# BAB III

# METODE PENELITIAN

Pada Bab III akan dilakukan pembahasan dimulai dengan profil perusahaan, gambaran struktur organisasi, dan dilanjutkan dengan tahapan-tahapan audit yang akan dilaksanakan sesuai dengan Gambar 2.7 di halaman 31.

## 3.1 Tahap Perencanaan Audit Sistem Informasi Manajemen Aset

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. melakukan identifikasi proses bisnis, 2. Melakukan penentuan ruang lingkup dan tujuan audit dan 4. Melakukan *identification of core TI application and the main IT relevant interfaces*. Tahap ini akan menghasilkan pengetahuan tentang proses bisnis TI perusahaan, ruang lingkup dan tujuan yang telah ditentukan serta klausul yang telah ditentukan.

### 3.1.1 Mengidentifikasi Proses Bisnis dan TI

Pada tahapan perencanaan audit, proses pertama yang dilakukan adalah melakukan pemahaman proses bisnis dan TI perusahaan yang diaudit (*auditee*) dengan mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut berupa profil perusahaan, *standard operating procedure*, kebijakan, standar, prosedur, portopolio, arsitektur, infrastruktur, dan aplikasi sistem informasi. Langkah selanjutnya adalah mencari informasi apakah sebelumnya perusahaan telah melaksanakan proses audit. Apabila pernah

dilakukan audit, maka auditor perlu mengetahui dan memeriksa laporan audit sebelumnya.

Untuk menggali pengetahuan tentang *auditee* langkah yang dilakukan adalah dengan cara mengetahui dan memeriksa dokumen-dokumen yang terkait dengan proses audit, wawancara manajemen dan staff, serta melakukan observasi kegiatan operasional dan teknologi sistem informasi yang digunakan. *Output* yang dihasilkan pada proses ini adalah profil perusahaan, visi, misi, dan *Principle & Management*, struktur organisasi, *document flow* serta bukti dan pernyataan bahwa auditor telah melihat serta mempelajari dokumen yang terkait dengan perusahaan.

### 3.1.2 Penentuan Ruang Lingkup dan Tujuan Audit Sistem Informasi

Proses kedua pada tahapan perencanaan ini adalah mengidentifikasi ruang lingkup dan tujuan yang akan dibahas dalam audit kali ini. Penentuan ruang lingkup dilakukan dengan cara melakukan observasi pada PT. Varia Usaha Beton. Ruang lingkup yang telah ditentukan akan dipaparkan pada bab IV.

Pada peoses ini, langkah yang selanjutnya dilakukan adalah mengidentifikasi tujuan yang berhubungan akan kebutuhan audit sistem informasi ini. Tujuan dari audit sistem informasi manajemen aset ini selanjutnya akan dipaparkan pada bab IV.

### 3.1.3 *Identification of core TI application and the main IT relevant interfaces*

Pada proses ini langkah yang dilakukan adalah menentukan klausul, obyektif kontrol dan kontrol  yang sesuai dengan permasalahan dan kebutuhan

PT. Varia Usaha Beton. Klausul, obyektif kontrol dan kontrol yang ditentukan harus berdasarkan kesepakatan antara auditor dengan *auditee*. Proses ini akan menghasilkan klausul, obyektif kontrol serta kontrol yang telah ditentukan dan disepakati oleh auditor dengan *auditee.*

## 3.2 Tahap Persiapan Audit Sistem Informasi

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1. Melakukan proses penyusunan audit *working plan*, 2. Membuat pernyataan, 3. Melakukan pembobotan dan 4. Membuat pertanyaan. Tahap ini akan menghasilkan tabel *working plan*, pernyataan yang telah dibuat berdasarkan standar ISO 27002, nilai pembobotan pada masing-masing pernyataan serta nilai *marturity level* dan pertanyaan yang telah dibuat berdasarkan pernyataan.

### 3.2.1 Penyusunan *Audit Working Plan*

Pada proses membuat audit *working plan* langkah yang dilakukan adalah membuat daftar semua kegiatan yang akan dilakukan dalam melakukan proses audit, kemudian memasukkan daftar kegiatan tersebut didalam tabel. Contoh audit *working plan* dapat dilihat pada Tabel 3.1 di halaman 36.

Tabel 3.1 Contoh Audit Working Plan

| No | Kegiatan | Bulan | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | September | | | | Oktober | | | | November | | | | Desember | | | |
| | | 1 | 2 | 3 | 1 | 1 | 1 | 1 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | Studi Literatur | | | | | | | | | | | | | | | | |
| 2 | Penentuan ruang lingkup | | | | | | | | | | | | | | | | |

### 3.2.2 Membuat Pernyataan

Proses selanjutnya pada tahapan persiapan audit ini dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang terdapat pada setiap klausul yang telah ditetapkan berdasarkan standar COBIT 4.1 dan ISO 27002. Pada setiap kontrol keamanan dapat ditentukan pernyataan yang mendiskripsikan implementasi dan pemeliharaan kontrol keamanan tersebut. Salah satu contoh pernyataan pada ISO 27002 dapat dilihat pada Tabel 3.2 di halaman 37, sedangkan salah satu contoh untuk pernyataan COBIT 4.1 dapat dilihat pada Tabel 3.3 di halaman 37 .

Tabel 3.2 Contoh Pernyataan Pada ISO 27002

| Klausul 6 Organisasi Keamanan Informasi | |
|---|---|
| Tujuan diperlukanya organisasi keamanan informasi yaitu: | |
| Memudahkan Pengelolaan SMKI pada PT. Varia Usaha Beton | |
| Kontrol Keamanan: 6.1.3<br>Pembagian Tanggung Jawab Keamanan Informasi | |
| No | Pernyataan |
| 1 | Terdapat pembagian tanggung jawab keamanan informasi yang telah ditetapkan dengan jelas. |
| 2 | Kebijakan keamanan informasi telah menyertakan panduan umum dalam pengalokasian peran keamanan di dalam organisasi. |

Tabel 3.3 Contoh Pernyataan Pada COBIT 4.1

| **Nama Proses** | **Mengidentifikasi Solusi Otomatis** |
|---|---|
| **Nomor Proses** | **AI1** |
| **No.** | **Pernyataan** |
| 1 | Organisasi mengidentifikasi kebutuhan fungsional untuk penerapan solusi seperti sistem, jasa, infrastruktur, perangkat lunak, dan data |
| 2 | Organisasi mengidentifikasi kebutuhan operasional untuk penerapan seperti sistem, jasa, infrastruktur, perangkat lunak, dan data |

### 3.2.3 Melakukan Pembobotan

Setelah membuat pernyataan, maka langkah selanjutnya adalah melakukan pengukuran pembobotan pada setiap pernyataan. Pembobotan dilakukan berdasarkan perhitungan yang dilakukan oleh Niekerk dan Labuschagne (2006: 7), dengan membagi tingkat pembobotan dalam manajemen menjadi 3 (tiga), yaitu: sangat penting, cukup penting dan kurang penting, seperti terlihat pada Tabel 3.6 dihalaman 39. Didalam Tugas Akhir ini dilakukan dua kali proses pembobotan yaitu pembobotan ISO 27002 dan COBIT 4.1. Hal tersebut dilakukan karena hasilnya pembobotan dan penilaian maturity level tersebut akan di setarakan. Salah satu contoh pembobotan pada ISO 27002 dan beberapa pembobotanya dapat dilihat pada Tabel 3.4 dihalaman 38 sedangkan salah satu pembobotan pada COBIT 4.1 dan beberapa pembobotanya dapat dilihat pada Tabel 3.5 dihalaman 39.

Tabel 3.4 Contoh Pembobotan Pada ISO 27002

| **Kontrol Keamanan: 6.1.1**<br>**Komitmen manajemen terhadap keamanan informasi** | | | |
|---|---|---|---|
| No | Pernyataan | Hasil Pemeriksaan | bobot |
| 1 | Terdapat kepemimpinan yang kondusif untuk menyetujui kebijakan keamanan informasi di seluruh tataran organisasi. | Kepemimpinan sudah ditetapkan secara kondusif dan telah ditingkatkan terus-menerus melalui pemantauan secara berkala.<br><br>Bukti:<br>Terdapat struktur organisasi resmi beserta kebijakan perusahaan yang tercantum pada dokumen audit yaitu:<br>Dokumen: Quality manual<br>ISO : 9001:2008<br>November 2011 | 0.8 |

Tabel 3.5 Contoh Pembobotan Pada COBIT 4.1

| **Nama Proses** | **Mendefinisikan Arsitektur Informasi** | | |
|---|---|---|---|
| **Nomor Proses** | **PO2** | **Level Kedewasaan** | **0** |
| **No.** | **Pernyataan** | | **Bobot** |
| 1 | Tedapat pengetahuan tentang bagaimana mengembangkan arsitektur informasi | | 0.80 |
| 2 | Terdapat keahlian mengembangkan arsitektur informasi | | 0.80 |
| 3 | Terdapat pertanggung jawaban dalam mengembangkan arsitektur informasi | | 0.80 |
| | | **Total Bobot =** | **2.40** |

Tabel 3.6 Tingkat Kepentingan dalam Pembobotan Pernyataan

| No | Nilai Kualitatif | Skala | Keterangan |
|---|---|---|---|
| 1 | Tinggi | 0,70 – 1,00 | Pernyataan tersebut mempunyai peranan yang sangat penting dalam proses sistem informasi |
| 2 | Cukup | 0,40 – 0,69 | Pernyataan tersebut cukup mempunyai peran dalam proses sistem informasi |
| 3 | Rendah | 0,00 – 0,39 | Pernyataan tersebut dalam melengkapi peran dalam sistem informasi |

Sumber: Niekerk dan Labuschagne (2006: 7)

### 3.2.4 Membuat Pertanyaan

Pada proses ini langkah yang dilakukan adalah membuat pertanyaan dari pernyataan yang telah ditentukan sebelumnya. Pada satu pernyataan bisa memiliki lebih dari satu pertanyaan, hal tersebut dikarenakan setiap pertanyaan harus mewakili pernyataan pada saat dilakukan wawancara. Contoh beberapa pertanyaan pada ISO 27002 dapat dilihat pada Tabel 3.7 di halaman 40 sedangkan contoh beberapa pertanyaan pada COBIT 4.1 dapat dilihat pada Tabel 3.8 di halaman 40.

Tabel 3.7 Contoh Pertanyaan Pada ISO 27002

| Klausul 6 Organisasi Keamanan Informasi | |
|---|---|
| Tujuan diperlukanya organisasi keamanan informasi yaitu: | |
| Memudahkan Pengelolaan SMKI pada PT. Varia Usaha Beton | |
| Kontrol Keamanan: 6.1.1<br>Komitmen manajemen terhadap keamanan informasi | |
| No | Pertanyaan |
| 1 | Apakah kepemimpinan untuk menyetujui kebijakan keamanan informasi di seluruh tataran organisasi telah kondusif? |
| 2 | - Apakah kepemimpinan untuk menetapkan peran keamanan di seluruh tataran organisasi telah kondusif?<br>- Siapakah yang bertangung jawab terhadap keamanan system informasi di seluruh tataran organisasi. |

Tabel 3.8 Contoh Pertanyaan Pada COBIT 4.1

| **Nama Proses** | **Mengidentifikasi Solusi Otomatis** |
|---|---|
| | **AI1** |
| **No.** | **Pertanyaan** |
| 1 | Apakah kebutuhan fungsional untuk penerapan solusi seperti sistem, jasa, infrastruktur, perangkat lunak dan data telah diidentifikasi? |
| 2 | Apakah kebutuhan operasional untuk penerapan seperti sistem, jasa, infrastruktur, perangkat lunak dan data telah diidentifikasi? |



## 3.3 Tahap Pelaksanaan Audit Sistem Informasi

Pada tahap ini langkah-langkah yang dilakukan yaitu: 1.Melakukan proses pemeriksaan data dan bukti, 2. Melakukan wawancara, 3. Melakukan uji kematangan dan 4. Melakukan penentuan temuan dan rekomendasi. Tahap ini akan menghasilkan temuan dan bukti, dokumen wawancara, nilai kematangan dan rekomendasi.

### 3.3.1 Pemeriksaan Data dan Bukti

Pemeriksaan data dilakukan dengan cara melakukan observasi dan melakukan wawancara kepada *auditee* sesuai dengan ruang lingkup serta klausul yang telah disepakati oleh PT. Varia Usaha Beton. Wawancara dan observasi dilakukan untuk mendapatkan bukti atau temuan mengenai fakta terkait dengan masalah yang ada. Bukti-bukti tersebut berupa foto dan data. Contoh hasil pemeriksaan ISO 27002 dapat dilihat pada Tabel 3.9 di halaman 41, sedangkan contoh hasil pemeriksaan COBIT 4.1 dapat dilihat pada Tabel 3.10 di halaman 41.

Tabel 3.9 Contoh Hasil Pemeriksaan ISO 27002

| Kontrol Keamanan: 6.1.1<br>Komitmen manajemen terhadap keamanan informasi | | |
|---|---|---|
| No | Pernyataan | Hasil Pemeriksaan |
| 1 | Terdapat kepemimpinan yang kondusif untuk menyetujui kebijakan keamanan informasi di seluruh tataran organisasi. | Kepemimpinan sudah ditetapkan secara kondusif dan telah ditingkatkan terus-menerus melalui pemantauan secara berkala.<br><br>Bukti:<br>Terdapat struktur organisasi resmi beserta kebijakan perusahaan yang tercantum pada dokumen audit yaitu:<br>Dokumen: Quality manual<br>ISO : 9001:2008<br>November 2011 |

Tabel 3.10 Contoh Hasil Pemeriksaan COBIT 4.1

| **Nama Proses** | **Mengidentifikasi Solusi Otomatis** | **Hasil Pemeriksaan** |
|---|---|---|
| **Nomor Proses** | **AI1** | |
| **No.** | **Pernyataan** | |
| 1 | Organisasi mengidentifikasi kebutuhan fungsional untuk penerapan solusi seperti sistem, jasa, infrastruktur, perangkat lunak, dan data | Kebutuhan fungsional telah teridentifikasi dan telah didokumentasikan didalam dokumen pencatatan aset.<br><br>Bukti:<br>Dokumen pencatatan aset |

### 3.3.2 Wawancara

Pada proses ini langkah yang dilakukan adalah melakukan wawancara berdasarkan pertanyaan yang telah dibuat. Wawancara dilakukan terhadap pihak-pihak yang terlibat dalam eksekusi. Penentuan *auditee* untuk audit sistem keamanan informasi dilakukan berdasarkan struktur organisasi. Contoh dokumen wawancara ISO 27002 dapat dilihat pada Tabel 3.11 di halaman 42 sedangkan contoh dokumen wawancara COBIT 4.1 dapat dilihat pada Tabel 3.12 di halaman 42.

Tabel 3.11 Contoh Dokumen Wawancara pada ISO 27002

| Klausul 6 Organisasi Keamanan Informasi | | | |
|---|---|---|---|
| Tujuan diperlukanya organisasi keamanan informasi yaitu: | | | |
| Memudahkan Pengelolaan SMKI pada PT. Varia Usaha Beton | | | |
| Kontrol Keamanan: 6.1.3<br>Pembagian Tanggung Jawab Keamanan Informasi | | | |
| No | Pernyataan | Pertanyaan | Jawaban |
| 1 | Terdapat pembagian tanggung jawab keamanan informasi yang telah ditetapkan dengan jelas. | - Apakah terdapat pembagian tanggung jawab keamanan informasi yang telah ditetapkan dengan jelas?<br>- Apakah pembagian tanggung jawab tersebut telah dirinci dandidokumentasikan dengan jelas? | Ya<br><br>Ya , untuk database sendiri, anti virus sendiri, keamanan jaringan sendiri, keamanan hardware dan software sendiri. |

Tabel 3.12 Contoh Dokumen Wawancara pada COBIT 4.1

| **Nama Proses** | **Mengidentifikasi Solusi Otomatis** | **Jawaban** |
|---|---|---|
| **AI1** | | |
| **No.** | **Pertanyaan** | |
| 1 | Apakah kebutuhan fungsional untuk penerapan solusi seperti sistem, jasa, infrastruktur, perangkat lunak dan data telah diidentifikasi? | Kebutuhan fungsional telah teridentifikasi dan telah didokumentasikan didalam dokumen pencatatan aset. |
| 2 | Apakah kebutuhan operasional untuk penerapan seperti sistem, jasa, infrastruktur, perangkat lunak dan data telah diidentifikasi? | Seluruh kebutuhan operasional telah diidentifikasi dan didokumentasikan didalam SOP perusahaan. |

### 3.3.3 Melakukan Uji Kematangan

Proses berikutnya yaitu melakukan uji kematangan berdasarkan metode yang ada pada standar COBIT 4.1. Contoh penilaian kematangan tersebut dapat dilihat pada Tabel 3.13 di halaman 44.

Setelah seluruh penentuan nilai telah ditetapkan, maka dapat langkah berikutnya yaitu melakukan perhitungan *marturity level* pada COBIT 4.1. Contoh kerangka kerja perhitungan *marturity* level pada COBIT 4.1 dapat dilihat pada Tabel 3.13 di halaman 44. Perhitungan tersebut dilakukan secara bertahap, berikut tahapan yang harus dilakukan adalah:

a. Setiap pernyataan pada kontrol keamanan diberikan nilai bobot yang sesuai.
b. Dari hasil wawancara didapatkan nilai tingkat kemampuan pada setiap pernyataan.
c. Pada setiap pernyataan bobot dikalikan dengan tingkat kemampuan masing-masing.
d. Jumlah dari perkalian bobot dan tingkat kemampuan dibagi dengan jumlah bobot yang ada pada seluruh pernyataan dalam satu kontrol keamanan.
e. Hasil dari tahapan sebelumnya merupakan nilai tingkat kemampuan pada kontrol keamanan tersebut.

Setelah didapatkan perhitungan *maturity level* pada COBIT 4.1 kemudian dilakukan perhitungan *maturity level* pada ISO 27002 dengan cara menyetarakan kontrol keamanan antara COBIT 4.1 dengan ISO 27002. Perhitungan *maturity level* pada ISO 27002 dapat dilihat pada Tabel 3.14 di halaman 44

Tabel 3.13 Contoh Tabel Penentuan *Maturity Level* Pada COBIT 4.1

| **Nama Proses** | **Mendefinisikan Arsitektur Informasi** | | | **Apakah sepakat?** | | | | |
|---|---|---|---|---|---|---|---|---|
| **Nomor Proses** | **PO2** | **Level Kedewasaan** | **0** | **Tidak Sama Sekali** | **Sedikit** | **Dalam Tingkatan Tertentu** | **Seluruhnya** | **NILAI** |
| **No.** | **Pernyataan** | | **Bobot** | **0.00** | **0.33** | **0.66** | **1.00** | |
| 1 | Tedapat pengetahuan tentang bagaimana mengembangkan arsitektur informasi | | 0.80 | | | | √ | 0.80 |
| 2 | Terdapat keahlian mengembangkan arsitektur informasi | | 0.80 | | | √ | | 0.53 |
| 3 | Terdapat pertanggung jawaban dalam mengembangkan arsitektur informasi | | 0.80 | | | | √ | 0.80 |
| **Total Bobot =** | | | **2.40** | **Tingkat Kepatutan** | | **0.89** | **Total Nilai** | **2.13** |

Tabel 3.14 Contoh Tabel Penentuan *Maturity Level* Pada ISO 27002

| **ISO/IEC 27002 Classification** | **Key ISO/IEC 27002 Areas** | **Cobit 4.1 IT Processes** | **Tingkat kemampuan Cobit 4.1** | **Tingkat Kemampuan ISO 27002** |
|---|---|---|---|---|
| 6.1 Internal Organisation | 6.0 Organisation of information security | | | |
| 6.1.1 Manajement commitment to information security | | PO3 Determine technological direction. | 3.37 | 3.09 |
| | | PO4 Define the IT processes, organization and relationship. | 3.52 | |
| | | PO6 Communicate management aims and direction. | 3.44 | |
| | | DS5 Ensure systems security. | 2.3 | |

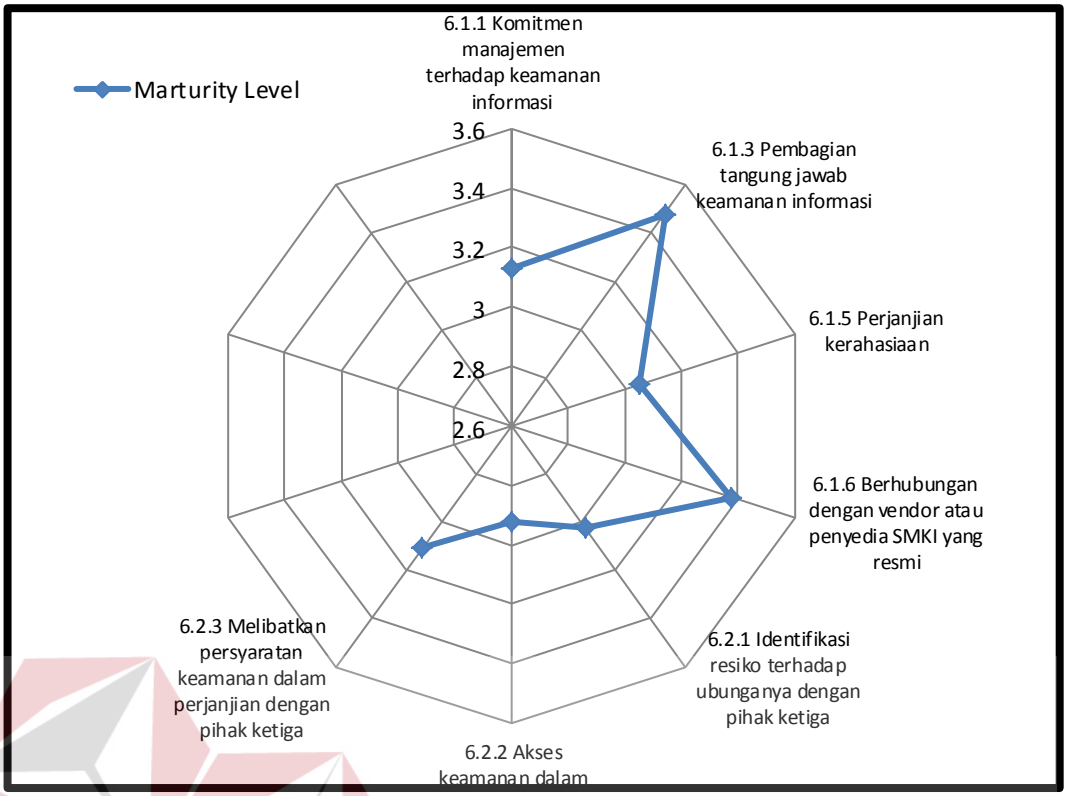
Setelah dihasilkan nilai *maturity level* ISO 27002 yang didapat dari seluruh penyetaraan rata-rata *maturity level* pada COBIT 4.1, selanjutnya nilai-nilai tersebut akan direpresentasikan kedalam diagram jaring yang ada pada Gambar 3.1 di halaman 46.

### 3.3.4 Penentuan Temuan dan Rekomendasi

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil perusahaan, kebijakan, standar, prosedur dan portopolio serta mengobservasi *standard operating procedure* dan melakukan wawancara kepada *auditee.* Seluruh aktivitas tersebut menghasilkan bukti *(evidence)* yang berarti terkait dengan sistem yang berlangsung diperusahaan. Contoh format dari laporan hasil audit keamanan sistem informasi dapat dilihat pada Tabel 3.15 di halaman 45.

Tabel 3.15 Contoh Laporan Hasil Audit Keamanan Sistem Informasi

| Klausul | Objektif Kontrol | Kontrol Keamanan | Temuan | Rekomendasi |
|---|---|---|---|---|
| 6 Organisasi keamanan informasi. | 6.1 Organisasi internal keamanan informasi. | 6.1.1 Komitmen manajemen terhadap keamanan informasi. | Belum ada pakar keamanan informasi. | - Melakukan observasi terhadap kejadian keamanan informasi. |
| | | | | |




Gambar 3.1 Contoh Representasi Nilai *Marturity level* Klausul 6

## 3.4 Tahap Pelaporan Audit Sistem Informasi

Berdasarkan seluruh kertas kerja audit, temuan, dan tanggapan *auditee*, maka langkah selanjutnya adalah menyusun *draft* laporan audit sistem informasi manajemen aset sebagai pertanggungjawaban atas penugasan audit sistem informasi manajemen aset yang telah dilaksanakan. Selanjutnya laporan audit ditunjukan kepada pihak yang berhak saja karena laporan audit sistem informasi manajemen aset merupakan dokumen yang bersifat rahasia. Tahap pelaporan audit sistem informasi yang dilakukan dimulai dengan penyusunan *draft* laporan hasil audit, persetujuan *draft* laporan hasil audit, dan pelaporan hasil audit.