BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

4.1.1. Identitas Responden Berdasarkan Bagian

Dari hasil pengumpulan serta pengerjaan informasi angket dengan jumlah ilustrasi sebesar 30 responden. Pada Bagan 4.1 selanjutnya ini adalah informasi responden bersumber pada bagian tipe genitalia responden, bisa diamati sebagai berikut:

Tabel 4.1 Rekapitulasi data responden berdasarkan bagian

No	Bagian	Jumlah	Persentase
1	Kepala Sekolah	1	3%
2	Wakil Kepala Sekolah	1	3%
3	Guru	21	70%
4	Staff	7	23%

Dari Tabel 4.1 di atas dapat diketahui bahwa responden yang mengisi kuesioner dari kepala sekolah berjumlah 1 orang, Bagian wakil kepala sekolah berjumlah 1 orang, guru berjumlah 21 orang, Staf/Karyawan berjumlah 7 orang.

Gambar 4.1 Data Responden

4.1.2 Identitas Responden Berdasarkan Jenis Kelamin

Dari hasil pengumpulan serta pengerjaan informasi angket dengan jumlah ilustrasi sebesar 30 responden diperoleh hasil pedaran tipe genitalia selaku selanjutnya semacam yang ditunjukkan pada tabel dibawah ini.

Tabel 4.2 Rekapitulasi data responden berdasarkan jenis kelamin

No	Jenis Kelamin	Jumlah	Persentase
1	Laki-laki	9	30%
2	Perempuan	21	70%

Hasil riset membuktikan kalau ada 21 ataupun 70% responden berjenis genitalia wanita, sebaliknya 9 ataupun 30% responden berjenis genitalia pria. Gambaran persentase bagan *chart pie* sebagai berikut :

Gambar 4.2 Data Responden Berdasarkan Jenis Kelamin

4.2.1 Membangun Kriteria Pengukuran Risiko *Oktave Allegro*

Ada delapan langkahyang harus dilakukan untuk melakukan analisi risiko sesuai dengan lembar 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. Keamanan

c. Produktivitas

d. Hukum dan Peraturan

e. Keuangan atau Biaya operasional

Tabel 4.3 Impact Area Reputasi dan Keberhasilan Pengguna

Lembar Kerja Allegro 1	**KRITERIA PENGUKURAN RISIKO - REPUTASI DAN KEBERHASILAN PENGGUNA**		
Area Dampak	**Rendah**	**Sedang**	**Tinggi**
Reputasi Sistem	Reputasi sedikit terpengaruh jika terjadi kerusakan terhadap sistem dengan usaha penanganan sistem yang dilakukan pada saat terjadi kerusakan	Reputasi sedikit terpengaruh jika terjadi kerusakan dalam sistem yang sedang dan dengan perbaikan dengan membutuhkan waktu yang singkat dengan biaya yang lebih	Reputasi pada tingkatan ini, dimana sangat mempengaruhi pengunjung dengan reputasi yang buruk dan mengganggu aktivitas utama pengunjung dan membutuhkan waktu yang lama dan biaya yang mahal
Kehilangan Pengunjung	Adanya pengurangan pengunjung yang diakibatkan hilangnya kepercayaan	Kurang dari 2% pengurangan pengunjung yang diakibatkan hilangnya kepercayaan	Tidak ada pengurangan pengunjung yang diakibatkan hilangnya kepercayaan

Tabel 4.4 Kriteria Penilaian Risiko Keamanan

Lembar Kerja Allegro 2	**KRITERIA PENGUKURAN RISIKO - KEAMANAN**		
Area Dampak	**Rendah**	**Sedang**	**Tinggi**
Reputasi Keamanan	Keamanan dipertanyakan, tapi tidak ada tanggapan peraturan dan sedikit atau tidak ada biaya	Keamanan berdampak, minimal ada tanggapan peraturan	Keamanan dilanggar, tanggapan peraturan yang signifikan denga melibatkan biaya yang mahal

Tabel 4.5 Kriteria Penilaian Risiko Produktivitas

Lembar Kerja Allegro 3	**KRITERIA PENGUKURAN RISIKO - PRODUKTVITAS**		
Area Dampak	**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 4.6 Kriteria Penilaian Risiko Hukum dan Peraturan

Lembar Kerja Allegro 4	**KRITERIA PENGUKURAN RISIKO – HUKUM DAN PERATURAN**		
Area Dampak	**Rendah**	**Sedang**	**Tinggi**
Tuntunan Hukum	Tidak ada tuntutan hukum atas kehilangan data diajukan terhadap website kepada pengelola	Adanya tuntutan hukum atas kehilangan data diajukan terhadap website kepada pengelola	Tuntutan hukum atas kehilangan data diajukan kepada pengelola dengan mengembalikan seluruh data yang sama atau mengembalikan 2 data yang berbeda

Tabel 4.7 Kriteria Penilaian Risiko Keuangan

Lembar Kerja Allegro 5	**KRITERIA PENGUKURAN RISIKO - KEUANGAN**		
Area Dampak	**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

Langkah 1 aktivitas 2

Pada tahap ini digunakan untuk mengevaluasi dampak yang akan terjadi pada perusahaan dilihat dari usaha instansi/sekolah untuk menanggulangi resiko yang ada dari masing masing area yang di identifikasi. Di dalamnya masih ada ukuran kualitatif yang risikonya bisa dinilai dan menciptakan landasan berdasarkan evaluasi risiko dari sistem informasi. Dari area yang berdampak rendah, sedang dan tinggi antara lain adalah:

Tabel 4.8 Skala Prioritas *Impact Area*

Lembar Kerja Allegro 6	**PRIORITAS AREA TERDAMPAK**
Prioritas	**Area Dampak**
5	Reputasi dan Kepercayaan Pengguna
4	Keamanan
2	Produktivitas
1	Hukum dan Peraturan
3	Keuangan atau Biaya Operasional

Dari Tabel 4.8 Skala Prioritas *Impact Area* diatas berdasarkan hasil wawancara di SDB, Reputasi dan Kepercayaan Pengguna berada pada prioritas 5, karena reputasi sistem mempengaruhi aktivitas pengolahan data Keamanan berada pada prioritas 4, karena semua data sudah terkomputerisasi pada website sekolah. Keuangan berada pada prioritas 3 karena sistem informasi sudah terkomputerisasi dan membutuhkan biaya yang cukup untuk memelihara sistem, agar selalu up to date dan berjalan dengan lancar, pada Produktivitas berada pada prioritas 2 karena ketika website terjadi masalah akan mempengaruhi jam kerja karyawan, sedangkan pada Hukum dan Peraturan berada pada prioritas 1 karena tidak mempngaruhi sistem yang digunakan.

Langkah 2 – Membuat Profil Aset Informasi.

Terdapat delapan kegiatan yaitu yang pertama adalah melakukan identifikasi aset prioritas area terdampak 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 4.9 Profil Aset Kritis

Lembar Kerja Allegro 7	**PROFIL ASET KRITIS**	
(1) Aset Kritis Aset informasi apa yang paling penting ?	(2) Dasar Pemikiran untuk Seleksi Mengapa aset informasi ini penting bagi organisasi?	(3) Deskripsi Apa uraian yang disepakati tentang aset informasi ini?
Aset Website Darma Bangsa	Karena data ada di asset tersebut jika Aset Website Darma Bangsa	Aset informasi ini berisi informasi sekolah, pendaftaran, dan informasi keuangan
(4) Pemilik (s) Siapa pemilik aset informasi ini?		
Bagian Operator Sekolah Darma Bangsa		
(5) Persyaratan Keamanan Apa persyaratan keamanan untuk aset informasi ini?		
Kerahasiaan	Memastikan bahwa hanya orang yang berwenang yang memiliki akses ke aset informasi	Anggota staff yang memiliki bagian tersendiri yang bertanggung jawab atas sistem yang dikerjakan
Integritas	Memastikan bahwa aset informasi tetap dalam kondisi yang dimaksudkan oleh pemilik dan untuk tujuan yang dimaksudkan oleh pemiliknya	Staff yang berwenang yang dapat memperbarui / mengubah informasi, hanya staff di bagian tersebut yang dapat memasukkan dan memodifikasi aset informasi
Tersedianya	Memastikan bahwa aset informasi tetap dapat diakses oleh pengguna yang berwenang	Website harus tersedia bagi petugas entri data untuk melakukan semua data yang ada.
(6) Persyaratan keamanan yang paling penting Apa persyaratan keamanan terpenting untuk aset informasi ini?		
✓ Kerahasiaan	❑ Integritas	❑ Ketersediaan

Langkah 3 – Mengidentifikasi Kontainer Aset Informasi

Tahapan ini menjelaskan tentang identifikasi suatu informasi aset dari suatu sistem mengenai tempat penyimpanan, pengiriman serta tempat pemprosesan sistem yang digambarkan dengan *worksheet Information Asset Risk Environment Map.* Tujuan dari tahapan ini yaitu untuk mengetahui tempat dimana aset informasi disimpan, dikirim, dan di proses.

Tabel 4.10. Peta Lingkungan Risiko Informasi Aset Informasi Teknikal

Lembar Kerja Allegro 9a	**INFORMATION ASSET RISK ENVIRONMENT MAP (TEKNIKAL)**
Dalam	
1. Server Website Darma Bangsa	Dikelola oleh Hosting Website
2. Workstation Website Darma Bangsa	Dikelola oleh Operator Sekolah
Luar	
1. Koneksi Internet	ISP

Tabel 4.11. Kontainer Aset Informasi Fisikal

Lembar Kerja Allegro 9b	**INFORMATION ASSET RISK ENVIRONMENT MAP (FISIKAL)**
Dalam	
1. Jaringan intranet di ruang server	Operator Jaringan Sekolah Darma Bangsa
2. Back UP Data Server	Bagian Operator Sekolah Darma Bangsa
Luar	

Tabel 4.12. Kontainer Informasi Aset Informasi Orang

Lembar Kerja Allegro 9c	**INFORMATION ASSET RISK ENVIRONMENT MAP (ORANG)**
Dalam	
1. Administrator Sistem	Operator Sekolah
2. User Aplikasi	Guru dan Staff
Luar	
1. Penyedia jasa Internet	Vendor ISP

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 4.13. Area Perhatian Aset Kritis

No	**Area Yang Menjadi Perhatian**
1	Mengalami kerusakan pada web SDB sehingga pihak sekolahan tidak dapat melakukan pengolahan data infromasi.
2	Bocornya hak akses seperti *username* dan *password*

Tabel 4.1.4. Tabel Identifikasi Pada *Quisoner*

Ancaman 1. Mengalami Kerusakan pada Web SDB				
Lembar kerja ini akan membantu anda memikirkan skenario yang dapat mempengaruhi asset formasi anda pada wadah teknis penyimpanan berada. Skenario ini dapat menimbulkan risiko yang harus anda hadapi. Pertimbangan setiap skenario dan ceklis respon yang tepat' Jika jawaban anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak sengaja atau keduanya.				
Skenario 1 : Pikirkan orang-orang yang bekerja di organisasi anda. Adakah situasi di mana seorang karyawan dafat mengakses satu atau lebih wadah teknis secara tidak sengaja atau sengaja sehingga menyebabkan aset informasi anda menjadi :				
1.	Diungkapkan kepada individu yang tidak berwenang ?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)
2.	Diubah agar tidak digunakan untuk tujuan yang diinginkan ?	Tidak	Ya	Ya (Sengaja)

			(Secara Tidak Sengaja)	
3.	Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan ?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)
4.	Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)

Ancaman 2. Bocornya Hak Akses seperti *Username* dan *Password*				
Lembar kerja ini akan membantu anda memikirkan skenario yang dapat mempengaruhi asset formasi anda pada wadah teknis user dan password. Skenario ini dapat menimbulkan risiko yang harus anda hadapi. Pertimbangan setiap skenario dan ceklis respon yang tepat' Jika jawaban anda adalah "iya" pertimbangkan apakah skenario bisa terjadi secara tidak sengaja atau keduanya.				
Skenario 1 : Pikirkan orang-orang yang bekerja di organisasi anda. Adakah situasi di mana seorang karyawan dafat mengakses satu atau lebih wadah teknis secara tidak sengaja atau sengaja sehingga menyebabkan aset informasi anda menjadi :				
1.	Diungkapkan kepada individu yang tidak berwenang ?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)
2.	Diubah agar tidak digunakan untuk tujuan yang diinginkan ?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)
3.	Terganggu sehingga tidak bisa diakses untuk tujuan yang diinginkan ?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)
4.	Dihancurkan secara permanen atau untuk sementara hilang sehingga tidak dapat digunakan untuk tujuan yang dimaksudkan?	Tidak	Ya (Secara Tidak Sengaja)	Ya (Sengaja)

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 4.15. Identifikasi Skenario Ancaman

Area Yang Menjadi Perhatian	**Skenario Ancaman**	
Mengalami kerusakan pada web SDB sehingga pihak sekolah tidak dapat melakukan pengolahan data infromasi.	*1.Actor*	Eksternal
	2. Means	Melakukan perusakan pada aplikasi Website sekolah
	3. Motiv	Ingin Merusak Website Sekolah
	4. Outcome	Modifikasi Interupsi/script
	5. Security requirements	Melakukan update secury server
Bocornya hak akses seperti *username* dan *password*	*1.Actor*	Eksternal
	2. Means	*Password cracking*
	3. Motiv	Ingin Merusak Website Sekolah
	4. Outcome	Modifikasi Interupsi/*script*
	5. Security requirements	Kebijakan standar keamanan *password*

Langkah 6 – Mengidentifikasi Risiko

Pada Tabel 4.15 Menghitung *Score Impact Area* menunjukkan bahwa dari konsekuensi memberikan nilai dampak dan skor total yang dapat digunakan untuk menganalisis risiko dan membantu organisasi menentukan strategi risiko yang tepat.

Tabel 4.16. Identifikasi Nilai Dampak

Area Dampak	**Prioritas**	**Nilai Dampak**		
		Rendah (1)	Sedang (2)	Tinggi (3)
Reputasi dan Kepercayaan Pengguna	**5**	**5**	**10**	**15**
Keamanan	**4**	**4**	**8**	**12**
Produktivitas	**2**	**2**	**4**	**6**
Hukum dan Peraturan	**1**	**1**	**2**	**3**
Keuangan atau Biaya operasional	**3**	**3**	**6**	**9**

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 berikut.

Tabel 4.17. Allegro Worksheet 10-a

<table>
<tr><td colspan="3">Allegro – Worksheet 10a</td><td colspan="5">Information Assets Risk Worksheet</td></tr>
<tr><td rowspan="11">Informasi Assets Risk</td><td rowspan="8">Threat</td><td>Asset Informasi</td><td colspan="4">SMP Darma Bangsa</td></tr>
<tr><td>Area Perhatian</td><td colspan="4">Mengalami kerusakan pada web SDB sehingga pihak sekolah tidak dapat melakukan pengolahan data infromasi.</td></tr>
<tr><td>(9) Actor</td><td colspan="4">External</td></tr>
<tr><td>(10)Means</td><td colspan="4">Melakukan perusakan pada aplikasi Website sekolah</td></tr>
<tr><td>(11)Motive</td><td colspan="4">Ingin Merusak Website Sekolah</td></tr>
<tr><td>(12)Outcome</td><td colspan="4">Modifikasi Interupsi/script</td></tr>
<tr><td>(13)Security Requirements</td><td colspan="4">Melakukan update security server</td></tr>
<tr><td>(14)Probability</td><td>High</td><td>Medium</td><td colspan="2">Low</td></tr>
<tr><td colspan="3">(15) Consequences</td><td colspan="3">(16) Severity</td></tr>
<tr><td colspan="3" rowspan="2">Informasi yang dimodifikasi menyebabkan kerusakan mengganggu validitas informasi tersebut</td><td colspan="2">Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td colspan="2">Reputasi dan kepercayaan Pengguna</td><td>High</td><td>15</td></tr>
<tr><td colspan="3"></td><td colspan="2">Keamanan</td><td>High</td><td>12</td></tr>
<tr><td colspan="3"></td><td colspan="2">Produktivitas</td><td>Low</td><td>2</td></tr>
<tr><td colspan="3"></td><td colspan="2">Hukum dan Peraturan</td><td>Low</td><td>1</td></tr>
<tr><td colspan="3"></td><td colspan="2">Keuangan dan Biaya Operasional</td><td>Medium</td><td>6</td></tr>
<tr><td colspan="6">Relative Risk Score</td><td>36</td></tr>
</table>

Tabel 4.18. Allegro Worksheet 10-b

<table>
<tr><td colspan="3">Allegro – Worksheet 10b</td><td colspan="5">Information Assets Risk Worksheet</td></tr>
<tr><td rowspan="11">Informasi Assets Risk</td><td rowspan="8">Threat</td><td>Asset Informasi</td><td colspan="4">SMP Darma Bangsa</td></tr>
<tr><td>Area Perhatian</td><td colspan="4">Bocornya hak akses seperti username dan password</td></tr>
<tr><td>(1) Actor</td><td colspan="4">External</td></tr>
<tr><td>(2) Means</td><td colspan="4">Password cracking</td></tr>
<tr><td>(3) Motive</td><td colspan="4">Ingin Merusak Website Sekolah</td></tr>
<tr><td>(4) Outcome</td><td colspan="4">Modifikasi Interupsi/script</td></tr>
<tr><td>(5) Security Requirements</td><td colspan="4">Kebijakan standar kemanan password</td></tr>
<tr><td>(6) Probability</td><td>High</td><td>Medium</td><td colspan="2">Low</td></tr>
<tr><td colspan="3" rowspan="2">(7) Consequences</td><td colspan="3">(8) Severity</td></tr>
<tr><td>Impact Area</td><td>Value</td><td>Score</td></tr>
<tr><td colspan="3">Informasi yang dimodifikasi menyebabkan kerusakan mengganggu validitas informasi tersebut</td><td>Reputasi dan kepercayaan Pengguna</td><td>High</td><td>15</td></tr>
<tr><td></td><td></td><td></td><td>Keamanan</td><td>High</td><td>12</td></tr>
<tr><td></td><td></td><td></td><td>Produktivitas</td><td>Low</td><td>2</td></tr>
<tr><td></td><td></td><td></td><td>Hukum dan Peraturan</td><td>Low</td><td>1</td></tr>
<tr><td></td><td></td><td></td><td>Keuangan dan Biaya Operasional</td><td>High</td><td>9</td></tr>
<tr><td colspan="6">Relative Risk Score</td><td>39</td></tr>
</table>

Langkah 8 – Memilih Pendekatan Mitigasi

Pada Tabel 4.18 *Relative Risk Matrix* diatas Pool digunakan untuk mengkategorikan risiko berdasarkan pada skor risikonya.

Tabel 4.19. 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.

Langkah 8 aktivitas 2

Risk Mitigation merupakan pengembangan strategi mitigasi risiko karena perlu dibuat suatu strategi untuk memitigasi risiko tersebut

Tabel 4.20. *Risk Mitigation*

Risk Mitigation	
Area yang menjadi perhatian	Mengalami kerusakan pada Website SDB sehingga pihak sekolah tidak dapat melakukan pengolahan data Informasi.
Tindakan	***Mitigate.***
Wadah	Kontrol.
Solusi	1. Meningkatakan sistem keamanan pada aplikasi Website SDB 2. Melakukan evaluasi terhadap Website Hosting yang digunakan.
Risk Mitigation	
Area yang menjadi perhatian	Bocornya hak akses seperti *username* dan *password.*
Tindakan	***Mitigate.***
Wadah	Kontrol.
Solusi	1. Meningkatakan sistem keamanan *password* dan username 2. Melakukan pergantian *username* dan *password* secara berkala.

Tabel. 4.21. Hasil analisis OCTAVE Allegro

Area Perhatian	***Action***
Mengalami kerusakan pada Website SDB sehingga pihak sekolah tidak dapat melakukan pengolahan data Informasi.	*Mitigate*
Bocornya hak akses seperti *username* dan *password*	*Mitigate*

4.3. Pembahasan

Berdasarkan hasil penelitian menggunakan metode *OCTAVE Allegro* terdapat 5 area dampak yang berisiko pada Website SDB. Area dampat tersebut yaitu Reputasi dan Kepercayaan Pengguna, Keamanan, Produktivitas, Hukum dan Peraturan, Keuangan atau Biaya operasional. Peneliti kemudian melakukan analisis area perhatian asset kritis yaitu pertama mengalami kerusakan pada web SDB sehingga

pihak sekolah tidak dapat melakukan pengolahan data infromasi yang kedua adalah bocornya hak akses seperti username dan password. Selanjutnya dilakukan identifikasi area dampak antara rendah, sedang, dan tinggi.

Setelah peroses dan tahapan octave allegro dilakukan penulis mengimplementasikan hasil analisis pada tahap *worksheet allegro 10a* dan *worksheet allegro 10b* didaptkan nilai sebesar 36 pada *worksheet allegro 10a* dan nilai 39 pada *worksheet allegro 10b.* Menurut table pendekatan mitigasi resiko matrik relative nilai dari *worksheet allegro 10a* dan *worksheet allegro 10b* tersebut harus melakukan mitigasi karena memiliki rentang nilai dia antara 30-45. Peneliti kemudian malakukan tahapan *risk mitigation* untuk meberikan Solusi kepada area dampak yang memiliki nilai ambang yang lumayan tinggi agar menjadi Solusi kepada operator website SDB untuk mempertimbangkan Solusi dari penulis.