

## **BAB II**

### **LANDASAN TEORI**

#### **2.1 Perencanaan Strategis SI/TI**

Menurut Ward dan Peppard (2002), Perencanaan strategis SI/TI merupakan proses identifikasi portofolio aplikasi SI berbasis komputer yang mendukung organisasi dalam pelaksanaan rencana bisnis dan merealisasikan tujuan bisnisnya. Perencanaan strategis SI/TI mempelajari pengaruh SI/TI terhadap kinerja bisnis dan kontribusi bagi organisasi dalam memilih langkah-langkah strategis. Selain itu, perencanaan strategis SI/TI juga menjelaskan berbagai *tools*, teknik, dan kerangka kerja bagi manajemen untuk menyelaraskan strategi SI/TI dengan strategi bisnis, bahkan mencari kesempatan baru melalui penerapan teknologi yang inovatif.

Jadi dapat disimpulkan bahwa perencanaan strategis SI/TI sangat diperlukan dalam upaya pengelolaan dan pemanfaatan TI untuk kepentingan organisasi dalam mencapai tujuan bisnis dan keunggulan kompetitif. Integritas dan keselarasan dalam proses bisnis organisasi sangat diperlukan, dengan begitu organisasi memiliki *capability*, *availability*, *reliability*, serta *adaptive* sehingga dapat menyelesaikan setiap transaksi dan melakukan perubahan dengan cepat dan akurat (Suralani, 2011).

#### **2.2 Information Technology Infrastructure Library (ITIL)**

ITIL adalah suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan, serta operasi teknologi informasi (TI). ITIL memberikan deskripsi detail tentang beberapa praktik TI penting dengan daftar cek, tugas, serta prosedur

yang menyeluruh yang dapat disesuaikan dengan segala jenis organisasi TI. ITIL merupakan *framework* untuk mengelola infrastruktur TI pada suatu organisasi dan bagaimana memberikan *service* terbaik bagi pengguna layanan TI (OGC, 2007). Penggunaan pendekatan ITIL V-3 sebagai kerangka acuan dapat digunakan untuk meningkatkan, memonitor, dan memastikan layanan teknologi informasi dapat berjalan sesuai dengan visi dan misi perusahaan. Tujuan utama dari penerapan ITIL:

1. Sebagai jembatan antara pihak manajemen dan divisi TI agar keduanya dapat berkomunikasi lebih efektif dan efisien
2. Dapat memanfaatkan infrastruktur teknologi informasi yang ada dengan optimal
3. Dapat memajemen infrastruktur TI dengan baik sehingga jika terjadi masalah dapat langsung memulihkan keadaan yang ada

ITIL V-3 terdiri atas lima bagian dan lebih menekankan pada pengelolaan siklus hidup layanan yang disediakan oleh teknologi informasi menurut OGC (2007). Kelima bagian tersebut adalah:

1. *Service Strategy*, sebuah panduan untuk menentukan strategi yang digunakan untuk mengimplementasikan system.
2. *Service Design*, memberikan panduan kepada organisasi TI untuk mendesain dan membangun layanan TI maupun implementasi ITSM. Desain layanan mengikuti strategi layanan dalam siklus hidup layanan. Hal ini tidak mengacu pada layanan baru saja, tetapi juga untuk layanan lama yang sudah diperbarui.
3. *Service Transition*, memberikan gambaran cara sebuah kebutuhan yang didefinisikan dalam *Service Strategy* kemudian dibentuk dalam *Service*

*Design* untuk selanjutnya secara efektif direalisasikan dalam *Service Operation*.

4. *Service Operation*, kegiatan operasional harian untuk pengelolaan layanan TI. Di dalamnya terdapat panduan cara mengelola layanan TI dan bertanggung jawab untuk melaksanakan dan melakukan proses pengoptimalan biaya dan kualitas layanan.
5. *Continual Service Improvement*, memberikan panduan penting dalam menyusun serta memelihara kualitas layanan dari proses desain, transisi dan pengoperasiannya.

Kelima siklus hidup dari ITIL V-3 di atas yang digunakan untuk mendukung penelitian Tugas Akhir ini adalah tahap *Service Operation*. Kegiatan umum pada *Service Operation* berisi tentang sejumlah kegiatan operasional yang memastikan bahwa teknologi sejalan dengan tujuan layanan dan proses organisasi secara keseluruhan. *Service Operation* memiliki lima proses yang saling berkaitan, adapun lima proses tersebut meliputi:

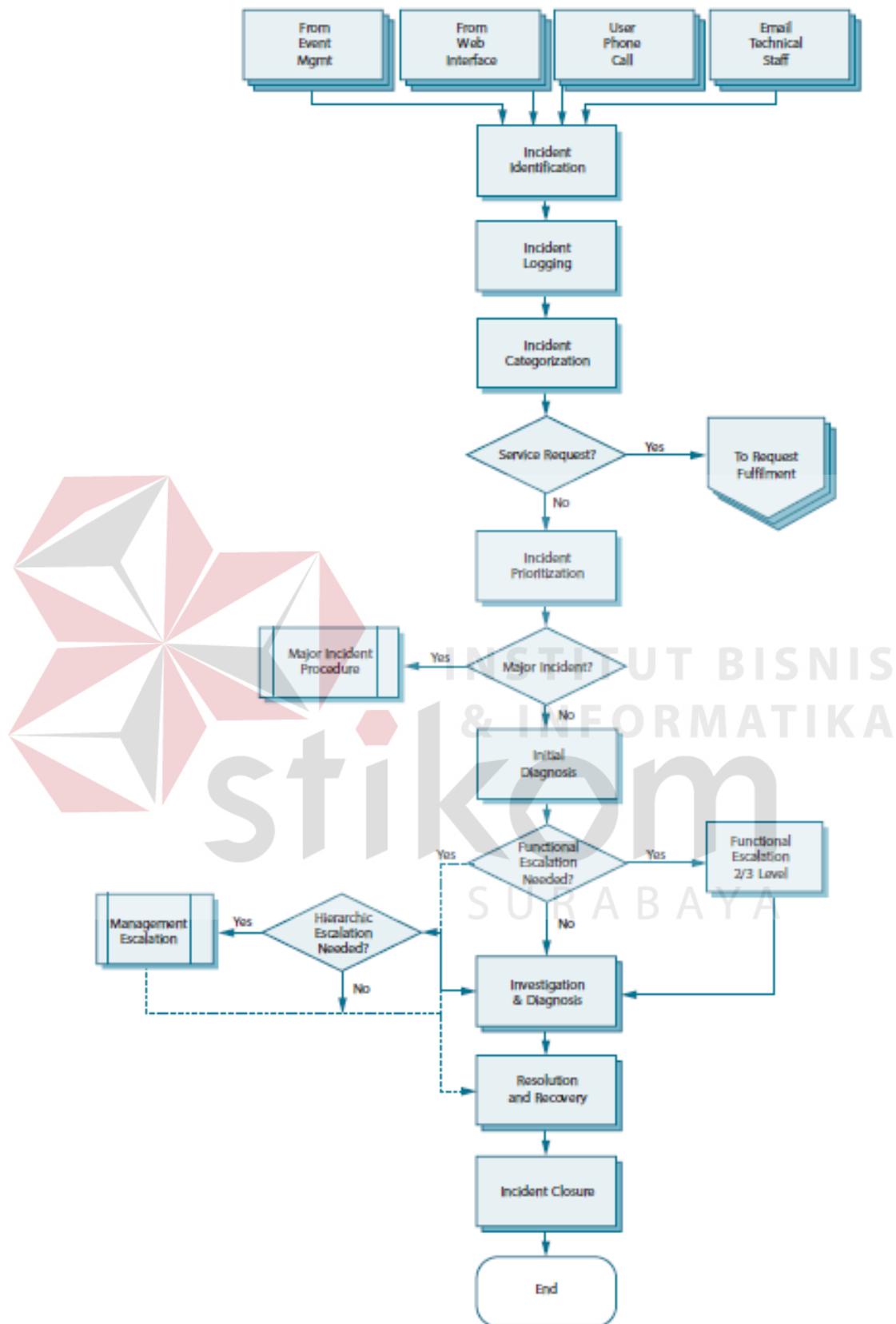
1. *Event Management*, memonitor semua peristiwa yang terjadi diseluruh infrastruktur TI.
2. *Incident Management*, berkonsentrasi pada pemulihan layanan tiba-tiba rusak atau terganggu secepat mungkin, untuk meminimalkan dampak bisnis.
3. *Request Fulfillment*, proses penanganan permintaan pengguna sesuai standar serta memungkinkan TI untuk memenuhi layanan untuk menyediakan akses yang cepat dan efektif untuk standar layanan. Contohnya, permintaan untuk mengubah password atau permintaan informasi.

4. *Problem Management*, analisis akar penyebab untuk menentukan dan mengatasi penyebab peristiwa dan kejadian, kegiatan proaktif untuk mencegah masalah dan insiden dimasa depan.
5. *Access Management*, proses pemberian pengguna resmi hak untuk menggunakan layanan, sementara membatasi akses ke pengguna non-resmi.

Penelitian ini lebih difokuskan lagi, yaitu hanya berfokus pada proses *Incident Management*. *Incident* merupakan gangguan yang tidak direncanakan untuk layanan TI dan biasanya akibat dari kegagalan sistem atau *error* pada infrastruktur TI yang menyebabkan atau berpotensi menjadi penyebab terganggunya operasional (OGC, 2007). Contoh dari *incident* adalah:

1. Adanya aplikasi potensial menyebabkan kerusakan sistem.
2. Sistem yang *down* dapat menyebabkan sistem lain terganggu.
3. Jaringan komputer yang terganggu menyebabkan sistem terganggu.

Menurut OGC (2007), *Incident Management* itu sendiri bertujuan untuk mengembalikan operasi layanan normal secepat mungkin “layanan operasi normal” didefinisikan di sini sebagai layanan operasi dalam batas SLA dan meminimalkan dampak negatif terhadap operasi bisnis, sehingga memastikan bahwa kemungkinan tingkat terbaik kualitas layanan dipertahankan. *Incident Management* memiliki beberapa proses yang harus diikuti selama pengelolaan insiden, ditunjukkan pada gambar 2.1 meliputi langkah berikut (OGC, 2007).



Gambar 2.1 Alur *Incident Management* Process

1. *Incident Identification*, dimulai dengan identifikasi dan yang paling umum dilakukan adalah melalui layanan *service desk* dan laporan dari staf teknis. Fase ini bermula ketika suatu insiden terjadi dan insiden itu dapat diketahui melalui:
  - a. Laporan dari pengguna melalui *website* perusahaan.
  - b. Laporan dari pengguna melalui telepon.
  - c. Laporan dari teknisi yang sedang melakukan perawatan peralatan perusahaan.
  
2. *Incident Logging*, pencatatan dilakukan melalui telepon *Service Desk* atau secara otomatis terdeteksi melalui peringatan acara. Semua informasi dicatat sehingga jika insiden terulang, memiliki semua informasi yang relevan untuk membantu. Informasi-informasi yang perlu dicatat dalam setiap insiden antara lain:
  1. Kategori insiden atau level insiden
  2. Urgensi insiden
  3. Dampak insiden
  4. Tanggal dan waktu pencatatan
  5. Nama atau pihak yang menangani insiden
  6. Metode munculnya notifikasi (telepon, *e-mail*, langsung, dsb)
  7. Nama/bagian
  8. Deskripsi insiden
  9. Kegiatan yang telah dilakukan dalam penanganan insiden
  10. Tanggal dan waktu penanganan insiden

3. *Incident Categorization*, dalam membuat kategori insiden dibutuhkan sebuah proses khusus antara pengelola TI dan pihak manajemen organisasi. Hal ini bertujuan untuk menghasilkan kategori insiden dan prioritas penanganannya sejalan dengan proses bisnis organisasi. Kategori insiden dapat dibuat berdasarkan perkiraan lamanya penanganan, implikasi terhadap proses bisnis organisasi, dan jumlah staf teknis terkait karena setiap organisasi atau perusahaan mempunyai level kategori sendiri-sendiri dalam mengartikan insiden yang terjadi. Langkah-langkah dalam menetapkan level kategori antara lain:

- a. Lakukan diskusi antara kepala bagian dengan pihak terkait yang menangani.
- b. Putuskan level-level kategori insiden dari *top level* ke *lower level*.
- c. Analisis insiden yang sering terjadi selama periode yang telah disepakati untuk menentukan level kategorinya.
- d. Lakukan *review* apakah kategori yang telah ditetapkan sudah cocok atau perlu dilakukan perubahan level kategori lagi.

4. *Incident Prioritization*, dapat dilakukan berdasarkan besarnya implikasi insiden terhadap kegiatan bisnis utama organisasi, ataupun berdasarkan lamanya penanganan insiden. Faktor-faktor yang berkontribusi dalam penentuan level dampak antara lain:

- a. Risiko terhadap keberlangsungan hidup perusahaan.
- b. Jumlah kegiatan atau layanan yang terkena dampak insiden.
- c. Level kehilangan finansial.
- d. Dampak terhadap reputasi bisnis.

e. Pelanggaran terhadap peraturan dan SPMI

Prioritas insiden kemungkinan dapat berubah secara dinamis, sehingga penyelesaian insiden yang sudah ditetapkan dalam SLA (*Service Level Agreement*) dapat berubah sesuai dengan kondisi terbaru penanganan insiden.

5. *Initial Diagnosis*, wajib dilakukan terhadap insiden oleh setiap pihak yang pertama kali berhubungan dengan insiden seperti, *service desk* dan staf teknis. Namun jika pihak yang pertama kali berhubungan masih belum dapat membantu menyelesaikan masalah secara langsung maka dapat meminta waktu kepada pengguna untuk mencatat insiden tersebut agar diselesaikan pihak atau bagian lain yang lebih kompeten menangani insiden tersebut.

6. *Incident Escalation*, adalah tindakan menaikkan level penanganan insiden. Hal ini berkaitan erat dengan hasil diagnosa awal terhadap insiden. Jika dari diagnosa ditemukan insiden yang tidak dapat ditangani, maka wajib dilakukan eskalasi insiden. Terdapat dua cara atau tahapan dalam penanganan insiden, antara lain:

1. *Functional escalation*: Tindakan menaikkan level penanganan kepada satu level di atasnya. Apabila bagian administrasi tidak dapat menyelesaikan insiden yang dikeluhkan maka secepatnya insiden tersebut dilimpahkan kepada staf level support berikutnya sampai pada level support tertinggi.

2. *Hierarchic escalation*: tindakan menaikkan level penanganan melintasi hierarki organisasi, misalnya kepada manajer IT atau manajer bisnis yang terkait. Apabila insiden yang terjadi pada level prioritas level satu maka harus ditangani dengan cepat oleh manajer-manajer bagian yang bersangkutan termasuk supplier jika diperlukan.

7. *Investigation and Diagnosis*, dilakukan untuk menemukan sumber masalah dari insiden. Dalam melakukan investigasi, setiap tindakan wajib dilaporkan juga ke dalam formulir insiden. Hal ini berguna sebagai data historis tindakan penanganan suatu insiden.

Berikut tindakan yang ada dalam investigasi, antara lain:

- a. Menetapkan apa yang sebenarnya terjadi (kesalahan) dan informasi yang diinginkan pengguna.
- b. Memahami kronologi terjadinya insiden.
- c. Mengkonfirmasi dampak yang ditimbulkan oleh insiden.
- d. Mengidentifikasi berbagai kegiatan yang menyebabkan terjadinya insiden.

8. *Resolution and Recovery*, langkah ini merupakan tindakan yang diambil untuk menyelesaikan suatu insiden. Langkah resolusi dapat dilakukan oleh *service desk* sebagai pihak yang pertama menemukan insiden dari pengguna dan staf teknisi yang sedang mengerjakan kegiatan konfigurasi. Pada saat langkah penyelesaian insiden sudah ditentukan, maka perlu dilakukan testing dan tindakan penyelesaian. Semua kegiatan dan pihak atau staf yang berwenang menangani gangguan yang terjadi tersebut harus dicatat secara detil sebagai histori perawatan perangkat. Tindakan-tindakan yang perlu dilakukan antara lain:

- a. Meminta dan memandu pengguna melakukan tindakan yang diperlukan secara langsung.
- b. Meminta staf ahli untuk menangani insiden secara langsung.
- c. Meminta pihak ketiga atau supplier dalam menangani insiden yang terjadi.

9. *Incident Closure*, adalah langkah yang dilakukan oleh *service desk* maupun staf teknisi terkait untuk memastikan apakah insiden telah benar selesai ditangani. Setelah penyelesaian insiden dilakukan maka perlu melakukan cek pada hal berikut ini:
- a. *Closure categorization*: cek dan konfirmasi bahwa inisiasi kategori insiden yang ditetapkan adalah sudah benar atau belum benar. Dilakukan update catatan insiden.
  - b. *User satisfaction survey*: meminta penilaian kepuasan pengguna atas penanganan insiden yang telah dilakukan.
  - c. *Incident documentation*: memastikan bahwa semua kegiatan penanganan insiden sudah dicatat secara lengkap.
  - d. *Ongoing or recurring problem?*: menetapkan apakah insiden benar-benar sudah terselesaikan dan memutuskan langkah-langkah pencegahan agar insiden tidak terjadi lagi.
  - e. *Formal closure*: membuat laporan catatan insiden secara formal.

### 2.3 *Standard Operating Procedure (SOP)*

SOP adalah sebagai dokumen yang menjabarkan aktifitas operasional yang dilaksanakan sehari-hari, dengan tujuan agar pekerjaan tersebut dilaksanakan secara benar, tepat, dan konsisten untuk menghasilkan produk sesuai standar yang telah ditetapkan sebelumnya. Pada dasarnya, prosedur merupakan instruksi tertulis yang berfungsi sebagai pedoman untuk menyelesaikan sebuah tugas rutin atau tugas yang berulang (repetitif) dengan cara yang efektif dan efisien untuk menghindari terjadinya variasi atau penyimpangan sehingga dapat mempengaruhi kinerja organisasi secara keseluruhan. Dalam pengertian secara luas, SOP

seringkali digunakan untuk menyebut semua dokumen yang mengatur aktifitas operasional organisasi, termasuk protokol, instruksi kerja, lembar kerja, dan lain sebagainya (Tathagati, 2014).

Menurut Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 50 tahun 2014 tentang Sistem Penjaminan Mutu Pendidikan Tinggi, Sistem Penjaminan Mutu Internal yang selanjutnya disingkat SPMI, adalah kegiatan sistemik penjaminan mutu pendidikan tinggi oleh setiap perguruan tinggi secara otonom untuk mengendalikan dan meningkatkan penyelenggaraan pendidikan tinggi secara berencana dan berkelanjutan. Dokumen SPMI terdiri atas dokumen standar dalam SPMI, dokumen prosedur, dan dokumen formulir yang digunakan dalam SPMI.

Dikarenakan template yang digunakan Bagian PPTI untuk pembuatan prosedur menggunakan standar Sistem Penjaminan Mutu Internal (SPMI) maka seluruh dokumen prosedur yang dibuat menggunakan standar tersebut. Untuk penamaan dokumennya sendiri juga berbeda dalam SPMI, seperti *Standard Operating Procedure* (SOP) berubah menjadi Standar, Instruksi Kerja berubah menjadi Prosedur, dan Rekam Kerja berubah menjadi Formulir.

Berdasarkan penjelasan tersebut maka dibuat Prosedur pada penelitian Tugas Akhir ini, Prosedur ini digunakan sebagai pedoman dalam menyelesaikan tugas rutin karena dapat digunakan untuk memastikan sebuah proses dilaksanakan dengan baik, konsisten, efektif, dan efisien.

## 2.4 *Work Instruction*

Berdasarkan prosedur yang dirancang pada proses sebelumnya, maka penelitian Tugas Akhir ini berlanjut pada pembuatan Instruksi Kerja (IK). IK adalah dokumen yang mengatur secara rinci dan jelas urutan suatu aktivitas dan hanya melibatkan satu fungsi sebagai pendukung. Dalam dokumen IK biasanya merinci langkah demi langkah urutan sebuah aktivitas yang bersifat teknis (Tathagati, 2014).

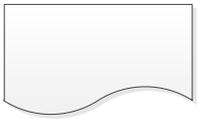
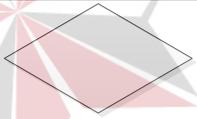
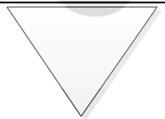
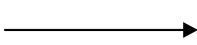
## 2.5 *Work Record*

Penelitian Tugas Akhir ini juga memerlukan Rekam Kerja sebagai bukti sah dengan tujuan untuk memantau pelaksanaan Prosedur dan Instruksi Kerja yang telah dilaksanakan berjalan dengan baik atau tidak. Menurut A. Tathagati (2014), Rekaman merupakan bukti bahwa sistem tata kerja yang tertuang dalam prosedur dan Instruksi Kerja telah dilaksanakan. Rekaman dapat berupa formulir yang telah diisi, lembar kerja, grafik, *database*, laporan, notulen rapat, persyaratan perundangan atau perizinan terkait organisasi/perusahaan, dan bentuk-bentuk lain yang dapat diterima oleh organisasi sebagai bukti yang sah.

## 2.6 *Bagan Alir Sistem*

Menurut Jogiyanto (2005), bagan alir sistem (*system flow*) merupakan bagan yang menunjukkan arus pekerjaan secara keseluruhan dari sistem, pekerjaan yang dilakukan oleh sistem, dan urutan dari prosedur yang ada dalam sistem. Berikut bagan alir sistem digambarkan dengan menggunakan simbol-simbol pada tabel 2.1.

Tabel 2.1 Bagan Alir Sistem

No.	Simbol	Nama Simbol <i>Flowchart</i>	Fungsi
1.		Dokumen	Untuk menunjukkan dokumen <i>input</i> dan <i>output</i> baik untuk proses manual, mekanik atau komputer.
2.		Proses Komputerisasi	Menunjukkan kegiatan dari operasi program komputer.
3.		<i>Database</i>	Untuk menyimpan data.
4.		Penghubung	Menunjukkan hubungan di halaman yang sama.
5.		Penghubung Halaman Lain	Menunjukkan hubungan di halaman lain.
6.		<i>Terminator</i>	Menandakan awal/akhir dari suatu sistem.
7.		<i>Decision</i>	Menggambarkan logika keputusan dengan nilai <i>true</i> atau <i>false</i> .
8.		Kegiatan Manual	Untuk menunjukkan pekerjaan yang dilakukan secara manual.
9.		Simpanan <i>Offline</i>	Untuk menunjukkan file <i>non</i> -komputer yang diarsip urut angka.
10.		Alur Data	Untuk menunjukkan alur dari setiap proses.