KREA-TIF: JURNAL TEKNIK INFORMATIKA
http://ejournal.uika-bogor.ac.id/index.php/krea-tif
p-ISSN: 2338-2910, e-ISSN: 2658-5836
Vol. 11, No. 1, Mei 2023, pp. 37 – 52
DOI: 10.32832/krea-tif.v11i1.14179

Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House

Phillbert Nevin Emmanuel[1], Raymond Maulany[1,2]
[1]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Advent Indonesia, Indonesia
[2]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Advent Indonesia, Indonesia
*E-mail koresponden: nevinphilbert15@gmail.com

***Diserahkan** 1 Mei 2023; **Direview** 1 Juli 2023; **Dipublikasikan** 1 Agustus 2023*

Abstrak

Penerapan sistem informasi merupakan salah satu bentuk pemanfaatan teknologi informasi oleh suatu organisasi untuk mendukung proses bisnisnya. Seiring dengan penggunaan sistem informasi, terjadinya risiko yang dapat berdampak negatif pada proses bisnis yang dijalankan tidak dapat dihindari. Penilaian risiko diperlukan agar organisasi dapat memberlakukan pengendalian guna meminimalisir dampak negatif dari risiko pada sistem informasi yang dapat merugikan organisasi berdasarkan impact area seperti reputasi, keuangan/finansial, kelancaran produktivitas, keselamatan dan kesehatan, serta denda dan penalti. Metode penilaian risiko yang digunakan dalam penelitian ini adalah OCTAVE Allegro. Data penelitian dikumpulkan dengan menggunakan teknik observasi dan wawancara dengan manajer tingkat senior dan kepala departemen IT, kemudian diolah dengan mengikuti kaidah-kaidah yang terdapat dalam kerangka kerja OCTAVE Allegro. Hasil akhir yang diperoleh adalah identifikasi atas lima aset informasi, empat container, dan 13 area of concern dimana tujuh di antaranya memiliki status yang memerlukan perencanaan mitigasi, sedangkan enam lainnya dapat ditangguhkan. Untuk mengurangi kerusakan yang dapat disebabkan, diberikan perencanaan kontrol strategis berdasarkan referensi annex ISO/IEC 27001:2013. Perencanaan kontrol ini dapat menjadi acuan mengenai manajemen risiko dan membantu organisasi terkait dalam meningkatkan keamanan informasi.

Kata kunci: *Keamanan Informasi, Manajemen Risiko, OCTAVE Allegro, Penilaian Risiko.*

Abstract

The application of information systems is a form of utilizing information technology by an organization to support its business processes. Along with the use of information systems, the occurrence of risks that can have a negative impact on the business processes being carried out is unavoidable. Risk assessment is needed so that the organization can implement controls to minimize the negative impact of risks on information systems that can be detrimental to the organization based on impact areas such as reputation, finance/financial, smooth productivity, safety and health, as well as fines and penalties. The risk assessment method used in this study is OCTAVE Allegro. Research data were collected using observation and interview techniques

with senior level managers and information system administrators, then processed according to the principles contained in the OCTAVE Allegro framework. The final result obtained is the identification of five information assets, four containers, and thirteen areas of concern where seven of them have a status that requires a mitigation plan, while the other six can be deferred. To reduce the damage that can be caused, a strategic control plan is provided based on the ISO/IEC 27001:2013 annex reference. This control plan can reference risk management and assist related organizations in improving information security.

Keywords: *Information Security, OCTAVE Allegro, Risk Assessment, Risk Management* .

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat di berbagai bidang menyebabkan penggunaannya diharuskan untuk lebih dapat menyesuaikan kegunaannya terhadap kebutuhan gaya dan pola hidup masyarakat [1]. Pemanfaatan teknologi informasi kini telah menjadi suatu hal yang penting bagi suatu organisasi jika organisasi tersebut memiliki keinginan untuk beroperasi secara efisien dan efektif dengan tujuan menguatkan tingkat produktivitas yang dimiliki [2]. Penggunaan sistem informasi merupakan salah satu upaya untuk mengefisienkan pemakaian serta pengelolaan data dan informasi agar dapat dimanfaatkan secara maksimal oleh setiap unit bisnis di dalam suatu organisasi. [3]. Dengan memanfaatkan dan mengoptimalkan perkembangan teknologi informasi secara baik dan benar, maka organisasi dapat memanfaatkan seluruh sumber daya yang dimiliki secara maksimal, sehingga dapat memiliki keunggulan kompetitif dibanding kompetitornya [3,4]. Namun dengan semakin berkembangnya suatu aset teknologi informasi dan pemanfaatannya, tentunya selalu ada kemungkinan terjadinya risiko yang membayang-bayangi dan mengancam organisasi dalam mencapai tujuannya [4].

Risiko merupakan konsekuensi yang dapat memberikan dampak negatif (merugikan atau berbahaya) dari suatu aktivitas yang telah dilakukan maupun akan dilakukan [5]. Risiko terjadi karena adanya kondisi yang menciptakan suatu ketidakpastian, misalnya investasi dapat mendatangkan keuntungan (kenaikan nilai) dan dapat juga menimbulkan kerugian (penurunan nilai) [6]. Risiko dalam pengelolaan sistem informasi dapat diklasifikasikan menjadi beberapa jenis, yaitu; risiko karyawan, risiko aset fisik, dan risiko hukum [7, 8, 9]. Beberapa penelitian telah membuktikan bahwa pemanfaatan sistem informasi pada suatu organisasi rentan terhadap jenis-jenis risiko tersebut dan kemungkinan terjadinya suatu risiko tidak dapat dihindar [6, 7, 8, 9]. Oleh karena itu, semua organisasi perlu melakukan manajemen risiko untuk menghindari dan meminimalisir dampak kerugian yang disebabkan oleh suatu risiko tersebut [5, 6, 7, 8, 9, 10].

Manajemen risiko dapat didefinisikan sebagai suatu kumpulan prosedur yang dilakukan di dalam suatu organisasi untuk memberikan hasil yang paling menguntungkan dan meminimalisir ketidakpastian atau fluktuasi terhadap *output* yang dihasilkan [8]. Manajemen risiko dapat dilakukan jika penilaian risiko dilakukan terlebih dahulu terlebih dahulu. Penilaian risiko merupakan proses mengidentifikasi potensi ancaman terhadap suatu aktivitas atau proses bisnis, menganalisa probabilitas dan tingkat kerusakan yang dapat disebabkan, dan mengembangkan langkah-langkah mitigasi untuk mengelola risiko tersebut dengan tujuan mengurangi dampak negatif dan memastikan setiap risiko yang tidak dapat dihindari dapat dikelola dengan baik [6, 8, 10].

Indonesia Publishing House (IPH) adalah sebuah lembaga penerbit dan percetakan yang beroperasi di Bandung, Jawa Barat, Indonesia, di bawah naungan Uni Indonesia Kawasan Barat (UIKB) dan Uni Indonesia Kawasan Timur (UIKT) [11]. IPH tengah mengembangkan dan

melakukan uji coba penerapan aplikasi sistem informasi *Enterprise Resource Planning* (ERP) pada skala industri menengah ke bawah yang mengintegrasikan fungsi tiap-tiap departemen di dalam organisasi. Pemanfaatan sistem informasi ini diharapkan dapat menciptakan suatu aliran informasi yang dinamis, segera, dan transparan baik dalam organisasi maupun dengan mitra-mitra kerjanya guna meningkatkan efektifitas dan efisiensi produktivitas dan nilai organisasi secara keseluruhan [12, 13].

Berdasarkan hasil observasi langsung terhadap sistem informasi dan wawancara dengan kepala departemen IT di IPH, didapati bahwa IPH belum pernah melakukan penilaian risiko terhadap pemanfaatan teknologi informasi yang dilakukan, sehingga organisasi belum memiliki kebijakan dalam melakukan antisipasi terhadap terjadinya risiko dan manajemen risiko yang baik. Oleh karena itu, dibutuhkan kesadaran untuk melakukan penilaian risiko terhadap pemanfaatan teknologi informasi yang dilakukan, agar organisasi dapat menerapkan manajemen risiko yang baik sebagai upaya untuk menghindari dan meminimalisir dampak kerugian yang dapat terjadi [6, 8, 10].

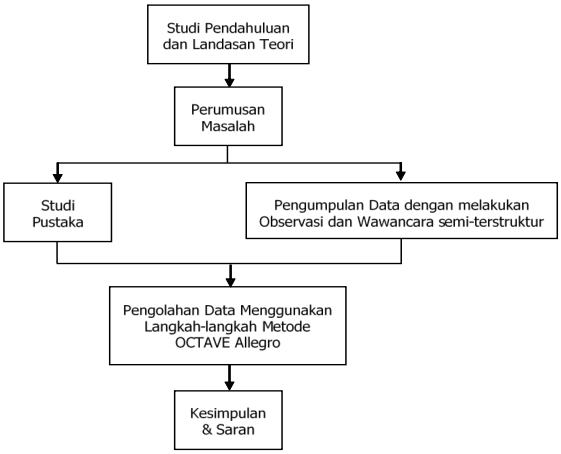
Terdapat beberapa kerangka/metode penilaian risiko yang dapat digunakan untuk mengukur layanan manajemen risiko. Penelitian ini menggunakan metode OCTAVE generasi terbaru sebagai pedoman dan acuan penilaian risiko yaitu OCTAVE Allegro, dimana metode ini memiliki penekanan yang lebih spesifik terhadap keamanan aset informasi dan data pendukung informasi [14]. Berdasarkan penelitian-penelitian serupa yang terdahulu, metode ini juga terbukti dapat menghasilkan penilaian risiko yang cukup baik hanya dengan investasi finansial dan waktu yang tergolong minim, terutama untuk organisasi yang belum memiliki manajemen risiko yang mumpuni terhadap sistem informasi yang dijalankan [15]. Metode OCTAVE Allegro sudah banyak digunakan pada berbagai macam organisasi, seperti perusahaan swasta, perpustakaan, institut pendidikan, instansi pemerintah, dan lain-lain [5, 10, 14]. Penelitian ini dapat memiliki acuan yang dibutuhkan untuk dilakukan berdasarkan penelitian serupa yang terdahulu, perbedaannya berada pada objek yang diteliti, yaitu sistem informasi yang dikelola oleh organisasi penerbit dan percetakan buku.

Tujuan dari penelitian ini merupakan pemberian rekomendasi perencanaan strategis/kontrol berdasarkan standar ISO/IEC 27001:2013 mengenai keamanan informasi [16] terhadap risiko yang telah diidentifikasi dan dievaluasi dengan mengikuti kaidah-kaidah penilaian risiko metode OCTAVE Allegro. Manfaat dari penelitian ini adalah agar organisasi dapat memiliki pemahaman yang cukup dan acuan berdasarkan standar yang telah teruji untuk melakukan pengelolaan atas risiko-risiko tersebut. Penting untuk diingat bahwa setiap metode penilaian risiko memiliki kelebihan dan keterbatasan masing-masing, dan pilihan metode terbaik tergantung pada konteks, tujuan penelitian, dan ketersediaan data yang relevan. Penilaian risiko dapat dikatakan "baik" jika memenuhi beberapa faktor seperti memenuhi standar kualitas data, metodologi analisis yang tepat, melibatkan pemangku kepentingan yang relevan, menggunakan pengetahuan dan metrik pengukuran yang relevan, serta menggunakan pendekatan yang konsisten dan transparan. Kombinasi dari beberapa metode juga sering digunakan untuk menghasilkan penilaian risiko yang lebih komprehensif dan dapat diandalkan

METODE PENELITIAN

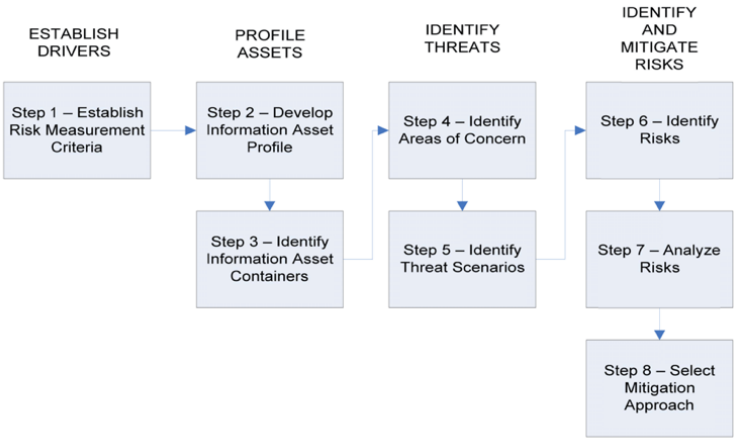
Sistematika penelitian dimulai dengan studi pendahuluan melalui referensi buku dan sumber lainnya untuk mengumpulkan informasi mengenai pengertian dan landasan teori yang diperlukan dari tema penelitian, kemudian melakukan perumusan masalah untuk menentukan identifikasi masalah, manfaat dan tujuan penelitian, serta ruang lingkup dan batasan masalah dari penelitian. Dilanjutkan dengan studi pustaka melalui laporan teknis dan penelitian-

penelitian dari bidang yang sama dari media cetak maupun media *online*/*internet* dengan pengumpulan data menggunakan teknik observasi secara langsung pada objek penelitian dan wawancara secara semi-terstruktur dengan memberikan pertanyaan yang disusun berdasarkan laporan teknis kerangka kerja OCTAVE Allegro [14] kepada manajer tingkat senior dan administrator sistem informasi dari IPH. Tahapan penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Sistematika Penelitian

Pertanyaan-pertanyaan kunci yang disusun dapat dikembangkan secara lebih lanjut selama sesi wawancara berlangsung agar peneliti dapat memiliki pemahaman lebih dalam sehubungan dengan indikator risiko terhadap *impact area*, sumber-sumber informasi dan individu-individu siapa saja yang terlibat dalam kepengurusan aset informasi organisasi. Data berupa jawaban-jawaban dari narasumber didokumentasikan ke dalam *worksheet-worksheet*, dan diolah dengan mengikuti kaidah-kaidah metode penilaian risiko OCTAVE Allegro pada Gambar 2 [14].



Gambar 2. Peta Jalan Framework OCTAVE Allegro

OCTAVE Allegro

Metode ini terbagi atas empat fase, yaitu:

1. Mengembangkan Penggerak

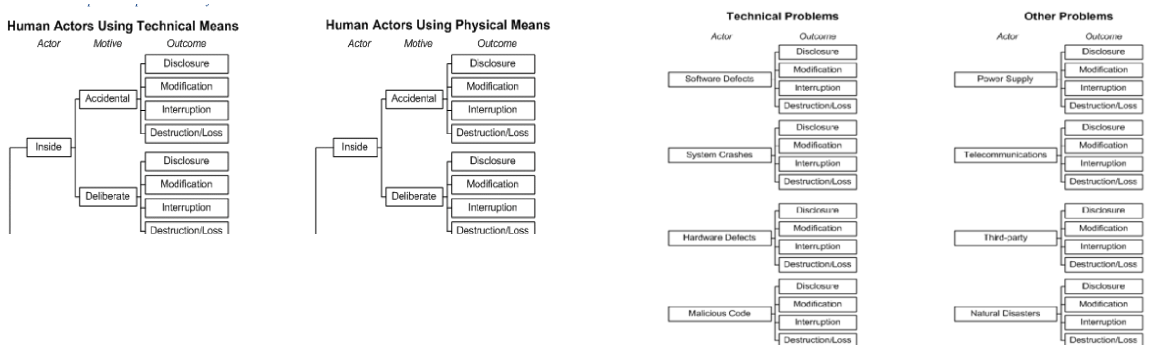
   Kriteria pengukuran risiko dikembangkan untuk mengevaluasi dampak risiko pada penggerak organisasi yang konsisten terhadap hal-hal yang membuat organisasi tetap bergerak *(organizational drivers)* yang dikategorikan menjadi lima; reputasi, finansial, produktivitas, keselamatan dan kesehatan, serta denda dan penalti. Kemudian diklasifikasikan tingkat kerusakannya menjadi *low, moderate* dan *high* [14].

2. Profil Aset

   Dimana aset informasi yang menjadi fokus penilaian risiko beserta *container*-nya diidentifikasi dan diprofilkan. Profil adalah representasi yang menggambarkan fungsi, karakteristik, dan kualitas serta nilai unik dari aset informasi [14], dan *container* merupakan media yang digunakan untuk menyimpan, mengirim dan memproses aset informasi [14]. Pengembangan profil aset informasi organisasi beserta *container*-nya dilakukan untuk menggambarkan aset informasi yang kritikal bagi proses bisnis secara lebih spesifik dan konsisten, menggambarkan dimana dan bagaimana aset tersebut disimpan dan diproses, serta mendefinisikan batasan dari aset untuk mempermudah penyusunan persyaratan keamanan informasi menurut aspek kerahasiaan, integritas, dan ketersediaan (*confidentiality, integrity* dan *availability*).

3. Identifikasi Ancaman

   Identifikasi ancaman merupakan proses identifikasi dan dokumentasi yang terstruktur atas ancaman yang dapat terjadi di dalam bentuk pernyataan deskriptif *(area of concern)* dan gambaran lengkapnya *(threat scenario)* terhadap aset informasi melalui *container*-nya. *Area of concern* adalah suatu pernyataan yang mendeskripsikan kondisi atau situasi nyata yang dapat memengaruhi keamanan aset informasi di organisasi [14]. Identifikasi *area of concern* dilakukan dengan melakukan evaluasi terhadap profil aset informasi dan *container*-nya untuk menggambarkan kondisi atau situasi apa saja yang dapat membahayakan keamanan aset informasi. *Threat scenario* adalah gambaran lengkap berupa properti ancaman (aktor, motif, sarana/akses, akibat dan persyaratan keamanan yang terdampak) dari sebuah *area of concern* [14]. Skenario ancaman diidentifikasi untuk menghasilkan informasi lengkap seputar *area of concern* dengan mengacukan properti ancaman terhadap *threat tree* (Gambar 3) yang terdapat pada laporan teknis [14].



Gambar 3. *Threat Tree*

4. Identifikasi dan Mitigasi Risiko

   Proses identifikasi risiko dideskripsikan akibat/konsekuensi kerugian secara spesifik dari masing-masing skenario ancaman yang telah dikembangkan dari jenis klasifikasinya terhadap proses bisnis atau organisasi secara keseluruhan, dilanjutkan dengan proses analisis risiko dimana kriteria pengukuran risiko yang telah dikembangkan dievaluasi kemudian dikembangkan secara lebih lanjut menjadi acuan untuk mendapatkan nilai risiko relatif (perkiraan sejauh mana akibat kerugian yang disebabkan oleh risiko terhadap organisasi [14]) dalam bentuk matriks berdasarkan skenario ancaman yang telah dikembangkan pada fase sebelumnya, kemudian diakhiri dengan pengembangan strategi mitigasi untuk mengatasi risiko tersebut berdasarkan referensi *annex* ISO/IEC 27001:2013 dan penarikan kesimpulan dari hasil penilaian risiko dan saran pengelolaan dalam menyikapi risiko yang telah dinilai untuk IPH.

ISO/IEC 27001:2013

ISO/IEC 27001:2013 merupakan suatu *framework* yang berfungsi untuk membantu suatu organisasi dalam melindungi informasi yang dimiliki dengan cara yang sistematis dan hemat biaya, melalui penerapan Sistem Manajemen Keamanan Informasi [16]. *Annex* merupakan tabel referensi acuan untuk dalam perencanaan strategi untuk mengimplementasikan pengelolaan risiko terhadap sistem informasi yang digunakan [16]. Adapun *annex* pada ISO/IEC 27001:2013 terdapat pada Tabel 1.

Tabel 1. Tabel *Annex* ISO/IEC 27001:2013

Kode	Kategori Kontrol
A.5	Kebijakan Keamanan Informasi, A.5.1: Arah manajemen untuk keamanan informasi
A.6	Pengelolaan Keamanan Informasi, A.6.1: Organisasi internal, A.6.2: Perangkat seluler dan *teleworking*
A.7	Keamanan Sumber Daya Manusia, A.7.1: Pra-dipekerjakan, A.7.2: Selama dipekerjakan, A.7.3: Pemutusan hubungan kerja dan perubahan pekerja
A.8	Manajemen Aset, A.8.1: Tanggung jawab terhadap aset, A.8.2: Klasifikasi informasi, A.8.3: Penanganan media
A.9	Kontrol Akses, A.9.1: Persyaratan bisnis kontrol akses, A.9.2: Manajemen akses user, A.9.3: Tanggung jawab user, A.9.4: Kontrol akses sistem dan aplikasi
A.10	Kriptografi, A.10.1: Kontrol kriptografi
A.11	Keamanan Fisik dan Lingkungan, A.11.1: Keamanan area, A.11.2: Peralatan
A.12	Keamanan Operasi, A.12.1: Prosedur dan tanggung jawab operasional, A.12.2: Perlindungan terhadap malware, A.12.3: Back-up/cadangan, A.12.4: Logging dan pemantauan, A.12.5: Kontrol terhadap *software* operasional, A.12.6: Manajemen kerentanan teknis, A.12.7: Pertimbangan audit sistem informasi
A.13	Keamanan Komunikasi, A.13.1: Manajemen keamanan jaringan, A.13.2: Transfer informasi
A.14	Akuisisi, Pengembangan dan Pemeliharaan Sistem, A.14.1: Persyaratan keamanan sistem informasi, A.14.2: Keamanan dalam pengembangan dan pendukung proses, A.14.3: *Test data*
A.15	Hubungan dengan *Supplier*, A.15.1: Keamanan informasi dalam hubungan dengan *supplier*, A.15.2: Manajemen layanan pengiriman *supplier*
A.16	Manajemen terhadap Kecelakaan pada Keamanan Informasi, A.16.1: Manajemen insiden dan peningkatan keamanan informasi
A.17	Aspek Keamanan Informasi dari Manajemen Keberlangsungan Bisnis, A.17.1: Keberlangsungan keamanan informasi, A.17.2: Redundansi
A.18	Kepatuhan/*Compliance*, A.18.1: Kepatuhan dengan persyaratan hukum dan kontrak, A.18.2: Tinjauan keamanan informasi.

HASIL DAN PEMBAHASAN

Langkah Pertama: Mengembangkan Kriteria Pengukuran Risiko

Kriteria pengukuran risiko dikembangkan dengan melakukan wawancara semi-terstruktur bersama manajer tingkat senior di IPH, Bapak Edward Ginting, M.M. Diberikan pertanyaan-pertanyaan seputar kondisi/situasi yang dapat merugikan serta kategori tingkat kerusakannya terhadap poin-poin dalam *impact area*, seperti:

"Untuk ukuran dampak kerugian ringan pada poin kepercayaan pelanggan, kurang dari ___% kah pengurangan pelanggan karena hilangnya kepercayaan?", "Untuk ukuran dampak kerugian sedang, kisaran antara ____% hingga ____% kah pengurangan pelanggan karena hilangnya kepercayaan?", "Untuk ukuran dampak kerugian tinggi, lebih dari ____% kah pengurangan pelanggan karena hilangnya kepercayaan?"

Pada tiap poin di dalam *impact area*, akan diberikan pertanyaan berbeda yang mengacu pada tingkat kerusakannya, kemudian jawabannya akan didokumentasikan ke dalam *risk measurement criteria worksheet* (*worksheet* 1-5) yang terlihat pada Tabel 2.

Penelitian dilanjutkan dengan mendiskusikan *impact area* mana yang paling penting dan

mengurutkan prioritasnya dalam bentuk skala penilaian pada *impact area ranking worksheet (worksheet 7)* pada Tabel 3.

Langkah Kedua: Mengembangkan Profil Aset Informasi

Profil yang dikembangkan adalah aset-aset informasi yang digunakan dalam proses bisnis IPH sehari-hari, dimulai dari proses pemesanan bahan baku untuk produksi dari *vendor*, hingga *shipment*/pengiriman produk kepada pelanggan dengan melakukan observasi langsung terhadap sistem informasi dan wawancara semi-terstruktur bersama kepala departemen IT, Bapak Ronald Frederick Karwur.

Tabel 2. Tabel Pengukuran Dampak pada *Impact Area*

Allegro Worksheet 1-5				
Impact Area	Poin/Kategori	*Low*	*Moderate*	*High*
Reputasi dan Kepercayaan	Reputasi	Reputasi terpengaruh secara minimal; dibutuhkan minim upaya dan biaya untuk pulih.	Reputasi rusak, diperlukan upaya serta biaya untuk memulihkannya.	Reputasi hancur atau rusak secara permanen
	Kepercayaan	Pengurangan pelanggan kurang dari 2% karena hilangnya kepercayaan.	Pengurangan antara 2% hingga 5% karena hilangnya kepercayaan.	Pengurangan lebih dari 5% karena hilangnya kepercayaan.
Finansial	Biaya Operasional	Peningkatan biaya operasional tahunan kurang dari 2%.	Peningkatan biaya operasional tahunan sebesar 3% sampai 19%.	Peningkatan biaya operasional tahunan lebih dari 20%.
	Kerugian Pendapatan	Hilangnya pendapatan tahunan kurang dari 2%.	Hilangnya pendapatan tahunan dari 3% sampai 19%.	Hilangnya pendapatan tahunan lebih dari 20%.
	Kerugian *One-time*	Kerugian finansial satu-kali kurang dari Rp. 5.000.000.	Kerugian sebanyak Rp. 5.000.000 hingga Rp. 50.000.000.	Kerugian lebih dari Rp. 50.000.000.
Produktivitas	Jam Kerja Staf	Jam kerja staf meningkat kurang dari 2 jam untuk 1 hari.	Jam kerja staf meningkat antara 3 hingga 7 jam dari 2 sampai 7 hari.	Jam kerja staf meningkat lebih dari 8 jam dari 8 sampai 30 hari.
	Beban Kerja Staf	Beban kerja staf meningkat kurang dari 20% untuk 1 hari.	Beban kerja meningkat antara 21% hingga 49% dari 2 sampai 7 hari.	Beban kerja meningkat lebih dari 50% untuk 8 sampai 30 hari.
	Keterlambatan Proses Bisnis	Proses bisnis mengalami interupsi, menyebabkan keterlambatan kurang dari 2 jam untuk 1 hari.	Proses bisnis terinterupsi, keterlambatan dari 3 hingga 7 jam untuk 2 sampai 7 hari.	Proses bisnis interupsi, keterlambatan lebih dari 8 jam untuk 8 sampai 30 hari.
Keselamatan dan Kesehatan	Kehidupan	Tak ada ancaman pada keselamatan karyawan.	Keselamatan terancam, dapat sembuh dengan perawatan medis.	Hilangnya nyawa karyawan.
	Kesehatan	Gangguan kesehatan minim, dapat sembuh dalam 1 hari.	Gangguan kesehatan sementara/penurunan kesehatan pada karyawan.	Penurunan permanen dari kesehatan karyawan.
Denda & Penalti	Denda	Denda kurang dari Rp. 100.000.	Antara Rp. 100.000 hingga Rp. 10.000.000.	Lebih dari Rp.10.000.000.
	Gugatan	Tuntutan hukum kecil bernilai kurang dari Rp. 10.000.000.	Tuntutan sedang dengan nilai antara Rp. 10.000.000 sampai Rp. 100.000.00.	Tuntutan dengan nilai lebih dari Rp. 100.000.000.
	Investigasi	Tidak ada pemeriksaan atau organisasi investigasi lainnya.	Pemerintah atau instansi meminta catatan terkait tuntutan.	Pemerintah atau instansi lainnya melakukan investigasi.

Pertanyaan akan disusun seputar alasan dibalik pemilihan aset informasi kritikal tersebut, identifikasi kepemilikan, dan evaluasi untuk pemenuhan persyaratan keamanan, seperti:

"Apa saja aset informasi milik organisasi yang kritis/bernilai dan digunakan dalam kegiatan operasional sehari-hari?", "jika aset informasi ini terancam, apakah dapat berdampak buruk bagi organisasi?", "Mengapa aset informasi ini dianggap kritis bagi organisasi?", "Apakah aset informasi ini berbentuk elektronik, fisik, atau keduanya?", "Apakah aset informasi ini bergantung pada kebutuhan regulasi?", "Siapa individu yang memiliki wewenang atas aset informasi ini?", "Apa yang dilakukan atau harus dilakukan untuk memenuhi persyaratan keamanan kerahasiaan/integritas/ketersediaan?"

Tabel 3. Tabel Urutan Prioritas *Impact Area*

Allegro Worksheet 7	
Prioritas	*Impact Area*
5	Reputasi dan Kepercayaan
4	Produktivitas
3	Finansial
2	Keselamatan dan Kesehatan
1	Denda dan Penalti

Hasil jawaban wawancara didokumentasikan pada *critical information asset profile worksheet (worksheet 8)* pada Tabel 4.

Tabel 4. Tabel Profil Aset Informasi Kritikal

Allegro Worksheet 8		*Critical Information Asset Profile*
Aset Kritikal		Rasionalisasi Seleksi
1. *Human Resource* *Administration* (Absensi, Biodata, dll.), *Development* (Pengembangan Staf) 2. *Supply Chain Management* *Inventory* (Bahan Mentah, Produk Jadi) *Manufacture* (Proses Produksi), *Shipping* (Pengiriman Produk) 3. *Sales* *Transaction* (Transaksi penjualan produk) 4. *Purchasing* *Purchase Order* (Transaksi pembelian bahan mentah) 5. *Report* *Work Order* (Ringkasan dari seluruh rangkaian proses produksi)		Aset-aset informasi ini merupakan aset yang digunakan dalam proses bisnis organisasi sehari-hari. Jika keamanan aset informasi terancam, maka dapat menyebabkan terhambat hingga tidak berjalannya proses bisnis IPH. Aset-aset informasi ini bergantung pada regulasi, sesuai dengan prosedur yang dijalankan oleh IPH.
Pemilik		Staf-staf IPH, *Administrator*
Persyaratan Keamanan Aset		
Kerahasiaan	Aset informasi hanya dapat dilihat dan diakses oleh pihak yang memiliki akun yang sudah ter-registrasi untuk dapat mengakses sistem informasi, sesuai dengan *role* yang diberikan.	
Integritas	Aset informasi hanya dapat dimodifikasi oleh pihak yang memiliki kewenangan, beberapa akun memiliki *role* yang terbatas dan hanya dapat memodifikasi beberapa aset tertentu saja, sesuai dengan *role* yang dimiliki.	
Ketersediaan	Aset-aset informasi ini harus dapat diakses 24 jam dalam seminggu, tersedia kapanpun dan dimanapun oleh pihak yang memiliki kewenangan.	

Langkah Ketiga: Mengidentifikasi *Container* dari Aset Informasi

Pada langkah ini semua informasi mengenai *container* yang digunakan oleh organisasi diidentifikasi dengan melakukan observasi secara langsung dan wawancara semi-terstruktur dengan administrator sistem informasi, Bapak Ronald Frederick Karwur. Pertanyaan yang diberikan adalah seputar deskripsi dari *container* seperti penggunaan aset informasi dalam proses bisnis, jenis *container*, dan pihak mana saja yang menggunakan aset informasi yang diproses di dalam *container*, seperti:

"Bagaimana aset informasi ini digunakan dalam proses bisnis?", "Proses apa saja yang bergantung pada aset informasi ini?", "Dimanakah aset informasi ini disimpan? Apakah dalam bentuk fisik/elektronik/keduanya?", "Apakah ada customer/mitra bisnis yang menggunakan sistem informasi ini secara eksternal?", "Proses apa saja yang menggunakan aset informasi ini oleh pihak eksternal?", "Dalam bentuk apakah aset informasi eksternal ini disimpan? Fisik/elektronik/keduanya?", "Siapa yang bertanggung jawab atas container ini?"

Hasil wawancara akan didokumentasikan pada *information asset risk environment map (worksheet 9)* pada Tabel 5.

Tabel 5. Tabel *Container*

Allegro Worksheet 9	*Information Asset Risk Environment Map*	
Internal (Di Bawah Kontrol Organisasi)		
	Deskripsi *Container*	Pemilik
Technical	*Database: Server* Seluruh aset informasi pada sistem informasi IPH disimpan, diambil dan diproses di dalam server.	IT Department
	Aplikasi: ABASE Aset-aset informasi dapat diakses dan dimodifikasi melalui aplikasi sistem informasi IPH, ABASE.	Staf IPH, Administrator
Physical	*Database: Server* Server yang menyimpan, mengambil dan memproses aset informasi dalam sistem informasi IPH berada di dalam ruangan server IPH.	IT Department
	Arsip Fisik/tertulis Aset-aset informasi sebelum sistem informasi digunakan disimpan dalam bentuk fisik/tertulis, disimpan di dalam arsip.	Staf IPH
People	*Container people* adalah pihak-pihak yang mengetahui dan memiliki akses terhadap aset-aset informasi yang digunakan dalam proses bisnis IPH.	IPH
Eksternal (Di Luar Kontrol Organisasi)		
	Deskripsi *Container*	Pemilik
	Aplikasi: ABASE Untuk proses *purchasing* dengan *vendor*, transaksi di input oleh pihak IPH kemudian dapat dilihat, disetujui/ditolak dan diberikan catatan oleh *vendor* melalui akun yang diberikan dengan *role* yang terbatas oleh pihak IPH.	*Vendor*
	Aplikasi: ABASE Untuk proses *sales* dengan *customer*, transaksi di input oleh pihak IPH kemudian dapat dilihat, disetujui/ditolak dan diberikan catatan oleh *customer* melalui akun yang diberikan dengan role yang terbatas oleh pihak IPH.	*Customer*

Langkah Keempat: Mengidentifikasi *Area of Concern*

Pada langkah ini, Penelitian melakukan identifikasi atas *area of concern* dan diberikan kode berdasarkan sarana terjadinya dalam tiga kategori yaitu teknis, fisik dan manusia untuk memudahkan pengelompokan dalam melakukan penilaian risiko seperti pada Tabel 6.

Langkah Kelima: Mengidentifikasi Skenario Ancaman

Pada langkah ini dilakukan identifikasi skenario ancaman dengan menjawab pertanyaan-pertanyaan seputar properti ancaman dari tiap-tiap *area of concern* yang telah dikembangkan dengan mengacu pada *threat tree* [14], seperti:

"Siapa atau apa yang mengeksploitasi aset informasi?", "Bagaimana aktor melakukannya?", "Apakah motif aktor melakukan hal tersebut secara sengaja atau tidak disengaja?", "Apa jenis klasifikasi dari akibat skenario risiko ini terhadap organisasi?" (penyingkapan/modifikasi/hambatan/kehilangan), "Persyaratan keamanan atas aset informasi mana yang terdampak berdasarkan skenario risiko ini? (kerahasiaan/integritas/ketersediaan)"

Tabel 7 merupakan hasil wawancara yang didokumentasikan pada *information asset risk worksheet (worksheet 10).*

Langkah Keenam: Mengidentifikasi Risiko

Identifikasi risiko dilakukan dengan mengacu pada tinjauan literatur terhadap buku-buku yang mengangkat tema manajemen risiko dan penelitian-penelitian serupa yang telah dilakukan sebelumnya [5, 6, 7, 9, 14, 15]. Konsekuensi risiko yang diberikan dapat dilihat pada Tabel 8.

Tabel 6. Tabel *Area of Concern*

Kode	*Area of Concern*
TK-1	Malfungsi perangkat keras, menyebabkan server *crash.*
TK-2	Ruangan server dapat diakses dengan mudah.
TK-3	Pemanfaatan celah keamanan sistem informasi oleh pihak internal/eksternal.
TK-4	Kebocoran dan penyebaran hak akses (*username/password*).
TK-5	Penyelewengan hak akses yang berujung terjadinya modifikasi atas aset informasi oleh pihak tidak berwenang.
TK-6	Pengambilan alih kendali penuh atas sistem informasi oleh pihak tidak berwenang.
TK-7	Bug/kegagalan fungsi sistem informasi ketika dilakukan *update* atau *maintenance*.
TK-8	Gangguan jaringan internet sehingga sistem informasi tidak dapat diakses *(network failure).*
TK-9	Kegagalan dalam melakukan *back-up* data.
TK-10	Kehilangan seluruh data (data normal dan data *back-up*).
FS-1	Terjadinya bencana alam yang berpotensi membahayakan perangkat keras yang memproses sistem informasi.
FS-2	Terjadinya kegagalan tenaga listrik, sehingga sistem informasi tidak dapat berfungsi.
PP-1	Kesalahan dalam penginputan data/informasi oleh staf, menyebabkan misinformasi.

Tabel 7. Tabel Skenario Ancaman

Allegro Worksheet 10		*Information Asset Risk Worksheet*			
			Properti Ancaman		
Kode	Aktor	Sarana	Motif	Akibat	Persyaratan Keamanan
TK-1	Kecacatan *Hardware (Defects)*	Teknis	Tidak Disengaja	Hambatan	Ketersediaan
TK-2	Manusia (internal/eksternal)	Teknis	Disengaja/Tidak disengaja	Hambatan	Kerahasiaan, Ketersediaan
TK-3	Manusia (internal/eksternal)	Teknis	Disengaja	Penyingkapan *(Disclosure)*	Kerahasiaan, Integritas
TK-4	Manusia (internal/eksternal)	Teknis	Disengaja	Penyingkapan *(Disclosure)*	Kerahasiaan
TK-5	Manusia (internal)	Teknis	Disengaja	Modifikasi	Integritas
TK-6	Manusia (internal/eksternal)	Teknis	Disengaja	Hambatan, Kehilangan	Kerahasiaan, Integritas, Ketersediaan
TK-7	Kegagalan *Software* (*Software Defects*)	Teknis	Tidak Disengaja	Hambatan	Ketersediaan
TK-8	Telekomunikasi (Jaringan)	Teknis	Tidak Disengaja	Hambatan	Ketersediaan
TK-9	Kegagalan *Software (Defects)*	Teknis	Tidak Disengaja	Hambatan, Kehilangan	Ketersediaan
TK-10	Kegagalan *Software*, Kegagalan *Hardware*	Teknis	Tidak Disengaja	Kehilangan	Ketersediaan
FS-1	Bencana Alam	Fisik	Tidak Disengaja	Hambatan, Kehilangan	Ketersediaan
FS-2	*Power Supply*	Fisik	Tidak Disengaja	Hambatan	Ketersediaan
PP-1	Manusia (Internal)	Manusia	Tidak Disengaja	Hambatan	Integritas

Tabel 8. Tabel Konsekuensi

Kode	Konsekuensi Risiko
TK-1	Sistem informasi tidak dapat digunakan, sehingga dapat menyebabkan interupsi proses bisnis.
TK-2	Server dapat mengalami kerusakan dalam tingkat yang tidak tentu untuk diukur karena akibat dari orang tidak berwenang yang masuk ke dalam ruangan server tidak dapat terduga.
TK-3	Kehilangan kepercayaan atas tingkat keamanan sistem informasi yang dimiliki, berujung pada menurunnya reputasi oleh *customer* maupun *vendor*.
TK-4	Kehilangan kepercayaan atas integritas staf dalam mengelola keamanan sistem informasi yang dimiliki, berujung pada menurunnya reputasi oleh *customer* maupun *vendor,* selain itu juga dapat berujung pada manipulasi atas aset informasi yang dimiliki.
TK-5	Aset informasi yang dimanipulasi dapat menyebabkan misinformasi pada internal maupun dengan pihak eksternal dan berujung pada kesalahan, interupsi hingga kekacauan dalam melakukan proses bisnis yang dijalankan.
TK-6	Kerugian finansial atas investasi oleh organisasi untuk mengembangkan dan menjalankan sistem informasi, produktivitas yang menyebabkan segala aktivitas proses bisnis harus dilakukan secara manual, serta reputasi organisasi ternodai di mata *customer* dan mitra/*vendor*.
TK-7	Terganggunya proses produktivitas yang dijalankan. Aktivitas bisnis yang terdampak oleh *bug* harus dijalankan secara manual.
TK-8	Sistem informasi tidak dapat diakses, sehingga proses bisnis dapat mengalami hambatan serta mengalami kerugian waktu dan finansial.
TK-9	Terjadinya kerentanan terhadap aspek ketersediaan oleh aset informasi yang dimiliki. Jika tidak ada back-up data, organisasi tidak dapat memiliki cadangan ketika terjadi kehilangan data.
TK-10	Organisasi mengalami kerugian yang sangat signifikan dari berbagai aspek, yaitu reputasi/kepercayaan, finansial, dan produktivitas.
FS-1	Kerugian yang dialami selain finansial dan integritas data adalah keselamatan dan kesehatan staf yang bekerja di sekitar infrastruktur.
FS-2	Terjadinya hambatan terhadap proses bisnis karena sistem informasi tidak berfungsi sebab server tidak hidup, selain itu dapat terjadi kehilangan atas data yang diproses saat terjadi.
PP-1	Terjadinya misinformasi dan dapat menyebabkan kerugian finansial, produktivitas maupun berdampak pada reputasi di mata *customer* maupun *vendor.*

Langkah Ketujuh: Menganalisis Risiko

Nilai risiko relatif didapatkan dari perkalian antara urutan prioritas *impact area* dengan nilai kategori tingkat kerusakannya yaitu *High* bernilai 3*, moderate* bernilai 2*,* dan *low* bernilai 1 seperti pada Tabel 9.

Kemudian berdiskusi kembali dengan manajer tingkat senior, Bapak Edward Ginting, M.M. untuk menganalisis dan memperkirakan tingkat kerusakan dari konsekuensi masing-masing *area of concern* untuk menghitung nilai risiko relatifnya. Pertanyaan yang akan diberikan adalah seperti berikut:

"Apakah dampak dari area of concern ini memenuhi kondisi kategori low, moderate atau high pada impact area A?" Cth: "Apakah dampak konsekuensi dari area of concern ini memenuhi kondisi kategori low, moderate atau high dalam menyebabkan hilangnya reputasi dan kepercayaan pelanggan?"

Pertanyaan akan disesuaikan dengan *impact area* terkait dan jawabannya dimasukkan ke dalam matriks pada Tabel 10 pengukuran nilai risiko relatif. Jika kondisi kategori risiko pada poin-poin *impact area* yang ditanyakan berbeda, misalnya pada *impact area* reputasi dan kepercayaan, poin reputasi mendapat kategori *high* dan poin kepercayaan *low*, maka dianggap tetap memenuhi kondisi *high* sehingga diberikan kategori tingkat kerusakan lebih tinggi yaitu *high*.

Tabel 9. Matriks Cara Penghitungan Nilai Risiko Relatif

Impact Area	*Priority*	*Low* (1)	*Moderate* (2)	*High* (3)
Reputasi dan Kepercayaan	5	5	10	15
Produktivitas	4	4	8	12
Finansial	3	3	6	9
Keselamatan dan Kesehatan	2	2	4	6
Denda dan Penalti	1	1	2	3

Tabel 10. Matriks Pengukuran Nilai Risiko Relatif

Kode	Reputasi & Kepercayaan	Produktivitas	Finansial	Keselamatan & Kesehatan	Denda & Penalti	Nilai Risiko Relatif
TK-1	*Low* (5)	*High* (12)	*Mod* (6)	*Low* (2)	*Low* (1)	26
TK-2	*High* (15)	*High* (12)	*High* (9)	*Low* (2)	*Low* (1)	39
TK-3	*High* (15)	*Mod* (8)	*Mod* (6)	*Low* (2)	*Low* (1)	32
TK-4	*Mod* (10)	*Mod* (8)	*Low* (3)	*Low* (2)	*Low* (1)	24
TK-5	*Mod* (10)	*High (12)*	*Mod* (6)	*Low* (2)	*Low* (1)	31
TK-6	*High* (15)	*High* (12)	*High* (9)	*Low* (2)	*Low* (1)	39
TK-7	*Mod* (10)	*High* (12)	*Mod* (6)	*Low* (2)	*Low* (1)	31
TK-8	*Low* (5)	*High* (12)	*High* (9)	*Low* (2)	*Low* (1)	29
TK-9	*High* (15)	*High* (12)	*Mod* (6)	*Low* (2)	*Low* (1)	36
TK-10	*High* (15)	*High* (12)	*Mod* (6)	*Low* (2)	*Low* (1)	36
FS-1	*Low* (5)	*High* (12)	*Mod* (6)	*Mod* (4)	*Low* (1)	28
FS-2	*Low* (5)	*High* (12)	*Mod* (6)	*Low* (2)	*Low* (1)	26
PP-1	*Low* (5)	*Mod* (8)	*Low* (3)	*Low* (2)	*Low* (1)	19

Langkah Kedelapan: Memilih Pendekatan Mitigasi

Tiap *area of concern* yang telah diukur kemudian dikelompokkan dalam *pool* matriks risiko relatif pada Tabel 11 untuk menentukan status pendekatan mitigasinya berdasarkan nilai risiko relatif yang diperoleh. Jika nilai yang didapat berada pada *range* 30-45 maka *area of concern* tersebut dimasukkan ke dalam *pool* 3 dimana *status* pendekatan yang diberikan adalah mitigasi, jika berada pada *range* 16-29 maka masuk pada *pool* 2 dan diberikan status pendekatan ditunda/ditangguhkan, jika berada pada *range* 0-15, maka masuk *pool* 1 dan diberikan status pendekatan diterima.

Tabel 11. Matriks Penentuan Status Pendekatan Mitigasi

Pool Penentuan Status Pendekatan Mitigasi		
Pool 3 (Mitigasi, 30-45)	Pool 2 (Tunda, 16-29)	Pool 1 (Terima, 0-15)
TK-2, TK-3, TK 5, TK-6, TK-7, TK 9, TK-10	TK-1, TK-4, TK-8, FS-1, FS-2, PP-1	

Tahapan penelitian dilanjutkan dengan pemberian rekomendasi kontrol berdasarkan *annex* pada standar ISO/IEC 27001:2013 [16] terhadap *area-area of concern* yang memiliki status dimitigasi (*pool* 3) untuk melakukan pengelolaan atas risiko tersebut kepada manajer tingkat senior dari organisasi untuk ditinjau secara lebih lanjut. Rekomendasi kontrol yang diberikan berdasarkan *area of concern* dapat dilihat pada Tabel 12 dan Tabel 13.

Tabel 12. Tabel Rekomendasi Kontrol

Kode	*Area of Concern*	Rekomendasi Mitigasi	Referensi
TK-1	Malfungsi perangkat keras, menyebabkan server *crash.*	Melakukan pemeliharaan terhadap perangkat keras secara rutin dan melakukan *monitoring* terhadap aspek-aspek seperti penggunaan CPU, suhu ruangan dan *disk health.* Melakukan back-up terhadap data di dalam *hardware* dan mempersiapkan rencana penanggulangan terhadap *server crash* agar penanggulangan dapat dilakukan secara terarah.	A.11.2, A.12.1, A.12.6, A.17.2
TK-2	Ruangan server dapat diakses dengan mudah.	Menetapkan perimeter keamanan untuk melindungi fasilitas penyimpanan dan pemrosesan informasi kritikal dengan kontrol masuk seperti *doorlock* yang hanya bisa diakses menggunakan sidik jari, *keycard*, atau kode akses untuk memastikan hanya dapat diakses oleh pihak berwenang.	A.11.1
TK-3	Pemanfaatan celah keamanan sistem informasi oleh pihak internal/eksternal.	Menginstall *firewall*, antivirus, memodifikasi sistem keamanan *default* untuk memenuhi kebutuhan keamanan yang optimal, melakukan pemantauan secara rutin dan berkala dan menyimpan secara eksternal serta melindungi *logging* atas aktivitas user selama menggunakan sistem informasi, serta membuat SOP dan melakukan penyuluhan kepada semua pengguna sistem informasi agar tidak menginstal aplikasi secara sembarangan terutama ketika menggunakan jaringan publik selama mengakses sistem informasi, baik melalui perangkat *mobile* maupun *desktop*.	A.6.1, A.6.2, A.10.1, A.12.4 A.12.5, A.12.6, A.13.1, A.14.1
TK-4	Kebocoran dan penyebaran hak akses (*username/password*).	Mempersiapkan *terms & conditions* mengenai kredibilitas dalam pengelolaan data *username dan password*, mengenakan sanksi yang tegas berdasarkan hukum agar pengguna enggan dalam melakukan pelanggaran. Menerapkan kebijakan *password* yang kuat: memberikan password yang rumit yang tidak dapat ditebak atau dipaksakan dengan mudah kepada *user*, mempertimbangkan penggunaan autentikasi multifaktor untuk memberikan lapisan keamanan tambahan. Melakukan perubahan terhadap *password* dari akun-akun yang digunakan secara berkala	A.7.2, A.7.3, A.9.2, A.9.3, A.9.4, A.10.1, A.18.1
TK-5	Penyelewengan hak akses yang berujung terjadinya modifikasi atas aset informasi oleh pihak tidak berwenang.	Menetapkan klasifikasi untuk melabel informasi yang dipakai untuk mempermudah proses perbaikan terhadap modifikasi yang terjadi, menetapkan SOP untuk akses kontrol terhadap sistem informasi, mereview alokasi terhadap hak *privileged access* dari *role-role* yang ada di dalam sistem informasi, menetapkan suatu bentuk autentikasi tambahan di sistem informasi ketika mengakses *role-role* tertentu yang memiliki hak untuk memodifikasi informasi.	A.8.2, A.9.2, A.9.3, A.9.4
TK-6	Pengambilan alih kendali penuh atas sistem informasi oleh pihak tidak berwenang.	Mengakses penyimpanan eksternal *logging* aktivitas *user* untuk mencari tahu individu yang melakukan pengambilan data untuk melakukan investigasi atas bagaimana individu tersebut dapat melakukannya, melakukan peninjauan ulang atas analisis kebutuhan keamanan dan memastikan terpenuhi atau tidaknya kebutuhan keamanan, melakukan penilaian dan menyiapkan keputusan untuk melakukan aksi tindakan preventif terhadap kejadian serupa untuk meningkatkan keamanan.	A.12.4, A.14.1, A.16.1, A.18.1, A.18.2

Tabel 13. Tabel Lanjutan Rekomendasi Kontrol

Kode	*Area of Concern*	Rekomendasi Mitigasi	Referensi
TK-7	Bug/kegagalan fungsi sistem informasi ketika dilakukan *update* atau *maintenance*.	Menyiapkan prosedur untuk melakukan *rollback* kepada versi sebelumnya agar proses bisnis dapat tetap berjalan selama *update* atau *maintenance* dilakukan, melakukan pengujian dan *quality assurance* terhadap *update* yang akan diimplementasikan untuk memastikan bebas dari *bug.*	A.14.2, A.14.3
TK-8	Gangguan jaringan internet sehingga sistem informasi tidak dapat diakses *(network failure).*	Mempertimbangkan penggunaan *ISP* secara ganda agar dapat beralih dari *ISP* yang tidak bisa digunakan ke *ISP* yang tersedia. Mempertimbangkan menggunakan *ISP* yang paling stabil, *reliable* dan jarang memiliki riwayat gangguan jaringan agar terhindar dari tidak dapat diaksesnya sistem informasi.	A.6.2, A.13.1, A.14.1
TK-9	Kegagalan dalam melakukan *back-up* data.	Mengembangkan prosedur perencanaan *back-up and recovery* untuk menciptakan, menyimpan dan memulihkan data *back-up*, melakukan *back-up* data secara rutin, melakukan pengujian secara rutin terhadap sistem yang digunakan untuk mengidentifikasi potensi kegagalan *back-up.*	A.12.3, A.13.2
TK-10	Kehilangan seluruh data (data normal dan data *back-up*).	Mengidentifikasi batasan kehilangan data, mengontak *provider hosting* secara segera untuk menginformasikan terjadinya kehilangan data demi mencari kemungkinan adanya *back-up* dari pihak *provider*, mengembangkan dan mengimplementasikan strategi dan prosedur *back-up and recovery* yang lebih baik, seperti menyiapkan *back-up dari back-up* data dan menyimpannya di berbagai sumber.	A.12.3, A.13.2
FS-1	Terjadinya bencana alam yang berpotensi membahayakan perangkat keras yang memproses sistem informasi.	Melakukan identifikasi terhadap bencana alam yang memiliki kemungkinan terjadi pada perangkat keras dalam organisasi, melakukan penilaian risiko terhadap bencana alam yang telah diidentifikasi, dan mempersiapkan rencana penanggulangan (SOP) dalam melakukan langkah-langkah perlindungan terhadap tiap-tiap bencana alam yang dapat terjadi. Melakukan percobaan terhadap langkah-langkah perlindungan bencana alam yang telah dibuat.	A.11.1, A.11.2,
FS-2	Terjadinya kegagalan tenaga listrik, sehingga sistem informasi tidak dapat berfungsi.	Mempertimbangkan investasi *backup power* dalam bentuk *Uninterruptible Power Supply (UPS)* atau *generator* listrik terutama terhadap ruangan server. Mempersiapkan prosedur pengamanan data kepada staf untuk menghindari terjadinya kehilangan data ketika padam listrik terjadi.	A.11.2, A.12.3, A.12.6, A.16.1
PP-1	Kesalahan dalam penginputan data/informasi oleh staf, menyebabkan misinformasi.	Mempersiapkan prosedur standar/SOP untuk staf dalam melakukan *input data* seperti *double-checking* dan *cross-checking*, melakukan *feedback* terhadap kinerja staf dan bagaimana meningkatkan performa mereka, memberikan pelatihan terhadap para staf dalam melakukan penginputan data. Mempertimbangkan penggunaan data-*validation tools* untuk mengatasi *error-error* seperti data yang tidak terisi, *formatting* yang tidak tepat, serta inkonsistensi.	A.9.1, A.14.2

KESIMPULAN

Berdasarkan penilaian risiko yang telah dilakukan pada sistem informasi ABASE IPH, didapatkan hasil berupa lima aset informasi, empat *container* dan 13 *area of concern* yang telah diidentifikasi. Dari *area of concern* yang telah diidentifikasi, terdapat tujuh yang memiliki status harus dilakukan perencanaan mitigasi, dan enam yang dapat ditangguhkan. Pada semua *area of concern* yang telah diidentifikasi, diberikan perencanaan strategis kontrol risiko

berdasarkan referensi *annex* ISO/IEC 27001:2013 untuk mengurangi dampak dari kerusakan yang dapat disebabkan, seperti pada *area-area of concern* teknis berupa pembuatan prosedur standar seperti pemantauan dan pemeliharaan untuk pencegahan, *area-area of concern* fisik berupa identifikasi jenis bencana dan pertimbangan investasi untuk solusi, dan *area-area of concern* manusia berupa pembuatan prosedur dalam melakukan operasi. Diharapkan penelitian ini dapat mempermudah IPH dengan memberikan referensi untuk melakukan perencanaan dan menciptakan prosedur operasi standar dalam melakukan manajemen terhadap risiko-risiko yang telah diidentifikasi.

DAFTAR PUSTAKA

1. R. Umar, I. Riadi, and E. Handoyo, "Analysis Security of SIA Based DSS05 on COBIT 5 Using Capability Maturity Model Integration (CMMI)," *Scientific Journal of Informatics*, vol. 6, no. 2, pp. 2407–7658, Nov. 2019, Accessed: Nov. 02, 2022. [Online]. Available: http://journal.unnes.ac.id/nju/index.php/sji
2. A. Wiraniagara and F. Wijaya, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Domain Deliver Support and Service (Studi Kasus: Yayasan Eka Tjipta)," *Sebatik*, vol. 23, no. 2, pp. 663–671, Dec. 2019, Accessed: Nov. 02, 2022. [Online]. Available: https://jurnal.wicida.ac.id/index.php/sebatik/article/view/831/243
3. A. Basir, A. Fadlil, and I. Riadi, "Enterprise Architecture Planning Sistem Informasi Akademik Dengan TOGAF ADM," *Jurnal Sains Komputer & Informatika (J-SAKTI)*, vol. 3, no. 1, pp. 1–10, Mar. 2019, Accessed: Nov. 03, 2022. [Online]. Available: http://tunasbangsa.ac.id/ejurnal/index.php/jsaktiEnterpriseArchitecturePlanning
4. F. M. Hutabarat and A. D. Manuputty, "Analisis Risiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *Jurnal Bina Komputer*, vol. 2, no. 1, pp. 52–65, Feb. 2020, Accessed: Nov. 03, 2022. [Online]. Available: https://journal.binadarma.ac.id/index.php/binakomputer/article/view/792
5. M. Sukri and I. Riadi, "Risk Management Analysis on Administration System using OCTAVE Allegro Framework," *Int J Comput Appl*, vol. 174, no. 17, pp. 975–8887, Feb. 2021, Accessed: Feb. 24, 2023. [Online]. Available: https://www.researchgate.net/profile/Imam-Riadi-2/publication/349764055_Risk_Management_Analysis_on_Administration_System_using_OCTAVE_Allegro_Framework/links/6040cd77299bf1e07854a666/Risk-Management-Analysis-on-Administration-System-using-OCTAVE-Allegro-Framework.pdf
6. M. Hanafi, *Manajemen Risiko, in: Risiko, Proses Manajemen Risiko, dan Enterprise Risk Management*. Yogyakarta: UPP STIM YKPN, 2016.
7. G. Blokdijk, C. Engle, and J. Brewster, *IT Risk Management Guide Risk Management Implementation Guide, Presentations, Blueprints, Templates; Complete Risk Management Toolkit Guide for Information Technology Processes and Systems*. Brisbane: The Art of Service, 2008. Accessed: Nov. 04, 2022. [Online]. Available: http://theartofservice.com
8. P. Hopkin, *Fundamentals of Risk Management*, 4th ed. New York: Kogan Page, Ltd., 2017.
9. R. Yasirandi, A. Rakhmatsyah, and F. Kurniawan, "IT Risk Management dalam Operasional untuk Peningkatan Layanan Informasi Pesanan," *Krea-TIF*, vol. 9, no. 2, p.

21, Nov. 2021, doi: 10.32832/kreatif.v9i2.5982.

10. R. Siregar, "Analisis Manajemen Resiko Keamanan Data Sistem Informasi Universitas Advent Indonesia Menggunakan Metode OCTAVE Allegro," Skripsi, Universitas Advent Indonesia, Bandung, 2019. Accessed: Feb. 22, 2023. [Online]. Available: https://library.unai.edu/skripsi/js/pdfjs/web/viewer.html?file=../../../repository//Raminson%20Siregar.pdf
11. J. Pardede, "Indonesia Publishing House, Encyclopedia of Seventh-Day Adventist," Nov. 28, 2020. https://encyclopedia.adventist.org/article?id=BAQA&highlight=y (accessed Feb. 24, 2023).
12. R. Jr. McLeod and G. Schell, *Sistem Informasi Manajemen*, 10th ed. DKI Jakarta: Salemba Empat, 2008.
13. L. F. Mottiwala and J. Thompson, *Enterprise Systems for Management*, 2nd ed. Hoboken, New Jersey: Prentice Hall, 2012.
14. R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," May 2007. Accessed: Oct. 04, 2022. [Online]. Available: http://www.sei.cmu.edu/publications/pubweb.html
15. B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *Jurnal Teknologi dan Informasi (JATI)*, vol. 12, no. 27, p. 12, 2022, doi: 10.34010/jati.v12i2.
16. *ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements*, 2013th ed. Geneva, Switzerland, Switzerland: International Standard Organization, 2013.