BAB II
LANDASAN TEORI

2.1 Sistem Manajemen Keamanan Informasi

2.1.1 Informasi Sebagai Aset

Informasi adalah salah satu aset bagi sebuah organisasi, yang sebagaimana aset lainnya memiliki nilai tertentu bagi organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan organisasi, meminimalisir kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha. Beragam bentuk informasi yang mungkin dimiliki oleh sebuah organisasi meliputi diantaranya : informasi yang tersimpan dalam komputer (baik *desktop* komputer maupun *mobile* komputer), informasi yang ditransmisikan melalui network, informasi yang dicetak pada kertas, dikirim melalui fax, tersimpan dalam disket, cd atau media penyimpanan lain, informasi yang dilakukan dalam pembicaraan (termasuk percakapan melalui telepon), dikirim melalui telex, email, informasi yang tersimpan dalam database, tersimpan dalam film, dipresentasikan dengan OHP atau media presentasi yang lain, dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi dan ide-ide baru organisasi atau perusahaan.

2.1.2 Keamanan Informasi

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai ‘ *quality or state of being secure-to be free from danger* ‘. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi masing-masing memiliki fokus dan dibangun pada masing-masing kekhususannya. Contoh dari tinjauan keamanan informasi adalah:

1. *Physical Security* yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai

ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

2. *Personal Security* yang overlap dengan '*phisycal security'* dalam melindungi orang-orang dalam organisasi
3. *Operation Security* yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
4. *Communications Security* yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
5. *Network Security* yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Masing-masing komponen di atas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi termasuk sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya. Keamanan informasi melindungi informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha.

2.1.3 Aspek Keamanan Informasi

Keamanan informasi memiliki beberapa aspek yang harus dipahami untuk bisa menerapkannya. Beberapa aspek tersebut, tiga yang pertama adalah yang paling umum, disebut C.I.A *triangle model*, adalah sebagai berikut:

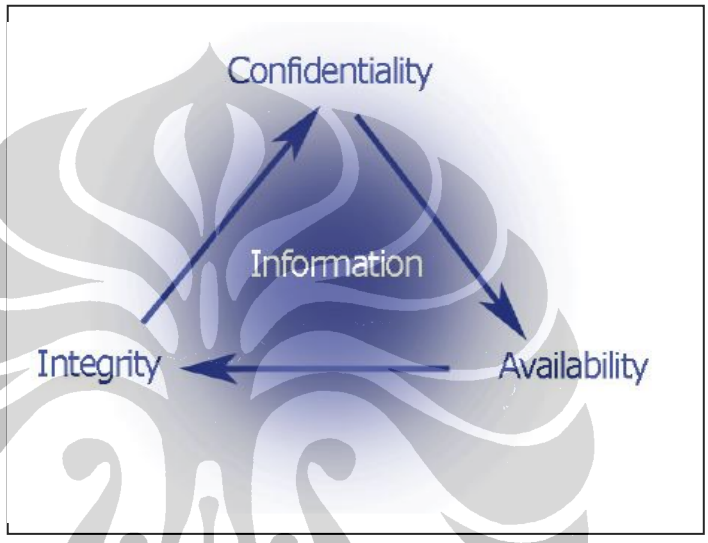
1. *Confidentiality*

   Confidentiality: harus bisa menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu.
2. *Integrity*

   Integrity: harus menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkannya berubah dari aslinya.
3. *Availability*

Availability: adalah aspek keamanan informasi yang menjamin pengguna dapat mengakses informasi tanpa adanya gangguan dan tidak dalam format yang tak bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses informasi.

Seperti terlihat pada gambar 2.1 berikut ini :



Gambar 2.1 Aspek Keamanan Informasi (BS7799)

Selain ketiga aspek tersebut, terdapat lima aspek lainnya yang juga perlu diperhatikan dalam pembahasan keamanan informasi, yaitu:

1 *Privacy*

Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.

2 *Identification*

Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali individu pengguna. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi secara umum dilakukan dalam penggunaan *user name* atau *user ID.*

3. *Authentication*

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang mereka klaim.

4. *Authorization*

   Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia ataupun komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari aset informasi.

5. *Accountability*

   Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktifitas terhadap aset informasi yang telah dilakukan, dan siapa yang melakukan aktifitas itu.

2.1.4 Manajemen keamanan Informasi

Untuk membuat proses keamanan informasi secara efektif, sangat penting memahami beberapa prinsip dalam manajemen. Secara sederhana, manajemen adalah proses untuk mencapai tujuan dengan menggunakan sumberdaya yang ada. Manajer adalah seseorang yang bekerja dengan orang lain dan melalui orang lain dengan cara mengkoordinasi kerja mereka untuk memenuhi tujuan organisasi. Tugas manajer adalah untuk memimpin pengelolaan sumberdaya organisasi, melakukan koordinasi penyelesaian pekerjaan orang-orang dalam organisasi, dan memegang aturan-aturan yang diperlukan untuk memenuhi tujuan organisasi. Diantara aturan-aturan itu adalah:

1. Aturan informasi : mengumpulkan, memproses, dan menggunakan informasi yang dapat mempengaruhi pencapaian tujuan.
2. Aturan interpersonal : berinteraksi dengan *stakeholder* dan orang atau organisasi lain yang mempengaruhi atau dipengaruhi oleh tercapainya tujuan organisasi dimana dia menjadi manajer.
3. Aturan keputusan : memilih diantara beberapa alternatif pendekatan, memecahkan konflik, dilema atau tantangan.

Manajer mengelola sumberdaya organisasi meliputi perencanaan biaya organisasi, otorisasi pengeluaran biaya, dan menyewa pekerja.

Sebagaimana telah disebutkan sebelumnya bahwa manajemen keamanan informasi adalah satu dari tiga bagian dalam komponen keamanan informasi menurut

NSTISSC. Sebagai bagian dari keseluruhan manajemen, tujuan manajemen keamanan informasi berbeda dengan manajemen teknologi informasi dan manajemen umum, karena memfokuskan diri pada keamanan operasi organisasi. Karena manajemen keamanan informasi memiliki tanggung jawab untuk program khusus, maka ada karakteristik khusus yang harus dimilikinya, yang dalam manajemen keamanan informasi dikenal sebagai 6P yaitu:

1. *Planning*

Planning dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu: (1)*strategic planning* yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih, (2)*tactical planning* memfokuskan diri pada pembuatan perencanaan dan mengintegrasi sumberdaya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan, (3)*operational planning* memfokuskan diri pada kinerja harian organisasi. Sebagi tambahannya, planning dalam manajemen keamanan informasi adalah aktifitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi. Ada beberapa tipe planning dalam manajemen keamanan informasi, meliputi :

a. Incident Response Planning (IRP)

IRP terdiri dari satu set proses dan prosedur detil yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumberdaya informasi dan aset organisasi, ketika insiden ini terdeteksi benar-benar terjadi dan mempengaruhi atau merusak aset informasi. Insiden merupakan ancaman yang telah terjadi dan menyerang aset informasi, dan mengancam *confidentiality*, *integrity* atau *availbility* sumberdaya informasi. *Insident Response Planning* meliputi *incident detection*, *incident response*, dan *incident recovery*.

b. *Disaster Recovery Planning* (DRP)

Disaster Recovery Planning merupakan persiapan jika terjadi bencana, dan melakukan pemulihan dari bencana. Pada beberapa kasus, insiden yang dideteksi dalam IRP dapat dikategorikan sebagai bencana jika skalanya sangat besar dan IRP

tidak dapat lagi menanganinya secara efektif dan efisien untuk melakukan pemulihan dari insiden itu. Insiden dapat kemudian dikategorikan sebagai bencana jika organisasi tidak mampu mengendalikan akibat dari insiden yang terjadi, dan tingkat kerusakan yang ditimbulkan sangat besar sehingga memerlukan waktu yang lama untuk melakukan pemulihan.

c. Business Continuity Planning

Business Continuity Planning menjamin bahwa fungsi kritis organisasi tetap bisa berjalan jika terjadi bencana. Identifikasi fungsi kritis organisasi dan sumberdaya pendukungnya merupakan tugas utama *business continuity planning*. Jika terjadi bencana, BCP bertugas menjamin kelangsungan fungsi kritis di tempat alternatif. Faktor penting yang diperhitungkan dalam BCP adalah biaya.

2. *Policy*

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

a. *Enterprise information security policy (EISP)* menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
b. *Issue-spesific security policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.
c. *System-spesific Policy (SSPs)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

3. Programs

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program security education training and awareness. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

4. Protection

Fungsi proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (*risk assessment*) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

5. *People*

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

6. *Project Management*

Komponen terakhir adalah penerapan kedisiplinan manajemen dalam setiap elemen kemanan informasi. Hal ini melibatkan identifikasi dan pengendalian sumberdaya yang dikerahkan untuk keamanan informasi, misalnya pengukuran pencapaian keamanan informasi dan peningkatannya dalam mencapai tujuan keamanan informasi.

2.2 Standarisasi Sistem Manajemen Keamanan Informasi

Ada banyak sekali model manajemen keamanan informasi dan penerapannya karena banyaknya konsultan keamanan informasi yang menawarkannya. Satu yang popular dan banyak diterima adalah model sistem manajemen keamanan informasi yang telah diratifikasi menjadi standarisasi internasional yaitu British Standard 7799 yang menyajikan dua komponen, masing-masing memfokuskan diri pada area yang berbeda dalam praktek manajemen keamanan informasi.

1. BS 7799:1

   Sekarang dikenal sebagai ISO/IEC 17799 setelah diadopsi oleh ISO, disebut sebagai *Information Technology—Code of Practice for Information Security Management.*

2. BS 7799:2

   Komponen ini disebut sebagai *Information Security Management: Specification with Guidance for Use.*

Untuk mendapatkan dokumen ini, organisasi yang akan menerapkannya harus mengeluarkan uang untuk membayarnya.

2.2.1 BS 7799:1

Information Technology-Code of Practice for Information Security Management dalam BS 7799:1 adalah yang banyak dijadikan referensi dan didiskusikan dalam lingkungan model keamanan informasi. Dokumen detil standarisasi ini hanya bisa diperoleh dengan cara membeli, tetapi deskripsi dan struktur umumnya dikenal secara luas sebagai " *The Ten Sections of ISO17799* ". Tujuan ISO/IEC 17799 adalah untuk memberikan rekomendasi manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggungjawab dalam inisiasi, implementasi, atau mengelola keamanan informasi pada organisasinya. BS 7799:1 memberikan ringkasan area keamanan informasi dan menyajikan 127 kendali dalam 10 kategori keamanan informasi.

1. Organizational Security Policy

Diperlukan untuk memberikan arah dan dukungan terhadap manajemen keamanan informasi yang akan diterapkan dalam organisasi. Hal ini tidak selalu menjadi yang pertama dilakukan dalam manajemen keamanan informasi, tetapi bisa merupakan refleksi dari hasil risk assessment yang telah dilakukan. Information Security Policy harus senantiasa dianalisa dan diupdate secara reguler karena adanya perubahan-perubahan ancaman terhadap keamanan informasi.

2. Organizational Security Infrastructure

Tujuan organizational security infrastructure meliputi: mengatur keamanan informasi di dalam organisasi, mengelola keamanan fasilitas pemrosesan informasi organisasi dan aset informasi yang diakses oleh pihak ketiga, mengelola keamanan informasi jika tanggungjawab pemrosesan informasi dilakukan oleh pihak ketiga atau organisasi lain.

3. Asset Classification and Control

Diperlukan untuk mengelola langkah proteksi yang tepat untuk aset organisasi dan menjamin bahwa aset informasi memperoleh tingkat perlindungan yang tepat.

4. Personnel Security

Bertujuan untuk: mengurangi kesalahan manusia, pencurian, kesalahan penggunaan fasilitas; menjamin bahwa pengguna mengetahui ancaman terhadap keamanan informasidan dilengkapi peralatan pendukung kebijakan keamanan informasi dalam kerja mereka; meminimalkan kerusakan akibat insiden keamanan dan malfungsi serta belajar dari insiden yang pernah terjadi.

5. Physical and Environmental Security

Memiliki tujuan mencegah akses tanpa otorisasi, kerusakan, dan interferensi terhadap tempat kerja dan informasi; mencegah kehilangan, kerusakan aset, dan gangguan terhadap aktifitas organisasi; mencegah pencurian informasi dan fasilitas pemrosesan informasi.

6. Communication and Operation Management

Menjamin keamanan operasi pada fasilitas pemrosesan informasi; Meminimalkan resiko kegagalan sistem; melindungi integritas software dan informasi; mengelola integrity dan availability proses informasi dan komunikasi; menjamin perlindungan informasi dalam jaringan dan perlindungan terhadap infrastruktur pendukung; mencegah kerusakan aset dan interupsi terhadap aktifitas organisasi; mencegah kehilangan, modifikasi, atau kesalahan pertukaran informasi antar organisasi.

7. System Access Control

Tujuannya meliputi: pengendalian akses informasi; mencgah akses tanpa otorisasi ke dalam sistem informasi; menjamin perlindungan layanan jaringan; mencegah akses komputer tanpa otorisasi; mendeteksi aktifitas tanpa otorisasi; menjamin keamanan informasi saat menggunakan perangkat bergerak dan jaringan telekomunikasi.

8. System Development and Maintenance

Tujuannya meliputi: menjamin keamanan terbangun dalam sistem operasional organisasi; mencegah kehilangan, modifikasi, atau kesalahan pemakaian data pengguna dalam sistem aplikasi; melindungi confidentiality, authenticity, dan integrity informasi; menjamin proyek teknologi informasi dan aktifitas pendukungnya berada dalam keamanan; mengelola keamanan software aplikasi dan data.

9. Business Continuity Management

Bertujuan untuk melakukan reaksi terhadap gangguan aktifitas organisasi dan proses bisnis yang kritis bagi organisasi ketika terjadi bencana.

10. Compliance

Memiliki tujuan: menghindari pelanggaran terhadap setiap hukum kriminal dan sosial,peraturan perundang-undangan, dan obligasi kontrak dalam setiap kebutuhan keamanan informasi; menjamin terpenuhinya organizational security policy dan standar keamanan informasi dalam penerapan manajemen keamanan informasi organisasi; memaksimalkan efektifitas dan meminimalkan pengaruh kepada atau dari proses audit.

Gambar berikut menyajikan struktur dari kesepuluh wilayah standar. Tiap wilayah berhubungan dengan topik tersendiri yang dibuat dalam pengukuran administratif, teknikal dan fisik. Dijalankan dari atas ke bawah, dengan kata lain pengaruhnya dapat dirasakan dari level manajemen sampai level operasional.

Gambar 2.2 Sepuluh wilayah standar ISO/IEC 17799

2.2.2 BS 7799:2

Bagian ke dua dalam BS 7799 menyajikan implementasi detil menggunakan siklus *Plan-Do-Check-Act*, seperti disebutkan berikut ini:

1. Plan
   - Mendefinisikan scope sistem manajemen keamanan informasi
   - Mendefinisikan kebijakan sistem manajemen keamanan informasi
   - Mendefinisikan pendekatan yang digunakan untuk risk assessment
   - Mengidentifikasi resiko
   - Memperkirakan resiko
   - Mengidentifikasi dan mengevaluasi pilihan perlindungan terhadap resiko
   - Memilih tujuan kendali dan kendalinya
   - Mempersiapkan sebuah *Statement of Aplicability*

2. Do
    - Membuat sebuah formulasi rencana pengelolaan resiko
    - Melakukan Implementasi rencana pengelolaan resiko
    - Melakukan implementasi kendali
    - Melakukan implementasi program pelatihan dan pemahaman keamanan informasi
    - Melakukan pengelolaan kegiatan
    - Melakukan pengelolaan sumberdaya
    - Melakukan implementasi prosedur untuk mendeteksi dan merespon insiden keamanan informasi
3. Check
    - Melakukan prosedur pemantauan
    - Melakukan evaluasi berkala terhadap sistem manajemen keamanan informasi
    - Melakukan pengkajian terhadap tingkatan resiko dan resiko yang dapat diterima
    - Melaksanakan audit sistem manajemen keamanan informasi secara internal
    - Melakukan peninjauan manajemen secara berkala terhadap pelaksanaan sistem manajemen keamanan informasi
    - Melakukan pencatatan aktifitas dan kejadian yang mempengaruhi sistem manajemen keamanan informasi
4. Act
    - Melakukan implementasi peningkatan yang telah diidentifikasi
    - Mengambil tindakan pencegahan dan koreksi
    - Melakukan implementasi pelatihan yang telah diterima
    - Mengkomunikasikan hasil kepada rekan yang berkepentingan
    - Menjamin peningkatan pencapaian tujuan

Siklus Plan-Do-Check-Act digambarkan dalam ilustrasi berikut :

Gambar 2.3 ***Siklus Plan-Do-Check-Act (ISO 17799)***

2.2.3 Security Management Index (SMI)

Satu cara untuk mengetahui sejauh mana sebuah organisasi memenuhi standarisasi ISO 17799 adalah dengan cara melakukan survey terhadap penerapan sistem manajemen keamanan informasi. Callio Technologie Inc. membuat satu set kuisioner yang terdiri dari 127 pertanyaan berkaitan dengan 10 aspek dalam sistem manajemen keamanan informasi menurut BS 7799 :2. Kuesioner ini diperlukan dalam melakukan survey pencapaian sistem manajemen keamanan informasi terhadap standarisasi ISO 17799. Untuk memperoleh keuntungan dari pengukuran *security management index*, Human Firewall Council merekomendasikan hal berikut:

1. Melakukan pengenalan lebih mendalam terhadap 10 kategori dalam manajemen keamanan informasi.
2. Melakukan benchmark penerapan manajemen keamanan informasi dengan melakukan survey

3. Mengevaluasi hasil survey dalam setiap kategori untuk mengidentifikasi kekuatan dan kelemahan
4. Menguji saran untuk peningkatan dalam setiap kategori pada laporan hasil survey
5. Menggunakan hasil SMI untuk memperoleh dukungan peningkatan keamanan informasi.

2.3 Audit Sistem Informasi di Lembaga Pemerintahan

Dengan pemahaman bahwa manajemen TIK di lembaga pemerintahan merupakan suatu hal rumit dan kompleks serta penting bagi layanan publik, maka sudah pasti semua pimpinan lembaga pemerintahan ingin mengetahui kondisi ketatakelolaan TIK yang selama ini telah dilaksanakan di lembaganya. Disinilah peranan Audit Sistem Informasi di dalam suatu lembaga pemerintahan, yaitu untuk memberikan suatu hasil evaluasi yang independen mengenai kesesuaian dan kinerja dari TIK yang ada, apakah sudah dapat melindungi aset TIK, menjaga integritas dan ketersediaan sistem dan data, menyediakan informasi yang relevan dan handal, dan mencapai tujuan organisasi dengan efektif, serta menggunakan sumber daya TIK dengan efisien.

Para pemeriksa dari BPK, BPKP dan Bawasda serta kantor akuntan publik atau konsultan audit yang melakukan audit atas lembaga pemerintahan, diharapkan dapat memberikan suatu hasil evaluasi yang independen atas kesesuaian dan kinerja pengelolaan TIK di lembaga pemerintahan, serta memberikan berbagai rekomendasi yang dapat dengan signifikan meningkatkan ketatakelolaan TIK di lembaga tersebut.

Keterpurukan ketatakelolaan TIK di lembaga pemerintahan saat ini, yang seringkali hanyalah berupa belanja-belanja proyek TIK tanpa kejelasan kesesuaian dan kinerja yang diharapkan, tentunya tidak lepas dari kemampuan para pemeriksa dalam melakukan evaluasi dan memberikan rekomendasi terkait ketatakelolaan TIK serta komitmen dari para pimpinan lembaga dalam menindaklanjuti rekomendasi tersebut. Audit Sistem Informasi tidak dilaksanakan untuk mencari temuan atau kesalahan, namun untuk memberikan kesimpulan serta merekomendasikan perbaikan yang dapat dilakukan atas pengelolaan TIK.

Secara sederhana, dapat dikatakan bahwa Audit Sistem Informasi di lembaga pemerintahaan akan dapat memberikan banyak manfaat, antara lain :

1. Meningkatkan perlindungan atas aset TIK lembaga pemerintahan yang merupakan kekayaan negara, atau dengan kata lain aset milik publik,

2. Meningkatkan integritas dan ketersediaan sistem dan data yang digunakan oleh lembaga pemerintahan baik dalam kegiatan internal lembaga maupun dalam memberikan layanan publik,

3. Meningkatkan penyediaan informasi yang relevan dan handal bagi para pemimpin lembaga pemerintahan dalam mengambil keputusan dalam menjalankan layanan publik,

4. Meningkatkan peranan TIK dalam pencapaian tujuan lembaga pemerintaha dengan efektif, baik itu untuk terkait dengan kebutuhan internal lembaga tersebut, maupun dengan layanan publik yang diberikan oleh lembaga tersebut,

5. Meningkatkan efisiensi penggunaan sumber daya TIK serta efisiensi secara organisasional dan prosedural di lembaga pemerintahan.

Dengan kata lain, Audit Sistem Informasi merupakan suatu komponen dan proses yang penting bagi lembaga pemerintahan dalam upayanya untuk memberikan jaminan yang memadai kepada publik atas pemanfaatan TIK yang telah dilaksanakan oleh lembaga pemerintahan.