian Keuangan
Personil Eksternal	
Tidak ada	

Langkah 4: Mengidentifikasi area yang menjadi perhatian

Pada langkah ini akan ditentukan pernyataan deskriptif yang menjelaskan kondisi atau situasi yang dapat mempengaruhi aset informasi. Penentuan area yang menjadi perhatian ini penting dikarenakan langkah ini berguna untuk memberikan pertimbangan atas kemungkinan skenario ancaman, dapat dilihat pada Tabel 7.

Tabel 7. *Area of Concern*

No.	***Area of Concern***
1.	Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi.
2.	Bocornya hak akses seperti *username* dan *password*.
3.	Ruangan *server* yang mudah diakses dapat mengakibatkan pihak yang tidak berwenang merusak *server*.
4.	Penyalahgunaan *harddisk* eksternal dan file folder *backup* data oleh pihak yang tidak bertanggung jawab.

Langkah 5: Mengidentifikasi skenario ancaman

Langkah ini memperjelas ancaman dengan mengidentifikasi skenario dengan memberikan gambaran secara rinci mengenai properti dari ancaman, antara lain *actor, means, motives, outcome* dan *securtiy* area-area yang telah diidentifikasi pada langkah sebelumnya diperluas menjadi skenario ancaman yang lebih jauh mendetailkan properti dari sebuah ancaman. Sebagai contoh akan disampaikan 1 (satu) contoh area yang menjadi perhatian *(area of concern)* dapat dilihat pada Tabel 8.

Tabel 8. Skenario Ancaman

Area of Concern		Ancaman	
1.	Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi.	***Actors***	Peretas (pihak yang tidak bertanggungjawab)
		Means	Cacat pada perangkat lunak *(software defect)*, sehingga terdapat celah keamanan
		Motives	Secara disengaja atau tidak disengaja
		Outcome	*Modification, Interruption, Disclosure*
		Security Requirement	Melakukan *update premium* antivirus pada *server* dan *monitoring* kondisi *hardware*
	Probabilitas	Tinggi	
...	...	...	...

Langkah 6: Mengidentifikasi risiko

Pada langkah ini aktivitas yang dilakukan adalah menentukan dampak dari skenario ancaman, dimana untuk setiap skenario yang telah dibuat harus ditentukan konsekuensi yang mungkin akan ditimbulkan ketika ancaman terjadi. Secara lengkap dapat dilihat pada Tabel 9.

Tabel 9. Skenario Ancaman dan Konsekuensi

Skenario Ancaman	Konsekuensi
Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi. Seperti: cacat pada perangkat lunak *(software defect)*, kerusakan sistem.	• Cacat pada perangkat lunak *(software defect)*: Perangkat lunak yang tidak rutin dilakukan *update* membuka peluang terdapat celah keamanan. • Kerusakan sistem: Rusaknya sistem atau bahkan *server* dapat menyebabkan terhentinya layanan yang diberikan.
Bocornya hak akses seperti *username* dan *password*.	• Penyalahgunaan hak akses oleh pihak lain. • Terbukanya dan pencurian informasi penting.
Ruangan *server* yang mudah diakses dapat mengakibatkan pihak yang tidak berwenang merusak *server*.	• Ancaman kerusakan terhadap perangkat yang terdapat di ruang *server*. • Layanan menjadi terhenti, dikarenakan *server* terjadi gangguan.
Penyalahgunaan *harddisk* eksternal dan file folder *backup* data oleh pihak yang tidak bertanggung jawab.	• Seluruh data hilang dikarenakan *harddisk* mengalami kerusakan. • Bocornya informasi ke pihak lain yang tidak bertanggungjawab.

Langkah 7: Menganalisis risiko

Pada langkah ini ditentukan penilaian risiko relatif terhadap risiko yang telah ditentukan sebelumnya. Masing-masing risiko akan ditentukan skor penilaian terhadap area dampak (tinggi = 3, menengah = 2, rendah = 1). Sebagian dapat dilihat pada Tabel 10.

Tabel 10. Analisis Risiko

Risiko Aset Informasi				
Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi.	Konsekuensi	• Cacat pada perangkat lunak *(software defect)*: Perangkat lunak yang tidak rutin dilakukan *update* membuka peluang terdapat celah keamanan. • Kerusakan sistem: Rusaknya sistem atau bahkan *server* dapat menyebabkan terhentinya layanan yang diberikan.		
		Area Dampak	Nilai	Skor
	Tingkat Keparahan	Reputasi dan kepercayaan pengguna	Tinggi	15
		Produktifitas	Tinggi	12
		Keuangan	Rendah	3
		Keamanan dan kesehatan	Menengah	4
		Denda dan hukum	Tinggi	3
		Skor risiko relatif		**37**
…	…	…	…	…

Pada Tabel 10, kolom skor didapatkan dari perhitungan prioritas area dapak (Tabel 2) dikalikan Kolom nilai yang diberikan, sehingga perhitungan menjadi prioritas area dampak = 5 dikalikan dengan nilai area dampak (tinggi) = 3, hasil akhir skor menjadi 15. Selanjutnya seluruh akan direkapitulasi dan dihitung penilaian risiko relatif untuk semua risiko, dapat dilihat pada Tabel 11.

Tabel 11. Penilaian Risiko Relatif

Risiko	**Skor Risiko Relatif**
Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi.	37
Bocornya hak akses seperti *username* dan *password*.	17
Ruangan *server* yang mudah diakses dapat mengakibatkan pihak yang tidak berwenang merusak *server*.	38
Penyalahgunaan *harddisk* eksternal dan file folder *backup* data oleh pihak yang tidak bertanggung jawab.	31

Langkah 8: Memilih pendekatan mitigasi yang akan dilakukan

Pada langkah ini, akan ditentukan kategori dari setiap kemungkinan (probabilitas) dari risiko sesuai dengan Tabel 12 dan ditentukan pendekatan mitigasi terhadap risiko berdasarkan Tabel 13.

Tabel 12. Matriks Risiko Relatif

Probabilitas	Skor Risiko		
	30 sampai 45	16 sampai 29	0 sampai 15
Tinggi	Kategori 1	Kategori 2	Kategori 2
Menengah	Kategori 2	Kategori 2	Kategori 3
Rendah	Kategori 3	Kategori 3	Kategori 4

Sumber: (Caralli et al., 2007)

Tabel 13. Pendekatan Mitigasi Terhadap Risiko

Kategori	Pendekatan Mitigasi
Kategori 1	Dilakukan mitigasi
Kategori 2	Dilakukan mitigasi atau ditunda
Kategori 3	Ditunda atau diterima
Kategori 4	Diterima

Sumber: (Caralli et al., 2007)

Pada langkah terakhir dilakukan rekapitulasi dari seluruh risiko yang telah ditentukan, dapat dilihat pada Tabel 14.

Tabel 14. Penentuan Mitigasi

Area of Concern	Skor Risiko Relatif	Probabilitas Risiko	Kategori	Pendekatan Mitigasi
Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi.	37	Tinggi	Kategori 1	Mitigasi
Bocornya hak akses seperti *username* dan *password*.	17	Menengah	Kategori 2	Diterima
Ruangan *server* yang mudah diakses dapat mengakibatkan pihak yang tidak berwenang merusak *server*.	38	Menengah	Kategori 2	Mitigasi
Penyalahgunaan *harddisk* eksternal dan file folder *backup* data oleh pihak yang tidak bertanggung jawab.	31	Rendah	Kategori 3	Diterima

Pada risiko dengan hasil pendekatan mitigasi perlu untuk dilakukan, maka ditentukan langkah-langkah mitigasi yang perlu dilakukan Perguruan Tinggi untuk mengatasi hal tersebut, yaitu:

Pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam *Perguruan* Tinggi

Langkah awal menampung seluruh insiden yang sedang/telah terjadi. Lakukan identifikasi dan membuat kategori insiden beserta dengan langkah-langkah dalam rencana respon setiap insiden yang sedang/telah terjadi. Sampaikan kepada *stakeholders* dan divisi yang terkena dampak insiden. Prioritaskan dahulu terhadap insiden yang terkini, waktu yang dibutuhkan dan bisa untuk ditanggulangi. Pastikan bahwa tindakan yang diambil sudah benar atau terbaik.

Selanjutnya catat seluruh insiden yang terjadi ke dalam daftar insiden. Daftar insiden nantinya akan berisi perencanaan respon insiden, cara penanggulangan insiden, penanggungjawab pengelolaan insiden.

Ruangan *server* yang mudah diakses dapat mengakibatkan pihak yang tidak berwenang merusak *server*

Langkah yang dilakukan, dengan melakukan *monitoring* risiko terhadap aset informasi. Setiap lini bisnis diberikan tanggungjawab untuk bekerja dalam level toleransi. Tentukan kontrol keamanan terhadap aset informasi yang penting tersebut. Selalu memantau kinerja dari kontrol yang telah ditetapkan.

Langkah selanjutnya, membuat *Standard Operating Procedure (SOP)* yang tepat untuk akses personil ke dalam ruangan yang penting. Kategorikan seluruh personil yang dapat masuk ke dalam ruangan untuk meminimalkan risiko terhadap kontrol keamanan yang telah disepakati.

KESIMPULAN

Dari penelitian yang dilakukan didapatkan risiko keamanan informasi yang sangat penting untuk dilakukan mitigasi, yaitu: pengeksplotasian celah keamanan sistem informasi oleh pihak luar atau dalam Perguruan Tinggi, dan ruangan *server* yang mudah diakses dapat mengakibatkan pihak yang tidak berwenang merusak *server*. Manajemen risiko keamanan informasi perlu dilakukan dan dipantau secara ketat dan rutin terhadap risiko yang ditentukan penting dan memiliki probabilitas risiko yang tinggi.

DAFTAR RUJUKAN

Arifudin, O., Wahrudin, U., & Rusmana, F. D. (2020). *Manajemen Risiko*. Penerbit Widina. https://books.google.co.id/books?hl=id&lr=&id=zd4cEAAAQBAJ&oi=fnd&pg=PA2&dq=penting+manajemen+risiko&ots=89xNLn-4Mn&sig=k0y9owAJkK1bGUwOJPrEvI5WOQM&redir_esc=y#v=onepage&q=penting manajemen risiko&f=false

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. In *Carnegie Mellon University* (Issue May). https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

Hamzah, R. F., Jaya, I. D., & Putri, U. M. (2020). Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X. *Jusifo*, *6*(1), 55–65. https://doi.org/10.19109/jusifo.v6i1.5880

Idris, M. S., Wahyuni, S., & Akbar, H. A. (2020). Analisis Manajemen Risiko Keamanan Data Sistem Transaksi Laundry (Studi Kasus: Yuni Laundry). *J-Sim: Jurnal Sistem Informasi*, *3*(2), 61–68. http://ojs.stmik-borneo.ac.id/index.php/J-SIm/article/view/61

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko

Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

Rachmaniah, M., & Mustafa, B. (2015). Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode Octave Allegro. *Jurnal Pustakawan Indonesia*, *14*(1), 14–22. https://journal.ipb.ac.id/index.php/jpi/article/view/11507

Rahardjo, B. (2005). Keamanan Sistem Informasi Berbasis Internet. In *PT Insan Infonesia* (5.3). PT Insan Infonesia. https://budi.rahardjo.id/files/keamanan.pdf

Ramadhintia, R., & Bisma, R. (2021). Perencanaan Mitigasi Risiko Menggunakan Metode OCTAVE Allegro pada SMA Semen Gresik. *Journal of Emerging Information System and Business Intelligence (JEISBI)*, *2*(2), 17–23. https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/39087

Rijayanti, R. (2018). Penilaian Tingkat Keamanan Informasi Dengan Pendekatan Risiko pada Inspection Kendaraan (Studi Kasus: Certificate of Roadworthiness di PT. XYZ). *Konferensi Nasional Sistem Informasi (KNSI) 2018*. http://jurnal.atmaluhur.ac.id/index.php/knsi2018/article/view/483

Sanjaya, J. (2020). Analisis Risk Assessment Terhadap Perusahaan IT di Bidang Finansial Menggunakan OCTAVE Allegro Framework. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, *10*(1), 57–67. https://doi.org/10.35585/inspir.v10i1.2528

Saputra, R. R., Setiawan, E., & Ambarwati, A. (2019). Manajemen Risiko Teknologi Informasi Menggunakna Metode Octave Allegro pada PT Hakiki Donarta Surabaya. *SITEKIN: Jurnal Sains, Teknologi Dan Industri*, *17*(1), 1–10. https://doi.org/10.24014/SITEKIN.V16I2.7457

Seta, H. B., Theresiawati, T., & Rahayu, T. (2017). Manajemen Risiko Aplikasi Pembelajaran Berbasis Online pada Universitas dengan Menggunakan Metode Octave Allegro. *Seminar Nasional Teknologi Informasi Dan Multimedia*, *5*(1), 8–12. https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1815

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Computer Science*, *135*, 202–213. https://doi.org/10.1016/j.procs.2018.08.167

Tobing, J. J. L., & Puspa, A. K. (2015). Analisis Manajemen Resiko untuk Evaluasi Aset Menggunakan Metode Octave Allegro. *EXPERT: Jurnal Manajemen Sistem Informasi Dan Teknologi*, *5*(1), 28–30. https://doi.org/10.36448/jmsit.v5i1.719

Zulfia, A., Ruskan, E. L., & Putra, P. (2021). Penilaian Risiko Aset Informasi dengan Metode OCTAVE Allegro: Studi Kasus ICT Fakultas Ilmu Komputer Universitas Sriwijaya. *JOINS (Journal of Information System)*, *6*(1), 40–47. https://doi.org/10.33633/joins.v6i1.4088