POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.09/1.1/8914/2019
	TANGGAL PEMBUATAN	9 Desember 2019
	TANGGAL REVISI	
	TANGGAL EFEKTIF	
	DISAHKAN OLEH	Direktur Satino, SKM., MScN NIP. 196101021989031001

PEDOMAN TEKNIK
PENGENDALIAN DAN PENGELOLAAN SISTEM INFORMASI DI LINGKUNGAN POLITEKNIK KESEHATAN SURAKARTA

Pedoman Teknis
Pengendalian dan
Pengelolaan Sistem informasi
di Lingkungan Poltekkes Surakarta

KATA PENGANTAR

Pembinaan penyelenggaraan Sistem Pengendalian Intern Pemerintah (SPIP) merupakan tanggung jawab semua institusi sesuai dengan pasal 59 Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah. Pembinaan ini merupakan salah satu cara untuk memperkuat dan menunjang efektivitas sistem pengendalian intern, di lingkungan masing-masing.

Pembinaan penyelenggaraan SPIP yang menjadi tugas dan tanggung jawab tersebut meliputi: diarahkan dalam rangka penerapan unsur-unsur SPIP, yaitu:

1. lingkungan pengendalian;
2. penilaian risiko;
3. kegiatan pengendalian;
4. informasi dan komunikasi; dan
5. pemantauan pengendalian intern.

Untuk memenuhi kebutuhan pedoman penyelenggaraan SPIP, telah menyusun Pedoman Teknis Umum Penyelenggaraan SPIP. Pedoman tersebut merupakan pedoman tentang hal-hal apa saja yang perlu dibangun dan dilaksanakan dalam rangka penyelenggaraan SPIP. Selanjutnya, pedoman tersebut dijabarkan ke dalam pedoman teknis penyelenggaraan masing-masing subunsur pengendalian. Pedoman teknis subunsur ini merupakan acuan langkah-langkah yang perlu dilaksanakan dalam penyelenggaraan subunsur SPIP.

Pedoman Teknis Penyelenggaraan SPIP sub unsur Pengendalian atas Pengelolaan Sistem Informasi pada unsur Kegiatan Pengendalian merupakan acuan yang memberikan arah bagi instansi pemerintah pusat dan daerah dalam menyelenggarakan subunsur tersebut, dan dapat disesuaikan dengan karakteristik masing-masing instansi, yang meliputi fungsi, sifat, tujuan, dan kompleksitas instansi tersebut.

Pedoman ini masih jauh dari sempurna. Oleh karena itu, masukan dan saran perbaikan dari pengguna pedoman ini, sangat diharapkan sebagai bahan penyempurnaan.

Surakarta , Oktober 2019

DAFTAR ISI

Halaman

BAB I
PENDAHULUAN

A. Latar Belakang

Kegiatan pengendalian dalam sistem pengendalian intern pemerintah (SPIP), salah satunya adalah subunsur pengendalian atas pengelolaan sistem informasi. Pimpinan instansi pemerintah wajib memiliki kegiatan pengendalian atas pengelolaan sistem informasi dilakukan untuk memastikan akurasi dan kelengkapan informasi, yang sangat menunjang penyajian laporan keuangan yang andal.

Kegiatan pengendalian atas pengelolaan sistem informasi meliputi pengendalian umum dan pengendalian aplikasi. Pengendalian umum terkait dengan lingkungan pengelolaan sistem informasi, sedangkan pengendalian aplikasi memastikan bahwa *input* telah lengkap dan diperoleh dari sumber yang valid, sistem yang memproses *input* dapat diandalkan, dan *output* yang dihasilkan dapat diuji kebenarannya.

Pedoman ini dimaksudkan untuk memberikan panduan maupun acuan dalam memahami dan melakukan kegiatan pengendalian pengelolaan atas sistem informasi. Pedoman ini merupakan penjabaran lebih lanjut dari pedoman teknis penyelenggaraan SPIP.

B. Sistematika Pedoman

Sistematika penyajian pedoman ini adalah sebagai berikut:

BAB I Pendahuluan

Bab ini berisi uraian mengenai alasan perlunya disusun pedoman, hubungan dengan pedoman sebelumnya, dan sistematika isi pedoman.

BAB II Gambaran Umum

Bab ini berisi uraian mengenai pengertian, tujuan dan manfaat pengendalian atas pengelolaan sistem informasi, peraturan per-undang-undangan terkait, serta parameter penerapan dilakukannya pengendalian atas pengelolaan sistem informasi.

BAB III Langkah-Langkah Penyelenggaraan

Bab ini menguraikan mengenai langkah-langkah yang perlu dilaksanakan dalam menerapkan subunsur Pengendalian atas Pengelolaan Sistem Informasi, yang terdiri dari langkah persiapan, pelaksanaan, dan pelaporan.

BAB IV Penutup

Penutup berisikan hal-hal penting yang perlu diperhatikan kembali dan penjelasan atas penggunaan pedoman ini.

BAB II
GAMBARAN UMUM

A. Pengertian

Kegiatan pengendalian merupakan suatu tindakan yang diperlukan untuk mengatasi risiko, penetapan, serta pelaksanaan kebijakan dan prosedur untuk memastikan bahwa tindakan mengatasi risiko telah dilaksanakan secara efektif. Kegiatan pengendalian dirancang dan dikembangkan berdasarkan hasil penilaian risiko yang telah dilakukan.

Sistem informasi diperlukan untuk mendukung pelaksanaan kegiatan tugas dan fungsi instansi pemerintah, serta untuk pemrosesan data akuntansi dan kinerja. Akurasi dan ketepatan waktu pengambilan keputusan pimpinan instansi pemerintah dapat ditingkatkan dengan bantuan teknologi komputer. Oleh karena itu, sistem informasi yang dikembangkan instansi pemerintah idealnya berbasis teknologi komputer.

Jenis dan kompleksitas sistem informasi yang dijalankan di instansi pemerintah berbeda-beda dan dapat dikelompokkan menjadi sistem informasi yang sederhana dan sistem informasi yang canggih. Dalam kelompok pertama, termasuk penggunaan sistem informasi yang bersifat manual dan penggunaan komputer yang berdiri sendiri, dengan aplikasi yang sederhana. Dalam kelompok kedua, termasuk sistem informasi berbasis komputer, menggunakan jaringan *Local Area Network* (LAN) dan/atau *Wide Area Network* (WAN), dengan penggunaan aplikasi-aplikasi dalam jumlah yang relatif besar dan kompleks.

Penerapan sistem informasi di suatu instansi pemerintah, dipengaruhi pula oleh sifat khusus instansi pemerintah. Instansi pemerintah yang kegiatan utamanya sangat bergantung pada informasi yang cepat dan akurat akan menjadikan sistem informasi sebagai bagian dari kegiatan penting, sedangkan instansi pemerintah yang kegiatan utamanya tidak bergantung pada sistem informasi akan menjadikan sistem informasi sebagai kegiatan pendukung.

Pengelolaan sistem informasi berbasis teknologi komputer memiliki risiko, antara lain:

1. *Garbage in Garbage out* (GIGO)

   Akurasi *output* yang dihasilkan sangat bergantung pada akurasi *input* dan ketepatan aplikasi yang memroses *input* tersebut. Hal ini merupakan konsekuensi dari prinsip *garbage in garbage out* (GIGO). Kesalahan *input* secara otomatis akan menghasilkan *output* yang salah pula.

2. Jejak transaksi

   Beberapa sistem komputer dirancang sedemikian rupa sehingga jejak transaksi yang lengkap hanya ada dalam jangka waktu yang pendek, atau dalam bentuk yang hanya dapat dibaca dengan komputer.

3. Pemrosesan transaksi secara seragam

   Dengan instruksi pemrosesan yang sama, maka komputer akan meminimalisasi kesalahan klerikal. Namun, apabila aplikasi program komputer ataupun perangkat keras yang digunakan tidak tepat, maka akan menghasilkan *output* yang salah, yang kemungkinan akan terjadi dalam cakupan *(magnitude)* yang besar.

4. Inisiasi atau pengerjaan selanjutnya oleh komputer

   Transaksi tertentu secara otomatis akan diinisiasi oleh sistem komputer atau prosedur tertentu yang diperlukan untuk melaksanakan transaksi secara otomatis dapat dilakukan oleh sistem komputer. Otorisasi manajemen atas transaksi tersebut mungkin dilakukan secara implisit melekat dalam desain sistem komputer.

5. Potensi kesalahan dan penyimpangan

   Pegawai memiliki potensi untuk dapat mengakses data atau mengubah data, tanpa meninggalkan bukti fisik yang kasat mata. Berkurangnya keterlibatan manusia dalam menangani transaksi dapat mengurangi pengamatan atas kesalahan dan penyimpangan. Kesalahan dan penyimpangan yang terjadi selama perancangan atau perubahan program aplikasi, bisa jadi tidak dapat terdeteksi dalam jangka waktu yang lama.

Pimpinan instansi pemerintah harus mengembangkan rencana pengamanan sistem informasi dan membangun kesadaran seluruh pegawai bahwa pengamanan sistem informasi adalah tanggung jawab bersama, bukan hanya tanggung jawab unit kerja atau pejabat yang bertugas mengembangkan program dan pengamanan sistem informasi saja.

Kegiatan pengendalian atas pengelolaan sistem informasi, dilakukan untuk memastikan akurasi dan kelengkapan informasi, yang meliputi pengendalian umum dan pengendalian aplikasi.

1. Pengendalian Umum

Pengendalian umum meliputi struktur, kebijakan, dan prosedur yang berlaku terhadap seluruh operasional sistem komputer instansi pemerintah. Pengendalian umum berkaitan dengan seluruh aktivitas komputer, seperti yang terkait dengan rencana instansi pemerintah atas aktivitas pemrosesan data dan pemisahan fungsi.

Kegiatan pengendalian umum meliputi:

a. Pengamanan sistem informasi;
b. Pengendalian atas akses;
c. Pengendalian atas pengembangan dan perubahan perangkat lunak aplikasi;
d. Pengendalian atas perangkat lunak sistem;
e. Pemisahan tugas;
f. Kontinuitas pelayanan;

a. Pengamanan Sistem Informasi

Pengendalian intern yang baik atas sistem informasi mensyaratkan adanya upaya yang dilakukan untuk memproteksi *file* dan program dari pengungkapan yang tidak diotorisasi, dan dari kerusakan/kehancuran yang diakibatkan oleh kecelakaan. Instansi pemerintah harus mengidentifikasi semua kemungkinan ancaman atau bahaya terhadap peralatan dan operasi pemrosesan data.

Pengamanan sistem informasi sekurang-kurangnya mencakup kegiatan:

1) Pelaksanaan penilaian risiko secara periodik yang komprehensif.
2) Pengembangan rencana yang secara jelas menggambarkan program pengamanan, serta kebijakan dan prosedur yang mendukungnya.
3) Penetapan organisasi untuk mengimplementasikan dan mengelola program pengamanan.
4) Penguraian tanggung jawab pengamanan secara jelas.
5) Implementasi kebijakan yang efektif atas sumber daya manusia terkait dengan program pengamanan.
6) Pemantauan efektivitas program pengamanan dan melakukan perubahan program pengamanan jika diperlukan.
7) Lokasi penyimpanan yang aman.
8) Rencana pemulihan setelah bencana (*disaster recovery plan*).

b. Pengendalian atas Akses

Instansi pemerintah harus melakukan pengendalian atas akses terhadap sistem komputer untuk mencegah penyalahgunaan sistem informasi dan menjaga keamanan *hardware, software,* maupun perangkat terkait lainnya dari penggunaan yang tidak sah. Hanya orang- orang tertentu yang diotorisasi, yang dapat masuk ke dalam lingkungan sistem informasi dan melakukan akses terhadap sistem.

Pengendalian atas akses, sekurang-kurangnya mencakup kegiatan:

1) Mengklasifikasikan sumber daya sistem informasi berdasarkan kepentingan dan sensitivitasnya.

2) Mengidentifikasi pengguna yang berhak dan otorisasi akses ke informasi dengan pengendalian logis, untuk mencegah dan mendeteksi akses yang tidak diotorisasi.

3) Pemantauan atas akses ke sistem informasi, investigasi atas pelanggaran, serta tindakan perbaikan dan penegakan disiplin.

Pengendalian keamanan fisik *(physical security control)* adalah pembatasan akses terhadap sumber daya informasi secara fisik, misalnya dengan memakai kartu akses ruangan untuk memasuki suatu ruangan penyimpanan komputer.

Pengendalian kemanan logis *(logical security control)* adalah pembatasan akses terhadap sumber daya informasi dengan menggunakan logika komputer, misalnya melalui penggunaan kode akses (*password*) untuk memasuki suatu sistem jaringan komunikasi.

C. Pengendalian atas Pengembangan dan Perubahan Perangkat Lunak Aplikasi

Instansi pemerintah harus mengendalikan pengembangan dan perubahan perangkat lunak aplikasi, sekurang- kurangnya mencakup kegiatan:

1) Otorisasi atas fitur pemrosesan sistem informasi dan modifikasi program.
2) Pengujian dan persetujuan atas seluruh perangkat lunak yang baru dan yang dimutakhirkan.
3) Penetapan prosedur untuk memastikan terselenggaranya pengendalian atas kepustakaan perangkat lunak.

Prosedur untuk memastikan terselenggaranya pengendalian atas kepustakaan perangkat lunak (*software libraries*), termasuk di dalamnya adalah pemberian label, pembatasan akses, dan penggunaan kepustakaan perangkat lunak yang terpisah.

d. Pengendalian atas Perangkat Lunak Sistem Pengendalian atas perangkat lunak sistem, sekurang- kurangnya mencakup kegiatan:

1) Pembatasan akses ke perangkat lunak sistem berdasarkan tanggung jawab pekerjaan dan dokumentasi atas otorisasi akses.
2) Pengendalian dan pemantauan atas akses dan penggunaan perangkat lunak sistem.
3) Pengendalian atas perubahan yang dilakukan terhadap perangkat lunak sistem.

e. Pemisahan Tugas

Dalam sistem informasi berbasis komputer, prosedur yang dilakukan oleh pegawai yang berbeda dalam sistem informasi manual mungkin akan digabung ke dalam fungsi pemrosesan yang ada di komputer. Oleh karena itu, pegawai yang memiliki akses ke komputer akan mempunyai kesempatan yang besar untuk melakukan kecurangan.

Pemisahan tugas, mensyaratkan bahwa kewenangan dan tanggung jawab dalam pengelolaan sistem informasi harus secara jelas dibagi ke dalam beberapa fungsi berikut: (1) sistem analis aplikasi dan programer, (2) operator komputer, (3) programer sistem, (4) otorisasi transaksi, (5) pemelihara *file* perpustakaan sistem, dan
(6) pengendali data.

Pengendalian pemisahan tugas sekurang-kurangnya mencakup kegiatan:

1) Identifikasi tugas yang tidak dapat digabungkan dan penetapan kebijakan untuk memisahkan tugas tersebut.
2) Penetapan pengendalian akses untuk pelaksanaan pemisahan tugas.
3) Pengendalian atas kegiatan pegawai, melalui penggunaan prosedur, supervisi, dan reviu.

f. Kontinuitas Pelayanan

Instansi pemerintah harus memiliki rencana untuk kejadian tidak terduga *(contingency plan),* seperti langkah pengamanan apabila terjadi kebakaran, sabotase, bencana alam (seperti gempa bumi dan banjir), dan terorisme, untuk menjaga agar kegiatan pelayanan instansi tidak terganggu.

Rencana tersebut sebaiknya memuat hal-hal seperti:

- struktur organisasi;
- tugas dan tanggung jawab semua pihak yang terkait dengan sistem informasi;
- struktur dokumentasi;
- uji coba dan pelaksanaan rencana;

- identifikasi sumber daya penting;
- pemantauan dan pelaporan atas ketersediaan sumber daya penting tersebut;
- prosedur alternatif dan prinsip *back-up* dan pemulihan data.

Kegiatan untuk menjaga kontinuitas pelayanan, sekurang- kurangnya mencakup:

1) Penilaian, pemberian prioritas, dan pengidentifikasian sumber daya pendukung atas kegiatan komputerisasi yang kritis dan sensitif.
2) Pencegahan dan peminimalisasian potensi kerusakan dan terhentinya operasi komputer.
3) Pengembangan dan pendokumentasian rencana komprehensif untuk mengatasi kejadian tidak terduga.
4) Pengujian secara berkala atas rencana untuk mengatasi kejadian tidak terduga dan melakukan penyesuaian, jika diperlukan.

Contoh langkah pencegahan dan peminimalisasian potensi kerusakan dan terhentinya operasi komputer, antara lain melalui penggunaan prosedur *back-up* data dan program, penyimpanan *back-up* data di tempat lain, pengendalian atas lingkungan, pelatihan staf, serta pengelolaan dan pemeliharaan perangkat keras.

2. Pengendalian Aplikasi

Pengendalian aplikasi, meliputi struktur, kebijakan, dan prosedur yang dirancang untuk membantu memastikan kelengkapan, keakuratan, otorisasi, serta keabsahan semua transaksi selama pemrosesan aplikasi.

Pengendalian aplikasi berkaitan dengan pekerjaan pemrosesan tertentu yang dilakukan pada fasilitas komputer, yang berhubungan dengan *input* data, *file*, program, dan *output* aplikasi komputer tertentu, bukan sistem komputer secara umum. Tujuan utama pengendalian aplikasi adalah untuk menjaga keakuratan *output* sistem, *file* data, dan catatan-catatan transaksi/kejadian.

Pengendalian aplikasi terdiri atas:

a. Pengendalian otorisasi;
b. Pengendalian kelengkapan;
c. Pengendalian akurasi; serta
d. Pengendalian terhadap keandalan pemrosesan dan *file* data.

a. Pengendalian otorisasi

Pengendalian otorisasi sekurang-kurangnya mencakup:

1) Pengendalian terhadap dokumen sumber;
2) Pengesahan atas dokumen sumber;
3) Pembatasan akses ke terminal entri data; dan
4) Penggunaan *file* induk dan laporan khusus untuk memastikan bahwa seluruh data yang diproses telah diotorisasi.

Laporan khusus sebagaimana dinyatakan dalam butir 4) di atas adalah laporan yang mengungkapkan hal- hal yang tidak normal, seperti rekening piutang karyawan yang bersaldo kredit dan tanggal surat keputusan suatu permohonan yang mendahului tanggal surat permohonannya.

b. Pengendalian kelengkapan

Pengendalian kelengkapan, dirancang untuk mengatasi risiko tidak lengkapnya laporan yang dihasilkan oleh sistem informasi, karena tidak semua data telah dientri ke dalam sistem informasi.

Pengendalian kelengkapan, sekurang-kurangnya mencakup:

1) Pengentrian dan pemrosesan seluruh transaksi yang telah diotorisasi ke dalam komputer; dan
2) Pelaksanaan rekonsiliasi data untuk memverifikasi kelengkapan data.

c. Pengendalian akurasi

Pengendalian akurasi dirancang untuk mengatasi risiko kesalahan pada *output* (laporan) yang dihasilkan sistem informasi (tidak akurat), karena kesalahan (ketidakakuratan) data yang dientri.

Pengendalian akurasi, sekurang-kurangnya mencakup:

1) Penggunaan desain entri data untuk mendukung akurasi data.
2) Pelaksanaan validasi data untuk mengidentifikasi data yang salah.
3) Pencatatan, pelaporan, investigasi, dan perbaikan data yang salah dengan segera.
4) Reviu atas laporan keluaran untuk mempertahankan akurasi dan validitas data.

Dalam merancang entri data agar diperhatikan fitur yang mendukung akurasi data. Misalnya, untuk tipe/jenis *field* (kolom) yang sudah terstandarisasi, seperti unit organisasi, pengentrian dilakukan dengan memasukkan nomor kode organisasi dan komputer secara otomatis akan menampilkan nama unit organisasi.

Pelaksanaan validasi data dapat dilakukan melalui suatu program (disebut *program edit*), yang menggunakan komputer untuk mengecek validitas dan akurasi entri data sebelum data diproses.

Pengendalian (berupa reviu) atas laporan keluaran, dilakukan oleh pegawai yang mengendalikan data dan oleh pemakai laporan keluaran. Pegawai dimaksud harus mereviu kewajaran dan kelayakan seluruh keluaran dan harus melakukan rekonsiliasi terhadap total keluaran dengan total *input* yang berkaitan.

d. Pengendalian terhadap keandalan pemrosesan dan *file* data

Pengendalian terhadap keandalan pemrosesan dan *file* data, sekurang-kurangnya mencakup:

1) Penggunaan prosedur yang memastikan bahwa hanya program dan *file* data versi terkini yang digunakan selama pemrosesan.
2) Penggunaan program yang memiliki prosedur untuk memverifikasi kesesuaian versi *file* komputer yang digunakan selama pemrosesan.

3) Penggunaan program yang memiliki prosedur untuk mengecek *internal file header labels* sebelum pemrosesan.

4) Penggunaan aplikasi yang mencegah perubahan *file* secara bersamaan.

Kebijakan dan prosedur pengendalian terhadap pengelolaan sistem informasi harus dibuat secara tertulis dan diinformasikan kepada seluruh pegawai. Dalam mengembangkan aktivitas pengendalian atas pengelolaan sistem informasi, instansi pemerintah harus tetap memertimbangkan prinsip biaya manfaat *(cost and benefit)*. Dengan prinsip ini, aktivitas pengendalian yang dibangun seharusnya memberikan manfaat yang lebih besar dibandingkan dengan biaya yang dikeluarkan.

Bagi instansi pemerintah yang belum memiliki sistem informasi berbasis teknologi komputer, aktivitas pengendalian atas pengelolaan sistem informasi, setidak-tidaknya meliputi:

1. Pengecekan ulang atas data masukan (dokumen sumber);
2. Pencatatan dilaksanakan dalam nomor yang berurutan;
3. Penyimpangan (pengecualian dan pelanggaran) yang diindikasikan dari kegiatan pengendalian lainnya (seperti hasil audit intern atau ekstern) harus diuji dan ditindaklanjuti dengan segera;
4. Akses ke data dan *file* dikendalikan dengan cara tertentu, seperti penggunaan *password.*

B. Tujuan dan Manfaat

Pedoman teknis ini bertujuan untuk memberikan arahan bagi pimpinan instansi pemerintah yang akan mengembangkan kegiatan pengendalian atas pengelolaan sistem informasi. Dengan mendasarkan pada pedoman teknis ini, maka kegiatan pengendalian yang disusun diharapkan sesuai dengan yang digariskan dalam PP Nomor 60 Tahun 2008, sehingga sistem informasi yang diimplementasikan dapat mendukung pencapaian tujuan organisasi.

Tujuan pengendalian atas pengelolaan sistem informasi adalah:

1. Meningkatkan akurasi *input*, proses, dan *output* dari pengelolaan sistem informasi;
2. Meningkatkan pengamanan data;
3. Menekan risiko kesalahan pengelolaan sistem informasi.

Jika pengendalian atas sistem informasi dilakukan secara memadai, maka instansi pemerintah akan memeroleh manfaat sebagai berikut:

1. peningkatan kualitas pengambilan keputusan;
2. produktivitas kinerja operasional dan keuangan; dan
3. tercapainya tujuan pengendalian.

C. Peraturan Perundang-undangan Terkait

Peraturan tentang pengendalian atas pengelolaan sistem informasi yang dapat dijadikan acuan antara lain:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

3. Peraturan Presiden Nomor 42 Tahun 2005 tentang Komite Kebijakan Percepatan Penyediaan Infrastruktur.
4. Keputusan Presiden Nomor 9 Tahun 2003 tentang Tim Koordinasi Telematika Indonesia.
5. Instruksi Presiden Nomor 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan *E-government*.
6. Instruksi Presiden Nomor 6 Tahun 2001 tentang Pengembangan dan Pendayagunaan Telematika di Indonesia.
7. Peraturan dari Departemen Komunikasi dan Informasi:
   a. Panduan Pembangunan Infrastruktur Portal Pemerintah.
   b. Panduan Manajemen Sistem Dokumen Elektronik.
   c. Panduan Penyusunan Rencana Induk Pengembangan *E-government* Lembaga.
   d. Panduan Penyelenggaraan Situs Web Pemerintah Daerah.

D. Parameter Penerapan

Pengendalian atas pengelolaan sistem informasi dilakukan untuk memastikan akurasi dan kelengkapan informasi. Pengendalian dilakukan melalui pengendalian umum dan pengendalian aplikasi. Parameter penerapan pengendalian atas pengelolaan sistem informasi adalah sebagai berikut:

1. Pengendalian Umum

a. Pengamanan Sistem Informasi

1) Instansi pemerintah secara berkala melaksanakan penilaian risiko secara periodik yang komprehensif. Hal- hal yang perlu dipertimbangkan adalah sebagai berikut:

a) Penilaian risiko dilaksanakan dan didokumentasikan secara teratur dan pada saat sistem, fasilitas, atau kondisi lainnya berubah;

b) Penilaian risiko tersebut sudah mempertimbangkan sensitivitas dan keandalan data;

c) Penetapan risiko akhir dan persetujuan pimpinan instansi pemerintah didokumentasikan.

2) Pimpinan instansi pemerintah mengembangkan rencana yang secara jelas menggambarkan program pengamanan serta kebijakan dan prosedur yang mendukungnya.

3) Pimpinan instansi pemerintah menetapkan organisasi untuk mengimplementasikan dan mengelola program pengamanan.

4) Pimpinan instansi pemerintah menetapkan uraian tanggung jawab pengamanan secara jelas.

5) Instansi pemerintah mengimplementasikan kebijakan yang efektif atas pegawai yang terkait dengan program pengamanan.

6) Instansi pemerintah memantau efektivitas program pengamanan dan melakukan perubahan program pengamanan jika diperlukan. Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

a) Pimpinan instansi pemerintah secara berkala menilai kelayakan kebijakan pengamanan dan kepatuhan terhadap kebijakan tersebut;

b) Tindakan korektif diterapkan dan diuji dengan segera dan efektif serta dipantau secara terus-menerus.

b. Pengendalian atas Akses

1) Instansi pemerintah mengklasifikasikan sumber daya sistem informasi berdasarkan kepentingan dan sensitivitasnya.

   Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

   a) Klasifikasi sumber daya dan kriteria terkait sudah ditetapkan dan dikomunikasikan kepada pemilik sumber daya;

   b) Pemilik sumber daya memilah-milah sumber daya informasi berdasarkan klasifikasi dan kriteria yang sudah ditetapkan dengan memperhatikan penetapan dan penilaian risiko serta mendokumentasikannya.

2) Pemilik sumber daya mengidentifikasi pengguna yang berhak dan otorisasi akses ke informasi secara formal.

3) Instansi pemerintah menetapkan pengendalian fisik dan pengendalian logik untuk mencegah dan mendeteksi akses yang tidak diotorisasi.

4) Instansi pemerintah memantau akses ke sistem informasi, melakukan investigasi atas pelanggaran, dan mengambil tindakan perbaikan dan penegakan disiplin.

c. Pengendalian atas Pengembangan dan Perubahan Perangkat Lunak Aplikasi

1) Fitur pemrosesan sistem informasi dan modifikasi program diotorisasi.

2) Seluruh perangkat lunak yang baru dan yang dimutakhirkan sudah diuji dan disetujui.

3) Instansi pemerintah telah menetapkan prosedur untuk memastikan terselenggaranya pengendalian atas kepustakaan perangkat lunak (*software libraries*), termasuk pemberian label, pembatasan akses, dan penggunaan kepustakaan perangkat lunak yang terpisah.

d. Pengendalian atas Perangkat Lunak Sistem

1) Instansi pemerintah membatasi akses ke perangkat lunak sistem berdasarkan tanggung jawab pekerjaan dan otorisasi akses tersebut didokumentasikan.
2) Akses ke dan penggunaan perangkat lunak sistem dikendalikan dan dipantau.
3) Instansi pemerintah mengendalikan perubahan yang dilakukan terhadap perangkat lunak sistem.

e. Pemisahan Tugas

1) Tugas yang tidak dapat digabungkan sudah diidentifikasi dan kebijakan untuk memisahkan tugas tersebut sudah ditetapkan.
2) Pengendalian atas akses sudah ditetapkan untuk pelaksanaan pemisahan tugas.
3) Instansi pemerintah melakukan pengendalian atas kegiatan pegawai melalui penggunaan prosedur, supervisi, dan reviu.

f. Kontinuitas Pelayanan

1) Instansi pemerintah melakukan penilaian, pemberian prioritas, dan pengidentifikasian sumber daya pendukung atas kegiatan komputerisasi yang kritis dan sensitif.

2) Instansi pemerintah sudah mengambil langkah-langkah pencegahan dan minimalisasi potensi kerusakan dan terhentinya operasi komputer, antara lain melalui penggunaan prosedur *backup* data dan program, penyimpanan *back-up* data di tempat lain, pengendalian atas lingkungan, pelatihan staf, serta pengelolaan dan pemeliharaan perangkat keras.

3) Pimpinan instansi pemerintah sudah mengembangkan dan mendokumentasikan rencana komprehensif untuk mengatasi kejadian tidak terduga (*contingency plan*), misalnya langkah pengamanan apabila terjadi bencana alam, sabotase, dan terorisme.

4) Instansi pemerintah secara berkala menguji rencana untuk mengatasi kejadian tidak terduga dan melakukan penyesuaian jika diperlukan.

2. Pengendalian Aplikasi

a. Pengendalian Otorisasi

1) Instansi pemerintah mengendalikan dokumen sumber. Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

a) Akses ke dokumen sumber yang masih kosong dibatasi;

b) Dokumen sumber diberikan nomor urut tercetak (*prenumbered*).

2) Atas dokumen sumber dilakukan pengesahan. Hal-hal yang perlu dipertimbangkan adalah sebagai berikut:

a) Dokumen sumber yang penting memerlukan tanda tangan otorisasi;

b) Untuk sistem aplikasi *batch*, harus digunakan lembar kendali *batch* yang menyediakan informasi seperti tanggal, nomor kendali, jumlah dokumen, dan jumlah kendali (*control totals*) dari *field* kunci;

c) Reviu independen terhadap data dilakukan sebelum data dientri ke dalam sistem aplikasi.

3) Akses ke terminal entri data dibatasi.

4) *File* induk dan laporan khusus digunakan untuk memastikan bahwa seluruh data yang diproses telah diotorisasi.

b. Pengendalian Kelengkapan

1) Transaksi yang dientri dan diproses ke dalam komputer adalah seluruh transaksi yang telah diotorisasi.

2) Rekonsiliasi data dilaksanakan untuk memverifikasi kelengkapan data.

c. Pengendalian Akurasi

1) Desain entri data digunakan untuk mendukung akurasi data.

2) Validasi data dan *editing* dilaksanakan untuk mengidentifikasi data yang salah.

3) Data yang salah dengan segera dicatat, dilaporkan, diinvestigasi, dan diperbaiki.

4) Laporan keluaran direviu untuk mempertahankan akurasi dan validitas data.

d. **Pengendalian terhadap Keandalan Pemrosesan dan *File* Data**

1) Terdapat prosedur untuk memastikan bahwa hanya program dan *file* data versi terkini yang digunakan selama pemrosesan.
2) Terdapat program yang memiliki prosedur untuk memverifikasi bahwa versi *file* komputer yang sesuai yang digunakan selama pemrosesan.
3) Terdapat program yang memiliki prosedur untuk mengecek *internal file header labels* sebelum pemrosesan.
4) Terdapat aplikasi yang mencegah perubahan *file* secara bersamaan.

Indikator keberhasilan penerapan pengendalian atas pengelolaan sistem informasi, yang meliputi indikator *output* dan *outcome,* adalah sebagai berikut:

1. Indikator *output*

a. Pelaksanaan penilaian risiko atas pengelolaan sistem informasi;
b. Dokumen pengamanan, berisi aturan mengenai:
   1) Rencana program pengamanan dan kebijakan serta prosedur yang mendukungnya;
   2) Organisasi yang mengimplementasikan dan mengelola program pengamanan;
   3) Uraian tanggung jawab pengamanan;
   4) Kebijakan efektif atas pegawai yang terkait program pengamanan;

c. Pelaksanaan pemantauan efektivitas program pengamanan;

d. Pelaksanaan penilaian kelayakan kebijakan pengamanan;

e. Pelaksanaan tindakan korektif;

f. Dokumen berisi kebijakan, prosedur, dan tingkatan akses terhadap sistem informasi;

g. Pelaksanaan pemantauan atas penerapan kebijakan dan prosedur akses;

h. Pelaksanaan otorisasi dan akses atas:

   a. Pengembangan dan perubahan perangkat lunak aplikasi;

   b. dokumen sumber;

   c. entri data;

   d. desain data entri;

i. Program *contingency plan* telah disusun.

2. Indikator *outcome*

a. Kebijakan dan prosedur pengendalian yang diatur dalam suatu pedoman telah diterapkan dengan tepat.

b. Seluruh pegawai memahami tujuan dari kegiatan pengendalian atas pengelolaan sistem informasi.

c. Sistem informasi berfungsi secara optimal.

d. Pelaporan yang handal.

e. Tidak terdapat gangguan dalam pelayanan instansi pemerintah yang disebabkan oleh tidak berfungsinya sistem informasi.

BAB III

LANGKAH-LANGKAH PENYELENGGARAAN

Penyelenggaraan SPIP berupa kegiatan pengendalian atas pengelolaan sistem informasi dilakukan melalui tiga tahap utama, yaitu:

1. **Tahap Persiapan**, merupakan tahap awal implementasi, yang ditujukan untuk memberikan pemahaman atau kesadaran yang lebih baik tentang pengelolaan sistem informasi dan pengendaliannya, serta pemetaan atas kondisi pengendalian atas pengelolaan sistem informasi yang ada di instansi pemerintah, dan kebutuhan penerapannya.
2. **Tahap Pelaksanaan**, merupakan langkah tindak lanjut atas pemetaan, yang meliputi kegiatan pembangunan infrastruktur dan internalisasi.
3. **Tahap Pelaporan**, merupakan tahap melaporkan kegiatan dan upaya pengembangan berkelanjutan.

Setiap tahapan implementasi dan beberapa contoh akan diuraikan di bab ini.

A. Tahap Persiapan

Langkah-langkah yang perlu dilakukan oleh instansi pemerintah dalam persiapan penerapan sistem pengendalian atas pengelolaan sistem informasi, terdiri dari proses pemahaman dan persamaan persepsi, serta pemetaan, yaitu:

1) **Pemahaman dan Persamaan Persepsi (*Knowing*)**

Tahap pemahaman merupakan langkah awal dalam membangun kesadaran (*building awareness*) terhadap arti penting pengendalian atas pengelolaan sistem informasi, memperkuat komitmen, serta dukungan seluruh pejabat dan pegawai instansi pemerintah.

Seluruh pegawai harus diinformasikan mengenai sistem informasi yang ada di instansi pemerintah tersebut yang meliputi seluruh rangkaian sistem informasi, berupa *input*, proses, dan *output* sistem. Mereka juga harus memahami seluruh perangkat sistem yang digunakan, baik perangkat keras maupun perangkat lunak. Pimpinan harus memberikan pemahaman kepada seluruh pegawai akan arti penting dan tujuan dari sistem informasi, serta kaitannya dengan pencapaian tujuan organisasi. Pimpinan agar memberikan pemahaman kepada pegawai mengenai risiko-risiko terkait dengan pengelolaan sistem informasi, yang meliputi risiko atas *input*, proses, dan *output* sistem informasi, serta perlunya kegiatan pengendalian untuk mengatasi risiko tersebut.

Dengan adanya kesepahaman dan kesamaan persepsi tersebut, diharapkan implementasi dari pengendalian atas pengelolaan sistem informasi akan lebih efektif dan dapat mengurangi resistensi dari seluruh lapisan pegawai, serta mereka akan berpartisipasi aktif dalam mendukung pengendalian atas pengelolaan sistem informasi.

Tahap pemahaman diawali dengan mengomunikasikan pentingnya pengendalian atas pengelolaan sistem informasi dalam rangka menyediakan informasi, memastikan akurasi, dan kelengkapan informasi untuk pembuatan laporan kinerja maupun laporan keuangan yang lengkap dan akurat, serta untuk mendukung pengambilan keputusan.

Untuk memberikan penyamaan pemahaman tersebut, beberapa langkah yang dapat dilakukan adalah sebagai berikut:

a. Sosialisasi

- Sosialisasi mengenai kegiatan pengendalian atas pengelolaan sistem informasi disampaikan kepada seluruh pegawai. Sosialisasi tersebut merupakan bagian dari sosialisasi SPIP secara umum (keseluruhan).
- Kegiatan sosialisasi dilakukan oleh Satgas SPIP, yang dibentuk oleh pimpinan instansi pemerintah, beranggotakan perwakilan dari seluruh unit (bidang/bagian) di instansi tersebut, dan ada anggota Satgas yang memiliki pemahaman yang baik atas pengelolaan sistem informasi. Jika diperlukan, pimpinan instansi pemerintah dapat meminta bantuan narasumber dari untuk memberikan sosialisasi.
- Dalam kegiatan sosialisasi tersebut, satgas menyampaikan pula rencana tindak *(action plan)* pengembangan kegiatan pengendalian atas pengelolaan sistem informasi.
- Sosialisasi dilakukan melalui kegiatan ceramah, tanya jawab, diskusi, dan/atau seminar.

Dengan sosialisasi ini, diharapkan seluruh pegawai memahami pentingnya pengendalian atas pengelolaan sistem informasi yang ada di instansi, dan *road map,* serta rencana tindak pengembangan kegiatan pengendaliannya.

b. Penyebaran Informasi

Informasi mengenai sistem informasi yang dimiliki organisasi dan kegiatan pengendalian yang terkait disampaikan kepada pegawai melalui berbagai cara, antara lain melalui jaringan informasi internal (*Intranet*) dan tulisan dalam bulletin kantor, yang menganalisis dan mengkaji tentang kegiatan pengendalian atas pengelolaan sistem informasi.

2) Pemetaan (*Mapping*)

Setelah dilakukan sosialisasi pemahaman kegiatan pengendalian atas pengelolaan sistem informasi, maka perlu dilakukan suatu pemetaan terhadap kegiatan pengendalian atas pengelolaan sistem informasi yang dijalankan di instansi pemerintah. Pemetaan terhadap kegiatan pengendalian atas pengelolaan sistem informasi, dilakukan bersamaan dengan pemetaan yang dilakukan di subunsur kegiatan pengendalian dan unsur-unsur SPIP lainnya (pemetaan dilakukan serentak terhadap semua unsur dan subunsur SPIP, dengan mendasarkan pada Pedoman *Diagnostic Assessment*)

Pemetaan dilakukan untuk melihat kondisi kegiatan pengendalian yang sudah diimplementasikan dan berjalan pada instansi pemerintah, serta keberadaan infrastruktur dalam bentuk kebijakan dan prosedur pengelolaan sistem informasi.

Pemetaan juga untuk mengetahui apakah instansi telah mendokumentasikan penyelenggaraan pengendalian sistem informasi dan telah melakukan monitoring dan evaluasi atas kegiatan tersebut.

Dengan pemetaan, akan diketahui kondisi yang memerlukan perbaikan (*area of improvement*) agar kegiatan pengendalian atas pengelolaan sistem informasi dapat terbangun secara utuh.

B. Tahap Pelaksanaan

Setelah tahap persiapan, langkah berikutnya adalah tahap pelaksanaan penyelenggaraan pengendalian atas pengelolaan sistem informasi. Dalam tahap pelaksanaan ini, termasuk di dalamnya adalah tahap membangun infrastruktur (*norming*), tahap internalisasi (*forming*), dan tahap pengembangan berkelanjutan (*performing*).

Dalam tahap pelaksanaan ini, apabila dari hasil pemetaan diperoleh informasi bahwa instansi pemerintah telah melaksanakan pengendalian atas pengelolaan sistem informasi dan sudah berjalan efektif, maka langkah pelaksanaan tersebut tinggal dilanjutkan. Apabila suatu langkah pelaksanaan pengendalian belum ada/belum efektif, maka langkah tersebut perlu ditetapkan dan dilaksanakan.

1) Pembangunan Infrastruktur (*Norming*)

Instansi pemerintah menyusun kebijakan dan prosedur, serta pedoman lainnya terkait dengan pengendalian atas pengelolaan sistem informasi, dengan hasil pemetaan yang dilakukan dan hasil penilaian risiko.

Hasil pemetaan menggambarkan *area of improvement* secara umum di instansi. Hasilnya kemudian disesuaikan dengan hasil penilaian risiko atas pengelolaan sistem informasi, sehingga didapatkan *area of improvement* yang secara khusus ada di instansi.

Kebijakan, prosedur, dan pedoman lainnya yang perlu dibangun antara lain meliputi:

a. Kebijakan dan prosedur otorisasi atas:
   1) akses ke sistem informasi;
   2) akses perangkat lunak sistem;
   3) akses ke terminal entri;
   4) perubahan fitur dan modifikasi program;
   5) dokumen sumber;
   6) transaksi yang dientri dan diproses dalam komputer.
b. Penetapan aset teknologi informasi yang perlu dikelola dan rencana penyusunan kebijakan dan prosedur teknologi informasi.
c. Penetapan struktur organisasi untuk mengelola sistem informasi (termasuk program pengamanan).
d. Kebijakan dan prosedur pemisahan fungsi dalam pengelolaan sistem informasi.
e. Pedoman rencana kontinjensi (*contingency plan*).

2. Internalisasi (*Forming*)

Kebijakan, prosedur, dan pedoman lain yang terkait dengan pengendalian atas pengelolaan sistem informasi diinternalisasikan kepada seluruh pegawai.

Internalisasi adalah suatu proses untuk mewujudkan infrastruktur menjadi bagian dari kegiatan operasional sehari- hari. Perwujudannya, dapat tercermin dalam konteks seberapa jauh proses internalisasi memengaruhi pimpinan instansi pemerintah dalam mengambil keputusan, dan memengaruhi perilaku para pegawai dalam melaksanakan kegiatan.

Langkah-langkah yang perlu dilakukan sehubungan dengan internalisasi pengendalian atas pengelolaan sistem informasi, meliputi:

a. Melakukan pelatihan dan/atau *workshop* mengenai infrastruktur pengendalian yang telah dibangun kepada seluruh pegawai yang terkait dengan pengelolaan sistem informasi.

b. Mendistribusikan manual pedoman kegiatan pengendalian atas pengelolaan sistem informasi keseluruh unit yang ada di instansi pemerintah.

c. Memuat pedoman kegiatan pengendalian atas pengelolaan sistem informasi ke media informasi yang dimiliki instansi untuk dapat diakses oleh seluruh pegawai.

d. Pimpinan memberikan pengarahan secara rutin tentang pentingnya pengendalian umum dan pengendalian aplikasi atas pengelolaan sistem informasi.

e. Melaksanakan pedoman pengendalian atas pengelolaan sistem informasi.

3. Pengembangan Berkelanjutan (*Performing*)

Pengembangan berkelanjutan, dilakukan untuk memantau penerapan kebijakan dan prosedur yang terkait dengan pengelolaan sistem informasi, serta melakukan penyempurnaan kebijakan dan prosedur terkait apabila diperlukan.

Pengembangan berkelanjutan atas penyelenggaraan aktivitas pengendalian atas pengelolaan sistem informasi dilakukan dengan langkah-langkah berikut:

a. Pemantauan atas pelaksanaan pengendalian pengelolaan sistem informasi.

b. Evaluasi secara berkala atas hasil yang diperoleh dari kegiatan pemantauan.

c. Identifikasi perubahan lingkungan organisasi yang memengaruhi sistem informasi.

d. Identifikasi *gap* antara sistem informasi yang sedang berjalan dengan kebutuhan baru sehubungan dengan perubahan lingkungan organisasi.

e. Lakukan upaya penyempurnaan atas pengendalian sistem informasi yang ada.

Pada tahap awal pembangunan SPIP, pemantauan penerapan kegiatan pengendalian dilakukan oleh Tim Satgas, sedangkan pada periode-periode berikutnya merupakan bagian tidak terpisahkan dari unsur Pemantauan.

C. Tahap Pelaporan

Setelah tahap pelaksanaan selesai, seluruh kegiatan penyelenggaraan sub unsur perlu didokumentasikan. Pendokumentasian ini merupakan satu kesatuan (bagian yang tidak terpisahkan) dari kegiatan pelaporan berkala dan tahunan penyelenggaraan SPIP. Pendokumentasian dimaksud meliputi:

1. Pelaksanaan kegiatan, yang terdiri dari:

   a. Kegiatan pemahaman, antara lain kegiatan sosialisasi (ceramah, diskusi, seminar, rapat kerja, dan *focus group*) mengenai pengendalian sistem informasi.

b. Kegiatan pemetaan keberadaan dan penerapan infrastruktur, yang antara lain berisi: 1) pemetaan penerapan pengendalian atas pengelolaan sistem informasi, 2) masukan atas rencana tindak yang tepat untuk menyempurnakan kebijakan dan prosedur pengendalian yang sudah ada, baik pengendalian umum maupun pengendalian aplikasi.

c. Kegiatan pembangunan infrastruktur, yang antara lain berisi: 1) kebijakan dan prosedur pengelolaan sistem informasi, 2) penyusunan kebijakan dan prosedur pengendalian umum dan pengendalian aplikasi.

d. Kegiatan internalisasi, yang antara lain berisi: 1) kegiatan sosialisasi kebijakan dan prosedur pengelolaan sistem informasi, 2) kegiatan yang memastikan seluruh pegawai telah menerima informasi, serta memahami kebijakan dan prosedur pengelolaan sistem informasi.

e. Kegiatan pengembangan berkelanjutan, yang antara lain berisi: 1) kegiatan pemantauan penerapan kebijakan dan prosedur pengelolaan sistem informasi, 2) masukan bagi pimpinan instansi pemerintah untuk menyatakan asersi di Teknologi Informasi (TI) bahwa TI telah dikelola dengan baik.

2. Hambatan kegiatan

Apabila ditemukan hambatan-hambatan dalam pelaksanaan kegiatan yang menyebabkan tidak tercapainya target/tujuan kegiatan tersebut, agar dijelaskan penyebab terjadinya hambatan.

3. Saran

Saran diberikan berkaitan dengan adanya hambatan pelaksanaan kegiatan dan dicarikan saran pemecahan masalah agar kejadian serupa tidak terulang, dan guna peningkatan pencapaian tujuan. Saran yang diberikan agar realistis dan benar-benar dapat dilaksanakan.

4. Tindak lanjut atas saran periode sebelumnya

Bagian ini mengungkapkan tindak lanjut yang telah dilakukan atas saran yang telah diberikan pada kegiatan periode sebelumnya.

Dokumentasi ini merupakan bahan dukungan bagi penyusunan laporan berkala dan tahunan (penjelasan penyusunan laporan dapat dilihat pada Pedoman Teknis Umum Penyelenggaraan SPIP). Kegiatan pendokumentasian menjadi tanggung jawab pelaksana kegiatan, yang hasilnya disampaikan kepada pimpinan instansi pemerintah sebagai bentuk akuntabilitas, melalui Satuan Tugas Penyelenggaraan SPIP di instansi pemerintah terkait.

BAB IV
PENUTUP

Pedoman ini disusun dengan tujuan agar tersedia acuan bagi instansi pemerintah pusat dan satuan kerja dalam membangun aktivitas pengendalian, khususnya pada sub unsur Pengendalian atas Pengelolaan Sistem Informasi. Lebih lanjut, dengan terwujudnya pengendalian yang baik ini, maka kegiatan pengendalian yang dibangun dapat menjamin akurasi dan kelengkapan informasi untuk pengambilan keputusan, serta untuk mendukung penyusunan laporan yang dapat diandalkan.

Di dalam pedoman ini disajikan bahwa kegiatan pengendalian atas pengelolaan sistem informasi dikembangkan dengan mendasarkan pada hasil penilaian risiko terhadap sistem informasi organisasi. Kegiatan pengendalian terdiri atas pengendalian umum dan pengendalian aplikasi. Pengendalian umum berhubungan dengan pengendalian atas pengelolaan sistem informasi secara umum, sedangkan pengendalian aplikasi berkaitan dengan entri data, *file*, program, dan keluaran dari aplikasi tertentu

Langkah-langkah yang tertuang dalam pedoman ini merupakan langkah pelaksanaan minimal yang sebaiknya dibangun. Instansi pemerintah hendaknya dapat mengembangkan lebih jauh langkah-langkah yang perlu diambil sesuai dengan kebutuhan, dengan tetap mengacu pada (dan tidak boleh bertentangan dengan) peraturan perundang-undangan yang berlaku.

Kami sadar bahwa pedoman ini belum sempurna, dan kami pun mengerti bahwa perkembangan teori dan praktik-praktik sistem pengendalian intern tidak mungkin terhentikan. Oleh karenanya, pedoman ini akan terus diperbarui dan perlu masukan-masukan dari pihak mana pun demi lebih baiknya pedoman ini.