Bakuan Audit Keamanan Informasi Kemenpora

Agustus 2012

Bakuan Audit Keamanan Informasi Kemenpora
ISBN : 978- 979- 1278 - 37-9
Ukuran Buku :15,7 cm x 24 cm
Jumlah Halaman: 98 + xii

Penanggung Jawab
Dr. H. Amar Ahmad, M.Si

Ketua
H. Nurdin Ibrachim, SE

Tim Penyusun
Dr. rer. nat. I Made Wiryana, S.Kom, S.Si, MAppSc
Andreas Hadiyono, ST, MMSI
Sutresna Wati, ST, MMSI
Miftah Andriansyah, S.Si, MMSI
Ahmad Musawir, S.Si, M.Si
Bambang Eko Wibowo
M. Ihsan B. Tjenreng, S.Kom
Wulan Asri Meidyasari, S.Si
Kunto Widyatmoko, S.Kom

Sekretariat
Yordania, Fergi Restya, Fetri Asnadi,
Sanen Arafat, Umriansyah, Diah Ariyani,
Riri Hardiyanti, Beni Setyawan

Penyiapan Data
Kemenpora

Diterbitkan Oleh:
Kementerian Pemuda dan Olahraga
Republik Indonesia

Boleh dikutip dengan menyebut sumbernya

Daftar Isi

Ringkasan Eksekutif **vii**

Kata Pengantar **viii**

Sambutan **ix**

1 Pendahuluan **1**
1.1 Tujuan 1
1.2 Lingkup Penggunaan 2
1.3 Dasar Hukum 2

2 Konsep Keamanan Informasi **4**
2.1 Konsep Dasar 4
2.2 Siklus Hidup Keamanan Informasi 5
2.3 Jenis-jenis Audit 6
2.4 Faktor Keamanan Utama 7
2.4.1 Jaringan dan Koneksi Internet 9
2.4.2 Faktor Manusia 9
2.4.3 Perawatan Sistem TI 10
2.4.4 Penanganan Password dan Enksripsi 10
2.4.5 Perlindungan atas Bencana dan Kerusakan . . . 11

3 Standar Sistem Manajemen Keamanan Informasi **12**
3.1 ISO/IEC 27000ISMS 13
3.2 SNI ISO/IEC 27001 - Persyaratan Sistem Manajemen Keamanan Informasi 14
3.3 ISO/IEC 27002 – Code of Practice for ISMS 16
3.4 ISO/IEC 27003 - Information Security Management System Implementation Guidance 17
3.5 ISO/IEC 27004 - Information Security Management Measurement 17
3.6 ISO/IEC27005 - Information Security Risk Management. 18
3.7 ISO/IEC 27006 - Prasyarat Badan Audit dan Sertifikasi. 18

4 Dokumentasi Manajemen Keamanan Informasi 19
4.1 Struktur Dokumentasi 19
4.2 Dokumentasi Tingkat 1 20
4.3 Dokumentasi Tingkat 2 20
4.4 Dokumentasi Tingkat 3 21

5 Audit Keamanan Informasi 27
5.1 Penilaian Resiko Keamanan 27
5.2 Tujuan Audit Keamanan 28
5.3 Saat dan Kekerapan Audit 29
5.4 Tahapan Audit. 30
5.4.1 Perencanaan 30
5.4.2 Pengumpulan Data Audit 33
5.4.3 Pengujian Audit 34
5.4.4 Pelaporan Hasil Audit 34
5.4.5 Perlindungan Data dan Perangkat Audit 35
5.4.6 Penambahan dan Tindak Lanjut 35

6 Pelaksanaan Audit IS 36
6.1 Persetujuan Pimpinan dan Penetapan Organisasi 36
6.2 Pembagian Tanggung Jawab 37
6.2.1 Siklus Audit IS 39
6.2.2 Pengawasan Audit IS 39
6.2.3 Tim Audit IS 39
6.2.4 Struktur Keamanan Informasi suatu Organisasi . 41
6.2.5 Evaluasi Audit IS 41
6.3 Mendefinisikan Cakupan (Ruang Lingkup) 44
6.4 Teknik Audit IS 45
6.5 Melakukan Analisis Kesenjangan (*Gap Analysis*) 46
6.6 Penilaian Resiko dan Rencana Penilaian Resiko 46
6.7 Menetapkan Kontrol dan Sasaran Kontrol 47
6.8 Menetapkan Kebijakan dan Prosedur Audit SMKI . . . 47
6.9 Sosialisasi dan Pelatihan 47
6.10 Menerapkan Kebijakan dan Prosedur 49
6.11 Mengukur Efektivitas Kendali 50

7 Level Keamanan Informasi 52

8 Sumber Daya Manusia Tim Audit **55**
8.1 Etika Profesi 55
8.2 Tanggung Jawab Klien 56
8.3 Tanggung Jawab Auditor SI 57

9 Bakuan Pelaksanaan Audit Keamanan Informasi **59**
9.1 Langkah 1 - Persiapan Audit IS 61
9.2 Langkah 2 - Implementasi audit 63
9.3 Langkah 3 - Audit Operasional 64
9.4 Langkah 4 - Audit Infrastruktur 65
9.5 Langkah 5 - Evaluasi Audit *On-site* 67
9.6 Langkah 6 - Laporan Audit 67

10 Tindak Lanjut Audit **71**
10.1 Pengawasan dan Tindak Lanjut 73
10.2 Identifikasi Rekomendasi dan Perencanaan 73
10.3 Status Aksi dan Kemajuan 74

11 Pengujian dan Latihan **76**
11.1 Jenis Uji dan Latihan 77
11.2 Dokumen Latihan dan Pengujian 79
11.3 Melaksanakan Pengujian dan Latihan 82

12 Indeks KAMI **85**

13 Penutup **89**

Daftar Gambar

2.1 Proses Iteratif dari Manajemen Keamanan Informasi . . 6

3.1 Relasi antar keluarga standar SMKI 13

4.1 Struktur Organisasi Dokumentasi SMKI 19

5.1 Dokumen keamanan TI dalam pemerintahan 28
5.2 Diagram Tahapan Umum Audit 31

6.1 Fase prosedur audit IS dari sudut pandang organisasi . 38
6.2 Kinerja audit IS dari sudut pandang organisasi 40
6.3 Struktur Keamanan Informasi: Organisasi Besar 42
6.4 Struktur Keamanan Informasi: Organisasi Sedang . . . 42
6.5 Struktur Keamanan Informasi: Organisasi Kecil 43
6.6 Empat prinsip dasar dalam evaluasi 43

9.1 Langkah Pelaksanaan Audit IS 60

10.1 Tindak Lanjut atas Rekomendasi yang diberikan 72

Daftar Tabel

3.1 Peta PDCA dalam proses SMKI 15

4.1 Cakupan dokumen tingkat 1 (Prosedur) 22
4.2 Cakupan dokumen tingkat 1 (Prosedur) 23
4.3 Cakupan dokumen tingkat 1 (Prosedur) 24
4.4 Cakupan dokumen tingkat 2a (Kebijakan) 25
4.5 Cakupan dokumen tingkat 2b (Kebijakan) 26

6.1 Nilai standar untuk pengeluaran personil suatu audit IS . 41
6.2 Contoh Sasaran Keamanan Informasi 48
6.3 Pengukuran Ketercapaian Keamanan Informasi 51

9.1 Waktu Relatif yang diperlukan pada setiap langkah pada pelaksanaan audit IS 61
9.2 Visualisasi Warna Penekanan atas Kelemahan Keamanan 68

11.1 Jenis Latihan 79
11.2 Contoh Skrip Latihan 82

12.1 Kelengkapan Dokumen SMKI (1) 86
12.2 Kelengkapan Dokumen SMKI (2) 87

Ringkasan Eksekutif

Audit keamanan informasi (IS) atau penilaian resiko keamanan informasi merupakan komponen utama dalam Sistem Manajemen Keamanan Informasi (SMKI), walaupun tidak mencakup semua elemen dalam SMKI. Dalam buku ini diberikan model gambaran umum mengenai audit keamanan informasi dan penilaian resiko keamanan informasi.

Melalui pengenalan model ini, diharapkan pihak yang terlibat dalam keamanan sistem dan teknologi informasi seperti manajemen tingkat puncak, manajer, petugas/staf teknologi informasi, administrator sistem dan pihak yang bertanggung jawab dapat lebih memahami soal keamanan informasi, mulai dari perencanaan hingga evaluasi keamanan informasi. Audit keamanan informasi merupakan salah satu fase/proses yang harus dilakukan oleh organisasi/institusi untuk mendeteksi adanya kesalahan, deviasi, atau kerusakan dalam SMKI organisasi agara pelaksanaan sistem teknologi informasi dalam organisasi dapat berjalan aman, efektif dan efisien.

Panduan ini mengadopsi metode, teknologi, cakupan dan dokumentasi dasar yang harus ada mulai skala minimal hingga skala penuh. Panduan ini dibuat untuk acuan umum di lingkungan Kementerian Pemuda dan Olahraga yang memiliki sistem informasi yang tersebar dan yang sebagian saling terkoneksi di tingkat kantor pusat dan kantor daerah. Pelaksanaan audit di lingkungan Kemenpora dapat menggunakan panduan ini sebagai dokumen referensi atau rujukan mulai dari tahap perencanaan hingga evaluasi dan dokumentasi. Untuk mencapai level SMKI yang baik, maka diharapkan keterlibatan semua pihak untuk secara bertanggung jawab melaksanaan audit keamanan informasi sesuai dengan panduan ini.

Jakarta, Agustus 2012

Tim Penyusun
Kementerian Pemuda dan Olahraga

Kata Pengantar

Pengelolaan Teknologi Informasi dan Komunikasi yang baik akan mendorong hadir dan terwujudnya *good governance*. Metodologi dan tata kelola yang baik merupakan suatu prasyarat yang menjadi kewajiban dalam pengelolaan sebuah sistem yang baik. Dengan tata kelola yang baik, maka sistem informasi yang *accountable* serta *sustainable* dapat tercapai bagi badan pemerintah dan dapat memberikan manfaat kepada publik seluas-luasnya.

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik. Hal ini disebabkan oleh peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TIK akan terganggu jika informasi sebagai salah satu objek utama tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). untuk mempermudah kegiatan penilaian mandiri (*self assessment*) tentang kondisi keamanan informasi, maka perlu diterbitkan Panduan Bakuan Audit Keamanan Informasi Kemenpora.

Panduan ini akan direvisi sesuai kebutuhan dan tingkat kematangan penerapan tata kelola keamanan informasi di lingkungan Kemenpora baik di tingkat pusat maupun di tingkat/kantor daerah.

Jakarta, Agustus 2012

Jakarta, Agustus 2012
Plt. Kepala Biro Humas,
Hukum dan Kepegawaian

Dr. H. Amar Ahmad, M.Si

Sambutan

Sebagai lembaga negara yang memiliki keinginan untuk menuju tata kelola pemerintahan yang sesuai dengan konsep *good governance*, Kementerian Pemuda dan Olahraga berusaha mengikuti *good practice* yang ada dalam semua sisi pengelolaannya, tidak terkecuali dalam pengelolaan Teknologi Informasi dan Komunikasi. Pemanfaatan Teknologi Informasi dan Komunikasi (TIK) diyakini dapat memungkinkan terlaksananya prinsip-prinsip *good governance* secara lebih baik.

Portal Kemenpora yang telah beroperasi lebih dari dua tahun ini dengan berita mengenai kegiatan di lingkungan Kemenpora serta kegiatan kepemudaan dan keolahragaan, merupakan salah satu upaya menuju hal tersebut. Pemberitaan di portal Kemenpora selain untuk mempresentasikan kinerja Kemenpora juga di maksudkan sebagai salah satu bentuk pertanggungjawaban langsung kepada publik, menyangkut kegiatan-kegiatan telah, sedang dan akan berlangsung.

Pemanfaatan TIK yang baik pada suatu lingkungan kementerian membutuhkan beberapa persyaratan yang perlu dipenuhi, seperti kepercayaan (*trust*), akuntabilitas yang terukur serta keamanan. Untuk memenuhi hal tersebut, maka disusun panduan ini agar kegiatan menyangkut TIK dapat memenuhi kaidah-kaidah audit sistem yang baik.

Dengan telah selesainya penyusunan Panduan ini. Kami mengucapkan selamat kepada Biro Hukum, Humas, dan Kepegawaian, khususnya bagian Sistem Informasi, yang telah bekerja keras dan serius. Ucapan terima kasih dan penghargaan juga kami sampaikan kepada secara pihak yang telah membantu dan memberikan masukan, saran dan gagasan sehingga Panduan yang baru pertama kali di terbitkan oleh Kementerian Pemuda dan Olahraga ini dapat diselesaikan dengan baik. Langkah berikutnya adalah sosialisasi bagi seluruh pemangku kepentingan di Kementerian Pemuda dan Olahraga agar maksud dari tujuan pembuatan Panduan ini dapat tercapai

Jakarta, Agustus 2012
Sekretaris
Kementerian Pemuda dan Olahraga

Dra. Yuli Mumpuni Widarso

1

Pendahuluan

Pada saat ini sebagian besar proses pengelolaan adminsistrasi di badan pemerintah telah mulai menggunakan sistem elektronik yang menyimpan begitu besar informasi secara digital dan menggunakan jalur atau jaringan teknologi informasi dalam berkomunikasi. Dengan kata lain, kegiatan bisnis, administrasi, dan publik bergantung pada teknologi informasi apa yang digunakannya. Oleh karena itu, suatu hal yang penting untuk memahami dan mengimplementasikan keamanan informasi pada sistem informasi yang digunakannnya, baik untuk kalangan organisasi bisnis/swasta maupun instansi pemerintahan.

Penerapan keamanan informasi dimaksudkan untuk mengatasi segala masalah dan kendala baik secara teknis maupun non-teknis seperti faktor ketersediaan (*availability*), kerahasiaan (*confidentiality*), dan kesatuan (*integrity*). Audit keamanan informasi merupakan bagian dari setiap manajemen keamanan informasi yang sukses. Audit keamanan informasi merupakan suatu alat atau perangkat dalam menentukan, mendapatkan, dan mengelola setiap level keamanan dalam suatu organisasi.

1.1 Tujuan

Tujuan utama dari penyusunan panduan audit keamanan informasi (selanjutnya ditulis audit IS. IS: *Information Security*) adalah memberikan panduan pengelolaan, menyediakan manajemen, dan khususnya bagi petugas keamanan TI (Teknologi Informasi) sebagai pihak

yang mendukung implementasi dan optimasi keamanan informasi.

Audit IS dimaksudkan untuk meningkatkan tingkat/level keamanan informasi, mencegah rancangan keamanan informasi yang tidak layak, dan mengoptimalkan efisiensi benteng keamanan, dan proses keamanan informasi itu sendiri. Audit ini akan memastikan atau menjamin berjalannya proses operasional, reputasi dan aset suatu organisasi.

Hasil dari audit IS adalah tersusunnya dokumen laporan audit yang terkait pada keamanan teknologi informasi yang digunakan di lingkungan organisasi tersebut.

1.2 Lingkup Penggunaan

Penggunaan panduan ini bersifat umum, dalam arti semua petugas yang bertanggungjawab dalam pelaksanaan terkait keamanan informasi dapat menggunakannya. Di lingkungan Kementerian Pemuda dan Olahraga yang memiliki kantor pusat dan kantor daerah dapat menggunakan panduan ini agar tiga kriteria ujian keamanan informasi dapat ditempuh dengan optimal. Area penggunaan dibedakan menjadi dua menurut geografis dan tingkatannya yaitu kantor pusat dan kantor daerah.

1.3 Dasar Hukum

Di dalam menuliskan panduan ini maka beberapa aturan digunakan sebagai dasar hukum yaitu:

- **Undang-Undang Republik Indonesia No. 11 Tahun 2008**. Undang-Undang mengenai Informasi dan Transaksi Elektronik (UUITE) adalah ketentuan yang berlaku untuk setiap orang yang melakukan perbuatan hukum sebagaimana diatur dalam Undang-Undang ini, baik yang berada di wilayah hukum Indonesia maupun di luar wilayah hukum Indonesia, yang memiliki akibat hukum di wilayah hukum Indonesia dan/atau di luar wilayah hukum Indonesia dan merugikan kepentingan Indonesia. Undang-Undang Informasi dan Transaksi Elektronik (UUITE) mengatur berbagai perlindungan hukum atas kegiatan yang memanfaatkan internet sebagai medianya, baik transaksi maupun pemanfaatan informasinya. Pada UUITE ini juga

diatur berbagai ancaman hukuman bagi kejahatan melalui internet. UUITE mengakomodir kebutuhan para pelaku kegiatan di internet dan masyarakat pada umumnya guna mendapatkan kepastian hukum, dengan diakuinya bukti elektronik dan tanda tangan digital sebagai bukti yang sah di pengadilan.

- **Undang-Undang Republik Indonesia No. 14 tahun 2008**, tentang Keterbukaan Informasi Publik adalah salah satu produk hukum Indonesia yang dikeluarkan dalam tahun 2008 dan diundangkan pada tanggal 30 April 2008 dan mulai berlaku dua tahun setelah diundangkan. Undang-undang yang terdiri dari 64 pasal ini pada intinya memberikan kewajiban kepada setiap Badan Publik untuk membuka akses bagi setiap pemohon informasi publik untuk mendapatkan informasi publik, kecuali beberapa informasi tertentu.

- **Standard Nasional Indonesia ISO/IEC 27001:2009**. Standard Nasional Indonesia ini merupakan pengadopsian standard ISO/IEC 27001:2009 mengenai Sistem manajemen keamanan informasi. Pengelolaan serta kegiatan audit di Indonesia sebaiknya mengacu pada standard nasional ini.

- **Surat Edaran Menteri Komunikasi dan Informatika. No. 05/SE/M.KOMINFO/07/2001**, tentang Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Sebagai upaya meningkatkan kualitas dan menjamin penyediaan pelayanan publik yang sesuai dengan tata kelola pemerintahan dan korporasi yang baik, khususnya pengelolaan informasi yang menggunakan Sistem Elektronik, maka setiap Penyelenggara Pelayanan Publik harus menerapkan Tata Kelola Keamanan Informasi secara andal dan aman serta bertanggung jawab sesuai dengan ketentuan Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Penyelenggara Pelayanan Publik adalah setiap institusi penyelenggara negara, korporasi, lembaga independen yang dibentuk berdasarkan Undang-Undang untuk kegiatan pelayanan publik, dan badan hukum lain yang dibentuk semata-mata untuk kegiatan pelayanan publik

2

Konsep Keamanan Informasi

2.1 Konsep Dasar

Terdapat tiga kriteria mendasar dari keamanan teknologi informasi:

Kerahasiaan (*confidentiality*). Informasi bersifat rahasia dan harus dilindungi terhadap keterbukaan dari yang tidak berhak atau berkepentingan.

Ketersediaan (*availability*). Layanan, fungsi sistem teknologi informasi, data dan informasi harus tersedia bagi penggunaa saat diperlukan

Integritas (*integrity*). Data harus komplit dan tidak diubah. Dalam teknologi informasi, kata ”informasi” terkait dengan ”data”. Hilangya integritas informasi berarti data tersebut telah tanpa adanya ijin atau ilegal.

Sedangkan untuk penggunaan Sistem Informasi yang terkait pada suatu keamananan negara. Biasanya ditambahkan kriteria tambahan (biasa diterapkan di negara Uni Eropa). Kriteria tersebut adalah:

Ketidakbergantungan (independency). Suatu sistem yang aman dalam pengoperasian dan perawatannya tidak boleh bergantung pada entitas luar. Ketika suatu badan pemerintah bergantung pada entitas luar (apalagi perusahaan/organisasi luar negeri), maka badan tersebut menjadi tidak aman.

Adapun istilah lainnya terkait keamanan informasi seperti:

Autentikasi. Pada saat seseorang log in ke dalam sistem, sistem tersebut akan menjalakan pemeriksaan proses autentikasi untuk memverifikasi identitas orang tersebut.

Autorisasi. Merupakan proses pemeriksaan apakah seseorang, komponen TI atau aplikasi diberikan otoritas/ijin untuk menjalan aksi tertentu.

Perlindungan data. Merujuk pada perlindungan data personal terhadap penyalahgunaan dari pihak ketiga

Keamanan data. Merujuk pada perlindungan data terkait dengan kebutuhan atas kerahasiaan, ketersediaan dan integritas.

Cadangan Pendukung (Backup) Data. Melibatkan tindasan atau *copy* dari data yang ada untuk mencegah kehilangan atau kerusakan data aslinya/utama.

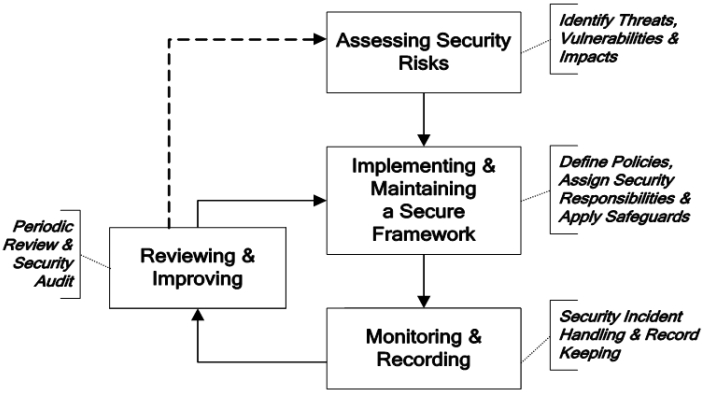
Pengujian penetrasi. Pengujian dengan mensimulasikan serangan terhadapa sistem TI. Digunakan untuk menguji efisiensi perlindungan keamanan (*safeguards*) yang ada.

Penilaian atau Analisis Resiko: Menyediakan informasi atas probabilitas dari kejadian kerusukaan dan konsekuensi negatif dari kerusakan.

Kebijakan Keamanan: Dalam kebijakan keamanan, tujuan dari keamanan diformulasikan sesuai dengan kebijakkkan masing masing institusi baik swasta maupun pemerintah.

2.2 Siklus Hidup Keamanan Informasi

Manajemen Keamanan Informasi dapat dijelaskan dalam bentuk siklus hidup yang memiliki proses iteratif yang diperlukan dalam pengawasan dan pengendalian. Setiap proses terdiri dari aktifitas yang berbeda sebagaimana pada Gambar 2.1.



Gambar 2.1: Proses Iteratif dari Manajemen Keamanan Informasi

Penilaian resiko keamanan informasi merupakan langkah awal untuk mengevaluasi dan mengidentifikasi resiko dan konsekuensi yang terkait keringkihan (vulnerabilitas), dan untuk menyediakan bahan bagi manajemen untuk menetapkan program keamanan yang berbiaya efektif.

2.3 Jenis-jenis Audit

Tujuan utama dari audit teknologi informasi (audit TI) awalnya untuk memeriksa sistem akuntansi berdaya dukung TI. Sudut pandang tersebut tidak dapat diterapkan lagi secara maksimal, karena sebagaimana diketahui kebanyakan sistem yang sekarang sudah terkoneksi kuat dalam banyak jaringan dan tingkat ketergantungan yang tinggi anatara sistem dengan proses bisnis.

Oleh karena itu, seluruh infrastruktur TI suatu organisasi akan diperiksa manakala menjalankan proses audit TI atau audit IS. Dalam audit TI, selalu diperhatikan tiga kriteria pengujian utama yaitu:

- efisiensi.
- keamanan.
- kebenarannya.

Perbandingan yang mencolok antara audit TI dengan audit IS adalah merupakan kegiatan audit gaya baru, yang menekankan pada pemeriksaan menyeluruh akan keamanan informasi. Hal tersebut dimaksudkan bahwa pada setiap level atau tingkatan, mulai dari pembangunan keamanan informasi suatu organisasi, sampai faktor manusia/personil akan diperiksa dan diuji dengan ketat. Dua kriteria, yakni efisiensi dan kebenaran akan diperiksa pada urutan selanjutnya setelah kriteria keamanan.

2.4 Faktor Keamanan Utama

Ada 7 (tujuh) faktor perlindungan keamanan utama yang perlu dipertimbangkan:

- Pendekatan sistematik atas keamanan TI
- Keamanan sistem TI
- Jaringan dan koneksi internet
- Faktor manusia
- Perawatan sistem TI: penanganan atas update yang relevan dengan keamanan
- Penggunaan mekanisme keamanan: penanganan password dan eksripsi
- Perlindungan atas bencana dan kerusakan oleh elemen-elemen

Adapun dalam masing masing tujuh faktor tersebut dijelaskan langkah-langkah yang harus/tidak perlu dijalankan dalam penerapan keamanan utama. Secara sistematik beberapa hal harus perlu dipertimbangkan:

- Aspek keamanan TI harus dipertimbangkan secara jelas di awal semua proyek
- Perlu dipertimbangkan pendekatan solusi alternatif, ketika keterbatasan sumber daya
- Tujuan keamanan TI dalam rangka pendefinisian *safeguard* harus dispesifikasikan.

- Perlu dilakukan kontrol yang baik untuk setiap tujuan keamanan dan *safeguard* yang sesuai dengannya
- Rencana aksi harus memiliki prioritas yang jelas, sebagaimana harus adanya tujuan keamanan dan safeguards
- Beberapa prasyarat celah keamanan yang harus dihindari.
- Tanggung jawab harus didefinisikan.
- Adanya kebijakkan keamanan dan tanggung jawab harus diketahui.
- Keamanan TI harus diperiksa secara reguler.
- Rutinitas kerja yang ada dan kebijakan keamanan untuk menjamin kesesuaian dan efisiensi perlu diperiksa secara reguler.
- Manajemen keamanan yang penuh, dalam jangka panjang perlu direncanakan.
- Dokumentasi kebijakkan keamanan dalam konsep keamanan harus ada.

Di dalam menyediakan perlindungan keamanan sistem TI, beberapa hal harus dipertimbangkan, yaitu:

- Mekanisme perlindungan keamanan yang ada harus digunakan.
- Perangkat lunak anti virus dalam organisasi TI harus digunakan.
- Kemungkinan akses data untuk kebutuhan level yang minimum harus dibatasi.
- Peran dan profil ke semua pengguna sistem harus ditunjuk.
- *Previlages* administrator harus dibatasi untuk ke hal yang lebih penting
- *Program privilages* harus dibatasi.
- Setting/aturan standar dari pabrik perangkat keras/lunak harus dilakukan modifikasi secukupnya
- Dokumentasi produk dan manual harus dibaca.
- Dokumentasi sistem dan rincian instalasi harus dibuat dan diperbaharui.

2.4.1 Jaringan dan Koneksi Internet

Jaringan dan koneksi Internet, saat ini sudah tidak terpisahkan sebagai bagian dari suatu pemanfaatan Teknologi Informasi di badan pemerintah. Untuk itu beberapa hal terkait dengan jaringan perlu diperhatikan, antara lain:

- Firewall keamanan harus memenuhi kebutuhan minimum tertentu yang ditetapkan
- Data yang diberikan untuk pihak luar harus dibatasi hingga ke tingkat minimum.
- Fungsionalitas program dan layanan yang diberikan untuk pihak luar harus dibatasi hingga ke tingkat minimum
- Tidak diperbolehkan aksi yang beresiko, terutama terkait dengan penanganan web browser
- Perlu dilatihnya peringatan tertentu terkait dengan attachment e-mail untuk mencegah masuknya malware lewat email.
- Stand-alone PC digunakan untuk selancar internet merupakan solusi berbiaya ringan untuk kebanyakkan masalah keamanan terkait internet.

2.4.2 Faktor Manusia

Manusia merupakan titik terlemah dalam kaitannya dengan keamanan sistem. Untuk itu faktor manusia harus menjadi perhatian utama di dalam pengelolaan sistem. Beberapa hal perlu diperhatikan:

- Kebutuhan dan kebijakkan keamanan harus diikuti dengan baik dan benar
- Perlu adanya keketatan dan keteraturan pada ruang kerja dan tidak informasi bersifdat sensitif tidak dengan mudah dapat diakses
- Pencegahan khusus harus diambil dalam kasus perawatan dan perbaikan kerja
- Perlu adanya pelatihan teratur bagi staff

- Perlu adanya penilaian mandiri yang jujur dan untuk beberapa hal perlu mengundang pakar untuk saran dan perbaikan
- Perlu adanya audit untuk semua tujuan keamanan
- Konsekusensi dari peretasan keamanan harus spesifik dan dipublikasikan
- Peretasan keamanan yang terdeteksi harus diberikan reaksi

2.4.3 Perawatan Sistem TI

Perawatan TI tidak saja terkait pada perawatan rutin untuk perangkat keras dan jaringan saja. Tetapi juga meliputi perangkat lunak yang dikenal dengan istilah melalukan "*patching*" (penambalan) secara rutin. Pada dasarnya keamanan adalah suatu proses, bukanlah suatu produk. Jadi suatu sistem yang setelah diinstal dengan baik dan menjadi aman, maka tidak dapat selalu menjadi aman bila tidak dilakukan perawatan, penambalan, dan pengkinian yang dibutuhkan.

Untuk itu beberapa hal perlu diperhatikan pada saat menentukan stategi perawatan dalam upaya menjaga keamanan sistem adalah sebagai berikut:

- Update keamanan harus diinstal secara reguler
- Penelitian rinci harus dilakukan pada periode reguler pada karakteristik keamanan dari perangkat lunak yang digunakan
- Perlu adanya rencana aksi untuk menginstal setiap update keamanan
- Perlu pengujian pada pengubahan perangkat lunak

2.4.4 Penanganan Password dan Enksripsi

Salah satu penggunaan mekanisme keamanan minimal saat ini adalah password dan enkripsi. Dalam pengelolaan Access Control kepada sumber daya sistem informasi, maka pengguna wajib menggunakan password dan enkripsi. Hal ini bertujuan untuk mengontrol sehingga sistem hanya dapat diakses oleh mereka yang berhak saja. Sedangkan mereka yang tak berhak tak dapat mengakses sistem.

Penggunaan password dan enkripsi harus mempertimbangkan hal berikut ini:

- Perlu dipilihnya secara selektif atas mekanisme keamanan
- Password harus dipilih secara aman
- Password blank atau password bawaan awal harus diganti
- Workstation harus tetap aman walau tanpa kehadirannya pengguna dengan screen saver terproteksi password
- Perlu perlindungan atas data dan sistem yang sensitif

2.4.5 Perlindungan atas Bencana dan Kerusakan

Sebaik-baiknya instalasi sistem telah direncanakan dan diimplementasikan, tetapi sebagai pengelola sistem harus mempertimbangkan kemungkinan terburuk yang terjadi. Sebagai contoh beberapa pertimbangan yang perlu dilakukan terhadap terjadinya bencana adalah:

- Perlu dibuatnya daftar periksa darurat (*emergency checklist*) dan setiap pengguna harus terbiasa dengannya
- Perlu adanya backup reguler untuk semua data penting
- Perlu adanya perlindungan yang baik dari api, panas berlebihan, kerusakan karena air dan listrik terhadap sistem TI
- Perlu diterapkannya perlindungan anti penerobos dan perlindungan terhadap akses yang ilegal
- Perlu dicatat dalam daftar inventaris semua perangkat keras dan perangkat lunak.

3

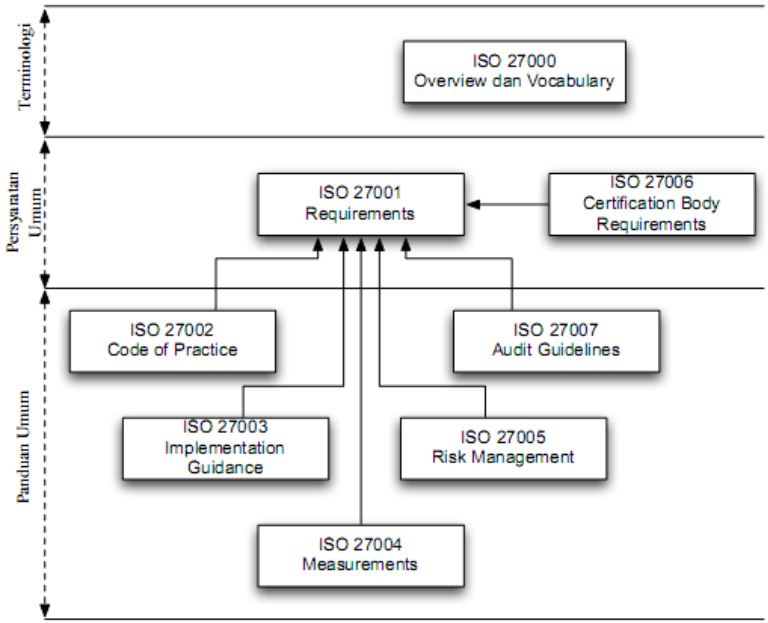
Standar Sistem Manajemen Keamanan Informasi

Sejak tahun 2005, International Organization for Standardization(ISO) atau Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang Information Security Management Systems (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan.

Standar SMKI ini dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri dari:

- ISO/IEC 27000:2009 – ISMS Overview and Vocabulary
- ISO/IEC 27001:2005 – ISMS Requirements
- ISO/IEC 27002:2005– Code of Practice for ISMS
- ISO/IEC 27003:2010 – ISMS Implementation Guidance
- ISO/IEC 27004:2009 – ISMS Measurements
- ISO/IEC 27005:2008 – Information Security Risk Management
- ISO/IEC 27006: 2007 – ISMS Certification Body Requirements
- ISO/IEC 27007 – Guidelines for ISMS Auditing

Dari standar seri ISO 27000 ini, hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi Badan Standarisasi Nasional



Gambar 3.1: Relasi antar keluarga standar SMKI

(BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009. Catatan: angka di belakang tanda titik dua (:) menunjukkan tahun terbit.

3.1 ISO/IEC 27000ISMS

Standar ini dirilis tahun 2009, memuat prinsip-prinsip dasar Information Security Management Systems(Sistem Manajemen Keamanan Informasi – SMKI), definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang dalam tahap pengembangan. Hubungan antar standar keluarga ISO 27000 dapat dilihat pada Gambar 3.1.

3.2 SNI ISO/IEC 27001 - Persyaratan Sistem Manajemen Keamanan Informasi

SNI ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI).

Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (*review*), pemeliharaan dan peningkatan suatu SMKI. Pendekatan proses mendorong pengguna menekankan pentingnya:

- Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
- Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
- Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
- Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran

Model **PLAN – DO – CHECK – ACT (PDCA)** diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti Tabel 3.1.

Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut:

- Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi)
- Tanggung jawab manajemen

Tabel 3.1: Peta PDCA dalam proses SMKI

PLAN (Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola resiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dari sasaran
DO (menerapkan dan mengoperasikan SMKI	Menetapkan dan mengoperasikan kebijakan SMKI
CHECK (memantau dan melakukan tinjau ulang SMKI)	Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya
ACT (memelihara dan meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatkan yang berkelanjutan.

- Audit internal SMKI
- Manajemen tinjau ulang SMKI

Disamping persyaratan utama di atas, standar ini mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 11 area pengamanan sebagai berikut:

- Kebijakan keamanan informasi
- Organisasi keamanan informasi
- Manajemen aset
- Sumber daya manusia menyangkut keamanan informasi
- Keamanan fisik dan lingkungan
- Komunikasi dan manajemen operasi
- Akses kontrol
- Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
- Pengelolaan insiden keamanan informasi
- Manajemen kelangsungan usaha (business continuity management)
- Kepatuhan

3.3 ISO/IEC 27002 – Code of Practice for ISMS

ISO/IEC 27002 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan dalam ISO/IEC 27001.

ISO/IEC27002 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil kajian risiko yang telah dilakukannya. Pengguna juga dapat memilih kontrol di luar daftar kontrol yang dimuat standar ini sepanjang sasaran kontrolnya dipenuhi.

3.4 ISO/IEC 27003 - Information Security Management System Implementation Guidance

Tujuan dari ISO/IEC 27003 adalah untuk memberikan panduan bagi perancangan dan penerapan SMKI agar memenuhi persyaratan ISO 27001. Standar ini menjelaskan proses pembangunan SMKI meliputi persiapan, perancangan dan penyusunan dan pengembangan SMKI yang digambarkan sebagai suatu kegiatan proyek.

Sebagai kegiatan proyek, tahapan utama yang dijelaskan dalam standar ini meliputi:

1. Mendapatkan persetujuan manajemen untuk memulai proyek SMKI
2. Mendefinisikan ruang lingkup, batasan dan kebijakan SMKI
3. Melakukan analisis persyaratan SMKI
4. Melakukan kajian risiko dan rencana penanggulangan risiko
5. Merancang SMKI
6. Merencanakan penerapan SMKI

3.5 ISO/IEC 27004 - Information Security Management Measurement

Standar yang diterbitkan pada bulan Desember 2009 ini menyediakan panduan penyusunan dan penggunaan teknik pengukuran untuk mengkaji efektivitas penerapan SMKI dan kontrol sebagaimana dipersyaratkan ISO/IEC 27001. Standar ini juga membantu organisasi dalam mengukur ketercapaian sasaran keamanan yang ditetapkan.

Standar ini mencakup bagian utama sebagai berikut:

- Penjelasan tentang pengukuran keamanan informasi;
- Tanggung jawab manajemen;
- Pengembangan metode pengukuran;
- Pengukuran operasi;

- Analisis data dan pelaporan hasil pengukuran;
- Evaluasi dan perbaikan program pengukuran keamanan informasi.

3.6 ISO/IEC27005 - Information Security Risk Management.

Standar ini menyediakan panduan bagi kegiatan manajemen risiko keamanan informasi dalam suatu organisasi, khususnya dalam rangka mendukung persyaratan-persyaratan SMKI sebagaimana didefinisikan oleh ISO/IEC 27001. Standar ini diterbitkan pada bulan Juni 2008.

3.7 ISO/IEC 27006 - Prasyarat Badan Audit dan Sertifikasi.

Standar ini menetapkan persyaratan dan memberikan panduan bagi organisasi yang memiliki kewenangan untuk melakukan audit dan sertifikasi sistem manajemen keamanan informasi (SMKI). Standar ini utamanya dimaksudkan untuk mendukung proses akreditasi Badan Sertifikasi ISO/IEC 27001 oleh Komite Akreditasi dari negara masing-masing.

4

Dokumentasi Manajemen Keamanan Informasi

4.1 Struktur Dokumentasi

Pekerjaan audit sistem TI membutuhkan dokumentasi yang baik. Berlandaskan dokumentasi inilah dapat dilakukan assestment serta perbaikan semestinya. Struktur dokumentasi sistem manajemen keamanan informasi pada umumnya terdiri dari 3 (tiga) level/tingkatan, seperti terlihat pada Gambar 4.1.

Gambar 4.1: Struktur Organisasi Dokumentasi SMKI

4.2 Dokumentasi Tingkat 1

Dokumen tingkat 1 merupakan dokumen dengan hirarki tertinggi dalam struktur dokumentasi SMKI. Dokumen ini bersifat strategis yang memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan sistem (*development*), penerapan (*implementation*) dan peningkatan (*improvement*) sistem manajemen keamanan informasi.

Dokumen Tingkat 1 paling tidak memiliki bagian yang terdiri dari:

- Kebijakan Keamanan Informasi
- Peran dan tanggung jawab organisasi keamanan informasi
- Klasifikasi informasi
- Kebijakan Pengamanan Akses Fisik dan Lojik
- Kebijakan Manajemen Risiko TIK
- Manajemen Kelangsungan Usaha (*Business Continuity Management*)
- Ketentuan Penggunaan Sumber Daya TIK

4.3 Dokumentasi Tingkat 2

Dokumen tingkat 2 ini umumnya meliputi prosedur dan panduan yang dikembangkan secara internal oleh instansi/lembaga penyelenggara pelayanan publik dan memuat cara menerapkan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan. Dokumen ini bersifat operasional.

Prosedur-prosedur dalam dokumen tingkat 2 meliputi antara lain:

- Prosedur pengendalian dokumen
- Prosedur pengendalian rekaman
- Prosedur audit internal SMKI
- Prosedur tindakan perbaikan dan pencegahan
- Prosedur penanganan informasi (penyimpanan, pelabelan, pengiriman/pertukaran, pemusnahan)

- Prosedur penanganan insiden/gangguan keamanan informasi
- Prosedur pemantauan penggunaan fasilitas teknologi informasi

4.4 Dokumentasi Tingkat 3

Dokumen tingkat 3 meliputi petunjuk teknis, instruksi kerja dan formulir yang digunakan untuk mendukung pelaksanaan prosedur tertentu sampai ke tingkatan teknis. Instruksi kerja tidak selalu diperlukan untuk setiap prosedur. Sepanjang prosedur sudah menguraikan langkah-langkah aktivitas yang jelas dan mudah dipahami penanggung jawab kegiatan, petunjuk teknis / instruksi kerja tidak diperlukan lagi.

Menurut Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik Kemenkominfo 2011, cakupan dokumentasi SMKI dapat dijelaskan pada tabel yang pada umumnya dibangun sebagai kelengkapan kerangka kerja keamanan informasi. Mengenai nama dokumen tidak harus sama dengan panduan yang ada, namun cakupan dokumen hendaknya memenuhi penjelasan dalam tabel 4.2,4.3 4.4, dan 4.5.

Tabel 4.1: Cakupan dokumen tingkat 1 (Prosedur)

No	Nama Dokumen	Cakupan Dokumen
1	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain: • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan kontrol • Struktur dan metodologi manajemen risiko • Organisasi dan tanggungjawab keamanan informasi
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggung jawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah
3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara intenal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.

Tabel 4.2: Cakupan dokumen tingkat 1 (Prosedur)

No	Nama Dokumen	Cakupan Dokumen
4	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain: • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan kontrol • Struktur dan metodologi manajemen risiko • Organisasi dan tanggungjawab keamanan informasi
5	Organisasi, peran dan tanggung-jawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggung jawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah
6	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara intenal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.

Tabel 4.3: Cakupan dokumen tingkat 1 (Prosedur)

No	Nama Dokumen	Cakupan Dokumen
7	Kebijakan Manajemen Risiko TIK	Berisi metodologi / ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.
8	Kerangka Kerja Manajemen Kelangsungan Usaha (*Business Continuity Management*)	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana/k darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.
9	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).

Tabel 4.4: Cakupan dokumen tingkat 2a (Kebijakan)

No	Nama Prosedur/Pedoman	Cakupan Dokumen
1	Pengendalian Dokumen	Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan dokumen jika tidak digunakan dan daftar serta pengendalian dokumen eksternal yang menjadi rujukan.
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi.
3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor.
4	Tindakan Perbaikan & Pencegahan	Berisi tatacara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TIK.
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/daya “rahasia” baik softcopy maupun hardcopy, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada instansi/lembaga.
6	Pengelolaan Removable Media&Disposal Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (tape/hard disk/flashdisk/CD) dan penghapusan informasi ataupun penghancuran media.

Tabel 4.5: Cakupan dokumen tingkat 2b (Kebijakan)

No	Nama Prosedur/Pedoman	Cakupan Dokumen
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Berisi proses pemantauan penggunaan CPU, storage, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil pemantauan.
8	User Access Management	Berisi proses dan tatacara pendaftaran, penghapusan dan peninjauan hak akses user, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, database, internet, email dan internet).
9	Teleworking	Pengendalian dan pengamanan penggunaan hak akses secara remote (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.
10	Pengendalian Instalasi Software& Hak Kekayaan Intelektual	Berisi daftar software standar yang diijinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan software yang tidak diizinkan.
11	Pengelolaan Perubahan (Change Management) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/basis data/versi dari aset TIK yang mengalami perubahan.
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan dan pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.

5

Audit Keamanan Informasi

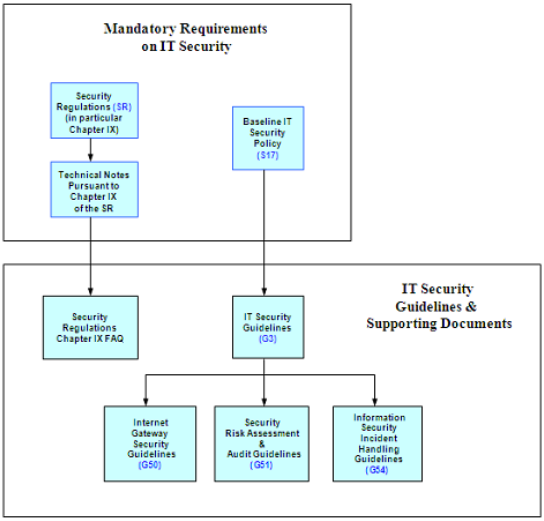
Untuk mempermudah pemahaman hubungan hubungan beberapa dokumen keamanan TI dalam pemerintahan, disajikan pada diagram Gambar 5.1 berikut ini (merujuk pada *Security Risk Assestment & Audit Guidelines, Pemerintah Hongkong*):

Audit keamanan adalah sutu proses atau kejadian yang memiliki basis pada kebijakan atau standar keamanan untuk menentukan semua keadaan dari perlindungan yang ada, dan untuk memverifikasi apakah perlindungan yang ada berjalan dengan baik. Target dari audit ini adalah untuk mencari tau apakah lingkungan yang ada sekarang telah aman dilindungi sesuai dengan kebijakkan keamanan yang ditetapkan.

Untuk menjaga independensi hasil audit, audit keamanan informasi harus dilaksanakan oleh pihak ketiga yang terpercaya dan independen.

5.1 Penilaian Resiko Keamanan

Melihat dari Gambar 2.1 Audit Keamanan dan Penilaian Resiko Keamanan (Security Risk Assessment) adalah sesuatu hal yang berbeda dari sisi terminologi asal dan fungsi dalam siklus manajemen keamanan informasi.



Gambar 5.1: Dokumen keamanan TI dalam pemerintahan

Penilaian resiko keamanan (PRK) adalah dilakukan pada permulaan tahapan yang dilakukan untuk mengindentifikasi apakah dibutuhkannya pengukuran keamanan dan kapan terjadi perubahan pada aset informasi atau lingkungannya. Sedangkan audit keamanan adalah proses pemeriksaan berulang (repetitif) untuk menjamin bahwa pengukuran keamanan diimplementasikan dengan baik dari waktu ke waktu. Maka itu, audit keamanan biasanya dilakukan lebih sering dibandingkan PRK.

5.2 Tujuan Audit Keamanan

Tujuan utama dari audit keamanan, diantaranya adalah:

- Memeriksa kesesuaian dari mulai kebijakkan, bakuan, pedoman, dan prosedur keamanan yang ada
- Mengidentifikasi kekurangan dan memeriksa efektifitas dari kebijakkan, bakuan, pedoman, dan prosedur keamanan yang ada
- Mengidentifikasi dan memahami kelemahan (vulnerability) yang ada

- Mengkaji kendala keamanan yang ada terhadap permasalahan operasional, administrasi, dan manajerial, dan memastikan kesesuaian dengan bakuan keamanan minimum
- Memberikan rekomendasi dan aksi perbaikan/koreksi untuk peningkatan

Dalam melaksanan audit perlu memperhatikan hal berikut ini, yaitu:

- Saat dan frekuensi audit
- Perangkat audit
- Langkah-langkah audit.

5.3 Saat dan Kekerapan Audit

Audit keamanan harus dilakukan secara periodik untuk memastikan kesesuaian atau kepatuhan pada kebijakkan, bakuan, pedoman, dan prosedur dan untuk menentukan suatu kendali minimum yang diperlukan untuk mengurangi resiko pada level yang dapat diterima. Sebagai catatan, audit keamanan hanya memberikan snapshot dari kelemahan yang diungkapkan pada titik waktu tertentu.

Audit keamanan adalah aktivitas yang terus berjalan, yang kontinu. Secara umum, audit keamanan dilaksanakan dalam dua putaran. Yang keduanya berlaku pada pola tertentu, namun putaran kedua merupakan proses verifikasi untuk memastikan ditemukannya semua kelemahan pada putaran pertama yang mana telah diperbaiki dan diatasi sebagai rekomendasi hasil laporan putaran pertama.

Terdapat situasi yang berbeda ketika harus melakukan audit keamanan. Waktu yang pasti tergantung kebutuhan dan sumber daya sistem yang dimiliki.

- **Instalasi Baru**. Audit yang dilakukan pertama kali setelah implementasi, dalamrangka memastikan konformasi pada kebijakkan dan petunjuk yang ada serta memenuhi bakuan konfigurasi
- **Audit Regular**. Audit ini adalah audit yang dilakukan secara periodik baik manual maupun otomatis dengan menggunakan perangkat dalam rangka mendeteksi lubang (*loopholes*) atau kelemahan, yang paling tidak dilakukan sekali dalam setahun

- **Audit Acak**: Audit ini dilakukan dengan melakukan pemeriksaan acak dalam rangka merefleksikan dengan praktik sesungguhnya
- **Audit di Luar Jam Kerja**: Audit ini dilakukan untuk mereduksi resiko pengauditan dengan melakukannya di luar jam kerja, biasanya pada malam hari.

Ada banyak perangkat audit yang dapat digunakan untuk mencari kelemahan. Pemilihan perangkat audit bergantung pada kebutuhan keamanan dan dampak beban kerja dari pengawasan. Sebagai contoh, perangkat pemindai keamanan dapat memeriksa untuk setiap kelemahan pada jaringan dengan melakukan pindaian dan simulasi serangan.

5.4 Tahapan Audit.

Secara umum, tahapan audit dibagi menjadi bagian berikut ini:

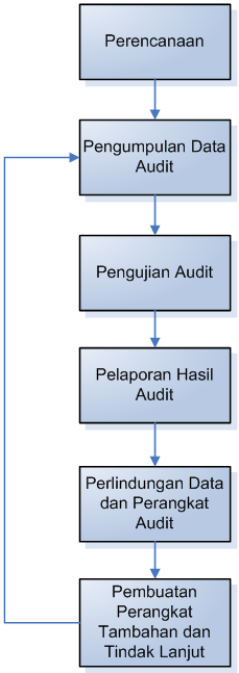
1. Perencanaan
2. Pengumpulan data audit
3. Pengujian audit
4. Pelaporan hasil audit
5. Perlindungan atas data dan perangkat audit
6. Penambahan dan tindak lanjut

5.4.1 Perencanaan

Tahapan perencanaan dapat membantu dalam menentukan dan memilih metode yang efisien dan efektif untuk melakukan audit dan mendapatkan semua informasi penting yangdibutuhkan. Waktu yang dibutuhkan dalam tahapan ini disesuaikan dengan lingkungan/keadaan, tingkat perluasan, dan kerumitan dari audit tersebut.

Dalam tahapan ini akan dirincikan sub tahapan, diantaranya:

1. Ruang lingkup dan tujuan
2. Kendala
3. Peran dan tanggung jawab



Gambar 5.2: Diagram Tahapan Umum Audit

Ruang Lingkup dan Tujuan

Ruang lingkup dan tujuan audit harus didefinisikan dan ditetapkan dengan jelas. Kebutuhan pengguna harus diidentifikasi dan disetujui dengan auditor keamanan sebelum melanjutkan kerjanya. Berikut adalah contoh cakupan audit keamanan:

- Keamanan internet
- Keamanan umum dari jaringan internal
- Sistem tugas kritis
- Keamanan host
- Keamanan server jaringan seperti web server, email server, dan lain lain
- Komponen dan devais jaringan seperti firewall, router, dan lain lain
- Keamanan umum dari ruang komputer

Adapun tujuan dari audit keamanan diantaranya adalah:

- Memberikan kesesuaian /kepatuhan dengan kebijakkan keamanan sistem
- Memeriksa dan menganalisa pengamanan sistem dan lingkungan operasional kerja
- Menilai implementasi teknis dan non teknis dari rancangan keamanan
- Memvalidasi wajar atau tidaknya integrasi dan operasi dari semua fitur keamanan.

Kendala

Waktu yang diperbolehkan untuk audit haruslah cukup untuk menyelesaikan semua pengujian. Kadang kala pada saat proses audit, sistem atau jaringan harus pada keadaan off-line. Dan interupsi layanan dapat saja dilakukan. Yang perlu diperhatikan adalah, adanya backup dan pemulihan konfigurasi dan informasi yang ada perlu dilakukan sebelum proses aduit berjalan.

Peran dan Tanggung jawab

Peran dan tanggung jawab semua pihak yang terlibat dalam audit haruslah didefinisikan dengan jelas sebelumnya. Adapun khusus bagi para auditor, haruslah melakukan tahapan pra-audit seperti:

- Mengidentifikasi dan verifikasi lingkungan yang ada dan sedang berjalan melalui dokumentasi, wawancara, pertemuan/rapat, dana telaah manual
- Mengidentifikasi area atau operasi yang signifikan/berarti yang terkait dengan proses audit
- Mengidentifikasi kendali umum yang mungkin berdampak pada audit
- Memperkirakan dan mengidentifikasi sumber daya yang diperlukan seperti perangkat audit dan tenaga kerja
- Mengidentifikasi proses khusus atau proses tambahan untuk audit.

Dalam proses audit, perlu adanya kendali dan otorisasi sebelum dimulai dan perlu dibangunnya jalur komunikasi antara klien dengan auditor.

5.4.2 Pengumpulan Data Audit

Jumlah data yang dikumpulkan tergantung pada cakupan dan tujuan audit, ketersediaan data dan ketersediaan penyimpanan media. Dan merupakan yang tidak bisa dilewatkan yaitu menentukan seberapa banyak dan jenis apa dari data yang akan diambil dan bagaimana untuk memfilter, menyimpan, mengakses dan menelaah data dan log audit.

Perencanaan yang teliti diperlukan dalam pengumpulan data. Pengumpulan data yang dilakukan harus sejalan dengan peraturan dan regulasi pemerintah dan tidak menyebabkan/menimbulkan ancaman dan keamanan bagi sistem. Pengumpulan data harus memenuhi kriteria, antara lain sebagai berikut:

- Harus memadai untuk investigasi di masa depan atas insiden keamanan

- Harus baik dalam penyimpanan dan perlindungan data dari akses yang ilegal/tidak terotorisasi
- Harus dengan baik diproses dengan perencanaan penanganan data.

Data audit dapat simpan dalam banyak cara, diantaranya yaitu:

- *Files logging*: menyimpan data audit dalama file read/write, sebagai contoh: informasi sistem start up dan shutdown; percobaan logon dan logout, eksekusi command (perintah), dan lain lain
- Laporan: mencetak data audit dalam bentuk laporan, sebagai contoh: jurnal, summaries, laporan lengkap, laporan statistik.
- *Write-once storage*: data disimpan pada media sekali cetak seperti: CD-ROM/DVD-ROM.

5.4.3 Pengujian Audit

Setelah melakukan dua tahap sebelumnya, auditor keamanan dapat melakukan kegiatan berikut:

- Telaah umum atas kebijakkan atau bakuan keamanan yang ada menurut pada cakupan audit yang ditentukan
- Telaah umum atas konfigurasi keamanan
- Penyelidikan teknis dengan menggunakan perangkat otomasi berbeda untuk mendiagnosa telaah atau pengujian penetrasi.

5.4.4 Pelaporan Hasil Audit

Pelaporan audit keamanan dibutuhkan untuk penyelesaian akhir dari pekerjaan audit. Auditor keamanan harus menganalisa hasil pengauditan dan menyediakan laporan besertanya yang menjelaskan lingkungan keamanan yang berlaku.

Laporan audit yang ada harus dapat dibaca pihak yang berkepentingan, diantaranya oleh:

- Manajemen TI,
- Manajemen eksekutif,

- Administrator sistem
- Pemilik sistem.

5.4.5 Perlindungan Data dan Perangkat Audit

Setelah pelaksanaan audit, penting untuk melakukan perlindungan data dan perangkat audit untuk audit selanjutnya atau dikemudian hari. Data audit tidak diperkenankan disimpan online. Jika memungkinkan, sebaiknya data audit dienkrispi terlebih dahulu sebelum disimpan dalam media pemyimpanan sekunder. Semua dokumen fisik terkait dengan audit seharusnya aman juga secara fisik dari pihak atau pengguna yang tidak berkepentingan.

Perangkat audit harus dirawat, dijaga dan diawasi dengan baik untuk mencegah penyalahgunaan. Perangkat tersebut harus dipisahkan dari sistem pengembangan maupun sistem pengoperasian. Cara lainnya yaitu, dengan menghilangkan/menyingkirkan perangkat audit secepatnya setelah penggunaan selesai, kecuali dilindungi dari akses yang tidak diinginkan.

Auditor keamanan harus segera mengembalikan semua informasi audit ke setiap departemen setelah penyelesaian proses audit.

5.4.6 Penambahan dan Tindak Lanjut

Jika langkah pembetulan dibutuhkan, harus melakukan alokasi sumber daya untuk menjamin bahwa penambahan/peningkatan dapat dilakukan pada kesempatan paling awal.

6

Pelaksanaan Audit IS

Suatu organisasi harus menilai keamanan sistem informasi secara reguler. Hal tesebut dilakukan dengan melalukan prosedur audit IS berdasarkan konsep keamanan informasi yang diadopsi organisasi.

6.1 Persetujuan Pimpinan dan Penetapan Organisasi

Setiap proyek memerlukan investasi baik untuk penyediaan sumber daya maupun untuk pelatihan yang diperlukan. Pimpinan harus memberikan persetujuannya terhadap rencana investasi tersebut. Sebelum rencana penerapan audit SMKI, pimpinan harus mendapatkan penjelasan yang memadai tentang seluk beluk, nilai penting dan untung rugi menerapkan audit SMKI serta konsekuensi ataupun komitmen yang dibutuhkan dari pimpinan sebagai tindak lanjut persetujuan terhadap proyek audit SMKI.

Persetujuan pimpinan harus diikuti dengan arahan dan dukungan selama berlangsungnya proyek tersebut. Oleh karena itu, perkembangan proyek audit SMKI harus dikomunikasikan secara berkala kepada pimpinan pasca persetujuannya agar setiap masalah yang memerlukan pengambilan keputusan pimpinan dapat diselesaikan secara cepat dan tepat.

Salah satu bentuk komitmen pimpinan pasca persetujuan terhadap rencana penerapan audit SMKI adalah dengan menetapkan organ-

isasi atau tim penanggung-jawab keamanan informasi. Organisasi atau tim ini harus ditetapkan secara formal dan diketuai oleh koordinator atau ketua tim. Jumlah anggota tim disesuaikan dengan ruang lingkup organisasinya. Tugas utama tim ini adalah menyiapkan, menjamin dan/atau melakukan seluruh kegiatan dalam tahapan penerapan audit SMKI (yang diuraikan dalam Bab ini) agar dapat terlaksana dengan baik sesuai rencana.

Organisasi penanggung-jawab keamanan informasi ini dapat ditetapkan sebagai struktur organisasi yang bersifat permanen atau sebagai "*tim adhoc*" (tim proyek) sesuai kebutuhan. Tanggung-jawab ketua dan anggota tim serta unit kerja terkait dalam hal keamanan informasi harus diuraikan secara jelas. Ketua tim hendaknya ditetapkan/dipilih dari pejabat tertinggi sesuai ruang lingkup penerapan audit SMKI atau yang pejabat/petugas/perwakilan yang didelegasikan.

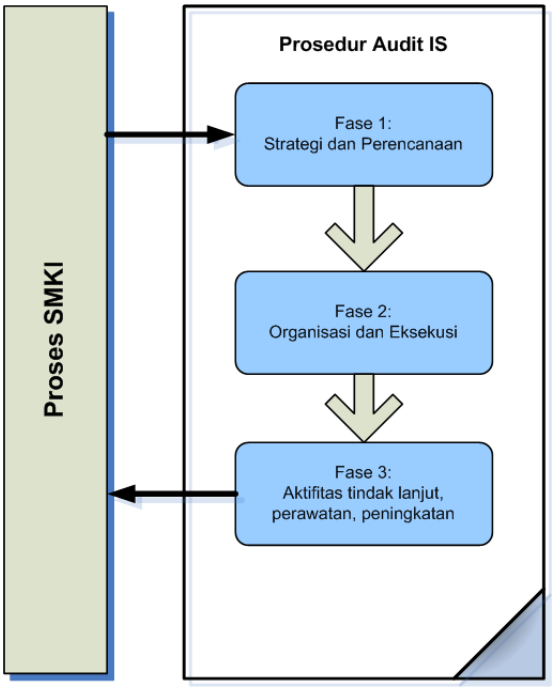
6.2 Pembagian Tanggung Jawab

Level manajemen menanggung semua tanggung jawab audit IS. Pihak manajemen harus diinformasikan secara reguler tentang semua masalah dan hasilnya serta aktifitas dari Audit IS. Manajemen juga harus mengetahui/diberitahu mengenai pengembangan baru, kondisi umum perubahan atau hal yang baru, atau kemungkinan untuk peningkatan dalam rangka memenuhi fungsi dan kendalinya atas sistem.

Satu orang dalam organisasi (sebagai contoh, petugas keamanan TI) harus bertanggung jawab dalam audit IS. Petugas tersebut yang kemudian mengawasi atau mensupervisi keseluruhan proses dan eksekusi aktual dari audit IS. Petugas tersebut harus memiliki hal-hal sebagai berikut:

- posisi independen dalam struktur organisasi (untuk mencegah konflik kepentingan)
- hak untuk berbicara langsung kepada pihak manajamen, dan
- memilki kemampuan yang cukup dan memenuhi dalam bidang keamanan informasi.

Tugas dari seseorang yang bertanggung jawab dalam audit IS suatu organisasi, yaitu: menyusun rencana kasar untuk projek audit IS sebagai dasar dalam audit IS. Orang tersebut akan berperan sebagai kontak person utama dalam tim audit IS selama audit berlangsung



Gambar 6.1: Fase prosedur audit IS dari sudut pandang organisasi

dan bertanggung jawab khususnya dalam menyediakan dokumen referensi dan mengkordinasikan jadwal serta sumber daya materi atau personil lainnya pada saat pemeriksaan langsung.

Setiap spesifikasi terkait dengan prosedur audit IS dan penugasan harus didokumentasikan secara individual dalam manual audit IS. Manual tersebut harus mengandung aspek-aspek berikut ini:

- Tujuan strategis yang dicapai dari audit IS
- Ordinansi dan regulasi legal yang mungkin
- Pengorganisasi audit IS dalam suatu organisasi
- Sumber daya (baik waktu, keuangan, dan manusia/personil)
- Pengarsipan dokumentasi

Manual audit IS merupakan dasar dan instruksi manual dari audit IS. Manual ini mengatur satu sama lainnya mengenai hak dan tugas individu yang terlibat dalam audit IS. Perwakilan personil harus dicantumkan dalam proses sebelum diadopsi oleh pihak manajemen.

6.2.1 Siklus Audit IS

Pada dasarnya suatu audit Information Security (IS) dilakukan dengan siklus berikut ini:

- Audit parsial IS untuk proses bisnis yang kritis harus direncanakan. Proses bisnis yang kritis, khususnya yang memerlukan ketersediaan tinggi (*High Availability*) harus lebih sering dilakukan. Interval audit harus dengan benar dilakukan untuk hal kritis yang khusus.
- Audit parsial IS tambahan dapat dilakukan, misalnya pada saat hal berikut: pemeriksaan mendalam setelah terjadinya kecelakaan keamanan, setelah penerapan prosedur baru, atau pada saat perencanaan restrukturisasi.

6.2.2 Pengawasan Audit IS

Orang yang bertanggung jawab dalam audit IS juga merupakan orang yang dapat dihubungi pada saat audit IS. Orang tersebut membantu tim audit IS dalam menjawab pertanyaan teknis dan organisasional (sebagai contoh pada saat rapat organisasi, pada saat mengumpulkan dokumen, dan pada saat pemeriksaan langsung (*on-site*)).

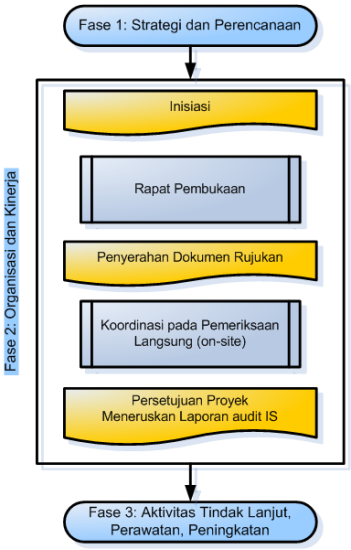
Tugas organisasional orang yang bertanggung jawab dalam audit IS suatu organisasi ditunjukkan dalam Gambar 6.2.

6.2.3 Tim Audit IS

Untuk setiap audit dilakukan, perlu dibangunnya tim audit yang sesuai. Anggota dari tim audit ini harus memiliki kualifikasi teknis yang sesuai baik secara tim maupun kualifikasi individu.

Berikut ini adalah tim-tim audit yang ada dalam organisasi:

- **Tim Audit IS Internal**. Perlu dibentuknya tim audit IS internal yang tergantung pada tipe dan ukuran suatu organisasi. Dengan menugaskan beberapa orang untuk melakukan audit



Gambar 6.2: Kinerja audit IS dari sudut pandang organisasi

IS akan memberikan keuntungan tersedianya pengetahuan dari kompleksitas struktur dan prosedur organisasi.

- **Kerjasama antara Tim Audit IS**. Karena tidak semua organisasi dapat membentuk tim audit internal yang lengkap, perlu dilakukannya kerjasama dengan tim audit dari organisasi lainnya, seperti penukaran pakar keamanan.
- **Departemen/Divisi Tim Audit IS**. Dengan membentuknya departemen/divisi khusu yang melakukan audit IS.
- **Penyedia layanan audit IS eksternal**. Pihak eksternal yang menyediakan layanan audit.

Berikut ini adalah nilai dari sumber daya personil dari tim audit IS, yang didapatkan berdasarkan pengalaman yang dapat digunakan sebagai dasar untuk memperkirakan total waktu dan pengeluaran dari audit IS berdasarkan tingkat kompleksitasnya:

Waktu yang digunakan adalah perkiraan waktu kotor.

Kompleksitas	**Ukuran Organisasi: Kecil (<101 karyawan)**	**Ukuran Organisasi: Medium (<501 karyawan)**	**Ukuran Organisasi: Besar (>501 karyawan)**
Normal	30 hari personil	50 hari personil	60 hari personil
Tinggi	50 hari personil	65 hari personil	80 hari personil
Sangat Tinggi	60 hari personil	80 hari personil	100 hari personil

Tabel 6.1: Nilai standar untuk pengeluaran personil suatu audit IS

6.2.4 Struktur Keamanan Informasi suatu Organisasi

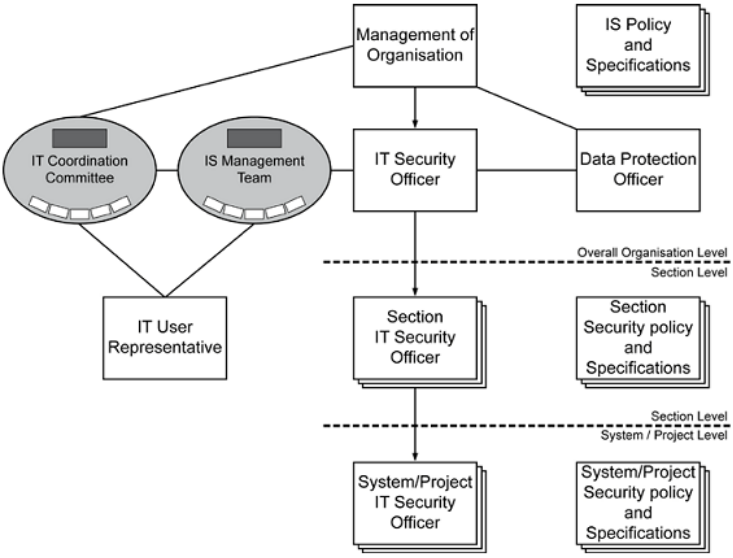
Struktur organisasi keamanan informasi, bergantung pada ukuran organisasi itu sendiri. dapat berukuran kecil, sedang atau besar. Gambar berikut menunjukkan tiga kemungkinan. Gambar 6.3 menunjukkan struktur organisasi IS dalam organisasi besar. Gambar 6.4 kedua menunjukkan organisasi ukuran sedang, dimana adanya kombinasi peran petugas TI dan Manajemen IS. Gambar 6.5 menunjukkan struktur organisasi IS berukuran kecil, dimana petugas TI melakukan semua tugasnya.

6.2.5 Evaluasi Audit IS

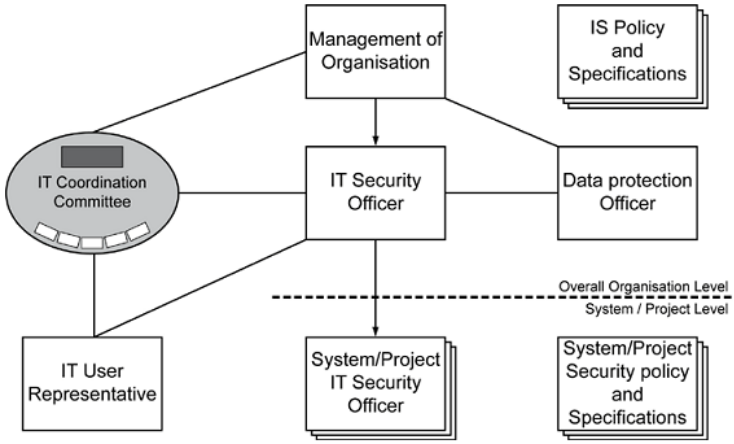
Ada empat prinsip dasar dalam evaluasi:

- Objectiviy
- Impartiality
- Reproducibility
- Repeatability

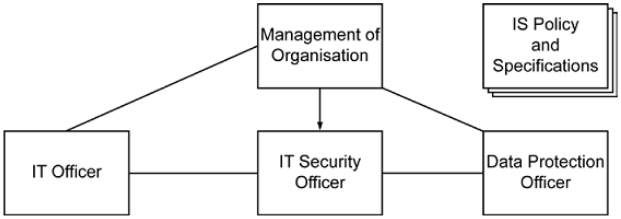
Yang semuanya memiliki hubungan satu sama lainnya, seperti dilustrasikan pada Gambar 6.6.



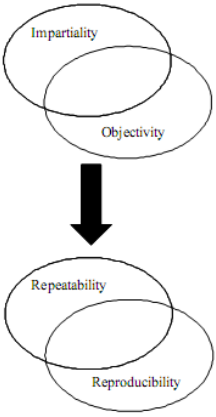
Gambar 6.3: Struktur Keamanan Informasi: Organisasi Besar



Gambar 6.4: Struktur Keamanan Informasi: Organisasi Sedang



Gambar 6.5: Struktur Keamanan Informasi: Organisasi Kecil



Gambar 6.6: Empat prinsip dasar dalam evaluasi

Implementasi seluruh kebijakan, prosedur atau standar yang ditetapkan kemudian dievaluasi efektivitasnya. Periksalah kebijakan dan prosedur mana yang telah dapat diterapkan dengan tepat dan mana yang belum. Jika prosedur belum diterapkan dengan tepat, maka dilakukanlah analisis mengapa hal itu terjadi. Apakah karena sosialiasi yang terlalu singkat atau prosedurnya yang terlalu rumit atau kurang praktis.

Hasil pengukuran efektivitas kontrol dan laporan audit internal juga dievaluasi untuk diperiksa mana kontrol yang belum mencapai sasaran, masih lemah (belum efektif) atau yang masih menjadi temuan dalam audit internal. Seluruh kelemahan kontrol harus segera diperbaiki ataupun disempurnakan sehingga tidak menimbulkan kelemahan/kesalahan yang sama di kemudian hari.

Hasil dari audit IS dilaporkan kepada manajemen organisasi, orang yang bertanggung jawab untuk audit IS, dan petugas keamanan TI serta diintegrasikan ke dalam proses SMKI. Prosedur yang didefinisikan dengan jelas harus tersedia dan dinyatakan dalam petunjuk pemeriksaan dan peningkatan proses keamanan informasi.

Kebutuhan dalam menghilangkan ketidak efisienan dan peningkatan kualitas merupakan hasil evaluasi dari laporan audit IS. Petugas keamanan TI kemudian akan mengarahkan tindak lanjut dari kebutuhan tersebut. Akitifitas tindak lanjut tersebut termasuk di dalamnya: pemutakhiran/update dokumen keamanan, sebagai contoh, pemeriksaan keamanan dasar dan konsep keamanan.

6.3 Mendefinisikan Cakupan (Ruang Lingkup)

Dalam pelaksanaan audit keamanan informasi, perlu ditentukan ruang lingkup dari pekerjaan audit tesrebut. Ruang lingkup ini meliputi:

- **Proses dan/atau Kegiatan**. Misalnya: Penyediaan layanan publik, Pengamanan Pusat Data, pengembangan aplikasi, penggunaan jaringan dan fasilitas email, dan sebagainya.
- **Satuan Kerja**. Misalnya: Direktorat, Departemen atau Bidang.
- **Lokasi kerja**. Misalnya: Tingkat Pusat, daerah atau keduanya. Mana saja lokasi yang dipilih untuk menerapkan audit SMKI? Apakah audit SMKI akan langsung diterapkan ke seluruh lokasi

kerja? Atau apakah diterapkan secara bertahap dengan memprioritaskan pada lokasi tertentu terlebih dahulu?

Penetapan ruang lingkup ini harus didiskusikan dengan Satuan Kerja terkait dengan memperhatikan tingkat kesiapan masing-masing termasuk ketersediaan sumber daya yang diperlukan untuk membangun dan menerapkan audit SMKI.

6.4 Teknik Audit IS

Teknik audit dipahami sebagai metode yang digunakan untuk menentukan fakta dari permasalahan. Berikut adalah beberapa teknik audit yang dapat digunakan selama audit IS:

- Wawancara (pertanyaan verbal)
- Inspeksi visual suatu sistem, lokasi, ruang, kamar, dan objek
- Observasi
- Analisis file/berkas (termasuk data elektronik)
- Pemeriksaan teknis (misal menguji sistem alarm, sistem kontrol akses, aplikasi)
- Analisis Data (misal log files, evaluasi database, dll)
- Pertanyaan tertulis (misal, kuesioner).

Teknik audit sebenarnya digunakan tergantung pada kasus spesifik dan akan dispesifikasikan oleh tim audit IS. Tim audit IS harus memastikan bahwa hasil yang didapat selama semua pemeriksaan disesuaikan dengan jumlah data dan usaha yang dikeluarkan.

Jika tim audit IS menemukan adanya deviasi atau penyimpangan dari status dokumen selama pemeriksaan dari sampel yang dipilih, maka jumlah sampel perlu ditambahkan guna mendapatkan penjelasan yang lebih baik. Pemeriksaan dapat dihentikan apabila masalah deviasi atau penyimpangan dapat dicari alasan dan dijelaskan. Beberapa teknik audit dapat dikombinasikan untuk menentukan suatu deviasi.

6.5 Melakukan Analisis Kesenjangan (*Gap Analysis*)

Kegiatan ini dilakukan dengan tujuan utamanya untuk membandingkan seberapa jauh persyaratan klausul-klausul ISO 27001 telah dipenuhi, baik pada aspek kerangka kerja (kebijakan dan prosedur) maupun aspek penerapannya. Untuk aspek kerangka kerja, identifikasilah apakah kebijakan dan prosedur sebagaimana dicantumkan telah dipenuhi.

Sedang untuk aspek penerapan, ketersediaan rekaman perlu diperiksa sebagai bukti-bukti penerapan. Gap Analysis umumnya dilakukan dengan bantuan checklist pemeriksaan. Selain Checklist Indeks KAMI, checklist lain untuk kegiatan gap analysis ISO 27001 dapat diunduh dari berbagai situs tentang keamanan informasi.

6.6 Penilaian Resiko dan Rencana Penilaian Resiko

Sebelum melakukan risk assessment (pengkajian risiko), metodologi *risk assessment* harus ditetapkan terlebih dahulu. Periksalah apakah instansi anda telah memiliki atau menetapkan kebijakan/metodologi risk assessment. Metodologi *risk assessment* TIK harus merujuk pada metodologi risk assessment yang ditetapkan di tingkat pusat, jika sudah ada. Jika belum ada metodologi risk assessment, lakukan penyusunan metodologinya dengan merujuk pada standar-standar yang ada, baik standar nasional ataupun internasional. Khusus untuk risk assessment TIK beberapa dokumen standar di bawah ini dapat dijadikan rujukan, antara lain:

1. Pedoman Standar Penerapan Manajemen Risiko bagi Bank Umum (Lampiran Surat Edaran No.5/21/DPNP tanggal 29 September 2003)

2. ISO/IEC27005 - Information Security Risk Management yang telah diadopsi menjadi SNI

3. Handbook of Risk Management Guidelines Companionto AS/NZ 4360:2004 d. NIST Special Publication 800-30:Risk Management Guide for Information Technology Systems.

Dalam metodologi risk assessment juga terdapat kriteria penerimaan risiko, dimana risiko yang berada pada tingkat tertentu (umumnya tingkat "RENDAH") akan diterima tanpa perlu melakukan rencana penanggulangan (Risk Treatment Plan). Risk Assessment dilakukan dengan merujuk pada metodologi yang telah ditetapkan tersebut.

6.7 Menetapkan Kontrol dan Sasaran Kontrol

Dari hasil identifikasi risiko kemudian dipilih kontrol dan sasaran kontrol ISO 27001 yang dapat diterapkan sesuai dengan ruang lingkup yang ditetapkan. Sasaran kontrol dapat ditetapkan sebagaisasaran keamanan informasi tahunan yang digunakan sebagai patokan untuk mengukur efektivitas penerapan SMKI pada periode yang ditetapkan. Sasaran keamanan informasi tahunan dapat ditetapkan sesuai hasil kajian risiko dan prioritas pembenahan dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.

Contoh sasaran keamanan informasi tahunan, misal tahun 2011, diberikan pada Tabel 6.2 dalam berikut.

Catatan: Sasaran keamanan ini belum lengkap. Masing-masing instansi/lembaga dapat menambahkan sasarannya sesuai dengan hasil kajian risiko dan skala prioritas yang ditetapkan.

6.8 Menetapkan Kebijakan dan Prosedur Audit SMKI

Kebijakan dan prosedur disusun dengan memperhatikan kontrol yang memang berlaku dan diterapkan dalam penyelenggaraan pelayanan publik.

6.9 Sosialisasi dan Pelatihan

Seluruh kebijakan dan prosedur yang telah disetujui oleh pimpinan kemudian disosialisasikan kepada seluruh personel/karyawan yang

Tabel 6.2: Contoh Sasaran Keamanan Informasi

No	Kontrol ISO 27001	Sasaran
1	A.13.1 Pengelolaan insiden	Menurunkan jumlah insiden karena virus 10% dibanding tahun sebelumnya
2	A.8.3.3 Penutupan hak akses	Hak akses user yang menjalani mutasi/berhenti bekerja harus ditutup maksimum 2 hari setelah statusnya dilaporkan secara resmi
3	A.9.1.2 Akses data center (ruang server)	Seluruh pihak ketiga (vendor, konsultan) yang memasuki Pusat Data harus didampingi karyawan
4	A.11.2 Manajemen password	80% perangkat komputer yang sensifit sudah menerapkan *strong password*
5	A.8.2.2 Kepedulian, pendidikan dan pelatihan keamanan informasi	Seluruh karyawan dalam satuan kerja yang dimasukkan dalam ruang lingkup harus telah mengikuti sosialisasi/pelatihan keamanan informasi
6	A.10.1.2 Pengelolaan perubahan (*change management*)	Versi aplikasi yang operasional harus sama dengan versi source code terakhir
7	A.10.1.3 Pemisahan tugas	Setiap instalasi aplikasi dilakukan oleh penanggung-jawab operasional TI (bukan oleh programmer)

terkait sesuai dengan ruang lingkup yang ditetapkan di atas. Kegiatan ini untuk menjamin bahwa kebijakan dan prosedur SMKI telah dipahami sehingga penerapannya dilakukan secara tepat. Sosialisasi dapat dilakukan dengan berbagai cara, seperti:

- Tatap muka di dalam kelas
- Simulasi langsung di lokasi kerja
- Penyampaian brosur, leaflet, spanduk untuk meningkatkan kepedulian karyawan
- Penggunaan email, nota dinas, portal atau majalah internal
- Media komunikasi lainnya

Untuk meningkatkan kompetensi personel, perlu dilakukan pelatihan yang lebih mendalam baik pada aspek teknis maupun tata kelola TIK. Berbagai jenis pelatihan menyangkut pengamanan informasi yang dapat diprogramkan, misalnya: pengenalan ISO 27001, audit internal, pelatihan lead auditor, risk management, pelatihan untuk administrator ataupun jenis-jenis pelatihan untuk programmer.

Bukti sosialisasi dan pelatihan baik berupa:

- materi,
- daftar hadir,
- hasil pre/post test,
- laporan evaluasi pelatihan ataupun
- sertifikat

Yang kesemua bukti harus disimpan dan terpelihara dengan baik.

6.10 Menerapkan Kebijakan dan Prosedur

Strategi penerapan/implementasi audit SMKIsebaiknya dilakukan dengan menyelaraskan kegiatan yang sedang berlangsung di instansi/lembaga. Jika instansi/lembaga sedang melakukan proyek pengembangan aplikasi, arahkan dan dampingi agar setiap tahapan pengembangan aplikasi dapat mematuhi kebijakan dan prosedur yang telah ditetapkan yang antara lain mencakup:

- Persetujuan investasi proyek (untuk proyek outsource atau kegiatan yang memerlukan anggaran)
- Persyaratan keamanan aplikasi (syarat password minimum, session time-out, otentikasi, dan sebagainya)
- Non Disclosure Agreement (perjanjian menjaga kerahasiaan) untuk pihak ketiga
- Manajemen Perubahan (*Change Management*)
- Lisensi dan standar software yang digunakan.

Hasil penerapan SMKI harus dicatat dalam bentuk laporan, log, rekaman atau isian formulir yang relevan yang mendukung kebijakan atau prosedur yang ditetapkan seperti laporan pencatatan insiden dan penyelesaiannya, daftar pengguna aplikasi, log aktivitas user, laporan pelatihan/sosialisasi, permintaan perubahan dan realisasinya, hasil pengujian aplikasi, laporan perawatan komputer, dan sebagainya.

6.11 Mengukur Efektivitas Kendali

Kontrol yang telah ditetapkan baik berupa kebijakan, prosedur atau standar yang telah ditetapkan diukur efektivitasnya dengan mempelajari hasil-hasil penerapan yang dicatat atau dituliskan dalam laporan atau formulir-formulir yang relevan. Metode pengukuran kontrol harus ditetapkan terlebih dahulu, baru kemudian diukur efektivitas kontrolnya secara periodik sesuai kebutuhan dan karakteristik kegiatan. Pengukuran ketercapaian sasaran keamanan informasi dapat menjadi salah satu alat untuk mengukur efektivitas kontrol seperti pada Tabel 6.3 berikut ini.

Tabel 6.3: Pengukuran Ketercapaian Keamanan Informasi

No	Kontrol ISO 27001	Sasaran	Metoda Pengukuran	Frekuensi Pengukuran	Hasil Pengukuran
1	A.13.1 Pengelolaan insiden	Menurunkan jumlah insiden karena virus sebanyak 10% dibanding tahun sebelumnya	Prosentase jumlah insiden tahun lalu dikurangi prosentase insiden sekarang	Per 3 bulan	
2	A.8.3.3 Penutupan hak akses	Hak akses user yang menjalani mutasi/berhenti bekerja harus ditutup maksimum 2 hari setelah statusnya dilaporkan secara resmi	Prosentase jumlah user yang telah ditutup haknya dibagi jumlah user yang mutasi/keluar	Per 6 bulan	
3	A.9.1.2 Akses data center (ruang server)	Seluruh (100%) pihak ketiga (vendor, konsultan) yang memasuki Pusat Data harus didampingi karyawan	Prosentase pihak ketiga yang memasuki Pusat Data yang didampingi karyawan	Per 6 bulan	
4	A.11.2 Manajemen password	80% perangkat komputer yang sensifit sudah menerapkan *strong password*	Jumlah PC dengan *strong password* dibanding jumlah PC yang ada	Per 6 bulan	
5	A.8.2.2 Kepedulian, pendidikan dan pelatihan keamanan informasi	Seluruh karyawan dalam satuan kerja yang dimasukkan dalam ruang lingkup harus telah mengikuti sosialisasi/pelatihan keamanan informasi	Jumlah karyawan yang mengikuti pelatihan dibanding jumlah total karyawan	Per tahun	
6	A.10.1.2 Pengelolaan perubahan (*change management*)	Versi aplikasi yang operasional harus sama dengan versi source code terakhir	Bandingkan versi operasional dengan versi terakhir		
7	A.10.3.2 Penerimaan sistem	Setiap aplikasi yang operasional harus menjalani UAT yang disetujui pengguna	Periksa UAT untuk setiap aplikasi yang operasional		

7

Level Keamanan Informasi

Kriteria level/tingkat keamanan informasi (normal, tinggi, atau sangat tinggi) ditentukan menurut keadaan yang sangat berkaitan dengan situasi yang terjadi. Adapun level keamanan informasi:

Sangat Tinggi

- Perlindungan informasi rahasia harus dijamin dan mematuhi kebutuhan kerahasiaan dalam area kritis keamanan
- Sangat penting akan informasi yang benar
- Tugas utama tidak dapat dilakukan tanpa TI. Waktu reaksi yang tanggap untuk keputusan kritis mensyaratkan kehadiran/kemunculan yang konstan dari informasi up-date; downtime merupakan suatu keadaan yang tidak dapat diterima
- Perlindungan atas data personal mutlak harus dijamin. Karena dikhawatirkan resiko kecelakaan atau kematian dapat terjadi pada pihak yang terlibat, atau dapat membahayakan kebebasan personil pihak yang terlibat.

Tinggi

- Perlindungan atas informasi rahasia harus memenuhi persyaratan tinggi, dan bahkan lebih kuat untuk area kritis keamanan

- Informasi yang diproses harus benar; error/kesalahan harus terdeteksi dan dapat dihindari
- Ada prosedur waktu kritis atau multitude dari tugas yang dilakukan dalam area pusat suatu organisasi yang tidak dapat dilaksanakan tanpa penggunaan TI. Hanya downtime singkat yang dapat ditoleransi.
- Perlindungan atas data personal harus memenuhi persyaratan tinggi. Jika tidak, akan ada resiko sosial maupun keuangan bagi pihak yang terlibat atau terkena dampak.

Normal

- Perlindungan informasi hanya dimaksudkan untuk penggunaan internal juga harus dijamin
- Error/kesalahan kecil dapat ditoleransi. Error signifikan yang mempengaruhi kemampuan untuk melakukan tugas harus terdeteksi dan dapat dihindari.
- Downtime tambahan yang mengarah pada lewatnya tenggat waktu, tidak dapat ditoleransi
- Harus adanya penjaminan data personil. Jika tidak, maka akan ada resiko sosial atau keuangan yang terjadi.

Perlu dicatat, bahwa setelah menentukan level keamanan yang diinginkan, beberapa pertanyaan masih perlu dijawab oleh pengelola sistem:

- Informasi apa yang kritis bagi organisasi yang terkait kerahasiaan, integritas, dan ketersediaan?
- Tugas kritis apa dalam organisasi yang tidak semuanya dapat dilakukan, hanya dilakukan secukupnya, atau hanya dapat dianggap sebagai usaha tambahan tanpa dukungan TI?
- Keputusan esensial apa yang diambil dalam organisasi yang bergantung pada kerahasiaan, integritas, dan ketersediaan informasi dan sistem pemrosesan informasi?
- Efek apa yang mungkin dari kejadian keamanan yang tidak diinginkan?

- Sistem TI apa yang digunakan untuk memproses informasi yang membutuhkan perlindungan khusus terkait kerahasiaan?
- Apakah keputusan kunci/penting yang bergantung pada kebenaran, kemutakhiran (up-dateness), dan ketersediaan informasi yang diproses menggunakan TI?
- Persyaratan legal apa atas hasil dari perlindungan?

8

Sumber Daya Manusia Tim Audit

8.1 Etika Profesi

Untuk mendapatkan kepercayaan dalam proses audit IS, perlu adanya etika profesional yang dimiliki dan dijalankan oleh individu yang melaksanakan dan institusinya. Adapun prinsip etika diantaranya adalah sebagai berikut:

- **Jujur dan Rahasia**. Kejujuran adalah dasar dari kepecayaan dan akan membentuk kehandalan (reliabilitas) dari penilaian. Dan kerahasiaan juga menjadi hal yang penting, karena proses bisnis dan informasi bersifat bergantung pad keamanan informasi, oleh karena itu prinsip kerahasiaan sangat diperlukan menyangkut hasil audit. Auditor IS harus sadar akan nilai suatu informasi yang diterima dan diketahuinya, oleh karena itu tidak diperkenankan membuka informasi tanpa ijin dari pemiliknya kecuali terkait dengan peraturan/hukum dan kepentingan profesional jika diperlukan.
- **Kepakaran dalam ilmu**. Audior IS hanya menerima pekerjaan yang sesuai dengan kepakarannya. Harus senantiasa meningkatkan pengetahuan, efektifitas, dan kualitas dari pekerjaan.
- **Teliti dan objektif**. Auditor IS harus mampu mendemonstasikan objektifitas dan ketelitian kepakarannya pada level yang paling tinggi dan pada saat mengumpulkan, mengevaluasi dan

memberikan informasi pada proses bisnis dan aktifitas auditnya. Evaluasi pada segala kemungkinan pekerjaan auditnya tidak boleh memimak dan dipengaruhi oleh kepentingan/keinginan pemiliknya atau orang lain.

- **Presentasi objektif**. Auditor IS harus dapat melaporkan hasil penilaiannya secara tepat dan jelas serta jujur kepada kliennya. Presentasi yang mudah dimengerti dan imparsial serta sesuai fakta harus dilakukan atas laporannya. Serta harus dapat menyampaikan evaluasi atas fakta temuannya, rekomendasi khusus/spesifik untuk meningkatkan proses dan perlindungan (safeguards).

- **Verifikasi dan reproduksibilitas**. Harus dapat melakukan verifikasi dan memilki kemampuan untuk mereproduksi dengan mengikuti dokumentasi dan metodologi reproduksi (rencana audit IS, laporan audit IS) dalam menuju suatu kesimpulan.

8.2 Tanggung Jawab Klien

Dalam pelaksanaan audit keamanan IS oleh tim audit, klien harus atau pihak manajemen organisasi yang di audit harus memantau dan bertanggung jawab atas aktifitas berikut ini:

- Memeriksa latar belakang dan kualifikasi dari vendor pendukung dan auditor keamanan untuk melihat apakah memiliki pengalaman dan keahlian khusus.

- Mempersiapkan perjanjian untuk kerjasama dengan vendor pendukung yang, seperti *disclaimer liability* , detail layanan, pernyataan non-disclosure, sebelum memulai satu kegiatan audit atau penilaian. Hal ini penting ketika memutuskan untuk melakukan pengujian penetrasi eksternal, misalkan peretasan/hacking ke dalam jaringan internal dari Internet.

- Menugaskan staf sebagai kontak utama atau tambahan dengan vendor

- Menyediakan daftar kontak ke vendor yang dapat dihubungi pada saat jam kerja atau bukan jam kerja, jika dibutuhkan

- Dapat bekerjasama dan berfikiran terbuka

- Mengijinkan akses fisik dan logikal hanya ke sistem, jaringan atau peralatan komputer yang penting untuk melakukan evaluasi, dan melindungi semua aset yang dapat terkena dampak dengan layanan/kegiatan tersebut.
- Mendapatkan peringatan atau pemberitahuan formal dari vendor mengenai tingkat/level dampak atau kerusakan pada jaringan, layanan atau sistem pada saat pengujian, sedemikian hingga skema recovery dan prosedur penanganan kejadian dapat dijalankan sebelum kejadian.
- Memberikan tanggapan/respon terhadap permintaan auditor keamanan IS sepanjang dalam waktu yang sesuai
- Memberikan ruang kerja yang memadai beserta peralatannya bagi vendor atau tim audit dalam menjalankan tugasnya
- Menyediakan semua dokumen yang diperlukan sesuai dengan area audit atau penilaian yang disepakati
- Memiliki hak untuk mengadakan rapat/pertemuan dengan vendor untuk proses kontrol dan review
- Melakukan perubahan atau penambahan pada kesempatan awal, terutama pada hal yang beresiko tinggi

8.3 Tanggung Jawab Auditor SI

Auditor IS seharusnya memiliki tanggung jawab sebagai berikut:

- Memiliki keahlian dan kepakaran yang sesuai/dibutuhkan
- Mengetahui dampak dari setiap perangkat dan memperkirakan dampaknya ke klien yang sesuai dengan kebutuhan bisnis
- Memilki otoritas/ijin tertulis dari pihak terkait seperti dari ISP dan kepolisian, terutama pada pengujian peretasan/hacking
- Mendokumentasikan setiap pengujian apapun hasilnya, baik sukses maupun tidak
- Menjamin bahwa laporan sesuai dengan kebutuhan dan kebijakkan klien

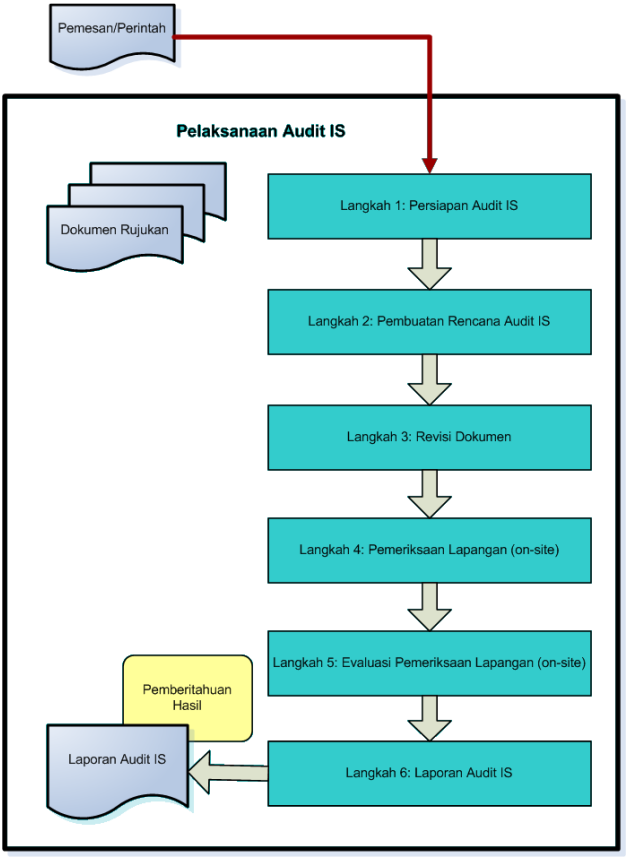
- Memberikan penilaian yang baik dan melaporkan dengan segera setiap resiko signifikan yang ditemukan kepada klien

9

Bakuan Pelaksanaan Audit Keamanan Informasi

Pelaksanaan audit IS dapat mengikuti metodologi dasar berikut ini, seperti ditunjukkan pada Gambar 9.1.

1. Langkah 1. Pada prosedur awal, penentuan kondisi umum perlu dilakukan dan dokumen pendukung perlu disiapkan untuk bahan rapat terbuka institusi dengan tim audit IS
2. Langkah 2. Dengan dokumen pendukung yang telah diterima pada langkah 1, tim audit akan memperoleh gambaran besar institusi/organisasi yang akan diperiksa dan membuat rencana audit IS.
3. Langkah 3. Berdasarkan rencana audit IS yang dibuat, maka dilakukan penilaian konten/isi dokumen yang ada. Apabila diperlukan, dokumen lainnya akan diminta untuk penilaian. Berdasarkan pada dokumen revisi dan rencana audit IS (dimana telah di update selama proses audit berlangsung), terminologi kronologis dan organisasi pada pemeriksaan langsung di tempat (on-site) dikordinasikan dengan penanggung jawab (contact person) yang ditunjuk sebagai perwakilan organisasi/institusi.



Gambar 9.1: Langkah Pelaksanaan Audit IS

Fase	**Tugas**	**Waktu dalam %**
Langkah 1	Persiapan Audit IS	5
Langkah 2	Pembuatan Rancangan Audit IS	15
Langkah 3	Revisi Dokumen	20
Langkah 4	Pemeriksaan on-site	35
Langkah 5	Evaluasi Pemeriksaan on-site	5
Langkah 6	Pembuatan Laporan Audit IS	20

Tabel 9.1: Waktu Relatif yang diperlukan pada setiap langkah pada pelaksanaan audit IS

4. Langkah 4. Pemeriksaan langsung di tempat (on-site) dimulai dengan rapat terbuka yang dihadiri oleh partisipan utama. Setelah itu, akan dilakukan wawancara, lokasi akan diinspeksi/dikunjungi, dan evaluasi permulaan dilaksanakan. Fase pemeriksaan on-site diakhiri dengan rapat tertutup.

5. Langkah 5. Informasi yang diperoleh dari pemeriksaan on-site dikonsolidasikan dan dievaluasi lebih jauh oleh tim audit IS.

6. Langkah 6. Hasil dari audit IS diringkas dalam laporan audit IS pada akhir telaah/review. Perkiraan jumlah kerja yang diperlukan untuk setiap langkah harus berdasarkan pada jadwal pada berikut ini:

9.1 Langkah 1 - Persiapan Audit IS

Manajemen tingkat atas untuk setiap instansi pemerintah dan perusahaan bertanggung jawab untuk: pelaksanaan tugas dan fungsi di semua area bisnis, pencapaian target proses bisnis, dan pendeteksian dan minimalisasi resiko tiap waktunya. Sebagaimana ketergantungan proses bisnis dengan TI meningkat, persyaratan untuk menjamin keamanan informasi eksternal dan internal juga meningkat.

Pihak manajemen harus memulai, mengendalikan dan mengawasi proses keamanan. Tanggung-jawab sepenuhnya di pihak manajemen, namun usaha untuk mencapai level keamanan yang diinginkan dapat didelegasikan ke petugas TI. Dalam prosesnya, manajemen harus secara intensif terlibat dalam proses manajemen keamanan informasi, hal tersebut merupakan satu-satunya jalan bahwa manajemen keamanan informasi dapat menjamin tidak adanya resiko yang tidak dapat diterima dan sumber daya diinvestasikan secara tepat.

Ketika memulai audit IS, pihak manajemen harus berpartisipasi pada saat institusi atau organisasinya sedang diperiksa. Dalam tahapan ini, objek yang akan diperiksa harus spesifik/jelas, adanya kontrak yang jelas, dan dalam kontrak tim audit IS harus diberikan otoritas (misalkan otoritas untuk melihat dokumen yang ada).

Orang yang bertanggung jawab dalam organisasi dalam audit IS, bagaimanapun haru menjelaskan fungsi inti organisasi kepada auditor dan menyediakan penjelasan singkat akan teknologi informasi (TI) yang digunakan. Dokumen rujukan berikut ini harus disediakan oleh institusi bagi tim audit IS, yang akan menjadi dasar bagi pelaksanaan audit IS:

- Dokumen Institusi/Organisasi
  - Diagram Struktur Organisasi (Organigram)
  - Konsep kerangka kerja (framework) TI
  - Jadwal Pertanggungjawaban
- Dokumen Teknis
  - **Konsep Keamanan**. Konsep keamanan adalah dokumen utama dalam proses dan konten keamanan, seperti rencana jaringan, analisis struktur, definisi kebutuhan perlindungan, analisis keamanan tambahan, pemeriksaan keamanan dasar.
  - Ekspor **database manajemen keamanan informasi**, jika memungkinkan
  - **Kebijakkan Keamanan**. Pihak manajemen bertanggung jawab atas fungsi organisasi yang berjalan layak dan efisien dan juga menjamin keamanan informasi baik internal maupun eksternal. Untuk alasan tersebut, pihak manajemen harus memulai kontrol,dan memandu atau

proses keamanan informasi. Hal tersebut termasuk diantaranya mengeluarkan pernyataan strategis menyangkut keamanan informasi, spesifikasi konseptual, dan kondisi umum organisasi dalam rangka untuk mencapai level keamanan informasi yang diinginkan dalam seluruh proses bisnis.

- **Daftar Proses Bisnis yang penting**. Daftar tersebut haruslah ditampilkan karena merupakan kepentingan pilihan dari objek target dan pemutakhiran (up-date) dari rencana audit IS dengan pendekatan berbasis resiko berikut.
- Jika memungkinkan, diperlukan adanya **laporan audit IS dari enam (6) tahun sebelumnya**.

9.2 Langkah 2 - Implementasi audit

Langkah ini pada dasarnya adalah pembuatan rencana audit IS dan tahapan pemindaian dokumen. Semua dokumen rujukan harus diperiksa kelengkapan dan kemutakhirannya (*up-date-ness*). Pada saat mengevaluasi kemutakhiran dokumen, sebagai catatan, bahwa beberapa dokumen akan lebih umum (generik) dibandingkan dokumen lainnya,oleh karena itu diperlukan untuk dan tergantung pad dokumen tersebut.

Bagaimanapun, suatu institusi/organisasi harus mengevaluasi seluruh dokumen secara reguler untuk melihat apakan sudah sesuai dengan keadaan sekarang/yang berlaku. Tim audit IS memeriksa prosedur tersebut dengan penyaringan apakah sesuai atau tidak dengan membandingkannya dengan hasil pemeriksaan langsung (*on site*).

Untuk faktor kelengkapan, konten/isi dari dokumen diperiksa untuk melihat jika semua aspek telah didokumentasi dan jika adanya penugasan yang sesuai. Dokumen yang ditampilkan haruslah komprehensif untuk tim audit IS.

Dengan penyaringan dokumen, tim audit IS akan mendapatkan gambaran tugas-tugas utama, organisasi itu sendiri, dan penggunaan TI dalam organisasi yang diperiksa. Berdasarkan hal-hal tersebut di atas, tim audit mulai membuat rencana audit IS. Dimana rencana tersebut merupakan perangkat (*tools*) utama yang digunakan dalam keseluruhan audit, dan mendokumentasikan semua aktifitas audit.

9.3 Langkah 3 - Audit Operasional

Pemeriksaan dokumen dilaksanakan dengan dasar atas perlindungan yang spesifik dalam rencana audit IS. Pemeriksaan dokumen utamanya berfokus pada kelengkapan (*completeness*) dan pemahaman atas dokumen. Dalam pengertian kelengkapan, dokumen harus diperiksa untuk menjamin semua aspek utama (seperti sistem, jaringan, aplikasi TI, dan ruangan) terdokumentasi dan peran yang dijelaskan sudah ditugaskan secara aktual.

Evaluasi kelayakan mencakup antara lain, evaluasi personil, organisasi, dan perlindungan teknik dalam lingkup keefektifannya. Untuk mengevaluasi kelayakan dari perlindungan, pertanyaan berikut ini seharusnya dijawab:

- Ancaman apa yang seharusnya direduksi dengan penerapan perlindungan (*safeguards*)
- Apakah resiko sampingan/residual yang harus diambil oleh organisasi? Apakah level resiko sampingan dapat ditangani organisasi menurut dokumen yang ada?
- Apakah perlindungan yang ada sesuai dan dapat secara aktual diterapkan dalam prakteknya?
- Apakah perlindungan dapat diaplikasikan, mudah dipahami, dan tidak cenderung mengakibatkan error?

Dokumen yang dipresentasikan harus dapat dipahami komprehensif oleh tim audit IS. Alasan atas keputusan yang dibuat organisasi harus disediakan dan tercantum dalam dokumen yang diperiksa.

Bagian kecil dari perlindungan yang diperiksa dapat dievaluasi dengan lengkap sebelumnya dalam fase pemeriksaan dokumen. Rencana audit IS harus dilengkapi oleh hasil perlindungan dari perbedaan yang ditemukan pada saat pemeriksaan dokumen. Untuk setiap perlindungan dalam rencana audit IS, pertanyaan utama yang perlu dijawab dikumpulkan dalam spesifikasi teknis audit yang digunakan, dan partner wawancara dalam organisasi untuk pemeriksaan langsung di lokasi (on-site).

Setelah itu, pertanyaan ini perlu dilakukan konsolidasi. Hal tersebut berarti bahwa pertanyaan mengenai perlindungan harus diurutkan, dan jika mungkin, menurut rekan wawancara diringkas menurut sistem yang diperiksa, dan pertanyaaan yang redundan dihilangkan. Hal

tersebut akan memudahkan prosedur audit IS, meningkatkan kemudahan pemahaman atas hasil, dan diberikan pada dokumen pengujian aksi.

Dalam kerjasama dengan dengan staff penghubung dari organisasi yang diperiksa, tim audit IS bekerja diluar waktu penjadwalan untuk pemeriksaan langsung (on-site) yang tercakup dalam rencana audit IS. Staff penghubung dalam organisasi yang diperiksa bertanggung jawab untuk penjadwalan koordinasi dan menyediakan ruangan yang dibutuhkan apabila perlu.

Rencana audit pada saat ini terdiri dari hal-hal berikut ini:

- Spesifikasi dari objek dan perlindungan target modul yang diperiksa
- Perlindungan tambahan untuk menguji kemunculan konjungsi dengan defisiensi yang ditemukan selama pemeriksaan berlangsung
- Pemilihan teknik audit untuk tipe perlindungan tertentu
- Jika memungkinkan, spesifikasi dan peran dari rekanan wawancara
- Spesifikasi dari penjadwalan

9.4 Langkah 4 - Audit Infrastruktur

Langkah ini dilakukan dengan pemeriksaan di lokasi (on site). Tujuan dari pemeriksaan langsung di lokasi adalah untk membandingkan dan memeriksa dokumen yang dsajikan, seperti konsep dan panduan, dengan kondisi aktual di lokasi sehingga dapat dilihat apakah keamanan informasi digaransi dalam bentuk yang cukup dan praktis dengan jenis perlindungan yang dipilih.

Namun pada pelaksanaannya, tim audit IS tidak harus mutlak berpaku setiap saat pada rencana audit IS. Mungkin dan wajar pada suatu waktu melewatkan beberapa bagian dari rencana audit. Hal tersebut merupakan kasus yang terjadi dikarenakan perlindungan untuk sampel pertama yang direview tidak diimplentasikan dengan baik dan cukup, yang berarti perlu dilakukan pengujian mendalam. Selain pengujian mendalam perlu diperlukan pengujian lebih jauh untuk mencari kesenjangan (*gap*) keamanan. Rencana audit IS perlu dilakukan pemutakhiran atasnya.

Keputusan untuk membatalkan atau memperluas pemeriksaan objek target modul atau perlindungan merupakan diskresi dari tim audit IS. Perluasan pemeriksaan merupakan suatu keharusan, yang bagaimanapun juga tetap ada pembatasan atas objek audit sesuai dengan spesifikasi dalam kontrak dengan manajemen.

Tim audit IS mengadakan rapat pembukaan pada permulaan pemeriksaan on-site dengan pihak manajemen institusi/organisasi yang bersangkutan diantaranya, baik orang yang bertanggung jawab akan audit IS, Kepala TI, dan petugas TI. Jika dibutuhkan, dimungkin juga rapat dihadiri perwakilan dari bagian lain. Pada saat rapat perlu dijelaskan oleh mengenai objek audit dan prosedur audit. Tim audit harus mempresentasikan mengenai dokumen apa saja yang diperlukan untuk memperlancar proses audit IS. Perlu dijelaskan juga dalam rapat mengenai anggota tim auditor, waktu pemeriksaan, regulasi akses, dan jam kerja.

Rencana audit IS yang digunakan oleh tim audit IS berperan sebagai perangkat bantuan yang bertujuan mempercepat proses pengerjaan, dan digunakan untuk mendokumentasikan kegiatan pengujian yang dilakukan.

Pengujian dilaksanakan pada permulaan menggunakan teknik audit yang dipilih, biasanya dalam bentuk wawancara dan inspeksi. Tim audit IS tidak dapat langung mengintervensi langsung ke sistem, terutama ketika sistem dan metode yang rumit atau karena ukuran data yang sangat besar telah berjalan. Untuk mengatasinya, tim dapat meminta informasi pendukung seperti berkas atau dokumentasi elektronik untuk proses evaluasi lebih lanjut. Tetap, tim audit IS harus ter-up-date setiap saat.

Jika tim audit menemukan adanya deviasi atau penyimpangan dari status dokumen yang ada pada saat pemeriksaan sampel, oleh karena itu perlunya penambahan jumlah sampel untuk mendapatkan penjelasan yang beralasan. Pemeriksaan hanya bisa berhenti manakala penjelasan mengenai alasan deviasi sudah dapat terjawab.

Selama pemeriksaaan berlangsung, semua fakta seperti spesifikasi sumber daya dan informasi dari dokumentasi yang diminta baik dalam hasil wawancara atau dokumen tertulis. Bantuan teknis seperti foto dan screen shot dapat digunakan untuk dokumentasi. Semua sumber daya dokumentasi teknis harus disetujui oleh pihak manajemen institusi dan hanya dapat digunakan dengan ijin.

Pada akhir pemeriksaan on-site, semua hasil sementara, sisa kerja dan prosedur yang belum terlaksana perlu disampaikan dalam rapat

penutupan. Pihak terkait seperti Kepala TI, Petugas TI, penanggung jawab TI institusi harus hadir dalam rapat tersebut, termasuk perwakilan bidang/bagian lain jika diperlukan.

9.5 Langkah 5 - Evaluasi Audit *On-site*

Setelah pemeriksaan/audit on-site, informasi yang didapat perlu digabungankan dan dievaluasi. Tahap evaluasi ini dapat pula dilakukan oleh pakar/ahli apabila memerlukan pengetahuan pakar tersebut, jika tim audit tidak dapat menjalankan tahap tersebut. Jika ada kontrak dengan pakar tersebut, perlu dijelaskan dan meminta izin dari institusi yang diperiksa, atau dapat membuat informasi anonim sedemikian dapat ditarik kesimpulan terkait organisasi atau personil. Evaluasi informasi termasuk kedalam evaluasi keseluruhan dari pengujian atas perlindungan (safeguards).

Setelah evaluasi dokumen dan informasi lainnya, dilakukan evaluasi final/akhir pada perlindungan yang diuji dan hasil diringkas dalam laporan audit IS.

9.6 Langkah 6 - Laporan Audit

Laporan audit IS, termasuk dokumen rujukan, dilaporkan dalam bentuk tertulis untuk diserahkan pada pihak manajemen institusi yang diperiksa, Kepala TI, Penanggung jawab audit, dan petugas TI terkait. Versi draft laporan audit IS diberikan kepada pihak manajemen untuk memverifikasi fakta yang ditemukan oleh tim audit IS. Pihak manajemen institusi yang diaudit bertanggung jawab untuk memastikan bahwa memberikan informasi kepada semua pihak yang terkena dampak terkait hasil audit.

Laporan audit IS, minimal terdiri dari isi sebagai berikut:

- Ringkasan Eksekutif,
- Evaluasi bergambar dari status keamanan informasi
- Deskripsi lengkap atas fakta temuan
- Evaluasi setiap perlindungan (safeguards) yang diuji.

Laporan audit terdiri dari bagian berikut ini:

Evaluasi Keamanan	**Visualisasi Warna dalam Laporan**
Kelemahan Keamanan tingkat Serius	Merah
Kelemahan Keamanan	Kuning
Rekomendasi Keamanan	Hijau

Tabel 9.2: Visualisasi Warna Penekanan atas Kelemahan Keamanan

1. **Bagian 0**, terdiri atas informasi institusi/organisasi, misal dasar pengauditan, kronologis per langkah kegiatan audit IS, deskripsi singkat tentang kontrak audit
2. **Bagian 1**, merupakan ringkasan eksekutif/manajemen. Ringkasan ini terdiri dari maksimal dua halaman, isi fakta utama yang ditemukan dalam audit IS dalam bentuk singkat dan menyeluruh, rekomendasi hasil dari fakta temuan.
3. **Bagian 2**, sebagai tambahan bagi ringkasan eksekutif, perlu didukung dengan gambar atau grafik hasil audit.
4. **Bagian 3**, terdiri dari deskripsi detil area pengujian dan fakta temuan berikut detil teknis dan rekomendasi. Disarankan untuk mempersingkat bagian ini sesuai dengan objek target modul dan pengujian perlindungan. Hanya perlindungan yang tidak memadai dan rekomendasi perlindungan keamanan yang perlu dicantumkan di bagian ini. Sebaiknya digunakan visualisasi warna yang menarik/mentereng untuk memberi penekanan mengenai fakta dan rekomendasi, seperti pada Tabel 9.2:

Pada pembuatan laporan audit IS, aspek formal berikut harus dicantumkan. Semua uji yang dilakukan, hasilnya, dan evaluasi hasil harus dokumentasi yang dapat direproduksi dan dimengerti.

- Tabel dari isi harus mengandung laporan aktual termasuk apendik (misal: screen shot, gambar, log file, dll). Setiap apendik harus mudah diidentifikasi sehingga pengecekan laporan audit dan apendik dengan lengkap.

- Semua dokumen rujukan harus didaftarkan
- Data yang disimpan, misalkan catatan notulensi rapat atau log file evaluasi yang merujuk pada laporan harus disertakan dalam apendik
- Setiap halaman dirancang untuk kemudahan proses identifikasi (misalkan, menggunakan nomor halaman, nomor versi dan judul serta tanggal laporan)
- Jika ada perangkat lunak yang digunakan dalam kegiatan audit, misal perangkat untuk analisis, maka perlu dicantumkan jenis dan versinya serta hasil cetaknya.
- Terminologi khusus atau singkatan yang tidak biasa digunakan dan muncul dalam laporan, maka perlu ditulis dalam glossary atau indeks singkatan

Pihak manajemen perlu mendapatkan secara reguler laporan sebagai berikut:

- Hasil utama dari laporan audit IS
- Status keamanan dan pengembangan status keamanan ditunjukkan dalam laporan audit IS
- Tindak lanjut kegiatan

Laporan audit dan dokumen referensi harus disimpan dalam bentuk bebas dari revisi (revision-proof) dari insitusi yang diaudit minimal untuk selama 10 tahun sejak laporan diserahkan. Laporan tersebut menjadi rujukan dasar bagi audit di periode selanjutnya.

Kriteria untuk pengarsipan bebas dari revisi adalah sebagai berikut (IT-Grundschutz module 1.12):

- Ketepatan (Correctness)
- Kelengkapan (Completeness)
- Perlindungan dari perubahan dan kesalahan
- Aman dari kehilangan
- Hanya dapat digunakan oleh pihak yang memiliki otoritas
- Perawatan untuk setiap periode pengarsipan

- Dokumentasi prosedur
- Dapat diuji
- Dapat direproduksi

10

Tindak Lanjut Audit

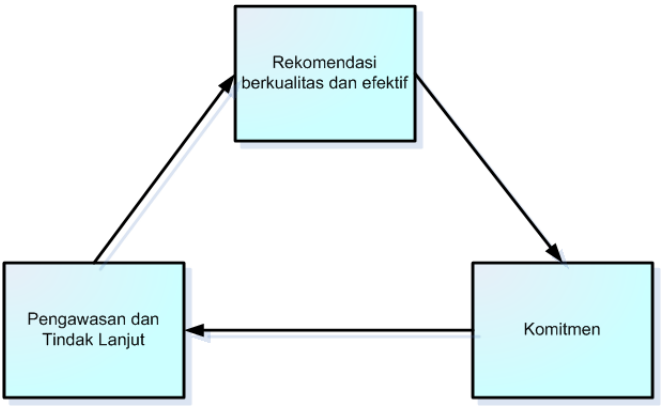
Keuntungan dari penilaian resiko IS dan audit adalah bukan dari rekomendasi yang dihasilkan, namun pada implementasi yang efektif. Ketika rekomendasi diberikan, pada dasarnya pihak manajemen akan merespon untuk penerapannya. Namun, keputusan manajemenlah yang menentukan terjadinya resiko keamanan apabila diterapkan atau tidaknya rekomendasi tersebut. Perlu alasan-alasan yang cukup guna mendukung keputusan yang dibuat.

Ada tiga hal penting terkait dengan rekomendasi yang dibuat dalam audit:

- Rekomendasi yang berkualitas, dan efektif
- Komitmen
- Pengawasan dan tindak lanjut

Auditor IS diperlukan untuk menghasilkan rekomendasi yang berkualitas dan efektif, yang harus memiliki karakteristik berikut ini:

- Spesifik dan jelas, mudah dimengerti dan teridentifikasi
- Meyakinkan dan persuasif dengan bukti yang cukup
- Signifikan (berarti)
- Memungkinkan untuk diterapkan



Gambar 10.1: Tindak Lanjut atas Rekomendasi yang diberikan

Komitmen seseorang atau suatu departemen sangatlah penting untuk implementasi suatu rekomendasi. Auditor, staff, dan pihak manajemen memiliki bermacam kepentingan, penekanan dan prioritas atas suatu rekomendasi yang diberikan.

- **Auditor IS,** merupakan pihak pertama yang memberikan rekomendasi untuk peningkatan lebig baik, oleh karena itu auditor harus:
  - percaya diri atas rekomendasi yang diberikannya dan jika rekomendasi ditindaklanjuti maka seharusnya ada suatu peningkatan yang terjadi
  - memahami lingkungan kerja unit/departemen berikut kendalanya seperti kendala waktu, sumber daya dan budaya
  - berkomunikasi melalui jalur yang efektif dan seharusnya dalam memberikan rekomendasi
- **Staff,** merupakan pihak yang secara langsung atau tidak langsung terpengaruh oleh rekomendasi.Seorang staff haruslah:
  - dimotivasi dan didorong untuk bekerjasama dengan auditor IS
  - diberikan waktu dan sumber daya yang cukup untuk melakukan kerja tambahan dan pengembangan

  - dijamin mendapatkan keuntungan atas suatu rekomendasi

- **Manajemen**, memegang peranan penting dalam pemberdayaan pengembangan. Pihak manajemen seharusnya:

  - proaktif bukan reaktif terhadap permasalahan keamanan
  - menyediakan dukungan yang berarti akan proses audit dan penilaian
  - mengalokasikan sumber daya yang cukup untuk pengembangan
  - memahami bahwa penindaklajutan merupakan hal yang berharga dan menjadi tanggung jawabnya
  - mendorong munculnya pengembangan dengan rencana, kendali dan komunikasiyang cukup
  - mempromosikan kesadaran dan pelatihan bagi staff

10.1 Pengawasan dan Tindak Lanjut

Pengawasan dan tindak lanjut memiliki 3 langkah utama:

- Menyiapkan sistem pengawasan dan tindak lanjut yang efektif
- Mengidentifikasi rekomendasi dan mengembangkan rencana tindak lanjut
- Melakukan pengawasan aktif dan pelaporan

Pihak manajemen seharusnya menyiapkan sistem tindak lanjut dan pengawasan untuk menindak lanjuti suatu rekomendasi. Selain itu, manajemen bertanggung jawab memberikan dukunga yang cukup, panduan keseluruhan, dan arahan.

10.2 Identifikasi Rekomendasi dan Perencanaan

Untuk melakukan pengembangan yang efektif, hal berikut perlu dilakukan:

- Mengidentifikasi rekomendasi yang kritis, signifikan dan rekomendasi kunci dengan tambahan pengawasan dan kerja maksimal
- Mengembangkan rencana tindak lanjut untuk semua rekomendasi; termasuk rencana implementasi, perkiraan waktu, daftar aksi, metode dan prosedur verifikasi hasil
- Menekankan pada rekomendasi kunci yang dilaporkan dan menjadi prioritas pada proses tindak lanjut
- Menindaklanjuti semua rekomendasi sesuai rencana

Secara proaktif mengawasi dan melaporkan kemajuan dan status aksi, dan mengambil langkah penindaklajutan semua rekomendasi yang dibutuhkan sampai implementasi selesai.

10.3 Status Aksi dan Kemajuan

Ada beberapa status aksi dan kemajuan:

- Aksi belum dimulai
- Aksi selesai/lengkap/selesai
- Aksi sedang dilakukan dengan tanggal penyelesaian target
- Alasan suatu aksi belum dijalankan
- Aksi alternatif jika ada perbedaan dari rekomendasi

Berikut ini adalah beberapa aksi tindak lanjut sebagai pertimbangan:

- Review/telaah rencana implementasi, dokumentasi dan jadwal waktu rencana aksi
- Temukan alasan yang kuat kenapa suatu aksi tidak dilakukan
- Tetapkan langkah atau tugas tambahan untuk menangani kesulitan teknis, operasional dan manajerial
- Temukan rekomendasi alternatif terkait dengan lingkungan yang tidak diharapkan atau ada perubahan persyaratan

- Tentukan penyelesaian atau pemberhentian rekomendasi apabila sudah berhasil diterapkan dan diujikan, atau tidak lagi valid atau tidak berhasil walaupun sudah dilakukan aksi lebih lanjut
- Menilai keefektifan dari aksi korektif
- Melaporkan pencapaian, status dan kemajuan/progress ke pihak manajemen
- Eskalasikan ke manajemen apabila dapat diterapkan, terutama ketika implementasi atas rekomendasi kunci tidak cukup atau tertunda.

11

Pengujian dan Latihan

Setelah mengetahui konsep manajemen keamanan informasi, dan sebelum memulai secara aktual proses audit IS, manajemen dapat melakukan uji/pengujian dan latihan terlebih dahulu terhadap rencana audit IS yang ditentukan agar proses audit IS nanti dapat berjalan dengan efektif dan efisien serta meminimalkan resiko atau dampak yang mungkin terjadi pada proses audit.

Pengujian dan latihan memverifikasi asumsi dasar dari konsep itu berada. Penerapan pengukuran atau paket pengukuran individu memeriksa aspek ketepatan (*correctness*), dan operasional akan teknologi yang digunakan. Latihan juga menunjukkan jika dokumentasi keberlangsungan bisnis dapat berguna dan juga melihat apakah faktor yang terlibat dapat menjalankan tugas yang diperintahkan pada saat darurat.

Latihan-latihan akan melatih prosedur yang dijelaskan dalam rencana audit IS, membuat personil menjalankan aksi yang dibutuhkan secara rutin, dan memverifikasi apakah solusi efisien. Latihan akan meningkatkan waktu reaksi dan menyediakan rasa atau tingkat keamanan bagi pegawai pada saat bekerja menggunakan sistem TI. Karena kecenderungan orang yang bertindak tanpa berfikir secara benar dan rasional ketika terjadinya krisis, maka latihan sangat perlu dilakukan dan jangan pernah dianggap hal yang remeh.

Pengujian dan latihan akan selalu terkait dengan faktor waktu dan pengeluaran. Untuk memastikan investasi yang ditanam dalam pengujian dan latihan menjadi hal yang masuk akal, maka perlu adanya

suatu rencana. Rencana yang dibuat harus memasukan serangkaian tes dan latihan, tidak hanya satu. Jenis pengujian dan latihan dipilih bergantung pada tipe dan ukuran organisasi beserta lingkungan lokalnya dan harus dipilih dalam bentuk kasus -per-kasus.

11.1 Jenis Uji dan Latihan

Berikut ini adalah beberapa jenis uji dan latihan, mulai dari yang sederhana hingga komplek:

- **Pengujian pengukuran pencegahan teknis**. Untuk menjamin kelayakan dan operasional dan solusi teknis, solusi tersebut haruslah diuji. Sebagai contoh, pengujian baris yang redundant, power supply, restorasi data dari backup data, keandalan cluster, teknologi alarm yang digunakan, infrastruktur teknis atau komponen-komponen TI lainnya. Komponen individual dan masing-masing fungsinya harus diuji secara reguler dan diuji ketika ada perubahan besar akan sistem untuk melihat dan memastikan interoperasinya.

- **Pengujian fungsi**. Jenis uji ini, fungsionalitas dari prosedur-prosedur, subproses, dan kelompok sistem dinyatakan dalam sub rencana yang bermacam-macam dari buku tangan (handbook) keberlangsungan bisnis yang akan diperiksa. Selam pemeriksaan berlangsung, prosedur-prosedur, perlu diperiksa terutama menyangkut interoperasi dan ketergantungan dari komponen atau pengukuran yang berbeda. Hal tersebut termasuk diantaranya rencana recovery, rencana restorasi, dan rencana keberlangsungan bisnis untuk pengukuran segera (misal proses evakuasi personil ketika alarm kebakaran berbunyi).

- **Telaah (*review*) rencana**. Tujuan dari telaah rencana adalah untuk memeriksa rencana individual atas tanggapan akan krisis dan keadaan darurat.

- **Latihan tabletop**. Pengertian latihan tabletop digunakan untuk merujuk pada pemeriksaan teoritis suatu masalah dan skenario di atas meja. Dalam latihan ini, skenario hipotesis diberikan dan kemudian secara teoritis diperiksa. Latihan jenis mudah dalam pelaksanaannya. Latihan ini harus dilakukan berulang kali selama penetapan fase manajemen keberlangsungan bisnis.

- **Latihan tim krisis**. Merupakan bentuk khusus dari latihan tabletop, dalam hal ini latihan dilakukan bekerjasama dengan tim krisis

- **Latihan command post (ruang kendali)**. Juga merupakan bentuk lain dari latihan tabletop yang berdasar pada versi tambahan/pengembangan dari latihan tim krisis yang digunakan untuk memeriksa dan melatih kerjasama dalam tim krisis serta memeriksa tingkat kerjasama antara tim krisis dengan tim operasional. Secara umum struktur dari command post diuji dalam latihan praktik yang simultan dengan implementasi operasional secara teoritis

- **Latihan alam dan komunikasi**. Titik kritis pada saat merespon keadaan darurat atau krisis adalah melaporkan dan memperingatkan (alarm) tim krisis dan orang lain yang bertanggung jawab. Oleh karena itu, perlu diperiksa secara reguler akan prosedur pelaporan, eskalasi dan alarming (peringatan). Ruang lingkup dari tes ini mulai dari pemeriksaan sederhana atas sumber daya komunikasi hingga pengumpulan tim krisis dalam ruang pertemuan tim krisis. Dalam uji ini, tanggung jawab dan nomor telepon perlu dicantumkan dalam rencana, seperti halnya strategi eskalasi, prosedur, dan kemampuan menjangkau orang terkait serta aturan pergantian. Contohnya adalah pencantuman dalam rencana untuk komponen: sistem alarm, telepone darurat, SMS, pager,Internet, komunikasi radio atau satelit)

- **Simulasi skenario**. Dalam simulasi realistis, prosedur dan pengukuruan dinyatakan untuk merespon skenario atau kejadian keberlangsungan bisnis harus dilakukan pengujian.

- **Latihan keberlangsungan bisnis atau skala penuh**. Tipe simulasi yang paling komplek adalah latihan keberlangsungan bisnis atau skala penuh. Adalah hal yang harus dilakukan untuk memasukan organisasi eksternal seperti pemadam kebakaran, organisasi bantuan, instansi pemerintahan dalam latihan. Latihan skala penuh berdasarkan situasi realistis dan integrsi semua level hirarki, mulai manajemen hingga ke tingkat bawah seperti karyawan yang perlu dilatih. Rencana dan pengeluaran yang dibutuhkan untuk persiapan, eksekusi, dan evaluasi tidak boleh dianggap sepele. Latihan skala penuh dilakukan apabila ingin dicapainya persyaratan keberlangsungan bisnis tingkat tinggi.

Tabel 11.1: Jenis Latihan

Exercise type	Target group			Procedure		Extent/ scope
	Strategic	Tactical	Operative	Discussion -based	Action- based	Low/ Medium/ High/ Very high
Test of the technical preventive measures			X		X	Low
Function test			X		X	Medium
Plan review		X	X	X		Low
Tabletop exercise		X	X	X		Low-medium
Crisis team exercise	X	X		X		Low-medium
Command post exercise	X	X	X	X	X	Medium-high
Communication and alarm exercise		X	X		X	Low
Simulation of scenarios		X	X		X	High
Business continuity or full scale exercise	X	X	X		X	Very high

Latihan keberlangsungan bisnis dilakukan secara reguler dengan interval waktu yang lebih panjang antara tiap latihan.

- **Perbandingan tipe latihan berbeda**. Berbagai kriteria digunakan untuk membedakan antaa tipe latihan dan pengujian. Yang dapat diklasifikasikan menurut jenis prosedur, kelompok target, lingkup atau perluasan. Terdapat tiga area tanggung jawab untuk kelompok sasaran/target: area strategi, area taktik, dan area operasional. Tabel 11.1 merupakan peta untuk tiga area tersebut.

11.2 Dokumen Latihan dan Pengujian

Untuk mendukung pengujian dan latihan diperlukan adanya dokumen pendukung, adapun jenisnya adalah sebagai berikut.

- **Manual/Panduan Latihan**. Semua pengujian dan latihan manajemen keberlangsungan bisnis dalam organisasi harus diren-

canakan dan disiapkan. Oleh karena itu untuk tetap menjaga jumlah gangguan pada tingkat yang rendah, perlu dilakukan uji dan latihan atas faktor berikut: keputusan strategis, spesifikasi dasar, kondisi umum dan perjanjian-perjanjian. Manual latihan harus dapat menjawab pertanyaan-pertanyaan berikut:

- Apa strategi penting dari uji dan latihan keberlangsungan bisnis dari organisasi?
- Apa tujuan dari uji dan latihan?
- Berapa besar bobot nilai yang diberikan organisasi untuk kegiatan pengujian dan latihan?
- Masuk dalam klasifikasi jenis apa suatu pengujian dan latihan dilakukan? Berapa banyak waktu yang dibutuhkan untuk tiap jenis dan berapa biaya kasar untuk tiap jenisnya?
- Apa tujuan dari setiap jenis pengujian dan latihan?
- Berapa banyak pengujian dan latihan yang harus dilakukan? Apakah ada badan/institusi pengawas resmi terkait dengan frekuensi latihan dan pengujian?
- Peran apa yang didefinisikan ketika merencanakan dan melakukan pengujian dan latihan? Apa tugas, hak, dan kewajiban dari peran tersebut?
- Area mana yang harus diuji: pengetahuan dan kemampuan partisipan dan karyawan, prosedur manajemen keberlangsungan bisnis, mekanisme dan teknologi yang digunakan, dokumentasi keberlangsungan bisnis, operasional sumber daya pusat, pengukuran terencana , dan lain lain?
- Metode latihan apa yang digunakan?
- Pada level apa suatu latihan dioerbolehkan mempengaruhi operasi bisnis harian?
- Bagaimana dokumentasi pengujian dan latihan? Seberapa detil akan didokumentasikan?
- Bagaimana cara mendapatkan hasil latihan tersebut?

Manual latihan terdiri dari prinsip dasar strategis sebagai bantuan detil untuk merencanakan, melakukan dan mengevaluasi pengujian dan latihan. Termasuk di dalamnya, sebagai contoh, template dokumen untuk undangan, pengumuman, rekaman log, atau kuesioner evaluasi yang perlu diisi untuk atau diadaptasi untuk latihan khusus.

- **Rencana latihan**. Merupakan kewajaran membuat serangkaian pengujian dan latihan yang sesuai, yang mencakup semua area organisasi atas rencana keberlangsungan bisnis yang hendak diujikan. Dalam rencana latihan, skenario terrencana, jenis latihan, tujuannya, metode latihan (diumumkan atau tidak), peran yang terrencana, dan durasi waktu latihan yang diharapkan harus jelas disebutkan dalam setiap pengujian dan setiap latihan. Taksiran kasar dari persyaratan sumber daya personil dan sumber daya keuangan harus dibuat.

- **Konsep pengujian dan latihan**. Konsep terpisah pengujian dan latihan harus bekerja untuk setiap uji dan latihan. Konsep ini terdiri dari rencana eksekusi detil. Konsep pengujian menjelaskan pengunaan metode dalam pengujian sistem, perangkat apa yang digunakan , dan penjelasan kondisi umum. Konsep latihan menjelaskan kelompok/grup partisipan, asumsi peran setiap partisipan, kerangka kerja kronologis, dan kriteria untuk menyelesaikan atau mengakhiri latihan. Dan spesifikasi minimum berikut yang harus ada dalam konsep pengujian latihan:

  – Nama latihan
  – Waktu, Tanggal, Durasi Latihan yang direncanakan
  – Lokasi latihan
  – Jenis latihan
  – Tujuan
  – Pemimpin latihan
  – Partisipan, pengamat dan penjaga rekaman
  – Petunjuk latihan (dalam bentuk singkat)
  – Skenario

  Konsep latihan harus dibuat dalam dua tahap. Pertama, konsep dasar dibuat dan masukkan dalam persetujuan manajemen. Yang kemudian dibuat konsep detailnya. Tambahan berikut harus diambil dalam akun jangka panjang, latihan skala besar dan latihan skala penuh. Termasuk di dalamnya, sebagai contoh, mengambil langkah pencegahan selama latihan yang mencegah partisipan dalam mendapatkan makanan dan minuman.

Tabel 11.2: Contoh Skrip Latihan

Exercise: XYZ											
No.	**Real-time**	**Scenario-**	**Keyword**	**Activity**	**Goal / reaction expected**	**Person taking action**	**Players**				**Aids/ tools/ type of action**
							A	**B**	**C**	**…**	
1	…		…		…		…	…	…	…	…
2	10:10		Report to Alarm Centre	(Description of the single situation with background information)	Examination of the alarm, escalation	Mr. Jansen		X	X		Mobile phone
3	…		…	…	…		…	…	…	…	…

- **Skrip latihan**. Skrip latihan harus dibuat untuk skenario latihan ekstensif. Dalam skrip, situasi awal, rangkaian spesifik dari kejadian dalam latihan, kejadian-kejadian, dan urutan dimana even terjadi dijelaskan sedetil mungkin. Skrip dapat membantu moderator latihan untuk menspesifikasikan rentetan kejadian selama latihan berlangsung. Format skrip latihan dapat menggunakan Tabel 11.2. Tabel tersebut, nomor sekuensial diletakkan disamping tiap aktifitas individual (situasi tunggal).

- **Waktu Pengujian dan Latihan**. Eksekusi dan serangkaian kejadian dalam pengujian dan latihan didokumentasikan secara cermat dalam menit pengujian dan latihan. Menit tersebut mengandung informasi dimana jadwal waktu digunakan sebagai dasar. Menit pengujian dan latihan membentuk basis untuk melakukan penilaian setelah pengujian dan latihan, penentuan kelemahan, dan masukkan untuk peningkatan.

11.3 Melaksanakan Pengujian dan Latihan

Beberapa prinsip dasar berikut harus diikuti pada saat pelaksanaan pengujian dan latihan. Sebagai contoh, uji atau latihan tidak hanya

untuk meminimalkan gangguan operasi normal. Pada saat memilih waktu dan tanggal eksekusi harus dimasukkan dalam akun bahwa uji dan latihan tersebut memiliki pengaruh langsung pada operasional. Sistem yang diuji mungkin saja dapat berada pada kinerja produktif tingkat rendah selama tes atau mungkin tidak tersedia sama sekali. Oleh karena itu, perlu direkomendasikan untuk melakukan pengujian dan latihan di luar jam kerja biasa.

Karyawan yang terlibat dalam ujian latihan harus meninggalkan pekerjaan hariannya selama fase latihan. Waktu megikuti latihan bagi karyawan harus dianggap sebagai waktu kerja karyawan bersangkutan dan sekaligus penilaian. Jika ujian dan latihan dilakukan di luar jam kerja biasa maka perlu adanya perjanjian kerja dibuat dengan perwakilan manajemen.

Pengukuran harus direncanakan dan memastikan bahwa latihan tetap di bawah kendali pihak yang terlibat dan tidak boleh mengarah pada malfungsi. Kriteria penghentian/pengakhiran untuk latihan dapat termasuk ekspirasi waktu tertentu atau pengenalan bahwa pengukuran diimplementasikan tidak dapat digunakan untuk mencapai sukses yang diinginkan.

Kerja ekstensif dibutuhkan untuk perencanaan, persiapan dan eksekusi latihan. Untuk alasan ini, peran untuk mempersiapkan dan eksekusi latihan harus di jelaskan bersama dengan tugas dan haknya.

- **Penulis latihan** (*exercise author*). Penulis/pengarang latihan harus ditentukan untuk mempersiapkan latihan. Pekerjaan orang ini terdiri dari pengembangan rencana latihan termasuk perancangan latihan individu, dimulai dari spesifikasi skenario dan seleksi atas partisipan hingga ke persiapan lingkungan dimana latihan akan dilaksanakan. Tugas ini tidak boleh dipandag sepele dan membutuhkan banyak waktu tergantung pada jenis latihan yang dilaksanakan. Penulis latihan ini harus terbiasa dengan konsep rencana kontigensi dan rencan darurat individu, rencana recovery dan rencana restorasi. Peran ini bisa dialamatkan pada petugas keberlangsungan bisnis atau pemimpin tim krisis.

- **Tim persiapan**. Untuk membuat dan membangun konsep latihan dan skrip latihan, penulis latihan membutuhkan bantuan dari tim persiapan. Tim ini dapat terdiri dari kepala unit atau kepala bagian.

- **Manajer/moderator latihan**. Peran sentral pada latihan yaitu

moderator/manajer latihan. Tugas orang ini adalah mengawali latihan, mengkordinasikan aktifitas masing-masing individu, membuat keputusan alternatif atau simpangan dari rencana, mengakhiri latihan.

- **Tim inti**. Tugas tim inti terdiri dari penyediaan konsultasi teknis, menjawab pertanyaan dari peserta latihan atau mengenalkan situasi tunggal untuk mengilustrasikan situasi dalam skenario latihan.
- **Penjaga waktu**. Tugas dari kelompok ini menentukan sehingga waktu latihan tidak berkepanjangan atau kurang.
- **Pengamat**. Pengamat bisa berasal dari anggota departemen audit, pegawai dari bagian lain yang ditunjuk, atau pakar dari luar atau perwakilan instansi pemerintah atau lembaga bantuan lainnya.
- **Pemain**. Kelompok pemain dapat berasal dari orang yang bertanggung jawab terhadap proses, perwakilan karyawan, pelanggan/nasabah, dan lain lain.

Eksekusi suatu latihan secara mendasar dibagai ke dalam empat fase:

1. Fase Perencanaan dan pelepasan (*planning and release*)
2. Fase Persiapan
3. Fase eksekusi
4. Fase evaluasi

12

Indeks KAMI

Kementerian Komunikasi dan Informatik telah mengeluarkan indeks KAMI (Keamanan Informasi) yang digunakan untuk melakukan penilaian dari penerapan tata kelola keamanan Sistem Informasi di lingkungan badan pemerintah.

Indeks KAMI merupakan alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di Instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005.

Kelengkapan Dokumen Kerangka Kerja Sistem Manajemen Keamanan Informasi (SMKI) secara ditail dapat dilihat pada Tabel 12.1 dan Tabel 12.2.

Setelah dilakukan verifikasi makan akan dinilai berdasarkan :

1. Kekuatan Kematangan SMKI
    (a) Aspek Kerangka Kerja
    (b) Aspek Perencanaan Keamanan Informasi
    (c) Aspek Penerapan

Tabel 12.1: Kelengkapan Dokumen SMKI (1)

No	Nama Dokumen	Ya	Tidak	Keterangan D: Draft, R:Rilis T: Tersosialisasikan
	Kebijakan, Sasaran, Rencana, Standard			
1	Kebijakan Keamanan Informasi (ref. kebijakan yang disyaratkan ISO 27001)			
2	Penggunaan Email dan Internet			
3	Sasaran TI/Keamanan Informasi			
4	Organisasi TI/ Keamanan Informasi (IT Streering Commitee, Fungsi Keamanan TI)			
5	Metodologi Manajemen Resiko TI			
6	Business Continuity Plan			
7	Kualifikasi Informasi			
8	Standard software desktop			
9	Metoda Pengukuran Efektifitas Kontrol			

Tabel 12.2: Kelengkapan Dokumen SMKI (2)

No	Nama Dokumen	Ya	Tdk	Keterengan D: Drat, R:Rilis T: Tersosialisasikan
	Prosedur-prosedur			
1	Pengendalian dokumen			
2	Pengendalian rekaman			
3	Tindakan perbaikan dan pencegahan			
4	Audit internal			
5	Penanganan (*handling*)			
6	Pengelolaan media removable			
7	Change Control Sistem TI			
8	Pengelolaan Akses Kontrol			
9	Pengelolaan gangguan TI/Insidn Keamanan Informasi			
10	Monitoring Sumber Daya TI			
11	Instalasi software			
12	Backup & restore (prosedur/jadwal)			
13	Teleworking			

2. Kelemahan/Kekurangan SMKI

    (a) Aspek Kerangka Kerja
    (b) Aspek Perencanaan Keamanan Informasi
    (c) Aspek penerapan

13

Penutup

Kegiatan audit dan penilaian resiko keamanan informasi di suatu organisasi seperti badan pemerintahan memerlukan tahapan-tahapan yang tepat, dokumen pendukung yang lengkap dan memadai. Tentu saja proses audit harus dilakuan oleh pihak-pihak yang bertanggung jawab. Perencanaan kegiatan merupakan tahapan utama yang harus dilakukan untuk menjamin optimasi dan pengawasan serta evaluasi kegiatan audit dan penilaian resiko keamanan.

Pihak yang terlibat harus dapat duduk bersama dan memiliki visi dan misi yang sama dan selaras yaitu tercapainya tujuan keamanan informasi bagi organisasi. Pihak pejabat badan pemerintah eselon 1 dan 2 wajib memberi dukungan awal dan keseluruhan bagi pelaksanaan kegiatan. Staff dan petugas TI harus didukung dan mendukung penuh pelaksanaan kegiatan. Keterbukaan dari pihak organisasi mutlak diperlukan bagi arahan audit ke depan. Kemampuan, keahlian dan reputasi pihak ketiga yakni tim audit harus dipenuhi oleh tim audit itu sendiri. Kolaborasi dan kordinasi tiga pihak utama tersebut menjadi nilai tersendiri bagi pencapaian level keamanan informasi yang diinginkan.

Sistem informasi yang semakin kompleks ini memerlukan penanganan, pengelolaan, dan perawatan oleh badan pemerintah pengguna sistem informasi tersebut. Banyak kendala yang dihadapi dalam pelaksaan audit IS pada badan pemerintah seperti di Kemenpora harus dapat ditangani, seperti dukungan manajemen puncak yang penuh, ego sektoral yang cenderung memiliki ketertutupan, petugas TI yang

minim pengalamanan, dan keterbukaan dokumentasi dari vendor yang sebelumnya telah menjalin kerjasama dengan Kemenepora dalam pengembangan sistem, kesemuanya itu harus segera diminimalisasi dan diselesaikan dengan segera dan menyeluruh. Keamanan informasi di lingkungan Kemenpora harus mencapai level yang tertinggi sesuai dengan kebutuhan dan kemampuan yang miliki olehnya.

Level keamanan informasi yang maksimal di lingkungan Kemenpora baik di tingkat pusat dan daerah diharapkan dapat menjadi motivasi bagi perkembangan Kemenpora ke depan. Hal ini diharapkan secara tidak langsung dapat menjadi tolak ukur atau cerminan bagi instansi lainnya di pemerintahan.

Bibliography

[1] *IT Security Guidelines. Section 114 IT Security Management and IT-Grundschutz* . Federal Office for Information Security. 2007.

[2] Security Risk Assessment & Audit Guidelines [G51] Version: 4.0. The Government of the Hong Kong Special Administrative Region. December 2009.

[3] *Information Technology Security Evaluation Criteria (ITSEC).* Department of Trade and Industry, London, Juni 1991.

[4] *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*. Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika RI. Edisi: 2.0,September 2011.

[5] Bel G. Raggad dan Emilio Collar, Jr. The Simple Information Security Audit Process: SISAP. *IJCSNS International Journal of Computer Science and Network Securit*y, VOL.6 No.6, June 2006.

[6] *Information Technology Security Evaluation Manual (ITSEM) Version 1.0*. COMMISSION OF THE EUROPEAN COMMUNITIES. ECSC-EEC-EAEC,Brussels - Luxembourg 1992, 1993.

[7] *BSI-Standard 100-1: Information Security Management System (ISMS)*. Version 1.5. 2008. `http://www.bsi.bund.de/grundschutz`.

[8] B*SI-Standard 100-2: IT-Grundschutz Methodology*. Version 2.0. 2008. `http://www.bsi.bund.de/grundschutz`.

[9] *BSI-Standard 100-3: Risk analysis based on IT-Grundschutz.* Version 2.5. 2008. `http://www.bsi.bund.de/grundschutz`

[10] *BSI-Standard 100-2: Business Continuity Management*. Version 1.0. 2009. `http://www.bsi.bund.de/grundschutz`.

[11] *CISA (Certified Information System Auditor): CISA Review Questions, Answers & Explanations Manual 2006*. Information Systems Audit and Control Association 2005.

[12] *CISA: Chapter 3: System and Infrastructure Life Cycle Management*. CISA Review Manual 2008.

[13] *CISA: Chapter 5: Protection of Information Assets*. CISA Review Manual 2008.

[14] *CISA: Chapter 6: IT Service Delivery and Support*. CISA Review Manual 2008.

[15] Abadi, Martin (1997). Secrecy by typing in security protocols. *Theoretical Aspects of Computer Software, third International Symposiumm TACS 97*. hlm. 611 - 637.

[16] Abadi, Martin, Roger Needham (1996). Prudent engineering practice for Cryptographic Protocols. *IEEE Transactions on Software Engineering*, vol 22 (1), Januari 1996, hlm. 6 - 15.

[17] Adams, Anne dan Martina Angela Sasse (1999). Users are not the enemy. *Communication of the ACM* . Desember 1999, vol 42 (12), 41-45.

[18] Butler, Randy, Von Welch, Douglas Engert, Ian Foster, Steven Tuecke, John Volmer, Carl Kesselman (2000). A national scale authentication infrastructure. *IEEE Computer* , Desember 2000, 60-64.

[19] Cybenko, George, Guofei Jiang (2000). Developing a distributed system for infrastructure protection. *IT Pro* , July/Agustus 1999 hlm. 17 - 22.

[20] Edwards, John (2001). Next-generation viruses present new chanllenges, IEEE Computer, May 2001, hlm. 16-18.

[21] Feiertag, Richard J, Peter G Neumann (1979). *The Foundation of Provable Secure System*.

[22] Felten, Edward W, Dirk Balfans, Drew Dean, Dan S Wallach (1997). Web Spoofing : An Internet Con Came. Technical Report 540-96. Department of Computer Science, Princeton University

[23] Gollmann, Dieter (1999). *Computer Security*. England : John Willey & Sons Inc.

[24] Gutzmann, Kurt (2001). Access Control and Session Management in the HTTP Environment. *IEEE Internet Computing*, January-February 2001, hlm 26-35.

[25] Heintze, Nevin, J. D. Tyger (1996). A model for secure protocols and their compositions. *IEEE Transactions on Software Engineering*, vol 22 (1), Januari 1996. hlm. 16 - 30.

[26] James B.D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford (2001). Security Models for Web-Based Applications. *Communications of the ACM*, February 2001/Vol. 44. No 2, page 38-44.

[27] James B.D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford (2001). Digital Government Security Infrastructure Design Challenges. I*EEE Computer*, February 2001, hlm 66-72.

[28] Joshi, Ghafoor, Aref, Spafford, "Digital Government Security Infrastructure Design Challenges"

[29] Michener, John (1999). System Insecurity in the Internet Age. *IEEE Software* , July/August 1999, 62-68.

[30] Ronald, Edmund M.A, Moshe Sipper (2000). The challenge of tamperproof Internet Computing. *IEEE Computer*. Oktober 2000, hlm 98-99.

[31] Schneier, Bruce (2008). *Applied Cryptography*. Canada : John Willey & Sons Inc.

[32] Schneier, Bruce (2000). Semantic Network Attacks. *Communications of the ACM* vol 43(12), Desember 200.

[33] Schneier, Bruce (2000). *Secrets & Lies*. USA : John Willey and Sons.

[34] Simon Liu, John Sullivan, Jerry Ormaner. A Practical Approach to Enterprise IT Security. *IT Pro*, September-Oktobe 2001, 35-42.

[35] White House (2000). *National Plan for Information System Protection ver 1.0*

[36] Zwicky, Elizabeth D, Simon Cooper, D. Brent Chapman (2000). *Building Internet Firewall*. OReilly and Associates

Lampiran

Lembar Kuesioner

Nama : .....
Jabatan : .....
Tanggal : .....

A. **Kebijakan Keamanan**

- ☐ Kebijakan keamanan telah didokumentasikan dengan baik dan mudah dimengerti.
- ☐ Mudah diakses oleh seluruh pihak yang terlibat.
- ☐ Semua peran dan tanggung jawab yang jelas telah didefiniskan.
- ☐ Kebijakan keamanan diperiksa dan diperbarharui.
- ☐ Pengguna informasi dan berkomitmen untuk kebijakan **
- ☐ Pelatihan keamanan yang diberikan telah cukup bagi pihak terkait.
- ☐ Semua aturan yang tercantum dalam kebijakan telah diimplementasikan.

B. **Keamanan Fisik**

1. **Ruang Komputer/ Server**

- ☐ Terdapat standar keamanan yang digunakan pada ruang komputer.
- ☐ Lingkungan fisik memenuhi persyaratan yang ditentukan dalam departemen TI kebijakan keamanan, Peraturan Keamanan dan standar terkait lainnya.
- ☐ Keseluruhan kabel dipasang secara rapih dan diberi label untuk membantu pemeliharaan dan pendeteksian kesalahan.
- ☐ Semua ruang di bawah lantai, dibersihkan secara teratur.
- ☐ Langit-langit dibersihkan secara teratur untuk menghindari debu dan kotor.
- ☐ Pendeteksi air dipasang di bawah lantai untuk mendeteksi banjir.
- ☐ Kabel di langit-langit terpasang dengan benar.
- ☐ UPS dipasang untuk keperluan perlengkapan.
- ☐ UPS mampu menyediakan pasokan tenaga selama waktu tertentu.
- ☐ UPS diperiksa secara teratur.
- ☐ UPS ditempatkan di tempat yang aman.
- ☐ Operator yang berada di ruang komputer/ server selalu diberi pelatihan dalam mengontrol power supply.
- ☐ Tidak meninggalkan peralatan / bahan yang mudah terbakar di ruang komputer/ server

- □ Seluruh sistem pendeteksi api otomatis dioperasikan dengan pemeriksaan secara teratur
- □ Seluruh sistem pemadam kebakaran otomatis yang telah terpasang diperiksa secara teratur dan selalu berkondisi baik
- □ Seluruh pipa air yang melewati ruangan atau bawah lantai berada dalam kondisi yang baik.
- □ Suhu dan kelembaban ruangan dimonitor dan diatur dengan cara yang sesuai untuk peralatan komputer untuk dioperasikan pada kondisi yang baik.
- □ Seluruh kunci pintu ruang komputer disimpan dengan benar.
- □ Terdapat prosedur dalam menangani dan mendistribusikan kunci.
- □ Seluruh personil dilatih dan diinformasikan mengenai mekanisme penggunaan pemadam kebakaran dan peralatan pelindung lainnya.
- □ Makanan, minuman, merokok tidak diijinkan masuk ke ruang komputer/ server.
- □ Notebook, komputer, dan peralatan komputer lainnya yang dibawa ke ruang komputer dikontrol.
- □ Terdapat staf khusus yang ditugaskan untuk bertanggung jawab mengatur kebersihan ruang komputer.

2. **Daftar Komputer/ Media Penyimpanan**

- □ Seluruh media cadangan diberi nama dan dikunci di tempat yang aman.
- □ Tempat atau lemari penyimpanan media cadangan selalu di kunci.
- □ Terdapat kontrol transportasi yang tepat untuk penyimpanan.
- □ Pengaksesan media dikontrol dan dicatat secara teratur.
- □ Inventarisasi disimpan untuk semua media penyimpanan.
- □ Peralatan komputer diadakan di ruang komputer hanya cukup untuk operasi.
- □ Semua alat tulis komputer mahal benar dijaga dan dikendalikan.
- □ Ada prosedur untuk mengeluarkan, otorisasi dan pencatatan alat tulis komputer mahal.
- □ Sebuah persediaan yang tepat disimpan untuk semua peralatan komputer.
- □ Contoh fisik memeriksa peralatan komputer terhadap catatan persediaan benar.

3. **Akses Kontrol Media Fisik**

- □ Seluruh pengunjung harus diidentifikasi sebelum memasuki ruang komputer.

- □ Seluruh pengunjung harus didampingi dengan internal staf setiap waktu.
- □ Seluruh pengunjung disediakan tanda pengenal pengunjung ketika masuk ke ruang komputer/ server.
- □ Seluruh staf yang datang harus dicatat.
- □ Terdapat pengontrol batasan yang dapat masuk ke ruang komputer.
- □ Seluruh tempat masuk ruang komputer dikontrol dengan pintu berkunci.
- □ Hanya staf yang diberi kuasa yang dapat masuk ke ruang komputer.
- □ Seluruh panduan dan dokumen tidak disimpan secara bebas melainkan terdapat akses kontrol untuk memperolehnya.

C. **Backup dan Recovery**

- □ Terdapat prosedur yang dibangun dan didokumentasikan untuk backup dan recovery.
- □ Log selalu disimpan untuk kebutuhan backup dan recovery meliputi tanggal/ waktu, media yang digunakan untuk backup, siapa yang mengambil, dll.
- □ Minimum terdapat 2 backup yang berada di satu tempat.
- □ Ada periode retensi yang didefinisikan dengan baik untuk backup.

D. **Pengaturan Perubahan**

- □ Prosedur pengaturan perubahan didokumentasikan dengan baik
- □ Evaluasi dan perkiraan dibuat berdasarkan efek dari permintaan perubahan
- □ Seluruh perubahan disetujui, disimpan dan diuji terlebih dahulu sebelum diimplementasi.
- □ Dilakukan backup yang memadai sebelum dan setelah perubahan.
- □ Prosedur perbaikan didefinisikan terlebih dahulu sebelum terjadi perubahan.
- □ Terdapat kontrol yang menjamin tidak adanya data/program pengujian yang tertinggal di lingkungan produksi.
- □ Setelah menerapkan di lingkungan produksi, verifikasi dibuat untuk memastikan bahwa itu dilaksanakan seperti yang diinginkan dan direncanakan.
- □ Terdapat hak akses yang tepat yang mengijinkan hanya staf dan administror untuk mengubah konfigurasi sistem/ jaringan.

E. **Logical Access Control**

1. Kebijakan Sandi

- □ Kebijakan sandi sistem/ jaringan didokumentasikan dengan baik.
- □ Panjang sandi paling sedikit 6 karakter
- □ Sandi tidak ditampilkan dalam plain text selama dimasukkan.
- □ Sandi hanya diketahui oleh pemiliknya atau administrator ketika pertama kali membuat.
- □ Terdapat masa kadaluarsa sandi.
- □ Maksimum 3 kali mencoba mengisi sandi.
- □ Tidak ada kamus kata, nama pengguna, atau fase yang jelas yang ditemukan pada isi sandi.
- □ Pengguna mengubah sandi segera ketka akun baru mereka dibuat.
- □ Pengguna tidak menulis sandinya di label atau di tempat yang jelas.
- □ Pengguna merubah sandinya paling sedikit setiap 60 - 90 hari.

2. **Kebijakan Akun Pengguna**

- □ Setiap user diberikan identitas pengguna yang unik.
- □ Semua pengguna diberikan dengan hak akses minimum yang cukup untuk menjalankan tugas mereka.
- □ Pengguna diinformasikan mengenai hak istimewa dan hak asksesnya.
- □ Ada prosedur yang tepat dan aman untuk distribusi akun pengguna dan sandi. Sandi ditulis di kertas dianggap sebagai informasi rahasia.
- □ Log disimpan selama aktivitas pengguna seperti waktu log in/ out, periode koneksi, sambungan koneksi, dll.
- □ Tidak ditemukannya akun yang tidak terpakai pada sistem/ jaringan.
- □ Administrator juga memiliki akun pengguna.
- □ Akun administrator digunahan hanya untuk pekerjaan administrasi.
- □ Pengguna dibagi kedalam kategori yang berbeda dengan pendefinisian hak istimewa yang jelas bagi setiap kategorinya.

F. Keamanan Jaringan

- □ Jaringan yang terhubung dengan internet dilindungi oleh Firewall.
- □ Semua akses ke jaringan internal dikontrol dengan autentikasi dan log.
- □ Administrasi untuk jaringan komputer dilakukan hanya oleh staf.
- □ Kontrol diletakkan pada penggunaan sumber daya jaringan seperti file sharing, percetakan dll untuk hanya memperbolehkan dan mengkonfirmasi pengguna untuk menggunakan.
- □ Upgrade pada perangkat lunak yang terletak dalam jaringan dilakukan oleh orang yang berwenang saja.

- □ Kebijakan ditetapkan untuk mengontrol penggunaan yang tepat dari jaringan dan sumber dayanya.
- □ Terdapat perlindungan keamanan (misal enkripsi) bagi informasi yang akan dikirim.
- □ Log harian misalnya sistem log, error log atau log aktivitas pengguna selalu ditinjau dan dianalisis.
- □ Seseorang ditugaskan untuk memantau kinerja jaringan dan operasi sehari-hari.
- □ Profil jaringan pengguna Semua benar dilindungi dari akses yang tidak sah.
- □ Konfigurasi jaringan didokumentasikan dan dimasukkan ke tempat yang aman.
- □ Komponen jaringan ditempatkan di tempat yang aman.

G. Sistem Operasi

- □ Update dilakukan secara teratur pada sistem operasi untuk memperbaiki kelemahan yang diketahui mereka.
- □ Terdapat kontrol pada perubahan konfigurasi sistem operasi.
- □ Akses ke utilitas sistem operasi dibatasi untuk orang yang berwenang saja.
- □ Tidak ada layanan yang tidak digunakan/ mencurigakan yang berjalan di akun sistem operasi.
- □ Tidak ada akun pengguna yang tidak terpakai yang tetap dalam sistem operasi.
- □ Log sistem dihasilkan dan diperiksa setiap hari secara teratur.