AUDIT SISTEM INFORMASI / TEKNOLOGI INFORMASI DENGAN KERANGKA KERJA SDLC BERBASIS COBIT UNTUK EVALUASI MANAJEMEN TEKNOLOGI INFORMASI

Labib Falah Athallah : 1462200221

Abdul Rohman Masrifan : 1462200195

Okky Hendrawan : 14622001279

M. Aprilian rizal wahyudi : 1462200276

Nofan wahyu setiawan : 1462200170

Fakultas Teknik Indormatika, Universitas 17 Agustus Surabaya

Data Audit SDLC

No.	Area Pertanyaan	Pertanyaan	Jawaban
1.	Kesiapan Tata Kelola	Bagaimana kerangka kerja tata kelola TI, termasuk kebijakan, prosedur, dan struktur organisasi, telah ditetapkan dan dipelihara untuk mendukung pengelolaan sistem informasi SIAKAD?	Auditor: Apakah ada dokumen formal yang menetapkan kerangka kerja tata kelola TI untuk sistem informasi SIAKAD? Pemangku Kepentingan: Ya, kami memiliki kebijakan dan prosedur yang telah ditetapkan untuk mengatur pengelolaan dan pemeliharaan sistem informasi SIAKAD. Dokumen ini secara teratur diperbarui sesuai dengan kebutuhan organisasi.
		Bagaimana komunikasi dan koordinasi antara komite tata kelola TI dan manajemen operasional dalam konteks SIAKAD?	Auditor: Bagaimana komunikasi dan koordinasi antara komite tata kelola TI dan manajemen operasional dalam konteks SIAKAD? Pemangku Kepentingan: Komite tata kelola TI secara rutin berinteraksi dengan manajemen operasional untuk memastikan bahwa kebutuhan dan tujuan sistem informasi SIAKAD terpenuhi sesuai dengan strategi organisasi.
2.	Pengelolaan Keamanan	Bagaimana kontrol keamanan, termasuk akses pengguna, enkripsi data, dan pemantauan keamanan, diterapkan dan dipelihara dalam sistem informasi SIAKAD?	Auditor: Bagaimana pengelolaan akses pengguna diatur dalam SIAKAD? Pemangku Kepentingan: Akses pengguna dalam SIAKAD diatur berdasarkan peran dan tanggung jawab, dengan izin akses yang diberikan sesuai dengan kebutuhan pekerjaan. Selain itu, data sensitif dienkripsi dan pemantauan keamanan dilakukan secara teratur untuk mendeteksi potensi ancaman.
		Apakah telah dilakukan evaluasi risiko keamanan untuk sistem informasi SIAKAD?	Auditor: Apakah telah dilakukan evaluasi risiko keamanan untuk sistem informasi SIAKAD? Pemangku Kepentingan: Ya, kami melakukan evaluasi risiko keamanan secara berkala untuk mengidentifikasi potensi ancaman dan kerentanan. Langkah-langkah mitigasi kemudian diimplementasikan untuk mengurangi risiko keamanan.
3.	Manajemen Proyek	Bagaimana proyek implementasi atau pengembangan sistem informasi SIAKAD dipantau dan dikendalikan?	Auditor: Apakah ada rencana proyek yang telah ditetapkan untuk implementasi sistem informasi SIAKAD? Pemangku Kepentingan: Ya, kami memiliki rencana proyek yang mencakup tujuan, jadwal, anggaran, dan sumber daya yang dibutuhkan. Rencana ini secara teratur diperbarui sesuai dengan kemajuan proyek.
		Bagaimana pengeluaran dan sumber daya proyek dikendalikan dalam konteks SIAKAD?	Auditor: Bagaimana pengeluaran dan sumber daya proyek dikendalikan dalam konteks SIAKAD? Pemangku Kepentingan: Pengeluaran proyek dipantau secara rutin untuk memastikan bahwa anggaran yang dialokasikan sesuai dengan rencana proyek. Sumber daya proyek, termasuk

			personil dan infrastruktur, dialokasikan secara efisien sesuai dengan kebutuhan proyek.
4.	Ketersediaan dan Kapasitas	Bagaimana ketersediaan dan kapasitas sistem informasi SIAKAD dipantau dan dikelola?	Auditor: Bagaimana ketersediaan sistem informasi SIAKAD dijaga dalam situasi darurat atau kegagalan sistem? Pemangku Kepentingan: Kami memiliki rencana pemulihan bencana yang mencakup langkah-langkah untuk mengembalikan operasi sistem dalam waktu yang minimal jika terjadi kegagalan atau gangguan.
		Bagaimana kinerja sistem informasi SIAKAD dipantau dalam konteks ketersediaan dan kapasitas?	Auditor: Bagaimana kinerja sistem informasi SIAKAD dipantau dalam konteks ketersediaan dan kapasitas? Pemangku Kepentingan: Kami menggunakan alat pemantauan otomatis untuk memantau kinerja sistem secara terus-menerus. Pemantauan ini membantu kami mengidentifikasi potensi masalah ketersediaan atau kapasitas dan mengambil tindakan yang sesuai.
5.	Operasi dan Pemeliharaan	Bagaimana operasi sehari-hari sistem informasi SIAKAD dilakukan?	Auditor: Bagaimana operasi sehari-hari sistem informasi SIAKAD dilakukan? Pemangku Kepentingan: Tim operasional kami bertanggung jawab atas pemantauan kinerja sistem secara terus-menerus. Mereka menggunakan alat pemantauan untuk memantau kinerja sistem, melacak masalah, dan menanggapi perubahan yang diperlukan.
		Bagaimana pemeliharaan rutin sistem informasi SIAKAD dilakukan?	Auditor: Bagaimana pemeliharaan rutin sistem informasi SIAKAD dilakukan? Pemangku Kepentingan: Pemeliharaan rutin sistem termasuk penerapan patch keamanan, pembaruan perangkat lunak, dan pembersihan data. Proses ini dijadwalkan dan dilaksanakan secara berkala untuk memastikan kinerja sistem yang optimal.
6.	Pemantauan dan Evaluasi	Bagaimana kinerja sistem informasi SIAKAD dievaluasi secara berkala?	Auditor: Bagaimana kinerja sistem informasi SIAKAD dievaluasi secara berkala? Pemangku Kepentingan: Kami menetapkan metrik kinerja yang relevan untuk mengukur kinerja sistem, termasuk waktu respon, ketersediaan sistem, dan tingkat kesalahan. Evaluasi dilakukan secara berkala untuk memastikan bahwa sistem tetap berkinerja optimal.
		Bagaimana hasil evaluasi kinerja sistem digunakan untuk mengidentifikasi perbaikan atau peningkatan yang diperlukan?	Auditor: Bagaimana hasil evaluasi kinerja sistem digunakan untuk mengidentifikasi perbaikan atau peningkatan yang diperlukan? Pemangku Kepentingan: Hasil evaluasi kinerja sistem digunakan untuk mengidentifikasi area perbaikan atau peningkatan yang mungkin diperlukan dalam infrastruktur, proses operasional, atau kebijakan keamanan.

Data Pengujian Sistem

No.	Area Pengujian	Sub-Area Pengujian	Deskripsi Pengujian	Metode Pengujian	Hasil Pengujian	Tindakan Selanjutnya
1.	Pengujian Fungsionalitas	1.1. Pendaftaran Mahasiswa	Memeriksa apakah fungsi pendaftaran mahasiswa berfungsi dengan baik, termasuk proses pendaftaran, verifikasi identitas, dan pengelolaan data mahasiswa.	Uji Fungsional	Fungsi pendaftaran mahasiswa berjalan dengan baik.	Tidak diperlukan.
		1.2. Manajemen Kurikulum	Memeriksa apakah sistem dapat mengelola kurikulum dengan efisien, termasuk penjadwalan kelas, pengelolaan program studi, dan pembaruan kurikulum.	Uji Fungsional	Manajemen kurikulum berfungsi dengan baik.	
		1.3. Pengarsipan Data	Memeriksa proses pengarsipan data untuk memastikan bahwa data mahasiswa, pengajar, dan program akademik disimpan dengan aman dan dapat diakses dengan tepat.	Uji Fungsional	Proses pengarsipan data berjalan dengan baik.	
2.	Pengujian Keamanan	2.1. Uji Penetrasi	Melakukan serangan kontrol keamanan untuk mengidentifikasi kerentanan dalam sistem dan mencoba mendapatkan akses tanpa izin.	Uji Penetrasi	Beberapa kerentanan keamanan ditemukan dan diperbaiki.	Perbaiki kerentanan yang ditemukan.

No.	Area Pengujian	Sub-Area Pengujian	Deskripsi Pengujian	Metode Pengujian	Hasil Pengujian	Tindakan Selanjutnya
		2.2. Pengecekan Vulnerabilitas	Memeriksa sistem untuk menemukan kelemahan atau celah keamanan yang mungkin dimanfaatkan oleh penyerang.	Pengecekan Vulnerabilitas	Pengecekan menemukan beberapa vulnerabilitas yang perlu diperbaiki.	
		2.3. Analisis Kerentanan	Melakukan analisis mendalam terhadap kerentanan yang ditemukan untuk memahami sumber masalah dan menentukan tindakan perbaikan yang diperlukan.	Analisis Kerentanan	Analisis kerentanan telah dilakukan dan langkah perbaikan telah ditetapkan.	
3.	Pengujian Kinerja	3.1. Pengukuran Waktu Respons	Mengukur waktu yang diperlukan sistem untuk merespons permintaan pengguna, seperti waktu pemuatan halaman dan respon formulir.	Pengukuran Waktu Respons	Waktu respons sistem memadai di bawah beban normal.	Tingkatkan kapasitas atau performa sistem jika diperlukan.
		3.2. Pengukuran Kinerja saat Beban Tinggi	Mengukur kinerja sistem saat menghadapi beban tinggi, seperti pendaftaran massal atau penggunaan simultan oleh banyak pengguna.	Pengukuran Kinerja saat Beban Tinggi	Kinerja sistem memerlukan peningkatan saat beban tinggi.	
4.	Pengujian Integrasi	4.1. Integrasi dengan Sistem Keuangan	Memeriksa integrasi antara Sistem Informasi SIAKAD dan sistem keuangan untuk memastikan data transaksi	Uji Integrasi	Integrasi dengan sistem keuangan berhasil.	Pastikan interaksi antara sistem tetap stabil.

No.	Area Pengujian	Sub-Area Pengujian	Deskripsi Pengujian	Metode Pengujian	Hasil Pengujian	Tindakan Selanjutnya
			dapat dipindahkan dengan benar antara sistem.			
		4.2. Integrasi dengan Sistem Perpustakaan	Memeriksa integrasi antara Sistem Informasi SIAKAD dan sistem perpustakaan untuk memastikan pengelolaan koleksi dan data peminjaman dapat terjadi tanpa masalah.	Uji Integrasi	Integrasi dengan sistem perpustakaan berjalan dengan lancar.	
5.	Pengujian Pemulihan Bencana	5.1. Uji Pemulihan Data dari Cadangan	Mensimulasikan kegagalan sistem dan mencoba memulihkan data mahasiswa, pengajar, dan kurikulum dari cadangan untuk memastikan bahwa data dapat dipulihkan dengan cepat dan tepat.	Uji Pemulihan Bencana	Pemulihan bencana berhasil dan data dapat dipulihkan dengan cepat.	Pastikan cadangan data teratur dan berfungsi dengan baik.
6.	Pengujian Kebutuhan Khusus Pengguna (User Acceptance Testing)	6.1. Uji Fungsional oleh Pengguna Akhir	Melibatkan pengguna akhir dalam pengujian fungsional sistem untuk memastikan bahwa fungsionalitas sistem sesuai dengan harapan dan kebutuhan pengguna.	Uji oleh Pengguna Akhir	Pengguna akhir puas dengan fungsionalitas dan antarmuka pengguna sistem.	Pastikan umpan balik dari pengguna diintegrasikan untuk perbaikan.

Pengendalian Fisik

No.	Prosedur Audit	Keterangan Auditor/ Tanggal	Referensi Kertas Kerja	Hasil Pengujian Pengendalian Fisik
1.	Verifikasi akses fisik ke ruang server	12/04/2024	AA-01	Kebijakan akses fisik telah ditetapkan dan dipelihara. Daftar akses yang diotorisasi telah disusun dan diterapkan secara konsisten. Pemantauan akses dilakukan secara teratur.
2.	Pengecekan kunci dan kontrol akses	13/04/2024	AA-02	Penggunaan kunci ganda diterapkan pada semua ruang server. Pengelolaan kunci dilakukan secara ketat. Penggunaan kartu akses telah diimplementasikan.
3.	Evaluasi keamanan ruang server	14/04/2024	AA-03	Pendingin server berfungsi dengan baik. Sistem deteksi kebakaran dan pemadam kebakaran beroperasi dengan baik.
4.	Pengecekan keberadaan dan kondisi ruang penyimpanan	15/04/2024	AA-04	Sistem kebersihan, keamanan, dan pencegahan kebocoran terjaga. Sistem pengawasan kelembapan dan suhu berfungsi normal.
5.	Verifikasi keamanan ruang penyimpanan backup	16/04/2024	AA-05	Akses ke ruang penyimpanan backup terbatas hanya untuk personil yang ditunjuk. Prosedur pemantauan kebakaran telah diterapkan.

Pengendalian Lingkungan

No.	Prosedur Audit	Keterangan Auditor/ Tanggal	Referensi Kertas Kerja	Hasil Pengujian Pengendalian Lingkungan
1.	Evaluasi fisik lokasi pusat data	12/04/2024	A-01	Gedung pusat data dalam kondisi baik dan terjaga kebersihannya. Lokasi pusat data terlindungi dari potensi ancaman alam seperti banjir dan gempa.
2.	Pengecekan infrastruktur fisik (listrik, pendingin, dll)	13/04/2024	A-02	Sistem listrik dilengkapi dengan UPS dan generator cadangan. Sistem pendingin beroperasi dengan baik dan suhu terjaga optimal.
3.	Verifikasi sistem deteksi dan pemadaman kebakaran	14/04/2024	A-03	Detektor asap dan pemicu alarm diuji secara berkala dan berfungsi dengan baik. Sistem pemadam kebakaran dilengkapi dengan sprinkler dan alat pemadam portabel.
4.	Penilaian keberadaan dan pengelolaan bahan berbahaya	15/04/2024	A-04	Bahan berbahaya disimpan sesuai dengan standar keselamatan yang berlaku. Prosedur penanganan kebocoran dan kecelakaan telah ditetapkan dan dipahami oleh personil.
5.	Evaluasi keamanan akses fisik ke pusat data	16/04/2024	A-05	Sistem pengamanan akses termasuk kartu akses dan pengawasan CCTV.

Pengendalian Logis

No.	Prosedur Audit	Keterangan Auditor/ Tanggal	Referensi Kertas Kerja	Hasil Pengujian Pengendalian Logis
1.	Evaluasi kebijakan keamanan informasi	22/04/2024	B-01	Kebijakan keamanan informasi telah ditetapkan dan dipahami oleh personil terkait. Kebijakan keamanan informasi dijalankan dengan baik dan diikuti secara konsisten oleh seluruh personil.
2.	Penilaian kontrol akses dan otentikasi pengguna	23/04/2024	B-02	Prosedur pengelolaan identitas dan akses telah ditetapkan dan dijalankan dengan baik. Autentikasi kuat diterapkan untuk mengamankan akses ke sistem dengan efektif.
3.	Verifikasi keamanan sistem operasi	24/04/2024	B-03	Sistem operasi diperbarui secara berkala dan dikonfigurasi sesuai dengan keamanan. Kontrol akses pada sistem operasi diterapkan untuk membatasi hak akses pengguna. Konfigurasi firewall telah disusun untuk memantau dan mengatur lalu lintas jaringan.
4.	Pengecekan keamanan jaringan	25/04/2024	B-04	Sistem deteksi intrusi aktif dan berfungsi dengan baik untuk mendeteksi serangan. Konfigurasi firewall telah disusun untuk memantau dan mengatur lalu lintas jaringan.
5.	Evaluasi perlindungan data	26/04/2024	B-05	Data sensitif dienkripsi saat disimpan dan dikirimkan melalui jaringan. Kebijakan retensi data ditetapkan untuk memastikan data disimpan sesuai kebutuhan.

Pengendalian Operasi Sistem Informasi

No.	Prosedur Audit	Keterangan Auditor/ Tanggal	Referensi Kertas Kerja	Hasil Pengujian Pengendalian Operasi Sistem Informasi
1.	Evaluasi prosedur backup dan pemulihan data	27/04/2024	C-01	Proses backup data dilakukan secara rutin sesuai dengan kebijakan yang ditetapkan. Prosedur pemulihan data telah ditetapkan dan diuji untuk memastikan keefektifannya.
2.	Pengecekan keamanan pengelolaan sandi (password)	28/04/2024	C-02	Kebijakan sandi yang kuat diterapkan untuk mengamankan akses pengguna ke sistem. Autentikasi dua faktor diterapkan untuk meningkatkan keamanan akses pengguna.
3.	Verifikasi pengawasan akses ke sistem	29/04/2024	C-03	Akses pengguna dibatasi sesuai dengan peran dan tanggung jawab mereka dalam sistem. Akses dari jaringan eksternal dibatasi dan dimonitor untuk mencegah akses yang tidak sah.

No.	Prosedur Audit	Keterangan Auditor/ Tanggal	Referensi Kertas Kerja	Hasil Pengujian Pengendalian Operasi Sistem Informasi
4.	Pengecekan catatan aktivitas sistem (log)	30/04/2024	C-04	Proses pengumpulan dan pemantauan log aktivitas sistem berjalan secara teratur. Catatan log disimpan secara aman dan dijaga keasliannya untuk keperluan audit.
5.	Evaluasi prosedur penanganan insiden keamanan	01/05/2024	C-05	Prosedur pelaporan dan penanganan insiden keamanan telah ditetapkan dan diuji secara berkala. Tim tanggap darurat keamanan telah dibentuk dan dilatih untuk mengatasi insiden dengan cepat.

Jawaban Pertanyaan Pusat Data

NO	PERTANYAAN	Jawaban
1.	Apakah dilakukan evaluasi fisik lokasi pusat data?	Ya, evaluasi fisik lokasi pusat data dilakukan setiap tahun untuk memastikan keamanan bangunan.
2.	Bagaimana keamanan dan kebersihan gedung pusat data dipelihara?	Gedung pusat data dipelihara dengan baik oleh tim kebersihan dan keamanan yang ditugaskan.
3.	Apakah lokasi pusat data terlindungi dari potensi ancaman alam?	Ya, lokasi pusat data dilindungi dengan sistem peringatan dini dan peralatan keamanan tambahan.
4.	Bagaimana kondisi infrastruktur fisik (listrik, pendingin, dll) dari pusat data?	Infrastruktur fisik pusat data terawat dengan baik dan dilengkapi dengan perangkat cadangan.
5.	Apakah sistem listrik dilengkapi dengan UPS dan generator cadangan?	Ya, sistem listrik dilengkapi dengan UPS dan generator cadangan untuk memastikan kelangsungan.
6.	Bagaimana operasional sistem pendingin di pusat data?	Sistem pendingin pusat data dijalankan secara berkala dan diawasi untuk menjaga suhu optimal.
7.	Apakah sistem pemadam kebakaran berfungsi dengan baik?	Ya, sistem pemadam kebakaran diuji secara berkala dan siap digunakan dalam situasi darurat.
8.	Bagaimana keberadaan dan penyimpanan bahan berbahaya di pusat data?	Bahan berbahaya disimpan dalam ruang yang terpisah dan dipantau dengan ketat sesuai peraturan.
9.	Apakah prosedur penanganan kebocoran dan kecelakaan telah ditetapkan?	Ya, prosedur penanganan kebocoran dan kecelakaan telah ditetapkan dan dipraktekkan secara rutin.
10.	Bagaimana keamanan akses fisik ke pusat data?	Akses fisik ke pusat data dibatasi dan dipantau menggunakan kartu akses dan sistem CCTV.
11.	Apakah sistem pengamanan akses termasuk kartu akses dan pengawasan CCTV?	Ya, akses ke pusat data terbatas dan dipantau 24/7 menggunakan kartu akses dan kamera CCTV.

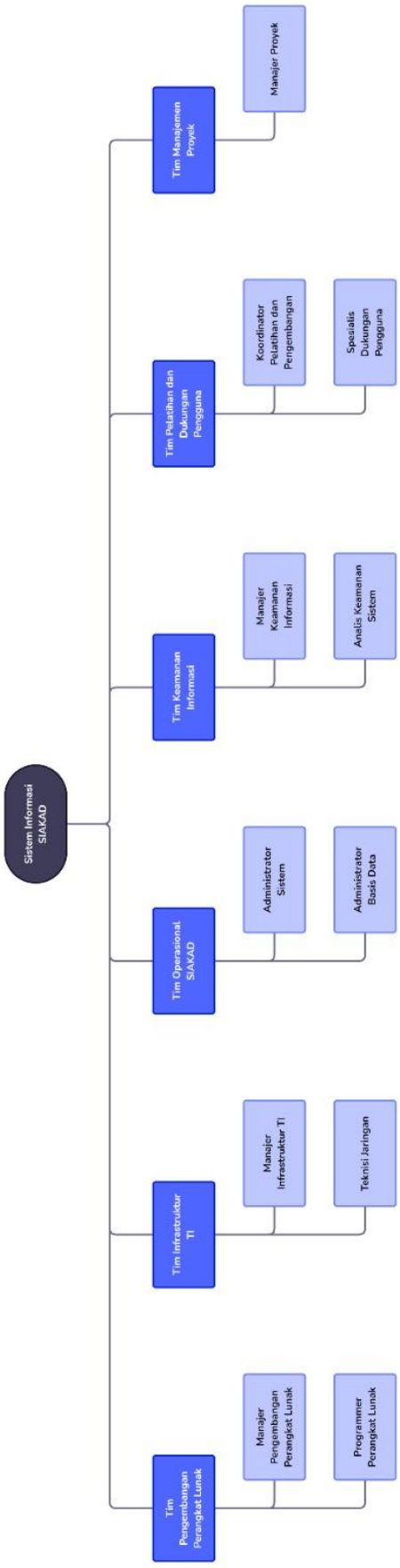
Jawaban Pertanyaan Keamanan IT

NO	PERTANYAAN	Jawaban
1.	Apakah dilakukan evaluasi keamanan jaringan dan infrastruktur IT?	Ya, evaluasi keamanan jaringan dan infrastruktur IT dilakukan secara berkala.
2.	Bagaimana pengelolaan hak akses dan otorisasi pengguna di sistem?	Pengelolaan hak akses dan otorisasi pengguna diatur melalui sistem manajemen hak akses.
3.	Apakah dilakukan pemantauan dan deteksi intrusi pada sistem?	Ya, sistem dilengkapi dengan perangkat pemantauan dan deteksi intrusi yang aktif.
4.	Bagaimana proses pengamanan data dan enkripsi informasi sensitif?	Proses pengamanan data meliputi enkripsi informasi sensitif dan penggunaan protokol yang aman.
5.	Apakah terdapat kebijakan dan prosedur untuk penanganan kejadian keamanan?	Ya, terdapat kebijakan dan prosedur yang telah ditetapkan untuk penanganan kejadian keamanan.
6.	Bagaimana manajemen patch dan pembaruan keamanan dilakukan?	Manajemen patch dan pembaruan keamanan dilakukan secara berkala sesuai dengan rencana yang telah ditetapkan.

Jawaban Pertanyaan Keamanan IT

NO	PERTANYAAN	Jawaban
1.	Bagaimana proses autentikasi dan otentikasi pengguna dilakukan?	Proses autentikasi dan otentikasi pengguna dilakukan melalui penggunaan mekanisme yang kuat dan terpercaya, seperti otentikasi dua faktor.
2.	Apakah dilakukan monitoring terhadap aktivitas pengguna pada sistem?	Ya, aktivitas pengguna pada sistem dipantau secara real-time menggunakan perangkat lunak pemantauan aktivitas.
3.	Bagaimana manajemen keamanan pada sistem operasi dan aplikasi dilakukan?	Manajemen keamanan pada sistem operasi dan aplikasi dilakukan dengan menerapkan kebijakan dan konfigurasi yang sesuai standar keamanan.
4.	Apakah terdapat prosedur untuk manajemen sandi dan kebijakan password?	Ya, terdapat prosedur yang telah ditetapkan untuk manajemen sandi dan kebijakan password, termasuk kebijakan rotasi sandi dan kompleksitas sandi.
5.	Bagaimana proses backup dan pemulihan data diatur?	Proses backup dan pemulihan data diatur dengan menjadwalkan backup secara berkala dan menguji prosedur pemulihan secara rutin.
6.	Apakah dilakukan penilaian rentang waktu pemeliharaan dan pembaruan sistem?	Ya, dilakukan penilaian rentang waktu pemeliharaan dan pembaruan sistem untuk memastikan sistem tetap up-to-date dengan patch keamanan terbaru.

BAGAN STRUKTUR DATA



ANTARMUKA PENGGUNAI UI