Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 675-685
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Analisis Manajemen Risiko Keamanan Sistem Pengolahan Data *Accurate* Menggunakan Metode OCTAVE-S

Fajar Rido Butar Butar[1], Eki Saputra[2], Arif Marsal[3], Muhammad Luthfi Hamzah[4], Mona Fronita[5]
[1,2,3,4,5]Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau, Indonesia
e-mail: rbfajar19@gmail.com

Abstract
PT.XYZ is a palm oil company currently implementing the Accurate data processing system to manage data at its factory. This system is utilized for weighing incoming palm fruit, processing palm fruit within the factory, and generating various reports. However, during the implementation process, the system has encountered several threats that have had an impact on the company. These threats include connection errors, human errors, and server downtime. To address these issues, a threat risk analysis is necessary to minimize the likelihood of similar problems occurring in the future. In this study, the OCTAVE-S method is employed as it offers solutions for managing other threats. The risk analysis results indicate that there are six security practices that pose a high risk to the company's system security. These practices are IT Security Monitoring and Audit, Authorization and Authentication, Vulnerability Management, Encryption, Security Planning and Architecture, and Incident Management. Based on these findings, it is recommended that the company conducts a review of its security practices to prevent the emergence of new risks that may affect its business processes.

Keywords*: Accurate; OCTAVE-S; Stoplights; IT Risk Management; Information System Security*

Abstrak
PT.XYZ merupakan perusahaan sawit yang dalam proses pengelolaan data dipabriknya menggunakan sistem pengolahan data Accurate, dimana sistem ini digunakan dalam proses penimbangan buah sawit yang masuk, pengolahan buah sawit di dalam pabrik serta laporan yang lainnya. Namun selama penerapannya sistem tersebut pernah mengalami ancaman yang berdampak pada perusahaan seperti connection eror, human eror serta server down. Untuk mengatasi permasalahan tersebut diperlukan analisis risiko ancaman agar masalah yang terjadi dapat diminimalisir terjadi lagi. Dalam penelitian ini menggunakan metode OCTAVE-S, karena metode ini memberikan solusi bagi pihak manajemen perusahaan untuk mengatasi ancaman lainnya. Hasil dari analisis risiko ini menyimpulkan bahwa terdapat 6 praktek keamanan yang berada pada status berisiko tinggi terjadinya ancaman pada keamanan sistem diperusahaan yaitu Pemantauan dan Audit Keamanan IT, Pengesahan dan Otoritas, Manajemen Kerentanan, Enkripsi, Perencanaan dan Arsitektur Keamanan, dan Manajemen Insiden. Dari hasil yang diperoleh pihak perusahaan perlu melakukan peninjauan ulang terhadap praktek keamanan untuk mencegah terjadinya risiko baru yang berdampak pada proses bisnis perusahaan.

Kata kunci*: Accurate, OCTAVE-S, Stoplight, Manajemen Risiko IT, Keamanan Sistem Informasi*

1. PENDAHULUAN

Teknologi merupakan seperangkat komputer untuk mengelola data, sesuai kebutuhan, serta teknologi telekomunikasi dipakai agar data bisa disebar dan diakses. Teknologi yang digunakan dalam mengolah data, memproses, menyimpan, mengubah data untuk menghasilkan informasi yang bermanfaat disebut Teknologi

Informasi [1]. Teknologi informasi adalah bagian yang tidak terpisahkan dalam suatu perusahaan karena dapat membantu menambah efektifitas dan efisiensi proses bisnis perusahaan [2]. Penggunaan teknologi informasi berkembang menjadi kebutuhan yang sangat penting untuk meningkatkan efektifitas, efisiensi dan produktivitas kinerja melalui tiap pekerjaannya [3]. Terdapat studi sistem informasi dalam setiap penerapan teknologi informasi, umumnya menyelidiki dan mendiskusikan langkah kerja di mana sistem itu sendiri diimplementasikan dan disebarkan untuk memastikan bahwa semua bagian terkait serta aset sistem informasi yang terhubung dalam sistem dapat diperoleh secara efektif [1].

Aset sistem informasi (perangkat keras, perangkat lunak, sistem, informasi dan pengguna) ialah aset yang vital bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak bisa hanya disandarkan pada teknologi keamanan informasi, melainkan harus adanya pemahaman dari organisasi mengenai apa yang harus dilindungi serta menentukan secara tepat solusi yang bisa menangani permasalahan kebutuhan keamanan informasi [7]. Tujuan Keamanan Informasi adalah untuk memastikan kerahasiaan, integritas, ketersediaan dan akuntabilitas sumber daya yang menjadi tanggung jawab organisasi [8]. Keamanan informasi dapat memastikan kelanjutan bisnis, mengurangi permasalahan, mengoptimalkan *return on investment* dan mencari peluang bisnis [12]. Di samping untuk mendukung pengambilan keputusan koordinasi, dan pengawasan, sistem informasi juga membantu para manajer dan karyawan dalam menganalisis risiko, menggambarkan hal-hal yang sulit, serta menghasilkan produk baru. Namun penggunaan sistem informasi memiliki risiko bermacam hal seperti kegagalan kelistrikan karena faktor alam, *human error*, kehilangan data karena *hacker*, kerusakan sistem disebabkan virus, kebakaran dan lainnya. Risiko tersebut dapat dikendalikan menggunakan manajemen risiko [2].

Manajemen risiko adalah bidang penegtahuan yang mempelajari bagaimana suatu organisasi atau perusahaan menggunakan pengukuran untuk memetakan risiko yang ada dari aplikasi kompleks dan pendekatan manajemen yang berbeda secara komperhensif dan teratur [3]. Adapun menurut [4] manajemen risiko merupakan strategi sistematis untuk mengelola ketidakpastian yang berhubungan dengan permasalahan atau urutan aktivitas manusia, yang meliputi evaluasi risiko, merancang strategi pengelolaan risiko, dan meminimalkan risiko lewat pengelolaan sumber daya. Manajemen risiko juga digunakan untuk landasan dalam penanganan risiko, perencanaan risiko, dan pengambilan keputusan oleh pimpinan suatu organisasi [16]. Adapun tujuan dari manajemen risiko agar mengurangi atau meminimalisir adanya kemungkinan kesalahan yaitu dengan cara dihadapi dan dimitigasi terhadap teknologi informasi tersebut [13]. Manfaat penerapan manajemen risiko salah satunya untuk dapat mengukur kinerja dan mendukung efektivitas kerja dari sebuah organisasi [15].

PT. XYZ merupakan sebuah perusahaan yang bergerak pada bidang pengolahan buah sawit mentah. Dalam menunjang proses bisnis yang ada di perusahaan, PT. XYZ menggunakan sistem informasi pengolahan data. Salah satu Sistem Informasi yang di gunakan adalah Sistem pengolahan data *Accurate*. Sistem

pengolahan data *Accurate* merupakan Sistem untuk penimbangan buah sawit yang masuk bersama dengan mobil truk, dan juga sistem ini mengolah seluruh laporan yang ada di PT. XYZ. Sistem pengolahan data *Accurate* ini dapat diakses tiap admin staf bagian dan juga kepala gudang dengan cara login terlebih dahulu dengan menggunakan ID yang telah ditentukan. Sistem pengolahan data *Accurate* ini telah digunakan oleh PT.XYZ sejak tahun 2012 dengan user sebanyak 4 orang. Dalam penerapan sistem pengolahan data Accurate selama 11 tahun pernah terjadi ancaman yang memberikan dampak bagi PT. XYZ.

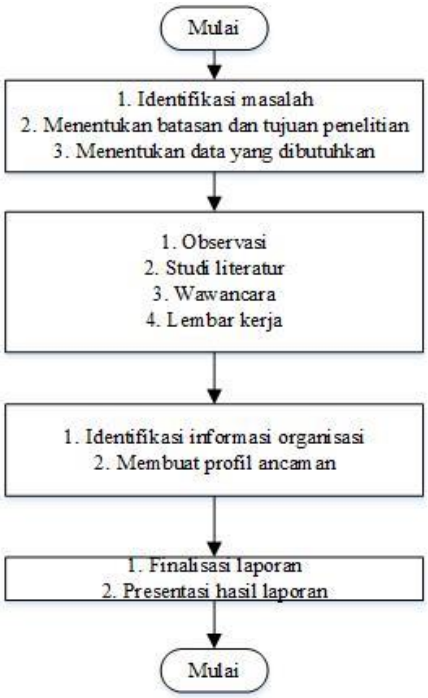
Berdasarkan observasi dan wawancara yang dilakukan di PT. XYZ, permasalahan yang sering terjadi pada Sistem pengolahan data *Accurate* adalah human error. Sering kali terjadi kesalahan input data oleh admin dan menyebabkan kesalahan order. Hal tersebut berpengaruh pada order pembelian kebutuhan pabrik dan rekapan pengeluaran dikeuangan. Kemudian adanya risiko *connection error* pada sistem yang disebabkan oleh jaringan internet down yang sering terjadi hampir setiap tahun dan hal ini dapat menghambat produktivitas kinerja admin pegawai, dan kejadian listrik mati yang kadang kala muncul sehingga dapat mengganggu proses kerja karyawan yang menggunakan sistem pengolahan data *Accurate* ini. Namun tidak dapat dihindari bahwa akan ada risiko dan ancaman lain yang dapat mengganggu proses bisnis dan operasional serta menyebabkan kerugian yang lebih besar pada PT.XYZ. Untuk mengurangi peristiwa terjadinya ancaman ataupun risiko teknologi , dilakukan sebuah analisa risiko Sistem Pengolahan Data *Accurate* yang ada pada PT.XYZ dengan tujuan untuk mengidentifikasi adanya risiko dalam penggunaan sistem tersebut, serta membuat perencanaan penanganan risiko terhadap risiko keamanan sistem pengolahan data *Accurate* yang tepat dan sesuai. Untuk merealisasikannya diperlukan sebuah kerangka kerja yang sesuai untuk mengetahui risiko keamanan informasi yang digunakan ada banyak metode penilaian risiko yang tersedia, diantaranya tuntunan untuk melakukan Penilaian Risiko (Institut Nasional Standard dan teknologi (NIST) 2012, ISO 27001 [10], FMEA [11], COBIT [14], dan OCTAVE [5]. Menurut Carnegie Mellon Software Engineering Institute metode OCTAVE-S yang merupakan pengembangan dari metode OCTAVE merupakan salah satu cara yang efektif mengurai sebuah gambaran secara menyeluruh terhadap keamanan informasi yang dibutuhkan oleh organisasi. Selain itu digunakan juga sebagai praktek keamanan informasi dan strategi keamanan informasi.

Metode OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation-Small*) ialah model dari pendekatan OCTAVE yang dikembangkan untuk memenuhi kebutuhan organisasi kecil dan kurang hierarkis. Hal ini membutuhkan analisis dari sebuah kelompok untuk melihat risiko keamanan pada aset organisasi terhadap tujuan bisnis. Dengan menerapkan hasil OCTAVE-S, maka sebuah organisasi berusaha untuk melindungi semua informasi lebih baik lagi dan meningkatkan bagian keamanan informasi secara keseluruhan. Dalam pelaksanaannya OCTAVE-S juga dapat membantu dalam melakukan evaluasi risiko, identifikasi aset TI yang penting sesuai organisasi, juga melakukan identifikasi kerentanan dan ancaman terhadap aset TI tersebut serta melakukan evaluasi potensi jika ancaman tersebut terjadi [9].

Metode OCTAVE-S ini dapat memberikan masukan untuk manajemen sistematis ancaman keamanan sistem informasi dan juga dapat mencakup semua aktivitas dengan memiliki 3 fase, 5 proses, 16 aktivitas Serta 30 langkah yang dapat membantu proses pengelolaan risiko keamanan dalam sebuah organisasi [2]. Dalam penelitian ini digunakan fase 1 dengan 2 proses. Dengan melakukan analisis risiko keamanan pada sistem pengolahan data *Accurate* di PT.XYZ diharapkan dapat mengetahui seberapa besar tingkat keamanan sistem yang bisa meningkatkan efektivitas dan efisiensi kerja perusahaan.

2. METODOLOGI PENELITIAN

Pada Gambar 1. Merupakan alur dari penelitian yang akan dilakukan pada PT. XYZ dimulai dari perencanaan, pengumpulan data, analisis, dan dokumentasi akhir penelitian.



Gambar 1. Alur dari penelitian

3. HASIL DAN PEMBAHASAN

3.1. Analisis Risiko

Analisis risiko dilakukan untuk mengetahui tingginya risiko yang memiliki dampak pada instansi dan teknologi informasi yang digunakan [19]. Penilaian dilaksankan berdasarkan lembar kerja metode OCTAVE-S, dan pengumpulan data dilakukan dengan cara memberikan lembar kerja kepada tim yang sudah dibentuk yang berasal dari bagian admin staf penimbangan, admin staf pengolahan buah sawit dan kepala gudang.

Adapun yang menjadi responden yang dipilih oleh peneliti berdasarkan RACI *Chart* [18]. Responden lembar kerja adalah orang-orang yang terlibat pada proses

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 675-685
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

pengelolaan sistem. Dalam hal ini keseluruhan responden mendapatkan perlakuan yang sama dalam dalam pengisian data kusioner sebelum nantinya akan diolah.

Tabel 1. *RACI Chart* Responden

Peranan / Aktivitas	Penanggung jawab IT	Kepala Gudang	Admin staf penimbangan	Admin staf pengolahan buah
1. Mengidentifikasi dan mengelola sistem *Accurate*	A	R/A	C/I	C/I
2. Mengelola, mengoperasikan dan mengevaluasi kegiatan IT	A	R	C/I	C/I
3. Memutuskan dan menyetujui serta bertanggung jawab atas pekerjaan staf	R/A/I	R/I	I	I
4. Memelihara sistem, jaringan, server dan memberikan rekomendasi untuk perbaikan	A/I	R	R	R

Pada Tabel 1. diatas merupakan *RACI Chart* dari responden yang akan mengisi lembar kerja dalam penelitian ini.

3.2. Identifikasi Informasi Organisasi

Penilaian risiko dimulai dari proses mengidentifikasi informasi dari PT.XYZ, agar dapat diketahui tingkat risiko yang dapat berdampak pada keberlangsungan kegiatan bisnis perusahaan serta untuk mendapatkan perencanaan tindakan risiko. Pada proses ini terdapat 3 aktifitas yang akan dilaksanakan untuk mengimpun data dan dilakukan menggunakan lembar kerja yang ada pada OCTAVE-S [20].

3.2.1. Membangun Dampak Dari Kriteria Evaluasi

Pada proses ini dilakukan pengumpulan data untuk aktifitas membangun dampak risiko dari kriteria evaluasi pada lembar kerja OCTAVE-S yang digunakan sebagai penilaian kriteria dampak risiko pada PT.XYZ. Adapun data yang didapat bisa dilihat pada Tabel 2 yaitu sebagai berikut:

Tabel 2. Data Identifikasi Risiko dari kriteria Dampak Evaluasi

No	Kriteria Dampak	Tipe/Dampak	Level
1	Reputasi dan Kehilangan Data	Reputasi	Rendah
		Kehilangan Data	Sedang
2	Keuangan	Biaya Operasional	Rendah
		Kehilangan Pendapatan	Rendah

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 675-685
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

No	Kriteria Dampak	Tipe/Dampak	Level
3	Produktivas	Jam Kerja	Sedang
4	Kesehatan/ Keselamatan	Kesehatan/Keselamatan Pegawai	Rendah

3.2.2. Mengidentifikasi Aset Organisasi

Pada tahap ini dilaksanakan pengumpulan data untuk aktifitas identifikasi aset instansi pada lembar kerja OCTAVE-S yang digunakan sebagai penilaian pada aset yang berada pada PT.XYZ. Adapun data yang diperoleh dapat dilihat sebagai berikut:

Tabel 3. Data Aset Instansi

Sistem	Informasi	Aplikasi/Layanan
Accurate	Informasi penimbangan buah masuk, data pengolahan buah di dalam pabrik, laporan data buah sawit	Server, Jaringan Internet, PC

Tabel 4. Data Aset Instansi

Sumber Daya Manusia	
Jabatan	Keahlian
Penanggung Jawab IT	Bagian Penanggung Jawab IT dipilih karena memiliki tanggung jawab dalam pengelolaan IT yang digunakan di lingkungan Stasiun PT.XYZ

3.2.3. Mengevaluasi Praktek Keamanan Organisasi

Untuk melaksanakan penilaian pada bagian praktek keamanan dilakukan berdasarkan status stoplight dengan berdasarkan hasil pengisian lembar kerja, yang dapat dilihat sebagai berikut:

Tabel 5. Definisi Tingkat Risiko dan Status Stoplight

Tingkat Level	Nilai Dampak	Status Stoplight	Deskripsi Tingkat Risiko dan Tindakan Diperlukan
RENDAH (Low)	**1**	**GREEN**	Jika pengamatan dinilai sebagai risiko rendah maka dapat dikatakan bahwa organisasi telah melakukan praktik keamanan di area dengan baik, maka tindakan perbaikan tidak perlu dilakukan.
SEDANG (Medium)	**2-3**	**YELLOW**	Jika hasil pengamatan dinilai sebagai risiko sedang maka dapat dik- atakan bahwa organisasi telah menjalankan praktik keamanan hanyadi area tertentu saja, maka ada celah kemungkinan tindakan perbaikan perlu dilakukan.
TINGGI (High)	**4-5**	**RED**	Jika hasil pengamatan dinilai sebagai risiko tinggi maka dapat dika- takan bahwa organisasi tidak melakukan praktik keamanan di area tersebut, maka tindakan perbaikan perlu dilakukan.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 7 Nomor 2, September 2023, pp. 675-685
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Tabel 6. Evaluasi Praktek Keamanan Instansi

No.	PRAKTEK KEAMANAN	STOPLIGHT		
		RED	YELLOW	GREEN
1.	Kesadaran Keamanan dan Pelatihan			[x]
2.	Strategi Keamanan		[x]	
3.	Manajemen Keamanan		[x]	
4.	Peraturan dan Kebijakan Keamanan		[x]	
5.	Manajemen Keamanan dan Kolaborasi			[x]
6.	Perencanaan Contingency			[x]
7.	Pengendalian Akses Fisik			[x]
8.	Pemantauan dan Audit Keamanan Fisik			[x]
9.	Sistem dan Manajemen Jaringan		[x]	
10.	Pemantauan dan Audit Keamanan IT	[x]		
11.	Pengesahan dan Otoritas	[x]		
12.	Manajemen Kerentanan	[x]		
13.	Enkripsi	[x]		
14.	Perencanaan dan Arsitektur Keamanan	[x]		
15.	Manajemen Insiden	[x]		

Terlihat pada Tabel 6. terdapat enam praktek keamanan PT.XYZ yang berada pada status stoplight *Red* yang menyimpulkan PT.XYZ belum melaksanakan praktek keamanan pada bagian tersebut, dan empat praktek keamanan berada pada status *Yellow* hal ini menyimpulkan PT.XYZ sudah menerapkan praktek keamanan namun belum cukup baik, dan lima praktek keamanan berada pada status *Green* yang menyimpulkan PT.XYZ sudah melaksanakan praktek keamanan tersebut dengan baik. Adapun analisis pada praktek keamanan dengan lembar kerja pada PT.XYZ dilihat melalui indikator praktek keamanan penggunaan teknologi informasi.

1. Kesadaran Keamanan dan Pelatihan

Melalui pengukuran yang dilakukan melalui lembar kerja untuk melihat tingkat kesadaran karyawan terhadap keamanan dan pelatihan sistem yang dipakai maka memperoleh hasil bahwa PT.XYZ berada pada status stoplight *green*, hal ini disebabkan para karyawan sudah paham tentang pentingnya suatu keamanan.

2. Strategi Keamanan

Salah satu bagian yang menjadi pertimbangan yakni strategi keamanan dan kebijakan. Strategi keamanan telah didokumentasikan oleh pihak perusahaan namun kurang dilakukan peninjauan, karena faktor ini indikator strategi keamanan berada pada status stoplight *yellow*.

3. Manajemen Keamanan

Pada indikator Manajemen Keamanan PT. XYZ berada pada status stoplight *yellow*, hal ini disebabkan PT. XYZ menyalurkan sumber daya yang cukup, mendefinisikan peran keamanan dan tanggung jawab kepada semua admin staf. Namun, tugas dan tanggung jawab pada penjagaan informasi tersebut belum terdokumentasi.

4. Peraturan dan Kebijakan Keamanan

Dari indikator Peraturan Keamanan PT. XYZ berada pada status stoplight *yellow*, itu disebabkan telah dilakukan pembuatan SOP tentang kebijakan serta cara pelaksanaannya namun belum sering dilakukan.

5. Manajemen Keamanan dan Kolaborasi

Indikator Manajemen Keamanan dan Kolaborasi memiliki status stoplight *green*, karena PT. XYZ sudah memiliki prosedur dalam setiap pelaksanaan kerja sama dengan pihak ketiga.

6. Perencanaan Contingency

Perencanaan contingency berada pada status stoplight *green*, hal itu disebabkan karena PT. XYZ sudah menentukan pihak yang memiliki tanggung jawab, seandainya sebuah ancaman terjadi.

7. Pengendalian Akses Fisik

Indikator Pengendalian Akses fisik berada pada status stoplight *green*, hal ini karena instansi telah melakukan pengendalian akses fisik dengan baik, dapat dibuktikan dengan adanya pengamanan dalam akses ke area informasi sensitif, seperti amin staf yang mendapatkan akun asing-masing dengan password yang berbeda satu sama lain.

8. Pemantauan dan Audit Keamanan Fisik

Pemantauan dan Audit Keamanan Fisik instansi berada pada status stoplight *green*, hal ini dikarenakan PT. XYZ telah melakukan *backup* data maupun informasi yang ada pada sistem secara rutin yakni setiap 1 bulan sekali.

9. Sistem dan Manajemen Jaringan

Indikator Sistem dan Manajemen Jaringan berada pada status stoplight *yellow*, ini disebabkan oleh adanya pemantauan pada permasalahan koneksi yang terjadi namun tidak ada dokumen yang berisi mengenai hasil atau keadaan jaringan pada PT. XYZ.

10. Pemantauan dan Audit Keamanan TI

Indikator Pemantauan dan Audit Keamanan TI berada pada status stoplight *red*, ini karena instansi belum melakukan pemantauan terhadap hardware, dan PT. XYZ juga tidak melaksanakan pemeliharaan terhadap sistem pengolahan data *Accurate* secara berkala, karena *maintenance* dilakukan hanya pada saat terjadi masalah saja.

11. Pengesahan dan Otoritas

Pengesahan dan Otoritas berada pada status stoplight *red*, hal ini karena pemahaman otoritas dibagian admin staf masih tidak ada.

12. Manajemen Kerentanan

Indikator Manajemen Kerentanan berada pada status stoplight *red*, hal tersebut karena pihak perusahaan belum melaksanakan penilaian terhadap keretanan teknologi informasi yang dimiliki.

13. Enkripsi

Enkripsi berada pada status stoplight *red*, hal tersebut disebabkan karena PT. XYZ belum adanya kebijakan perihal enskripsi didalam perusahaan.

14. Perancangan dan Arsitektur Keamanan

Perancangan dan Arsitekrut Keamanan berada pada status stoplight *red*, hal tersebut karena dalam melaksanakan perancangan keamanan pihak ketiga yang terlibat dalam hal tersebut tidak seluruhnya terikat dengan kontrak.

15. Manajemen Insiden

Indikator Manajemen Insiden berada pada status stoplight *red*, hal ini disebabkan tidak adanya dokumen yang mencatat mengenai insiden terkait teknologi informasi yang digunakan.

3.3. Rekomendasi Hasil Analisis

Analisis praktik keamanan pada PT.XYZ memiliki 6 praktik keamanan yang berada pada status *red* yaitu dapat dikatakan bahwa instansi tidak melakukan praktik keamanan pada area tersebut, maka perlu dilakukan tindakan perbaikan. Berikut merupakan daftar tindakan risiko terhadap praktik keamanan pada yang dapat digunakan kedepannya, dapat dilihat sebagai berikut:

Tabel 7. Daftar Tindakan Risiko

No.	Praktek Keamanan	Tindakan Risiko
1.	Pemantauan dan Audit Keamanan TI	Melakukan pemantauan dan audit berkala terhadap sistem dan jaringan di dalam instansi
2.	Pengesahan dan Otoritas	Lakukan pengelolaan dengan baik sesuai dengan kebijakan yang ada
3.	Manajemen Kerentanan	Terapkan langkah-langkah untuk mengelola tingkat kerentanan pada instans serta lakukan penilaian kerentanan sistem pengolahan data *Accurate* secara teratur
4.	Enkripsi	Menerapkan manajemen keamanan sesuai kebutuhan instansi serta lindungi sensitivitas informasi
5.	Perancangan dan Arsitektur Keamanan	Mengelola sistem desain yang digunakan oleh instansi dan menerapkan arsitektur keamanan yang baik
6.	Manajemen Insiden	Pelaksanaan prosedur yang di dokumentasikan oleh instansi untuk mengidentifikasi , melaporkan, dan menindaklanjuti dugaan insiden dan pelanggaran keamanan

4. SIMPULAN

Berdasarkan analisis yang dilaksanakan pada keamanan sistem pengolahan data *Accurate* di PT. XYZ, dapat ditarik beberapa kesimpulan dari proses identifikasi informasi perusahaan terdapat tiga indikator dampak yang berada pada level sedang yaitu reputasi, kehilangan data serta jam kerja. Dan dari proses identifikasi aset instansi diketahui bahwa PT.XYZ mempunyai aset kritis yakni Sistem Pengolahan Data *Accurate*. Terdapat 6 praktek keamanan PT. XYZ yang berada pada status stoplight *Red* yaitu Pemantauan dan Audit Keamanan IT, Pengesahan dan Otoritas, Manajemen Kerentanan, Enkripsi, Perencanaan dan Arsitektur Keamanan, Manajemen Insiden. Kemudian terdapat 4 praktek keamanan berada pada status *Yellow* yaitu Strategi Keamanan, Manajemen Keamanan, Peraturan dan Kebijakan Keamanan, Sistem dan Manajemen Jaringan.

Kemudian 5 praktek keamanan berada pada status *Green* yaitu Kesadaran Keamanan dan Pelatihan, Manajemen Keamanan dan Kolaborasi, Perencanaan Contingency, Pengendalian Akses Fisik, Pemantauan dan Audit Keamanan Fisik.

DAFTAR PUSTAKA

[1] Wardiana, W. (2002). "Perkembangan Teknologi Informasi di Indonesia". Seminar dan Pameran Teknologi Informasi.

[2] Mahersmi, B. (2016). "Analisis Risiko Dengan Menggunakan Metode Octave Dan Kontrol Iso 27001 Pada Dinas Perhubungan Komunikasi Dan Informatika Kabupaten Tulungagung". Final Project Institut Teknologi Sepuluh Nopember.

[3] Aisha, L., dkk. (2016). "Perancangan Tata Kelola Manajemen Layanan Teknologi Informasi Menggunakan ITIL V3". Service Operation di Pemerintahan Kota Bandung.

[4] Norken, I., Purbawijaya, I., dan Suputra, I. (2015). "Pengantar analisis dan manajemen risiko pada proyek konstruksi". Denpasar: Udayana University Press.

[5] Fahmi, I., dan Mulia, S. (2011). "Analysis of financial performance in a form of financial ratio before and after right issue at the indonesia's stock exchange (bursa efek indonesia)". International Journal of Business and social science.

[6] Alberts, C., Dorofee, A., Stevens, J., dan Woody, C. (2005). "Octave-s implementation guide, version 1.0". Manuel e´lectronique. Pittsburg, PA: Software Engineering Institute, Carbegie Mellon University.

[7] Nyoman, B., Indrawan, G., Gunadi, A. (2022). "Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Dan Analytical Hirarchy Process Pada Data Center Pemerintah Kabupaten Buleleng". Jurnal Ilmu Komputer Indonesia (JIK), Vol. 7, No. 1.

[8] Supradono, B. (2009). "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat, Asset, And Vulnerability Evaluation)". Media Elektrika, Vol. 2, No. 1.

[9] Rivai, A., Suroso, J., Pangemanan, F. (2020). "ICIMTech 2020: proceedings of 2020 International Conference on Information Management and Technology". ICIMTech.

[10] Moteff, J. (2005). "Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences". Library of Congress Washington DC Congressional Research Service.

[11] Budiarto, R. (2017). "Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA Dan ISO 27001 Pada Organisasi XYZ". CESS (Journal of Computer Engineering System and Science), Vol. 2, No. 2.

[12] Cahyabuana, B., Pribadi, A. (2020). "Konsistensi Penggunaan Metode FMEA (Failure Mode Effects and Analysis) terhadap Penilaian Risiko Teknologi Informasi (Studi kasus: Bank XYZ)". Institut Teknologi Sepuluh Nopember (ITS).

[14] Perdana, T. (2018). "Manajemen Resiko Keamanan Informasi pada Kantor Pelayanan Pajak Menggunakan METODE FMEA Dan ISO 27001". Sriwijaya University.

[15] Mutiah, N., Rusi, I., Tutik. (2022). "Analisis Dan Manajemen Risiko Keamanan Informasi Menggunakan Metode Failure Mode And Effects Analysis (FMEA) Dan Kontrol ISO/IEC 27001:2013 (Studi Kasus : Dinas Komunikasi Dan Informatika Kabupaten Sambas)". Jurnal Komputer dan Aplikasi, Vol. 10, No. 02.

[16] Novitasari, B., Tanaamah, A. (2021). "Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma)". Journal of Information Systems and Informatics, Vol. 3, No. 3.

[17] Tupa, J., Simota, J., Steiner, F. (2017). "Aspects of Risk Management Implementation for Industry 4.0." Procedia Manufacturing.
[18] Oliveira, E., dkk. (2017). "The ISO 31000 Standard in Supply Chain Risk Management." Journal of Cleaner Production.
[19] Ambarwati, A., Rusady, R. (2017). "Analisis Implementasi Teknologi Informasi pada Domain Deliver And Support di PT. RDPI". Jurnal INFORM, Vol. 2, No. 2.
[20] Nisa, F., dkk. (2022). "Analisis Manajemen Risiko Keamanan Sistem Bmkgsoft Menggunakan Metode OCTAVE-S". Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 8, No. 1.
[21] Setyawan, A., Wijaya, A. (2018). "Analisis Manajemen Risiko Teknologi Informasi Pada Diskominfo Kota Salatiga Menggunakan Metode OCTAVE-S". Seminar Nasional Sistem Informasi Indonesia.