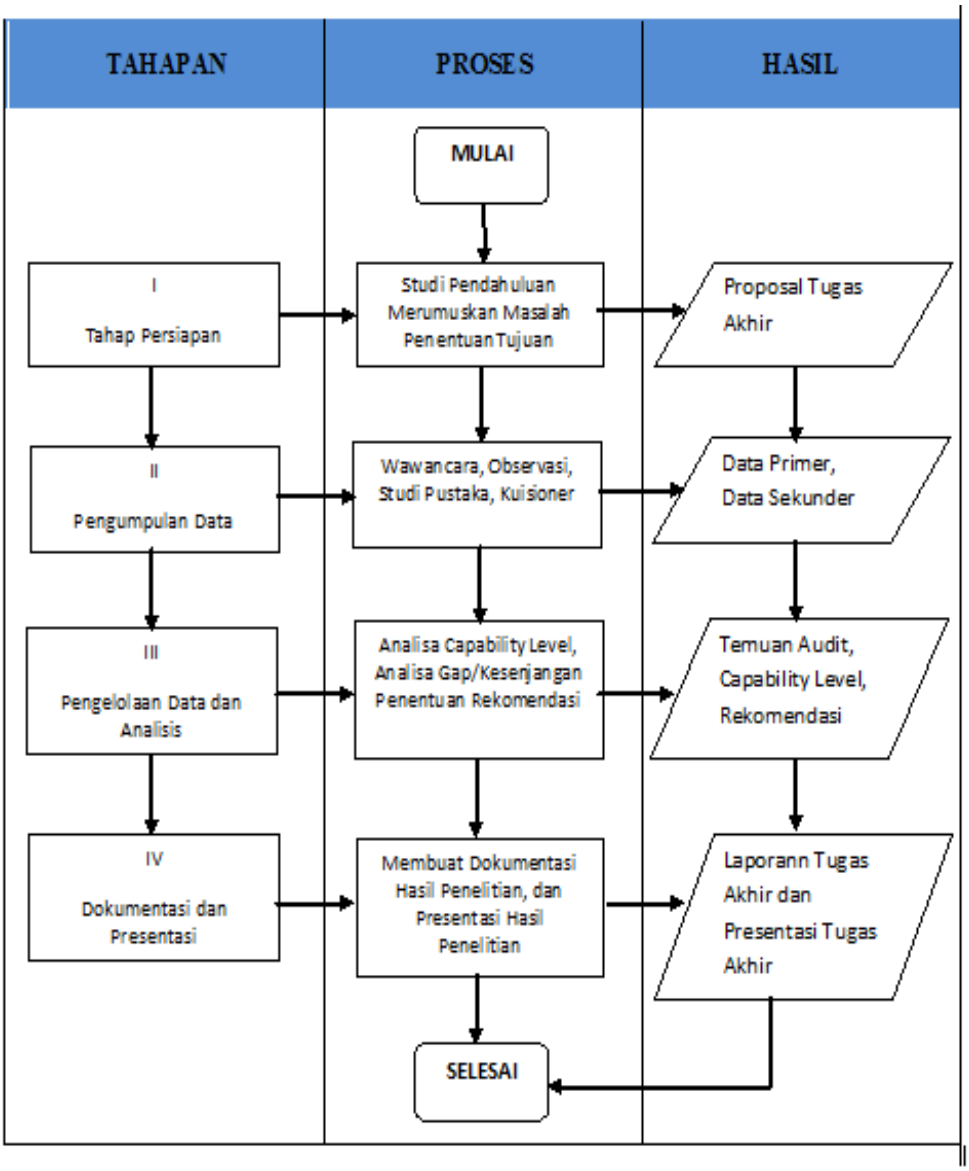
BAB III

METODOLOGI PENELITIAN

3.1 Kerangka Penelitian

Kerangka penelitian ini adalah langkah demi langkah dalam penyusunan tugas akhir mulai dari tahap persiapan penelitian hingga pembuatan dokumentasi tugas akhir.



Gambar 3.1 *Flowchart* Penelitian

3.2 Langkah – Langkah Penelitian

3.2.1. Tahap persiapan

Pada tahap ini yang dilakukan oleh peneliti adalah sebagai berikut:

1. Studi pendahuluan

   pendahuluan merupakan tahap awal penelitian, yaitu dengan melakukan observasi dan survei langsung ke lapangan untuk mengetahui permasalahan yang akan dijadikan sebagai bahan penelitian oleh peneliti.

2. Merumuskan masalah

   Agar memudahkan peneliti dalam menentukan konsep-konsep teoritis yang ditelaah dan memilih metode penguji data yang tepat maka diperlukan rumusan masalah. Berdasarkan identifikasi masalah yang ada, maka dirumuskan permasalahan pada penelitian ini yaitu bagaimana menerapkan *Control Objectives For Information and Related Technology Framework* (COBIT) 5 dalam melakukan audit terhadap sistem informasi akademik (SISKA) IIB DARMAJAYA.

3. Tujuan penelitian

   Tujuan penelitian adalah maksud akhir dari penelitian, hal ini berdasarakan pada rumusan masalah. Tujuan penelitian adalah jawaban dari masalah-masalah yang telah dirumuskan.

3.2.2. Tahap Pengumpulan Data

Tahap pengumpulan data merupakan faktor penting dalam keberhasilan penelitian yang akan dilakukan. Tahap ini dilakukan untuk memperoleh informasi yang terkait dengan penelitian yang akan diteliti sehingga tujuan yang diinginkan dapat tercapai. Berikut metode pengumpulan data yang dilakukan dalam penelitian ini:

3.2.2.1 Observasi

Observasi yang dilakukan di Institut Informatika dan Bisnis (IIB) DARMAJAYA LAMPUNG bertujuan untuk mengidentifikasi dan mencari beberapa informasi yang dapat dikumpulkan. Pengumpulan data melalui observasi yang dilakukan dengan melihat langsung bagaimana sistem dan pelayanan yang diberikan oleh SISKA.

3.2.2.2 Wawancara

Metode ini dilakukan dengan cara diskusi dengan bagian ICT Center dan mahasiswa IIB DARMAJAYA. Metode ini dilakukan untuk mendapatkan data lebih mendalam dengan bertatapan langsung dengan narasumber. Wawancara ini berguna untuk memperoleh data-data yang diperlukan dalam analisis terhadap proses bisnis yang saat ini berjalan diinstansi terkait terutama pada bagian yang terkait dengan sistem informasi akdemik (SISKA) IIB DARMAJAYA.

3.2.2.3 Kajian Literatur

Kajian literatur dilakukan dengan mengumpulkan data-data berupa deskripsi atau penjelasan yang berhubungan dengan yang diteliti. Pengumpulan data dilakukan dengan meninjau ulang beberapa jurnal, skripsi dan buku-buku yang terkait dengan penelitian yang akan dilakukan yang membahas mengenai audit teknologi informasi, COBIT 5, serta teori *capability level* sebagai penilaian tingkat kematangan dari teknologi informasi yang digunakan. Kajian literatur digunakan untuk mendapatkan sejauh mana yang sudah dilakukan oleh orang lain dan bagai mana mengerjakannya, dan melakukan penelitian apa yang berbeda dari apa yang kita lakukan dalam penelitian.kajian literatur ini digunakan untuk menambah referensi teori – teori yang dibutuhkan

dalam penelitian dengan mempelajariliteratur yang turut menddukung penelitian.

3.2.2.4 Kuesioner

Pada penelitian ini, audit teknologi pada SISKA IIB DARMAJAYA dalam pengelolaan kualitas layanan dengan pihak internal dan eksternal instansi akan dilakukan pada domain *Deliver, Support and Service* (DSS) serta *Align, Plan, and Organize* (APO) dari *framework* COBIT 5. Untuk mendapatkan data yang dibutuhkan dalam penelitian ini, maka dibuatlah kuesioner yang dikembangkan dari *framework* COBIT 5.

Kuesioner dibuat berdasarkan *Key Management Practice* dalam COBIT 5 yaitu dengan menggunakan domain DSS (*Deliver, Service and Support*) pada proses DSS 5(*Manage Scutity Services*) dan domain APO (*Align, Plan, and Organize*) pada proses APO13 (*Manage Scurity*).

a. Proses DSS05 *Mange Scurity Services* (Mengelola Layanan Keamanan)

Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Menetapkan dan memelihara peran keamanan informasi dan hak akses dan melakukan pemantauan keamanan.

- Tujuan

  Meminimalkan dampak bisnis dari kerentanan keamanan informasi operasional dan insiden.

- *Output*

  a. Keamanan jaringan dan komunikasi terpenuhi
  b. Informasi yang diproses, disimpan dan dikirim oleh perangkat endpoint terlindungi

c. Semua pengguna dikenali secara unik dan memiliki hak akses sesuai dengan peran bisnis mereka.
d. Tindakan fisik telah diterapkan untuk melindungi informasi dari akses, kerusakan dan gangguan yang tidak sah saat diproses, disimpan atau dikirim.
e. Informasi elektronik diamankan dengan benar saat disimpan, dikirim atau dimusnahkan.

- *Bese Practice* (*Activity*)

a. Melindungi terhadap malware.

Melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (mis., Virus, worm, spyware, spam).

b. Kelola keamanan jaringan dan konektivitas.

Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas

c. Mengelola keamanan titik akhir.

Pastikan titik akhir (mis., Laptop, desktop, server dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditetapkan dari informasi yang diproses, disimpan atau dikirim.

d. Mengelola identitas pengguna dan akses logis.

Pastikan semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis.

e. mengeelola akses fisik ke aset TI.

Tentukan dan terapkan prosedur untuk memberi, membatasi dan mencabut akses ke bangunan, bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau. Ini harus berlaku untuk semua orang yang memasuki tempat itu, termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga lainnya.

f. Mengelola dokumen sensitif dan perangkat output.

Menetapkan pengamanan fisik, praktik akuntansi dan pengelolaan persediaan yang tepat atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau token keamanan.

g. Memantau infrastruktur untuk acara yang berhubungan dengan keamanan.

Menggunakan alat deteksi intrusi, memantau infrastruktur untuk akses yang tidak sah dan memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian secara umum.

b. Proses APO 13 *Manage Scurity* (Mengelola Keamanan)

Mentukan mengoperasikan dan memonitor sistem pengelolaan keamanan informasi.

- Tujuan

  Pertahankan dampak dan kejadian insiden keamanan informasi di dalam tingkat risk appetite perusahan.

- *Output*
  a. Suatu sistem ada di tempat yang mempertimbangkan dan secara efektif menangani persyaratan keamanan informasi perusahaan.
  b. Rencana keamanan telah ditetapkan, diterima dan dikomunikasikan ke seluruh perusahaan.
  c. Solusi keamanan informasi diimplementasikan dan dioperasikan secara konsisten di seluruh perusahaan.

- *Bese Practice (Activity)*
  a. **Menetapkan dan memelihara sistem manajemen keamanan informasi (ISMS).**

     Menetapkan dan memelihara ISMS yang memberikan pendekatan standar, formal dan berkesinambungan terhadap manajemen keamanan untuk mendapatkan informasi, memungkinkan proses teknologi dan bisnis yang aman yang sesuai dengan persyaratan bisnis dan manajemen keamanan perusahaan.

  b. **Mentukan dan mengeelola rencana penanganan risiko keamanan informasi.**

     Menjaga rencana keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan disesuaikan dengan strategi perusahaan dan arsitektur perusahaan. Memastikan bahwa rekomendasi untuk menerapkan perbaikan keamanan didasarkan pada kasus bisnis yang disetujui dan diterapkan sebagai bagian integral dari pengembangan layanan dan solusi, kemudian dioperasikan sebagai bagian integral dari operasi bisnis.

c. Mantau dan meninjau ISMS.

Menjaga dan secara teratur mengkomunikasikan kebutuhan akan, dan manfaat, perbaikan keamanan informasi terus-menerus. Mengumpulkan dan menganalisa data tentang ISMS, dan memperbaiki keefektifan ISMS Benar ketidaksesuaian untuk mencegah kekambuhan. Promosikan budaya keamanan dan perbaikan terus-menerus.

Tahap awal yang dilakukan untuk mengetahui tingkat kapabilitas adalah dengan membuat kuesioner. Kuesioner diartikan sebagai alat (*tool*) dalam membantu untuk mengumpulkan data berdasarkan fokus proses DSS5 dan APO13 pada COBIT 5. Objek pertanyaan pada *Capability Level* dikembangkan dari deskripsi model tingkat kapabilitas COBIT 5 pada proses DSS5 dan APO13. Pengukuran yang digunakan dalam menjawab pertanyaan dari kuesioner yang disusun menggunakan skala Likert yaitu dengan penilaan 5 (Sangat Baik), 4 (Baik),3 (Cukup), 2 (Tidak Baik), 1 (Sangat Tidak Baik) . Data diolah menggunakan Ms Excel dan program aplikasi Netbeans.

Tabel 3.1 Kuisioner Untuk User

NO	PERTANYAAN	PERFORMANCE					EXPECTACY				
		5	4	3	2	1	5	4	3	2	1
DSS5 MANAGE SCURITY SERVICE											
1	Seberapa baik pihak ICT dalam melakukan pencegahan terhadap malware yang dapat merusak sistem serta keamanan data ?										
2	Seberapa baik pihak ICT dalam melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (mis., Virus, worm, spyware, spam)?										
3	Seberapa baik pihak ICT dalam memasikan bahwa semua Informasi yang diproses, disimpan dan dikirim oleh perangkat endpoint terlindungi dari serangan maleware atau lainnya?										
4	Seberapa baik pihak ICT dalam mengelola keamanan jaringan dan konektivitas sesuai standar yang telah ditentukan?										
5	Seberapa baik pihak ICT dalam menggunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk										

	melindungi informasi dari semua metode konektivitas?										
6	Seberapa baik pihak ICT dalam memastikan bahwa keamanan jaringan dan komunikasi sudah memenuhi kebutuhan bisnis instansi ?										
7	Seberapa baik pihak ICT dalam memastikan keamanan sistem hingga sampai pada titik akhir (end point)?										
8	Seberapa baik pihak ICT dalam memastikan titik akhir (misalnya : Laptop, desktop, server dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditetapkan dari informasi yang diproses, disimpan atau dikirim?										
9	Seberapa baik pihak ICT dalam menggunakan teknik keamanan dan prosedur pengelolaan terkait (contoh :firewalls, perangkat keamanan, segmentasi jaringan,deteksi kekacauan) untuk otorisasi akses dan mengendalikan alur informasi dari dan menuju jaringan?										
10	Seberapa baik pihak ICT dalam memastikan bahwa semua pengguna (user)dikenali secara unik dan memiliki hak akses sesuai dengan peran kebutuhan pengguna (user)?										

11	Seberapa baik pihak ICT dalam mengelola identitas pengguna(user) dan akses secara logis?										
12	Seberapa baik pihak ICT dalam memastikan semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis (perkuliahan)?										
13	Seberapa baik pihak ICT telah menerapkan tindakan untuk melindungi informasi dari akses, kerusakan dan gangguan yang tidak sah saat diproses, disimpan atau dikirim?										
14	Seberapa baik pihak ICT dalam mengelola akses fisik ke aset TI,menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut izin akses ke bangunan? (sistem), bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat?										
15	Seberapa baik pihak ICT dalam memberikan hak aksess ke sistem, dan telah dibenarkan, disahkan, dicatat dan dipantau untuk semua user yang memasuki sistem , termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga lainnya?										

16	Seberapa baik pihak ICT dalam mengelola dokumen sensitif (privasi) dan perangkat output secara optimal?										
17	Seberapa baik pihak ICT dalam menetapkan pengamanan fisik, praktik akuntansi dan pengelolaan persediaan yang tepat atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan?										
18	Seberapa baik pihak ICT dalam melakukan penukaran data transaksi sensitif hanya melalui jalur atau media dengan kendali untuk menyediakan keaslian konten?										
19	Seberapa baik pihak ICT dalam memantau infrastruktur untuk hal yang berhubungan dengan keamanan?										
20	Seberapa baik pihak ICT dalam menggunakan alat deteksi untuk memantau infrastruktur untuk mengetahui akses yang tidak sah?										
21	Seberapa baik pihak ICT dalam memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian secara umum sesuai standar?										
APO 13 MANAGE SCURITY											
22	Seberapa baik pihak ICT dalam										

	menetapkan dan memelihara ISMS (Information Scurity Managenemt Sistem) yang memberikan pendekatan standar, formal dan berkesinambungan terhadap manajemen keamanan untuk mendapatkan informasi?										
23	Seberapa baik pihak ICT dalam memastikan bahwa dengan menetapkan ISMS (Information Scurity Managenemt Sistem) proses teknologi dan bisnis yang aman yang sesuai dengan persyaratan bisnis dan manajemen keamanan perusahaan?										
24	Seberapa baik pihak ICT dalam mempertimbangkan dan secara efektif telah menangani persyaratan keamanan informasi perusahaan?										
25	Seberapa baik pihak ICT dalam menetukan dan mengelola rencana penanganan risiko keamanan informasi?										
26	Seberapa baik pihak ICT dalam menjaga rencana keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan disesuaikan dengan strategi perusahaan dan arsitektur perusahaan?										
27	Seberapa baik pihak ICT dalam emastikan bahwa rekomendasi untuk menerapkan perbaikan keamanan didasarkan pada										

	kasus bisnis yang disetujui dan diterapkan sebagai bagian integral dari pengembangan layanan dan solusi, kemudian dioperasikan sebagai bagian integral dari operasi bisnis?										
28	Seberapa baik pihak ICT dalam memantau dan meninjau ISMS (Information Scurity Managenemt Sistem) agar solusi keamanan informasi diimplementasikan dan dioperasikan secara konsisten di seluruh perusahaan?										
29	Seberapa baik pihak ICT dalam menjaga dan secara teratur mengkomunikasikan kebutuhan akan, dan manfaat, perbaikan keamanan informasi terus-menerus?										
30	Seberapa baik pihak ICT dalam Mengumpulkan dan menganalisa data tentang ISMS, dan memperbaiki keefektifan ISMS Benar ketidaksesuaian untuk mencegah kerusakan/resiko, serta telah memromosikan budaya keamanan dan perbaikan terus-menerus?										

Tabel 3.2 Kuisioner untuk manajemen

NO	PERTANYAAN	PERFORMANC					EXPECTACY				
		5	4	3	2	1	5	4	3	2	1
DSS5 MANAGE SCURITY SERVICE											
1	Pihak ICT telah melakukan pencegahan terhadap malware yang dapat merusak sistem serta keamanan data										
2	Pihak ICT telah melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama patch keamanan dan pengendalian virus terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (mis., Virus, worm, spyware, spam).										
3	Pihak ICT telah memasikan bahwa semua Informasi yang diproses, disimpan dan dikirim oleh perangkat endpoint terlindungi dari serangan maleware atau lainnya										
4	Pihak ICT telah mengelola keamanan jaringan dan konektivitas sesuai standar yang telah ditentukan										
5	Pihak ICT telah menggunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas										
6	Pihak ICT telah memastikan bahwa keamanan jaringan dan komunikasi sudah memenuhi kebutuhan bisnis instansi										

7	Pihak ICT telah memastikan keamanan sistem hingga sampai pada titik akhir (end point)										
8	Pihak ICT telah memastikan titik akhir (misalnya : Laptop, desktop, server dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditetapkan dari informasi yang diproses, disimpan atau dikirim.										
9	Pihak ICT telah menggunakan teknik keamanan dan prosedur pengelolaan terkait (contoh :firewalls, perangkat keamanan, segmentasi jaringan,deteksi kekacauan) untuk otorisasi akses dan mengendalikan alur informasi dari dan menuju jaringan										
10	Pihak ICT telah memastikan bahwa semua pengguna (user)dikenali secara unik dan memiliki hak akses sesuai dengan peran kebutuhan pengguna (user)										
11	Pihak ICT telah mengelola identitas pengguna(user) dan akses secara logis										
12	Pihak ICT telah memastikan semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis (perkuliahan).										

13	Pihak ICT telah menerapkan tindakan untuk melindungi informasi dari akses, kerusakan dan gangguan yang tidak sah saat diproses, disimpan atau dikirim.										
14	Pihak ICT telah mengelola akses fisik ke aset TI,menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut izin akses ke bangunan (sistem), bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat.										
15	Pihak ICT telah memberikan hak aksess ke sistem, dan telah dibenarkan, disahkan, dicatat dan dipantau untuk semua user yang memasuki sistem , termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga lainnya										
16	Pihak ICT telah mengelola dokumen sensitif (privasi) dan perangkat output secara optimal										
17	Pihak ICT Telah menetapkan pengamanan fisik, praktik akuntansi dan pengelolaan persediaan yang tepat atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan.										
18	Pihak ICT telah melakukan penukaran data transaksi sensitif hanya melalui jalur atau media dengan kendali untuk menyediakan keaslian konten.										
19	Pihak ICT telah memantau infrastruktur untuk hal yang berhubungan dengan										

	keamanan										
20	Pihak ICT telah menggunakan alat deteksi untuk memantau infrastruktur untuk mengetahui akses yang tidak sah.										
21	Pihak ICT telah memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian secara umum sesuai standar										
APO 13 MANAGE SCURITY											
22	Pihak ICT telah menetapkan dan memelihara ISMS (Information Scurity Managenemt Sistem) yang memberikan pendekatan standar, formal dan berkesinambungan terhadap manajemen keamanan untuk mendapatkan informasi.										
23	Pihak ICT telah memastikan bahwa dengan menetapkan ISMS (Information Scurity Managenemt Sistem) proses teknologi dan bisnis yang aman yang sesuai dengan persyaratan bisnis dan manajemen keamanan perusahaan.										
24	Pihak ICT telah mempertimbangkan dan secara efektif telah menangani persyaratan keamanan informasi perusahaan.										
25	Pihak ICT telah menetukan dan mengelola rencana penanganan risiko keamanan informasi										

26	Pihak ICT telah menjaga rencana keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan disesuaikan dengan strategi perusahaan dan arsitektur perusahaan										
27	Pihak ICT telah emastikan bahwa rekomendasi untuk menerapkan perbaikan keamanan didasarkan pada kasus bisnis yang disetujui dan diterapkan sebagai bagian integral dari pengembangan layanan dan solusi, kemudian dioperasikan sebagai bagian integral dari operasi bisnis.										
28	Pihak ICT telah memantau dan meninjau ISMS (Information Scurity Managenemt Sistem) agar solusi keamanan informasi diimplementasikan dan dioperasikan secara konsisten di seluruh perusahaan.										
29	Pihak ICT telah menjaga dan secara teratur mengkomunikasikan kebutuhan akan, dan manfaat, perbaikan keamanan informasi terus-menerus.										
30	Pihak ICT telah Mengumpulkan dan menganalisa data tentang ISMS, dan memperbaiki keefektifan ISMS Benar ketidaksesuaian untuk mencegah kerusakan/resiko, serta telah memromosikan budaya keamanan dan perbaikan terus-menerus.										

3.2.2.5 Sumber Data

Sumber data dalam penelitian ini dibedakan menjadi dua jenis yaitu :

a. Data Primer

   Data primer merupakan data yang diperoleh langsung dari obyek penelitian. Data primer dapat berupa pendapat dari responden baik individu maupun kelompok, data observasi, terhadap suatu benda, kegiatan atau kejadian. Data primer mencerminkan kenyataan yang benar-benar terjadi di obyek penelitian.

b. Data Sekunder

   Data sekunder merupakan data yang diperoleh secara tidak langsung atau melalui perantara. Contoh data sekunder seperti buku, *ebook*, jurnal penelitian, laporan perusahaan, dan lain-lain. Data sekunder memiliki manfaat yaitu meminimalkan biaya dan waktu, mengklasifikasikan permasalahan, dan mengetahui tingkat kesenjangan informasi.

3.2.2.6 Gambaran Umum Biro ICT Center

Untuk melakukan audit pada bagian ICT Center IIB DARMAJAYA Lampung secara efesien, penulis mengevaluasi terlebih dahulu data skunder instansi yaitu identitas, visi, misi, struktur organisasi, dari biro ICT Center IIBI DARMAJAYA. Data sekunder merupakan gambaran umum yang menjelaskan tentang biro ICT Center IIB DARMAJAYA dan akan diuraikan sebagai berikut.

3.2.2.6.1 Identitas Biro ICT Center IIB DARMAJAYA

ICT Center merupakan Biro di IIB Darmajaya yang menangani Teknologi Informasi yang meliputi, *Network Infrastructure*,

Software Developer , *Data Center* , Management Laboratorium Komputer , Keamanan Jaringan, Pengolahan Data, dan sebagainya mengenai ICT. Dahulu Biro ini dinamakan UPT PUSKOM (Pusat Komputer), Seiring dengan meluasnya bidang layanan dan pengerjaan maka dirubah dengan nama ICT Center (*Information & Communication Technology*).

Dalam perkembangan Teknologi Informasi dan Komputer, ICT Center selalu berusaha meng-update sistem mengikuti perkembangan zaman, tidak hanya sebatas sistem , hardware, teknologi , tetapi dari Sumber Daya Manusia pada Biro ICT Center terus dilakukan peng-upgrade-tan skill, sehingga Produk dan layanan ICT Center bisa selalu *Up to Date.*

3.2.2.6.2 Visi Biro ICT Center IIB DARMAJAYA

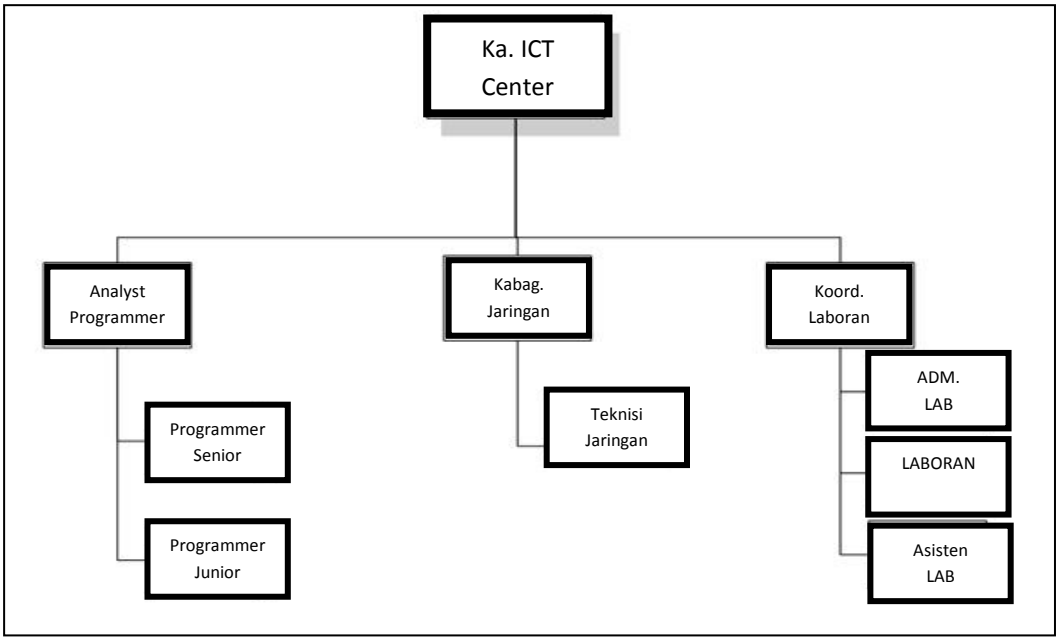
Menjadi pusat teknologi informasi dan komunikasi yang handal, unggul, kreatif dan inovatif dalam mengembangkan sistem-sistem pendukung demi tercapainya visi dan terlaksananya misi institusi.

3.2.2.6.3 Misi Biro ICT Center IIB DARMAJAYA

1. Secara berkesinambungan merencanakan dan mengembangkan sistem-sistem informasi dilingkungan IIB DARMAJAYA sehingga terwujud suatu sistem teritegrasi yang menunjang seluruh proses bisnis dan meningkatkan daya saing institusi.
2. Melakukan perencanaan, pengembangan, pengelolaan dan perawatan perangkat teknologi yang dimiliki sehingga siap mendukung pelaksanaan kegiatan institusi secara maksimal

3.2.2.6.4 Struktur Biro ICT Center IIB DARMAJAYA

Berikut adalah gambaran struktur organisasi di biro ICT Center IIB DARMAJAYA :



Gambar 3.2 Struktur Organisasi biro ICT Center

- Programmer

  Bagian Programmer ICT Center dipimpin oleh Analyst Programmer, Bagian Programmer bertanggung jawab atas seluruh Sistem Informasi yang ada di IIB Darmajaya, pembuatan sistem informasi ataupun perawatan sistem informasi. Bagian Programmer memiliki 2 bagian yaitu, Senior Programmer, dan Junior Programmer. Sistem Informasi yang dibuat meliputi berbasis desktop, Java , Web dan Mobile, serta mengikuti perkembangan zaman akan teknologi terkini.

- Jaringan dan Komputer

  Bagian Jaringan & Komputer Bertanggung jawab pada infrastruktur , pengelolaan dan perawatan Jaringan Komunikasi dan Informasi di IIB Darmajaya, pengelolaan Data Center, Teknologi

Nirkabel, Local Area Network (LAN) , Internet , Intranet , Keamanan Jaringan dan sebagainya yang berkenaan dengan Jaringan & Komputer.

- Laboratorium

  Laboratorium Komputer merupakan salah satu hal yang penting dalam kegiatan pengajaran, merupakan sebagai penunjang perkuliahan di IIB DARMAJAYA. Sebelumnnya Laboratorium Komputer berada dibawah jurusan masing – masing, dan pada akhirnya saat ini dikelola oleh ICT Center IBI DARMAJAYA dikarenakan untuk mempermudah Kontrol dan pengelolaan di bidang ICT yang ada di IBI DARMAJAYA.

3.2.2.6.5 Proses Bisnis Biro ICT Center

1. Data Center

a. Dedicated Server

   Dedicated Server adalah sebuah server fisik (komputer dengan spesifikasi dan konfigurasi tertentu) yang mampu menjalankan proses komputasi dari aplikasi berat dan beban yang sangat tinggi. Dedicated Server merupakan solusi dari shared hosting ataupun VPS yang tidak mampu menjalankan aplikasi berat dengan proses komputasi yang kompleks ini.Dedicated Server biasanya digunakan oleh perusahaan-perusahaan bersekala menengah keatas dimana perusahaan tersebut memiliki system informasi yang membutuhkan keamanan ekstra. Mereka lebih memilih Dedicated Server dari pada shared hosting atauVPS dikarenakan Dedicated Server dinilai lebih powerfull.

b. Shared Hosting

Shared hosting adalah layanan hosting dimana sebuah account hosting diletakan bersama-sama beberapa account hosting lain dalam satu server yang sama, dan memakai services bersama-sama. Keuntungan shared hosting adalah harganya yang murah, namun kerugiannya adalah tingkat privasi dan performa yang tidak sebaik Dedicated Hosting.

c. Colocation Server

Colocation server adalah adalah server yang dititipkan ke suatu tempat yang aman untuk menyimpan server yang memiliki standar dan keamanan penyimpanan server yang memadai. Biasanya tempat untuk menyimpan server tersebut bernama data center atau colocation. Alasan menyimpan server di data center adalah untuk menghindari berbagai hal yang mungkin akan menjadi penghambat dan penghalang eksistensi data yang tersimpan dalam sever akibat dari tidak stabilnya arus listrik yang menyuplai server, kurang stabilnya akses internet serta keamanan yang tinggi.

2. Network Infrastructure

ICT Center memfasilitasi setiap Sivitas Akademika IBI Darmajaya untuk dapat menerima informasi atau bertukar informasi dilinkungan IIB DARMAJAYA atau External IBI Darmajaya dengan membuat, memetakan kebutuhan jaringan baik sekala kecil maupun sekala besar dengan menggunakan topology terkini, teknologi terkini dan keamanan dari jaringan tersebut, serta pemeliharaan rutin pada jaringan tersebut.

3. Software Developer

   Pengembang perangkat lunak (Inggris: Software Developer) adalah individu, komunitas atau perusahaan yang membuat perangkat lunak. Pengembang perangkat lunak kemudian mengkhususkan diri untuk mengembangkan perangkat lunak kategori tertentu misalnya Sistem Operasi, RDBMS, web server, bahasa pemrograman dan lain-lain.

4. Network Scurity

   Keamanan jaringan (Bahasa Inggris: Network Security) dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan.

3.2.3 Tahap Pengelolaan Data dan Analisa

3.2.3.1 Analisa Tingkat Kapabilitas (*Capability Level*)

Analisa tingkat kapabilitas dilakukan berdasarkan hasil kuesioner mengenai audit teknologi informasi terkait proses layanan SISKA IIB DARMAJAYA yang mengacu pada *best practice framework* COBIT 5 domain DSS (*Deliver,Service, and Support*) dan domain APO13 (*Align, Plan, and Organize*). Pada tahap ini peneliti melakukan validasi terhadap kuesioner yang telah dijawab oleh para responden , meliputi rekapitulasi jawaban masing-masing responden, rekapitulasi hasil perhitungan kuesioner dengan menggunakan skala likert pada masing- masing proses, sampai tahap interpretasi data yang menunjukan posisi *capability level* saat ini dan *capability level* yang diharapkan sampai nilai maksimum *capability level.* Perhitungan kuesioner yang akan dilakukan pada penelitian ini adalah sebagai berikut:

a. Pembuatan kuesioner dilakukan dengan menggunakan skala likert sebagai acuan.

b. Setiap kriteria pada kuesioner yaitu 5 (Sangat Baik), 4 (Baik), 3 (Cukup), 2 (Tidak Baik), 1 (Sangat Tidak Baik).

c. Hasil konversi kemudian akan dilakukan normalisasi dengan membagi nilai total dengan jumlah pertanyaan yang ada pada setiap level, kemudian setelah dilakukan normalisasi dilakukan perhitungan rata-rata dengan membagi total nilai jawaban dengan jumlah responden.

d. Dari hasil perhitungan tersebut didapatkan hasil akhir yang kemudian dapat dikategorikan sesuai aturan berikut:

Tabel 3.3 Penilaian kapabilitas

Rentang Nilai	Nilai Kapabilitas	Tingkat Kapabilitas
0-0,50	0,00	0 *Incomplete Process*
0,51-1,50	1,00	1 *Performed Process*
1,51-2,50	2,00	2 *Managed Process*
2,51-3,50	3,00	3 *Established Process*
3,51-4,50	4,00	4 *Predictable Process*
4,51-5,00	5,00	5 *Optimizing Process*

3.2.3.2 Analisa Kesenjangan (GAP)

Setelah dapat menemukan temuan-temuan dari hasil perhitungan *capability level* maka penulis dapat menganalisa kesenjangan apa yang terdapat dari hasil temuan tersebut. Dalam penentuan *gap* yang dilakukan, didapat dari analisis hasil dari kuesioner yang menghasilkan selisih dari tingkat kapabilitas yang diperoleh dengan tingkat yang diharapkan.

3.2.3.3 Penentuan Rekomendasi

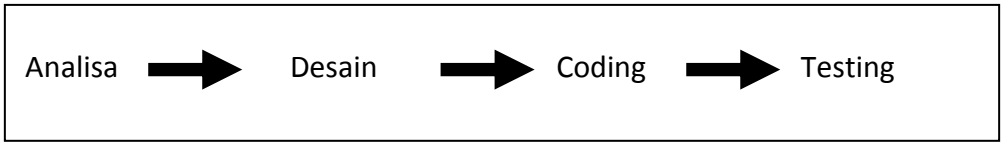
Penentuan rekomendasi berdasarkan pada temuan audit dari hasil penelitian, penentuan rekomendasi ini bertujuan untuk memberikan pandangan kepada pihak manajemen yang mengarah kepada perbaikan proses yang mengacu pada peningkatan level kematangan.

3.2.4 Dokumentasi dan Presentasi

Pada tahap ini yang dilakukan adalah melakukan dokumentasi hasil dari tahap – tahap yang dilakukan sebelumnya, mulai dari pengumpulan data, pengolahan data dan pelaksanaan audit. Hasil dokumentasi tersebut digunakan sebagai rekomendasi atau masukan bagi pihak Biro ICT Center.

3.3 Metode Pengembangan Perangkat Lunak

Metode yang akan digunakan dalam pengembangan perangkat lunak yaitu model *waterfall.* Pada tahap ini penulis memerlukan bantuan untuk menghasilkan suatu rancangan dalam membuat sebuah Perancangan dan Implementasi aplikasi untuk melakukan audit menggunakan framework COBIT 5.



Gambar 3.3 Metode Pengembangan Sistem (Waterfall)

3.3.1 Analisa

- Analisa Kebutuhan

a. Hardware

Satu unit laptop dengan spesifikasi :

- Intel pentium
- Ram 2 GB
- Hardidisk 500 GB
- VGA 2 GB

b. Software

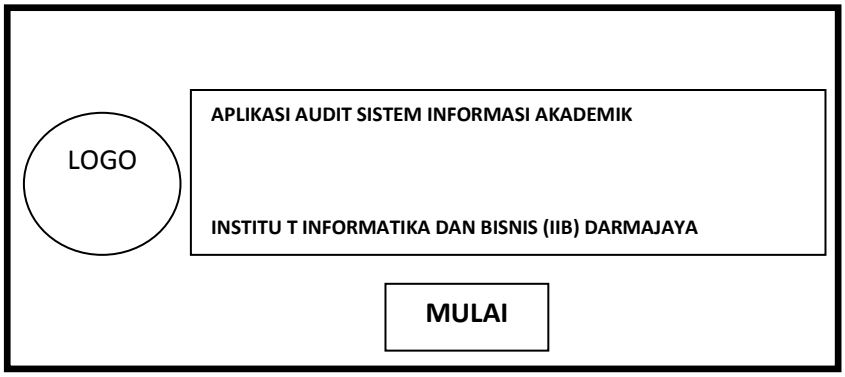
- Microsoft Excel
- JDK 8
- Netbeans IDE 8.01.
- Xampp Control Panel
- PHP MyQQL

3.3.2 Desain

Desain merupakan tampilan aplikasi untuk memudahkan user dalam melakukan pengisian kuisioner untuk menemukan hasil ouputan untuk mengambil kesimpulan. Berikut adalah rancangan desain interface :

- **Tampilan Halaman Awal**

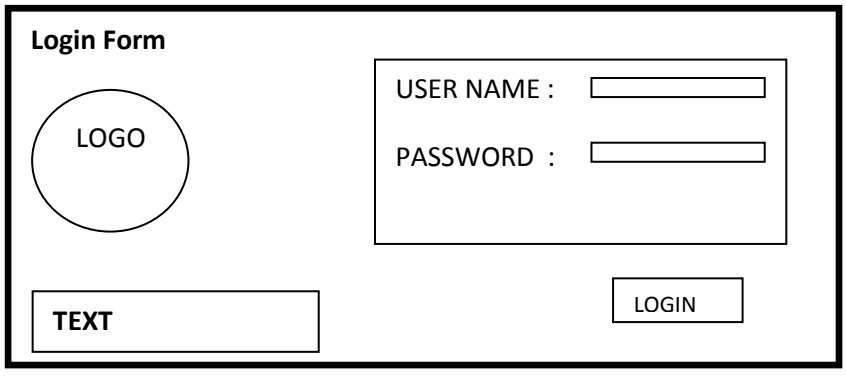
  Merupakan halaman pertama yang akan ditampilkan saat pengguna mengakses aplikasi ini. Pada halaman ini, layar akan menampilkan tulisan “Aplikasi Audit Sistem Informasi Institut Informatika dan Bisnis (IIB) Darmajaya Menggunakan Framework COBIT 5”, logo IIB Darmajaya, serta tombol *botton* “Mulai”.Setelah kita memilih tombol *button* “mulai” maka akan menuju ke halaman selanjutnya. Rancangan form dapat dilihat pada gambar 3.4



Gambar 3.4 Rancangan Tampilan *Form* Halaman Awal

- **Tampilan Halaman Login**

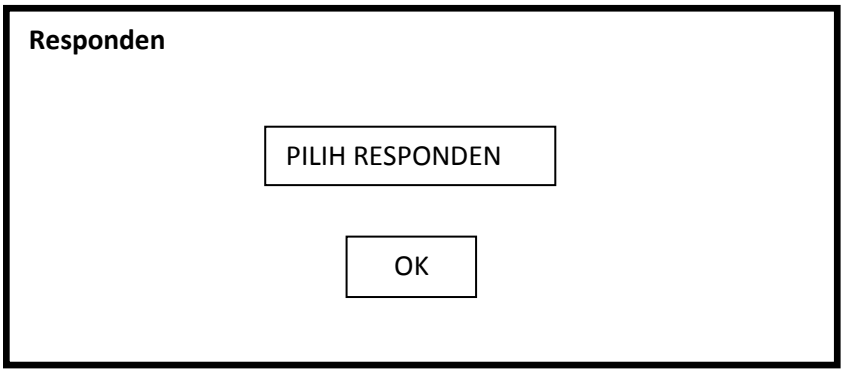
  Merupakan halaman yang dijadikan autentikasi untuk masuk kedalam aplikasi. Pada halaman ini, layar akan menampilkan isian yang terdiri dari username , password, dan tombol *"login".* Ketika user memasukkan username dan password dengan benar kemudian memilih tombol login maka akan muncul tampilan pesan "login berhasil"dan menuju kehalaman selanjutnya. Ketika user memasukkan username dan password salah kemudian memilih tombol login maka akan muncul tampilan pesan "login gagal". Rancangan halaman login dapat dilihat pada gambar 3.5.



Gambar 3.5. Rancangan Tampilan *Form* Halaman *Login.*

- **Tampilan Halaman Responden**

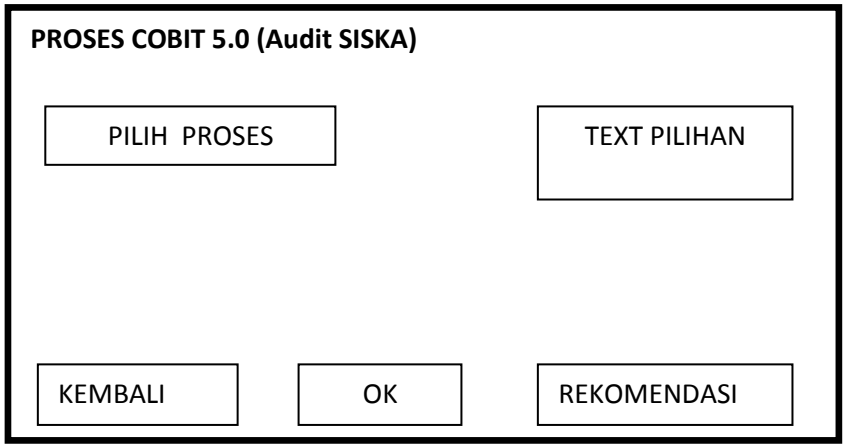
  Pada halaman ini berisi pilihan bagian responden. Pada halaman ini terdapat 2 pilihan responden yaitu user dan menejemen, serta tombol "OK". Ketika sudah memilih pilihan yang ada kemudian memilih tombol "OK" maka akan menuju ke halaman selanjutnya sesuai dengan pilihannya. Rancangan halaman responden dapat dilihat pada gambar 3.6.



Gambar 3.6 Rancangan Tampilan *Form* Halaman Responden

- **Tampilan Halaman Proses**

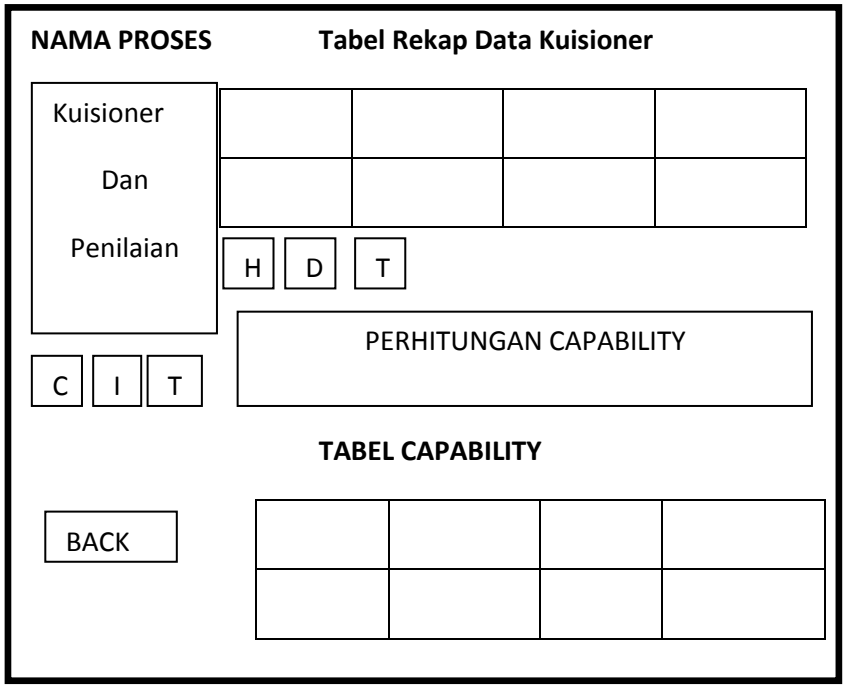
  Pada halaman ini, berisi pilihan proses yang akan dilakukan dalam melakukan audit. Pada halaman ini terdapat pilihan proses ada pada tombol *combo box*. User harus mimilih proses mana yang akan digunakan. Selain itu terdapat tombol "OK" untuk pergi ke halaman selanjutnya dan tombol "kembali" untuk kembali ke halaman sebelumnya. Tombol "REKOMENDASI" untuk masuk kehalaman rekomendasi. Rancangan halaman proses dapat dilihat pada gambar 3.7.



Gambar 3.7. rancangan tampilan halaman proses

- **Tampilan Halaman Audit (Pertanyaan/pernyataan dan Rekapitulasi).**

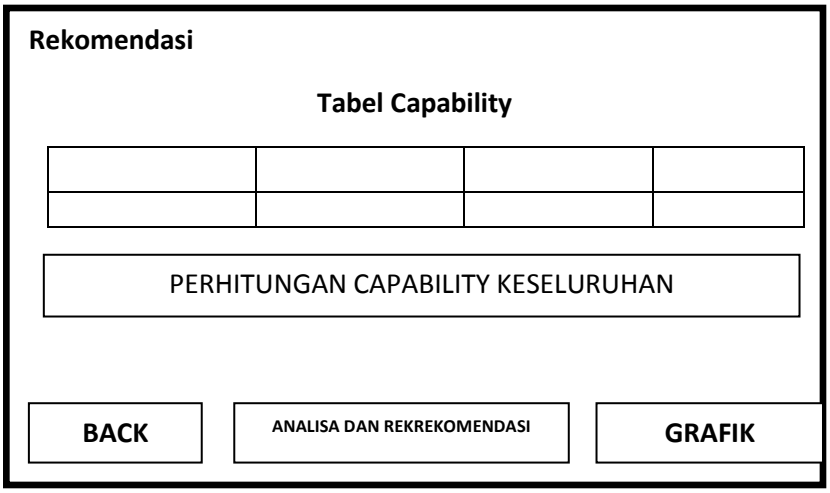
  Pada halaman ini berisi tentang kuisioner yang akan diberikan pada pengguna sesuai dengan pemilihan proses yang dipilih, tabel rekap kuisioner, perhitungan hasil tabel kuisioner,serta tabel hasil capability darihasil perhitungan rekapitulasi. Rancangan halaman kuisioner dapat dilihat pada gambar 3.8.



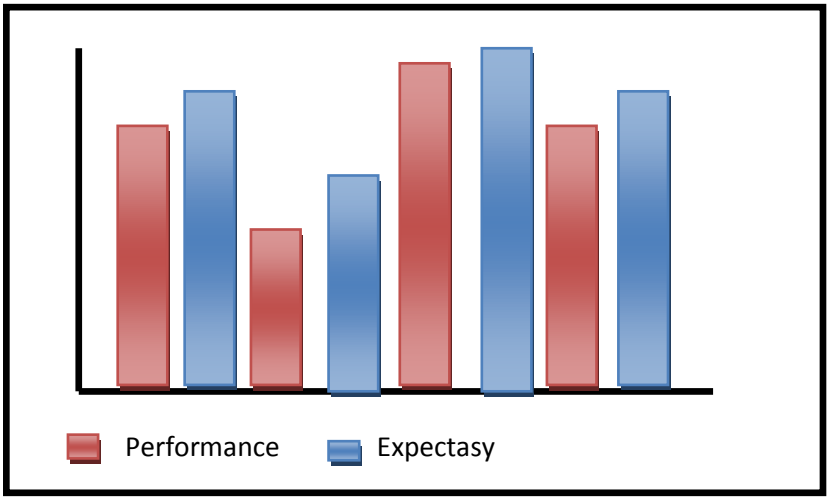
Gambar 3.8. Rancangan Tampilan *Form* Halaman Audit

- **Tampilan Halaman Rekomendasi**

  pada halaman ini terdapat tabel capability yang diambil dari perhitungan tiapp proses audit, selanjutnya data tabel tersebut dihitung. Setelah hasil hasil total keseluruhan didapatkan ketika kita memilih tombol "Analisa dan Rekomendasi" maka akan muncul sebuah form tampilan pesan analisa hasil dan rekomendasi sesuai dengan hasil *capability* yang dicapai . untuk menampilkan grafik *capability* berdasarkan hasil *capability* yang dicapai maka pilih tombol "Grafik". Rancangan halaman rekomendasi dan grafik dapat dilihat pada gambar 3.9 dan gambar 3.10



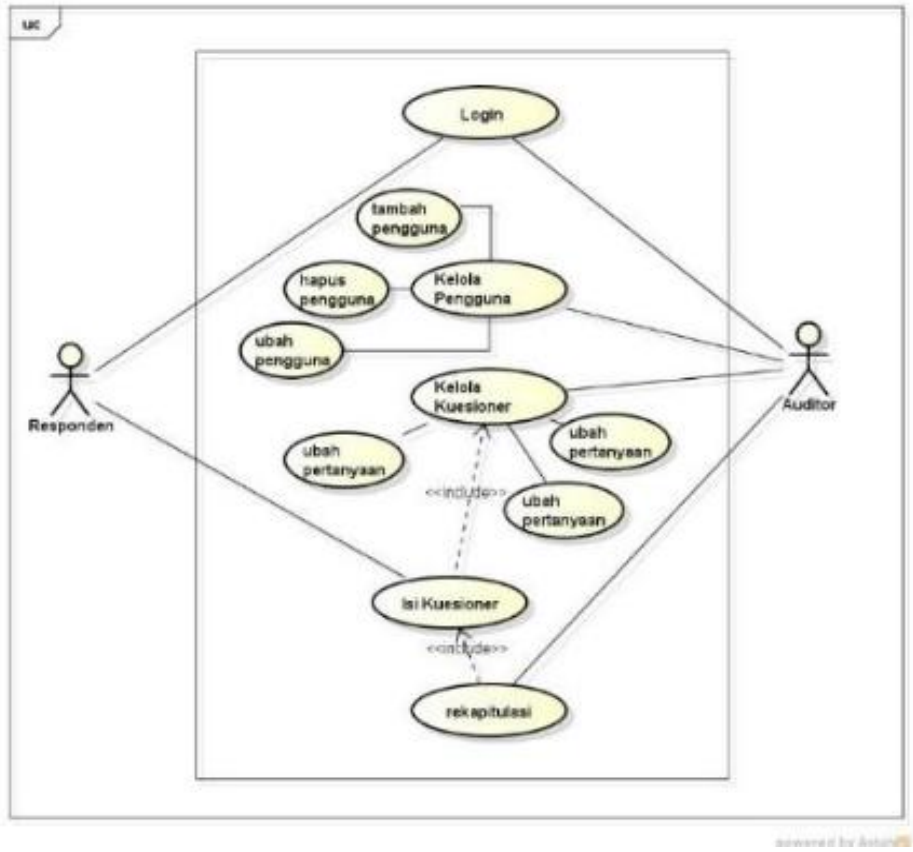
Gambar 3.9. Rancangan tampilan Form halaman rekomendasi



Gambar 3.10. Rancangan tampilan Grafik *Capability*

- **Desain Perangkat Lunak pendukung Audit**

Perangkat lunak dibuat untuk mendistribusikan kuisioner kepada reponden terpilih, dan menghitung nilai *capability* berdasarkan data yang diperoleh. Fitur yang ada pada sistem informasi audit digambarkan ke dalam *usecase diagram* yang ditunjukan pada gambar 3.11



Gambar 3.10 *Usecase Diagram* Sistem Informsi pendukung audit

3.3.3 Coding

Coding digunakan untuk digunakan mencari inputan atau dari pengisian kuisioner, hasil pengamatan yang dilakuakan penulis untuk mengambil keputusan dan atau outputan (rekomendasi).

3.3.4 Testing

Test diigunakan untuk menguji software apakah ada kekurangan atau tidak pada sistem. Pengujian aplikasi merupakan tahap selanjutnya setelah program atau aplikasi perangkat lunak selesai dalam pembuatannya. Pengujian tersebut dilakukan untuk mengevaluasi hasil sistem yang dibuat.

3.4 Proses Kerja Aplikasi Audit Sistem Informasi Akademik

1. Pada saat user membuka aplikasi, akan langsung mucul *form* halaman awal aplikasi audit.
2. Setelah itu klik tombol **"MULAI"** untuk memulai proses audit, maka user akan masuk pada *form login*. Masukan username dan password yang sesuai dan tersimpan pada database. Jika berhasil maka akan menuju halaman *form* responden.
3. Pilih responden yang akan diinputkan datanya, lalu pilik **"OK"** maka akan menuju ke *form* halaman proses.
4. Setelah muncul *form* halaman proses, langkah selanjutnya adalam memilih proses dalam audit, lalu pilih **"OK"** maka akan muncul *form* pengisian kuisioner. Isikan kuisioner sesuai data, setelah itu hitung nilai *capability level.*
5. Setelah dihitung nilai *capability level* simpan data, selanjutnya menuju halaman rekomendasi. Tampilkan data *capability level* lalu pilih "**REKOMENDASI**" maka akan muncul tampilan pesan rekomendasi.
6. Untuk menampilkan grafik *capability* pilih tombol **"GRAFIK"** pada halaman rekomendasi, maka akan muncul *form* tampilan grafik *capability*
7. Selesai.