Analisis Risk Assesment Aplikasi Website Instansi XYZ dengan Menggunakan Metode Octave Allegro

Heri Susanto[1], Mohhamad Iqbal[2]
Universitas Gunadarama [1,2]
heri.s.aja@gmail.com, mohiqbal@staff.gunadarma.ac.id

Abstrak – Keamanan informasi telah menjadi elemen penting dalam suatu instansi seiring dengan kemajuan teknologi informasi. Kesenjangan dalam keamanan informasi berpotensi berdampak pada hilangnya informasi sensitif dan berharga karena berbagai ancaman yang akan datang yang dapat mempengaruhi organisasi di berbagai tingkatan, seperti pengeluaran keuangan , reputasi, dampak hukum, keselamatan kerja, insiden terhadap layanan, dan kinerja. Seringkali dampak yang terjadi dalam organisasi adalah karena kegagalan untuk mengidentifikasi atau menilai ancaman dan kerentanan diawal . Penelitian ini bertujuan untuk menganalisis risiko pada web aplikasi instansi XYZ, mendapatkan tingkat kerawanan informasi, dan menghasilkan rekomendasi untuk meningkatkan keamanan informasi pada aplikasi instansi tersebut, dengan menggunakan delapan langkah dalam metode OCTAVE Allegro. OCTAVE Allegro membuat profil aset informasi penting organisasi, menjalankan analisis risiko terhadap aset, dan mendefinisikan strategi mitigasi untuk setiap risiko yang teridentifikasi. Penelitian ini menghasilkan pendekatan mitigasi terhadap web aplikasi instansi XYZ berdasarkan nilai relative risk score (RSS) sehingga membantu organisasi dalam menganalisis risiko serta menentukan strategi yang tepat untuk menghadapi risiko.

Kata Kunci : Penilaian Risiko, Octave Alegro, Keamanan Informasi, Keamanan Asset Informasi, Analisis Web Aplikasi.

Abstract - *Information security has become an important element in an agency along with advances in information technology. Gaps in information security have the potential to result in the loss of sensitive and valuable information due to various impending threats that can affect organizations at various levels, such as financial expenses, reputation, legal repercussions, workplace safety, service incidents, and performance. Often the impact that occurs in organizations is due to a failure to identify or assess threats and vulnerabilities in advance . This study aims to analyze the risks in the XYZ agency web application, obtain the level of information vulnerability, and produce recommendations to improve information security in the agency's application, using eight steps in the OCTAVE Allegro method. OCTAVE Allegro profiles the organization's critical information assets, performs risk analysis on assets, and defines mitigation strategies for each identified risk. This research produces a mitigation approach to the XYZ agency web application based on the relative risk score (RSS) so that it helps organizations analyze risks and determine the right strategy to deal with risks.*

Keyword : Risk Asessment , Octave Alegro, Information Security, Information Assets Security, Web Application Analysis.

1. Latar Belakang

Berdasarkan laporan pemantauan keamanan internet Badan Siber dan Sandi Nasional (BSSN) terdapat 495.337.202 serangan siber ke Indonesia sepanjang 2020. Mengutip laporan dunia sekitar 60 hingga 70 persen sektor publik menjadi sasaran serangan siber. Sementara di Indonesia, situs pemerintah dengan domain .go.id menjadi sasaran empuk serangan. BSSN mencatat data serangan siber ini juga mencakup 2.885 serangan dari laporan publik dan 1.872 peretasan dari celah keamanan. Disamping itu, BSSN juga mencatat ada 16.939 insiden situs [1]. Perlindungan terhadap aset informasi dilakukan agar dapat menjaga tiga karakteristik penting dari informasi, yaitu confidentiality, integrity, dan availability. Dalam rangka untuk melindungi aset informasi yang krusial dan vital tersebut maka dibutuhkan pengelolaan yang akurat dan cepat, salah satunya adalah dengan mengimplementasikan manajemen risiko terkait keamanan informasi sesuai dengan kebutuhan perusahaan [2]. manajemen risiko yang tepat diperlukan oleh setiap perusahaan, baik perusahaan yang menjalankan bisnisnya secara langsung maupun melalui media online seperti e-commerce. Berbagai bidang bisnis pada e-commerce baik retail maupun finansial harus memperhatikan risiko yang mungkin dihadapi oleh perusahaan agar dapat menjaga confidentiality, integrity, dan availability dari informasi yang dikelola [3]. Saat ini belum banyak institusi yang melakukan risk assessment pada sistem informasi yang digunakan. Di satu sisi sistem informasi telah menjadi bagian yang sulit dipisahkan pada

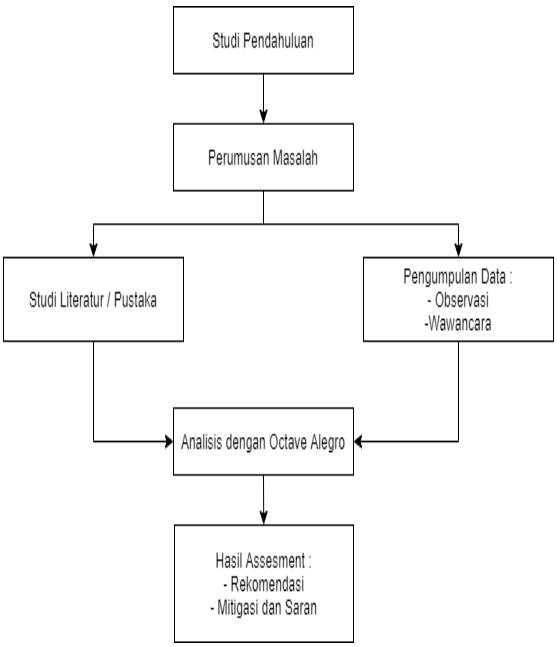
hampir setiap proses bisnis di institusi tersebut. Dengan demikian jika terdapat gangguan pada sistem informasi maka dapat mengganggu keberlangsungan proses bisnis institusi yang bersangkutan [4].
Dalam rangka untuk mengantisipasi risiko keamanan informasi dan kelangsungan TIK aplikasi tersebut, Instansi XYZ perlu untuk melakukan asesmen risiko aplikasi website Instansi XYZ dengan Metode Allegro Octave. Dari hasil assessment tersebut maka akan dapat ditentukan rekomendasi dan tindak lanjut yang harus dilakukan oleh manajemen terhadap kelangsungan proses bisnis organisasi

2. Kajian Pustaka

Dokumen yang dibuat oleh Richard A. Caralli, James F. Stevens, Lisa R. Young, dan William R. Wilson tahun 2007 dengan judul "The OCTAVE Allegro Guidebook, v1.0". Pada dokumen tersebut terdapat tahapan-tahapan yang perlu dilakukan ketika melakukan penilaian risiko dengan menggunakan framework OCTAVE Allegro
Selain itu salah satu penelitian sebelumnya yang memiliki kemiripan dengan penelitian yang dilakukan penulis saat ini yaitu penelitian yang dilakukan oleh Grafit Dwiananto (2012) dengan judul penelitian "Analisis Penerapan Kerangka Kerja Small to Medium Entity Risk Assessment Model (SMERAM) dalam Melakukan IT Risk Assessment di Bank Perkreditan Rakyat (BPR)". Dalam penelitian tersebut Grafit melakukan penilaian risiko terhadap aset teknologi informasi yang dimiliki oleh perusahaan keuangan kecil dan menengah Bank Perkreditan Rakyat (BPR) dengan menggunakan framework Small to Medium Entity Risk Assessment Model (SMERAM). Penelitian tersebut penulis anggap memiliki kemiripan dengan penelitian yang penulis lakukan karena sama-sama melakukan penilaian risiko dari aset yang dimiliki oleh perusahaan
Joshua Jenriwan L. Tobing dan Ayu Kartika Puspa (2015) menulis dalam jurnal EXPERT (jurnal sistem informasi) yang berjudul "Analisis Manajemen Risiko untuk Evaluasi Aset Menggunakan Metode Octave Allegro" bahwa metode octave allegro bisa digunakan opsi dalam melakukan manajemen risiko TIK spesifik/khusus untuk setiap pelanggan, kemudahan konsultasi dalam pembelian produk furniture, dapat menampung jumlah produk furniture lebih banyak tanpa terkendala luas bangunan.

3. Metode Penelitian

Metodelogi penelitian yang dilakukan penulis dalam melakukan tahapan tahapan penelitian tertuang dalam bentuk flowchart sebagai berikut



Gambar 1. Flowchart Penelitian

3.1 Studi Pendahuluan

Studi Pendahuluan yaitu dengan melakukan penelaahan terlebih dahulu dengan informasi data yang ada, realita yang ada, sumber ilmiah seperti jurnal, skrispi dan karya tulis lainnya.

3.2 Perumusan Masalah

Setelah dilakukan studi pendahuluan kemudian dilakukan identifikasi masalah yang ada untuk dilakukan perumusan masalah dan pembatasan ruang lingkup untuk menjadi topik penelitian ini. Masalah yang ditemukan yaitu terkait pengelolaan risiko IT aplikasi website Intansi XYZ dengan menggunakan metode octave allegro

3.3 Studi Literatur

Masalah yang ditemukan tersebut kemudian dipecahkan dengan melakukan studi pustaka untuk menjadi panduan dan pedoman dalam mencari solusi dari masalah yang ditentukan. Kegiatan yang dilakukan yaitu dengan melihat studi pustaka terkait pengelolaan manajemen risiko TIK dengan menggunakan octave allegro. Terdapat tiga kriteria yang digunakan sebagai landasan dalam penelitian, yaitu relevansi, kemutakhiran dan keaslian. Relevanasi berati teori yang dikemukakan sesuai dengan permasalahan yang diteliti. Kemutakhiran berarti terkait dengan kebaruan

teori atau referensi yang digunakan. Keaslian terkait dengan keaslian sumber penelitian. Dalam penelitian ini dilakukan studi literatur dari buku-buku, jurnal atau referensi lain yang berhubungan dengan penulisan laporan penelitian.

3.4 Pengumpulan Data

a. Observasi

Dalam penelitian ini dilakukan observasi untuk mendapatkan data tentang keadaan objek yang sedang terjadi saat ini. Hasil observasi tersebut digambarkan dengan sistem flowchart untuk menggambarkan alur proses bisnis yang sedang berjalan. Adapun jenis dan sumber pengumpulan data yang penulis gunakan saat melakukan penelitian di Instansi XYZ adalah dengan menggunakan Data Primer dan data sekunder.Data primer adalah data atau segala informasi yang diperoleh dan didapat langsung berupa tanggapan, saran, kritik, pernyataan dan penilaian dari Manajemen Instansi XYZ dan stakeholder Instansi XYZ. Data sekunder yaitu merupakan data yang diperoleh secara tidak langsung yang didapatkan dari data atau arsip yang dimiliki oleh pihak Instansi XYZ melalui pihak

b. Wawancara

Dalam penelitian ini dilakukan wawancara kepada Manajemen Instansi XYZ untuk mengetahui pendapat/pemaparan terkait dengan aplikasi website Instansi XYZ

Tabel 1. Pertanyaan Terkait Organisasi XYZ

No.	Pertanyaan
1.	Apakah Instansi XYZ selama ini melakukan manajemen risiko IT terhadap aplikasi website Instansi XYZ dengan baik?
2.	Adakah indikator-indikator keberhasilan yang ditetapkan untuk kegiatan Manajemen Risiko IT yang diadakan oleh Instansi XYZ?
3	Apakah dengan adanya sistem ini berdampak pada Instansi XYZ dan selanjutnya mendukung dalam peningkatan kualitas kegiatan yang dapat berpengaruh pada peningkatan Manajemen Risiko IT?
4	Area apa sajakah yang terdampak akibat penggunaan aplikasi Website Instansi XYZ?

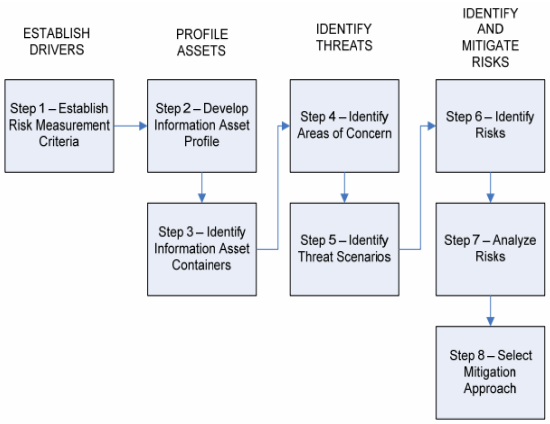
Selain itu dalam penelitian ini dilakukan pula wawancara terkait portal aplikasi untuk user dimana user dapat menjawab secara langsung tanpa pengaruh dari orang lain.

Tabel 2. Pertanyaan terkait portal aplikasi untuk user

No.	Pertanyaan
1.	Apakah Anda puas dengan pelayanan yang tersedia ketika megakses terhadap aplikasi website Instansi XYZ?
2.	Adakah indikator-indikator keberhasilan apa yang anda harapkan terhadap website Instansi XYZ? Pilihan: *Confidentiality, Integrity, Availability*
3	Apakah dengan adanya sistem ini berdampak pada Instansi XYZ dan selanjutnya mendukung dalam peningkatan kualitas kegiatan yang dapat berpengaruh pada peningkatan kinerja Anda?
4	Apa saja yang anda lakukan bila terjadi gangguan pada aplikasi website Instansi XYZ?

3.5 Analisis dengan Octave Alegro

Kegiatan ini yaitu dengan melakukan analisis risiko dengan menggunakan octave allegro terhadap aplikasi website Instansi XYZ dengan tahapan sebagaimana dijelaskan pada telaah pustaka. Konsep Analisis Risiko dengan Metode Octave Allegro adalah sebagaimana pada Gambar Tahapan Octave Allegro.



Gambar 2. Tahapan Octave Alegro

3.6 Hasil Asessment

Hasil dari analisis Analisis risiko aplikasi website Instansi XYZ akan menghasilkan output berupa hasil asesmen dan rekomendasi sehingga bisa ditarik kesimpulan dan saran

4. Hasil dan Pembahasan

4.1 Hasil Pengumpulan Data

Hasil yang diperoleh dari pengumpulan data dengan beberapa pihak managemen adalah sebagai berikut

Tabel 3. Hasil dan Jawaban Manajemen

No.	Pertanyaan dan Jawaban
1.	Apakah Instansi XYZ selama ini melakukan manajemen risiko IT terhadap aplikasi website Instansi XYZ dengan baik? Jawab: iya, Instansi XYZ saat ini melakukan manajemen risiko dengan pendekatan *Balance Score Card (BSC)* dan Indikator Kinerja Utama. Hal itu sesuai dengan Ketentuan dan Keputusan Manajemen pada Instansi XYZ.
2.	Adakah indikator-indikator keberhasilan yang ditetapkan untuk kegiatan Manajemen Risiko IT yang diadakan oleh Instansi XYZ? Jawab: Indikator keberhasilan dari manajemen risiko yang ada saat ini yaitu mampu memitigasi risiko yang ada dengan baik sehingga risiko tersebut tidak memberikan dampak yang besar terhadap kelangsungan organisasi.
3	Apakah dengan adanya sistem manajemen risiko ini berdampak pada Instansi XYZ dan selanjutnya mendukung dalam peningkatan kualitas kegiatan yang dapat berpengaruh pada peningkatan Manajemen Risiko IT? Jawab: iya berdampak dan itu sesuai dengan amanah Ketentuan dan Keputusan Instansi XYZ.
4	Area apa sajakah yang terdampak akibat penggunaan aplikasi Website Instansi XYZ? Jawab: Seluruh stakeholder TIK Instansi XYZ akan terhadap yaitu meliputi layanan TIK yang akan terganggu dan akan berdampak pada layanan lain.

Dan hasil yang diperoleh dari pengumpulan data dengan beberapa responden adalah sebagai berikut

Tabel 3. Hasil dan Jawaban Responden

No.	Pertanyaan dan Jawaban
1.	Apakah Anda puas dengan pelayanan yang tersedia ketika megakses terhadap aplikasi website Instansi XYZ? Jawab: 8 Responden Puas, 2 Responden Sangat Puas, hanya saja ketersediaan layanan website Intansi XYZ tidak mencapai 100%.
2.	Adakah indikator-indikator keberhasilan apa yang anda harapkan terhadap website Instansi XYZ? Jawab: 10 Responden mengatakan *Confidentiality, Integrity, Availability*
3	Apakah dengan adanya sistem ini berdampak pada Instansi XYZ dan selanjutnya mendukung dalam peningkatan kualitas kegiatan yang dapat berpengaruh pada peningkatan kinerja Anda? Jawab: 10 Responden mengatakanakan berdampak karena dengan digital working yang diterpkan menuntut *availability* website 100%
4	Apa saja yang anda lakukan bila terjadi gangguan pada aplikasi website Instansi XYZ? Jawab: 7 Responden mengatakan akan melaporkan ke unit layanan pengguna. 3 Responden menuggu perbaikan.

4.2 Hasil Analisa dengan Octave Alegro

a. Membangun kriteria pengukuran risiko

Langkah pertama adalah pembanguanan kriteria pengukuran risiko untuk impact area dan penentuan skala prioritas. Untuk impact area yang akan diukur disesuaikan dengan metode octave allegro yaitu meliputi lima kriteria. Penentuan level impact area sebagaimana hasil wawancara dengan manajemen adalah sebagaimana tabel berikut ini:

Tabel 5. Impact Area Reputasi Dan Kepercayaan Pelanggan

Reputasi Dan Kepercayaan Pelanggan		
Low	**Moderate**	**High**
Reputasi pelanggan sedikit terpengaruh jika terjadi kerusakan terhadap sistem dengan usaha penanganan sistem yang dilakukan pada saat kerusakan sistem	Reputasi pelanggan sedikit terpengaruhi jika terjadi kerusakan dalam sistem yang sedang, dengan perbaikan dengan membutuhkan waktu yang singkat	Reputasi pada tingkatan ini, dimana sangat mempengaruhi pelanggan dengan reputasi yang buruk dan menggangu membutuhkan waktu yang lama dan biaya yang cukup banyak

Tabel 6. Impact Area Finansial

Finansial		
Low	**Moderate**	**High**
Terjadi kerugian keuangan sampai dengan 100 juta ($x \leq$ *100 juta)*	Terjadi kerugian keuangan di atas 100 juta sampai dengan 1 Milyar (*100 juta* $< x \leq$ *1 Milyar)*	Terjadi kerugian keuangan di atas 1 Milyar ($x >$ 1 Milyar*)*

Tabel 7. Impact Area Kinerja

Kinerja		
Low	**Moderate**	**High**
Target kinerja pegawai akan menurun sampai dengan 10 % dari target kinerja	Target kinerja pegawai akan menurun 10% < x ≤ 20% dari target kinerja target kinerja	Target kinerja pegawai akan menurun di atas 20% dari target kinerja

Tabel 8. Impact Area Keamanan dan Kesehatan

Keamanan dan kesehatan		
Low	**Moderate**	**High**
Terjadi Cedera fisik Ringan, Gangguan kesehatan fisik ringan, Gangguan kesehatan mental ringan	Terjadi Cedera fisik sedang, Gangguan kesehatan fisik sedan, Gangguan kesehatan mental sedang	Terjadi Cedera fisik berat, Gangguan kesehatan fisik berat, Gangguan kesehatan mental berat

Tabel 9. Impact Area Denda dan Penalty

Denda dan *Penalty*		
Low	**Moderate**	**High**
Terjadi denda dan *penalty* keuangan sampai dengan 100 juta ($x \leq$ *100 juta)*	Terjadi Denda dan *Penalty* di atas 100 juta sampai dengan 1 Milyar (*100 juta* $< x \leq$ *1 Milyar)*	Terjadi kerugian keuangan di atas 1 Milyar ($x >$ 1 Milyar*)*

Tabel 10. Priority Impact Area

Priority	*Impact Areas*
5	Reputasi dan kepercayaan pelanggan
4	Finansial
2	Kinerja
1	Keamanan dan kesehatan
3	Denda dan penalti

Reputasi dan kepercayaan pelanggan memiliki tingkat prioritas paling tinggi sehingga dia mendapatkan poin 5 dari kelima impact area yang ditentukan. Sedangkan keamanan dan kesehatan memiliki tingkat prioritas paling rendah sehingga mendapatkan poin 1

b. Mengembangkan Profil Aset Informasi

Profil aset informasi kritis (Critical information asets profile) terdiri dari deskripsi aset informasi kritis itu sendiri, alasan pemilihan, dan pemiliknya (pengelola). Profil aset informasi kritis dilengkapi dengan persyaratan (requirements) keamanan yang harus ada untuk melindungi aset informasi kritis tersebut dengan menyatakan kerahasiaan (confidentiality), integritas (integrity), ketersediaan (availability), dan persyaratan keamanan lainnya, lalu dipilih persyaratan keamanan yang dianggap paling penting untuk aset informasi kritis tersebut. Pada tabel di bawah ini akan diberikan informasi tentang layanan informasi, pengguna sistem adalah orang yang menggunakan sistem dan core proses dari website Instansi XYZ

Tabel 11. Transaksi Layanan Informasi

Critical Asset		**Aplikasi Website Instansi XYZ**
Rationale for selection		Server Aplikasi Portal Instansi XYZ
Description		Terdiri dari database, aplikasi, dan jaringan
Owner		Instansi XYZ
Security Requirements	*Confidentiality*	Layanan informasi dapat diakses oleh seluruh user Instansi XYZ
	Integrity	Layanan informasi harus dan benar akurat, dapat dirubah dan di ganti oleh operator, hanya staff pelaksana harian bagian operasional pusat data atau pengelola aplikasi yang dapat memasukkan atau memodifikasi value dari database server dan jaringan
	Availability	Web aplikasi harus selalu tersedia bagi user terkait
Most Important Security Requirements		*Integrity* Alasan : database pada server merupakan aset penting bagi layanan informasi, jika terdapat error akan merugikan seluruh layanan.

c. Mengidentifikasi Kontainer dari Aset Informasi

Tahap ini akan menjelaskan tentang identifikasi suatu informasi asset dari suatu sistem mengenai tempat menyimpanan, dipindahkan serta tempat proses sistem yang digambarkan dengan worksheet Information Asset Risk Environment Map seperti pada tabel berikut.

Tabel 12. Kontainer Aset Informasi

Data Transaksi Website Instansi XYZ	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	***Owner(s)***
Module : Aset yang di dalamnya terdiri dari database, jaringan dan aplikasi yang digunakan Instansi XYZ dalam menggunakan layanan Instansi XYZ.	Instansi XYZ
External	***Owner(s)***
Container Description	User
Aplikasi : Portal Instansi XYZ	Instansi XYZ

d. Mengidentifikasi Area Masalah

Identifikasi areas of concern dengan meninjau kembali setiap container untuk melihat dan menentukan areas of concern yang potensial dilanjutkan dengan melakukan dokumentasi setiap areas of concern yang telah diidentifikasi. Areas of concern diperluas untuk mendapatkan threat scenarios kemudian didokumentasikan untuk melihat apakah mempengaruhi security requirements. Tabel berikut ini adalah area of concern web aplikasi Instansi XYZ dari sisi internal dan eksternal:

Tabel 13. Area of Concern (Server)

No.	*Area of Concern*
1	Akses terhadap ruangan server sangat mudah dapat mengakibatkan pihak yang tidak berwewenang mengakses server.
2	Penyebaran akses password transaksi layanan informasi oleh operator yang memiliki akses
3	Celah keamanan pada aplikasi portal Instansi XYZ dapat dieksploitasi oleh pihak dalam/ luar
4	Berhentinya layanan terjadi pada saat listrik padam karena tidak mempunyai *backup power* terhadap ruangan server

Tabel 13. Area of Concern (Client)

No.	*Area of Concern*
1	User tidak dapat mengakses portal aplikasi Instansi XYZ dengan availability 100% *(zero downtime)*

e. Mengidentifikasi Skenario Ancaman

Identifikasi threat scenario yang memberikan gambaran secara rinci mengenai property dari threat, antara lain actor, means, motives, outcome dan security requirement. Melengkapi Information Asset Risk Worksheets untuk setiap threat scenario yang umum. Tabel di bawah ini merupakan contoh properties of threat hasil perluasan dari areas of concern service catalog pada aplikasi portal Instansi XYZ.

Tabel 14. Threat Properties Akses Ruangan Server

Area of Concern	*Threat Properties*	
Akses terhadap ruangan server sangat mudah dapat mengakibatkan pihak yang tidak berwewenang mengakses server.	*1. Actor*	(Operator) Petugas Pusat Data
	2. Means	operator menggunakan
	3. Motives	Secara sengaja/tidak sengaja memeberikan akses server *(delibrate, accidental)*
	4. Outcome	*Disclosure, Modification, Interruption*
	5. Security Requirements	Memberikan pemahaman terhadap operator untuk menjaga akses ke ruangan server

Tabel 15. Threat Properties Akses Server

Area of Concern	*Threat Properties*	
Penyebaran akses password transaksi layanan informasi oleh operator yang memiliki akses	*1. Actor*	Operator aplikasi
	2. Means	operator menggunakan
	3. Motives	Secara sengaja/tidak sengaja pemberitahukan password *(delibrate, accidental)*
	4. Outcome	*Disclosure, Modification, Interruption*
	5. Security Requirements	Memberikan pemahaman terhadap operator untuk menjaga kerahasiaan password

Tabel 16. Threat Properties Celah Keamanan

Area of Concern	*Threat Properties*	
Celah keamanan pada aplikasi portal Instansi XYZ dapat di eksploitasi oleh pihak dalam/ luar	*1. Actor*	*Internal or external hackers*
	2. Means	a. *Improper information security infrastructure;* b. Pegawai masih kurang dalam hal *responsibility and security policy.* c. Aplikasi tidak dilakukan *update patching* dan *version.*
	3. Motives	Secara sengaja/tidak sengaja dengan adanya celah keamanan *(delibrate, accidental)*
	4. Outcome	*Disclosure, Modification, Interruption*
	5. Security Requirements	Memberikan pemahaman terhadap operator untuk menutup celah keamanan

Tabel 17. Threat Properties Back up power dan listrik

Area of Concern	*Threat Properties*	
Berhentinya layanan terjadi pada saat listrik padam karena tidak mempunyai *backup power* terhadap ruangan server	*1. Actor*	Operator/ Teknisi listrik
	2. Means	Operator/ Teknisi listrik salah dalam mengelola kehandalan listrik
	3. Motives	Secara sengaja/tidak sengaja *(delibrate, accidental)*
	4. Outcome	*Disclosure, Modification, Interruption*
	5. Security Requirements	Memberikan pemahaman terhadap operator untuk mengelola kehandalan listrik

Tabel 18. Threat Properties Availablilty Access oleh user

Area of Concern	*Threat Properties*	
User tidak dapat mengakses portal aplikasi Instansi XYZ dengan availability di bawah 100%	*1. Actor*	User Instansi XYZ
	2. Means	User tidak dapat mengakses aplikasi dengan tingkat availability di bawah 100%
	3. Motives	Secara sengaja/ tidak sengaja *(delibrate, accidental)*
	4. Outcome	*Disclosure, Modification, Interruption*
	5. Security Requirements	Memberikan pemahaman terhadap teknis menjaga *availability* sistem aplikasi

f. Mengidentifikasi Risiko

Identifikasi risiko bertujuan untuk menentukan bagaiman threat scenario memberikan dampak bagi organisasi serta menentukan tingkatannya apakah high, medium atau low. Dilanjutkan dengan menghitung relative score untuk membantu organisasi dalam menganalisis risiko serta menentukan strategi yang tepat untuk menghadapi risiko. Tabel di bawah ini menunjukan cara menghitung relative score.

Tabel 19. Cara Menghitung Relative Score

Impact Areas	Priority	Low (1)	Moderate (2)	High (3)
Reputasi dan kepercayaan pelanggan	5	5	10	15
Finansial	4	4	8	12
Produktivitas	3	3	6	9
Keamanan dan Kesehatan	1	1	2	3
Denda dan Penalti	2	2	4	6

g. Menganalisis Risiko

Tahap ini melakukan analisis terhadap total risiko yang merupakan hasil tahap sebelumnya. Hal ini dilakukan dengan mengkuantifikasikan kriteria pengukuran risiko dari tahap awal. Hasil kuantifikasi ini disebut skor risiko relatif yang diperoleh dengan cara menghitung skor untuk setiap area dampak dengan mengalikan nilai area dampak dengan nilai prioritas area dampak yang diperoleh dari urutan prioritas yang telah dibuat pada tahap awal. Kemudian nilai dampak dikuantitatifkan sebagai berikut : rendah (nilai 1), sedang (nilai 2), dan tinggi (nilai 3). Jumlah hasil perkalian tersebut di atas dan hasilnya adalah skor risiko relatif. Dibawah ini adalah table analisis risiko

Tabel 20. Area of Concern Ruangan Server

Area of Concern	*Risk*			
Akses terhadap ruangan server sangat mudah dapat mengakibatkan pihak yang tidak berwewenang mengakses server.	*Consequences*	Diperlukan pemahaman lebih terhadap operator akan pentingnya menjaga akses server oleh Pihak yang tidak berwenang		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Low	5
		Finansial	Low	4
		Produktivitas	Low	3
		Keamanan dan kesehatan	Low	2
		Denda dan *penalty*	Low	1
		Relative Risk Score		15

Tabel 21. Area of Concern Akses Pasword

Area of Concern	*Risk*			
Penyebaran akses password Transaksi layanan informasi oleh operator yang memiliki akses	***Consequences***	Diperlukan pemahaman lebih terhadap operator akan pentingnya menjaga kerahasiaan data dan password		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Low	5
		Finansial	Low	4
		Produktivitas	Low	3
		Keamanan dan kesehatan	Low	2
		Denda dan *penalty*	Low	1
		Relative Risk Score		15

Tabel 22. Area of Concern Celah Keamanan

Area of Concern	*Risk*			
Celah keamanan pada aplikasi portal Instansi XYZ dapat dieksploitasi oleh pihak dalam/ luar	***Consequences***	Diperlukan penutupan celah keamanan dan dilakukan asesmen keamanan informasi secara rutin		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Low	5
		Finansial	Low	4
		Produktivitas	Low	3
		Keamanan dan kesehatan	Low	2
		Denda dan *penalty*	Low	1
		Relative Risk Score		15

Tabel 23. Area of Concern Backup power dan listrik

Area of Concern	*Risk*			
Berhentinya layanan terjadi pada saat listrik padam karena tidak mempunyai backup power terhadap ruangan server	***Consequences***	Diperlukan backup power untuk mencegah berhentinya layanan saat terjadi listrik utama mati		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Low	5
		Finansial	Low	4
		Produktivitas	Low	3
		Keamanan dan kesehatan	Low	2
		Denda dan *penalty*	Low	1
		Relative Risk Score		15

Tabel 24. Area of Concern Akses Portal

Area of Concern	*Risk*			
User tidak dapat mengakses portal aplikasi Instansi XYZ dengan availability di bawah 100%	***Consequences***	Diperlukan monitor selama 7 x 24 jam dan redundansi aplikasi apabila aplikasi utama *down*		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Low	15
		Finansial	Low	4
		Produktivitas	High	9
		Keamanan dan kesehatan	Low	2
		Denda dan *penalty*	Low	1
		Relative Risk Score		31

Tabel 25. Relative Risk Matrix and Mitigation Approach

RISK SCORE		
30 TO 45	16 TO 29	0 TO 15
POOL 1	POOL 2	POOL 3
Mitigate	*Mitigate or Defer*	*Accept*

h. Memilih Pendekatan Mitigasi

Setelah melaukan identifikasi aset kritis, identifikasi risko dan penilaian risiko selanjutnya adalah melakukan mitigasi terhadap risiko tersebut. Mitigasi dilakukan dengan menggunakan standar ISO 27001 dan diskusi langsung dengan pihak Manajemen Instansi XYZ. Dari hasil identifikasi dan penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO 27001 yang direkomendasikan untuk penanganan risiko – risiko yang telah diidentifikasi tersebut.

4.3 Hasil Assesment

Dari hasil assessment manajemen risiko Aplikasi Website Instansi XYZ dengan menggunakan Metode Alegro Octave diperoleh Relative Risk Score (RSS) sebagaimana tabel di bawah ini:

Tabel 26. Hasil assessment manajemen risiko

No.	*Area of Concern*	*Relative Risk Score*	*Mitigation Approach*
1	Akses ruangan server	15	Accept
2	Penyebaran akses password	15	Accept
3	Celah keamanan aplikasi	15	Accept
4	Backup power dan listrik	15	Accept
5	*Availability* aplikasi	31	Mitigate

Rekomendasi atas manajemen risiko Aplikasi Website Instansi XYZ yaitu dengan menggunakan standar ISO 27001 dan diskusi langsung dengan pihak Manajemen Instansi XYZ. Dari hasil identifikasi dan penilaian risiko maka berikut beberapa kontrol objektif dari standar ISO 27001 yang direkomendasikan untuk penanganan risiko - risiko yang telah diidentifikasi tersebut adalah :

a. Identifikasi risiko modifikasi dan pencurian database
b. Identifikasi risiko backup data failure
c. Identifikasi risiko human/technician error
d. Identifikasi risiko Hardware dan Software failure
e. Identifikasi risiko power failure
f. Identifikasi risiko network failure
g. Identifikasi risiko kebakaran dan bencana alam
h. Identifikasi risiko Pencurian media atau dokumen penting.

5. Kesimpulan

Penelitian ini telah menghasilkan analisis risiko yang dapat terjadi dalam aplikasi Website Instansi XYZ. Penerapan metode OCTAVE Allegro telah menghasilkan pemetaan sistem dampak dengan hasil pendekatan Mitigasi untuk sistem aplikasi Website Instansi XYZ. Dari hasil identifikasi risiko ada 12 kontrol dalam ISO 27001 yang dapat digunakan sebagai referensi untuk menentukan rekomendasi mitigasi risiko. Hasil ini dapat merekomendasikan manajemen tingkat atas untuk mengubah pola kerja operator layanan untuk lebih meningkatkan kesadaran kerahasiaan data. Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah - langkah pemulihan jika skenario ancaman benar - benar terjadi..

6. Pustaka

[1] Laporan pemantauan keamanan internet Badan Siber dan Sandi Nasional (2020) Retrieved from https://bssn.go.id/bssn-publikasikan-hasil-monitoring-keamanan-siber-tahun-2020/

[2] Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson. (1999). Operationally Critical Threat, Asset, And Vulnerability Evaluations (Octave(Sm)) Framework. Pittsburgh: Carnegie Mellon University.

[3] A. M. Suduc, M. Bîzoi dan F. G. Filip. (2010). Audit for Information Systems Security. Jakarta: Journal Informatica Economica.

[4] AS/NZS. (2004). Risk Management Guidelines: Companion to AS/NZS 4360 : 2004. Sydney: Standards Australia Internasional.

[5] Caralli, R. A. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Pittsburgh: Carnegie Mellon University.

[6] Isaca. (2009). An introduction to the business model for information security', isaca journal it and governance profe ssion a l s, certified information systems auditor (cisa). United State: ISACA.

[7] Jakaria, D. A., Dirgahayu, R. T., & Hendrik. (2013). Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metode Octave Allegro. Seminar Nasional Aplikasi Teknologi Informasi (pp. E-37 - E-42). Yogyakarta: Universitas Islam Indonesia.

[8] Moleong, L.J. (2011). Metodologi Penelitian Kualitatif Edisi Revisi. Bandung: PT. Remaja Rosdakarya.

[9] Supradono, b. (2009). Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat , Asset , And Vulnerability Evaluation)', 2(1), pp. 4–8.

[10] Ufri, M. T., Hendayun, M. And 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), Pp. 1–6. Doi:10.1109/Iac.2017.8280541..