Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Kajian Manajemen Risiko Sistem Informasi Menggunakan Metode *Octave Allegro*

Berkat Samuel Gunawan Naibaho[1*], Djajasukma Tjahjadi[2]
Magister Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Likmi
Jl. Ir. H. Juanda No.96, Lebakgede, Bandung, Jawa Barat, Indonesia
**e-mail Corresponding Author*: snaibahoo@gmail.com

Abstrak

Berbagai ancaman yang timbul pada sistem informasi membuktikan pentingnya keamanan sistem informasi sehingga untuk melindunginya diperlukan pengelolaan yang tepat dan akurat. Salah satunya dengan menerapkan manajemen risiko yang bertujuan untuk meminimalisir ancaman kerusakan dan ekspoitasi terhadap sistem informasi perusahaan. Artikel ini bertujuan untuk mengidentifikasi dan menganalisis risiko dan dampak yang timbul pada sistem informasi PT. XYZ, serta mengidentifikasi langkah-langkah potensial sebagai upaya mitigasi. Pengumpulan data dilakukan melalui wawancara dan observasi. Data yang dihasilkan berupa data kualitatif dengan menghasilkan pendekatan mitigasi terhadap risiko sistem informasi. Selanjutnya data yang diperoleh diolah dengan menggunakan metode *OCTAVE Allegro*. Hasil menunjukkan *impact area financial* memiliki nilai prioritas paling tinggi. Sementara *data budgeting* menjadi salah satu informasi data paling penting dalam aspek *financial*. Analisis risiko terhadap *data budgeting* menghasilkan 8 *areas of concern*, 6 diantaranya dapat menimbulkan kerugian yang besar sehingga diperlukan pembangunan langkah untuk memitigasinya.
Kata kunci: *Data budgeting; Keamanan sistem informasi; Manajemen risiko; OCTAVE Allegro*

Abstract

Various threats which arise in the information system prove the importance of information system security. To protect it, proper and accurate management is needed. Risk management implementation aims to minimize the threat of damage and exploitation to the company's information system. This study aimed to identify and analyze the risks and impacts which arise on the information system of PT. XYZ, as well as identified potential measures as mitigation efforts. Qualitative data were obtained through interviews and observations. Data analysis was conducted using the OCTAVE Allegro method. Results showed the financial impact area had the highest priority value. Meanwhile, budgeting data was one of the most crucial data information in the financial aspect. The risk analysis of budgeting data resulted in 8 areas of concern, 6 of which can cause losses, so mitigation approaches are needed to minimize the impact of risk.
Keywords*: Budgeting data; Information system security; Risk management; OCTAVE Allegro*

1. Pendahuluan

Teknologi informasi dituntut untuk lebih peka terhadap kondisi gaya hidup masyarakat saat ini yang sangat bergantung pada teknologi maupun sistem informasi, pun sama halnya dengan organisasi/perusahaan dalam berbagai bidang bisnis [1]. Sebuah organisasi/perusahaan membutuhkan sistem informasi jika ingin berjalan secara efektif dan efisien [2]. Semakin meningkatnya tuntutan kebutuhan teknologi dan sistem informasi mendorong penggunaan data seluler maupun layanan internet. PT. XYZ merupakan perusahaan telekomunikasi seluler terbesar di Indonesia yang sekarang memiliki lebih dari 170 juta pelanggan. Seiring berjalannya waktu dan perkembangan teknologi, kebutuhan pelanggan PT. XYZ terhadap layanan *broadband* menjadi semakin tinggi. Hal ini mendorong PT. XYZ untuk terus berinovasi meningkatkan optimalisasi jaringan *broadband* untuk dapat memenuhi kebutuhan tersebut. PT. XYZ sendiri tidak terlepas dari kebutuhan akan sistem informasi agar strategi bisnis berjalan secara efektif dan efisien. Kehadiran sistem informasi di setiap aspek

dan proses bisnis menjadikannya sangat krusial bagi perusahaan, sehingga adanya ancaman terhadap sistem informasi dapat menimbulkan masalah bagi keberlangsungan perusahaan.

Menurut Jakaria, Dirgahayu, dan Hendrik [3] sistem informasi beserta asetnya rentan terhadap risiko kerusakan fisik yang timbul akibat bencana alam, kebakaran, lonjakan listrik, pencurian, dan perusakan yang mengakibatkan kerusakan pada perangkat keras. Selain itu ada pula risiko kerusakan logik berupa akses tidak sah terhadap sistem informasi dan data perusahaan [4]. Ancaman kerusakan dan eksploitasi pada aset perusahaan yang terkait dengan sistem informasi dapat menimbulkan gangguan pada proses bisnis bahkan kerugian secara finansial [5]. Dewasa ini, infrastruktur sistem informasi banyak menghadapi ancaman peratas yang berujung pada kerugian besar bagi perusahaan [6]. Banyak perusahaan yang telah mengalami kerugian besar akibat ancaman-ancaman tersebut. Salah satu perusahaan mesin pencari internet mengalami serangan peratas pada tahun 2014 yang menyebabkan dicurinya 500 juta akun sehingga reputasi perusahaan menjadi rusak dan nilai saham menurun. Salah satu perusahaan yang bergerak pada bidang *Automotive Wire* dan *Wiring Harness* juga mengalami berbagai ancaman pada tahun 2017 yang akhirnya merusak aset dan mengganggu proses bisnis hingga menyebabkan kerugian finansial [7].

Ancaman-ancaman yang timbul pada sistem informasi dan asetnya membuktikan pentingnya keamanan sistem informasi. Keamanan aset informasi memiliki tiga karekteristik penting yaitu kerahasiaan, integritas, dan ketersediaan [8], sehingga untuk melindunginya diperlukan pengelolaan yang tepat dan akurat. Salah satunya dengan menerapkan manajemen risiko terhadap keamanan sistem informasi. Oleh karena itu, manajemen risiko sangat dibutuhkan perusahaan untuk dapat menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikelola. Manajemen risiko ini diterapkan untuk meminimalisir ancaman kerusakan dan ekspoitasi terhadap sistem informasi perusahaan serta dampak yang ditimbulkannya. Penelitian ini menggunakan metode OCTAVE Allegro dalam melakukan kajian manajemen risiko sistem informasi pada PT. XYZ dengan tujuan mengidentifikasi dan menganalisis risiko dan dampak yang timbul pada sistem informasi, serta mengidentifikasi langkah-langkah potensial sebagai upaya mitigasi.

2. Tinjauan Pustaka

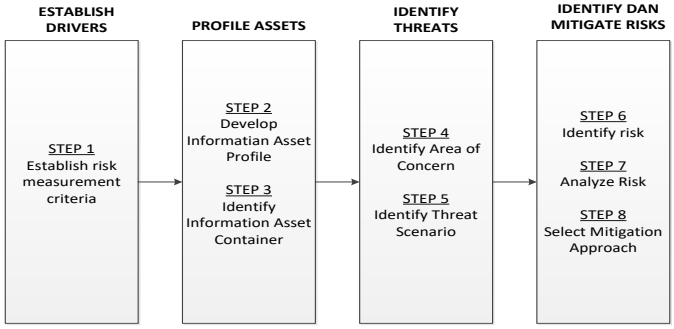
Beberapa penelitian sebelumnya telah melakukan analisis risiko terhadap sistem informasi menggunakan OCTAVE Allegro. Suroso & Fakhrozi melakukan penelitian di Universitas Thamrin yang bertujuan untuk mengurangi dampak negatif bagi pengguna sistem informasi. Langkah mitigasi yang perlu dilakukan seperti melakukan validasi terhadap hasil input data, memperpendek waktu *login* dan mengharuskan penggantian *password* akun pada periode tertentu [9]. Sardjono & Cholik melakukan analisis risiko pada sistem informasi perusahaan perbankan yang menghasilkan rekomendasi langkah-langkah seperti menerapkan peraturan bahwa semua aset informasi penting hanya bisa diakses oleh pihak berwenang, serta menerapkan rencana pemulihan bencana apabila sistem utama mengalami kerusakan [10]. Suroso *et al.* meneliti sistem informasi di bidang keuangan PT Autocomp *System* Indonesia (PASI) untuk menetapkan serangkaian strategi manajemen risiko. Hasil menunjukkan adanya kesenjangan pada *contingency plan/disaster recovery plan* dan manajemen kerentanan. Penggunaan OCTAVE Allegro diketahui dapat mengendalikan risiko dengan baik [7]. Wagiu, Siregar, dan Maulany mengidentifikasi risiko yang berpotensi mengancam proses bisnis Universitas Advent Indonesia. Hasil menunjukkan bahwa perlu dilakukannya pengurangan risiko terhadap aset-aset kritis seperti melakukan evaluasi secara berkala setiap 2 tahun [11]. Hom *et al.* melakukan analisis risiko sistem informasi akademik. Risiko paling utama adalah terjadinya eror dalam penginputan data sehingga perlu dilakukan pemeriksaan ulang. Selain itu, penyebarluasan informasi secara ilegal oleh pihak tertentu dapat dikurangi dengan memperketat otorisasi data dan memberikan sanksi terhadap staff yang teledor [12].

Berdasarkan riset-riset relevan di atas, peneliti melakukan penelitian dengan konsep serupa yaitu mengidentifikasi dan menganalisis risiko terhadap sistem informasi menggunakan metode OCTAVE Allegro. Perbedaan penelitian ini dengan reset sebelumnya terletak pada bidang bisnis yang diteliti, yaitu pada perusahaan telekomunikasi seluler.

3. Metodologi

Penelitian dilakukan di wilayah regional Sumatra Bagian Selatan (Sumbagsel) pada bulan Agustus 2021 sampai Desember 2021. Pengumpulan data dilakukan melalui wawancara

dan observasi. Wawancara dilakukan terhadap *user* yang berkaitan langsung dengan pengembangan, *maintenance* dan penggunaan sistem informasi. Obervasi dilakukan dengan mengamati kegiatan yang dilakukan oleh *user* dalam hubungannya menggunakan sistem informasi pada proses tersebut. Proses observasi ini juga menjadi sarana mengumpulkan dokumen mengenai otoritas penggunaan sistem informasi, kebijakan, tata cara, hasil audit yang memperlihatkan kondisi dan bagian yang akan dikembangkan berkaitan dengan risiko sistem informasi. Data yang dihasilkan berupa data kualitatif dengan menghasilkan pendekatan mitigasi terhadap risiko sistem informasi pada PT. XYZ. Selanjutnya data yang diperoleh diolah dengan menggunakan metode OCTAVE Allegro. OCTAVE Allegro terdiri dari delapan tahap yang terbagi dalam empat fase [13,14] yang ditunjukkan pada gambar dibawah ini.



Gambar 1. Tahapan Metode OCTAVE Allegro

4. Hasil dan Pembahasan

4.1 *Establish Risk Measurement Criteria*

Kriteria manajemen risiko yang dapat berpengaruh pada visi misi organisasi diklasifikasikan pada 5 *impact area* yaitu *reputation and customer*, *financial, productivity, safety and health,* dan *fines and legal penalty.* Reputasi berpengaruh terhadap kepercayaan mitra yang diukur dengan keterlambatan memproses dokumen, dan keterlambatan pembayaran kepada mitra. Biaya operasional dan penambahan pengeluaran merupakan area dampak prioritas yang dapat mempengaruhi keuangan pada PT. XYZ seperti laba dan pengaturan anggaran perusahaan. Jam kerja staff digambarkan sebagai faktor yang paling memiliki dampak terhadap produksi. Setiap penambahan jam kerja 1 hari, maka karyawan harus lembur. Produktivitas memiliki keterkaitan pada keselamatan dan kesehatan kerja. Jumlah jam kerja yang meningkat dapat menyebabkan penurunan kondisi kesehatan karyawan. Denda yang berlaku pada PT. XYZ yaitu jika berkaitan dengan keterlambatan pembayaran. Setiap keterlambatan pembayaran pada ketentuan tertentu, maka akan dikenakan denda sebesar 1%. Kelima kriteria *impact area* diatas kemudian diberi nilai prioritas yang ditentukan pada skala 1 hingga 5. Semakin besar nilai skalanya maka semakin penting kriteria *impact area* tersebut. Nilai prioritas *impact area* disajikan pada Tabel 1.

Tabel 1. *Impact Area Prioritazion Worksheet*

Priority	*Impact Areas*
4	*Reputation and Customer Confidence*
5	*Financial*
2	*Productivity*
1	*Safety and Health*
3	*Fines and Legal Penalties*

Berdasarkan Tabel 1, kriteria *financial* merupakan area yang memiliki dampak dengan nilai prioritas tertinggi. Sementara keselamatan dan kesehatan kerja memiliki dampak prioritas terendah. Pada penelitian ini, fokus area dampak PT. XYZ yaitu pada kriteria *financial*.

4.2 *Develop an Information Asset Profile*

Informasi *asset* perusahaan PT. XYZ dikelola oleh divisi GS (*general service*) yang terdiri dari data nilai kontrak kerjasama, data serah terima, data tagihan, data *budgeting*, data mitra, dan data *asset.* Aset informasi *finance* yang memiliki skala prioritas tertinggi salah

satunya adalah data *budgeting* sehingga menjadi informasi data yang paling penting. Profil aset informasi kritis pada data *budgeting* disajikan pada Tabel 2.

Tabel 2. *Critical Information Aset Profile*

(1) *Critical Asset*	**(2) *Rationale for Selection***	**(3) *Description***
Data *Budget*	Tugas utama adalah pembelanjaan kebutuhan perusahaan, dimana itu bisa terlaksana jika data atau informasi budget itu ada. Contoh: pembelian laptop karyawan itu ada nomor rekeningnya (nomor akun) maka jika data itu hilang maka pengadaan tersebut tidak bisa terealisasikan.	Nomor akun, nominal akun, restriksi, data lokasi.
(4) *Owner (s*)		
Divisi *General Service*		
(5) *Security Requirements*		
Confidentiality	Hanya orang yang berwenang yang dapat melihat aset informasi ini adalah manager, supervisor, dan staf.	
Integrity	Hanya orang yang berwenang yang dapat memodifikasi aset informasi ini adalah divisi *general manager finance*	
Availability	Aset ini harus tersedia untuk orang yang berwenang melakukan tugasnya adalah manager, supervisor, dan staf *general service*. Aset ini harus tersedia setiap saat.	
Others	Aset ini memiliki persyaratan perlindungan kepatuhan peraturan khusus, yaitu untuk membuka aset ini, ada otorisasi sehingga butuh autentifikasinya user yang akan menggunakan.	
(6) *Most Important Security Requirement*		
Confidentiality	*Integrity*	*Availability*	*Others*

Data *budget* merupakan aset informasi yang penting dan menjadi prioritas karena mencakup data pembelanjaan kebutuhan perusahaan. Data *budget* merupakan aset informasi yang bersifat rahasia, sehingga keamanan kerahasiaannya (*confidentiality*) harus terjaga. Data *budget* memiliki aset yang mencakup nomor akun, nominal akun, restriksi, dan data lokasi yang hanya dapat dikelola oleh divisi *general service*. Persyaratan keamanan yang diterapkan pada sistem informasi data *budget* yaitu hanya orang yang berwenang yang dapat mengakses dan memodifikasinya berupa sistem otorisasi pada *user*.

4.3 *Identify Information Asset Containers*

Identifikasi *information asset container* dilakukan menggunakan *Information Asset Risk Environment Map* yang dibagi kedalam tiga aspek yaitu *technical*, *physical*, dan *people*. Aspek *Technical* merupakan *container* pada aset informasi berupa perangkat keras, perangkat lunak, sistem yang berada dalam kontrol PT. XYZ (internal) maupun diluar kontrol PT. XYZ (eksternal). Informasi *asset container* pada aspek taknis disajikan pada Tabel 3.

Tabel 3. *Information Asset Risk Environment Map (Technical)*

Internal	
Container Description	***Owner(s)***
Sistem Informasi: SIENNA	PT XYZ
Drive Cloud Corporate	PT XYZ
PC User	Divisi General Service
External	
Container Description	***Owner(s)***
Sistem Informasi: SIENNA (*user* dan *dashboard* beserta fungsinya berbeda)	PT XYZ yang digunakan Mitra

PT. XYZ memiliki sistem informasi SIENNA dan *drive cloud corporate* dalam mengelola sistem informasi pada data *budget,* sedangkan secara khusus divisi *general service* memiliki sistem yaitu *PC user*. Pihak mitra yang berhubungan dengan PT. XYZ memiliki akses dapat

menggunakan sistem informasi SIENNA namun dengan batasan tertentu. Aspek *physical* merupakan dokumen fisik yang berada dibawah kontrol PT XYZ (internal) maupun diluar kontrol PT XYZ (eksernal). Informasi *Asset Container* pada aspek fisik disajikan pada Tabel 4.

Tabel 4. *Information Asset Risk Environment Map (Physical)*

Internal	
Container Description	***Owner(s)***
Permintaan *budget* untuk kebutuhan rutin dan non-rutin dalam operasional justifikasi, nama pekerjaan, dan nilai *budge*t yang dibutuhkan.	Divisi *General Service*
Laporan penyerapan anggaran nilai dinamis dari penggunaan *budge*t terhadap pekerjaan yang sudah direncanakan sebelumnya.	Divisi *General Service*
External	
Container Description	***Owner(s)***

Divisi *general service* memiliki kuasa penuh dalam mengontrol permintaan *budget* dan laporan penyerapan anggaran. Selain itu pada data *budget*, divisi *general service* mengontrol kebutuhan operasional PT. XYZ dan mengontrol agar nilai keuangan menjadi dinamis sesuai dengan anggaran yang telah direncanakan. Aspek *people* merupakan pihak yang berwenang mengetahui sistem informasi dalam kontrol PT XYZ (internal) maupun diluar kontrol PT XYZ (eksternal). Informasi *Asset Container* pada aspek ini disajikan pada tabel 5.

Tabel 5. *Information Asset Risk Environment Map* (*People*)

Internal Personal	
Container Description	***Owner(s)***
GM *General Service*	Divisi General Service
GM *Finance*	*Finance Business Partner*
Manager General Service	Divisi *General Service*
Manager Finance	*Finance Business Partner*
Supervisor General Service	Divisi *General Service*
Staf *General Service*	Divisi *General Service*
External	
Container Description	***Owner(s)***
Container, Vendor, Dll	*Organization*

Pihak yang berwenang dalam mengelola dan mengontrol data data *budget* pada PT. XYZ yaitu GM *general service*, *manager general service*, *supervisor general service* dan staf *general service* pada divisi *general service*, serta GM *finance* dan *manager finance* pada divisi *finance business partner*.

4.4 *Identify Areas of Concern*

Identifikasi *areas of concern* dikembangkan untuk memasukkan skenario ancaman. Kemudian dokumentasi dilakukan pada setiap area masalah untuk melihat potensi pengaruhnya terhadap persyaratan keamanan informasi. Daftar *areas of concern* disajikan pada Tabel 6.

Tabel 6. Daftar *Areas of Concern*

No	*Areas of Concern*
1	Kesalahan penggunaan akun
2	Kesalahan penginputan nilai
3	*Error* di SIENNA
4	*Crash* di SIENNA
5	Spesifikasi PC tidak memadai
6	Terjadi disconnection dengan jaringan internal
7	Ketidaksesuaian fungsi pada sistem SIENNA
8	Kerusakan pada *server*

Data *budget* pada PT. XYZ yang menjadi perhatian khusus yaitu kesalahan penggunaan akun dan penginputan nilai, *error* dan *crash* serta ketidaksesuaian fungsi pada sistem informasi SIENNA, dan kerusakan *server*, gangguan jaringan internal serta PC yang tidak memadai.

4.5 *Identify Threat Scenarios*

Skenario ancaman merupakan situasi dimana aset informasi pada PT. XYZ khususnya data *budget* dapat terancam. Identifikasi skenario ancaman dilakukan untuk mendeskripsikan ancaman-ancaman secara lebih rinci. Setelah ancaman-ancaman tersebut diidentifikasi, tahap selanjutnya adalah melengkapi *information asset risk worksheet* dari skenario ancaman yang ada. Daftar skenario ancaman pada informasi data *budget* PT. XYZ disajikan pada tabel 7.

Tabel 7. Daftar Skenario Ancaman

1	*Information Asset*	Data Budgeting
	Area of Concern	Kesalahan penggunaan akun
	Actor	Staf dan *Supervisor General Service*
	Means	Staf atau supervisor salah menggunakan akun
	Motive	Ketidakpahaman penggolongan pekerjaan dengan pemakaian akun
	Outcome	[ ] *Disclosure* [ ] *Destruction* [√] *Modification* [ ] *Interuption*
	Security Recruitment	Diperlukannya klasifikasi dalam penggunaan akun
2	*Information Asset*	Data Budgeting
	Area of Concern	Kesalahan penginputan nilai
	Actor	Staf dan *Supervisor General Service*
	Means	Staf atau supervisor salah menginputkan nilai
	Motive	Karena *human error*
	Outcome	[ ] *Disclosure* [ ] *Destruction* [√] *Modification* [ ] *Interuption*
	Security Recruitment	Diperlukannya *pop up questions*
3	*Information Asset*	Data Budgeting
	Area of Concern	*Error* di SIENNA
	Actor	IT dan Developer
	Means	Kesalahan *syntax* pada saat *development* sistem
	Motive	Karena kerumitan bahasa pemrograman
	Outcome	[ ] *Disclosure* [√] *Destruction* [ ] *Modification* [ ] *Interuption*
	Security Recruitment	Diperlukannnya *retesting* terhadap sistem
4	*Information Asset*	Data Budgeting
	Area of Concern	*Crash* di SIENNA
	Actor	IT dan Developer
	Means	Kesalahan *syntax* pada saat *development* sistem, pemeliharaan perangkat pendukung sistem yang kurang berkesinambungan
	Motive	Karena kerumitan bahasa pemrograman, kurangnya prioritas dalam penjadwalan *maintenance* perangkat atau sistem
	Outcome	[ ] *Disclosure* [√] *Destruction* [ ] *Modification* [ ] *Interuption*
	Security Recruitment	Diperlukannnya penjadwalan rutin untuk *retesting* sistem
5	*Information Asset*	Data Budgeting
	Area of Concern	Spesifikasi perangkat tidak memadai
	Actor	IT
	Means	Kesalahan dalam menentukan spesifikasi dari perangkat
	Motive	Menekan budget pembelian perangkat
	Outcome	[ ] *Disclosure* [ ] *Destruction* [ ] *Modification* [√] *Interuption*
	Security Recruitment	Diperlukan pemenuhan anggaran untuk pengadaan perangkat dengan spesifikasi yang lebih baik

		Tabel 7. Lanjutan……
6	*Information Asset*	Data Budgeting
	Area of Concern	Terjadi *disconnection* dengan jaringan internal
	Actor	IT
	Means	Limitasi terhadap koneksi dari *soft token*
	Motive	Untuk *security system*
	Outcome	[ ] *Disclosure* [ ] *Destruction* [ ] *Modification* [√] *Interuption*
	Security Recruitment	Diperlukannya klasifikasi limit yang berbeda antar user
7	*Information Asset*	Data Budgeting
	Area of Concern	Ketidaksesuaian fungsi pada sistem SIENNA
	Actor	IT dan Developer
	Means	*Development* sistem tidak mencapai ekspektasi dari user
	Motive	Kerumitan dalam *developmen*t dan perspektif yang berbeda antara *user* dan *developer*
	Outcome	[ ] *Disclosure* [ ] *Destruction* [ ] *Modification* [√] *Interuption*
	Security Recruitment	Diperlukannya *testing* yang berkesinambungan dengan melibatkan *user*
8	*Information Asset*	Data Budgeting
	Area of Concern	Kerusakan pada server akibat bencana alam
	Actor	IT
	Means	*Force Major*
	Motive	*Unpredictable*
	Outcome	[ ] *Disclosure* [√] *Destruction* [ ] *Modification* [ ] *Interuption*
	Security Recruitment	Diperlukan ruang khusus untuk peletakan *server*

Area ancaman yang menjadi perhatian pada data *budget* PT. XYZ diantaranya, aktor yang menjadi perhatian khusus dalam melakukan kesalahan pada penggunaan akun dan penginputan nilai adalah staf dan *supervisor general service*, yang disebakan karena kurang pahamnya penggolongan pekerjaan dengan penggunaan akun dan adanya kesalahan dalam menginput nilai yang ada pada sistem informasi PT. XYZ. Kesalahan penggunaan akun dan penginputan nilai dapat dimodifikasi dengan persyaratan keamanan yaitu adanya klasifikasi dalam penggunaan akun serta diberlakukannya *pop up questions*. Selanjutnya, pada kondisi *error* dan *crash* serta ketidaksesuaian sistem pada SIENNA, aktor yang terlibat yaitu divisi IT dan *developer*. Kondisi tersebut terjadi karena adanya kesalahan *syntax* pada sistem *development*, kurangnya prioritas dalam penjadwalan *maintenance*, serta sistem *development* yang tidak mencapai ekspektasi dari *user*. Selain itu kerumitan bahasa pemprograman menjadi masalah utama pada kondisi data *budget* di PT.XYZ. Jika terjadi *error* dan *crash* pada sistem SIENNA, maka sistem tersebut harus dihancurkan, dan ketidaksesuaian fungsi pada sistem SIENNA perlu diberikan interupsi. Persyaratan keamanan pada *error* dan *crash* di SIENNA yaitu diperlukan adanya *retesting* dan penjadwalan rutin pada *retesting* terhadap sistem, serta persyaratan keamanan pada ketidaksesuaian fungsi yaitu diperlukan *testing* yang berkesinambungan dengan melibatkan *user*.

Kemudian, aktor yang terlibat dalam spesifikasi perangkat yang tidak memadai, adanya *disconnection* pada jaringan internal, serta kerusakan pada *server* akibat bencana alam adalah divisi IT. Kondisi tersebut terjadi akibat adanya kesalahan dalam menentukan spesifikasi dari perangkat, adanya limitasi terhadap koneksi dari *soft token*, serta adanya pemaksaan mayor. Oleh karena itu pada ancaman spesifikasi perangkat yang tidak memadai dan *disconnection* pada jaringan internal diperlukan adanya interupsi, namun adanya kerusakan pada *server* akibat bencana alam harus dihancurkan. Persyaratan keamanan yang perlu dilakukan adalah diperlukan pemenuhan anggaran sehingga diadakan pengadaan perangkat, adanya klasifikasi limit yang berbeda antar *user*, serta diperlukan ruang khusus untuk peletakan *server*.

4.6 *Identify Risks*

Pada tahap ini ditentukan skenario ancaman yang telah diteliti dan dicatat pada setiap lembar kerja risiko aset informasi yang dapat memberikan dampak/pengaruh pada PT. XYZ. Dampak tersebut digolongkan menjadi 3, yaitu rendah, sedang, dan tinggi. Perhitungan *relative risk score* dapat dilihat pada Tabel 8. Dampak yang rendah maka prioritas akan dikalikan 1, sedangkan dampak sedang maka hasil prioritas dikalikan 2, dan dampak tinggi maka hasil prioritas dikalikan 3.

Tabel 8. Pedoman Menghitung *Relative Risk Score*

Impact Area	*Priority*	*Low*	*Medium*	*High*
Reputation and Customer Confidence	4	4	8	12
Financial	5	5	10	15
Productivity	2	2	4	6
Safety and Health	1	1	2	3
Fines and Legal Penalties	3	3	6	9

Berdasarkan Tabel 8 diketahui bahwa jika risiko *financial* memiliki dampak yang besar maka nilai relatifnya sebesar 15 yang berasal dari prioritas dikalikan 3. Financial memiliki prioritas tertinggi dengan poin 5 dan dampaknya adalah tinggi maka perhitungan *relative score* nya 5 dikalikan 3. Namun jika dampak dari risiko keuangan tersebut adalah rendah maka nilai relatifnya sebesar 5. Begitu pula dengan dampak dari area *safety and health* yang rendah maka skor relatif nya sebesar 1 dan jika dampaknya tinggi maka skornya menjadi 3.

4.7 *Analyze Risks*

Tahap ini merupakan tahap menganalisis risiko total dengan melakukan *review* pada *risk measurement criteria*. Kemudian menghitung nilai risiko relatif. Penghitungan dilakukan untuk menganalisis risiko dan menentukan strategi dalam menghadapi risiko. Setiap aktifitas pada tahap ini diwajibkan mengacu pada *information asset risk worksheet* agar didapatkan hasil strategi yang terbaik. Hasil analisis risiko pada data *budget* PT.XYZ disajikan pada tabel 9.

Tabel 9. Analisis Risiko

	Area of Concern		*Risk*		
1	Kesalahan penggunaan akun	*Consequences*	Data penyerapan aset menjadi tidak *valid*		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*High*	12
			Financial	*High*	15
			Productivity	*Med*	4
			Safety & Health	*Low*	1
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**35**
2	Kesalahan penginputan nilai	*Consequences*	Data penyerapan dan saldo *budget* yang kurang tepat		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*High*	12
			Financial	*High*	15
			Productivity	*Med*	4
			Safety & Health	*Low*	1
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**35**
3	*Error* di SIENNA	*Consequences*	Terjadi kesalahan pada pemrosesan inputan dari user		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*High*	*12*
			Financial	*High*	*15*
			Productivity	*High*	*6*

	Area of Concern		*Risk*		
			Safety & Health	*Low*	*1*
			Fines & Legal Penalties	*Low*	*3*
			Relative Risk Score		***37***
4	*Crash* di SIENNA	*Consequences*	Terjadi kerusakan terhadap proses yang sedang dijalankan pada sistem		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*High*	12
			Financial	*High*	15
			Productivity	*High*	6
			Safety & Health	*Low*	1
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**37**
5	Spesifikasi perangkat tidak memadai	Consequences	*Lead time* yang semakin panjang		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*High*	12
			Financial	*Med*	10
			Productivity	*High*	6
			Safety & Health	*Low*	1
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**32**
6	Terjadi *disconnection* dengan jaringan internal	*Consequences*	*Machine time* yang lebih lama		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*High*	12
			Financial	*Low*	5
			Productivity	*High*	6
			Safety & Health	*Low*	1
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**27**
7	Ketidaksesuaian fungsi pada sistem SIENNA	*Consequences*	Produktivitas dari sistem tidak maksimal		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*Med*	8
			Financial	*Low*	5
			Productivity	*High*	6
			Safety & Health	*Low*	1
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**23**
8	Kerusakan pada server akibat bencana alam	*Consequences*	*System down* dan operasional sistem terhenti		
		Severity	*Impact Area*	*Value*	*Score*
			Reputation & Customer Confidence	*Low*	4
			Financial	*High*	15
			Productivity	*High*	6
			Safety & Health	*High*	3
			Fines & Legal Penalties	*Low*	3
			Relative Risk Score		**31**

4.8 *Select Mitigation Approach*

Pada tahap ini dilakukan penyusunan *relative risk matrix* dan pendekatan mitigasi risiko. Penyusunan *relative risk matrix* bertujuan untuk memetakan skor dari risiko yang ada yang disajikan pada Tabel 10. Sementara pendekatan mitigasi berdasarkan skor risiko disajikan pada Tabel 11.

Tabel 10. *Matrix* Skor Relatif

Skor risiko	30 - 45	16 – 29	0 - 15
Pool	Pool 1	Pool 2	Pool 3

Tabel 11. Pendekatan Mitigasi

Pool	Pendekatan Mitigasi
1	*Mitigate*
2	*Defer*
3	*Accept*

Jika skor berada pada *pool 1* maka diperlukan tahapan mitigasi terhadap risiko yang ada karena akan memberikan dampak atau kerugian yang besar bagi perusahaan (Tabel 10 dan Tabel 11). Apabila risiko tersebut berada pada pool 2 dan 3 maka dampak yang dihasilkan tidak terlalu besar sehingga tidak perlu dilakukan mitigasi dan risikonya dapat diterima oleh perusahaan. Dampak yang timbul dari adanya risiko membuat operasional terganggu. Untuk itu, sebaiknya perusahaan dapat mencegah timbulnya risiko tersebut dengan melakukan mitigasi. Mitigasi risiko yang dapat dilakukan perusahaan dapat dilihat pada Tabel 12.

Tabel 12. Mitigasi Risiko

1	*Areas of Concern*	Kesalahan penggunaan akun
	Action	*Mitigate*
	Container	*Control*
	Staf dan Supervisor *General Service*	2. *Auto tracing* akun pada sistem untuk mempermudah ketepatan penggunaan nomor akun 3. Mengubah notasi akun menjadi lebih sederhana dan lebih spesifik 4. Membuat *pop up suggestion* pada saat proses penginputan akun, yang mengarah pada transaksi yang akan dilakukan
2	*Areas of Concern*	Kesalahan penginputan nilai
	Action	*Mitigate*
	Container	*Control*
	Staf dan Supervisor *General Service*	1.Membuat *second layer* dalam proses penginputan nilai untuk menguji kecocokan angka 2.Merancang sistem *robotic* untuk melakukan penginputan nilai secara otomatis
3	*Areas of Concern*	Error di SIENNA
	Action	*Mitigate*
	Container	*Control*
	IT dan Developer	1.Melakukan penjadwalan tetap untuk maintenance sistem 2.Menyediakan call center 24 jam untuk problem solver dari sistem 3.Melakukan checkup secara keseluruha*n terhadap aplikasi baik secara* syntax, dashboard maupun bahasa pemrograman 4.Merangkum *experience user* untuk menjadi bahan evaluasi dan perbaikan sistem
4	*Areas of Concern*	Crash di SIENNA
	Action	*Mitigate*
	Container	*Control*
	IT dan Developer	1.Melakukan *checkup* terhadap struktur *developing system* untuk menemukan *faulty* yang mungkin ada pada saat membangun sistem 2.Menyediakan *call center* 24 jam untuk *problem solver* dari sistem 3.Penambahan fitur *self-refresh* pada sistem untuk mencegah *crash*

Tabel 12. Lanjutan …..

5	Areas of Concern	Spesifikasi perangkat tidak memadai
	Action	*Mitigate*
	Container	*Control*
	IT	1. Mengkalkulasikan dengan tepat kebutuhan spesifikasi perangkat yang sesuai dengan penggunaan *user* dan pengembangan sistem 2. Melakukan uji coba penggunaan sistem pada perangkat sebelum memutuskan untuk dipakai di perseroan 3. Memilih perangkat yang dapat di *upgrade* spesifikasinya
6	*Areas of Concern*	Terjadi disconnection dengan jaringan internal
	Action	*Defer*
7	*Areas of Concern*	Ketidaksesuaian fungsi pada sistem SIENNA
	Action	*Defer*
8	*Areas of Concern*	Kerusakan pada server akibat bencana alam
	Action	*Mitigate*
	Container	*Control*
	IT	1. Menempatkan *server* pada ruang khusus yang sudah dirancang untuk dapat bertahan ketika ada bencana 2. Menjalankan dengan ketat SOP pemeliharaan dan kunjungan ke ruangan server 3. Pemasangan alarm bencana pada ruang *server* yang terkoneksi dengan *device* divisi yang bertanggung jawab

Mitigasi risiko yang bisa diterapkan di *General Service* PT. XYZ Regional Sumbagsel berdasarkan hasil penelitian diantaranya melakukan penjadwalan tetap untuk *maintenance system*. Hal ini sangat penting untuk segera dilaksanankan dengan jadwal tetap sehingga sistem tetap dalam kondisi yang baik dan pencegahan dini *faulty* pada sistem. Selanjutnya, menyediakan *help center* 24 jam untuk *problem solver* dari sistem. Ketersediaan *help center* akan menjadi solusi tercepat yang dapat dijangkau oleh karyawan yang mengalami masalah dengan sistem. Kondisi operasional yang berjalan 24 jam mendorong kebutuhan *help center* yang tetap *standby*. Kemudian, penambahan fitur *self-refresh* pada sistem untuk mencegah *crash. Self-refresh* diharapkan dapat menjadi fitur kecil yang dapat membantu *user* dalam menjaga sistem tetap *standby*, karena pada operasionalnya, sistem yang *vacuum* dalam beberapa saat cenderung mengalami *crash*.

Pada penelitian ini ditemukan bahwa fokus area dampak PT. XYZ yaitu pada kriteria *financial* karena memiliki prioritas paling tinggi. Beberapa penelitian terdahulu menemukan hasil yang berbeda pada skala prioritas tertinggi. Abdullah *et al*. dan Hom *et al*. menemukan bahwa kriteria reputasi dan kepercayaan mitra merupakan area dampak paling penting [12,15]. Sementara Sukri & Riadi serta Suroso *et al*. menyatakan bahwa prioritas tertinggi yaitu pada produktivitas [2,7]. Penemuan hasil yang berbeda ini bergantung pada organisasi/perusahaan yang diteliti yang tentu saja memiliki latar belakang, faktor, serta bidang yang berbeda. Perbedaan prioritas area dampak akan berpengaruh terhadap tahap-tahap selanjutnya seperti penentuan *information asset profile, information asset containers, hingga* identifikasi *areas of concern* dan penentuan pendekatan mitigasi. Namun demikian, persamaan penelitian ini dengan riset-riset sebelumnya terletak pada perlunya pengambilan langkah mitigasi pada *areas of concern* yang telah ditemukan, terutama pada risiko yang dapat mempengaruhi kegiatan operasional dan menimbulkan kerugian bagi perusahaan.

5. Simpulan

Berdasarkan hasil penelitian *data budgeting* merupakan salah satu informasi data paling penting bagi PT. XYZ regional Sumbagsel. Apabila data tersebut mengalami kerusakan atau hilang maka dapat mempengaruhi operasional perusahaan hingga mengakibatkan kerugian bagi perusahaan. Data *budgeting* menghasilkan 8 *areas of concern*, 6 diantaranya dapat menimbulkan kerugian yang besar sehingga diperlukan pembangunan langkah untuk memitigasinya. Enam area tersebut yaitu kesalahan penggunaan akun, kesalahan penginputan nilai, *error* di SIENNA, *crash* di SIENNA, spesifikasi perangkat tidak memadai, dan kerusakan

pada *server* akibat bencana alam. Penggunaan metode OCTAVE Allegro dapat dilakukan oleh PT. XYZ regional Sumbagsel setahun sekali. Dengan adanya tahapan identifikasi hingga mitigasi risiko, kerugian yang dihasilkan oleh perusahaan dapat dikurangi atau dicegah. Selain itu, hasil analisis OCTAVE Allegro pada penelitian ini dapat dijadikan acuan sebagai referensi untuk mengembangkan profil risiko perusahaan.

Daftar Referensi

[1] E. Handoyo, R. Umar, I. Riadi, "Analysis Security of SIA Based DSS05 on COBIT 5 using Capability Maturity Model Integration (CMMI)", Scientific Journal of Informatics. vol. 6, no. 2, pp. 193–202, 2019. doi: 10.15294/sji.v6i2.17387

[2] M. Sukri, I. Riadi, "Risk Management Analysis on Administration System using OCTAVE Allegro Framework", Int. J. of Computer Applications, vol. 174, no. 17, pp. 5–11, 2021. doi: 10.5120/ijca2021920981

[3] D.A. Jakaria, R.T. Dirgahayu, Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi menggunakan Metoda Octave Allegro", In: Seminar Nasional Aplikasi Teknologi Informasi. Yogyakarta: Universitas Islam Indonesia; pp. 37–42, 2013.

[4] A.M. Suduc, M. Bîzoi, F.G. Filip, "Audit for Information Systems Security", Informatica Economica, vol. 14, no. 1, pp. 43–48, 2010.

[5] M. Jouini, L.B.A. Rabai, A. Aissa, "Classification of Security Threats in Information Systems", *Procedia Computer Science*. vol. 32, pp. 489–96, 2014. doi: 10.1016/j.procs.2014.05.452

[6] M. Zineddine, "Vulnerabilities and Mitigation Techniques Toning in The Cloud: A Cost and Vulnerabilities Coverage Optimization Approach using Cuckoo Search Algorithm with Lévy Flights", *Computers & Security*, vol. 48, pp. 1–18, 2015. Available from: 10.1016/j.cose.2014.09.002

[7] J.S. Suroso, S.M.N. Rahaju, Kusnadi, "Evaluation of IS Risk Management using Octave Allegro in Education Division", *In: 2018 International Conference on Orange Technologies, ICOT 2018*. Bali: IEEE; pp. 1–8, 2018. doi: 10.1109/ICOT.2018.8705866

[8] M.E. Whitman, H.J. Mattord, *Principles of Information Security*. 4th ed. Boston: Thomson Course Technology, 2012.

[9] J.S. Suroso, M.A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution", *Procedia Computer Science*, vol. 135, pp. 202–213, 2018. doi: 10.1016/j.procs.2018.08.167

[10] W. Sardjono, C. muhamad, "Information Systems Risk Analysis using Octave Allegro Method Based at Deutsche Bank", *In: International Conference on Information Management and Technology (ICIMTech)*. Jakarta: IEEE, pp. 38–42, 2018. doi: 10.1109/ICIMTech.2018.8528108

[11] E.B. Wagiu, R. Siregar, R. Maulany, "Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method", *In: International Scholars Conference Proceedings*. Bandung: ISC; pp. 1741–50, 2019. doi: 10.35974/isc.v7i1.1387

[12] J. Hom, B. Anong, K.B. Rii, L.K. Choi, K. Zelina, "The Octave Allegro Method in Risk Management Assessment of Educational Institutions", *Aptisi Transactions on Technopreneurship (ATT)*. vol. 2, no. 2, pp. 167–79, 2020. doi: 10.34306/att.v2i2.103

[13] R.A. Caralli, J.F. Stevens, L.R. Young, W.R. Wilson, "Introducing Octave Allegro: Improving the Information Security Risk Assessment Process", Pittsburgh: Carnegie Mellon University, 2007.

[14] Rosini, M. Rachmaniah, B. Mustafa, "Penilaian Risiko Kerawaran Informasi dengan Menggunakan Metode Octave Allegro", J. Pustakawan Indonesia, vol. 14, no. 1, pp. 14–22, 2016. doi: https: 10.29244/jpi.14.1.%25p

[15] K. Abdullah, I.N. Isnainiyah, M.I. Faried, "Risk Management Analysis on Organizational Website using Octave Allegro Method", *In: Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*. Jakarta: IEEE; pp. 201–206, 2020. doi: 10.1109/ICIMCIS51567.2020.9354298