ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ANALYTICAL HIRARCHY PROCESS PADA DATA CENTER PEMERINTAH KABUPATEN BULELENG

TESIS

Oleh

NYOMAN BUDARSA

NIM : 1729101006

UNIVERSITAS PENDIDIKAN GANESHA

PASCASARJANA

PROGRAM STUDI ILMU KOMPUTER

FEBRUARI 2022


UNIVERSITAS PENDIDIKAN GANESHA
UNDIKSHA

ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ANALYTICAL HIRARCHY PROCESS PADA DATA CENTER PEMERINTAH KABUPATEN BULELENG

TESIS Diajukan

Kepada

Universitas Pendidikan Ganesha untuk

Memenuhi Sebagian Persyaratan

Memperoleh Gelar Magister Ilmu Komputer

Program Studi Ilmu Komputer

Oleh :

Nyoman Budarsa

NIM : 1729101006

UNIVERSITAS PENDIDIKAN GANESHA

PASCASARJANA

PROGRAM STUDI ILMU KOMPUTER

FEBRUARI 2022

LEMBAR PERSETUJUAN PEMBIMBING

Tesis oleh Nyoman Budarsa ini telah diperiksa dan disetujui untuk mengikuti ujian Tesis

Singaraja, Desember 2021

Pembimbing I

DR. GEDE INDRAWAN,S.T.,M.T
NIP. 197601012003121001

Pembimbing II

DR. I GEDE ARIS GUNADI,S.SI.,M.KOM
NIP. 197703182008121004

LEMBAR PERSETUJUAN TIM PENGUJI

Tesis oleh Nyoman Budarsa ini telah berhasil dipertahankan di depan tim penguji dan dinyatakan diterima sebagai Sebagian persyaratan untuk memperoleh gelar Magister Komputer di Program Studi Ilmu Komputer, Program Pascasarjana Universitas Pendidikan Ganesha.

Disetujui 17 Februari 2022

Oleh

Tim Penguji

.....	Ketua (Dr. Gede Indrawan, S.T.,M.T) NIP. 197601022003121001
.....,	Anggota (Dr. I Gede Aris Gunadi,S.Si.,M.Kom) NIP. 197703182008121004
.....	Anggota (Prof. Drs. Sariyasa,M.Sc.,Ph.D. NIP. 196406151989021001
.....	Anggota (Kadek Yota Ernanda Aryanto,S.Kom.,M.T NIP. 197803242005011001
.....	Anggota (Dr. Gede Indrawan, S.T.,M.T) NIP. 197601022003121001

Mengetahui Direktur
Pascasarjana UNDIKSHA

Prof. Dr. I Gusti Putu Suharta,M.Si
NIP. 196212151988031002

LEMBAR PERNYATAAN

Saya menyatakan dengan sesungguhnya bahwa tesis yang saya susun sebagai syarat untuk memperoleh gelar Magister Komputer dari Program Pascasarjana Universitas Pendidikan Ganesha seluruhnya merupakan hasil karya sendiri. Bagian – bagian tertentu dalam penulisan tesis yang saya kutip dari hasil karya orang lain telah dituliskan sumbernya secara jelas dan sesuai dengan norma, kaidah, serta etika akademis.

Apabila di kemudian hari ditemukan seluruh atau sebagian tesis ini bukan hasil karya sendiri atau adanya plagiat dalam bagian bagian tertentu, saya bersedia menerima sanksi pencabutan gelar akademik yang saya sandang dan sanksi – sanksi lainya sesuai dengan peraturan perundang – undangan yang berlaku di wilayah Negara Kesatuan Republik Indonesia.

Singaraja, Desember 2021

Yang memberi pernyataan,

Nyoman Budarsa

PRAKATA

Puji syukur penulis panjatkan kehadapan Tuhan Yang Maha Esa atas segala rahmat dan karunia-Nya sehingga penulis bisa menyelesaikan tugas akhir ini sesuai dengan waktu yang ditentukan. Tugas akhir yang berjudul "Analisis Risiko Keamanan Informasi Menggunakan Metode OCTAVE Allegro dan Analytical Hicarchy Process pada Data Center Pemerintah Kabupaten Buleleng".

Penulisan tugas akhir ini merupakan salah satu persyaratan akademis untuk memperoleh gelar Magister Komputer pada program studi Ilmu Komputer. Dalam penyusunan tugas akhir ini, penulis banyak mendapat dukungan dan masukan dari berbagai pihak.

Untuk itu dengan segala ketulusan dan kerendahan hati, penulis mengucapkan terima kasih kepada:

1. Bapak Dr. Gede Indrawan, S.T., M.T. selaku dosen pembimbing I yang telah memberikan petunjuk dan bimbingan kepada penulis selama penyusunan tesis ini.
2. Bapak Dr. I Gede Aris Gunadi, S.Si. M.Kom. selaku dosen pembimbing II yang telah memberikan petunjuk dan bimbingan kepada penulis selama penyusunan tesis ini.
3. Bapak Ketua Program Studi Ilmu Komputer dan staff dosen pengajar yang telah banyak membantu dan memotivasi penulis selama perjalanan studi dan penyusunan tesis ini.
4. Bapak Direktur Program Pascasarjana Undiksha dan staff, yang telah banyak membantu penulis mengikuti studi dan menyelesaikan penulisan tesis ini;

5. Bapak Rektor Universitas Pendidikan Ganesha, yang telah memberikan bantuan secara moral dan memfasilitasi berbagai kepentingan studi, selama penulis menempuh perkuliahan di Program Pascasarjana Undiksha;
6. Orang tua tercinta, yang telah memberikan dorongan sehingga penulis dapat menyelesaikan tesis ini.
7. Istri, anak dan saudara yang selalu memberikan support dan doa.

Penulis menyadari bahwa tesis ini masih jauh dari kesempurnaan. Oleh sebab itu penulis mengharapkan saran dan kritik yang bersifat membangun demi kesempurnaan tesis ini. Akhir kata penulis berharap semoga tesis ini bermanfaat bagi pembaca.

Singaraja, Desember 2021

Penulis

ABSTRAK

Budarsa,Nyoman (2021), *Analisis Risiko Keamanan Informasi Menggunakan Metode OCTAVE Allegro dan Analytical Hirarchy Proces (AHP) pada Data Center Pemerintah Kabupaten Buleleng*. Tesis,Ilmu Komputer, Pascasarjana, Universitas Pendidikan Ganesha.

Tesis ini sudah disetujui dan diperiksa oleh Pembimbing I : Dr. Gede Indrawan,S.T.,MT dan Pembimbing II : Dr. I Gede Aris Gunadi,S.Si.,M.Kom

Kata- kata kunci : keamanan informasi, OCTAVE Allegro, AHP

Penggunaan teknologi informasi dan komunikasi dalam bidang pemerintahan merupakan suatu hal yang penting untuk mendukung sistem pemerintahan berbasis elektronik. Data center merupakan pusat dari infrastruktur teknologi informasi yang memiliki peran yang sangat strategis yang menentukan kelangsungan sistem pemerintahan berbasis elektronik untuk pelayanan publik dan administrasi pemerintahan. Namun, dalam impelementasi sistem pemerintahan berbasis elektronik pada data center Pemerintah Kabupaten Buleleng terdapat peluang munculnya risiko keamanan informasi yang mengakibatkan terganggunya pelayanan publik dan administrasi pemerintahan. Aspek keamanan informasi ini meliputi aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Penelitian ini bertujuan untuk menghasilkan analisis risiko keamanan teknologi informasi dan komunikasi pada instansi pelayanan publik. Metode yang digunakan untuk analisis risiko keamanan informasi ini adalah OCTAVE Allegro karena metode ini sangat sesuai dengan karakteristik pada instansi pemerintah. Sebagai tindak lanjut dari hasil profil risiko yang dihasilkan, selanjutnya diolah sistem penunjang keputusan, yaitu Analitic Hirarchy Process (AHP). Hasil analisis risiko menggunakan metode OCTAVE Allegro ditemukan 9 area perhatian terhadap asset informasi yang dianggap paling kritis. Selanjutnya menggunakan metode AHP dapat ditentukan peringkat risiko dari area perhatian dari yang memiliki risiko paling besar sampai paling kecil. Hasil penelitian ini diharapkan dapat dijadikan pedoman dalam kebijakan pengelolaan data center pada instansi pemerintah.

ABSTRACT

Budarsa,Nyoman (2021), *Information Security Risk Analisis Using OCTAVE Allegro Method and Analytical Hirarchy Proces (AHP) at Data Center of Buleleng Regency.* Tesis,Ilmu Komputer, Pascasarjana, Universitas Pendidikan Ganesha.

This thesis has been approved anda examined by Supervisor I : Dr. Gede Indrawan,S.T.,MT dan Supervisor II : Dr. I Gede Aris Gunadi,S.Si.,M.Kom

Keyword : Information Security, OCTAVE Allegro, AHP

The use of information and communication technology in the field of government is an important thing to support an electronic-based government system. Data center is the center of the information technology infrastructure that has a very strategic role in determining the continuity of the electronic-based government system for public services and government administration. However, in the implementation of an electronic-based government system at data center of Buleleng Regency Government, there is an opportunity for information security risks to arise which result in disruption of public services and government administration. Aspects of information security include aspects of confidentiality, integrity, and availability. This study aims to produce a risk analysis of information and communication technology security in public service agencies. The method used for this information security risk analysis is OCTAVE Allegro because this method is very in line with the characteristics of government agencies. As a follow-up to the results of the resulting risk profile, a decision support system is then processed, namely the Analytical Hierarchy Process (AHP). The results of the risk analysis using the OCTAVE Allegro method found 9 areas of concern for information assets that are considered the most critical. Furthermore, using the AHP method, the risk rating of the area of concern can be determined from the one with the greatest to the least risk. The results of this study are expected to be used as guidelines in data center management policies in government agencies.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi informasi dan komunikasi dalam bidang pemerintahan merupakan suatu hal yang penting untuk mendukung sistem pemerintahan berbasis elektronik. Data center merupakan pusat dari infrastruktur teknologi informasi yang memiliki peran yang sangat strategis yang menentukan kelangsungan sistem pemerintahan berbasis elektronik untuk pelayanan publik dan administrasi pemerintahan.

Pemerintah Kabupaten Buleleng memiliki data center yang berada di Dinas Komunikasi Informatika Persandian dan Statistik yang di dalamnya terdapat infrastruktur teknologi informasi seperti komputer server dan perangkat jaringan. Terdapat 12 (dua belas) server fisik yang digunakan untuk menampung sistem informasi untuk pelayanan publik dan administrasi pemerintahan.

Namun, dalam impelementasi sistem pemerintahan berbasis elektronik pada data center Pemerintah Kabupaten Buleleng terdapat peluang munculnya risiko keamanan informasi yang mengakibatkan terganggunya pelayanan publik dan administrasi pemerintahan. Aspek keamanan informasi ini meliputi aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Keamanan informasi tidak hanya tergantung pada alat dan teknologi, akan tetapi membutuhkan kesadaran dalam organisasi tentang apa yang harus dilindungi dan pemilihan solusi yang tepat untuk menangani masalah dalam kebutuhan keamanan informasi(Jufri et al., 2018).

Diperlukan analisis risiko keamanan informasi untuk mengetahui adanya ancaman dan kerentanan informasi sehingga dapat ditentukan peringkat risiko dari yang terbesar

sampai yang terkecil. Hasil analisis risiko ini dapat dijadikan acuan dalam membuat perencanaan pengelolaan data center serta sebagai penunjang keputusan ketika terjadi gangguan dalam implementasi sistem pemerintahan berbasis elektronik. Beberapa permasalahan yang yang sering dialami oleh pengguna data center pemerintah Kabupaten Buleleng antara lain, server tidak dapat diakses dari beberapa pengguna, adanya peretasan terhadap aplikasi yang berbasis website, dan lambatnya koneksi ke aplikasi pelayanan publik maupun administrasi pemerintahan.

Ada banyak metode penilaian risiko yang tersedia, diantaranya Panduan untuk Melakukan Penilaian Risiko (Institut Nasional Standard dan teknologi [NIST],2012, COBIT, ISO 27005 dan OCTAVE. Penelitian ini fokus pada analisis, identifikasi dan penilaian risiko keamanan informasi pada Data Center Pemerintah Kabupaten Buleleng menggunakan metode OCTAVE Allegro dan Analytical Hirarchy Process.(Prajanti & Ramli, 2019). Penggunaan dua metode ini diharapkan dapat memberikan hasil berupa peringkat risiko yang lebih cepat, akurat, dan bisa diterapkan sesuai dengan kondisi khususnya pada instansi pemerintah.

1.2 Identifikasi Masalah

Dari latar belakang pemasalahan dapat diidentifikasi masalah yaitu belum adanya analisis dan perencanaan terhadap risiko keamanan informasi pada Data Center Pemerintah Kabupaten Buleleng yang dapat digunakan untuk mengukur kerentanan informasi yang ada.

1.3 Pembatasan Masalah

Adapun penelitian ini dibatasi hanya analisis risiko keamanan informasi menggunakan metode OCTAVE Alegro dan AHP pada Data Center Pemerintah

Kabupaten Buleleng yang berada di Dinas Komunikasi Informatika Persandian dan Statistik Kabupaten Buleleng.

1.4 Rumusan Masalah

Berdasarkan latar belakang masalah yang dijelaskan diatas maka rumusan masalah dalama penelitian ini adalah:

1. Bagaimana menyusun analisis risiko keamanan informasi yang ada pada data center Pemerintah Kabupaten Buleleng menggunakan metode OCTAVE Allegro?
2. Bagaimana membuat peringkat potensi risiko menggunakan sistem penunjang keputusan AHP?

1.5 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengetahui gambaran yang lengkap dan komprehensif mengenai risiko keamanan informasi pada data center milik Pemerintah Kabupaten Buleleng yang dikelola oleh Dinas Komunikasi Informatika Persandian dan Statistik menggunakan metode OCTAVE Allegro. Hasil analisis tersebut selanjutnya dibuat peringkat risiko agar dapat dijadikan sebuah sistem penunjang keputusan dalam pengelolaan data center yang lebih baik.

1.6 Manfaat Penelitian

Manfaat penelitian ini adalah dapat diketahuinya risiko keamanan informasi pada Data Center Pemerintah Kabupaten Buleleng sehingga bisa ditentukan langkah perencanaan dan mitigasi terhadap keamanan informasi yang ada. Hasil dari penelitian

ini juga bisa diterapkan pada organisasi yang mengelola pusat data baik instansi swasta maupun instansi pemerintah.

BAB II
LANDASAN TEORI

2.1. Pengertian Risiko

Menurut Kamus Besar Bahasa Indonesia, risiko adalah akibat kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Setiap kegiatan atau proses selalu akan menyebabkan risiko karena risiko muncul karena ketidakpastian.

2.1.1. Analisis Risiko

Pengukuran risiko keamanan informasi adalah pekerjaan yang sulit dilakukan secara akurat pada sebuah sistem informasi (Munteanu, 2006). Analisis risiko dapat menggunakan pendekatan kuantitif dan kualitatif. Pada pendekatan kuantitatif terdapat tahapan penilaian dari masing – masing asset. Untuk mendapatkan niali asset seperti informasi atau database, sangat terbuka peluang munculnya subjektifitas penilai. Karena dalam proses penilaian tersebut terdiri dari elemen yang harus ditaksir.

Sementara metode pendekatan kualitatif menggunakan kuesioner untuk mendapatkan fakta melalui perkiraan secara statistic dengan hasil *low, medium* dan *high* sehingga ada kesulitan untuk menghitung kerugian finansial jika hanya berdasar pada asumsi.

Analisis risiko menggunakan pendekatan kualitatif sangat diominasi oleh pengukuran subjektif, sedangkan pendekatan kuantitatif dapat menghilangkan sifat subjektif yang ada (Mazareanu, 2011). Metode kuantitatif lebih objektif dibandingkan motode kualitatif.

Manajemen risiko adalah bagian dari manajem sistem informasi yang ditujukan untuk menilai bagaimana ancaman dan kerentanan sistem informasi dan aset yang dimiliki. (Sardjono & Cholik, 2018). Manajemen risiko dapat mengurangi risiko seperti proses bisnis yang tidak optimal, pemborosan anggaran dan turunnya reputasi institusi.(Suroso & Fakhrozi, 2018).

Menurut Rhoespada tahun 2013 mengurangi risiko tidak berarti menghilangkannya, tetapi menurunkan tingkat risiko ke tingkat yang dapat diterima oleh organisasi tersebut. Untuk menjamin keamanan informasi, mengelola dan mengantisipasi risiko secara efektif diperlukanan alisis risiko, definisi ancaman dan dampak atau akibat yang ditimbulkan oleh risiko tersebut.

Dengan melakukan analisis dan identifikasi terhadap risiko yang ada, hal ini dapat memberikan strategi yang tepat untuk keamanan informasi dan mengurangi peluang munculnya area risiko berdampak pada asset – asset penting atau rahasia yang tidak terlindungi. Fokus pada evaluasi asset yang dimiliki adalah kunci keberlangsungan perusahaan.(Dorofee, 2005b). Tujuan melakukan analisis terhadap risiko adalah untuk memberikan gambaran terhadap peluang munculnya ancaman yang bisa terjadi sehingga organisasi bisa menyusun strategi dan langkah untuk mitigasi dan evaluasi risiko. Hasil analisis risiko dapat digambarkan ke dalam matrik risiko.

2.2. Sistem Pemerintahan Berbasis Elektronik

Sistem Pemerintahan Berbasis Elektronik (SPBE) atau sebelumnya disebut dengan *e-government* adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE(RI,

2020).Secara umum layanan SPBE ini adalah untuk pelayanan publik dan administrasi pemerintahan. Pengguna layanan SPBE ini meliputi instansi pemerintah, aparatur sipil negara, pelaku bisnis, masyarakat dan pihak – pihak lainnya. Agar sistem pemerintahan berbasis elektronik bisa berjalan dengan baik maka diperlukan tata kelola, infrastruktur dan sumber daya manusia yang handal.

2.3. Data Center

2.2.1. Pengertian Data Center

Data center adalah kumpulan server dan sistem penyimpanan data yang membutuhkan fasilitas khusus untuk menampung sumber daya yang dimiliki.(Riasetiawan, 2016) Pusat penampungan data ini memiliki criteria khusus dalam perancangannya, antara lain :

a. *Aviability*, yaitu mampu menjalankan opersi secara berkelanjutan dan terus menerus dalam kondisi apapun.

b. *Scalability*, yaitu mampu berdaptasi dengan penambahan kebutuhan dan teknologi baru tanpa merubah substansi data center secara keseluruhan.

c. *Security*, data center mampu melindungi asset data yang tersimpat pada server secara fisik maupun non fisik.

2.2.2. Data Center Pemerintah Kabupaten Buleleng

Server adalah infratruktur sistem pemerintahan berbasis elektronik yang memiliki peran yang sangat penting karena karena semua sistem informasi dan data tersimpan disana. Seluruh server harus ditempatkan pada data center yang memenuhi aspek keamaman informasi. Sesuai dengan tugas pokok dan fungsinya,

Pemerintah Kabupaten Buleleng memiliki data center yang ada di Dinas Komunikasi Informatika Persandian dan Statistik. Sistem informasi untuk pelayanan publik dan administrasi pemerintahan tersimpan pada data center ini. Berikut adalah aplikasi yang ada pada data center Pemerintah Kabupaten Buleleng:

Tabel 2.1. Data Sistem Informasi

No	Nama Sistem Informasi/ Aplikasi	Unit Pengelola	Pengguna
1	Aplikasi Perizinan Online	Dinas Perizinan	Instansi dan Publik
2	Sistem Informasi Kepegawaian	BKPSDM	Instansi
3	Sistem Pengadaan Barang Jasa	BPBJ	Instansi dan Publik
4	Website resmi Pemerintah Kabupaten Buleleng dan subdomainnya	Diskominfosanti	Publik
5	Aplikasi surat elektronik	Diskominfosanti	Instansi

Selain layanan untuk pengelolaan server dan sistem informasi, data center Pemerintah Kabupaten Buleleng juga sebagai pusat dari jaringan komunikasi antar unit perangkat daerah. Koneksi internet untuk seluruh unit SKPD terpusat pada data center. Oleh sebab itu jika ada gangguan pada data center maka seluruh kegiatan pemerintahan dan pelayanan publik menjadi terganggu.

2.4. Keamanan Informasi

Informasi merupakan aset yang sangat penting bagi organasisasi terutama instansi pemerintah. Keamanan informasi adalah usaha untuk melindungi aset informasi dalam segala bentuknya, baik tertulis, lisan, elektronik, grafis, dan lain-lain. Keamanan

informasi diusahakan untuk mencapai tiga sasaran utama yaitu aspek kerahasiaan, ketersediaan, dan ketersediaan informasi serta mencegah dan mengurangi hal-hal yang dapat terjadi seperti kerusakan, kehilangan atau juga informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak berkepentingan.

Ada tiga komponen yang memberi kontribusi kepada risiko keamanan informasi, yaitu asset (aset), vulnerabilities (kelemahan), dan threats (ancaman)(Rahardjo, 1998). Aset terdiri dari infrastruktur perangkat keras, perangkat lunak, dokumentasi, data, lingkungan dan manusia. Kelemahan meliputi *software bugs*, radiasi, *tapping*, hard copy, keteledoran dan media penyimpanan, Sementara ancaman meliputi pemakai, kecelakaan, dan *crackers*.

Keamanan informasi bagi instansi pelayanan publik sangat penting artinya karena akan mempengaruhi keberlangsungan pelayanan publik.

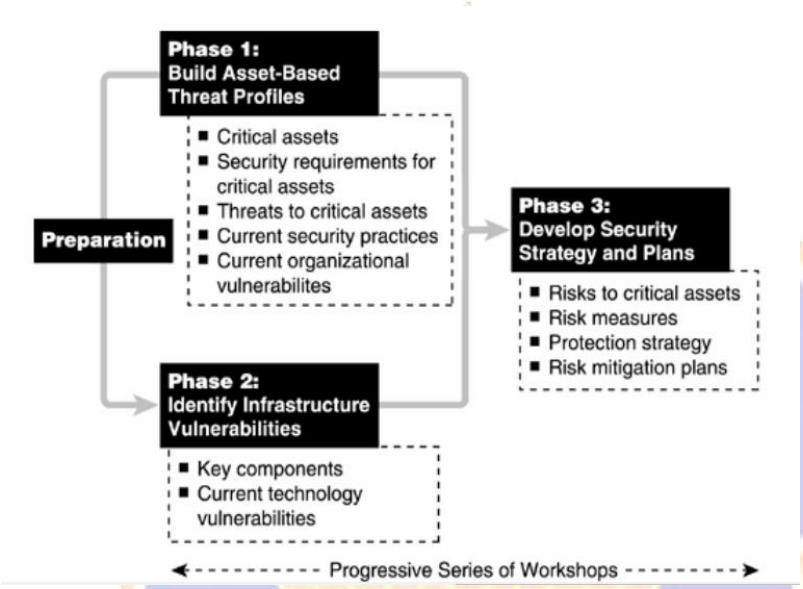
2.5. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) merupakan pendekatan untuk mengelola dan analisis risiko keamanan teknologi informasi. yang dikembangkan oleh Software Enginerring Insitute Universitas Carnegie Mellon. OCTAVE memiliki seperangkat peralatan, teknik, dan metode untuk penilaian dan perencanaan keamanan informasi. OCTAVE memiliki tiga varian, yaitu OCTAVE, OCTAVE S, dan OCTAVE Allegro. Ketiga metode tersebut bukanlah untuk saling melengkapi atau mengantikan satu dengan yang lain, namun untuk memenuhi kebutuhan sfesifik dari pengguna OCTAVE yang akan melakukan penilaian risiko.

Metode OCTAVE adalah versi OCTAVE yang pertama kali dikembangkan. Metode OCTAVE dilaksanakan dengn mengadakan serangkaian workshop dan

difasilitasi oleh tim analisis yang dibuat pada organisasi atau departemen teknologi informasi. Metode ini ditujukan untuk perusahaan besar yang memiliki lebih dari 300 karyawan.

OCTAVE menggunakan pendekatan tiga tahap dengan menguji isu – isu organisasi dan teknologi terhadap penyusunan masalah yang komperhensif berdasarkan kebutuhan keamanan informasi suatu organisasi.



Gambar 2.1. Metode OCTAVE

Dari gambar 2.1. diatas, metode OCTAVE dimulai pada tahap 1, yaitu tim analisis melakukan identifikasi aset informasi yang penting dan strategi perlindungan saat ini untuk asset dimaksud. Selanjutnya menentukan aset mana yang paling penting bagi organisasi, dokumen persyaratan keamanan informasi yang ada, dan melakukan identifikasi ancaman. Pada tahap 2, tim analisis melakukan evaluasi terhadap infrastruktur unttuk melengkapi analisis ancaman pada tahap 1. Pada tahap 3, tim analisis melakukan identifikasi dan membuat mitigasi risiko untuk aset yang bernilai kritis(Dorofee, 2005a).

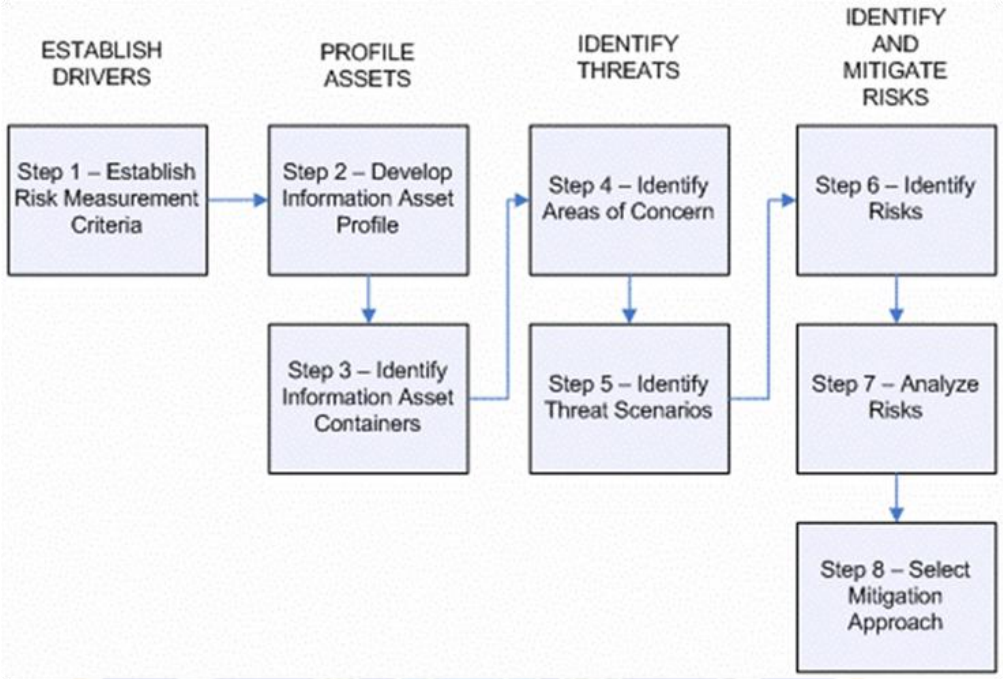
Sama seperti metode OCTAVE, OCTAVE-S juga terdiri dari tiga tahapan. Namun, pada metode OCTAVE-S dilakukan oleh tim analisis yang memiliki pengetahuan yang mendalam tentang perusahaan atau organisasi. OCTAVE-S tidak menggunkan informasi yang didapatkan dari workshop karena OCTAVE-S menggunakan asumsi bahwa timanalisis sudah memiliki pengetahuan tentang aset penting yang berkaitan dengan informasi, kebutuhan keamanan, ancaman dan prosedur keamaanan informasi yang ada pada organisasi.

2.5.1. Pengertian Metode OCTAVE Allegro

OCTAVE Allegro bertujuan untuk melakukan penilaian luas terhadap lingkungan risiko operasional dalam suatu organisasi tanpa perlu pengetahuan yang luas dalam hal penilaian risiko. Kata Allegro berarti dalam tempo yang lincah(Keating, 2014). Metode ini menggunakan pengetahuan seseorang tentang praktik dan proses keamanan informasi pada sebuah organisasi untuk melihat keadaan praktik keamanan saat ini pada organisasi.

OCTAVE Allegro merupakan sebuah kerangka kerja yang menggunakan pendekatan OCTAVE dan didesain untuk melakukan penilaian risiko terhadap operasional organisasi atau perusahaan. Tujuannya adalah untuk menghasilkan hasil penilaian profil risiko yang lebih cepat tanpa memerlukan pengetahuan mendalam terkait penilaian risiko atau audit. (Caralli et al., 2007). OCTAVE Allegro sedikit memiliki perbedaan jika dibandingkan dengan pendekatan OCTAVE lainnya karena framework ini fokus pada aset informasi yang oleh instansi dalam konteks bagaimana aset tersebut digunakan, bagaimana asset informasi ini disimpan, dipindahkan, dan diproses. Disamping juga bagaimana ancaman, kerentanan, dan gangguan dapat terjadi

pada aset tersebut. *Framework* OCTAVE Allegro terdiri atas delapan tahapan yang diklasifikasikan menjadi empat fase.



Gambar 2.2. Tahapan OVTAVE Allegro

Metode OCTAVE Allegro adalah salah satu contoh evaluasi yang konsisten dengan prinsip, atribut dan output.(Dorofee, 2005a) Metode ini bisa mengasilkan profil risiko dengan atribut yang konsisten sehingga dapat digunakan untuk proses pengambilan keputusan selanjutnya.

Instansi pemerintah memiliki karakteristik yang khusus terkait pengelolaan anggaran, sumber daya manusia dan waktu pengelolaan risiko keamanan informasi. OCTAVE Allegro bisa diterapkan pada organisasi dengan sumber daya seperti pada instansi pemerintah.(St et al., 2020)

Metode OCTAVE Allegro dapat diterapkan pada institusi pendidikan seperti universitas yang mengelola sistem informasi sendiri. (Kuntari et al., 2018). Sedangkan pada penilaian risiko pada rumah sakit, metode OCTAVE Allegro dapat menunjukan data

yang paling rentan dan memerlukan prioritas untuk mitigasi secepatnya. Tahap – tahap OCTAVE Allegro.(Matondang et al., 2018)

Terdapat empat tahap dalam OCTAVE Allegro, yaitu:

1. Membangun kriteria pengukuran, dimana instansi mengembangkan kriteria pengukuran risiko yang konsisten dengan organizational drivers (hal yang menggerakkan organisasi).
2. Mengembangkan profil aset, dimana asset informasi yang kritis digambarkan, dan mengidentifikasikan container asset.
3. Mengidentifikasikan ancaman, dimana ancaman terhadap aset (dalam lingkup container mereka) diidentifikasikan dan didokumentasikan melalui proses terstruktur.
4. Mengidentifikasi dan mitigasi risiko, dimana risiko yang diidentifikasikan dan dimitigasi selanjutnya mengembangkan pendekatan unttuk mitagsi yang akan dipilih.

2.5.1. Langkah – langkah OCTAVE Allegro:

Dari empat tahap tersebut, terdapat delapan langkah OCTAVE Allegro, yaitu:

1. Menetapkan kriteria pengukuran risiko

   Aktivitas pertama yaitu membuat defines ukuran kualitatif yang dituangkan pada *Risk Criteria Worksheet.* Kriteria pengukuran risiko digunakan untuk mengevaluasi akibat di setiap area dan memberikan nilai prioritas.
2. Membangun profil aset informasi

Langkah kedua adalah membangun profil aset informasi yang ada pada instansi. Profil asset adalah perwujudan dari aset informasi yang menggambarkan secara detail asset – asset yang sifatnya unik. Keluaran dari kegitan ini adalah profi asset informasi kritis yang dimiliki oleh instansi.

3. Mengidentifikasi container dari aset informasi

   Container adalah tempat dimana aset informasi disimpan, dikirim, dan diproses. Dalam langkah ketiga, semua container yang menyimpan, mengirim, dan memproses, baik internal maupun eksternal diidentifikasikan.

4. Mengidentifikasikan area yang diperhatikan

   Kegiatan pada langkah ini adalah identifikasi risiko menggunakan cara wawancara atau kolaboratif mengenai kondisi atau situasi yang memungkinkan yang dapat mengancam aset informasi organisasi.

5. Mengidentifikasi skenario ancaman

   Skenario ancaman akan menghasilkan informasi yang lengkap dan hasil pengembangan scenario ancaman dari area yang diperhatikan. Keluaran dari kegiatan ini adalah daftar asset informasi.

6. Mengidentifikasi risiko

   Pada langkah keenam, konsekuensi bagi organisasi jika sebuah ancaman terjadi dicatat, dalam mendapatkan gambaran risiko secara lengkap. Sebuah ancaman dapat mempunyai akibat – akibat yang potensial bagi organisasi.

7. Menganalisis risiko

Kegiatan langkah ketujuh, pengukuran kuantitatif sederhana dari sejauh mana organisasi terkena dampak dari ancaman dihitung. Memberi nilai risiko relative didapatkan dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai area terdampak, dan memperkirakan kemungkinannya.

8. Memilih pendekatan pengurangan risiko.

   Hasil dari pendekatan mitigasi resiko antari lain, matriks rasio relative, tingakat kerawanan informasi, daftar mitigasi untuk semua risiko yang ditemukan dan strategi mitigasi untuk setiap resikoyang telah diputuskan untuk dilakukan mitigasi.

2.6. Pengertian Analytic Hierarchy Process (AHP)

Analytic Hierarchy Process (AHP) adalah teknik terstruktur untuk mengatur, menganalisis dan membuat keputusan yang komplek dan didasarkan pada matematika dan psikologi.(Magdalenić et al., n.d.). AHP dikembangkan oleh Prof. Thomas Lorie Saaty (1998) dari Wharston Business school untuk mencari ranking atau urutan prioritas dari berbagai alternatif dalam pemecahan suatu permasalahan.

AHP adalah suatu teori umum tentang pengukuran untuk menemukan skala rasio baik dari perbandingan berpasangan yang diskrit maupun kontinu.AHP memiliki perhatian khusus tentang penyimpangan dari konsistensi, pengukuran dan ketergantungan di dalam dan di luar kelompok elemen strukturalnya(Saaty, 1987).

AHP dapat digunakan untuk mencari ranking dari hasil analisis risiko keamanan informasi. (Badie & Lashkari, 2012) Peran manusia memegang peranan penting pada

terjadinya risiko keamanan informasi. Mengingat banyaknya faktor penyebab terjadinya risiko maka perlu prioritas yang akan di mitigasi.(Thibadeau, 2007)

*Analytic Hierrchy Process (*AHP) mempunyai beberapa landasan aksiomatik sebagai berikut:

1. *Resiprocal Comparison*, yang dapat diartikan bahwa matriks perbandingan berpasangan yang terbentuk harus bersifat berkebalikan.
2. *Homogenity*, yang dapat diartikan sebagai kesamaan dalam melakukan perbandingan.
3. *Dependence*, yang berarti setiap tingkatan mempunyai kaitan (*complete hierarchy)* walaupun mungkin saja terjadi hubungan yang tidak sempurna *(incomplete hierarchy)*.
4. *Expectation*, yang artinya menonjolkan penilaian yang bersifat ekspektasi dan pilihan dari pengambilan keputusan. Penilaian dapat merupakan data kuantitatif atau yang bersifat kualitatif.

Tiga prinsip yang harus dipahami untuk menyelesaikan suatu permasalahan dengan metode AHP yaitu:

1. *Decomposition*, yaitu memecah persoalan yang utuh menjadi unsur – unsur yang saling berhubungan dalam bentuk struktur hirarki.

2. *Comparative Judgement*, yaitu dengan memberikan penilaian tentang kepentingan relative dua elemen pada suatu tingkat tertentu dalam kaitannya dengan tingkatan diatasnya untuk memberikan urutan prioritas dari elemennya.

3. *Logical Consistency*, yaitu objek yang serupa dapat dikelompokkan sesuai dengan keseragaman dan relevansinya.

2.6.1. Langkah – Langkah Penggunaan *Analytical Hierarchy Proses* (AHP)

Adapun langkah – langkah dalam menentukan peringkat menggunakan metode AHP (Pangestika & Siregar, 2018) adalah sebagai berikut :

1. Mendefinisikan masalah dan menetukan solusi yang diinginkan.
2. Membuat struktur hirarki yang diawali dari tujuan umum dan dilanjutkan dengan kriteria dan alternatif yang akan dibuatkan peringkat atau rangking.
3. Membentuk matriks perbandingan berpasangan yang akan menggambarkan kontribusi *relative* atau pengaruh setiap elemen terhadap masing – masing kriteria yang setingkat diatasnya.
4. Menghitung niali *eigen vector* dan menguji nilai konsistensinya, jika tidak konsisten maka pengambilan data harus diulang
5. Menghiting nilai eigen vector dari setiap matriks perbandingan berpasangan.
6. Menguji konsistensi hirarki. Prinsip kerja dari rasio konsistensi adalah menentukan bobot sesuai kriteria(Naskar & Bose, 2011).

   Rumus untuk Consistency Ratio:

$$CR = \frac{Ci}{Ri}$$

   Keterangaan:

   Consitensi Ratio (CR) = apabila niali CR ≤ 0.1, maka perhitungan perbandingan berpasangan diulang Kembali hingga menghasilkan matriks yang konsisten.

   Ci = Consistensi Indeks

   Ri = Random Indeks ditunjukkan pada Tabel 2.1

Rumus untuk Consistency Indeks adalah:

$$Ci = \frac{\lambda \max - n}{n - 1}$$

λmax =Eigen Value tertinggi dari matriks

N = banyaknya elemen /ukuran matriks

Tabel 2. 1 Random consistency indeks

n	1	2	3	4	5	6	7	8	9	10	11
Ri	0	0	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51

Prinsip kerja dari AHP adalah menyederhanakan sebuah persoalan yang kompleks dengan menata dan menampilkannya ke dalam suatu hirarki keputusan. Untuk menentukan variabel yang mempengaruhi hasil maka setiap variable diberikan nilai numerik secara subjektif antara satu variabel dengan variabel yang lain diberikan skala perbandingan Tingkat Kepentingan Relatif. Skala perbandingan relative ditunjukkan pada tabel 2.2.

Tabel 2. 2 Tingkat Kepentingan Relatif

Nilai Kepentingan	Definisi	Penjelasan
1	Sama penting	Kedua elemen sama pentingnya
3	Elemen satu sedikit lebih penting	Pengalaman dan penilaian sedikit mendukung satu elemen atas elemen lainnya
5	Elemen satu lebih penting dari elemen lainnya	Pengalaman dan penilaian sangat mendukung satu elemen atas lainnya
7	Sangat penting	Satu elemen sangat dominan
9	Mutlak lebih penting	Bukti mendukung satu elemen memeiliki tinggak penegasan tertinggi

2,4,6,8	Nilai antara dua pertimbangan yang berdekatan	Kompromi diperlukan antara dua pertmbangan.

2.7. Kajian Penelitian yang Relevan

1. Hasil penelitian sebelumnya yang masih relevan dengan penelitian ini adalah penelitian yang dilakukan oleh Greenhard Sitorus (2020) yang melakukan analisis risiko keamanan informasi menggunakan metode OCTAVE Allegro pada Dinas Komunikasi dan Informatika Jawa Barat. Hasil penelitian ini menunjukkan sebanyak 37 area risiko teridentifikasi dan konsekukensinya.
2. Prajanti,A.D (2019) dalam penelitiannya yang berjudul *A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Asesment Using the OCTAVE Allegro Methode with Decision Support System Method* mengusulkan adanya rangking terhadap risiko kemamanan aset informasi untuk menghemat anggaran dan waktu mitigasi risiko.

BAB III
METODE PENELITIAN

3.1. Waktu dan Tempat Penelitian

3.1.1. Waktu Penelitian

Pelaksanaan penelitian ini akan dilakukan dalam waktu selama empat bulan, dimana langkah – langkah yang akan diambil dalam penelitian ini adalah dimulai dengan pengusulan proposal, pengumpulan data dan pembuatan laporan sesuai dengan tabel 3.1.

Tabel 3.01. Jadwal Penelitian

No	Kegiatan	Bulan			
		Bulan 1	Bulan 2	Bulan 3	Bulan 4
1	Pengusulan Proposal				
2	Pengumpulan Data				
3	Analisis Data				
4	Pembuatan Laporan				

3.1.2. Tempat Penelitian

Penelitian ini mengambil tempat pada lokasi Data Center Pemerintah Kabupaten Buleleng yaitu di Dinas Komunikasi Informatika Persandian dan Statistik. Data Center

3.2. Data

3.2.1. Bentuk Data

Adapun bentuk data dalam penelitian ini adalah data kualitatif dan kuantitatif :

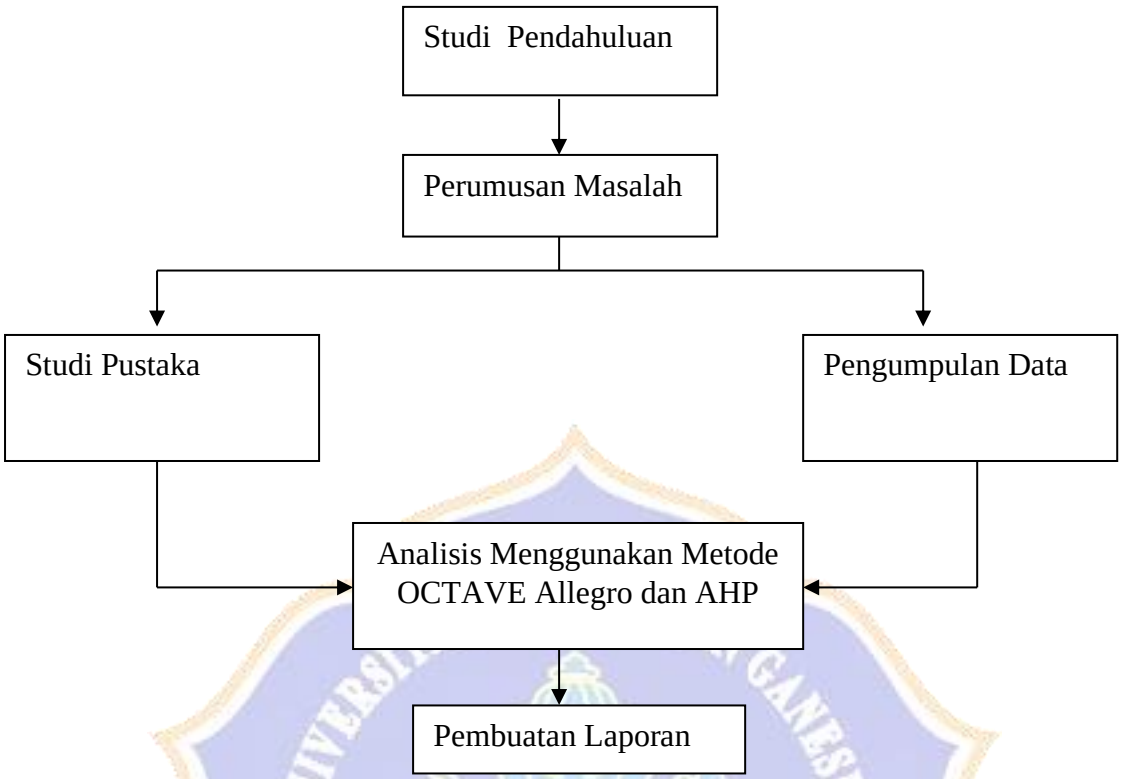
a. Data kualitatif, yaitu data yang disajikan dalam bentuk kata aau verbal bukan angka seperti profil organisasi, personil, nama aplikasi dan infrasruktur lainnya.
b. Data kuantitatif, yaitu data yang langsung dapat diukur menggunakan angka, misalnya jumlah aplikasi, jumlah server dan frekuensi terjadinya suatu kejadian.

3.2.2. Teknik Pengumpulan Data

Teknik pengumpulan data pada penelitian ini adalah antara lain adalah dengan brainstorming, survey, wawancara dan informasi historis dari pengelola data center Pemerintah Kabupaten Buleleng dan melakukan observasi di lapangan bagaimana prosedur yang telah diterapkan sebelumnya.

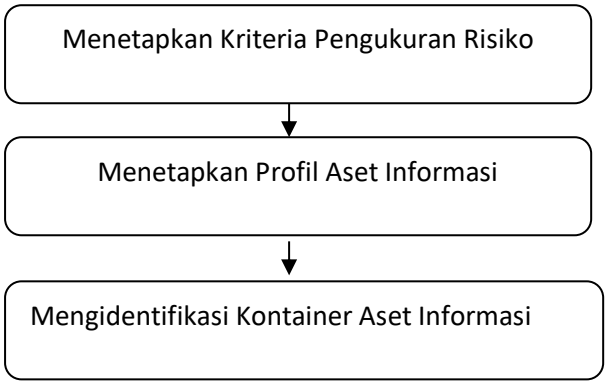
3.3. Tahapan Penelitian

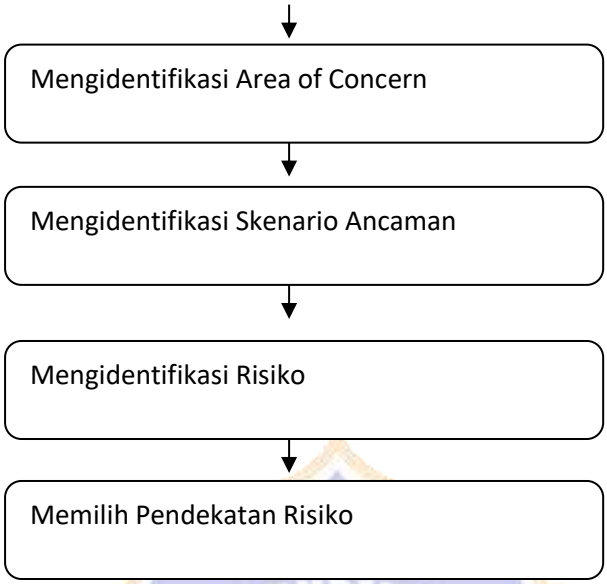
Tahapan penelitian dimulai dari studi literatur yang berkaitan dengan topik penelitian, pengumpulan data menggunakan metode wawancara, workshop dan kolaboratif. Selanjutnya akan dilakukan analisis data menggunakan metode OCTAVE Allegro dan AHP dan penyusunan laporan.



Gambar 3.1 Tahapan Penelitian

Analisis risiko menggunakan kerangka kerja OCTAVE Allegro yang terdiri dari 8 tahap seperti terlihat pada Gambar 3.2





Langkah 1 - Menetapkan Kritera Pengukuran Risiko. Kegiatan pada langkah ini adalah mulai membentuk penggerak organisasi untuk mengevaluasi dampak risiko terhadap misi dan tujuan bisnis organisasi. Semua kegiatan dicatat pada nilai prioritas dampak menggunakan Lembar Kerja peringkat Wilayah Dampak.

Langkah 2 – Mengembangkan Profil Aset Informasi. Pada langkah ini ada delapan kegiatan,

3.4. Metode Analisis

3.4.1 Metode OOCTAVE Allegro

Metode analisis data yang digunakan dalam penelitian ini dengan mengisi semua worksheet sesuai dengan kerangka kerja OCTAVE Allegro. Ada empat tingkatan dengan delapan langkah dalam melakukan penilaian risiko keamanan terhadap asset informasi. Proses ini akan menghasilkan sepuluh tabel *worksheet* hasil penilaian. Dari hasil tahapan identifikasi risiko mengacu pada asset risk worksheet OCTAVE Allegro maka akan didapatkan tabel area terdampak.

Salah satu contoh hasil penilaian risiko setelah semua tahapan metode OCTAVE Allegrp dilakukan ada pada gambar 3.2 Allegro –Worksheet 10

Allegro - Worksheet 10		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk		Aset Informasi	Data Pengadaan Barang jasa		
		Area Perhatian	Akses informasi oleh pihak yang tidak berhak		
	Threat	(1) Actor *Who would exploit the area of concern or threat?*	Admin jaringan		
		(2) Means *How would the actor do it? What would they do?*	Akses server		
		(3) Motive *What is the actor's reason for doing it?*	Mengambil data lelang pengadaan		
		(4) Outcome *What would be the resulting effect on the information asset?*	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements *How would the information asset's security requirements be breached?*	Mengganti password root		
		(6) Probability *What is the likelihood that this threat scenario could occur?*	**High**	**Medium**	✓ **Low**

(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*	(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
	Area Terdampak	**Value**	**Score**
Low	Reputasi	5	10
	Keuangan	3	6
	Produktifitas	2	2
	Keselamatan	1	2
	Denda	4	8
	User Defined Impact Area	N/A	
		Relative Risk Score	**28**

Gambar 3.2. Allegro Worksheet 10

Tahapan terakhir dari metode OCTAVE Allegro adalah pemilihan mitigasi risiko berdasarkan skor risiko relative pada *worksheet* 10.

3.4.2 Metode AHP

Selanjutnya adalah membuat matrix inisiasi berdasarkan nilai dari *worksheet* nomor 10 yang akan menjadi input dalam menghitung rating dari AHP.

Tabel 2 Matriks Inisiasi Awal

	Reputasi	Keuangan	Keselamatan	Denda	Produktifitas	Probalility
Prioritas	1	2	3	4	5	1
1. Area Perhatian (1)	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10
2. Area perhatian (2)	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10
3. Area perhatian (n)	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10	Nilai dari worksheet 10

Menggunakan metode AHP, maka dapat dibuat urutan dari seluruh area perhatian yang didapatkan pada tahapan identifikasi. Peringkat risiko diurutkan berdasarkan pada nilai yang terbesar.

BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

Sebelum memulai penilaian risiko, peneliti melakukan mengumpulkan data dan informasi mengenai pengelolaan data center Pemerintah Kabupaten Buleleng yang ada pada Dinas Komunikasi Informatika Persandian dan Statistik di Bidang Infrastruktur dan Layanan Sistem Pemerintahan Berbasis Elektronik. Proses wawancara dilakukan untuk mendapatkan informasi tentang aset operasional yang dianggap penting oleh organisasi.

4.1 OCTAVE Allegro Risk Assesment

Ada delapan langkahyang harus dilakukan untuk melakukan analisi risiko sesuai dengan kertas kerja dari OCTAVE Allegro.

Langkah 1 - Menetapkan Kriteria Pengukuran Risiko

Terdapat dua aktivitas pada langkah ini, yang diawali dengan mengevaluasi dampak risiko dengan mengukur semua aspek kriteria penetapan risiko menggunakan tabel kertas kerja dari OCTAVE Allegro.

Penetapan kriteria penilaian risiko ditetapkan berdasarkan area terdampak meliputi:

a. Reputasi dan kepercayaan pengguna
b. Keuangan
c. Produktifitas organisasi
d. Keselamatan dan kesehatan pegawai
e. Denda dan tuntutan hukum

Tabel 4. 1 Kriteria Penilaian Risiko Reputasi

Allegro Worksheet 1	**KRITERIA PENILAIAN RISIKO – REPUTASI DAN KEPERCAYAAN PENGGUNA**		
Area Terdampak	**Rendah**	**Sedang**	**Tinggi**
Reputasi (Instansi)	Reputasi Instansi berdampak minimal: tidak ada usaha untuk pemulihan.	Reputasi Instansi rusak dan perlu usaha dan biaya untuk pemulihan.	Reputasi Instansi rusak parah.
Kepercayaan Pengguna dan Masyarakat	Kepercayaan pengguna dan masyarakat berkurang dibawah dari 10%	20 to 50% pengurangan dari kepercayaan pengguna dan masyarakat	Lebih dari setengah pengguna kehilangan kepercayaan terhadap instansi

Tabel 4. 2 Kriteria Penilaian Risiko Keuangan

Allegro Worksheet 2	**KRITERIA PENILAIAN RESIKO – KEUANGAN**		
Area Terdampak	**Rendah**	**Sedang**	**Tinggi**
Penambahan Anggaran	Penambahan Anggaran kurang dari 20% pada tahun berikutnya	Penambahan anggaran 30 sampai 50 %	Penambahan anggaran lebih dari 50 %.
Kerugian Anggaran	Kerugian anggaran kurang dari 20 %	Kerugian Anggaran 20 – 40 %	Kerugian lebih dari 50 % anggaran

Tabel 4. 3 Kriteria Penilaian Risiko Produktifitas

Allegro Worksheet 3	**KRITERIA PENILAIAN RISIKO – PRODUKTIFITAS**		
Area Terdampak	**Rendah**	**Sedang**	**Tinggi**
Penambahan Waktu Bekerja	Penambahan Waktu bekerja pegawai kurang dari 1 hari.	Penambahan Waktu bekerja pegawai kurang dari 2 sampai 4 hari	Penambahan Waktu bekerja pegawai lebih dari 5 hari

Tabel 4. 4 Kriteria Penilaian Risiko Keselamatan

Allegro Worksheet 4	**KRITERIA PENILAIAN RESIKO – KESELAMATAN DAN KESEHATAN PEGAWAI**		
Area Terdampak	**Rendah**	**Sedang**	**Tinggi**
Keselamatan	Tidak ada bahaya keselamatan pegawai	Kemungkinan menyebabkan cidea pegawai	Membahayakan nyawa pegawai
Kesehatan	Menyebabkan cidera ringan bisa diobati	Perlu penanganan rumah sakit	Cidera berat

Setelah menetapkan kritera pengukuran risiko, selanjutnya adalah membuat peringkat prioritas area terdampak yang berdasarkan

Tabel 4. 5 Prioritas Area Terdampak

Allegro Worksheet 6	**PRIORITAS AREA TERDAMPAK**
PRIORITY	**IMPACT AREAS**
5	**Reputasi dan Kepercayaan Pengguna**
4	**Keuangan**
3	**Produktifitas Pegawai**
2	**Keselamatan dan Kesehatan Pegawai**
1	**Tuntutan Hukum**

Langkah 2 – Membuat Profil Aset Informasi.

Terdapat delapan kegiatan yaitu yang pertama adalah melakukan identifikasi aset informasi dan dilanjutkan dengan melakukan penilaian risiko tersetruktur pada aset yang dinilai kritis. Kegiatan ketiga dan keempat adalah pengumpulan informasi yang dinilai penting selanjutnya membuat dokumentasi alasan pemilihan aset kritis. Kegiatan kelima dan keenam adalah membuat deskripsi aset informasi kritis selanjutnya melakukan identifikasi kepemilikan aset informasi kritis tersebut. Kegiatan ketujuh dan kedelapan adalah mengisi kebutuhan keamanan untuk aspek keamanan informasi yaitu kerahasiaan, integritas, dan ketersediaan.

Semua hasil dari langkah kedua ini didokumentasi pada tabel profil aset kritis.

Tabel 4. 6 Profil Aset Kritis

Allegro Worksheet 8	**PROFIL ASET KRITIS**	
(1) Critical Asset	**(2) Rationale for Selection**	**(3) Description**
Nama asset informasi kritis ?	*Kenapa asset informasi ini penting bagi instansi ?*	*Deskripsi asset informasi ini ?*

Data Penyedia Barang Jasa	Aset ini sangat penting bagi instansi karena menyimpan aplikasi pengadaan seperti data perusahaan.	Data pengadaan Penyedia barang dan jasa berisi riwayat pengadaan yang harus tersimpan dalam waktu lama.
(4) Owner(s) *Siapa pemilik asset informasi ini ?*		
Bagian Pengadaan Barang dan Jasa		
(5) Security Requirements *Apa saja aspek keamanan informasi yang dibutuhkan oleh asset ini ?*		
❑ **Kerahasiaan**	Hanya yang berhak boleh melihat informasi ini.	**Pejabat pembuat komitmen, pengguna anggaran, auditor**
❑ **Integritas**	Hanya pegawai tertentu yang boleh mengubah informasi ini	**Pejabat pembuat komitmen, pengguna anggaran, auditor**
❑ **Ketersediaan**		
	Aset ini harus tersedia 24 jam.7 hari /minggu	
❑ **Other**		
(6) Most Important Security Requirement *What is the most important security requirement for this information asset?*		
✓ Kerahasiaan	❑ Integritas	❑ Ketersediaan ❑ Other

Langkah 3 – Mengidentifikasi Kontainer Aset Informasi

Kegiatan pada langkah ketiga ini adalah melakukan identifikasi kontainer atau wadah dimana aset informasi disimpan, dikirim dan diproses.

Tabel 4. 7 Kontainer Aset Informasi (Teknikal)

Allegro Worksheet 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TEKNIKAL)**
INTERNAL	
DESKRIPSI KONTAINER	**PEMILIK**
1. Database – Database Aplikasi Pengadaan	Bagian Pengadaan Barang jasa

Database detail pegawai disimpan pada server aplikasi sistem informasi kepegawaian.	
2.	
EKSTERNAL	
CONTAINER DESCRIPTION	**PEMILIK**
1. Koneksi internet ke ruang server	ISP
2.	

Tabel 4. 8 Kontainer Aset Informasi Fisikal

Allegro Worksheet 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (FISIKAL)**
INTERNAL	
CONTAINER DESCRIPTION	**PEMILIK**
1. Jaringan intranet di ruang server	Bidang Infrastruktur dan Layanan SPBE
2. Back UP Data Server	Seksi Jaringan
EXTERNAL	
DESKRIPSI KONTAINER	**PEMILIK**
1.	
2.	

Tabel 4. 9 Kontainer Aset Informasi Manusia

Allegro Worksheet 9c	**INFORMATION ASSET RISK ENVIRONMENT MAP (MANUSIA)**
INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	**DEPARTMENT OR UNIT**
Administrator Sistem	Seksi Jaringan
User Aplikasi	Programmer
Petugas ruang server	Bidang tata kelola
EXTERNAL PERSONNEL	
CONTRACTOR, VENDOR, ETC.	**ORGANIZATION**
1. Penyedia jasa Internet	Vendor
2. Admin Aplikasi	Dinas/Bidang terkait

Langkah 4 – Mengidentifikasi Area yang diperhatikan

Kegiatan pada langkah empat adalah meninjau setiap kontainer untuk menentukan area yang menjadi perhatian selanjutnya membuat dokumentasi setiap area yang diperhatikan.

Tabel 4. 10 Area Perhatian Aset Kritis

No	Area Perhatian – Database Pengadaan Barang /Jasa
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam
2	Bocornya hak akses seperti username dan password administrator
3	Kesalahan ketika maintenance jaringan di ruang server
4	Gangguan koneksi internet
5	Kerusakan pada hardware server
6	Ruang server diakses oleh pihak tidak berwenang
7	Adanya bugs/error pada saat update sistem
8	Terhentinya layanan karena supply listrik mati
9	Bencana alam yang mengakibatkan kerusakan perangkat terkait

Langkah 5 – Mengidentifikasi Skenario Ancaman

Pada tahap ini, kegiatan yang dilaksakan adalah melakukan indentifikasi skenario ancaman dengan memberikan properti dari setiap ancaman yang ada seperti actor, means, motives, outcome dan security untuk setiap area yang diperhatikan.

Tabel 4. 11 Identifikasi Skenario Ancaman

No	Area Perhatian	Skenario Ancaman	
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam	Actor	Tidak diketahui
		Mean	- Percobaan login (*bruteforce attack*) - *Password cracking*
		Motive	Secara sengaja
		Outcome	Interuption
		Security Requirement	- Melakukan update secury server
2	Bocornya hak akses seperti username dan password administrator	Actor	Tidak diketahui
		Mean	*Password cracking*
		Motive	Secara sengaja
		Outcome	Interuption
		Security Requirement	Kebijakan standar keamanan password

Langkah 6 – Mengidentifikasi Risiko

Kegiatan pada langkah enam ini adalah mengidentifikasi nilai dampak risiko bagi organisasi berdasarkan area dampak yang sudah didefinisikan sebelumnya.

Tabel 4. 12 Identifikasi Nilai Dampak

Area Dampak	Prioritas	Nilai Dampak

		Rendah (1)	Sedang (2)	Tinggi (3)
Reputasi dan Kepercayaan Pengguna	1	5	10	15
Keuangan	2	4	8	12
Produktifitas	3	3	6	9
Keselamatan dan Kesehatan Pegawai	4	2	4	6
Tuntutan Hukum	5	1	2	3

Tabel diatas selanjutnya digunakan sebagai dasar melakukan perhitungan nilai risiko relative.

Langkah 7 – Menganalisis Risiko

Tahapan menganalisis risiko menggunakan metode OCTAVE Allegro selanjutnya adalah menggunakan *worksheet* 10. Pada tahap ini, seluruh data hasil dokumentasi pada tahap sebelumnya dimasukkan untuk memperoleh nilai risiko *relative*. Tabel hasil penilaian risiko ini dibuat masing – masing sesuai dengan are perhatian yang ada pada table area perhatian.

Hasil penilaian risiko untuk area perhatian ekspolitasi celah keamanan sistem di server dari pihak luar dan dalam adalah seperti pada table 4.13.

Tabel 4. 13 Allegro Worksheet 10-a

Allegro - Worksheet 10-a		**INFORMATION ASSET RISK WORKSHEET**	
Information Asset Risk	**Threat**	Aset Informasi	Data Penyedia Barang jasa
		Area Perhatian	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam
		(1) Actor	Tidak diketahui
		(2) Means	Mengambil atau melakukan modifikasi data penyedia barang jasa
		(3) Motive	Dengan sengaja
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**
		(5) Security Requirements	Meningkatkan keamanan software, hardware dan jaringan.

		(6) Probability	**High**	**Medium**	**Low**	
	(7) Consequences			(8) Severity		
				Area Terdampak	**Nilai**	**Score**
	Informasi yang dimodifikasi menyebabkan kerusakan mengganggu validitas informasi tersebut			Reputasi dan Kepercayaan Pengguna	Tinggi	10
				Keuangan	Rendah	4
				Produktifitas	Tinggi	6
				Keselamatan dan kesehatan	Rendah	2
				Tuntutan Hukum	Tinggi	3
					Relative Risk Score	**25**

Tabel hasil penilaian risiko untuk area perhatian bocornya hak akses seperti username dan password administrator.

Tabel 4. 14 Allegro Worksheet 10-b

Allegro - Worksheet 10 -b		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Bocornya hak akses seperti username dan password administrator		
		(1) Actor	Administrator server		
		(2) Means	Mengambil atau melakukan modifikasi data penyedia barang jasa		
		(3) Motive	Dengan sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements	Kebijakan pengelolaan akses masuk server		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences			(8) Severity	

		Area Terdampak	Nilai	Score
	Informasi yang dimodifikasi menyebabkan kerusakan mengganggu validitas informasi tersebut	Reputasi dan Kepercayaan Pengguna	Tinggi	10
		Keuangan	Rendah	4
		Produktifitas	Tinggi	9
		Keselamatan dan kesehatan	Rendah	2
		Tuntutan Hukum	Tinggi	3
			Relative Risk Score	**28**

Tabel hasil penilaian risiko untuk area perhatian kesalahan ketika ada pemeliharaan jaringan di ruang server.

Tabel 4. 15Allegro Worksheet 10--c

Allegro - Worksheet 10- c		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Kesalahan ketika maintenance jaringan di ruang server		
		(1) Actor	Staff Jaringan		
		(2) Means	Kesalahan dalam melakukan konfigurasi		
		(3) Motive	Tidak sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements	Melakukan monitoring jaringan secara berkala.		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences		(8) Severity		
			Area Terdampak	**Nilai**	**Score**
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan	Tinggi	15
			Keuangan	Tinggi	12

		Produktifitas	Tinggi	9
		Keselamatan dan kesehatan	Rendah	2
		Tuntutan Hukum	Tinggi	3
			Relative Risk Score	**36**

Tabel hasil penilaian risiko untuk area perhatian adanya gangguan pada koneksi internet.

Tabel 4. 16 Allegro Worksheet 10-d

Allegro - Worksheet 10-d		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Gangguan koneksi internet		
		(1) Actor	Penyedia jasa internet		
		(2) Means	Kesalahan dalam melakukan konfigurasi		
		(3) Motive	Tidak sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirement	Melakukan monitoring jaringan secara berkala.		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences		(8) Severity		
			Area Terdampak	**Nilai**	**Score**
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan	Sedang	10
			Keuangan	Tinggi	12
			Produktifitas	Tinggi	9
			Keselamatan dan kesehatan	Rendah	2
			Tuntutan Hukum	Tinggi	3
				Relative Risk Score	**36**

Hasil penilaian risiko untuk area perhatian adanya kerusakan pada perangkat keras di ruang server.

Tabel 4. 17Allegro Worksheet 10-e

Allegro - Worksheet 10- e		**INFORMATION ASSET RISK WORKSHEET**			
Information Asset Risk	**Threat**	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Kerusakan pada hardware server		
		(1) Actor	Tidak diketahui		
		(2) Means	Tidak diketahui		
		(3) Motive	Tidak sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements	Melakukan monitoring dan pemeliharaan server secara berkala.		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences *What are the consequences to the organization or the information asset owner as a result of the outcome and breach of security requirements?*		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Area Terdampak	**Nilai**	**Score**
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan	Sedang	10
			Keuangan	Tinggi	12
			Produktifitas	Tinggi	9
			Keselamatan dan kesehatan	Rendah	2
			Tuntutan Hukum	Sedang	2
				Relative Risk Score	**35**

Tabel hasil penilaian risiko untuk area perhatian ketika ruang server diakses oleh pihak yang tidak berwenang.

Tabel 4. 18 Allegro Worksheet 10-f

Allegro - Worksheet 10 - f		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Ruang server diakses oleh pihak tidak berwenang		
		(1) Actor	Pegawai		
		(2) Means	Melakukan pengambilan data		
		(3) Motive	Sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements	Melakukan monitoring jaringan secara berkala.		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences		(8) Severity *How severe are these consequences to the organization or asset owner by impact area?*		
			Area Terdampak	**Nilai**	**Score**
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan	Tinggi	15
			Keuangan	Rendah	4
			Produktifitas	Rendah	3
			Keselamatan dan kesehatan	Rendah	2
			Tuntutan Hukum	Tinggi	3
				Relative Risk Score	**33**

Hasil penilaian risiko untuk area perhatian adanya bugs/error pada saat *update system.*

Tabel 4. 19 Allegro Worksheet 10-g

Allegro - Worksheet 10-g		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Adanya bugs/error pada saat update sistem		
		(1) Actor	Admin sistem		
		(2) Means	Kesalahan dalam melakukan konfigurasi		
		(3) Motive	Tidak sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements	Testing sistem		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences		(8) Severity		
			Area Terdampak	**Nilai**	**Score**
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan	Tinggi	15
			Keuangan	Rendah	4
			Produktifitas	Tinggi	9
			Keselamatan dan kesehatan	Rendah	2
			Tuntutan Hukum	Tinggi	3
				Relative Risk Score	**36**

Hasil penilaian risiko untuk area perhatian karena terhentinya layanan akibat supply listrik mati.

Tabel 4. 20 Allegro Worksheet i

Allegro - Worksheet 10- h		INFORMATION ASSET RISK WORKSHEET			
Information Asset Risk	Threat	Aset Informasi	Data Penyedia Barang jasa		
		Area Perhatian	Terhentinya layanan karena supply listrik mati		
		(1) Actor	Staff Jaringan		
		(2) Means	Kesalahan dalam melakukan konfigurasi		
		(3) Motive	Tidak sengaja		
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**		
		(5) Security Requirements	Melakukan monitoring jaringan secara berkala.		
		(6) Probability	**High**	**Medium**	✓ **Low**
	(7) Consequences		(8) Severity		
			Area Terdampak	**Nilai**	**Score**
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan Pengguna	Sedang	10
			Keuangan	Tinggi	12
			Produktifitas	Tinggi	9
			Keselamatan dan kesehatan	Sedang	4
			Tuntutan Hukum	Sedang	2
				Relative Risk Score	**37**

Hasil penilaian risiko untuk area perhatian adanya bencana alam yang mengakibatkan kerusakan perangkat terkait.

Tabel 4. 21 Allegro Worksheet 10-i

Allegro - Worksheet 10-i		INFORMATION ASSET RISK WORKSHEET	
Information	Threat	Aset Informasi	Data Penyedia Barang jasa

		Area Perhatian	Bencana alam yang mengakibatkan kerusakan perangkat terkait			
		(1) Actor	Staff Jaringan			
		(2) Means	Kesalahan dalam melakukan konfigurasi			
		(3) Motive	Tidak sengaja			
		(4) Outcome	✓ **Disclosure** ✓ **Destruction** ✓ **Modification** ✓ **Interruption**			
		(5) Security Requirements	Melakukan monitoring jaringan secara berkala.			
		(6) Probability	**High**	**Medium**	✓ **Low**	
	(7) Consequences		(8) Severity			
			Area Terdampak	**Nilai**	**Score**	
	Jika data penyedia tidak bisa diakses maka proses pengadaaan barang jasa tidak dapat dilaksanakan		Reputasi dan Kepercayaan	Rendah	5	
			Keuangan	Tinggi	12	
			Produktifitas	Tinggi	9	
			Keselamatan dan kesehatan	Tinggi	6	
			Tuntutan Hukum	Rendah	1	
				Relative Risk Score	**29**	

Langkah 8 – Memilih Pendekatan Mitigasi

Tabel 4. 22 Matriks Risiko Relatif

Risk Relative Matrix		
Risk Score	POOL	Mitigation Approach
30-45	1	Mitigasi
16-29	2	Defer
0-15	3	Accept

Berdasarkan pada tabel Risk Relative Matrix, maka pendekatan mitigasi akan ditentukan untuk tiap risiko. Jika nilai skor risiko antara 0 sampai 15 maka risiko tersebut bisa diterima. Nilai Skor antara 16 sampai 29 maka risiko tersebut dimitigasi atau bisa ditangguhkan. Jika nilai risiko antara 30 sampai 45 maka risiko tersebut harus dimitigasi. Hasil lengkap pendekatan mitigasi risiko seperti terlihat pada table.

Tabel 4. 23 Tabel hasil analisis OCTAVE Allegro

Area Perhatian	*Action*
Kesalahan ketika maintenance jaringan di ruang server	*Mitigate*
Terhentinya layanan karena supply listrik mati	*Mitigate*
Gangguan koneksi internet	*Mitigate*
Kerusakan pada hardware server	*Mitigate*
Bencana alam yang mengakibatkan kerusakan perangkat terkait	*Mitigate*
Bocornya hak akses seperti username dan password administrator	*Defer*
Ruang server diakses oleh pihak tidak berwenang	*Defer*
Adanya bugs/error pada saat update sistem	*Defer*
Eksploitasi celah keamanan sistem di server dari pihak luar dan dalam	*Defer*

4.2 Analisis Risiko OCTAVE Allegro –AHP

Setelah semua tahapan analisis OCTAVE Allegro dilakukan maka tahapan selanjutnya adalah menentukan peringkat area yang diperhatikan menggunakan metode AHP.

Tahap pertama adalah dengan membuat matrix inisiasi yang diambil dari nilai pada metode OCTAVE Allegro yaitu pada Worksheet 10. Hasil dari matrik inisiasi dapat dilihat pada tabel 4.23.

Tabel 4. 24 Tabel Inisiasi AHP

		Reputasi	Keuangan	Produktifitas	Keselamatan	Hukum	Probabilitas
No	**Area Perhatian (AP)**						
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam	10	4	6	2	3	8
2	Bocornya hak akses seperti username dan password administrator	10	4	9	2	3	4
3	Kesalahan ketika maintenance jaringan di ruang server	15	12	6	4	3	4
4	Gangguan koneksi internet	10	12	9	2	3	8
5	Kerusakan pada hardware server	10	12	9	2	2	8
6	Ruang server diakses oleh pihak tidak berwenang	15	4	3	2	3	4
7	Adanya bugs/error pada saat update sistem	15	4	3	2	3	12
8	Terhentinya layanan karena supply listrik mati	10	12	9	4	2	4
9	Bencana alam yang mengakibatkan kerusakan perangkat terkait	5	12	9	6	1	4

Matriks berpasangan

Tabel 4. 25 Matrik Perbandingan Berpasangan

1. Matriks Perbandingan Berpasangan							Eigen	Bobot Prioritas
Dampak	Reputasi	Keuangan	Produktifitas	Keselamatan	Hukum	Probabilitas	0,16666667	
Reputasi	1,0000	0,3333	0,2000	0,3333	1,0000	3,0000	0,6368	0,09597934
Keuangan	3,0000	1,0000	0,2000	3,0000	0,3333	0,2000	0,7023	0,105857876
Produktifitas	5,0000	5,0000	1,0000	3,0000	0,2000	1,0000	1,5704	0,236705408
Keselamatan	3,0000	0,3333	0,3333	1,0000	0,2000	3,0000	0,7647	0,115265137

Hukum	1,0000	3,0000	5,0000	5,0000	1,0000	1,0000	2,0536	0,309530308
Probabilitas	0,3333	5,0000	1,0000	0,3333	1,0000	1,0000	0,9067	0,136661931
Jumlah total	13,3333	14,6667	7,7333	12,6667	3,7333	9,2000	6,6345	1,0000

Normalisasi matriks

Tabel 4. 26 Matriks Normalisasi

Dampak	Reputasi	Keuangan	Produktifitas	Keselamatan	Hukum	Probabilitas	Bobot Sintesa	Eigen Maks
Reputasi	0,0750	0,0227	0,0259	0,0263	0,2679	0,3261	0,7438	7,750097356
Keuangan	0,2250	0,0682	0,0259	0,2368	0,0893	0,0217	0,6669	6,300058717
Produktifitas	0,3750	0,3409	0,1293	0,2368	0,0536	0,1087	1,2443	5,256866052
Keselamatan	0,2250	0,0227	0,0431	0,0789	0,0536	0,3261	0,7494	6,501848668
Hukum	0,0750	0,2045	0,6466	0,3947	0,2679	0,1087	1,6974	5,483749959
Probabilitas	0,0250	0,3409	0,1293	0,0263	0,2679	0,1087	0,8981	6,571603481

Lamda maksimal: 6,310704039 dengan konsistensi indeks 0,0621400808

Indeks Ratio 6 kriteria adalah 1,24 sehingga konsistensi ratio didapat adalah 0,050113555

Tahap selanjutnya adalah menghitung bobot alternatif masing – masing dampak. Hasil bobot alternatif untuk dampak reputasi dapat dilihat pada tabel 4.26.

Tabel 4. 27 Bobot Alternatif - Reputasi

		10		10	15		10		10	15	15		10		5	Eigen	Bobot Alternatif
Reputasi	AP1		AP2		AP3	AP4		AP5		AP6	AP7	AP8		AP9		0,111111	

10	AP1	1	1	1,5	1	1	1,5	1,5	1	0,5	1,059862	0,107734156
10	AP2	1	1		1	1	1,5	1,5	1	0,5	1,013173	0,10298826
15	AP3	0,666667	0,666667	1	0,666667	0,666667	1	1	0,666667	0,333333	0,706575	0,071822771
10	AP4	1	1	1,5	1	1	1,5	10	1	0,5	1,308563	0,133014452
10	AP5	1	1	1,5	1	1	1,5	1,5	1	0,5	1,059862	0,107734156
15	AP6	0,666667	0,666667	1	0,666667	0,666667	1	1	0,666667	0,333333	0,706575	0,071822771
15	AP7	1	0,666667	1	0,666667	0,666667	1	1	0,666667	0,333333	0,739135	0,075132502
10	AP8	1	1	1,5	1	1	1	1,5	1	0,5	1,013173	0,10298826
5	AP9	2	2	3	2	2	3	3	2	1	2,119724	0,215468313
											9,837753	

Menghitung bobot alternatif area perhatian terhadap dampak keuangan.

Tabel 4. 28 Bobot Alternatif - Keuangan

		4	4	12	12	12	4	4	12	12	Eigen	Bobot Alternatif
	Keuangan	AP1	AP2	AP3	AP4	AP5	AP6	AP7	AP8	AP9	0,111111	
4	AP1	1	1	3	3	3	1	1	3	3	1,841058	0,175330829
4	AP2	1	1		3	3	1	1	3	3	1,629498	0,155183239
12	AP3	0,333333	0,333333	1	1	1	0,333333	0,333333	1	1	0,613686	0,05844361
12	AP4	0,333333	0,333333	1	1	1	0,333333	12	1	1	0,913837	0,087028106
12	AP5	0,333333	0,333333	1	1	1	0,333333	0,333333	1	1	0,613686	0,05844361
4	AP6	1	1	3	3	3	1	1	3	3	1,841058	0,175330829
4	AP7	0,333333	1	3	3	3	1	1	3	3	1,629498	0,155183239
12	AP8	0,333333	0,333333	1	1	1	1	0,333333	1	1	0,693361	0,0660314
12	AP9	0,333333	0,333333	1	1	1	0,333333	0,333333	1	1	0,613686	0,05844361
											10,50048	

Menghitung bobot alternatif untuk area perhatian terhadap produktifitas.

Tabel 4. 29 Bobot Alternatif - Produktifitas

		6	9		6	9	9	3	3	9	9	Eigen	Bobot Alternatif

	Produktifitas	AP1	AP2	AP3	AP4	AP5	AP6	AP7	AP8	AP9	0,111111	
6	AP1	1	1,5	0,666667	1	1,5	0,5	0,5	1,5	1,5	0,981299	0,095861085
9	AP2	0,666667	1		1	1	0,333333	0,333333	1	1	0,748872	0,073155699
6	AP3	1	1,5	1	1,5	1,5	0,5	0,5	1,5	1,5	1,073824	0,104899575
9	AP4	0,666667	1	0,666667	1	1	0,333333	9	1	1	1,032481	0,100860911
9	AP5	0,666667	1	0,666667	1	1	0,333333	0,333333	1	1	0,715882	0,06993305
3	AP6	2	3	2	3	3	1	1	3	3	2,147647	0,20979915
3	AP7	0,666667	3	2	3	3	1	1	3	3	1,900857	0,185690742
9	AP8	0,666667	1	0,666667	1	1	1	0,333333	1	1	0,808826	0,079012525
9	AP9	0,666667	1	0,666667	1	1	0,333333	0,333333	1	1	0,715882	0,06993305
											10,23668	

Menghitung bobot alternatif area perhatian terhadap keselamatan

Tabel 4. 30 Bobot Alternatif - Keselamatan

		2	2	4	2	2	2	2	4	6	Eigen	Bobot Alternatif
	Keselamatan	AP1	AP2	AP3	AP4	AP5	AP6	AP7	AP8	AP9	0,111111	
2	AP1	1	1	2	1	1	1	1	2	3	1,317981	0,135327585
2	AP2	1	1		1	1	1	1	2	3	1,220285	0,125296389
4	AP3	0,5	0,5	1	0,5	0,5	0,5	0,5	1	1,5	0,65899	0,067663793
2	AP4	1	1	2	1	1	1	2	2	3	1,423498	0,146161876
2	AP5	1	1	2	1	1	1	1	2	3	1,317981	0,135327585
2	AP6	1	1	2	1	1	1	1	2	3	1,317981	0,135327585
2	AP7	0,5	1	2	1	1	1	1	2	3	1,220285	0,125296389
4	AP8	0,5	0,5	1	0,5	0,5	1	0,5	1	1,5	0,711749	0,073080938
6	AP9	0,333333	0,333333	0,666667	0,333333	0,333333	0,333333	0,333333	0,666667	1	0,439327	0,045109195
											9,739187	

Menghitung bobot alternatif area perhatian terhadap hukum

Tabel 4. 31 Bobot Alternatif - Hukum

2	2	4	2	2	2	2	4	6	Eigen	Bobot Alternatif

	Hukum	AP1	AP2	AP3	AP4	AP5	AP6	AP7	AP8	AP9	0,111111	
2	AP1	1	1	2	1	1	1	1	2	3	1,317981	0,135327585
2	AP2	1	1		1	1	1	1	2	3	1,220285	0,125296389
4	AP3	0,5	0,5	1	0,5	0,5	0,5	0,5	1	1,5	0,65899	0,067663793
2	AP4	1	1	2	1	1	1	2	2	3	1,423498	0,146161876
2	AP5	1	1	2	1	1	1	1	2	3	1,317981	0,135327585
2	AP6	1	1	2	1	1	1	1	2	3	1,317981	0,135327585
2	AP7	0,5	1	2	1	1	1	1	2	3	1,220285	0,125296389
4	AP8	0,5	0,5	1	0,5	0,5	1	0,5	1	1,5	0,711749	0,073080938
6	AP9	0,333333	0,333333	0,666667	0,333333	0,333333	0,333333	0,333333	0,666667	1	0,439327	0,045109195
											9,739187	

Menghitung bobot area perhatian terhadap probabililitas

Tabel 4. 32 Bobot Alternatif - Probabilitas

		2	2	4	2	2	2	2	4	6	Eigen	Bobot Alternatif
	Probabilitas	AP1	AP2	AP3	AP4	AP5	AP6	AP7	AP8	AP9	0,111111	
8	AP1	1	0,25	1	0,5	0,25	0,25	0,25	0,5	0,75	0,448374	0,092174752
4	AP2	0,5	0,5		0,5	0,5	0,5	0,5	1	1,5	0,65899	0,135472413
4	AP3	0,5	0,5	1	0,5	0,5	0,5	0,5	1	1,5	0,65899	0,135472413
8	AP4	0,25	0,25	0,5	0,25	0,25	0,25	8	0,5	0,75	0,48427	0,099554239
8	AP5	0,25	0,25	0,5	0,25	0,25	0,25	0,25	0,5	0,75	0,329495	0,067736206
4	AP6	0,5	0,5	1	0,5	0,5	1	0,5	1	1,5	0,711749	0,146318299
12	AP7	0,5	0,166667	0,333333	0,166667	0,166667	0,166667	0,166667	0,333333	0,5	0,248183	0,051020309
4	AP8	0,5	0,5	1	0,5	0,5	0,166667	0,5	1	1,5	0,583265	0,119905028
4	AP9	0,5	0,5	1	0,5	0,5	0,5	0,5	1	1	0,629961	0,129504593
											4,864388	

Bobot Prioritas

Tabel 4. 33 Bobot Prioritas - Dampak

	Bobot Prioritas
Reputasi	0,09597934
Keuangan	0,105857876
Produktifitas	0,236705408
Keselamatan	0,115265137
Hukum	0,309530308
Probabilitas	0,136661931

Tabel 4. 34 Bobot Prioritas - Area Perhatian

	Reputasi	**Keuangan**	**Produktifitas**	**Keselamatan**	**Hukum**	**Probabilitas**	**Nilai Matrix**
AP1	0,107734	0,17533083	0,095861085	0,135327585	0,135328	0,09217475	0,121674561
AP2	0,102988	0,15518324	0,073155699	0,125296389	0,125296	0,13547241	0,11536772
AP3	0,071823	0,05844361	0,104899575	0,067663793	0,067664	0,13547241	0,085167708
AP4	0,133014	0,08702811	0,100860911	0,146161876	0,146162	0,09955424	0,121547747
AP5	0,107734	0,05844361	0,06993305	0,135327585	0,135328	0,06773621	0,099824003
AP6	0,071823	0,17533083	0,20979915	0,135327585	0,135328	0,1463183	0,152596928
AP7	0,075133	0,15518324	0,185690742	0,125296389	0,125296	0,05102031	0,127790408
AP8	0,102988	0,0660314	0,079012525	0,073080938	0,073081	0,11990503	0,083008283
AP9	0,215468	0,05844361	0,06993305	0,045109195	0,045109	0,12950459	0,080281282

Tahap terakhir dari metode AHP membuat tabel peringkat area perhatian dengan memasukkan bobot dari nilai matriks yang didapatkan. Hasil peringkat risiko dapat dilihat pada tabel 4.34.

Tabel 4. 35 Peringkat Area Perhatian

No	**Area Perhatian**	Bobot	Rangking
1	Eksploitasi celah keamanan sistem di server dari pihak luar atau dalam	0,121674561	3
2	Bocornya hak akses seperti username dan password administrator	0,11536772	5
3	Kesalahan ketika maintenance jaringan di ruang server	0,085167708	7
4	Gangguan koneksi internet	0,121547747	4
5	Kerusakan pada hardware server	0,099824003	6

6	Ruang server diakses oleh pihak tidak berwenang	0,152596928	1
7	Adanya bugs/error pada saat update sistem	0,127790408	2
8	Terhentinya layanan karena supply listrik mati	0,083008283	8
9	Bencana alam yang mengakibatkan kerusakan perangkat terkait	0,080281282	9

Berdasarkan tabel peringkat area perhatian tersebut maka dapat ditentukan prioritas penanganan keamanan informasi dari yang memiliki risiko paling besar sampai dengan risiko paling rendah.

Berikut adalah hasil akhir peringkat risiko keamanan informasi berdasarkan metode OCTAVE Allegro dan AHP serta rekomendasi untuk mitigasinya:

1. Ruang Server diakses oleh pihak yang tidak berwenang
   - Menerapkan standar operasional prosedur yang ketat untuk akses ke ruang server.
   - Melengkapi ruang server dengan *doorlock fingerprint, face recognition* atau *access code*
   - Menutup *port* pada server yang tidak dibutuhkan
2. Adanya *bugs/error* pada saat update sistem
   - Melakukan *backup* data secara berkala
   - Melakukan pengujian dan standarisasi perangkat lunak yang digunakan
3. Eksploitasi celah keamanan di *server* dari pihak luar atau dalam
   - Melakukan update patching terhadap *software* dan sistem operasi
   - Instalasi dan *update firewall* yang digunakan
4. Gangguan koneksi internet
   - Menyediakan *backup* koneksi internet dari penyedia jasa internet yang berbeda
   - Memperbaharui perangkat jaringan di ruang data center
5. Bocornya hak akses seperti *username* dan *password administrator*
   - Melakukan peruubahan password secara berkala
6. Kerusakan pada *hardware server*
   - Melakukan pergantian berkala terhadap perangkat server

- Melakukan monitoring terhadap penggunaan subberdaya server

7. Kesalahan *maintenance* jaringan di ruang server
   - Menerapkan standar untuk pemeliharaan peralatan yang ada di ruang server
8. Terhentinya layanan karena supply listrik mati
   - Melakukan penambahan kapasitas sumber listrik cadangan yaitu UPS (*uniteruptible power supply*)
   - Melakukan perbaikan berkala terhadap generator set yang dimiliki.
9. Bencana alam yang mengakibatkan kerusakan perangkat terkait.
   - Menyiapkan rencana *Disaster Recovery Center* (DRC) dengan menempatkan server backup pada datacenter di tempat lain.

BAB V
PENUTUP

5.1 Rangkuman

OCTAVE Allegro adalah salah satu metode analisis risiko yang dapat dilakukan dengan cepat tanpa memerlukan pengetahuan mendalam tentang risiko. Langkah – langkah analisis risiko menggunakan OCTAVE Allegro akan menghasilkan profil aset, identifikasi area yang harus diperhatikan, identifikasi dan mitigasi risiko. Namun hasil mitigasi risiko masih sederhana sehingga membutuhkan analisis untuk memprioritaskan asset informasi atau area risiko yang harus dimitigasi terlebih dahulu.

AHP adalah metode sistem penunjang keputusan yang dapat digunakan untuk melakukan pemeringkatan berdasarkan kriteria yang diberikan. Hasil identifikasi risiko yang diperoleh menggunakan metode OCTAVE Allegro dapat digunakan data dalam perhitungan menggunakan metode AHP.

Kombinasi dari dari OCTAVE Allegro dan AHP dapat digunakan sebagai sebuah sistem penunjang keputusan bagi organisasi yang mengelola asset informasi. Manajemen risiko yang fokus pada keamanan asset informasi dan peringkat yang spesifik dapat digunakan sebagai dasar mengambil keputusan maupun perencanaan.

5.2 Simpulan

Berdasarkan hasil penelitian dan pembahasan tersebut diatas, maka dapat dirumuskan beberapa simpulan sebagai berikut:

1. Metode OCTAVE Allegro dapat digunakan untuk melakukan analisis risiko keamanan informasi terhadap aset informasi yang dimiliki data center Pemerintah Kabupaten Buleleng.
2. Metode AHP dapat digunakan untuk menentukan peringkat risiko sehingga organisasi dapat menentukan prioritas dalam perencanaan mitigasi risiko.

5.3 Saran

Berikut adalah beberapa saran yang dapat digunakan sebagai acuan dalam penelitian selanjutnya:

1. Menggunakan sistem keputusan lain seperti SAW, TOPSIS atau PROMETHEE untuk membandingkan hasil peringkat risiko keamanan informasi.
2. Mengembangkan *framework* yang menggabungkan beberapa metode analisis risiko keamanan informasi.

DAFTAR PUSTAKA

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *J. Basic. Appl. Sci. Res*, *2*(9), 9331–9347. www.textroad.com

Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. *Young*, *May*, 1–113.

Dorofee, A. (2005a). Managing Information Security Risks across the Enterprise. In *Guarding Your Business* (Issue April, pp. 151–172). https://doi.org/10.1007/0-306-48638-5_9

Dorofee, A. (2005b). Managing Information Security Risks across the Enterprise. In *Guarding Your Business* (pp. 151–172). Kluwer Academic Publishers. https://doi.org/10.1007/0-306-48638-5_9

Jufri, M. T., Hendayun, M., & Suharto, T. (2018). Risk-assessment based academic information System security policy using octave Allegro and ISO 27002. *Proceedings of the 2nd International Conference on Informatics and Computing, ICIC 2017*, *2018-Janua*, 1–6. https://doi.org/10.1109/IAC.2017.8280541

Keating, C. G. (2014). *Validating the Octave Allegro Information Systems Risk Assessment Methodology: A Case Study*. https://nsuworks.nova.edu/gscis_etd

Kuntari, N. L., Chrisnanto, Y. H., & ... (2018). Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda Octave Allegro. *Seminar Nasional …*. http://prosiding.uika-bogor.ac.id/index.php/semnati/article/view/106/88

Magdalenić, I., Ivkovic, N., Maček, D., & Ivković, N. (n.d.). *Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard*. Retrieved May 22, 2021, from https://www.researchgate.net/publication/268369522

Matondang, N., Isnainiyah, I. N., & Muliawatic, A. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *2*(1), 282–287. https://doi.org/10.29207/resti.v2i1.96

Mazareanu, V. P. (2011). Risk Management and Analysis: Risk Assessment (Qualitative and Quantitative). *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1549186

Munteanu, A. (2006). Information security risk assessment: The qualitative versus quantitative dilemma. *Managing Information in the Digital Economy: Issues and Solutions - Proceedings of the 6th International Business Information Management Association Conference, IBIMA 2006*, 227–232.

Naskar, S. K., & Bose, D. (2011). Performance Ranking of Diploma Institutions Based on Some Selected Criteria By Applying Scoring Model- a Sample Study. *Journal of Technical Education and Training*, *2*(2).

Pangestika, M. W., & Siregar, A. C. (2018). Analytic Hierarchy Process Dalam Pembobotan Untuk Pengaturan Jadwal Dosen. *CYBERNETICS*, *2*(01), 189. https://doi.org/10.29406/cbn.v2i01.1145

Prajanti, A. D., & Ramli, K. (2019, June 1). A Proposed Framework for Ranking Critical Information Assets in Information Security Risk Assessment Using the OCTAVE Allegro Method with Decision Support System Methods. *34th International Technical Conference on Circuits/Systems, Computers and Communications, ITC-CSCC 2019*. https://doi.org/10.1109/ITC-CSCC.2019.8793421

Rahardjo, B. (1998). *Keamanan Sistem Informasi Berbasis Internet*.

RI, K. S. (2020). Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. *Menteri Hukum Dan Hak Asasi Manusia Republik Indonesia*, 110.

Riasetiawan, M. (2016). Pusat Data untuk Pemerintahan. *Departemen Ilmu Komputer Dan Elektronik, FMIPA UGM*, 1–57. http://mardhani.staff.ugm.ac.id/files/2016/03/Pusat-Data-untuk-Pemerintahan.pdf

Saaty, R. W. (1987). The analytic hierarchy process-what it is and how it is used. *Mathematical Modelling*, *9*(3–5), 161–176. https://doi.org/10.1016/0270-0255(87)90473-8

Sardjono, W., & Cholik, M. I. (2018). Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank. *Proceedings of 2018 International Conference on Information Management and Technology, ICIMTech 2018*, 38–42.

https://doi.org/10.1109/ICIMTech.2018.8528108

St, R. F., Adhitya, R., & St, N. (2020). *Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro Pada Dinas Komunikasi Dan Informatika*. *7*(2), 7003–7008.

Suroso, J. S., & Fakhrozi, M. A. (2018). Assessment of Information System Risk Management with Octave Allegro at Education Institution. *Procedia Computer Science*, *135*, 202–213. https://doi.org/10.1016/j.procs.2018.08.167

Thibadeau, B. (2007). Prioritizing project risks using AHP. *PMI Global Congress 2007*, 1–9. https://www.pmi.org/learning/library/project-decision-making-tool-7292

LAMPIRAN

DATA SERVER DINAS KOMINFOSANDI KABUPATEN BULELENG

No	NAMA SERVER	SISTEM OPERASI	VM	APLIKASI
1	HP PROLIANT DL 380 Gen 10	PROXMOX	KPM	INDUK
		CENTOS 7	602 (54K1P-BULELENG)	SAKIP
		CENTOS 7	603 (LibreNMS)	LIBRENMS KOMINFO
		CENTOS 7	604 (PERPUS)	INLIS LITE 3.0
		CENTOS 7	609 (ARSIP)	SIKN (APLIKASI ARSIP)
2	QNAP	QNAP		Backup Database
3	IBM X3530 M4	RUSAK		
4	IBM X3530 M4	UBUNTU SERVER	-	PILBKD
				SIMPEG
5	HP PROLIANT DL 380 P	CENTOS	-	LPSE
6	HP PROLIANT DL 120 GEN-9	PROXMOX	KPM	Sistem Informasi Desa (129 web)
7	ASUS RS 520-EB	PROXMOX	KPM	INDUK
			100 (WEBSERVICE)	BACKUP SICANTIK
				GISREKLAME
8	DELL MC	PROXMOX	-	ANJAB/ABK
				E-SURAT
				RB WEBSITE
9	HP PL 180 GEN-6	CENTOS	-	LPSE PROVINSI
10	HP TOWER	WINDOWS SERVER	-	INTEGRA SAKIP
11	SERVER TOWER			ASISEDAP
12	HP PROLIANT DL 380 GEN 10	PROXMOX		INDUK
				NEW BULELENGKAB
				DNS SERVER
				MAIL SERVER
13	HP PROLIANT DL 380	LPSE		LPSE
14	HP PROLIANT DL 380 P	LPSE		LPSE

SOP MASUK RUANG SERVER

No.	KEGIATAN	Pelaksana		MUTU BAKU		Keterangan
		Staf / Petugas Server	Kepala Seksi Jaringan dan DC	Kelengkapan	Output	
1	2	3	4	7	9	10
1	Petugas Operator Server memastikan pengunjung melakukan pengisian formulir secara lengkap serta menyerahkan tanda pengenal diri yang sah, misal: KTP.			Formulir akses ruang server	Laporan	
2	Pengunjung memberikan formulir yang telah diisi kepada Petugas Operator Server untuk diberikan ijin akses.			Formulir akses ruang server	Persetujuan masuk ruang server	
3	Petugas Operator Server memverifikasi formulir dan menentukan apakah ijin akan diberikan atau tidak.			Formulir kunjuangan ruang server	Persetujuan masuk ruang server	
4	Petugas Operator Server memastikan selama berada di dalam ruangan server pengunjung harus senantiasa ditemani dan diawasi			Formulir kunjuangan ruang server	Laporan aktifitas ruang server	
6	Seusai kunjungan Petugas Operator Server memastikan formulir dilengkapi dengan daftar dan nomor seri perangkat yang dibawa (jika ada) dan jam keluar, serta pengembalian tanda pengenal ditukar dengan tanda pengenal diri yang diserahkan pada awal kunjungan.		Ya	Ceklist perangkat ruang server	Server telah diperbaiki dan berfungsi kembali	
7	Pengunjung menyerahkan formulir kepada Petugas Operator Server untuk diarsip.		Ya	Formulir kunjuangan ruang server	Laporan kegiatan di ruang server	


UNIVERSITAS PENDIDIKAN GANESHA
UNDIKSHA