BAB III
METODOLOGI PENELITIAN

3.1 Subjek dan Objek Penelitian

Penelitian ini dilakukan di PERUMDA Tirta Satria Banyumas yang berlokasi di Jl. Prof. Dr. Suharso No.52, Mangunjaya, Purwokerto Lor, Kec. Purwokerto Timur, Kabupaten Banyumas, Jawa Tengah. PERUMDA Tirta Satria ini telah menggunakan layanan digital dalam proses pelayananan dan proses bisnisnya. Subjek penelitian melibatkan Supervisor Teknologi Informasi (TI) pada PERUMDA Tirta Satria Banyumas. Objek penelitian difokuskan pada standar ISO 27001: 2013 pada sistem keamanan informasi PERUMDA Tirta Satria Banyumas dengan fokus pada peningkatan prosedur penanganan insiden keamanan, pembentukan tim tanggap darurat keamanan siber serta memperkuat keamanan sistem informasi perusahaan dengan standar ISO 27001:2013.

3.2 Alat dan Bahan Penelitian

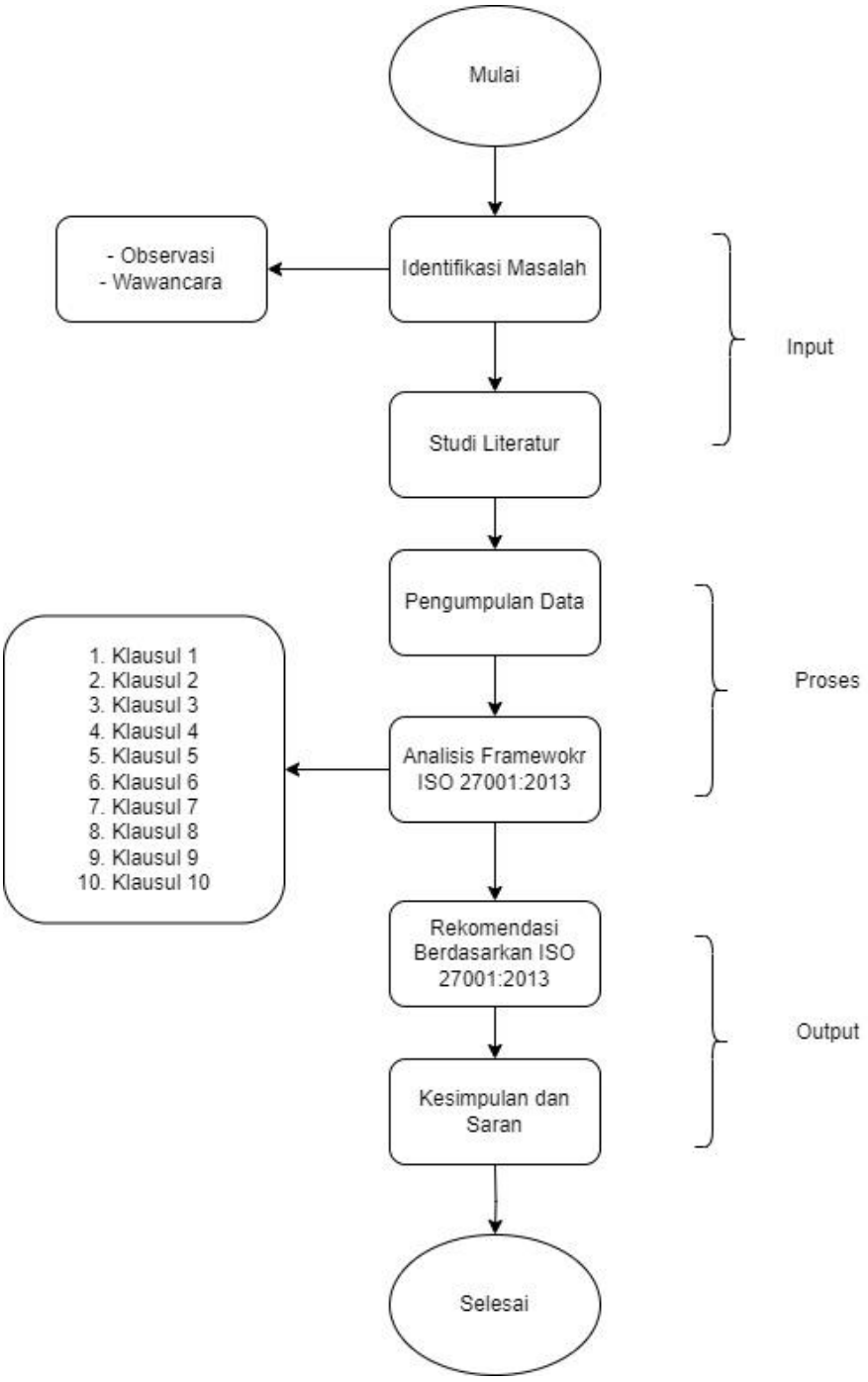
3.2.1 Alat

Selama kegiatan penyelesaian tugas akhir ini mengaplikasikan beberapa alat dan materi. Peralatan yang digunakan dalam tugas akhir antara lain laptop acer, handphone oppo a2020**,** wifi, mendeley, draw.io.

3.2.1.1 Bahan

Bahan penelitian sebagai aspek pendukung proses penelitian ini berupa data primer yaitu melakukan observasi langsung pada PERUMDA Tirta Satria Kabupaten Banyumas berupa wawancara langsung untuk mencari permasalahan yang terjadi pada organisasi tersebut di bagian Sumber Daya Manusia (SDM) dan Teknologi Informasi (TI). Data sekunder berupa tinjauan pustaka yang diperoleh dari penelusuran pada jurnal-jurnal penelitian sebelumnya untuk mengetahui teori-teori, penggunaan framwork dan hasil penyelesaian masalah pada penelitian sebelumnya.

3.3Diagram Alir Penelitian



Gambar 1. Alur Penelitian

Berikut penjelasan singkat mengenai tahap penelitian pada gambar 1.

3.3.1 Identifikasi Masalah

Penelitian dimulai dengan proses pengidentifikasian masalah yang ada pada objek penelitian yaitu PERUMDA Tirta Satria Kabupaten Banyumas. Tahap ini dilakukan dengan metode analisis deskriptif. Penggunaan analisis deskriptif memiliki untuk tujuan menggali lebih rinci dan memberikan gambaran yang mendalam mengenai topik penelitian ini. Analisis deskriptif juga digunakan untuk menjelaskan data kualitatif. Data kualitatif pada penelitian ini menggunakan data :

1) Data primer

   Data primer merupakan data yang diperoleh peneliti langsung di Divisi Sumber daya dan Manusia (SDM) & Teknologi Indformasi (TI). Data dipeoleh dengan beberapa metode yaitu

   a. Observasi

      Kegiatan observasi dilaksanakan secara langsung melalui pengamatan pada objek penelitian yaitu PERUMDA Tirta Satria Kabupaten Banyumas.

   b. Wawancara

      Proses mendapatkan data dan masalah-masalah yang terjadi pada perusahaan dilakukan dengan wawancara. Wawancara dilakukan dengan staff Sumber Daya Manusia (SDM) dan Teknologi Informasi(TI) yaitu Bapak Aziz.

2) Data Sekunder

   Data sekunder merupakan data yang diperoleh dari beberapa studi literatur yang terkait dengan topik dan permasalahan pada penelitian. Pada tahap studi literatur dilakukan dengan pengumpulan beberapa referensi yang berasal dari jurnal, website, dan dokumen pendukung lain dapat menjadi acuan dalam pembuatan penelitian ini.

3.3.2 Pengumpulan Data

Penelitian ini dilakukan dengan proses wawancara bersama staff PERUMDA Tirta Satria untuk memperoleh informasi mengenai tahap pegumpulan data. Jenis pertanyaan yang digunakan dalam pengumpulan data pada proses wawancara yaitu dengan menerapkan wawancara semi berstruktur. Pedoman wawancara berfokus pada subjek area tertentu yang diteliti, tetapi dapat direvisi setelah wawancara jika muncul ide-ide baru. Meskipun pewawancara bertujuan untuk mendapatkan perspektif partisipan, mereka harus tetap mengendalikan diri agar tujuan penelitian dapat tercapai dan topik penelitian dapat tergali secara mendalam.

Pada penelitian ini dilakukan tahap wawancara dengan pertanyaan sebegai berikut :

Tabel 3.1 Daftar Pertanyaan

No. Klausul	Requirement		Score	Status
4	Konteks Organisasi			
4.1	Memahami organisasi dan konteksnya	Memahami organisasi dan konteksnya dengan mempertimbangkan:		
		1. Organisasi memiliki pihak bertanggung jawab untuk memastikan kejelasan terkait pemahaman mengenai tujuan dan sasaran keamanan informasi.		
		2. Organisasi memanfaatkan pengalaman dan keahlian tim manajeman untuk mengidentifikasi faktor-faktor internal		

No. Klausul	Requirement		Score	Status
		yang mempengaruhi keamanan informasi.		
		3. Organisasi mempertimbangkan penerapan teknologi analitik atau alat manajemen informasi yang lebih canggih untuk meningkatkan pemahaman mereka tentang operasional untuk menunjang keamanan sistem		
4.2	Memahami Kebutuhan	Organisasi mampu memahami kebutuhankebutuhan yang relevan terhadap sistem manajemen keamanan informasi dengan mempertimbangkan :		
		1. Memiliki pihak-pihak yang sadar akan pentingnya kebutuhan yang relevan terhadap sistem manajemen keamanan informasi organisasi.		
		2. Organisasi mampu melakukan identifikasi dan paham mengenai kebutuhan pihak-pihak terkait dengan keamanan informasi		
4.3	Penentuan ruang lingkup Sistem Menejemen	Menentukan ruang lingkup pengelolaan lingkungan sistem manajemen keamanan informasi meliputi :		

No. Klausul	Requirement		Score	Status
	Keamanan Informasi(SMKI).	1. Organisasi mampu menentukan ruang lingkup sistem menejemen keamanan informasi pada perusahaan		
		2. Organisasi memiliki prosedural konkret dalam memastikan ruang lingkup sistem manajemen keamanan informasi mencakup semua aktivitas, proses, dan lokasi yang relevan untuk keamanan informasi.		
4.4	Sistem Menejemen Keamanan Informasi(SMKI)	Memahami sistem manajemen keamanan informasi denngan memperhatikan:		
		1. Oganisasi mampu menetapkan sistem manajemen keamanan informasi berjalan dengan baik		
		2. Organiasi memiliki mekanisme yang sistematis yang berguna dalam pemantauan perubahan regulasi yang berpotensi mempengaruhi sistem keamanan informasi pada perusahaan.		
5				

No. Klausul	Requirement		Score	Status
5.1	Kepemimpinan dan komitmen	Manajemen puncak mampu menunjukan kepemimpinan dan komitmen sehubung dengan sistem manajemen perusahaan meliputi :		
		1. Memiliki pemimpin utama yang bertanggung jawab dalam semua peran dan tanggung jawabnya		
		2. Memiliki pimpinan yang melibatkan diri secara aktif dalam pengembangan, pelaksanaan, dan pemeliharaan sistem manajemen keamanan informasi		
		3. Adanya keterlibatan pimpinan organisasi dalam pemberian dukungan dan keterlibatan dalam keadaan darurat atau insiden keamanan informasi.		
		4. Pimpinan organisasi melakukan pendemontrasikan dukungan dan keterlibatan mereka dalam keadaan darurat atau insiden keamanan informasi		
5.2	Kebijakan	Kebijakan perusahaan dengan memperhatikan:		

No. Klausul	Requirement		Score	Status
		1. Melakukan pengorganisasian dan pendokumentasian kebijkan keamanan informasi pada organisasi.		
		2. Adanya pihak yang bertanggung jawab atas pengembangan, persetujuan, dan pemeliharaan kebijakan keamanan informasi		
		3. Organisasi mampu memastikan bahwa kebijakan keamanan informasi mudah dipahami oleh semua anggota organisasi dan dipatuhi.		
5.3	Peran organisasi, tanggung jawab dan wewenang	Mementukan peran organiasi, tanggung jawab, dan wewenang perusahaan dengan memperhatikan		
		1. Organisasi memiliki kebijakan dan prosedur resmi terkait tata kelola teknologi informasi.		
		2. Organisasi melakukan pengawasan serta pengimplemantasikan pada kebijakan-kebijakan keamanan informasi		
6				
6.1	Tindakan untuk menangani risiko dan peluang	Tindakan dalam mengatasi risiko dan peluang dengen melihat :		

No. Klausul	Requirement		Score	Status
		1. Organisasimelakukan Penanganan Organisasi mengalami insiden keamanan teknologi informasi		
		2. Organisasi mampu mengidentifikasi risiko yang berkaitan dengan keamanan informasi		
		3. Organisasi mampu melakukan Langkah-langkah dalam menangani risiko keamanan data dan privasi.		
		4. Organisai memiliki perencanaan yang jelas untuk mengatasi risiko keamanan informasi yang signifikan.		
6.2	Sasaran keamanan informasi dan perencanaan untuk mencapainya	Sasaran keamanan informasi dan perencanaan dalam mencapainya mempertimbangkan :		
		1. Organisasi mampu menetapkan sasaran keamanan informasi		
		2. Organisasi memastikan bahwa sasaran keamanan informasi yang ditetapkan dapat diukur dan dapat dicapai.		
		3. Organisasi memiliki prosedur konkret		

No. Klausul	Requirement		Score	Status
		untuk merencanakan pencapaian sasaran keamanan informasi.		
7				
7.1	Sumber Daya	Organisasi memperhatikan dukungan sumberdaya perusahaan :		
		1. Organisasi mampu menentukan dan menyediakan sumber daya yang diperlukan untuk mendukung sistem manajemen keamanan informasi (SMKI).		
		2. Organisasi memastikan bahwa sumber daya yang diberikan memadai untuk mencapai dan memelihara keamanan informasi.		
		3. Organisasi memiliki pengukuran untuk mengevaluasi efektivitas pengelolaan sumber daya dalam konteks sistem manajeman keamanan informasi.		
7.2	Kompetensi	Organisasi memperhatikan dukungan kompetensi perusahaan :		
		1. Organisasi memastikan bahwa tim paham mengenai sistem manajemen keamanan informasi dan telah melakukan pembekalan		

No. Klausul	Requirement		Score	Status
		kompetensi yang cukup.		
		2. Organisasi memiliki program pelatihan atau pengembangan untuk meningkatkan kompetensi personel terkait keamanan informasi.		
		3. Organisasi memiliki kriteria atau standar tertentu untuk menilai kompetensi personel dalam konteks keamanan informasi.		
7.3	Kepedulian	Organisasi telah menyelenggarakan program kepedulian dalam keamanan sistem.		
7.4	Komunikasi	Organisasi telah melakukan komunikasi yang efektif terkait dengan risiko dan peluang keamanan informasi di seluruh organisasi.		
7.5	Informasi Terdokumentasi	Organisasi melakukan informasi terdokumentasi dengan memperhatikan:		
		1. Organisasi mampu menentukan dan memelihara informasi terdokumentasi yang diperlukan oleh sistem manajemen keamanan informasi		
		2. Organisasi memiliki prosedur dokumentasi yang mengatur pembuatan, perubahan, dan penarikan informasi		

No. Klausul	Requirement		Score	Status
		terdokumentasi di seluruh organisasi.		
		3. Organisasi mampu memastikan bahwa informasi terdokumentasi yang diperlukan untuk sistem manajeman keamanan informasi tetap tersedia dan dapat diakses oleh pihak yang berwenang		
		4. Organisasi memiliki prosedur untuk melindungi informasi terdokumentasi yang bersifat rahasia atau sensitif.		
8				
8.1	Perencanaan dan pengendalian operasional	Perencanaan dan pengendalian operasional mempertimbangkan :		
		1. Organisasi mampu mengambil Keputusan terkait perencanaan dan pengendalian operasioal.		
		2. Organisasi memiliki langkah-langkah pengendalian untuk memastikan keberlanjutan operasional dan ketersediaan sistem dan layanan informasi.		
		3. Organisasi memiliki prosedur untuk		

No. Klausul	Requirement		Score	Status
		memastikan bahwa kebijakan keamanan informasi diterapkan dan dipatuhi dalam setiap tahap operasional.		
		4. Organisasi memastikan bahwa setiap perubahan dalam operasional diuji coba atau diuji keamanannya sebelum diimplementasikan secara penuh.		
8.2	Penilaian resiko keamanan informasi	Penilaian resiko keamanan informasi dengan mempertimbangkan :		
		1. Organisasi mampu mendefinisikan dan mengidentifikasi aset informasi yang kritis atau penting untuk keberlanjutan operasional.		
		2. Organisasi memiliki kriteria yang digunakan untuk menilai dampak dan probabilitas risiko keamanan informasi.		
		3. Organisasi mampu menilai risiko terhadap kerahasiaan, integritas, dan ketersediaan aset informasi.		
8.3	Penanganan risiko keamanan informasi	Organisasi memiliki langkah-langkah yang diambil organisasi jika terjadi		

No. Klausul	Requirement		Score	Status
		perubahan dalam risiko keamanan informasi atau munculnya peluang baru.		
9				
9.1	Pemantauan, pengukuran, analisis, dan evaluasi	Pemantauan, pengukuran, analisis, dan evaluasi mempertimbangkan :		
		1. Organisasi memonitor keamanan informasi dan kinerja sistem manajemen keamanan informasi.		
		2. Organisasi mampu menilai keefektivitasan manajemen risiko keamanan informasi yang diukur dan dievaluasi secara berkala.		
		3. Organisasi memiliki langkah-langkah yang diambil memonitor perubahan dalam konteks organisasi atau dalam kebutuhan keamanan informasi.		
9.2	Audit Internal	Audit internal dengan mempertimbangkan :		
		1. Organisasi memiliki tim audit internal sendiri.		
		2. Organisasi mampu memastikan bahwa auditor internal memiliki keterampilan dan pengetahuan yang diperlukan untuk		

No. Klausul	Requirement		Score	Status
		mengevaluasi keamanan informasi.		
		3. Organisasi memiliki proses yang mengatur pelaksanaan audit internal, termasuk frekuensi dan metode pelaksanaannya.		
		4. Organisasi melakukan pelaporan hasil audit internal.		
		5. Organisasi memiliki langkah-langkah mengenai tindak lanjut hasil audit internal.		
		6. Organisasi memiliki proses dokumentasi untuk mengelola temuan dan rekomendasi audit internal.		
9.3	Review Manajemen	Review manajemen dengan mempertimbangkan :		
		1. Organisasi mampu melaksanakan review manajemen terkait dengan Sistem Manajemen Keamanan Informasi.		
		2. Organisasi melakukan penjadwalan review manajemen.		
		3. Organisasi mampu mengumpulkan dan menganalisis data yang relevan untuk		

No. Klausul	Requirement		Score	Status
		digunakan dalam review manajemen.		
		4. Organisasi mampu mengambil tindakan yang tepat sebagai respons terhadap hasil review manajemen, terutama jika terdapat ketidaksesuaian		
10				
10.1	Ketidaksesuaian dan Tindakan korektif	Ketika terjadi ketidaksesuain dan Tindakan korektif organisasi harus :		
		1. Organisasi mampu menilai tingkat dampak dan risiko yang terkait dengan ketidaksesuaian yang teridentifikasi.		
		2. Organisasi memiliki langkah-langkah untuk menanggapi ketidaksesuaian dengan cepat dan efektif.		
		3. Organisasi memiliki proses dokumentasi untuk menentukan dan melaksanakan tindakan korektif terhadap ketidaksesuaian.		
10.2	Perbaikan berkelanjutan	Perbaikan berkelanjutan dilakukan oleh organisasi dengan cara :		
		1. Organisasi mampu mengukur keberhasilan dan		

No. Klausul	Requirement		Score	Status
		perbaikan berkelanjutan dalam tata kelola informasi.		
		2. Organisasi memiliki rencana tindakan perbaikan dan pencegahan yang diimplementasikan dalam konteks keamanan informasi.		

3.3.3 Analisis Standar ISO 27001:2013

Penelitian ini melakukan kegiatan analisis standar ISO 27001:2013 dengan menerapkan langkah-langkah sebagai berikut ;

1. Membuat poin setiap pertanyaan berdasarkan standar ISO 27001:2013

   ISO 27001:2013 memiliki beberapa klausul dengan beberapa sub klausul didalamnya. Untuk mendapatkan nilai yang pasti, diperlukan beberapa sub pertanyaan. Hal ini juga dilakukan untuk memahami tujuan dari pertanyaan ISO 27001:201. Setiap pertanyaan iso 27001:2013 diidentifikasi, kemudian dianalisis memasuki pada variabel ISO 27001:2013 dengan penyebutan poin 1,2,3,4,dan 5. Pernyataan berdasarkan standar ISO 27001:2013 tersebut ditulis dalam tabel poin. Poin -poin dalam klausul standar ISO 27001:2013 sebagai berikut :

   1) klausa 4 – Konteks Organisasi

      Poin -poin dalam klausul 4 pada standar ISO 27001:2013 sebagai berikut :

      a. Memahami organisasi dan konteksnya.
      b. Memahami kebutuhan.

c. Penentuan ruang lingkup Sistem Menejemen Keamanan Informasi(SMKI).
d. Sistem Menejemen Keamanan Informasi(SMKI).

2) Klausa 5 – Kepemimpinan

Poin -poin dalam klausul 5 pada standar ISO 27001:2013 sebagai berikut :

a) Kepemimpinan dan komitmen
b) Kebijakan
c) Peran organisasi, tanggung jawab dan wewenang

3) Klausa 6 – Perencanaan

Poin -poin dalam klausul 6 pada standar ISO 27001:2013 sebagai berikut :

a) Tindakan untuk menangani risiko dan peluang
b) Sasaran keamanan informasi dan perencanaan untuk mencapainya.

4) Klausa 7 – Pendukung

Poin -poin dalam klausul 7 pada standar ISO 27001:2013 sebagai berikut :

a. Sumberdaya
b. Kompetensi
c. Kepedulian
d. Komunikasi
e. Informasi terdokumentasi

5) Klausa 8 – Operasi

Poin -poin dalam klausul 8 pada standar ISO 27001:2013 sebagai berikut :

a) Perencanaan dan pengendalian operasional
b) Penilaian resiko keamanan informasi
c) Penanganan resiko keamanan informasi

6) Klausa 9 – Evaluasi Kinerja

   Poin -poin dalam klausul 9 pada standar ISO 27001:2013 sebagai berikut :

   a) Pemantauan, pengukuran, analisis, dan evaluasi
   b) Audit internal

7) Klausa 10 – Perbaikan

   Poin -poin dalam klausul 10 pada standar ISO 27001:2013 sebagai berikut :

   a) Ketidaksesuaian dan Tindakan korektif
   b) Perbaikan berkelanjutan

2. Membuat daftar pertanyaan berdasarkan standar ISO 27001:2013

   Membuat daftar pertanyaan dilakukan setelah menetapkan poin-poin yang akan dianalisis pada proses penelitian ini. Pembuatan daftar pertanyaan ini dilakukan berdasarkan identifikasi poin-poin setiap klausul standar ISO 27001:2013 yang dilakukan secara terarah agar mempermudah proses wawancara. Daftar pertanyaan dapat dilihat di lampiran 5.

3. Menganalisis hasil wawancara dengan bantuan *gap analysis*

   Penerapan analisis gap dalam ISO 27001:2013 adalah proses evaluasi yang bertujuan untuk mengidentifikasi perbedaan (gap) antara kebijakan, prosedur, dan kontrol keamanan informasi yang ada di organisasi saat ini dengan persyaratan yang ditetapkan dalam standar ISO 27001:2013. Hasil dari analisis gap adalah laporan rinci yang mencantumkan setiap perbedaan yang ditemukan antara praktik yang ada dan persyaratan ISO 27001:2013. Analisis gap dengan menggunakan pendekatan AS-IS dan TO-BE organisasi dapat secara sistematis mengidentifikasi kekurangan dalam sistem manajemen keamanan informasi mereka dan merencanakan serta

melaksanakan perubahan yang diperlukan untuk mencapai kepatuhan dengan standar ISO 27001:2013

3.3.4 Rekomendasi Berdasarkan ISO 27001:2013

Pada proses penulisan ini dilakukan analisis yang dilakukan dengan merinci kebutuhan untuk pengembangan dalam pemaksimalan proses keamanan teknologi informasi. Analisis ini mencakup usulan penyempurnaan melalui standar ISO 27001:2013. Tahapan rekomendasi ini dilakukan sebagai saran perbaikan dan pengembangan Divisi Sumber Daya Manusia dan Teknologi Informasi PERUMDA Tirta Satria Banyumas dengan memberikan rekomendasi terhadap objektif kontrol dan kontrol keamanan informasi yang telah dianalisis sebelumnya. Rekomendasi yang diberikan mengacu pada ISO 27001:2013.

3.3.5 Kesimpulan dan Saran

Memaparkan mengenai temuan yang ada setelah melakukan, menilai sejauh mana hasil penelitian sejalan dengan tujuan penelitian yang diharapkan sebelumnya serta memaparkan saran berupa identifikasi area yang perlu dikembangkan pada penelitian selanjutnya.