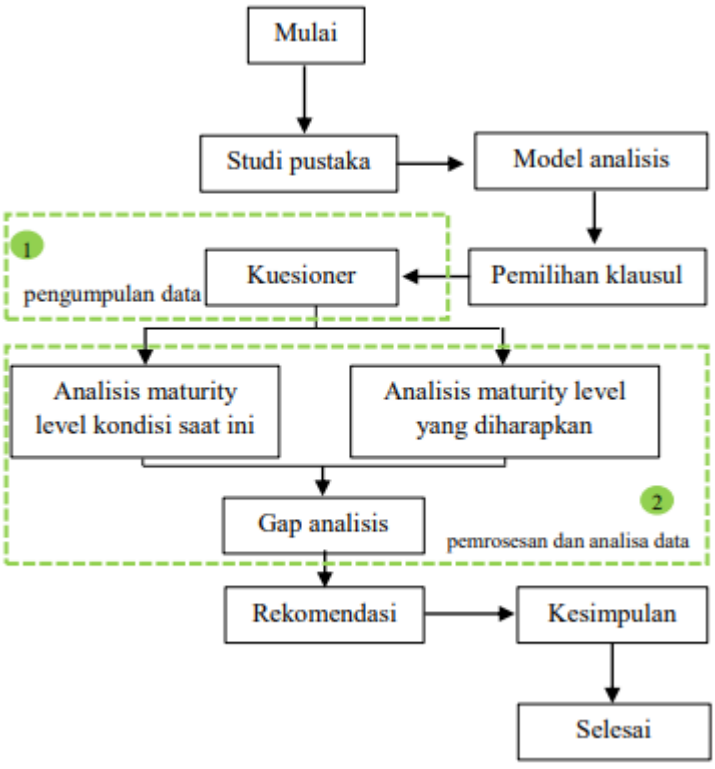
BAB III
ANALISA DAN PERANCANGAN

3.1 Desain Penelitian

Desain penelitian akan dibahas pada bagian ini dan bagaimana sebuah penelitian akan dilaksanakan, sehingga urutan langka-langka dalam penelitian ini dapat dipahami karena tersusun secara sistematis. Pada gambar 3.1 berikut akan dijelaskan langka-langka dalam penelitian ini.



Gambar 3.1 Desain Penelitian

3.2 Pengumpulan Data

Terdapat dua jenis data yang diperoleh oleh penulis, yaitu data primer dan juga data sekunder. Untuk pengertian kedua data tersebut yaitu, untuk data primer adalah sebuah data utama dalam penelitian ini, dan untuk data sekunder adalah sebuah data pendukung dalam penelitian. Data primer diperoleh dengan cara:

a. Observasi, khususnya melakukan pengamatan langsung terhadap cara PUSKOM menggunakan dan melaksanakan Siakad.
b. Wawancara, khusus menanyakan narasumber yang mengetahui dengan jelas Siakad untuk menanyakan pertanyaan-pertanyaan spesifik.
c. Kuesioner, dilakukan dengan memberikan kuesioner kepada 15 orang responden.

Selanjutnya, dilakukan perancangan kontrol yang dirancang untuk memastikan bahwa langkah manajerial bisa menjamin pencapaian target organisasi serta mencegah, mendeteksi, dan memperbaiki insiden yang tidak diinginkan. Tabel 3.1 menunjukkan klausul yang telah dipilih dan ditetapkan untuk penelitian ini, mengacu pada standar ISO 27002:2013.

Tabel 3.1 Tabel Klausul ISO 27002:2013

Klausul	Keterangan
9	Akses Kontrol
11	Keamanan Fisik dan Lingkungan
14	Akuisisi, Pengembangan dan Pengelolaan Sistem

Pada tahap pemberian kuesioner, sebelumnya penulis menyusun terlebih dahulu pertanyaan-pertanyaan yang sesuai dengan ISO 27002:2013 mengenai keamanan informasi. Pertanyaan-pertanyaan tersebut berkaitan dengan 40 kendali yang terdapat di dalam 8 objektif kontrol yang terbagi di dalam 3 klausul, yaitu klausul

9, 11, dan juga 14. Selain itu, penelitian ini mengumpulkan data sekunder dari jurnal, buku, studi literatur atau perpustakaan, dan halaman web.

Dalam penelitian ini dilakukan pemberian kuesioner kepada 15 responden yang menggunakan Siakad Universitas Labuhanbatu yaitu sebagai berikut:

Tabel 3.2 Daftar Responden

No	Keterangan	Jumlah
1	Kepala Puskom	1
2	Ka. BAAK Universitas Labuhanbatu	1
3	BAK Fakultas Sains Dan Teknologi	1
4	Ka. BAAK FKIP	1
5	Staf Keuangan	1
6	Staf Pascasarjana	1
7	BAAK Hukum	1
8	Dosen Universitas Labuhanbatu	4
9	Mahasiswa Universitas Labuhanbatu	4

Dalam penelitian ini perangkat lunak yang dipakai untuk menghasilkan nilai maturity level yaitu Microsoft Excel. Sebelum melakukan perhitungan terlebih dahulu semua jawaban dimasukkan ke dalam tabel, dari nilai masing-masing klausul nantinya akan dihitung rata-ratanya, dan nilai rata-rata ini akan mencerminkan tingkat kematangan, dan nantinya seluruh hasil *maturity level* dari setiap klausul akan dihitung rata-ratanya, dan nilai rata-rata ini akan mencerminkan tingkat kematangan dalam keamanan Siakad Universitas Labuhanbatu.

Pengkajian dan penafsiran data dari pemrosesan data dan hasil pemberian kuesioner untuk 15 pengguna Siakad Universitas Labuhanbatu dapat digunakan sebagai temuan penelitian. Berdasarkan penilaian tingkat kematangan, kita bisa mengidentifikasi kesenjangan yang dimiliki dan kemudian menetapkan nilai ekspektasi yang nantinya dijadikan rekomendasi untuk setiap objektif kontrol yang

memerlukan peningkatan. Dengan demikian, rekomendasi ini akan membantu untuk meningkatkan keamanan Siakad dengan cara yang lebih terarah dan efektif.

3.3 Pemrosesan dan Analisa Data

3.3.1 Melakukan Uji Kematangan

Dalam penelitian ini untuk memetakan posisi proses Siakad adalah dengan memberikan kuesioner kepada 15 pengguna Siakad Universitas Labuhanbatu. Berdasarkan hasil wawancara dan pemberian kuesioner, temuan untuk masing-masing *objective* digunakan untuk menetapkan *gap* yang ada dan menentukan tingkat kematangan yang diharapkan. Dari hasil yang telah didapatkan ini, bisa dibuat rekomendasi untuk tiap-tiap *control objective* yang mempunyai *gap maturity level* yang tentunya sesuai dengan detail *control objective*. Sebelum itu penelitian ini akan melalukan penilaian tingkat kematangan saat ini yang dilakukan melalui pemberian kuesioner, setiap pernyataan atau jawaban nantinya akan dinilai kelayakannya yang sesuai dengan memakai langkah-langkah evaluasi yang memenui standar penilaian tingkat kematangan. Standar penilaian yang dipakai mencakup *level non-eksisten* dengan nilai 0 (nol) sampai nilai 5 (lima) yaitu tingkat optimal. Jika dalam objective kontrol terdapat lebih dari satu pertanyaan, maka nilai yang diperoleh dari pertanyaan-pertanyaan tersebut dicari rata-ratanya untuk dijadikan tingkat kematangan pada *objective* kontrol tersebut. Contoh sebuah kerangka kerja yang bisa digunakan dalam penghitungan tingkat kematangan, bisa diperhatikan dalam Tabel 3.3:

Tabel 3.3 Contoh Untuk Kerangka Kerja Perhitungan *Maturity Level*

Kausul : 9 Kontrol Akses								
Kategori Keamanan Utama : 9.1Persyaratan bisnis untuk kontrol akses								
Kontrol Keamanan : 9.1.1Kebijakan kontrol akses								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan secara jelas dan komprehensif tentang bagaimana akses fisik dan logis ke sistem informasi dan aset-aset yang sensitif diatur dan dikelola.							

[Sumber: D. P. Haqqi, K. Ghozali, dan R. V. H. Ginardi, "Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM pada PDAM Surya Sembada Kota Surabaya," J. Teknik ITS, vol. 11, no. 2, pp. 149–156, 2022, doi: 10.12962/j23373539.v11i1.82095.]

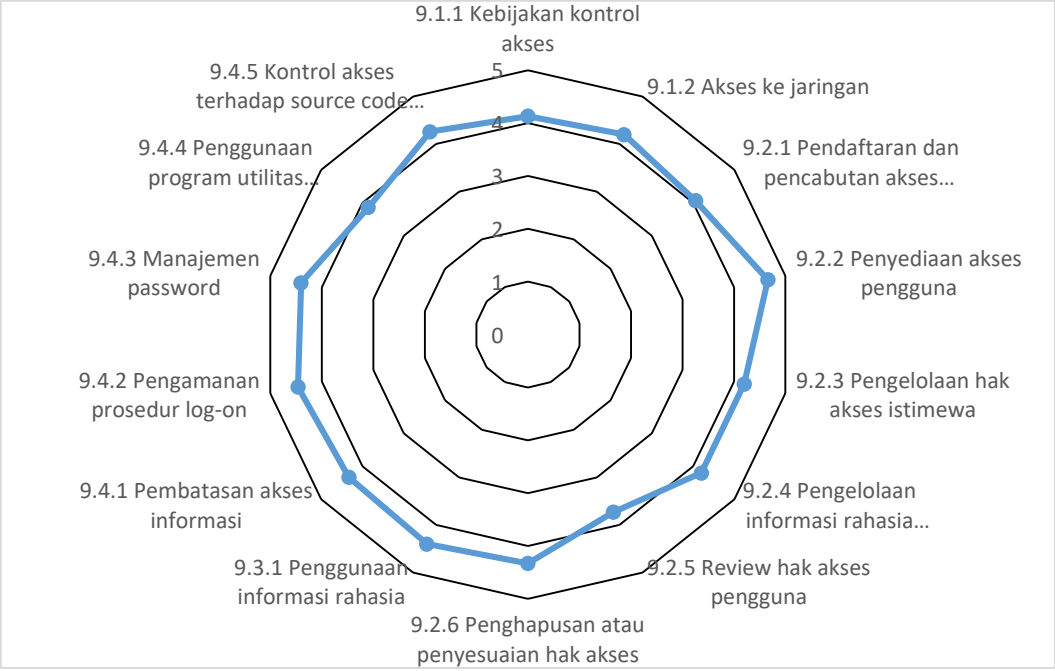
Setelah mengetahui level kematangan untuk masing-masing kontrol keamanan ISO 27002:2013, maka selanjutnya dapat dicari nilai *maturity level* untuk objektif kontrol, caranya yaitu dengan menambahkan seluruh nilai pada tiap-tiap kontrol keamanan dan dicari nilai-rata-ratanya, selanjutnya, hasil rata-rata ini akan menentukan tingkat kematangan (*maturity level*) untuk objektif kontrol tersebut, dan selanjutnya, untuk menghitung nilai tingkat kematangan pada klausul maka caranya dengan menambahkan *nilai maturity* level tiap-tiap objektif kontrol dan selanjutnya, dicari rata-ratanya, nilai tingkat kematangan akan didasarkan pada rata-rata ini dan nantinya akan menjadi tingkat kematangan klausul tersebut.Contoh untuk mendapatkan *maturity level* ISO 27002:2013 sebagai berikut:

Tabel 3.4 Contoh Untuk Tabel Penentuan *Maturity Level* ISO 27002:2013

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
9. Kontrol Akses	9.1. Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses	4,13	4,16
		9.1.2 Akses ke jaringan	4,2	
	9.2. Manajemen akses pengguna	9.2.1 Pendaftaran dan pencabutan akses pengguna	4,06	4,19
		9.2.2 Penyediaan akses pengguna	4,66	
		9.2.3 Pengelolaan hak akses istimewa	4,2	
		9.2.4 Pengelolaan informasi rahasia pengguna	4,2	
		9.2.5 *Review* hak akses pengguna	3,73	
		9.2.6 Penghapusan atau penyesuaian hak akses	4,33	
	9.3. Tanggungjawab pengguna	9.3.1 Penggunaan informasi rahasia	4,4	4,4
	9.4. Kontrol akses sistem dan aplikasi	9.4.1 Pembatasan akses informasi	4,33	4,26

		9.4.2 Pengamanan prosedur *log-on*	4,46	
		9.4.3 Manajemen *password*	4,4	
		9.4.4 Penggunaan program utilitas dengan hak akses level tinggi	3,86	
		9.4.5 Kontrol akses terhadap *source code* program	4,26	
***Maturity level* Klausul 9**				**4,25**

Berikut akan diberikan gambaran melalui diagram jaring, mengenai nilai-nilai maturity level pada tiap-tiap kontrol keamanan pada klausul 9 terdapat pada Gambar 3.2.



Gambar 3.2 Contoh Diagram Jaring Nilai *Maturity Level* Klausul 9

3.3.2 *Gap* Analisis

Pada tahap selanjutnya mencari *gap* analisis, *gap* analisis ini bermanfaat untuk membandingkan kinerja yang saat ini diperoleh dengan kinerja yang diharapkan. Selain itu dengan adanya gap analisis ini dapat menjadi rujukan untuk tindakan-tindakan apa saja yang harus dilakukan supaya kesenjangan dapat berkurang dan akhirnya dapat mencapai target kinerja masa depan. Selain itu, dengan adanya analisis ini maka suatu organisasi dapat memperkirakan biaya, waktu dan sumber daya yang tepat karena tindakan-tindakan yang perlu diperbaiki sudah diketahui. Detailnya diperlihatkan dalam Tabel 3.5 berikut ini:

Tabel 3.5 Contoh Untuk Hasil Perhitungan *Gap* Analisis

Klausul	**Keterangan**	***Maturity Level***		***Gap***
		Kondisi saat ini	**Kondisi yang diharapkan**	
9	Kontrol Akses	4,25	5	0,75
11	Keamanan Fisik dan Lingkungan			
14	Akuisisi, Pengembangan dan Pengelolaan Sistem			
Rata-rata				

[Sumber: A. Rosadi dan B. A. Wardijono, "Analisis Tingkat Keamanan Sistem Pembayaran Pajak dan Retribusi Daerah Berdasarkan Standar ISO/IEC 27002:2013 Menggunakan SSE-CCM," International Research Journal of Advanced Engineering Sciences, vol. 6, no. 1, pp. 205–211, 2021. Tersedia online: http://irjaes.com/wp-content/uploads/2021/02/IRJAES-V6N1P175Y21.pdf]

3.4 Melakukan Dokumentasi Data dan Bukti

Pada tahap ini selanjutnya akan dilaksanakan pemeriksaan tentang data-data dan bukti-bukti lainnya mengenai keamanan yang sudah diterapkan pada siakad universitas Labuhanbatu yang sudah sesuai dengan standar pedoman ISO 27002:2013. Untuk contoh tabel model jenis pemeriksaan realitas dan pembuktiannya bisa diperhatikan dalam Tabel 3.6:

Tabel 3.6 Contoh Untuk Pendokumentasian Fakta dan Bukti

Klausul		**:**	**9**	**Kontrol Akses**
Kategori Keamanan Utama		**:**	**9.1**	**Persyaratan bisnis untuk kontrol akses**
Kontrol Keamanan		**:**	**9.1.1**	**Kebijakan untuk kontrol akses**
No	**Pernyataan**	**Hasil Pemeriksaan**		
1	Telah ditetapkan kebijakan secara jelas dan komprehensif tentang bagaimana akses fisik dan logis ke sistem informasi dan aset-aset yang sensitif diatur dan dikelola.	Bukti:		

[Sumber: I. R. Pajar, "Analisis Tingkat Keamanan Aplikasi SIMAK Menggunakan Standar ISO/IEC 27002:2013 (Studi Kasus: UPTTIK Universitas Siliwangi)," Jurnal Serambi Engineering, vol. 6, no. 2, pp. 1797–1805, 2021. doi: 10.32672/jse.v6i2.2879.]

3.5 Rekomendasi

Pada proses pemberian rekomendasi ini, sebelumnya telah dilakukan pemeriksaan terlebih dahulu mengenai kebijakan, profil organisasi dengan cara melakukan wawancara dan juga pemberian kuesioner kepada pengguna siakad. Dari hasil wawancara dan juga pemberian kuesioner tersebut akan didapatkan bukti yang terikat dengan sistem yang tengah berlangsung saat ini. Dalam proses pemeriksaan ini akan ditemukan bahwa beberapa proses telah dilaksanakan dengan baik, namun terkadang terdapat hasil temuan yang harus ditingkatkan. Dari temuan yang harus ditingkatkan atau diperbaiki tersebut akan lebih diteliti dengan melakukan analisis penyebab dan dampak dari temuan tersebut, sehingga nantinya dapat diberikan rekomendasi kepada universitas supaya penerapan standar ISO 27002:2013 dapat diterapkan secara lebih efektif dan terus meningkat di masa mendatang.