BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil Penetapan Klausul

Selanjutnya ketika telah dilaksanakan pengamatan maka hasil yang didapatkan yaitu menetapkan bahwa analisis mencakup keamanan sistem informasi dan standar yang diterapkan adalah ISO 27002:2013. Dari langkah identifikasi ini, hasilnya mencakup pemetaan klausul, objektif kontrol, dan kontrol keamanan untuk nantinya dilakukan pemeriksaan. Klausul yang dipakai adalah klausul 9 tentang Akses Konrol, klausul 11 tentang Keamanan Fisik dan Lingkungan, dan klausul 14 tentang Akuisisi, Pengembangan, dan Pengelolaan Sistem.

4.2 Hasil Pengumpulan Data

Segmen ini memuat pencatatan informasi atau bukti terkini sehubungan dengan penemuan-penemuan yang diperoleh selama penilaian dan juga wawancara dengan Admin Siakad Universitas Labuhanbatu, bukti tersebut bisa berupa gambar, keterangan informasi atau video. Hasil pemeriksaan bisa diperhatikan dalam Tabel 4.1 dan informasi lebih lanjut dapat ditemukan di lampiran.

Tabel 4.1 Hasil Pemeriksaan Pernyataan

Klausul : 9. Kontrol Akses		
Kategori Keamanan Utama : 9.1 Persyaratan bisnis untuk kontrol akses		
Kontrol Keamanan : 9.1.1 Kebijakan kontrol akses		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan secara jelas dan komprehensif tentang bagaimana akses fisik dan logis ke sistem informasi dan	Kebijakan kontrol akses telah dilakukan dengan baik. Bukti: a. Pintu memiliki kunci b. Ruangan tersendiri

	aset-aset yang sensitif diatur dan dikelola.	c. Tidak boleh keluar masuk sembarangan d. Ada Id Card tersendiri e. Hanya bagian IT yang masuk f. Jika terdapat masalah pada siakad hanya melapor ke admin siakad g. Password/kata sandi hanya dapat diriset oleh admin
Kontrol Keamanan : 9.1.2 Akses ke jaringan		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang mengatur secara jelas pengendalian dan pengawasan akses ke jaringan, termasuk kebijakan penggunaan kata sandi yang kuat, dan pemantauan aktivitas jaringan yang mencurigakan.	Akses ke jaringan telah dikendalikan dengan baik. Bukti: a. Password/kata sandi hanya dapat diriset oleh admin b. User dan pasword diberikan kepada per individu sesuai dengan fungsi, terdapat user Admin, user mahasiswa, user keuangan, user Kepala keuangan, user Operator, user Kaprodi, user Dekan, user PMB, dan user Dosen
Kategori Keamanan Utama : 9.2 Manajemen akses pengguna		
Kontrol Keamanan : 9.2.1 Pendaftaran dan pencabutan akses pengguna		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang jelas untuk memvalidasi identitas pengguna sebelum memberikan akses ke sistem informasi, serta untuk mencabut akses pengguna yang tidak lagi memenuhi persyaratan keamanan atau kebutuhan bisnis.	Pendaftaran dan pencabutan akses pengguna telah dikendalikan dengan baik. Bukti: a. Akun siakad diberikan berdasarkan jabatan fungsionalnya b. Pembagian user dan pasword diberikan per individu sesuai dengan fungsi, terdapat user Admin, user mahasiswa, user keuangan, user Kepala keuangan, user Operator, user Kaprodi, user Dekan, user PMB, dan user Dosen. Seseorang yang ingin menjadi mahasiswa ULB harus melakukan pendaftaran terlebih dahulu seperti membawa ijazah, kk, ktp, membayar beberapa biaya dan lain-lain, setelah semua persyaratan lengkap baru secara resmi seseorang tersebut bisa masuk menjadi bagaian dari mahasiswa ULB dan

		mendapatkan akun di siakad ULB, itu untuk user mahasiswa dan untuk user lainnya juga memiliki persyaratan yang berbeda-beda sebelum mendapatkan akun di siakad harus memenuhi persyaratan-persyaratan yang ditentukan. c. Adanya penghapusan akun ketika dibutuhkan
Kontrol Keamanan : 9.2.2 Penyediaan akses pengguna		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa akses pengguna ke Sistem Informasi Akademik (SIAKAD) diberikan sesuai dengan peran, tanggung jawab, dan kebutuhan bisnis masing-masing pengguna, serta terdapat mekanisme untuk memastikan bahwa hak akses tersebut dikelola dengan baik dan sesuai dengan kebijakan keamanan informasi yang berlaku.	Penyediaan akses pengguna telah dikendalikan dengan baik. Bukti: a. Kebijakan atau problem pada akun siakad hanya dikelola oleh Admin b. Pembagian user dan pasword diberikan per individu sesuai dengan fungsi, terdapat user Admin, user mahasiswa, user keuangan, user Kepala keuangan, user Operator, user Kaprodi, user Dekan, user PMB, dan user Dosen. Seseorang yang ingin menjadi mahasiswa ULB harus melakukan pendaftaran terlebih dahulu seperti membawa ijazah, kk, ktp, membayar beberapa biaya dan lain-lain, setelah semua persyaratan lengkap baru secara resmi seseorang tersebut bisa masuk menjadi bagaian dari mahasiswa ULB dan mendapatkan akun di siakad ULB, itu untuk user mahasiswa dan untuk user lainnya juga memiliki persyaratan yang berbeda-beda sebelum mendapatkan akun di siakad harus memenuhi persyaratan-persyaratan yang ditentukan. c. Admin hanya 1 d. Jika siakad bermasalah hanya melapor ke admin
Kontrol Keamanan : 9.2.3 Pengelolaan hak akses istimewa		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan untuk mengelola dan memantau penggunaan hak	Pengelolaan hak akses istimewa telah dilakukan dengan baik. Bukti:

	akses istimewa pada SIAKAD, termasuk penetapan peran dan tanggung jawab yang jelas bagi pemegang hak akses istimewa serta mekanisme untuk memastikan bahwa hak akses tersebut tidak disalahgunakan atau dieksploitasi untuk tujuan yang tidak sah.	a. Pembagian user dan password per individu b. Akun siakad berdasarkan jabatan fungsionalnya, dan sebelum diberi jabatan harus memenuhi persyaratan-persyaratan yang telah ditentukan oleh ULB c. Admin hanya 1 d. Jika terdapat masalah pada siakad maka user-user siakad dapat melapor ke admin e. Admin dapat mereset kata sandi/password yang ada di siakad
Kontrol Keamanan : 9.2.4 Pengelolaan informasi rahasia pengguna		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa informasi rahasia pengguna (seperti kata sandi atau informasi identifikasi pribadi) yang disimpan dalam SIAKAD dikelola secara aman, termasuk penggunaan metode enkripsi dan tindakan perlindungan lainnya untuk mencegah akses yang tidak sah atau pengungkapan informasi tersebut.	Pengelolaan informasi rahasia pengguna dikendalikan dengan baik. Bukti: a. Memiliki akun siakad masing-masing. b. Masuk akun harus menggunakan password dan username c. Jika password rusak melapor ke admin
Kontrol Keamanan : 9.2.5 Review hak akses pengguna		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan untuk melakukan review secara periodik terhadap hak akses pengguna pada SIAKAD, termasuk pemeriksaan dan evaluasi terhadap kebutuhan akses pengguna, penghapusan hak akses yang tidak lagi diperlukan, serta pemantauan aktivitas pengguna guna mendeteksi potensi penyalahgunaan atau pelanggaran keamanan.	Review hak akses pengguna telah dikendalikan dengan baik. Bukti: a. Penghapusan hak akses yang tidak lagi diperlukan b. Terdapat kontrol akses
Kontrol Keamanan : 9.2.6 Penghapusan atau penyesuaian hak akses		

No	Pernyataan	Hasil Pemeriksaan
1	Telah ditetapkan kebijakan yang memastikan bahwa hak akses pengguna pada SIAKAD dihapus atau disesuaikan secara tepat waktu ketika pengguna tersebut tidak lagi memerlukan akses, telah berubah peran atau tanggung jawabnya, atau telah meninggalkan organisasi.	Penghapusan atau penyesuaian hak akses telah dilakukan dengan baik. Bukti: a. Adanya penghapusan akun ketika dibutuhkan b. Adanya reset password ketika diperlukan.
Kategori Keamanan Utama : 9.3 Tanggungjawab pengguna		
Kontrol Keamanan : 9.3.1 Penggunaan informasi rahasia		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa informasi rahasia yang disimpan dalam SIAKAD, seperti data pribadi mahasiswa atau hasil penelitian, digunakan dengan benar sesuai dengan kebutuhan bisnis.	Pengelolaan penggunaan informasi rahasia telah dikendalikan dengan baik. Bukti: a. Pengumpulan data pribadi seperti photocopy ijazah, photocopy KTP dan KK diminta sebagai syarat pendaftaran masuk ULB yang telah diinformasikan sebelumnya kepada para calon mahasiswa b. Data pribadi mahasiswa yang ada di siakad seperti nama, daftar pembayaran mahasiswa, NIK, NISN, tempat lahir, tanggal lahir, dilindungi dengan password dan username, seseorang yang akan masuk ke sebuah akun siakad harus login terlebih dahulu dengan password dan username, sehingga data pribadi tetap aman dan tidak sembarangan digunakan oleh orang lain c. Kebijakan atau problem pada akun siakad hanya dikelola oleh admin d. Admin hanya 1
Kategori Keamanan Utama : 9.4 Kontrol akses sistem dan aplikasi		
Kontrol Keamanan : 9.4.1 Pembatasan akses informasi		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan dan prosedur yang memastikan bahwa akses ke informasi sensitif atau	Pembatasan akses informasi telah dikendalikan dengan baik. Bukti:

	rahasia dalam SIAKAD dibatasi hanya kepada individu yang membutuhkan informasi tersebut untuk menjalankan tugas-tugas mereka.	a. Pembagian user dan password diberikan per individu yang telah memenuhi persyaratan sebelumnya b. Akun siakad diberikan berdasarkan jabatan fungsionalnya. Terdapat user Admin, user mahasiswa, user keuangan, user Kepala keuangan, user Operator, user Kaprodi, user Dekan, user PMB, dan user Dosen c. Admin hanya 1 dan Kebijakan atau problem pada akun siakad hanya dikelola oleh admin
Kontrol Keamanan : 9.4.2 Pengamanan prosedur log-on		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa kebijakan log-on ke dalam SIAKAD diamanatkan dengan menggunakan mekanisme autentikasi yang kuat, seperti kata sandi yang kompleks atau autentikasi multi-faktor, serta langkah-langkah keamanan tambahan, telah diimplementasikan untuk mengurangi risiko akses yang tidak sah.	Pengamanan prosedur log-on telah dikendalikan dengan baik. Bukti: a. Password yang dikunci oleh admin siakad b. Saat akan log-on ke siakad maka user harus memasukkan terlebih dahulu username dan password c. Agar bisa mendapatkan akun siakad, maka seseorang harus memenuhi persyaratan yang telah ditentukan terlebih dahulu, jadi tidak bisa sembarang orang memiliki akun
Kontrol Keamanan : 9.4.3 Manajemen password		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa manajemen password yang kuat diterapkan pada SIAKAD, termasuk penggunaan teknik enkripsi yang kuat untuk melindungi kata sandi yang disimpan, dan juga keamanan tambahan lainnya.	Manajemen password dikendalikan dengan baik. Bukti: a. Password yang dienkripsi b. Admin yang bisa mereset password seluruh akun siakad, dan admin hanya ada 1
Kontrol Keamanan : 9.4.4 Penggunaan program utilitas dengan hak akses level tinggi		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa penggunaan program utilitas	Penggunaan program utilitas dengan hak akses level tinggi telah dilakukan dengan baik.

	dengan hak akses level tinggi pada SIAKAD dibatasi dan dipantau secara ketat.	Bukti: a. User pada siakad berbeda-beda dan memiliki fungsi berdasarkan level akun masing-masing. Terdapat user Admin, user mahasiswa, user keuangan, user Kepala keuangan, user Operator, user Kaprodi, user Dekan, user PMB, dan user Dosen
Kontrol Keamanan : 9.4.5 Kontrol akses terhadap source code program		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa akses terhadap source code program dalam pengembangan, penyesuaian, atau pemeliharaan SIAKAD dibatasi hanya kepada individu yang memerlukan akses tersebut untuk kepentingan bisnis.	Kontrol akses terhadap source code program telah dilakukan dengan baik. Bukti: a. Pengembangan siakad hanya dikelola sesuai tim IT dengan SK yang ditugaskan
Klausul : 11 Keamanan fisik dan lingkungan		
Kategori Keamanan Utama : 11.1 Area aman		
Kontrol Keamanan : 11.1.1 Pembatas keamanan fisik		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa fasilitas fisik yang digunakan untuk menyimpan atau mengelola infrastruktur SIAKAD dilindungi secara kuat dengan langkah-langkah keamanan fisik, seperti pengamanan pintu, dan pengendalian akses fisik ke ruang server atau pusat data.	Pembatas keamanan fisik telah dikendalikan dengan baik. Bukti: a. Pintu memiliki kunci b. Ruangan tersendiri c. Ada Id Card tersendiri d. Tidak boleh keluar masuk sembarangan e. Hanya bagian IT yang masuk
Kontrol Keamanan : 11.1.2 Kontrol entri fisik		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa kontrol entri fisik diterapkan secara efektif untuk mengontrol akses ke ruang server atau pusat data yang menyimpan infrastruktur	Kontrol entri fisik telah dikendalikan dengan baik. Bukti: a. Hanya petugas IT yang boleh keluar masuk untuk kontrol akses

	SIAKAD, dan mekanisme otentikasi, seperti kartu akses atau biometrik, digunakan untuk memverifikasi identitas dan hak akses pengguna sebelum memasuki ruang tersebut.	
Kontrol Keamanan : 11.1.3 Keamanan ruang dan fasilitas kantor		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa keamanan ruang dan fasilitas kantor yang digunakan untuk operasi SIAKAD dilindungi secara kuat, termasuk pengaturan akses fisik ke ruang kerja, dan pengamanan perangkat keras komputer yang sensitif, untuk mencegah akses yang tidak sah atau pencurian informasi	Keamanan ruang dan fasilitas kantor telah dilakukan dengan baik. Bukti: a. Pintu memiliki kunci b. Ruangan tersendiri c. Ada Id Card tersendiri d. Tidak boleh keluar masuk sembarangan e. Hanya bagian IT yang masuk f. Hanya petugas IT yang boleh keluar masuk untuk kontrol akses g. Memakai AC karena server tidak boleh panas h. Terdapat UPS untuk server
Kontrol Keamanan : 11.1.4 Perlindungan dari ancaman luar (eksternal)		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa langkah-langkah perlindungan yang tepat telah diterapkan untuk mengurangi risiko dari ancaman luar (eksternal), seperti serangan siber, pencurian data, atau gangguan layanan, yang dapat memengaruhi operasi atau keamanan SIAKAD.	Perlindungan dari ancaman luar (eksternal) telah dikendalikan dengan baik. Bukti: a. Melakukan backup data b. Melakukan akses kontrol
Kategori Keamanan Utama : 11.2 Peralatan		
Kontrol Keamanan : 11.2.1 Penempatan dan perlindungan peralatan		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang digunakan dalam operasi SIAKAD ditempatkan dan dilindungi	Penempatan dan perlindungan peralatan telah dikendalikan dengan baik. Bukti:

	secara aman, termasuk langkah-langkah untuk mencegah kerusakan fisik, pencurian, atau gangguan yang dapat mempengaruhi ketersediaan atau integritas sistem.	a. Pintu memiliki kunci agar dapat menjaga barang-barang yang ada di dalamnya b. Memiliki ruangan tersendiri c. Hanya bagian IT yang boleh keluar masuk untuk kontrol akses d. Ruangan memiliki AC karena server tidak boleh panas
Kontrol Keamanan : 11.2.2 Utilitas pendukung		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa utilitas pendukung yang digunakan dalam operasi SIAKAD, seperti listrik, pendingin udara, atau saluran komunikasi, diidentifikasi, dan dilindungi dengan baik untuk memastikan ketersediaan dan keandalan operasi sistem.	Utilitas pendukung telah dikendalikan dengan baik. Bukti: a. Terdapat UPS untuk server b. Ruangan terdapat AC untuk menjaga server agar tidak panas
Kontrol Keamanan : 11.2.3 Keamanan kabel		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa kabel yang digunakan dalam infrastruktur SIAKAD, termasuk kabel jaringan dan kabel listrik, dipasang dan dilindungi dengan aman untuk mencegah kerusakan fisik, manipulasi yang tidak sah, atau akses yang tidak sah yang dapat mempengaruhi integritas atau ketersediaan sistem.	Keamanan kabel telah dikendalikan dengan baik. Bukti: a. Memiliki ruangan tersendiri b. Pada ruangan tersebut tidak boleh keluar masuk sembarangan c. Hanya petugas IT yang boleh keluar masuk
Kontrol Keamanan : 11.2.4 Perawatan asset		
No	**Pernyataan**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa asset yang digunakan dalam operasi SIAKAD, termasuk perangkat keras, perangkat lunak, dan data, dikelola dan dipelihara secara teratur	Perawatan asset telah dilakukan dengan baik. Bukti: a. Melakukan backup data, terdapat backup data mingguan dan backup data bulanan b. Melakukan kontrol akses

	untuk memastikan ketersediaan, keandalan, dan integritasnya selama siklus hidup penggunaannya.	c. Terdapat UPS untuk server d. Terdapat AC untuk menjaga server agar tidak panas

4.3 Hasil Pemrosesan Data Uji Kematangan

Berlandaskan analisa, pemeriksaan, dan pengumpulan bukti, maka didapatkan tingkat kematangan untuk tiap-tiap kontrol. Hasil dari menghitung tingkat kematangan yang diperoleh dari pemeriksaan keamanan dapat dilihat rinciannya sebagai berikut:

a. Maturity Level Klausul 9

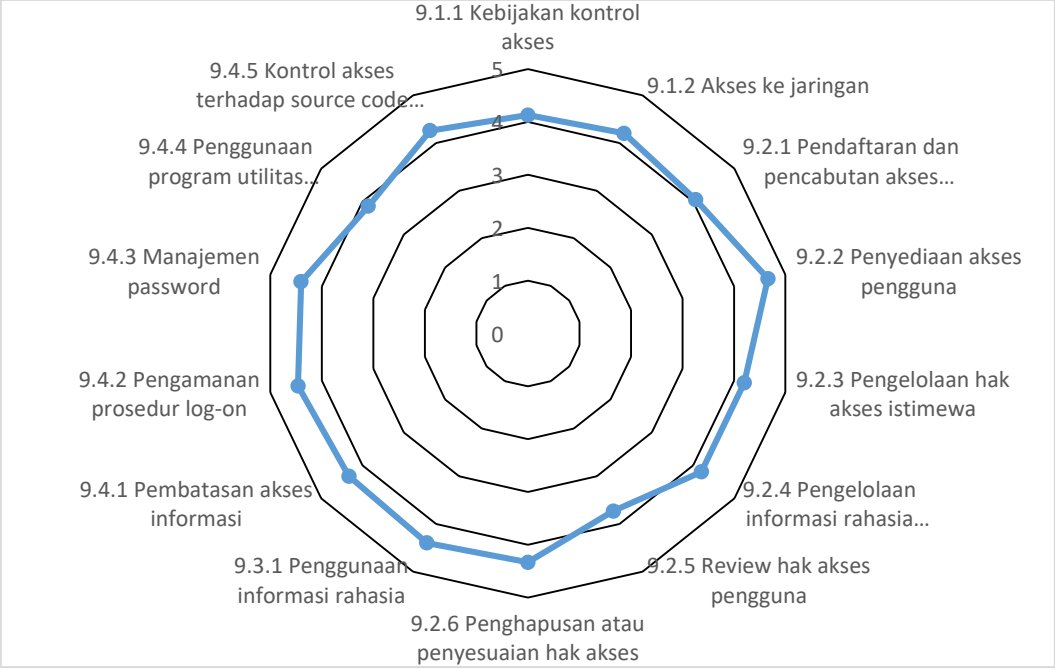
Hasil perhitungan tingkat kematangan klausul 9 sehubungan dengan kontrol akses adalah 4,25. Sistem sudah menerapkan kontrol akses dengan cukup baik terdapat Kebijakan kontrol akses, terdapat *password* dan *user* yang harus diisikan sebelum masuk ke Siakad, akun Siakad diberikan berdasarkan jabatan fungsionalnya, Jika Siakad bermasalah hanya melapor ke admin. Untuk hasil perhitungan tingkat kematangan pada klausul 9 mengenai kontrol akses bisa diperhatikan dalam tabel 4.2 dan untuk bentuk grafis pada gambar 4.1.

Tabel 4.2 Hasil Tingkat Kematangan Klausul 9

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**



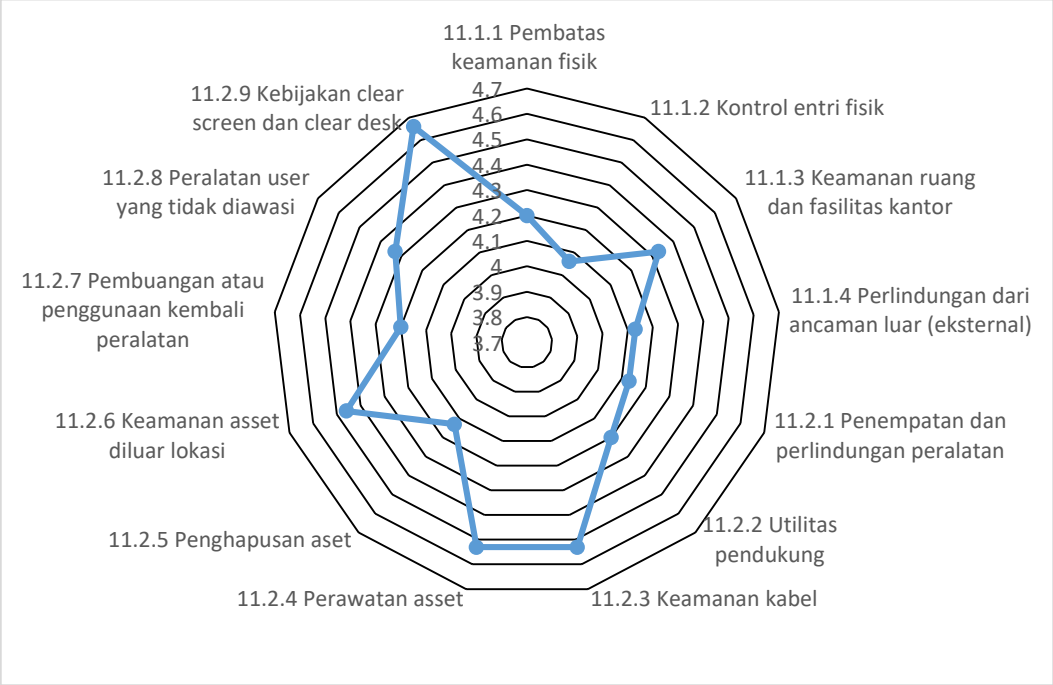
Gambar 4.1 Hasil Tingkat Kematangan Klausul 9

b. *Maturity Level* Klausul 11

Hasil dari proses tingkat kematangan klausul 11 (Keamanan fisik dan lingkungan) adalah 4,26. Sistem sudah menerapkan keamanan fisik dan lingkungan dengan cukup baik pintu memiliki kunci, berada pada ruangan tersendiri, terdapat *Id Card* tersendiri, tidak boleh keluar masuk sembarangan, hanya bagian IT yang boleh keluar masuk, ruangan memakai AC karena server tidak boleh panas, terdapat UPS untuk server. Hasil perhitungan tingkat kematangan klausul 11 bisa diperhatikan dalam tabel 4.3 dan dalam grafik dapat diperhatikan dalam gambar 4.2.

Tabel 4.3 Hasil Tingkat Kematangan Klausul 11

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11. Keamanan fisik dan lingkungan	11.1 Area aman	11.1.1 Pembatas keamanan fisik	4,2	4,18
		11.1.2 Kontrol entri fisik	4,06	
		11.1.3 Keamanan ruang dan fasilitas kantor	4,33	
		11.1.4 Perlindungan dari ancaman luar (eksternal)	4,13	
	11.2 Peralatan	11.2.1 Penempatan dan perlindungan peralatan	4,13	4,35
		11.2.2 Utilitas pendukung	4,2	
		11.2.3 Keamanan kabel	4,53	
		11.2.4 Perawatan asset	4,53	
		11.2.5 Penghapusan aset	4,13	
		11.2.6 Keamanan asset diluar lokasi	4,46	
		11.2.7 Pembuangan atau penggunaan kembali peralatan	4,2	
		11.2.8 Peralatan *user* yang tidak diawasi	4,33	
		11.2.9 Kebijakan *clear screen* dan *clear desk*	4,66	
***Marturity level* Klausul 11**				**4,26**



Gambar 4.2 Hasil Tingkat Kematangan Klausul 11

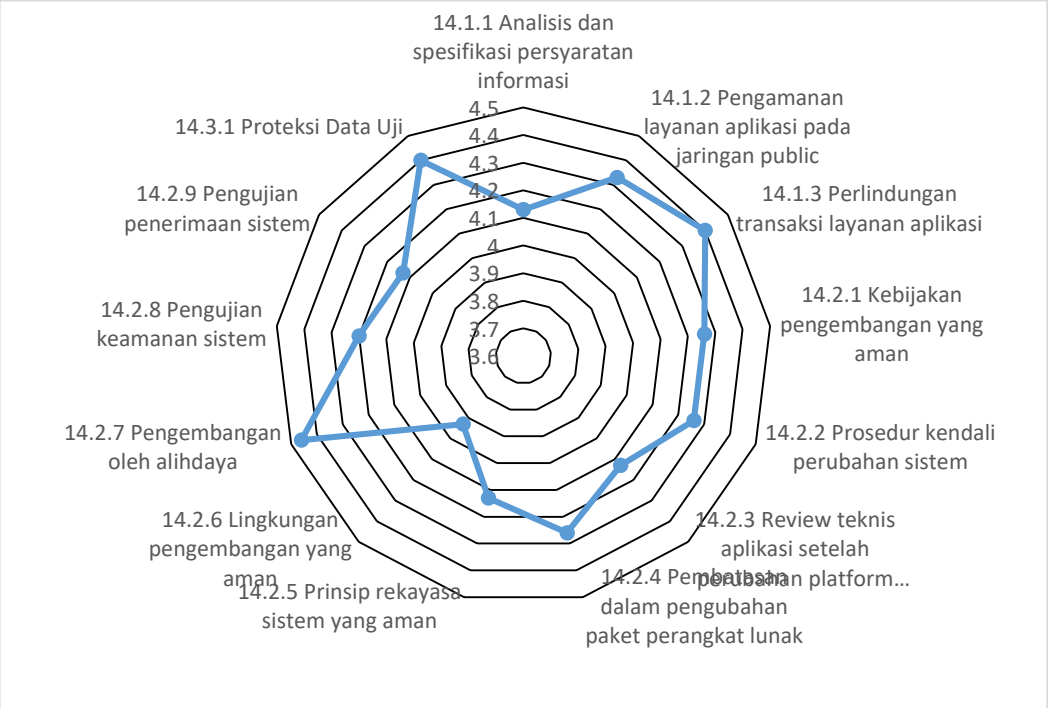
c. *Maturity Level* Klausul 14

Tingkat kematangan klausul 14 menunjukkan nilai 4,29 berdasarkan hasil perhitungan, hal ini memperlihatkan bahwa pada klausul 14 sistem telah sampai pada level *Managed* and *Measurable*, yaitu sistem saat ini di antaranya telah menerapkan kontrol akses, backup data dan lain-lain, untuk perhitungannya dapat dilihat pada tabel 4.4.

Tabel 4.4 Hasil Tingkat Kematangan Klausul 14

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
14 Akuisisi, Pengembangan dan Pengelolaan Sistem	14.1 Persyaratan keamanan sistem informasi	14.1.1 Analisis dan spesifikasi persyaratan informasi	4,13	4,28
		14.1.2 Pengamanan layanan aplikasi pada jaringan public	4,33	
		14.1.3 Perlindungan transaksi layanan aplikasi	4,4	
	14.2 Keamanan dalam proses pengembangan dan dukungan	14.2.1 Kebijakan pengembangan yang aman	4,26	4,19
		14.2.2 Prosedur kendali perubahan sistem	4,26	
		14.2.3 Review teknis aplikasi setelah perubahan platform operasi	4,13	
		14.2.4 Pembatasan dalam pengubahan paket perangkat lunak	4,26	
		14.2.5 Prinsip rekayasa sistem yang aman	4,13	
		14.2.6 Lingkungan	3,93	

		pengembangan yang aman		
		14.2.7 Pengembangan oleh alihdaya	4,46	
		14.2.8 Pengujian keamanan sistem	4,2	
		14.2.9 Pengujian penerimaan sistem	4,13	
	14.3 Data Uji	14.3.1 Proteksi Data Uji	4,4	4,4
***Maturity Level* Kausul 14**				**4,29**



Gambar 4.3 Hasil Tingkat Kematangan Klausul 14

4.4 *Gap* Analisis

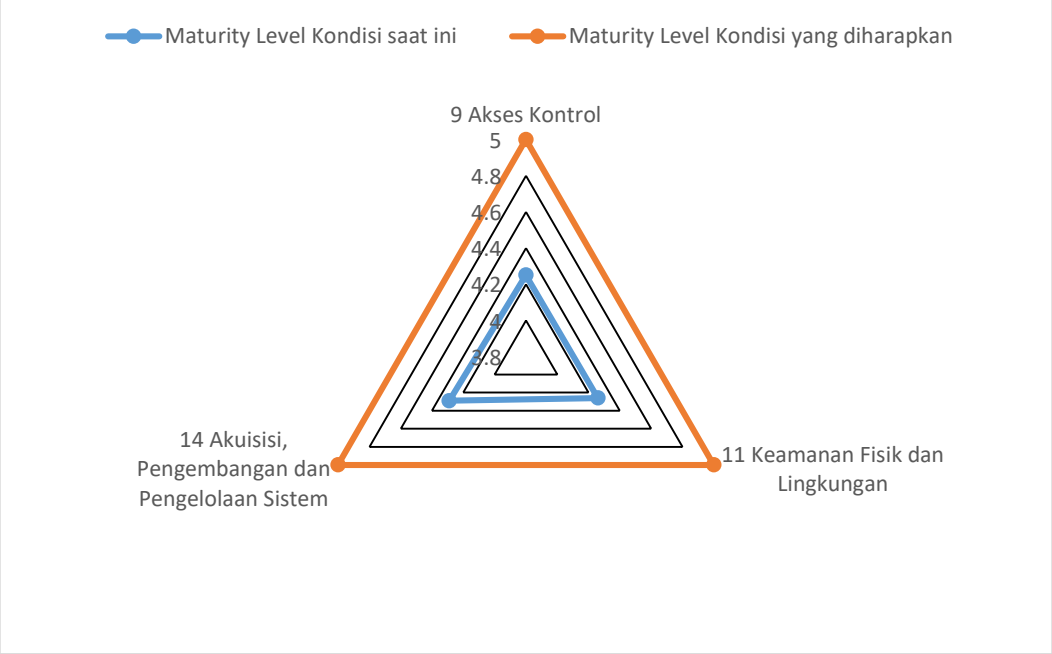
Berlandaskan perhitungan untuk memeperoleh tingkat kematangan tersebut, keamanan sistem informasi dari Siakad Universitas Labuhanbatu pada waktu sekarang memiliki nilai 4,26, nilai tersebut adalah nilai rata-rata tingkat kematangan 3 klausul yang telah dipilih dan nilai tersebut sudah termasuk berada pada tingkat *Managed* and *Measurable,* menunjukkan bahwa Siakad dikendalikan secara kuantitatif, ini berarti peningkatan kualitas dicapai melalui pemantauan setiap proses secara berkala. Perhitungan *gap* atau selisih untuk analisis keamanan sistem informasi bisa dilihat rincian tersebut dalam tabel 4.5.

Tabel 4.5 *Gap* Analisis

Klausul	**Keterangan**	***Maturity Level***		**Gap**
		Kondisi saat ini	**Kondisi yang diharapkan**	
9	Akses Kontrol	4,25	5	0,75
11	Keamanan Fisik dan Lingkungan	4,26	5	0,74
14	Akuisisi, Pengembangan dan Pengelolaan Sistem	4,29	5	0,71
Rata-rata				**0,73**

Pada tampilan tabel 4.5, terlihat selisih antara keadaan saat ini dengan kondisi yang diharapkan, untuk klausul 9 bernilai *gap* 0,75, klausul 11 bernilai *gap* 0,74, klausul 14 bernilai *gap* 0,71. Dari hasil yang didapatkan kemudian dicari nilai rata-ratanya untuk menghitung nilai *gap* atau kesenjangan dari 3 klausul tersebut, maka didapatkan nilai 0,73, artinya suatu organisasi sudah mencapai level 4 (*Managed* and *Measurable*), menunjukkan bahwa Siakad dikendalikan secara kuantitatif, ini berarti peningkatan kualitas dicapai melalui pemantauan setiap proses secara berkala. Namun, meskipun sudah berada pada tingkat 4, masih ada beberapa alasan

mengapa rekomendasi tetap diperlukan yaitu karena ancaman keamanan informasi terus berkembang, teknologi dan sistem informasi juga terus berkembang. Karena tujuan penelitian ini adalah untuk meningkatkan kontrol keamanan, maka rekomendasi akan dibuat. Perbandingan antara keadaan saat ini dan kondisi yang diharapkan dapat dilihat pada Gambar 4.4.



Gambar 4.4 *Gap* Analisis

4.5 Rekomendasi

Mengacu dari *gap* yang ada, maka penulis merekomendasikan untuk meningkatkan keamanan sistem informasi dengan mengacu pada kontrol keamanan yang terdapat pada objektif kontrol yang memiliki *gap* yang cukup banyak, sehingga nilai maturity level yang diharapkan dapat tercapai, sehingga keamanan informasi dapat terjaga di masa depan dengan baik. Berikut akan penulis sajikan beberapa rekomendasi, karena ancaman keamanan informasi terus berkembang,

teknologi dan sistem informasi juga terus berkembang. Berikut rekomendasi yang bisa penulis berikan untuk Siakad Universitas Labuhanbatu. Rekomendasi yang akan diberikan bisa diperhatikan dalam Tabel 4.6.

Tabel 4.6 Rekomendasi

9	**Kontrol Akses**
9.2	**Manajemen akses pengguna**
9.2.1	**Pendaftaran dan pencabutan akses pengguna**
Rekomendasi	
a. Laksanakan pelatihan untuk semua pengguna tentang pentingnya penggunaan kata sandi yang kuat, pengelolaan akun pengguna, dan praktik terbaik dalam menjaga kredensial akses	
11	**Keamanan fisik dan lingkungan**
11.2	**Peralatan**
11.2.8	**Peralatan user yang tidak diawasi**
Rekomendasi	
a. Sediakan pelatihan tentang cara melindungi perangkat fisik yang digunakan untuk mengakses Siakad dan menjaga keamanan lingkungan kepada seluruh pengguna Siakad termasuk mahasiswa	