ANALISIS RISK ASSESSMENT TERHADAP PERUSAHAAN IT DI BIDANG FINANSIAL MENGGUNAKAN OCTAVE ALLEGRO FRAMEWORK

Joseph Sanjaya
Program Studi Ilmu Komputer/Fakultas IT, Universitas Kristen Maranatha
Email : sanjayajosep@gmail.com

ABSTRAK

Risk assessment pada teknologi informasi adalah bagian yang sangat penting dari setiap strategi manajemen keamanan, khususnya pada perusahaan yang bergerak dibidang finansial. Risk assessment membantu organisasi untuk mengidentifikasi aset yang kritis dan memprioritaskan upaya mitigasi risiko yang bersangkutan. Namun, banyak metodologi risk assessment yang kompleks dan hanya dapat diselesaikan oleh para pakar keamanan yang berkualifikasi dan berpengalaman. Dan tentunya hal ini menjadi sebuah expense yang cukup besar untuk perusahaan sehingga organisasi berukuran kecil sulit mengimplementasikankan risk assessment ini. Oleh karena itu, sebagian besar perusahaan start-up di Indonesia tidak melakukan risk assessment ini, yang membuat data perusahaan rentan terhadap serangan keamanan. Konsekuensi negatif dari pelanggaran keamanan di lembaga-lembaga ini dapat mencakup penurunan reputasi lembaga, hilangnya pendapatan keuangan, dan paparan terhadap tuntutan hukum. Berdasarkan kenyataan tersebut, penelitian ini bertujuan untuk melakukan risk assessment pada aset salah satu perusahaan yang bekerja dibidang finansial planner. Risk assessment dilakukan menggunakan kerangka kerja OCTAVE Allegro. Diharapkan kebijakan yang direkomendasikan oleh penelitian ini dapat bermanfaat bagi perusahan yang bersangkutan sebagai perbaikan keamanan di masa depan.

Kata Kunci: Manajemen Resiko, *Risk Assessment, OCTAVE Allegro*

ABSTRACT

Risk assessment on information technology is a very important part of every security management strategy, especially in companies engaged in finance. Risk assessment helps organizations to identify critical assets and prioritize risk mitigation efforts concerned. However, many risk assessment methodologies are complex and can only be completed by qualified and experienced security experts. And of course this becomes a considerable expense for the company so that small-sized organizations find it difficult to implement this risk assessment. Therefore, most start-up companies in Indonesia do not carry out this risk assessment, which makes company data vulnerable to security attacks. Negative consequences of security breaches at these institutions can include deterioration of the institution's reputation, loss of financial income, and exposure to lawsuits. Based on this fact, this study aims to conduct a risk assessment on the assets of one company that works in the field of financial planner. Risk assessment is carried out using the OCTAVE Allegro framework. It is hoped that the policies recommended by this research can benefit the company concerned as a security improvement in the future.

Keywords: *Risk Management, Risk Assesment, OCTAVE Allegro*

1. PENDAHULUAN

Penilaian risiko Teknologi Informasi (TI) adalah proses formal yang memungkinkan risiko TI untuk diidentifikasi dan dimitigasi (Ghernaouti-Helie, Tashi, & Simms, 2011; Liu, Kuhn, & Rossman, 2009; Nikolic & Ruzic-Dimitrijevic, 2009). Penilaian risiko dirancang untuk mengidentifikasi aset TI dan untuk memberikan deskripsi kerentanan dan ancaman, pendekatan untuk mengklasifikasikan risiko, dan rencana mitigasi risiko (Nikolic & Ruzic-Dimitrijevic, 2009; Syalim, Hori, & Sakurai, 2009). Banyak metode untuk melakukan penilaian risiko tersedia, termasuk Panduan untuk Melakukan Penilaian Risiko (Institut Nasional Standar dan Teknologi [NIST], 2012); Tujuan Pengendalian untuk Informasi dan Teknologi Terkait (COBIT); Spesifikasi Sistem Manajemen Keamanan Informasi (sebagaimana didefinisikan oleh Organisasi Internasional untuk Standardisasi / Komisi Elektroteknik Internasional [ISO / IEC] 27005); dan Evaluasi Ancaman Kritis, Aset, dan Kerentanan Operasional (OCTAVE; Kouns & Minoli, 2010; Landoll, 2011; Liu et al., 2009). Penilaian risiko TI adalah komponen penting dari rencana keamanan komprehensif untuk setiap entitas, termasuk lembaga pendidikan tinggi (Kouns & Minoli, 2010; Liu et al., 2009; NIST Joint Task Force Transformation Initiative [JTF], 2011).

Saat ini, tidak banyak lembaga melakukan penilaian risiko pada sistem informasi mereka. Di satu sisi, sistem informasi menjadi tidak terpisahkan dari hampir semua proses bisnis di institusi (Ikhsan & Jarti, 2018). Salah satu alasannya adalah kurangnya kesadaran para pemangku kepentingan TI tentang keamanan informasi. Sebagai akibatnya, gangguan pada sistem informasi juga dapat mengganggu proses bisnis mereka.

Keamanan informasi tidak hanya bergantung pada alat atau teknologi, tetapi membutuhkan kesadaran dalam organisasi tentang apa yang perlu dilindungi dan pemilihan solusi yang tepat untuk menangani masalah dalam kebutuhan keamanan informasi. Untuk ini, manajemen keamanan informasi yang sistematis dan komprehensif sangat penting. Kebutuhan akan keamanan informasi harus mengandung 3 elemen penting: confidentiality, integrity, dan availability (Jufri et al., 2017).

Menurut Blestari, Chinniah, Newcomb, Plympton, dan Walsh (dalam pers), sangat penting bagi institusi akademik pasca-sekolah menengah untuk melakukan penilaian risiko untuk melindungi data kelembagaan mereka. Blestari, Chinniah et al. (in press) mencatat bahwa, untuk menetapkan prioritas untuk mengurangi risiko TI, rencana keamanan komprehensif untuk lembaga akademik harus mengidentifikasi area yang mengandung kerentanan terbesar. Kvavik (2006), dalam sebuah studi klasik tentang keamanan Teknologi Informasi (TI) di pendidikan tinggi, juga mencatat bahwa lembaga pasca sekolah dari semua ukuran harus melakukan penilaian risiko TI reguler sebagai bagian dari rencana manajemen risiko mereka.

Menurut penelitian klasik pada organisasi kecil oleh Beachboard et al. (2008), memvalidasi metodologi penilaian risiko yang tepat untuk lembaga

pendidikan tinggi berukuran kecil telah sulit karena banyak metodologi saat ini rumit. Beachboard et al. mencatat bahwa alat analisis risiko yang dikembangkan secara komersial, seperti RiskWatch®, mahal dan kompleks dan, dengan demikian, dapat mengakibatkan masalah kualitas data dan hasil penilaian risiko yang tidak dapat diandalkan. Beachboard et al. juga mengakui kesulitan yang dihadapi oleh organisasi kecil dalam menerapkan berbagai metodologi risiko non-komersial, seperti Analisis Risiko yang Difasilitasi dan Proses Penilaian (FRAAP), OCTAVE-S yang lebih tua, seperti yang dibahas di bawah ini, dan Panduan NIST untuk Melakukan Penilaian Risiko (2012). Menurut Beranek (2011), tidak mungkin untuk menerapkan metode manajemen keamanan TI yang dikembangkan terutama untuk institusi yang lebih besar secara langsung ke organisasi kecil dan menengah. OCTAVE Allegro adalah metodologi penilaian risiko populer yang dikembangkan pada 2007 oleh para peneliti di Carnegie Mellon University (CMU) Software Engineering Institute (SEI), sebagaimana dibahas dalam laporan oleh Caralli, Stevens, Young, dan Wilson (2007), Memperkenalkan OCTAVE Allegro: Meningkatkan Proses Penilaian Risiko Keamanan Informasi. OCTAVE Allegro dikembangkan untuk tujuan "mengidentifikasi, menganalisis dan memprioritaskan risiko keamanan TI" (Liu et al., 2009, hal. 57). Berdasarkan temuan dari penilaian risiko OCTAVE Allegro, profesional TI dapat mengidentifikasi risiko TI dan memprioritaskan upaya mitigasi dengan mengembangkan langkah-langkah keamanan untuk mengurangi dampak dari serangan keamanan (Caralli et al., 2007; Kouns & Minoli, 2010).

Berdasarkan uraian di atas, masalah yang diteliti di sini dirumuskan sebagai berikut: Bagaimana mengidentifikasi kerentanan dan ancaman terhadap aset informasi di perusahaan berbasis finansial planner terhadap proses bisnisnya. Bagaimana menerapkan mitigasi risiko keamanan informasi di perusahaan berbasis finansial planner berdasarkan penilaian risiko. Kebijakan keamanan informasi apa yang perlu diterapkan berdasarkan hasil penilaian risiko menggunakan metode OCTAVE Allegro.

2. LANDASAN TEORI

2.1 Keamanan Sistem Informasi

Sistem Informasi Keamanan adalah hal-hal yang perlu mendapat perhatian saat membangun sistem informasi. Bayangkan kita membuat rumah lengkap dengan jendela dan pintu, bukan kunci untuk pintu dan jendela. Ini dapat menyebabkan seseorang dengan mudah mengganti rumah kita, bahkan mungkin melakukan pencurian. Sama dengan membangun sistem informasi untuk menghindari seseorang yang tidak memiliki akses untuk masuk ke sistem. (Bakri & Irmayana, 2017).

2.2 Sistem Informasi

Suatu sistem informasi dapat secara teknis didefinisikan sebagai seperangkat komponen yang saling berhubungan yang mengumpulkan (atau mengekstrak), memproses, menyimpan, dan mendistribusikan informasi untuk memfasilitasi pengambilan keputusan dan kontrol dalam suatu organisasi. Selain memfasilitasi pengambilan keputusan, koordinasi, dan kontrol, sistem informasi

juga dapat membantu manajer dan pekerja menganalisis masalah, memvisualisasikan subjek yang kompleks, dan menciptakan produk baru. Sistem informasi berisi informasi tentang orang-orang kunci, tempat, dan aspek-aspek dalam organisasi atau lingkungan sekitarnya. Dengan informasi, data dibentuk menjadi faktor yang bermakna dan bermanfaat bagi manusia. Data, akibatnya, adalah aliran fakta mentah yang mewakili kejadian yang terjadi di dalam organisasi atau lingkungan fisiknya sebelum diorganisasikan dan diformulasikan menjadi bentuk yang dapat dipahami dan digunakan (Ifinedo, 2012).

2.3 Risiko

Risiko adalah kerentanan kritis yang mengarah pada perbedaan dalam penerapan teknologi informasi. Perbedaan mengacu pada kejadian positif atau negatif yang dapat mempengaruhi kinerja sistem informasi dan teknologi informasi.

2.4 Aset Informasi

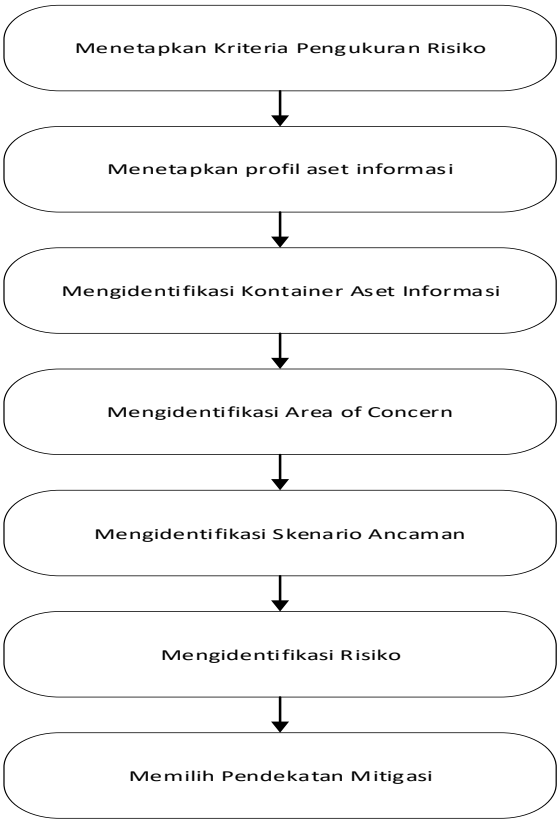
Aset informasi dapat digambarkan sebagai informasi atau data yang bernilai bagi organisasi; termasuk informasi seperti catatan pasien, kekayaan intelektual, atau informasi konsumen. Aset ini dapat berupa fisik (kertas, CD, atau media lain) atau bentuk elektronik (disimpan dalam basis data, file, PC) (Utomo, 2013).

2.5 OCTAVE Allegro

Pendekatan OCTAVE Allegro dirancang untuk memungkinkan penilaian luas lingkungan risiko operasional organisasi dengan tujuan menghasilkan hasil yang lebih kuat tanpa perlu pengetahuan penilaian risiko yang luas. Pendekatan ini berbeda dari pendekatan OCTAVE sebelumnya dengan berfokus terutama pada aset informasi dalam konteks bagaimana mereka digunakan, di mana mereka disimpan, diangkut, dan diproses, dan bagaimana mereka terpapar pada ancaman, kerentanan, dan gangguan sebagai hasilnya. Seperti metode sebelumnya, OCTAVE Allegro dapat dilakukan dalam gaya lokakarya, pengaturan kolaboratif dan didukung dengan panduan, lembar kerja, dan kuesioner, yang termasuk dalam lampiran dokumen ini. Namun, OCTAVE Allegro juga sangat cocok untuk digunakan oleh individu yang ingin melakukan penilaian risiko tanpa keterlibatan, keahlian, atau input organisasi yang luas.

3. METODE PENELITIAN

Risk assessment akan dilakukan menggunakan kerangka kerja OCTAVE Allegro. Kerangka kerja ini terdiri dari 8 tahap yang dapat dilihat pada gambar 1.



Gambar 1. 8 Tahap Risk Assessment OCTAVE Allegro

Langkah 1 - Menetapkan Kriteria Pengukuran Risiko. Langkah ini melibatkan dua kegiatan, mulai dengan membentuk penggerak organisasi untuk mengevaluasi dampak risiko terhadap misi dan tujuan bisnis organisasi, serta mengenali area dampak utama. Kegiatan 1 mendefinisikan tindakan kualitatif yang didokumentasikan pada Kegiatan 2, mencetak nilai prioritas area dampak menggunakan Lembar Kerja Peringkat Wilayah Dampak (Caralli et al., 2007).

Langkah 2 - Mengembangkan Profil Aset Informasi. Langkah ini terdiri dari delapan kegiatan, dimulai dengan mengidentifikasi informasi aset, kemudian melakukan penilaian risiko terstruktur pada aset kritis. Kegiatan 3 dan 4 berkaitan dengan pengumpulan informasi tentang aset penting, diikuti dengan mendokumentasikan alasan pemilihan aset tersebut. Kegiatan 5 dan 6 terdiri dari menggambarkan aset informasi kritis,

diikuti oleh identifikasi kepemilikan aset. Kegiatan 7 adalah mengisi persyaratan keamanan untuk kerahasiaan, integritas, dan ketersediaan. Kegiatan 8 adalah mengidentifikasi persyaratan keamanan mana yang paling penting untuk aset.

Langkah 3 - Mengidentifikasi Kontainer Aset Informasi. Hanya ada satu kegiatan dalam langkah ini: mengidentifikasi tiga poin utama mengenai keamanan dan konsep wadah informasi aset: cara aset dilindungi, tingkat perlindungan, dan kerentanan dan ancaman pada wadah.

Langkah 4 - Mengidentifikasi Area Kekhawatiran. Langkah ini dimulai dengan mengembangkan profil risiko aset informasi, dengan berbagi ide untuk mencari komponen ancaman dari situasi yang dapat mengancam aset informasi. Dengan mengikuti Peta Lingkungan Risiko Aset Informasi dan dokumen Lembar Kerja Risiko Aset Informasi, bidang-bidang yang menjadi perhatian dapat dipetakan. Mengikuti Lembar Kerja Risiko Aset Informasi, kontainer ditinjau untuk memetakan dan mendokumentasikan bidang-bidang yang menjadi perhatian.

Langkah 5 - Mengidentifikasi Skenario Ancaman. Aktivitas pertama dalam langkah ini adalah mengidentifikasi skenario ancaman tambahan, yang dapat difasilitasi menggunakan kuesioner Threat Scenario pada OCTAVE Allegro. Kegiatan kedua adalah menyelesaikan Lembar Kerja Risiko Aset Informasi untuk setiap skenario ancaman umum.

Langkah 6 - Mengidentifikasi Risiko. Menentukan skenario ancaman yang didokumentasikan dalam Lembar Kerja Risiko Aset Informasi yang dapat memengaruhi organisasi.

Langkah 7 - Menganalisis Risiko. Kegiatan harus merujuk pada dokumentasi Lembar Kerja Risiko Aset Informasi. Kegiatan pertama adalah meninjau kriteria pengukuran risiko, diikuti dengan menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik untuk mengatasinya.

Langkah 8 - Memilih Pendekatan Mitigasi. Aktivitas pertama dalam langkah ini adalah memilah semua risiko yang diidentifikasi berdasarkan nilai-nilainya, untuk memfasilitasi pengambilan keputusan tentang status mitigasi risiko.

Aktivitas kedua adalah menerapkan pendekatan mitigasi yang dipilih untuk setiap risiko, dengan mengikuti kondisi unik dalam organisasi.

4. HASIL DAN PEMBAHASAN

Sebelum memulai penilaian risiko dan menerapkan kontrol keamanan, peneliti telah menghubungi nara sumber utama yang peduli dengan manajemen keamanan perusahan finansial planner yang bersangkutan di Divisi Jaminan Kualitas perusahaan. Individu tersebut adalah: kepala Divisi Jaminan Kualitas, kepala Pusat Data Perusahaan, staf di divisi jaringan komputer, dan kepala divisi administrasi. Orang-orang ini dihubungi untuk mendapatkan data yang diperlukan. Langkah selanjutnya adalah melakukan wawancara untuk mendapatkan informasi tentang aset operasional yang dianggap penting bagi organisasi.

4.1 OCTAVE Allegro Risk Assessment

Langkah 1 - Menetapkan Kriteria Pengukuran Risiko. Tahap pertama risk assessment dimulai dengan berunding dengan narasumber mengenai manajemen keamanan perusahaan di Divisi Jaminan Kualitas, kepala Divisi Jaminan Kualitas, kepala Pusat Data Universitas, staf di divisi jaringan komputer, dan kepala divisi administrasi untuk mendapatkan data yang diperlukan. Langkah selanjutnya adalah melakukan wawancara untuk mendapatkan informasi tentang aset operasional penting organisasi. Hasil dari langkah ini dapat dilihat pada tabel 1 dan tabel 2.

Tabel 1. Impact Area – Reputasi dan Kehilangan Pelanggan

Kriteria Pengukuran Risiko – Reputasi dan Kepercayaan Pelanggan		
Penurunan kecil reputasi.	Kerusakan atau penurunan reputasi yang membutuhkan perbaikan.	Penurunan reputasi yang besar dan tidak dapat diperbaiki.
Penurunan kecil dalam hilangnya pelanggan.	Kehilangan besar pelanggan.	Kehilangan besar pelanggan yang menghasilkan hilangnya kepercayaan pelanggan.

Tabel 2. Impact Area Priority Scale

Priority	Impact Areas
5	Reputasi dan Kepercayaan Pelanggan
4	Produktivitas
3	Denda dan Penalti
2	Finansial
1	Keamanan dan Kesehatan

Langkah 2 - Membuat profil aset informasi. Ini terdiri dari delapan kegiatan, dimulai dengan identifikasi aset informasi, diikuti oleh penilaian risiko terstruktur pada aset kritis. Kegiatan ke-3 dan ke-4 terdiri dari pengumpulan informasi tentang aset penting, diikuti dengan mendokumentasikan alasan pemilihan aset penting. Kegiatan 5 dan 6 terdiri dari menggambarkan aset informasi kritis dan mengidentifikasi kepemilikan aset. Aktivitas ke-7 terdiri dari mengisi persyaratan keamanan untuk kerahasiaan, integritas, dan ketersediaan. Kegiatan ke-8 terdiri dari mengidentifikasi kebutuhan

keamanan paling penting untuk aset informasi.

Dari pertimbangan di atas, aset informasi yang dikategorikan sebagai aset kritis adalah Database Finansial Planner. Tabel 3 menyajikan profil aset untuk database Finansial Planner.

Tabel 3. Profil dasar Informasi Database Finansial Planner

Alasan Pemilihan	**Deskripsi**
Basis Data Finansial Planner mengumpulkan informasi tentang kegiatan pelanggan tentang Pendapatan, Pengeluaran, Asset, dan Investasi; semua disimpan dalam database dan dapat diakses melalui website dan mobil apps.	Penyimpanan data Finansial Planner yang saling berhubungan dan saling tergantung untuk sistem informasi. Data-data ini disimpan dalam database yang terdiri dari: tabel pengguna, tabel Transaksi, tabel Asset, dan tabel Investasi.
Pemilik	**Finansial Planner Admin**
Security Requierement	
Confidentiality	Kerahasiaan data perlu dijaga. Akses harus dibatasi hanya untuk pengguna tertentu berdasarkan ketentuan tertentu (Access Privilege Management)
Integrity	Integritas data perlu dipertahankan. Gangguan pada integritas data akan menghambat aktivitas sistem.
Availibility	Ketersediaan data perlu dipertahankan, sehingga mereka akan selalu tersedia untuk pengguna kapan saja.
Persyaratan Keamanan Paling Penting	
Confidentiality Karena sifat basis data, sebagai kumpulan tabel yang menyimpan data yang saling berhubungan dan terdapat data transaksi-transaksi yang dapat bersifat private, sehingga basis data perlu diamankan.	

Langkah 3 - Mengidentifikasi Kontainer Aset Informasi. Hanya ada satu kegiatan dalam langkah ini: mengidentifikasi tiga poin utama mengenai keamanan dan konsep wadah informasi aset: cara Assetis dilindungi, tingkat perlindungan, dan kerentanan dan ancaman pada wadah. Hasil dari langkah ini dapat dilihat pada Tabel 4.

Tabel 4. Finansial Planner Database Information Asset Risk Environtment

Information Asset Risk Environment Map (Technical)	
Internal	
Deskripsi Kontainer	**Pemilik**
Server basis data cenderung memenuhi kebutuhan klien untuk penyimpanan data. Server berisi ratusan atau ribuan	Finansial Planner Admin

database dari banyak pengguna. Biasanya database dikompilasi atau disimpan per pengguna, untuk mencegah pencurian data.	
External	
Deskripsi Kontainer	**Pemilik**
Administrator / Kepala Divisi Sistem Data & Informasi	Perusahaan Finansial Planner

Langkah 4 - Mengidentifikasi Area Kekhawatiran, dengan meninjau setiap wadah untuk melihat dan menentukan area yang menjadi perhatian, diikuti dengan mendokumentasikan setiap area yang diidentifikasi. Area kemudian diperluas untuk mendapatkan skenario ancaman, diikuti oleh dokumentasi untuk melihat apakah skenario mempengaruhi persyaratan keamanan. Tabel 5 menyajikan area sampel yang menjadi perhatian untuk Database.

Tabel 5. Area of Concern – Finansial Planner Database

No.	Area of Concern
1	Pemberitahuan akses masuk oleh Operator
2	Database menemukan kesalahan selama pemeliharaan sistem
3	Seorang staf / pembajak yang terhubung ke jaringan komputer melakukan sniffing.

Langkah 5 - Mengidentifikasi Skenario Ancaman. Aktivitas pertama dalam langkah ini adalah mengidentifikasi skenario ancaman tambahan, yang dapat difasilitasi menggunakan Threat Skenario Skenario di OCTAVE Allegro. Kegiatan kedua adalah menyelesaikan Lembar Kerja Risiko Aset Informasi untuk setiap skenario ancaman umum. Hasil dari langkah ini dapat dilihat pada tabel 6.

Tabel 6. Properties of Threats

Area of Concern	Threat Properties	
Pemberitahuan akses masuk oleh Operator	Actor	Staf / Administrator
	Means	Data masuk perusahaan dapat bocor ke staf atau pihak tidak resmi lainnya.
	Motive	Staf atau pihak lain yang tidak berwenang dapat mengakses, mengubah, menambah, dan menghapus data dalam sistem, secara sengaja atau tidak.
	Outcome	Pengungkapan, Modifikasi, Penghancuran
	Security Requirements	Kebijakan yang mengelola akses masuk pribadi pengguna ke

		sistem.
Database menemukan kesalahan selama pemeliharaan sistem.	Actor	Staf ETL Database admin
	Means	Data yang ditampilkan dapat salah atau tidak valid.
	Motive	Sistem yang salah dapat membuat user yang tidak wewenang dapat mengakses data penting dengan hanya mengubah url.
	Outcome	Pengungkapan, Modifikasi, Penghancuran, hilangnya pelanggan
	Security Requirements	Sistem dibuat agar tidak dapat diakses dengan mudah melalui url, dan sistem dibuat dengan sedikit mungkin bug.
Seorang staf / pembajak yang terhubung ke jaringan komputer melakukan sniffing.	Actor	Staf / Pembajak
	Means	Data-data yang penting atau data privasi pelanggan dapat bocor dan tersebar.
	Motive	Pihak yang tidak berwenang dapat mendapatkan data penting
	Outcome	Hilangnya kepercayaan pelanggan dan bahkan dapat masuk jalur hukum.
	Security Requirements	Menggunakan enkripsi untuk jaringan yang terhubung pada database penting, Staf yang tidak berwenang tidak dapat mengakses jaringan yang mengandung data penting.

Langkah 6 - Mengidentifikasi Risiko. Menentukan skenario ancaman yang didokumentasikan dalam Lembar Kerja Risiko Aset Informasi yang dapat memengaruhi organisasi. Hasil dari langkah ini dapat dilihat pada tabel 7.

Tabel 7. Kalkulasi Impact Area

Impact Areas	Priority	Low	Medium	High
Reputasi dan Kepercayaan Pelanggan	5	5	10	15
Produktivitas	4	4	8	12
Denda dan Penalti	3	3	6	9
Finansial	2	2	4	6
Keamanan dan Kesehatan	1	1	2	3

Langkah 7 - Menganalisis Risiko. Kegiatan harus merujuk pada dokumentasi Lembar Kerja Risiko Aset Informasi. Kegiatan pertama adalah meninjau kriteria pengukuran risiko, diikuti dengan menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik untuk mengatasinya. Hasil kalkulasi dapat dilihat pada tabel 8.

Tabel 8. Kalkulasi Impact Area

Severity		
Impact Areas	Value	Score
Reputasi dan Kepercayaan Pelanggan	High	15
Produktivitas	Low	4
Denda dan Penalti	High	9
Finansial	Medium	4
Keamanan dan Kesehatan	Medium	2
Relative Risk Score		34

Langkah 8 - Memilih Pendekatan Mitigasi. Aktivitas pertama dalam langkah ini adalah memilah semua risiko yang diidentifikasi berdasarkan nilai-nilainya, untuk memfasilitasi pengambilan keputusan tentang status mitigasi risiko. Aktivitas kedua adalah menerapkan pendekatan mitigasi yang dipilih untuk setiap risiko, dengan mengikuti kondisi unik dalam organisasi. Hasil dari langkah ini dapat dilihat pada tabel 9 dan tabel 10.

Tabel 9. Relative Risk Matrix

Relative Risk Matrix		
Risk Score		
30 - 50	19 - 29	0 - 19
Pool 1	Pool 2	Pool 3

Tabel 10. Relative Risk Matrix

Relative Risk Matrix	
Pool	Mitigation Approach
1	Mitigation
2	Defer
3	Accept

5. SIMPULAN DAN SARAN

Penelitian ini mengarah pada kesimpulan sebagai berikut:

OCTAVE Allegro adalah salah satu metode manajemen informasi yang dapat diterapkan ke perusahaan berbasis finansial planner dan ketersediaan informasi penting untuk kelangsungan perusahan yang bersangkutan dalam mencapai misi dan tujuannya.

Penilaian risiko dapat memberikan gambaran tentang potensi ancaman terhadap aset kritis dan mengambil tindakan pencegahan yang sesuai untuk melakukan tawar-menawar atas kemungkinan ancaman.

Penelitian ini menawarkan saran-saran berikut:

Perusahaan yang bersangkutan harus merumuskan seperangkat peraturan tertulis tentang tanggung jawab dalam memelihara informasi dan sanksi bagi mereka yang melanggar, dan kemudian menyebarluaskan peraturan ini secara berkala kepada semua stafnya.

Perusahaan harus membuat simulasi visual untuk memudahkan stafnya dalam memahami pentingnya aset informasi, potensi ancaman dan risiko, serta konsekuensinya.

Perusahaan harus mengevaluasi kembali keamanan informasinya menggunakan OCTAVE Allegro secara berkala; misalnya setahun sekali.

DAFTAR PUSTAKA

Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001. Jurnal Tekno Kompak, 11(2), 41. https://doi.org/10.33365/jtk.v11i2.162

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process: Defense Technical Information Center. https://doi.org/10.21236/ADA470450

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ikhsan, H., & Jarti, N. (2018). Analisis risiko keamanan teknologi informasi Menggunakan Octave Allegro. *JR : JURNAL RESPONSIVE Teknik Informatika*, *2*(1). https://doi.org/10.36352/jr.v2i1.127

Jufri, M. T., Hendayun, M., & Suharto, T. (2017). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. *2017 Second International Conference on Informatics and Computing (ICIC)*, 1–6. https://doi.org/10.1109/IAC.2017.8280541

Utomo, A. P. (2013). Analisa Dan Perancangan Sistem Informasi Parkir Di Universitas Muria Kudus. Simetris : Jurnal Teknik Mesin, Elektro Dan Ilmu Komputer, 3(1), 17. https://doi.org/10.24176/simet.v3i1.82