LAMPIRAN

1. Data Hasil Kuesioner

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan															Rata-rata Kontrol Keamanan	Rata-rata Objektif Kontrol
			R 1	R 2	R 3	R 4	R 5	R 6	R 7	R 8	R 9	R 10	R 11	R 12	R 13	R 14	R 15		
9	9.1	9.1.1	4	4	4	4	5	4	5	4	4	5	4	3	3	5	4	4.13	4.16
		9.1.2	5	4	4	4	5	4	5	4	4	5	5	3	3	4	4	4.2	
	9.2	9.2.1	4	5	5	4	5	4	3	4	4	5	4	3	3	5	3	4.06	4.19
		9.2.2	5	5	5	4	5	4	5	5	4	5	5	4	4	5	5	4.66	
		9.2.3	4	5	5	4	4	5	5	4	4	5	4	3	2	5	4	4.2	
		9.2.4	5	5	5	4	4	4	4	4	4	5	4	3	3	4	5	4.2	
		9.2.5	5	5	5	4	4	4	4	2	4	3	4	1	1	5	5	3.73	
		9.2.6	4	5	5	4	4	4	5	5	4	4	4	4	4	4	5	4.33	
	9.3	9.3.1	5	4	4	5	4	5	5	4	4	4	5	4	4	4	5	4.4	4.4
	9.4	9.4.1	4	5	5	4	4	5	5	4	4	5	4	3	3	5	5	4.33	4.26
		9.4.2	5	4	4	5	4	4	5	5	4	5	3	5	5	5	4	4.46	
		9.4.3	5	5	5	4	4	4	4	4	4	5	4	4	4	5	5	4.4	
		9.4.4	5	4	4	4	4	4	4	4	4	4	5	2	2	4	4	3.86	
		9.4.5	5	5	5	4	4	4	5	5	4	5	0	4	4	5	5	4.26	
***Maturity level* Klausul 9**																			**4.25**

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan															Rata-rata kontrol Keamanan	Rata-rata Objektif Kontrol
			R 1	R 2	R 3	R 4	R 5	R 6	R 7	R 8	R 9	R 10	R 11	R 12	R 13	R 14	R 15		
11	11.1	11.1.1	5	5	5	4	5	5	5	2	4	5	3	3	3	5	4	4.2	4.18
		11.1.2	5	4	4	4	5	4	5	0	4	5	4	4	4	4	5	4.06	
		11.1.3	5	5	5	5	5	5	5	1	4	4	5	4	4	5	3	4.33	
		11.1.4	4	4	4	5	5	5	5	3	4	4	3	3	3	5	5	4.13	
	11.2	11.2.1	5	4	4	4	5	5	5	2	4	4	5	3	3	5	4	4.13	4.35
		11.2.2	5	5	5	4	5	4	4	2	4	5	5	3	3	4	5	4.2	

		11.2.3	5	5	5	5	5	5	4	3	4	5	5	4	4	5	4	4.53	
		11.2.4	5	5	5	4	5	4	4	4	4	5	5	4	4	5	5	4.53	
		11.2.5	5	5	5	4	5	4	4	2	4	4	5	3	3	4	5	4.13	
		11.2.6	4	5	5	4	5	4	5	3	4	5	5	4	4	5	5	4.46	
		11.2.7	5	4	4	4	5	4	5	3	4	5	5	3	3	5	4	4.2	
		11.2.8	5	4	4	4	5	4	5	4	4	5	3	4	4	5	5	4.33	
		11.2.9	5	5	5	5	5	4	4	5	4	5	4	5	5	4	5	4.66	
***Maturity level* Klausul 11**																			**4.26**

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**	**Tingkat Kemampuan**															**Rata-rata Kontrol Keamanan**	**Rata-rata Objektif Kontrol**
			R 1	**R 2**	**R 3**	**R 4**	**R 5**	**R 6**	**R 7**	**R 8**	**R 9**	**R 10**	**R 11**	**R 12**	**R 13**	**R 14**	**R 15**		
14	14.1	14.1.1	4	4	4	5	5	4	5	3	4	5	4	3	3	5	4	4.13	
		14.1.2	4	4	4	4	5	4	5	4	4	5	4	4	4	5	5	4.33	4.28
		14.1.3	5	4	4	4	5	4	5	4	4	5	4	4	4	5	5	4.4	
	14.2	14.2.1	5	5	5	5	5	4	5	4	4	5	5	2	2	4	4	4.26	
		14.2.2	4	5	5	4	5	4	5	4	4	4	4	3	3	5	5	4.26	
		14.2.3	5	5	5	4	5	5	5	3	4	4	3	3	3	4	4	4.13	
		14.2.4	5	5	5	4	5	5	5	3	4	4	4	3	3	5	4	4.26	
		14.2.5	5	5	5	4	5	5	5	1	4	4	4	3	3	4	5	4.13	4.19
		14.2.6	5	4	4	4	5	5	4	1	4	4	4	3	3	4	5	3.93	
		14.2.7	5	5	5	5	5	4	5	5	4	5	4	3	3	5	4	4.46	
		14.2.8	5	5	5	4	5	4	5	2	4	4	4	4	3	5	4	4.2	
		14.2.9	5	4	4	5	5	4	3	5	4	4	4	3	3	4	5	4.13	
	14.3	14.3.1	5	5	5	4	5	4	5	5	4	5	4	3	3	5	4	4.4	4.4
***Maturity level* Klausul 14**																			**4.29**

Keterangan:

Klausul	Objektif Kontrol	Kontrol Keamanan
9. Kontrol Akses	9.1. Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses
		9.1.2 Akses ke jaringan
	9.2. Manajemen akses pengguna	9.2.1 Pendaftaran dan pencabutan akses pengguna
		9.2.2 Penyediaan akses pengguna
		9.2.3 Pengelolaan hak akses istimewa
		9.2.4 Pengelolaan informasi rahasia pengguna
		9.2.5 *Review* hak akses pengguna
		9.2.6 Penghapusan atau penyesuaian hak akses
	9.3. Tanggungjawab pengguna	9.3.1 Penggunaan informasi rahasia
	9.4. Kontrol akses sistem dan aplikasi	9.4.1 Pembatasan akses informasi
		9.4.2 Pengamanan prosedur *log-on*
		9.4.3 Manajemen *password*
		9.4.4 Penggunaan program utilitas dengan hak akses level tinggi
		9.4.5 Kontrol akses terhadap *source code* program

Klausul	Objektif Kontrol	Kontrol Keamanan
11. Keamanan fisik dan lingkungan	11.1 Area aman	11.1.1 Pembatas keamanan fisik
		11.1.2 Kontrol entri fisik
		11.1.3 Keamanan ruang dan fasilitas kantor
		11.1.4 Perlindungan dari ancaman luar (eksternal)
	11.2 Peralatan	11.2.1 Penempatan dan perlindungan peralatan
		11.2.2 Utilitas pendukung

		11.2.3 Keamanan kabel
		11.2.4 Perawatan asset
		11.2.5 Penghapusan aset
		11.2.6 Keamanan asset diluar lokasi
		11.2.7 Pembuangan atau penggunaan kembali peralatan
		11.2.8 Peralatan *user* yang tidak diawasi
		11.2.9 Kebijakan *clear screen* dan *clear desk*

Klausul	**Objektif Kontrol**	**Kontrol Keamanan**
14 Akuisisi, Pengembangan dan Pengelolaan Sistem	14.1 Persyaratan keamanan sistem informasi	14.1.1 Analisis dan spesifikasi persyaratan informasi
		14.1.2 Pengamanan layanan aplikasi pada jaringan public
		14.1.3 Perlindungan transaksi layanan aplikasi
	14.2 Keamanan dalam proses pengembangan dan dukungan	14.2.1 Kebijakan pengembangan yang aman
		14.2.2 Prosedur kendali perubahan sistem
		14.2.3 Review teknis aplikasi setelah perubahan platform operasi
		14.2.4 Pembatasan dalam pengubahan paket perangkat lunak
		14.2.5 Prinsip rekayasa sistem yang aman
		14.2.6 Lingkungan pengembangan yang aman
		14.2.7 Pengembangan oleh alihdaya
		14.2.8 Pengujian keamanan sistem
		14.2.9 Pengujian penerimaan sistem
	14.3 Data Uji	14.3.1 Proteksi Data Uji

R1 = Responden 1	R6 = Responden 6	R11 = Responden 11
R2 = Responden 2	R7 = Responden 7	R12 = Responden 12
R3 = Responden 3	R8 = Responden 8	R13 = Responden 13
R4 = Responden 4	R9 = Responden 9	R14 = Responden 14
R5 = Responden 5	R10 = Responden 10	R15 = Responden 15

2. Angket/Kuesioner

Klausul : 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.							
Kontrol Keamanan : 9.1.2 Akses ke jaringan								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kategori Keamanan Utama : 9.2 Manajemen akses pengguna								
Kontrol Keamanan : 9.2.1 Pendaftaran dan pencabutan akses pengguna								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kontrol Keamanan : 9.2.2 Penyediaan akses pengguna								

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kontrol Keamanan : 9.2.3 Pengelolaan hak akses istimewa								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan untuk mengelola dan memantau penggunaan hak 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.							
Kontrol Keamanan : 9.2.4 Pengelolaan informasi rahasia pengguna								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							

Kontrol Keamanan : 9.2.5 Review hak akses pengguna

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							

Kontrol Keamanan : 9.2.6 Penghapusan atau penyesuaian hak akses

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kategori Keamanan Utama : 9.3 Tanggungjawab pengguna								
Kontrol Keamanan : 9.3.1 Penggunaan informasi rahasia								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kategori Keamanan Utama : 9.4 Kontrol akses sistem dan aplikasi								
Kontrol Keamanan : 9.4.1 Pembatasan akses informasi								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan dan prosedur yang memastikan bahwa akses ke informasi sensitif atau rahasia dalam SIAKAD dibatasi hanya kepada individu yang membutuhkan informasi tersebut untuk menjalankan tugas-tugas mereka.							
Kontrol Keamanan : 9.4.2 Pengamanan prosedur log-on								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							

Kontrol Keamanan : 9.4.3 Manajemen password

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							

Kontrol Keamanan : 9.4.4 Penggunaan program utilitas dengan hak akses level tinggi

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa penggunaan program utilitas dengan hak akses level tinggi pada SIAKAD dibatasi dan dipantau secara ketat.							

Kontrol Keamanan : 9.4.5 Kontrol akses terhadap source code program

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Klausul : 11 Keamanan fisik dan lingkungan								
Kategori Keamanan Utama : 11.1 Area aman								
Kontrol Keamanan : 11.1.1 Pembatas keamanan fisik								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kontrol Keamanan : 11.1.2 Kontrol entri fisik								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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 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	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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							
Kontrol Keamanan : 11.1.4 Perlindungan dari ancaman luar (eksternal)								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							
Kategori Keamanan Utama : 11.2 Peralatan								
Kontrol Keamanan : 11.2.1 Penempatan dan perlindungan peralatan								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang digunakan dalam operasi							

	SIAKAD ditempatkan dan dilindungi secara aman, termasuk langkah-langkah untuk mencegah kerusakan fisik, pencurian, atau gangguan yang dapat mempengaruhi ketersediaan atau integritas sistem.							

Kontrol Keamanan : 11.2.2 Utilitas pendukung								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							

Kontrol Keamanan : 11.2.3 Keamanan kabel								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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.							

Kontrol Keamanan : 11.2.4 Perawatan asset								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
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 untuk memastikan ketersediaan, keandalan, dan integritasnya selama siklus hidup penggunaannya.							
Kontrol Keamanan : 11.2.5 Penghapusan aset								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa penghapusan aset yang tidak lagi diperlukan dalam operasi SIAKAD, seperti perangkat keras yang sudah tidak digunakan atau data yang sudah tidak relevan, dilakukan secara aman, termasuk penghapusan atau pemusnahan data yang sensitif secara permanen.							
Kontrol Keamanan : 11.2.6 Keamanan asset diluar lokasi								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa asset yang digunakan dalam operasi SIAKAD dan dibawa keluar lokasi, seperti laptop atau							

	perangkat mobile, dilindungi secara kuat dengan langkah-langkah keamanan, seperti enkripsi data dan mekanisme otentikasi, untuk mencegah risiko kehilangan atau akses yang tidak sah.							

Kontrol Keamanan : 11.2.7 Pembuangan atau penggunaan kembali peralatan

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang tidak lagi digunakan dalam operasi SIAKAD, seperti perangkat keras yang usang atau tidak lagi diperlukan, dibuang atau didaur ulang secara aman sesuai dengan standar keamanan dan lingkungan, dan langkah-langkah telah diambil untuk memastikan bahwa data sensitif telah dihapus dengan benar sebelum pembuangan.							

Kontrol Keamanan : 11.2.8 Peralatan user yang tidak diawasi

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang digunakan oleh pengguna untuk mengakses SIAKAD di luar lingkungan kerja, seperti perangkat mobile pribadi atau komputer yang tidak diawasi,							

	dilindungi dengan langkah-langkah keamanan yang sesuai, seperti penggunaan koneksi aman dan enkripsi data, untuk mengurangi risiko akses yang tidak sah atau pencurian informasi.							
Kontrol Keamanan : 11.2.9 Kebijakan clear screen dan clear desk								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa pengguna SIAKAD diharuskan untuk membersihkan layar monitor dan meja kerja mereka serta mengunci komputer ketika meninggalkan tempat kerja, dan melakukan log off jika pergi untuk jangka waktu lama.							
Klausul : 14 Akuisisi, pengembangan dan perawatan sistem								
Kategori Keamanan Utama : 14.1 Persyaratan keamanan sistem informasi								
Kontrol Keamanan : 14.1.1 Analisis dan spesifikasi persyaratan informasi								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa analisis dan spesifikasi persyaratan informasi untuk pengembangan, penyesuaian, atau pemeliharaan SIAKAD dilakukan secara komprehensif, termasuk identifikasi kebutuhan bisnis, keamanan, dan privasi, serta pemahaman yang jelas tentang fungsi dan							

	kinerja yang diharapkan dari sistem.							

Kontrol Keamanan : 14.1.2 Pengamanan layanan aplikasi pada jaringan public

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa layanan aplikasi yang diakses melalui jaringan publik dalam SIAKAD dilindungi secara kuat dengan langkah-langkah keamanan, seperti enkripsi data, autentikasi yang kuat, dan pemantauan lalu lintas jaringan, untuk mengurangi risiko serangan atau akses yang tidak sah dari pihak luar.							

Kontrol Keamanan : 14.1.3 Perlindungan transaksi layanan aplikasi

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa transaksi yang dilakukan melalui layanan aplikasi dalam SIAKAD dilindungi secara kuat dengan langkah-langkah keamanan, seperti otentikasi pengguna, enkripsi data, dan pemantauan aktivitas transaksi, untuk mengurangi risiko manipulasi atau pengungkapan informasi sensitif selama proses transaksi.							

Kategori Keamanan Utama : 14.2 Keamanan dalam proses pengembangan dan dukungan

Kontrol Keamanan : 14.2.1 Kebijakan pengembangan yang aman								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan pengembangan yang aman yang memastikan bahwa seluruh proses pengembangan atau perubahan pada SIAKAD, termasuk pembaruan perangkat lunak, pengujian, dan penerapan kode, memperhatikan prinsip-prinsip keamanan informasi, seperti penerapan kontrol akses, pemrosesan yang aman, dan mitigasi risiko keamanan.							
Kontrol Keamanan : 14.2.2 Prosedur kendali perubahan sistem								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan kendali perubahan sistem yang memastikan bahwa setiap perubahan pada SIAKAD, baik itu dalam bentuk perangkat keras, perangkat lunak, atau konfigurasi, disetujui, didokumentasikan, dan diuji secara menyeluruh sebelum diterapkan.							
Kontrol Keamanan : 14.2.3 Review teknis aplikasi setelah perubahan platform operasi								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa setiap kali terjadi perubahan pada platform operasi yang digunakan							

	untuk menjalankan aplikasi dalam SIAKAD, dilakukan review teknis aplikasi secara menyeluruh untuk memastikan bahwa aplikasi masih beroperasi dengan benar, aman, dan sesuai dengan kebutuhan bisnis, serta untuk mengidentifikasi dan memitigasi potensi risiko yang mungkin timbul.							

Kontrol Keamanan : 14.2.4 Pembatasan dalam pengubahan paket perangkat lunak

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan atau prosedur yang memastikan bahwa pengubahan atau penambahan paket perangkat lunak pada SIAKAD dibatasi hanya kepada paket perangkat lunak yang telah melalui evaluasi keamanan yang memadai, dan dilakukan pengawasan yang ketat terhadap perubahan tersebut untuk meminimalkan risiko terhadap keamanan dan ketersediaan sistem.							

Kontrol Keamanan : 14.2.5 Prinsip rekayasa sistem yang aman

No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah diterapkan prinsip rekayasa sistem yang aman dalam pengembangan atau penyesuaian SIAKAD, seperti penerapan kontrol akses yang tepat, perlindungan data, dan							

	pemisahan tugas, untuk memastikan bahwa sistem dirancang dan diimplementasikan dengan memperhatikan aspek keamanan informasi yang penting.							
Kontrol Keamanan : 14.2.6 Lingkungan pengembangan yang aman								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa lingkungan pengembangan yang digunakan untuk mengembangkan atau menguji perangkat lunak SIAKAD dilindungi secara kuat, termasuk pemisahan lingkungan produksi dan pengembangan, penggunaan data uji yang tidak sensitif, dan kontrol akses yang ketat, untuk mengurangi risiko terhadap keamanan dan ketersediaan sistem.							
Kontrol Keamanan : 14.2.7 Pengembangan oleh alihdaya								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan yang memastikan bahwa penyedia layanan atau pihak ketiga yang terlibat dalam pengembangan SIAKAD, termasuk pihak yang melakukan outsourcing, mematuhi standar keamanan yang ditetapkan, seperti pengelolaan akses yang ketat, perlindungan data,							

	dan pengawasan yang teratur, untuk mengurangi risiko terhadap keamanan informasi.							
Kontrol Keamanan : 14.2.8 Pengujian keamanan sistem								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah dilakukan pengujian keamanan secara teratur pada SIAKAD untuk mengidentifikasi dan mengatasi potensi celah keamanan.							
Kontrol Keamanan : 14.2.9 Pengujian penerimaan sistem								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah dilakukan pengujian penerimaan sistem secara menyeluruh sebelum penerapan sistem secara live, termasuk pengujian fungsionalitas, keamanan, dan kinerja, serta hasil pengujian telah diverifikasi dan disetujui oleh pihak yang berwenang sebelum sistem diimplementasikan secara penuh.							
Kategori Keamanan Utama : 14.3 Data Uji								
Kontrol Keamanan : 14.3.1 Proteksi Data Uji								
No	Pernyataan	Tingkat Kemampuan						Nilai
		0	1	2	3	4	5	
1	Telah ditetapkan kebijakan dan prosedur yang memastikan bahwa data uji yang digunakan dalam pengujian SIAKAD dilindungi secara kuat untuk mencegah akses yang tidak sah atau							

	pengungkapan informasi sensitif.							

3. Hasil pemeriksaan

Klausul : 9. Kontrol Akses				
Kategori Keamanan Utama : 9.1 Persyaratan bisnis untuk kontrol akses				
Kontrol Keamanan : 9.1.1 Kebijakan kontrol akses				
No	**Pernyataan**	**Ya**	**Tidak**	**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.	✓		Kebijakan kontrol akses telah dilakukan dengan baik. Bukti: a. Pintu memiliki kunci b. Ruangan tersendiri 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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan untuk mengelola dan memantau penggunaan hak 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.	✓		Pengelolaan hak akses istimewa telah dilakukan dengan baik. Bukti: 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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa hak akses pengguna pada SIAKAD dihapus atau disesuaikan secara tepat waktu ketika pengguna	✓		Penghapusan atau penyesuaian hak akses telah dilakukan dengan baik. Bukti:

	tersebut tidak lagi memerlukan akses, telah berubah peran atau tanggung jawabnya, atau telah meninggalkan organisasi.			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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan dan prosedur yang memastikan bahwa akses ke informasi sensitif atau rahasia dalam SIAKAD dibatasi hanya kepada individu yang membutuhkan informasi tersebut untuk menjalankan tugas-tugas mereka.	✓		Pembatasan akses informasi telah dikendalikan dengan baik. Bukti: 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**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa kebijakan log-on ke dalam SIAKAD diamanatkan dengan menggunakan	✓		Pengamanan prosedur log-on telah dikendalikan dengan baik. Bukti:

	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.			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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa penggunaan program utilitas dengan hak akses level tinggi pada SIAKAD dibatasi dan dipantau secara ketat.	✓		Penggunaan program utilitas dengan hak akses level tinggi telah dilakukan dengan baik. 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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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

	SIAKAD, dan mekanisme otentikasi, seperti kartu akses atau biometrik, digunakan untuk memverifikasi identitas dan hak akses pengguna sebelum memasuki ruang tersebut.			masuk untuk kontrol akses
Kontrol Keamanan : 11.1.3 Keamanan ruang dan fasilitas kantor				
No	**Pernyataan**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang digunakan dalam operasi SIAKAD ditempatkan dan dilindungi secara aman, termasuk langkah-langkah untuk mencegah kerusakan fisik, pencurian, atau gangguan yang dapat mempengaruhi ketersediaan atau integritas sistem.	✓		Penempatan dan perlindungan peralatan telah dikendalikan dengan baik. Bukti: 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**	**Ya**	**Tidak**	**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**	**Ya**	**Tidak**	**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	✓		Keamanan kabel telah dikendalikan dengan baik. Bukti: a. Memiliki ruangan tersendiri b. Pada ruangan tersebut tidak boleh keluar masuk sembarangan

	sah yang dapat mempengaruhi integritas atau ketersediaan sistem.			c. Hanya petugas IT yang boleh keluar masuk
Kontrol Keamanan : 11.2.4 Perawatan asset				
No	**Pernyataan**	**Ya**	**Tidak**	**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 untuk memastikan ketersediaan, keandalan, dan integritasnya selama siklus hidup penggunaannya.	✓		Perawatan asset telah dilakukan dengan baik. Bukti: a. Melakukan backup data, terdapat backup data mingguan dan backup data bulanan b. Melakukan kontrol akses c. Terdapat UPS untuk server d. Terdapat AC untuk menjaga server agar tidak panas
Kontrol Keamanan : 11.2.5 Penghapusan aset				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa penghapusan aset yang tidak lagi diperlukan dalam operasi SIAKAD, seperti perangkat keras yang sudah tidak digunakan atau data yang sudah tidak relevan, dilakukan secara aman, termasuk penghapusan atau pemusnahan data yang sensitif secara permanen.	✓		Penghapusan aset dikendalikan dengan baik. Bukti: a. Terdapat penghapusan akun ketika dibutuhkan yang hanya dilakukan oleh orang yang telah ditugaskan b. Terdapat pemisahan/pembuangan perangkat keras ketika dibutuhkan yang hanya dilakukan oleh orang yang telah ditugaskan c. Terdapat backup data mingguan dan backup data bulanan
Kontrol Keamanan : 11.2.6 Keamanan asset diluar lokasi				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**

1	Telah ditetapkan kebijakan yang memastikan bahwa asset yang digunakan dalam operasi SIAKAD dan dibawa keluar lokasi, seperti laptop atau perangkat mobile, dilindungi secara kuat dengan langkah-langkah keamanan, seperti enkripsi data dan mekanisme otentikasi, untuk mencegah risiko kehilangan atau akses yang tidak sah.	✓		Keamanan asset di luar lokasi telah dikendalikan dengan baik. Bukti: a. Saat akan log-on ke siakad maka user harus memasukkan terlebih dahulu username dan password b. Terdapat enkripsi data
Kontrol Keamanan : 11.2.7 Pembuangan atau penggunaan kembali peralatan				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang tidak lagi digunakan dalam operasi SIAKAD, seperti perangkat keras yang usang atau tidak lagi diperlukan, dibuang atau didaur ulang secara aman sesuai dengan standar keamanan dan lingkungan, dan langkah-langkah telah diambil untuk memastikan bahwa data sensitif telah dihapus dengan benar sebelum pembuangan.	✓		Pembuangan atau penggunaan kembali peralatan telah dikendalikan dengan baik. Bukti: a. Terdapat backup data, yaitu backup data mingguan dan backup data bulanan sehingga data tetap aman tersimpan walaupun nantinya peralatan seperti perangkat keras mengalami kerusakan dan harus dilakukan pembuangan
Kontrol Keamanan : 11.2.8 Peralatan user yang tidak diawasi				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa peralatan yang digunakan oleh pengguna untuk mengakses SIAKAD di luar lingkungan kerja, seperti perangkat mobile pribadi atau komputer yang tidak diawasi, dilindungi dengan	✓		Peralatan user yang tidak diawasi telah dikendalikan dengan baik. Bukti: a. Terdapat langka keamanan seperti harus memasukkan password dan

	langkah-langkah keamanan yang sesuai, seperti penggunaan koneksi aman dan enkripsi data, untuk mengurangi risiko akses yang tidak sah atau pencurian informasi.			username terlebih dahulu saat akan masuk ke dalam akun siakad b. Jika terjadi permasalahan maka password/kata sandi dapat di riset oleh admin siakad. Jadi, jika terjadi permasalahan pada akun siakad pengguna dapat melapor ke admin
Kontrol Keamanan : 11.2.9 Kebijakan clear screen dan clear desk				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa pengguna SIAKAD diharuskan untuk membersihkan layar monitor dan meja kerja mereka serta mengunci komputer ketika meninggalkan tempat kerja, dan melakukan log off jika pergi untuk jangka waktu lama.	✓		Kebijakan clear screen dan clear desk telah dikendalikan dengan baik. Bukti: a. Ruang puskom dan ruang user lainnya seperti ruang dosen, biro keuangan dan ruang lainnya terlihat bersih, untuk ruang puskom dapat dilihat pada foto yang terdapat pada lampiran b. Ketika masuk ke akun mahasiswa terdapat pemberitahun pada bagian home, terdapat pemberitahuan bahwa demi keamanan data Siakad ULB maka diharapkan untuk tidak lupa logout sebelum meninggalkan

				komputer yang digunakan
Klausul : 14 Akuisisi, pengembangan dan perawatan sistem				
Kategori Keamanan Utama : 14.1 Persyaratan keamanan sistem informasi				
Kontrol Keamanan informasi : 14.1.1 Analisis dan spesifikasi persyaratan				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa analisis dan spesifikasi persyaratan informasi untuk pengembangan, penyesuaian, atau pemeliharaan SIAKAD dilakukan secara komprehensif, termasuk identifikasi kebutuhan bisnis, keamanan, dan privasi, serta pemahaman yang jelas tentang fungsi dan kinerja yang diharapkan dari sistem.	✓		Analisis dan spesifikasi persyaratan informasi telah dikendalikan dengan baik. Bukti: a. Pada bagian home user mahasiswa terdapat pemberitahuan bahwa sistem siakad terus dikembangkan sesuai dengan informasi yang terupdate dan juga terdapat pemberitahuan bahwa saran dan kritikan sangat diperlukan untuk perbaikan di masa yang akan datang, ini menjadi salah satu bukti bahwa untuk pengembangan, penyesuaian, atau pemeliharaan Siakad dilakukan secara komprehensif sesuai dengan apa yang dibutuhkan user b. Pada informasi yang terdapat dalam Siakad berbeda-beda tergantung akun yang kita miliki, jika masuk menggunakan user mahasiswa maka informasi yang tersedia merupakan

				kebutuhan mahasiswa selama berkuliah, dan jika masuk menggunakan user Dosen, user Admin, user keuangan, user Kepala keuangan, user Operator, user Kaprodi, user Dekan, ataupun user PMB maka informasi yang ada di dalamnya juga berbeda dan sesuai dengan fungsi jabatannya
Kontrol Keamanan : 14.1.2 Pengamanan layanan aplikasi pada jaringan public				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa layanan aplikasi yang diakses melalui jaringan publik dalam SIAKAD dilindungi secara kuat dengan langkah-langkah keamanan, seperti enkripsi data, autentikasi yang kuat, dan pemantauan lalu lintas jaringan, untuk mengurangi risiko serangan atau akses yang tidak sah dari pihak luar.	✓		Pengamanan layanan aplikasi pada jaringan public telah dikendalikan dengan baik. Bukti: a. Jaringan stabil b. Pertahanan kuat
Kontrol Keamanan : 14.1.3 Perlindungan transaksi layanan aplikasi				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa transaksi yang dilakukan melalui layanan aplikasi dalam SIAKAD dilindungi secara kuat dengan langkah-langkah keamanan, seperti otentikasi pengguna, enkripsi data, dan pemantauan aktivitas transaksi, untuk mengurangi	✓		Perlindungan transaksi layanan aplikasi telah dikendalikan dengan baik. Bukti: a. Terdapat enkripsi data b. Jika terdapat permasalahan dengan data keuangan yang ditampilkan dalam

	risiko manipulasi atau pengungkapan informasi sensitif selama proses transaksi.			siakad, maka mahasiswa dapat langsung melapor ke biro keuangan,selanjutnya akan langsung dilakukan pemeriksaan
Kategori Keamanan Utama : 14.2 Keamanan dalam proses pengembangan dan dukungan				
Kontrol Keamanan : 14.2.1 Kebijakan pengembangan yang aman				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan pengembangan yang aman yang memastikan bahwa seluruh proses pengembangan atau perubahan pada SIAKAD, termasuk pembaruan perangkat lunak, pengujian, dan penerapan kode, memperhatikan prinsip-prinsip keamanan informasi, seperti penerapan kontrol akses, pemrosesan yang aman, dan mitigasi risiko keamanan.	✓		Kebijakan pengembangan yang aman telah dikendalikan dengan baik. Bukti: a. Terdapat kontrol akses
Kontrol Keamanan : 14.2.2 Prosedur kendali perubahan sistem				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan kendali perubahan sistem yang memastikan bahwa setiap perubahan pada SIAKAD, baik itu dalam bentuk perangkat keras, perangkat lunak, atau konfigurasi, disetujui, didokumentasikan, dan diuji secara menyeluruh sebelum diterapkan.	✓		Prosedur kendali perubahan sistem telah dikendalikan dengan baik. Bukti: a. Terdapat simulasi awal b. Terdapat tes uji c. Terdapat hasil/demo
Kontrol Keamanan : 14.2.3 Review teknis aplikasi setelah perubahan platform operasi				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa setiap kali terjadi perubahan	✓		Review teknis aplikasi setelah perubahan platform operasi telah

	pada platform operasi yang digunakan untuk menjalankan aplikasi dalam SIAKAD, dilakukan review teknis aplikasi secara menyeluruh untuk memastikan bahwa aplikasi masih beroperasi dengan benar, aman, dan sesuai dengan kebutuhan bisnis, serta untuk mengidentifikasi dan memitigasi potensi risiko yang mungkin timbul.			dikendalikan dengan baik. Bukti: a. Terdapat tes uji b. Terbuka terhadap saran dan kritikan, hal tersebut tertulis pada bagian home user mahasiswa, sehingga mahasiswa dapat memberikan reviewnya dengan tepat, karena mahasiswa lah yang merupakan salah satu pengguna siakad tersebut
Kontrol Keamanan : 14.2.4 Pembatasan dalam pengubahan paket perangkat lunak				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan atau prosedur yang memastikan bahwa pengubahan atau penambahan paket perangkat lunak pada SIAKAD dibatasi hanya kepada paket perangkat lunak yang telah melalui evaluasi keamanan yang memadai, dan dilakukan pengawasan yang ketat terhadap perubahan tersebut untuk meminimalkan risiko terhadap keamanan dan ketersediaan sistem.	✓		Pembatasan dalam pengubahan paket perangkat lunak telah dikendalikan dengan baik. Bukti: a. Terdapat simulasi awal b. Terdapat tes uji c. Terdapat hasil/demo
Kontrol Keamanan : 14.2.5 Prinsip rekayasa sistem yang aman				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah diterapkan prinsip rekayasa sistem yang aman dalam pengembangan atau penyesuaian SIAKAD, seperti penerapan kontrol akses yang tepat, perlindungan data, dan pemisahan tugas, untuk	✓		Prinsip rekayasa sistem yang aman telah dikendalikan dengan baik. Bukti: a. Backup data mingguan b. Backup data bulanan

	memastikan bahwa sistem dirancang dan diimplementasikan dengan memperhatikan aspek keamanan informasi yang penting.			c. Terdapat kontrol akses d. Hanya petugas IT yang boleh keluar masuk untuk kontrol akses, sehingga lebih aman untuk menjaga keamanan informasi yang penting
Kontrol Keamanan : 14.2.6 Lingkungan pengembangan yang aman				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa lingkungan pengembangan yang digunakan untuk mengembangkan atau menguji perangkat lunak SIAKAD dilindungi secara kuat, termasuk pemisahan lingkungan produksi dan pengembangan, penggunaan data uji yang tidak sensitif, dan kontrol akses yang ketat, untuk mengurangi risiko terhadap keamanan dan ketersediaan sistem.	✓		Lingkungan pengembangan yang aman telah dikendalikan dengan baik. Bukti: a. Pintu terdapat kunci b. Memiliki ruangan tersendiri c. Tidak boleh keluar masuk sembarangan d. Hanya bagian IT yang boleh keluar masuk e. Terdapat kontrol akses
Kontrol Keamanan : 14.2.7 Pengembangan oleh alihdaya				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan yang memastikan bahwa penyedia layanan atau pihak ketiga yang terlibat dalam pengembangan SIAKAD, termasuk pihak yang melakukan outsourcing, mematuhi standar keamanan yang ditetapkan, seperti pengelolaan akses yang ketat, perlindungan data, dan pengawasan yang teratur, untuk mengurangi risiko terhadap keamanan informasi.	✓		Pengembangan oleh alihdaya telah dikendalikan dengan baik. Bukti: a. Pengembangan Siakad hanya dikelola sesuai tim IT dengan SK yang ditugaskan
Kontrol Keamanan : 14.2.8 Pengujian keamanan sistem				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**

1	Telah dilakukan pengujian keamanan secara teratur pada SIAKAD untuk mengidentifikasi dan mengatasi potensi celah keamanan.	✓		Pengujian keamanan sistem telah dikendalikan dengan baik. Bukti: a. Terdapat tes uji pada sistem b. Terdapat kontrol akses
Kontrol Keamanan : 14.2.9 Pengujian penerimaan sistem				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah dilakukan pengujian penerimaan sistem secara menyeluruh sebelum penerapan sistem secara live, termasuk pengujian fungsionalitas, keamanan, dan kinerja, serta hasil pengujian telah diverifikasi dan disetujui oleh pihak yang berwenang sebelum sistem diimplementasikan secara penuh.	✓		Pengujian penerimaan sistem telah dikendalikan dengan baik. Bukti: a. Terdapat simulasi awal b. Terdapat tes uji c. Terdapat hasil/demo
Kategori Keamanan Utama : 14.3 Data Uji				
Kontrol Keamanan : 14.3.1 Proteksi Data Uji				
No	**Pernyataan**	**Ya**	**Tidak**	**Hasil Pemeriksaan**
1	Telah ditetapkan kebijakan dan prosedur yang memastikan bahwa data uji yang digunakan dalam pengujian SIAKAD dilindungi secara kuat untuk mencegah akses yang tidak sah atau pengungkapan informasi sensitif.	✓		Proteksi Data Uji telah dikendalikan dengan baik. Bukti: a. Kontrol akses yang aman

4. Foto-foto ruangan