BERITA NEGARA REPUBLIK INDONESIA

No.251, 2022 KEMENHAN. Pelaksanaan Pengendalian Intern atas Pelaporan Keuangan.

PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA

NOMOR 6 TAHUN 2022

TENTANG

PELAKSANAAN PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN DI LINGKUNGAN KEMENTERIAN PERTAHANAN DAN TENTARA NASIONAL INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PERTAHANAN REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk tersusunnya laporan keuangan yang akuntabel di lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia berdasarkan Peraturan Menteri Keuangan Nomor 17/PMK.09/2019 tentang Pedoman Penerapan, Penilaian dan Reviu Pengendalian Intern atas Pelaporan Keuangan Pemerintah Pusat, perlu pengaturan mengenai pengendalian internal atas pelaporan keuangan di lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Menteri Pertahanan tentang Pelaksanaan Pengendalian Intern atas Pelaporan Keuangan di Lingkungan Kementerian Pertahanan dan Tentara Nasional Indonesia;

www.peraturan.go.id

Mengingat : 1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 17 Tahun 2003 tentang Keuangan Negara (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 47, Tambahan Lembaran Negara Republik Indonesia Nomor 4286);
3. Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 5, Tambahan lembaran Negara Republik Indonesia Nomor 4355);
4. Undang-Undang Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 66, Tambahan Lembaran Negara Republik Indonesia Nomor 4400);
5. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
6. Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 127, Tambahan Lembaran Negara Republik Indonesia Nomor 4890);
7. Peraturan Presiden Nomor 58 Tahun 2015 tentang Kementerian Pertahanan (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 102);
8. Peraturan Menteri Keuangan Nomor 17/PMK.09/2019 tentang Pedoman Penerapan, Penilaian dan Reviu Pengendalian Intern atas Pelaporan Keuangan Pemerintah Pusat (Berita Negara Republik Indonesia Tahun 2019 Nomor 193);
9. Peraturan Menteri Pertahanan Nomor 14 Tahun 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan (Berita Negara Republik Indonesia Tahun 2019 Nomor 314);

www.peraturan.go.id

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PERTAHANAN TENTANG PELAKSANAAN PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN DI LINGKUNGAN KEMENTERIAN PERTAHANAN DAN TENTARA NASIONAL INDONESIA.

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Pengendalian Intern atas Pelaporan Keuangan yang selanjutnya disingkat PIPK adalah pengendalian yang secara spesifik dirancang untuk memberikan keyakinan yang memadai bahwa laporan keuangan yang dihasilkan merupakan laporan yang andal dan disusun sesuai dengan standar akuntansi pemerintahan.
2. Kementerian Pertahanan yang selanjutnya disebut Kemhan adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
3. Tentara Nasional Indonesia yang selanjutnya disingkat TNI adalah TNI Angkatan Darat, TNI Angkatan Laut, dan TNI Angkatan Udara.
4. Pelaporan Keuangan Kemhan yang selanjutnya disebut Pelaporan Keuangan adalah keseluruhan proses yang terkait dengan penyusunan laporan keuangan di lingkungan Kemhan dan TNI mulai dari otorisasi, transaksi sampai dengan terbitnya laporan keuangan, termasuk proses konsolidasi laporan keuangan Kementerian Pertahanan yang terdiri dari Laporan Keuangan Unit Organisasi dan Satuan Kerja Badan Layanan Umum.
5. Laporan Keuangan adalah laporan yang terstruktur mengenai posisi keuangan dan transaksi yang dilakukan oleh suatu entitas pelaporan.
6. Entitas Pelaporan adalah unit pemerintahan yang terdiri dari 1 (satu) atau lebih entitas akuntansi yang menurut Ketentuan Peraturan Perundang-undangan wajib menyampaikan laporan pertangggungjawaban berupa Laporan Keuangan.

www.peraturan.go.id

7. Entitas Akuntansi adalah unit pemerintahan pengguna anggaran/pengguna barang dan oleh karenanya wajib menyelenggarakan akuntansi dan menyusun Laporan Keuangan untuk digabungkan pada Entitas Pelaporan.
8. Laporan Keuangan Kemhan adalah laporan pertanggung jawaban atas pelaksanaan Anggaran dan Pendapatan Belanja Negara yang disusun oleh Pusat Pelaporan dan Pembinaan Keuangan Pertahanan Kementerian Pertahanan, dan merupakan konsolidasi dari Laporan Keuangan Kemhan yang terdiri atas Laporan Keuangan Unit Organisasi dan Satuan Kerja Badan Layanan Umum.
9. Penilaian PIPK adalah kegiatan yang dilakukan oleh manajemen untuk memastikan kecukupan rancangan dan efektivitas pelaksanaan pengendalian dalam mendukung keandalan Pelaporan Keuangan.
10. Tim Penilai PIPK yang selanjutnya disebut Tim Penilai adalah tim kerja pada Entitas Akuntansi dan/atau Entitas Pelaporan yang ditunjuk/memiliki tugas untuk membantu manajemen dalam melaksanakan Penilaian PIPK.
11. Catatan Hasil Reviu PIPK yang selanjutnya disebut CHR PIPK adalah dokumen yang berisi simpulan yang didapatkan dari suatu proses reviu PIPK.
12. Laporan Hasil Reviu PIPK yang selanjutnya disebut LHR PIPK adalah laporan yang berisi kompilasi dari simpulan yang terdapat pada CHR PIPK.
13. Pernyataan Telah Direviu Laporan Keuangan yang selanjutnya disebut PTD adalah pernyataan dari Aparat Pengawasan Intern Kemhan dan TNI atas hasil reviu terhadap Laporan Keuangan Kemhan dan TNI sebelum dipertanggungjawabkan oleh Menteri Pertahanan dan Kepala Unit Organisasi.
14. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pertahanan.
15. Unit Organisasi yang selanjutnya disingkat UO adalah tingkatan dalam organisasi pengelolaan program dan

www.peraturan.go.id

anggaran di lingkungan Kemhan dan TNI, terdiri dari UO Kemhan, UO Markas Besar TNI, UO TNI Angkatan Darat, UO TNI Angkatan Laut dan UO TNI Angkatan Udara.

16. Satuan Kerja yang selanjutnya disebut Satker adalah unit satuan pengelolaan Daftar Isian Pelaksanaan Anggaran yang ditetapkan oleh Menteri untuk mengelola keuangan untuk pelaksanaan anggaran belanja pada Kemhan dan TNI.
17. Unit Akuntansi dan Pelaporan Keuangan Kuasa Pengguna Anggaran yang selanjutnya disebut UAKPA adalah unit akuntansi yang melakukan kegiatan akuntansi dan pelaporan tingkat Satker.
18. Unit Akuntansi dan Pelaporan Keuangan Pembantu Pengguna Anggaran Wilayah yang selanjutnya disebut UAPPA-W adalah unit akuntansi pada tingkat wilayah atau unit kerja lain yang ditetapkan sebagai UAPPA-W yang melakukan kegiatan penggabungan Laporan Keuangan seluruh UAKPA yang berada dalam wilayah kerjanya.
19. Unit Akuntansi dan Pelaporan Keuangan Pembantu Pengguna Anggaran Eselon I yang selanjutnya disebut UAPPA-E1 adalah unit akuntansi pada unit eselon I yang melakukan kegiatan penggabungan Laporan Keuangan seluruh UAPPA-W yang berada di wilayah kerjanya serta UAKPA yang langsung berada di bawahnya.
20. Unit Akuntansi dan Pelaporan Keuangan Pengguna Anggaran yang selanjutnya disebut UAPA adalah unit akuntansi pada tingkat kementerian negara/lembaga (pengguna anggaran) yang melakukan kegiatan penggabungan Laporan Keuangan seluruh UAPPA-E1 yang berada di bawahnya.
21. Pengendalian Intern Tingkat Entitas yang selanjutnya disingkat PITE adalah pengendalian yang dirancang untuk memberikan keyakinan memadai atas pencapaian tujuan Laporan Keuangan suatu organisasi secara menyuruh dan mempunyai dampak yang luas terhadap

www.peraturan.go.id

organisasi meliputi keseluruhan proses, transaksi, akun atau asersi dalam Laporan Keuangan.

22. Pengendalian Umum Teknologi Informasi dan Komunikasi yang selanjutnya disingkat PUTIK adalah bentuk pengendalian yang bertujuan untuk meyakinkan keamanan, kestabilan, dan keandalan kinerja dari perangkat keras (*hardware*) dan perangkat lunak (*software*) komputer serta sumber daya manusia dan teknologi informasi dan komunikasi yang berhubungan dengan sistem keuangan, khususnya dalam rangka penyusunan Laporan Keuangan.
23. Aparat Pengawasan Intern Pemerintah yang selanjutnya disingkat APIP adalah instansi pemerintah yang memiliki tugas pokok melakukan pengawasan. Di lingkungan Kemhan dan TNI terdiri dari Inspektorat Jenderal Kemhan, Inspektorat Jenderal TNI, dan Inspektorat Jenderal Angkatan.

BAB II
PENERAPAN PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN

Pasal 2

Prinsip penerapan PIPK antara lain:

a. mendukung pencapaian tujuan organisasi;
b. merupakan bagian yang tidak terpisahkan dari proses organisasi dan pengambilan keputusan khususnya dalam perencanaan strategis;
c. sistematis, terstruktur, dan tepat waktu;
d. mempertimbangkan keseimbangan aspek biaya dan manfaat; dan
e. menjaga kepatuhan terhadap hukum dan Ketentuan Peraturan Perundang-undangan.

www.peraturan.go.id

Pasal 3

Penerapan PIPK bertujuan untuk memberikan keyakinan memadai bahwa Pelaporan Keuangan dilaksanakan dengan pengendalian intern yang memadai.

Pasal 4

PIPK diterapkan oleh setiap:

a. Entitas Akuntansi; dan
b. Entitas Pelaporan.

Pasal 5

(1) Entitas Akuntansi di lingkungan Kemhan dan TNI sebagaimana dimaksud dalam Pasal 4 huruf a terdiri atas Unit Akuntansi Uang/Barang pada:
    a. tingkat Satker;
    b. tingkat wilayah;
    c. tingkat eselon I; dan
    d. tingkat kementerian.
(2) Entitas Pelaporan di lingkungan Kemhan dan TNI sebagaimana dimaksud dalam Pasal 4 huruf b dilaksanakan oleh UAKPA, UAPPA-W, UAPPA-E1, dan UAPA di lingkungan Kemhan dan TNI.

Pasal 6

(1) Penerapan PIPK oleh Entitas Akuntansi dan Entitas Pelaporan sebagaimana dimaksud dalam Pasal 4 dilaksanakan pada:
    a. tingkat entitas; dan
    b. tingkat proses/transaksi.
(2) Penerapan PIPK pada tingkat entitas sebagaimana dimaksud pada ayat (1) huruf a meliputi unsur pengendalian intern yang ada dalam Entitas Akuntansi dan Entitas Pelaporan, yaitu:
    a. lingkungan pengendalian;
    b. penilaian risiko;
    c. kegiatan pengendalian;
    d. informasi dan komunikasi; dan

www.peraturan.go.id

e. pemantauan.

(3) Penerapan PIPK pada tingkat entitas sebagaimana dimaksud pada ayat (1) huruf a termasuk penerapan PUTIK.

(4) Penerapan PIPK pada tingkat proses/transaksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap proses/transaksi yang dilakukan secara manual dan/atau proses/transaksi yang dilakukan menggunakan sistem aplikasi.

Pasal 7

Setiap Entitas Akuntansi dan Entitas Pelaporan bertanggung jawab untuk mengelola, memelihara, dan memutakhirkan dokumentasi penerapan PIPK.

Pasal 8

Penerapan PIPK, Penilaian PIPK, dan reviu PIPK di lingkungan Kemhan dan TNI dilaksanakan sesuai dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB III

PENILAIAN PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN

Pasal 9

(1) Dalam menjaga efektivitas penerapan PIPK, Entitas Akuntansi dan Entitas Pelaporan di lingkungan Kemhan dan TNI melaksanakan Penilaian PIPK.

(2) Entitas Akuntansi yang melaksanakan Penilaian PIPK sebagaimana dimaksud pada ayat (1) dipilih dan ditetapkan oleh Unit Akuntansi Uang/Barang tingkat kementerian di lingkungan Kemhan dan TNI berdasarkan pertimbangan risiko.

(3) Pertimbangan risiko sebagaimana dimaksud pada ayat (2) merupakan pertimbangan yang terkait dengan hal yang dapat mempengaruhi opini atas Laporan Keuangan.

www.peraturan.go.id

(4) Pemilihan Entitas Akuntansi yang melaksanakan Penilaian PIPK sebagaimana dimaksud pada ayat (2) dilakukan dengan meminta pertimbangan kepada Unit Akuntansi Uang/Barang tingkat UO di lingkungan Kemhan dan TNI.

(5) Penetapan Entitas Akuntansi dan Entitas Pelaporan sebagaimana dimaksud pada ayat (2) dilaksanakan pada triwulan pertama.

Pasal 10

(1) Penilaian PIPK sebagaimana dimaksud dalam Pasal 9 ayat (1) dilaksanakan oleh Tim Penilai.

(2) Tim Penilai dibentuk pada tingkat:
   a. UAPA;
   b. UAPPA-E1;
   c. UAPPA-W; dan/atau
   d. UAKPA.

(3) Susunan Tim Penilai terdiri dari:
   a. Tim Penilai Tingkat UAPA terdiri dari:
      1. Menteri sebagai Pengarah;
      2. Direktur Jenderal Perencanaan Pertahanan Kemhan sebagai Ketua;
      3. Kepala Pusat Pelaporan dan Pembinaan Keuangan Pertahanan Kemhan sebagai Sekretaris I;
      4. Kepala Pusat Barang Milik Negara Badan Sarana Pertahanan Kemhan sebagai Sekretaris II; dan
      5. Tim Penilai ditetapkan melalui Surat Keputusan atau Surat Perintah Menteri berdasarkan usulan dari Direktur Jenderal Perencanaan Pertahanan Kemhan serta masukan dari Kepala Pusat Pelaporan dan Pembinaan Keuangan Pertahanan Kemhan dan Kepala Pusat Barang Milik Negara Badan Sarana Pertahanan Kemhan.
   b. Tim Penilai Tingkat UAPPA-E1 terdiri dari:

www.peraturan.go.id

1. Panglima TNI, Kepala Staf Angkatan, dan *Sekretaris* Jenderal Kemhan sebagai Pengarah;
2. Asisten Perencanaan Umum Panglima TNI, Asisten Perencanaan Angkatan, dan Kepala Biro Perencanaan dan Keuangan Sekretariat Jenderal Kemhan sebagai Ketua;
3. Susunan Keanggotaan Tim Penilai mulai dari dari sekretaris sampai dengan anggota ditetapkan oleh masing-masing UO; dan
4. Tim Penilai ditetapkan melalui Surat Keputusan atau Surat Perintah Panglima TNI, Kepala Staf Angkatan, dan Sekretaris Jenderal Kemhan.

c. Susunan Tim Penilai Tingkat UAPPA-W diatur sesuai dengan struktur organisasinya masing-masing;

d. Tingkat UAKPA terdiri dari:
1. Kepala Satker sebagai Pengarah;
2. Susunan Keanggotaan Tim Penilai mulai dari ketua sampai dengan anggota ditetapkan oleh masing-masing Satker;
3. Kepala Satker dapat mengajukan perbantuan personil penilai kepada entitas diatasnya jika diperlukan; dan
4. Tim Penilai ditetapkan melalui Surat Keputusan atau Surat Perintah Kepala Satker.

e. Anggota Tim Penilai mulai dari Tingkat UAPA sampai dengan Tingkat UAKPA merupakan perwakilan dari bagian perencanaan, bagian keuangan, bagian logistik, teknologi informasi dan komunikasi, bagian umum, dan bagian sumber daya manusia yang dipilih dengan pertimbangan profesionalisme meliputi pengetahuan (*knowledge*) dan keahlian (*skill*).

Pasal 11

(1) Penilaian PIPK dilaksanakan pada:
a. tingkat entitas; dan
b. tingkat proses/transaksi.

www.peraturan.go.id

(2) Penilaian PIPK tingkat entitas sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan dengan ketentuan sebagai berikut:
   a. Penilaian PIPK tingkat entitas dilaksanakan 1 (satu) tahun sekali dalam rentang waktu tanggal 1 September tahun berkenaan sampai dengan tanggal 15 Januari tahun berikutnya; dan
   b. Penilaian PIPK tingkat entitas pada tahun berikutnya dapat menggunakan hasil penilaian tahun sebelumnya apabila entitas dipandang tidak mengalami perubahan signifikan.

(3) Penilaian PIPK tingkat proses/transaksi sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan sekali dalam 1 (satu) tahun dalam rentang waktu tanggal 1 September tahun berkenaan sampai dengan tanggal 15 Januari tahun berikutnya.

Pasal 12

(1) Tim Penilai menyusun laporan hasil Penilaian PIPK.

(2) Laporan hasil Penilaian PIPK tingkat Satker.

(3) Laporan hasil Penilaian PIPK sebagaimana dimaksud pada ayat (1) disampaikan paling lambat 1 (satu) bulan setelah pelaksanaan Penilaian PIPK oleh Tim Penilai kepada:
   a. pimpinan Entitas Akuntansi dan/atau Entitas Pelaporan; dan
   b. Tim Penilai di atasnya secara berjenjang.

(4) Laporan hasil Penilaian PIPK sebagaimana dimaksud pada ayat (1) pada tingkat UAPPA-El dan UAPA, beserta Laporan Keuangan Kemhan disampaikan kepada APIP.

(5) Laporan hasil Penilaian PIPK sebagaimana dimaksud pada ayat (1) menyimpulkan efektivitas penerapan PIPK dalam 3 (tiga) tingkatan, yaitu:
   a. efektif;
   b. efektif dengan pengecualian; atau
   c. mengandung kelemahan material.

www.peraturan.go.id

(6) Laporan hasil Penilaian PIPK sebagaimana dimaksud pada ayat (1) dibuat sesuai dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(7) Batas waktu penyampaian pelaporan hasil Penilaian PIPK adalah:

a. untuk tingkat UAKPA pelaporan dikirimkan pada tingkat UAPPA-W paling lambat tanggal 17 Januari di tahun berikutnya. Khusus tingkat UAKPA yang diatasnya tidak memiliki tingkat UAPPA-W, maka dapat dikirimkan ke tingkat UAPPA-E1;

b. untuk tingkat UAPPA-W pelaporan dikirimkan pada tingkat UAPPA-E1 paling lambat tanggal 30 Januari di tahun berikutnya;

c. untuk tingkat UAPPA-E1 pelaporan dikirimkan pada tingkat UAPA Kementerian/Lembaga paling lambat tanggal 10 Februari di tahun berikutnya; dan

d. untuk tingkat UAPA Kementerian/Lembaga pelaporan dikirimkan pada tingkat UAPA Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah paling lambat tanggal 15 Februari di tahun berikutnya.

Pasal 13

Penilaian PIPK sebagaimana dimaksud dalam Pasal 9 sampai dengan Pasal 12 dilaksanakan sesuai dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB IV
REVIU PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN

Pasal 14

(1) Untuk memberikan keyakinan terbatas kepada pimpinan mengenai efektivitas penerapan PIPK secara memadai, dilakukan reviu PIPK.

www.peraturan.go.id

(2) Reviu PIPK sebagaimana dimaksud pada ayat (1) dilaksanakan oleh APIP.

(3) Reviu PIPK dilaksanakan terhadap penerapan PIPK yang berasal dari laporan hasil Penilaian PIPK yang disampaikan oleh Tim Penilai sebagaimana dimaksud dalam Pasal 12 ayat (3).

Pasal 15

Reviu PIPK dilaksanakan dengan tahapan sebagai berikut:

a. perencanaan reviu PIPK;

b. pelaksanaan reviu PIPK; dan

c. pelaporan reviu PIPK.

Pasal 16

(1) Pada tahap perencanaan reviu PIPK, APIP menyusun program kerja reviu PIPK berdasarkan penerapan PIPK, Penilaian PIPK, dan reviu PIPK.

(2) Reviu PIPK direncanakan pada semester I tahun berikutnya.

Pasal 17

Reviu PIPK dilaksanakan dengan metode uji petik (*sampling*) dan dilakukan paling lambat bersamaan dengan reviu Laporan Keuangan Kemhan.

Pasal 18

(1) Untuk setiap Entitas Akuntansi dan/atau Entitas Pelaporan yang direviu, APIP menyusun CHR PIPK dan/atau LHR PIPK.

(2) CHR PIPK dan/atau LHR PIPK sebagaimana dimaksud pada ayat (1) disampaikan kepada:

   a. Entitas Akuntansi yang direviu paling lambat 1 (satu) bulan setelah pelaksanaan reviu; dan

   b. Entitas Pelaporan yang direviu paling lambat bersamaan dengan waktu penyampaian PTD kepada Menteri.

www.peraturan.go.id

(3) CHR PIPK dan/atau LHR PIPK sebagaimana dimaksud pada ayat (1) menjadi dasar Pimpinan Satker untuk membuat pernyataan tanggung jawab atas Laporan Keuangan.

(4) Dalam hal tidak dilakukan reviu PIPK oleh APIP, hasil Penilaian PIPK oleh Tim Penilai digunakan sebagai dasar Pimpinan Satker untuk membuat pernyataan tanggung jawab atas Laporan Keuangan.

Pasal 19

Reviu PIPK sebagaimana dimaksud dalam Pasal 14 sampai dengan Pasal 18 dilaksanakan sesuai dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB IV

PENDANAAN

Pasal 20

Pendanaan yang diperlukan untuk penyelenggaraan kegiatan Penilaian PIPK sebagaimana yang dimaksud dalam Pasal 9 ayat (1) dibebankan pada anggaran Kemhan.

Pasal 21

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

www.peraturan.go.id

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 25 Februari 2022

MENTERI PERTAHANAN
REPUBLIK INDONESIA,

ttd

PRABOWO SUBIANTO

Diundangkan di Jakarta
pada tanggal 10 Maret 2022

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

BENNY RIYANTO

www.peraturan.go.id

LAMPIRAN
PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA
NOMOR 6 TAHUN 2022
TENTANG
PELAKSANAAN PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN DI LINGKUNGAN KEMENTERIAN PERTAHANAN DAN TENTARA NASIONAL INDONESIA

PEDOMAN PENERAPAN, PENILAIAN, DAN REVIU PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN DI LINGKUNGAN KEMHAN DAN TNI

a. Pendahuluan

Tujuan utama pengendalian intern memberikan keyakinan memadai atas tercapainya tujuan organisasi. Menurut Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah, pencapaian tujuan organisasi diwujudkan melalui kegiatan yang efektif dan efisien, keandalan pelaporan keuangan, pengamanan aset negara, dan ketaatan terhadap peraturan perundang-undangan.

Tujuan keandalan pelaporan, khususnya pelaporan keuangan, meliputi pemenuhan terhadap aspek reliabilitas, ketepatan waktu, transparansi, dan aspek-aspek lainnya yang telah ditetapkan dalam organisasi, termasuk organisasi pemerintah. Laporan Keuangan Kemhan, sebagai salah satu bentuk akuntabilitas pengelolaan keuangan negara, harus disajikan secara andal agar dapat meningkatkan akuntabilitas Kemhan. Mengingat pentingnya tujuan tersebut, setiap pimpinan dan seluruh pejabat/pegawai di lingkungan Kemhan dan TNI perlu meningkatkan penerapan Pengendalian Intern atas Pelaporan Keuangan (PIPK) secara sistematis, terstruktur, dan terdokumentasi dengan baik untuk mendapatkan hasil yang optimal. PIPK adalah pengendalian yang secara spesifik dirancang untuk memberikan keyakinan yang memadai bahwa laporan keuangan yang dihasilkan andal dan disusun sesuai dengan standar akuntansi yang berlaku. Di samping itu, penerapan PIPK diharapkan dapat memberikan keyakinan yang memadai kepada pembaca atau pengguna laporan keuangan bahwa:

www.peraturan.go.id

1. Laporan keuangan menggambarkan secara lengkap dan memadai seluruh transaksi keuangan yang terjadi;
2. Seluruh transaksi keuangan telah dicatat sesuai dengan peraturan, kebijakan, maupun standar yang berlaku;
3. Seluruh transaksi telah dilaksanakan sesuai dengan pembagian kewenangan yang telah ditetapkan; dan
4. Seluruh sumber daya keuangan telah diamankan dari kerugian yang material akibat adanya pemborosan, penyalahgunaan, kesalahan, kecurangan, atau sebab-sebab lainnya.

b. Tujuan dan Manfaat Pengendalian Intern atas Pelaporan Keuangan.

Penerapan PIPK bertujuan untuk memberikan keyakinan bahwa penyusunan laporan keuangan yang dilakukan oleh Kemhan dan TNI telah dilaksanakan dengan sistem pengendalian intern yang memadai. Adapun manfaat penerapan PIPK antara lain adalah:

1. Meningkatnya efektivitas dan efisiensi operasi;
2. Meningkatnya kualitas tata kelola dan sistem pelaporan keuangan;
3. Meningkatnya keandalan laporan keuangan;
4. Terjaganya kepatuhan terhadap hukum dan peraturan perundang-undangan; dan
5. Meningkatnya reputasi organisasi dan kepercayaan para pemangku kepentingan.

c. Keterbatasan Penerapan Pengendalian Intern.

Pengendalian intern secara umum dirancang untuk memberikan keyakinan memadai (*reasonable assurance*) terhadap pencapaian tujuan organisasi. Oleh karena itu, tidak ada jaminan mutlak bahwa tujuan tersebut akan dicapai secara sempurna. Hal ini terjadi karena pengendalian intern dirancang berdasarkan pertimbangan biaya dan manfaat serta keberhasilannya sangat dipengaruhi oleh faktor manusia. Meskipun telah dirancang dengan baik, pengendalian intern tetap memiliki keterbatasan, antara lain pertimbangan yang kurang matang, kegagalan menerjemahkan perintah, pengabaian manajemen, dan adanya kolusi. Keterbatasan ini juga berlaku dalam penerapan PIPK.

d. Tingkatan Penerapan Pengendalian Intern atas Pelaporan Keuangan.

Penerapan PIPK harus dilaksanakan oleh seluruh Entitas Akuntansi

www.peraturan.go.id

dan Entitas Pelaporan, mulai dari Entitas Akuntansi tingkat paling bawah sampai dengan Entitas Pelaporan tingkat UAPA. Selanjutnya untuk setiap Entitas Akuntansi dan/atau Entitas Pelaporan, PIPK harus dirancang dan diimplementasikan pada tingkat entitas dan tingkat proses/transaksi.

Penjelasan mengenai penerapan PIPK pada setiap tingkatan diuraikan sebagai berikut:

1. Pengendalian Intern tingkat Entitas.

   Sebagai elemen yang tak terpisahkan dari konsep pengendalian intern secara umum, PIPK juga perlu diimplementasikan pada tingkat entitas. Pengendalian pada tingkat entitas dirancang untuk memberikan keyakinan memadai atas pencapaian tujuan pelaporan keuangan suatu organisasi secara menyeluruh. Pengendalian ini mempunyai dampak yang luas terhadap organisasi meliputi keseluruhan proses, transaksi, akun, atau asersi dalam laporan keuangan. Bentuk aplikatif dari Pengendalian Intern Tingkat Entitas dapat mengacu pada penerapan komponen-komponen dan prinsip-prinsip pengendalian intern menurut *Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control-Integrated Framework*. Penggunaan *framework* COSO ini sesuai dengan konsep pengendalian intern pemerintah Indonesia sebagaimana diatur dalam Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah, beserta peraturan-peraturan turunannya, yang secara umum juga mengacu pada konsep pengendalian intern COSO. Pada tahun 2013, COSO telah merilis Internal *Control-Integrated Framework* (selanjutnya disebut COSO 2013) terbaru sebagai penyempurnaan dari COSO Internal *Control-Integrated Framework* 1992. Komponen-komponen dan prinsip-prinsip pengendalian intern menurut COSO 2013 (terdiri dari 5 (lima) komponen dan 17 (tujuh belas) prinsip) dapat diuraikan sebagai berikut:

   a) Lingkungan pengendalian

      1) Organisasi menunjukkan komitmen terhadap integritas dan nilai-nilai etika.

www.peraturan.go.id

2) Dewan pengawas atau komite audit menunjukkan independensi dari manajemen dan menjalankan pengawasan (*oversight*) atas proses pengembangan dan penerapan pengendalian intern.
3) Manajemen menetapkan struktur organisasi, jalur pelaporan, serta pemisahan wewenang dan tanggung jawab yang memadai dalam rangka pencapaian tujuan.
4) Organisasi menunjukkan komitmen untuk merekrut, mengembangkan, dan menempatkan pegawal yang kompeten sesuai dengan tujuan organisasi.
5) Organisasi memastikan akuntabilitas setiap pegawai dalam melaksanakan pengendalian intern yang menjadi tanggung jawabnya.

b) Penilaian risiko
1) Organisasi menetapkan tujuan secara jelas sehingga memungkinkan dilakukannya identifikasi dan penilaian risiko terkait pencapaian tujuan tersebut.
2) Organisasi mengidentifikasi dan menganalisis risiko yang dihadapi seluruh entitas dalam pencapaian tujuan sebagai dasar menentukan bagaimana risiko tersebut akan dikelola.
3) Organisasi mempertimbangkan potensi terjadinya kecurangan dalam proses penilaian risiko.
4) Organisasi mengidentifikasi dan menilai perubahan-perubahan yang dapat berdampak signifikan terhadap sistem pengendalian intern.

c) Kegiatan pengendalian
1) Organisasi menentukan dan mengembangkan kegiatan pengendalian yang berkontribusi terhadap mitigasi risiko hingga ke level yang dapat diterima.
2) Organisasi menentukan dan mengembangkan aktivitas pengendalian umum (*general control*) atas penggunaan teknologi untuk mendukung pencapaian tujuan.
3) Organisasi menentukan dan mengembangkan aktivitas pengendalian umum (*general control*) atas penggunaan

www.peraturan.go.id

teknologi untuk mendukung pencapaian tujuan.

d) Informasi dan komunikasi
   1) Organisasi memperoleh, menghasilkan, dan menggunakan informasi yang relevan dan berkualitas untuk mendukung terlaksananya pengendalian intern.
   2) Organisasi secara internal mengomunikasikan tujuan, tanggung jawab, dan informasi terkait pengendalian intern dalam rangka mendukung terlaksananya pengendalian intern.
   3) Organisasi berkomunikasi kepada pihak-pihak eksternal mengenai permasalahan yang dapat mempengaruhi pelaksanaan pengendalian intern.

e) Kegiatan pemantauan
   1) Organisasi menetapkan, mengembangkan, dan melaksanakan evaluasi berkelanjutan dan/atau evaluasi terpisah untuk menilai apakah komponen-komponen pengendalian intern telah ada dan berfungsi.
   2) Organisasi menetapkan, mengembangkan, dan melaksanakan evaluasi berkelanjutan dan/ atau evaluasi terpisah untuk menilai apakah komponen-komponen pengendalian intern telah ada dan berfungsi.

Di samping penerapan atas prinsip dan komponen pengendalian intern COSO 2013, Pengendalian Intern Tingkat Entitas juga harus memperhatikan PUTIK/*Information Technology General Control* (ITGC). Bentuk pengendalian ini juga merupakan penjabaran dari salah satu prinsip dalam komponen kegiatan pengendalian menurut COSO 2013 di atas. Hal ini perlu dilakukan oleh manajemen karena proses penyusunan Laporan Keuangan di semua tingkatan tidak dapat dipisahkan dari pemanfaatan Teknologi Informasi dan Komunikasi (TIK). Bahkan tren saat ini menunjukkan bahwa TIK mempunyai peran yang semakin vital dalam mewujudkan laporan keuangan yang andal. PUTIK adalah bentuk pengendalian yang bertujuan untuk meyakinkan keamanan, kestabilan, dan keandalan kinerja dari perangkat keras (*hardware*) dan perangkat lunak (*software*) komputer serta sumber

www.peraturan.go.id

daya manusia dan TIK yang berhubungan dengan sistem-sistem keuangan, khususnya dalam rangka penyusunan laporan keuangan. Secara umum, Pengendalian Umum TIK terdiri dari 4 (empat) komponen atau area pengendalian utama, yaitu:

a) Manajemen Risiko

Pengendalian umum berupa pendekatan sistematis yang meliputi budaya, proses, dan struktur untuk menentukan tindakan terbaik terkait kemungkinan terjadinya peristiwa yang berdampak negatif terhadap pencapaian tujuan Teknologi Informasi dan Komunikasi dan proses bisnis yang didukung Teknologi Informasi dan Komunikasi.

b) Manajemen Perubahan

Pengendalian umum berupa proses untuk meminimalkan dampak negatif akibat adanya perubahan (penambahan, perubahan/ modifikasi, pemindahan, atau pengurangan) komponen konfigurasi Teknologi Informasi dan Komunikasi, diantaranya perangkat keras, perangkat lunak, perangkat jaringan dan dokumen terkait dengan perubahan.

c) Akses logikal

Pengendalian umum berupa alat dan protokol yang bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi, khususnya perangkat pengolah informasi.

d) Operasional Teknologi Informasi dan Komunikasi dan Kelangsungan Layanan.

Pengendalian umum berupa pengelolaan operasional yang bertujuan untuk memastikan operasional yang aman dan benar pada perangkat pengolah informasi, mengimplementasikan dan memelihara keamanan informasi, mengelola layanan yang diberikan pihak ketiga, meminimalkan risiko kegagalan, melindungi keutuhan dan ketersediaan informasi dan perangkat lunak, memastikan keamanan pertukaran informasi, dan pemantauan terhadap proses operasional.

www.peraturan.go.id

Dalam konteks pelaporan keuangan, kebijakan terkait rancangan dan penerapan pengendalian umum Teknologi Informasi dan Komunikasi tidak seluruhnya menjadi kewenangan Entitas Akuntansi dan Entitas Pelaporan di semua tingkatan. Pada umumnya, dalam suatu sistem akuntansi tertentu, Entitas Akuntansi hanya bertindak sebagai pengguna atau operator aplikasi sehingga memiliki kewenangan yang terbatas dalam pembuatan kebijakan. Sebagian besar kewenangan berada pada Entitas Pelaporan yang menyusun dan mengembangkan sistem akuntansi dan aplikasi pendukungnya. Oleh karena itu, penerapan PUTIK juga perlu disesuaikan dengan kewenangan yang dimiliki oleh setiap Entitas Akuntansi dan Entitas Pelaporan berdasarkan ketentuan peraturan perundang-undangan yang berlaku.

2. Pengendalian Intern Tingkat Proses/Transaksi

Pengendalian Intern Tingkat Proses/Transaksi adalah pengendalian yang dirancang dan diimplementasikan untuk memitigasi risiko-risiko dalam pemrosesan transaksi secara spesifik. Pengendalian ini hanya terkait dan berdampak terhadap satu/sekelompok proses, transaksi, akun, atau asersi tertentu. Penerapan pengendalian ini perlu dilakukan baik terhadap pemrosesan transaksi secara manual maupun otomatis (misalnya menggunakan aplikasi berbasis sistem informasi), dan meliputi aspek *Input*, proses, dan *Output*. Dalam merancang Pengendalian Intern Tingkat Proses/Transaksi, suatu organisasi/sebaiknya berfokus pada akun atau kelompok akun signifikan. Akun atau kelompok akun merupakan akun signifikan apabila memiliki kemungkinan salah saji yang material, atau menurut pertimbangan manajemen perlu dievaluasi karena alasan tertentu. Penentuan akun atau kelompok akun signifikan merupakan kewenangan manajemen dan dapat bersifat *judgement*. Selanjutnya seluruh proses yang mempengaruhi akun atau kelompok akun signifikan tersebut harus diidentifikasi, termasuk proses yang melibatkan Teknologi Informasi dan Komunikasi. Dengan mengacu pada asersi manajemen atas laporan keuangan,

www.peraturan.go.id

setiap proses tersebut selanjutnya diidentifikasi risiko-risiko atau apa yang bisa salah dalam pelaksanaannya. Proses identifikasi risiko sebaiknya berfokus pada risiko-risiko utama, yaitu risiko-risiko yang apabila tidak dimitigasi dengan pengendalian yang memadai, dapat menyebabkan kesalahan material dalam laporan keuangan. Pengendalian yang dibangun dan diterapkan harus mampu mencegah dan mendeteksi risiko-risiko dimaksud. Untuk setiap risiko utama, setidaknya harus terdapat satu pengendalian utama yang terkait.

Pengendalian aplikasi (*application control*). Penggunaan sistem aplikasi dalam penyusunan laporan keuangan mempunyai banyak kelebihan, baik dari segi efisiensi proses maupun dari segi kualitas hasil, dibandingkan dengan proses manual. Akan tetapi, masih terdapat risiko sistem aplikasi yang digunakan tidak mampu berfungsi atau menghasilkan *output* sesuai dengan yang diharapkan. Oleh karena itu, pengendalian intern pada tingkat proses/transaksi juga perlu dirancang dan diimplementasikan secara khusus terhadap penggunaan aplikasi terkomputerisasi. Meskipun setiap aplikasi membutuhkan pengendalian yang spesifik dan unik, tujuan utama pengendalian aplikasi, khususnya dalam rangka penyusunan laporan keuangan, adalah untuk memastikan kelengkapan dan akurasi data, serta validitas dari pencatatan yang di-*input* ke dalam aplikasi. Pengendalian aplikasi dapat berbentuk pengendalian manual maupun terprogram/otomatis. Di samping itu, pengendalian aplikasi harus mencakup keseluruhan sistem mulai dari *input*, proses, hingga *output*. Sedangkan berdasarkan tahapan prosesnya, tujuan pengendalian aplikasi dapat diuraikan sebagai berikut:

a) Tahap penyiapan dan otorisasi data sumber. Tujuan pengendalian pada tahap ini diarahkan untuk memastikan bahwa dokumen-dokumen sumber telah disiapkan oleh pejabat/pegawai yang memiliki kewenangan dan kualifikasi sesuai dengan peraturan dan Standar Prosedur Operasional (SOP) yang telah ditetapkan. Di samping itu, pengendalian harus mampu meminimalisasi kesalahan *input* serta

www.peraturan.go.id

mendeteksi kesalahan yang terjadi sehingga dapat dilakukan tindakan perbaikan.

b) Tahap pengumpulan dan *input* data sumber. Tujuan pengendalian pada tahap ini diarahkan untuk memastikan bahwa *input* data dilaksanakan secara tepat waktu. Dalam hal terjadi perbaikan atau koreksi atas data yang telah di *input*, mekanisme perbaikan atau koreksinya harus tetap melalui tahapan otorisasi yang telah ditetapkan.

c) Tahap pengecekan akurasi, kelengkapan, dan otentisitas. Tujuan pengendalian pada tahap ini diarahkan untuk memastikan bahwa transaksi telah akurat, lengkap dan valid.

d) Tahap validitas dan integritas pemrosesan. Tujuan pengendalian pada tahap ini diarahkan untuk memastikan bahwa kemampuan aplikasi untuk mendeteksi kesalahan dalam transaksi tidak mengganggu pemrosesan transaksi yang benar dan valid.

e) Tahap reviu *output*, rekonsiliasi, dan penanganan kesalahan. Tujuan pengendalian pada tahap ini diarahkan untuk memastikan bahwa *output* aplikasi telah digunakan sesuai dengan kewenangan dan telah disampaikan kepada pihak-pihak yang tepat, serta memastikan bahwa proses verifikasi, deteksi, dan koreksi terhadap akurasi *output* aplikasi telah dilaksanakan.

f) Tahap keautentikan dan integritas *output*. Tujuan pengendalian pada tahap ini diarahkan untuk memastikan keautentikan dan integritas data selama proses transfer data antar aplikasi (termasuk antar modul atau menu dalam satu aplikasi yang sama), apabila *output* dari suatu aplikasi menjadi *output* antara atau *input* bagi aplikasi lain dalam rangka penyusunan laporan keuangan.

e. Dokumentasi Penerapan Pengendalian Intern atas Pelaporan Keuangan

Setiap Entitas Akuntansi dan Entitas Pelaporan bertanggung jawab untuk mengelola, penerapan PIPK. memelihara, dan memutakhirkan dokumentasi Dokumentasi penerapan PIPK secara umum mempunyai beberapa fungsi, antara lain:

www.peraturan.go.id

1. Sebagai rekaman seluruh proses kegiatan yang telah terjadi;
2. Sebagai dasar pengambilan keputusan di masa mendatang;
3. Sebagai bukti hukum atas apa yang telah diputuskan dan dilaksanakan, khususnya bila terjadi sengketa hukum; dan
4. Sebagai sarana pembelajaran untuk melakukan pemantauan dan kaji ulang.

Hal-hal yang perlu diperhatikan dalam pelaksanaan dokumentasi, yaitu:

1. Penataan dokumentasi sedemikian rupa sehingga informasi mudah diakses dan termutakhirkan dengan baik;
2. Pengamanan dokumentasi agar terjaga dari kemungkinan pencurian atau akses oleh pihak yang tidak berwenang;
3. Pemenuhan persyaratan dokumen yang memerlukan keabsahan hukum tertentu; dan
4. Penyimpanan dokumen orisinil dan masa retensi sesuai peraturan yang berlaku.

Dokumentasi mencakup rancangan, penerapan, dan mekanisme evaluasi pengendalian intern atas pelaporan keuangan yang tercermin dalam Petunjuk Teknis, Standar Prosedur Operasional (SOP), kebijakan administratif, pedoman akuntansi, dan pedoman lainnya, termasuk dokumentasi yang menggambarkan sistem informasi otomatis, pengumpulan dan penanganan data, serta pengendalian umum dan pengendalian aplikasi. Bentuk dan format dokumentasi disesuaikan dengan kebutuhan dan ketentuan yang berlaku di setiap Entitas Akuntansi dan Entitas Pelaporan. Untuk tujuan kemudahan, keseragaman, atau tujuan lain, Entitas Pelaporan dapat menetapkan peraturan tentang bentuk dan format dokumentasi yang harus dibuat oleh Entitas Akuntansi dan/atau Entitas Pelaporan yang secara organisatoris berada di bawahnya. Salah satu dokumentasi penerapan Pengendalian Intern atas Pelaporan Keuangan adalah dokumentasi identifikasi risiko dan kecukupan rancangan pengendaliannya sebagaimana tabel A dari kolom 1 sampai dengan kolom 9.

www.peraturan.go.id

- 11 -

Tabel A. Identifikasi Risiko dan Kecukupan Rancangan Pengendaliannya (Matriks Risiko-Pengendalian)

Nama Entitas Akuntansi/Pelaporan:

Akun Signifikan: diisi dengan akun-akun signifikan terkait

Diisi oleh Pemilik Pengendalian									Disi oleh Tim Penilai
No	Proses/ Transaksi Utama	Risiko Utama	Nama Pengendalian Utama	Aplikasi pendukung	Pelaksana Pengendalian	Dokumen Pendukung	Tipe Pengendalian	Asersi	Memadai Ya/Tidak
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Paraf Pemilik Pengendalian/Tanggal: Simpulan : Cukup/Tidak Cukup* Usulan koreksi *(feed back)* ** Penilaian Kelemahan Rancangan bila manajemen tidak memperbaiki*** 1. Proses/Transaksi Utama ..... : ..... 2. Dst. Paraf Tim Penilai/Tanggal:									

Keterangan:

Kolom (1) s.d. (9) diisi oleh Pemilik Pengendalian sedangkan Kolom (10), *, dan ** diisi Tim Penilai.

(1) Diisi nomor urut.

(2) Diisi proses/transaksi utama yang terkait akun signifikan tersebut

(3) Diisi risiko utama pada proses atau transaksi

(4) Diisi dengan Nomor pada kolom (1) diikuti tanda hubung (-) diikuti bentuk aktivitas pengendalian seperti pengendalian akses, pemeriksaan fisik, persetujuan, reviu atas persetujuan, validasi, monitoring, inventarisasi, penelitian lebih lanjut, klarifikasi, verifikasi keakuratan akun, rekonsiliasi. Contoh: 1-Validasi, 2-Rekonsiliasi, 3-Validasi, 4-Monitoring, 5-Klarifikasi, 6-Rekonsiliasi, 7-Validasi, dll.

Catatan: Perhatikan contoh terdapat 3 (tiga) validasi yang dibedakan satu sama lain dengan nomor sehingga terdapat Nama Pengendalian Utama 1-Validasi, 3-Validasi, dan 7-Validasi.

www.peraturan.go.id

(5) Diisi aplikasi yang khusus, misal: Sistem Informasi Manajemen dan Akuntansi Barang Milik Negara (SIMAK BMN), Sistem Perbendaharaan dan Anggaran Negara (SPAN), dll.

(6) Diisi pemilik pengendalian.

(7) Diisi dokumen terkait, misal: kuitansi, kontrak, Surat Perintah Membayar (SPM), dll.

(8) Diisi dengan tipe pengendalian dengan rincian:
   a. Manual
   b. Aplikasi
   c. ITDM (IT *Dependent Manual*)
   d. Pengendalian Umum TIK

(9) Diisi jenis asersi terkait: *Completeness, Existence and Occurance, Valuation and Allocation, Rights and Obligation, Presentation and Disclosure*.

(10) Diisi dengan "Ya" bila ada pengendalian utama (5) yang memitigasi risiko utama (3).

(*) Bila seluruh Risiko Utama ada pengendalian utamanya maka disimpulkan "Cukup", bila ada yang tidak ada pengendalian utamanya maka disimpulkan "Tidak Cukup".

(**) Bila rancangan disimpulkan "Tidak Cukup" berikan usulan koreksi (*feed back*) untuk melakukan koreksi.

(***) Bila manajemen tidak memperbaiki sesuai usulan rekomendasi Tim Penilai.

PEDOMAN PENILAIAN PENGENDALIAN INTERN ATAS PELAPORAN KEUANGAN DI LINGKUNGAN KEMHAN DAN TNI

a. Pendahuluan

Pentingnya Penilaian Pengendalian Intern atas Pelaporan Keuangan di samping perancangan dan penerapan, manajemen juga bertanggung jawab terhadap penilaian PIPK. Mengingat pelaporan keuangan merupakan muara semua pencatatan transaksi keuangan dalam suatu organisasi, maka penilaian PIPK merupakan kegiatan yang sangat penting. Melalui penilaian ini diharapkan manajemen mendapatkan informasi dan umpan balik mengenai pengendalian yang dijalankan. Berdasarkan informasi dan umpan balik tersebut, manajemen dapat

www.peraturan.go.id

mengetahui apakah pengendalian telah dirancang secara memadai dan telah diimplementasikan secara efektif sesuai dengan rencana. Selain informasi mengenai efektivitas pengendalian intern, kegiatan penilaian juga perlu mengungkapkan kelemahan-kelemahan pengendalian yang ditemukan serta saran perbaikannya. Berdasarkan informasi tersebut, manajemen melakukan perbaikan, penyesuaian, dan pengembangan sistem pengendalian yang ada agar lebih efektif. Pedoman penilaian PIPK perlu disusun untuk dapat dilaksanakan oleh Entitas Akuntansi dan Entitas Pelaporan yang melaksanakan PIPK.

b. Definisi Dalam pedoman ini, istilah-istilah penting yang digunakan didefinisikan sebagai berikut:

1) Pengendalian Intern atau Sistem Pengendalian Intern adalah proses yang integral pada tindakan dan kegiatan yang dilakukan secara terus menerus oleh pimpinan dan seluruh pegawai untuk memberikan keyakinan memadai atas tercapainya tujuan organisasi melalui kegiatan yang efektif dan efisien, keandalan pelaporan keuangan, pengamanan aset negara, dan ketaatan terhadap peraturan perundang-undangan.

2) *Control Self Assessment* (CSA) adalah proses penilaian efektivitas pengendalian intern yang dilakukan oleh manajemen. Tujuannya adalah memberikan asurans yang memadai bahwa tujuan organisasi dapat dicapai.

3) Kegiatan pengendalian (*control activities*) adalah kebijakan/prosedur untuk memastikan bahwa arahan manajemen telah dilaksanakan pada seluruh tingkatan dan fungsi dalam suatu entitas. Kegiatan pengendalian dilaksanakan antara lain melalui pemberian persetujuan (*approvan)*, otorisasi (*authorization*), verifikasi (*verification*), reviu atas kinerja operasi (*review of operating performance*), pengamanan aset (*security of asset*), dan pemisahan tugas (*segregation of duties*).

4) Pengendalian utama (*key control*) adalah pengendalian yang ketika dievaluasi dapat memberikan kesimpulan tentang kemampuan keseluruhan sistem pengendalian intern dalam mencapai tujuan kegiatan yang ditetapkan.

www.peraturan.go.id

5) Kelemahan adalah pelanggaran dan/atau penyimpangan terhadap penerapan pengendalian intern, baik berupa tidak dijalankannya pengendalian yang sudah ditetapkan, tidak diidentifikasinya risiko yang signifikan, atau tidak dibuatnya suatu pengendalian yang diperlukan.

6) Pemilik pengendalian (*control owner*) adalah pejabat pada tiap jenjang unit kerja yang bertanggung jawab atas terlaksananya suatu pengendalian di unit kerjanya, biasanya adalah atasan langsung pelaksana pengendalian.

7) Pengendalian preventif adalah pengendalian yang dirancang untuk menghindari kejadian yang tidak diharapkan atau kesalahan yang antara lain meliputi: pemberian persetujuan (*approvan*), otorisasi (*authorization*), pengamanan aset (*security of asset*), dan pemisahan tugas (*segregation of duties*).

8) Pengendalian detektif adalah pengendalian yang dirancang untuk menemukan kejadian yang tidak diharapkan atau kesalahan yang antara lain meliputi rekonsiliasi (*reconciliation*), verifikasi (*verification*), dan reviu atas kinerja operasi (*review of operating performance*).

9) Atribut pengendalian adalah karakteristik/ciri khusus yang melekat pada pengendalian atau bukti yang menunjukkan bahwa pengendalian telah dilaksanakan, seperti berita acara rekonsiliasi, paraf, tanda tangan, dan tanda centang.

10) Pengambilan uji petik atribut (*attribute sampling*) adalah metode pengambilan uji petik yang digunakan untuk meneliti sifat non angka dari data. Metode ini digunakan dalam pengujian pengendalian karena fokus perhatian pengujian pengendalian adalah pada jejak-jejak pengendalian yang terdapat pada data/dokumen yang diuji, seperti paraf, tanda tangan, nomor urut pracetak, bentuk formulir, dan sebagainya, yang juga bersifat non angka.

c. Tujuan dan Sasaran Pedoman Tujuan pedoman ini adalah untuk memberikan panduan bagi manajemen Entitas Akuntansi dan Entitas Pelaporan yang melakukan penilaian PIPK. Pedoman juga dimaksudkan untuk digunakan sebagai acuan bagi APIP dalam melaksanakan

www.peraturan.go.id

kegiatan asistensi kepada Entitas Akuntansi dan Entitas Pelaporan untuk mengembangkan pelaksanaan penilaian PIPK. Di samping itu, pedoman ini juga dapat dijadikan sebagai salah satu acuan dan kriteria bagi APIP dalam pelaksanaan reviu atas PIPK. Pedoman ini harus dilaksanakan untuk mencapai sasaran terwujudnya:

1) kesamaan pengertian, bahasa, dan penafsiran atas penilaian PIPK;
2) keseragaman perangkat penilaian PIPK; dan
3) efektivitas PIPK di lingkungan Kemhan dan TNI.

d. Pendekatan *Control Self Assessment* Proses penilaian PIPK dilaksanakan dengan pendekatan penilaian mandiri/*Control Self Assessment* (CSA). *Control Self Assessment* adalah sebuah proses menilai efektivitas pengendalian intern yang bertujuan untuk memberikan keyakinan yang memadai bahwa tujuan organisasi dapat tercapai. Dalam pelaksanaannya, teknik *Control Self Assessment* ini dilaksanakan sendiri oleh pihak manajemen sehingga memungkinkan keterlibatan manajemen secara penuh dalam proses penilaian pengendalian intern yang dilaksanakan dalam organisasinya. Hal ini dilatarbelakangi oleh pemikiran bahwa pihak yang paling memahami dan menguasai proses bisnis termasuk pengendalian intern dalam suatu organisasi adalah manajemen, mulai dari level pimpinan hingga pelaksana. Dengan demikian, diharapkan proses penilaian dapat berjalan secara cepat, efisien, dan efektif. Di samping itu, hasil penilaian diharapkan juga akan menjadi lebih komprehensif dan memberikan nilai tambah yang besar bagi organisasi karena berisi kelemahan yang kuat dan rekomendasi yang fokus pada tindakan perbaikan. Dalam praktiknya, teknik *Control Self Assessment* dapat dilaksanakan melalui beberapa cara, antara lain sebagai berikut:

1) *Workshop/Facilitated team meeting* dalam teknik ini, manajemen membentuk atau menunjuk sebuah tim yang terdiri dari para pejabat/pegawai di seluruh tingkatan dan bagian dalam organisasi yang memahami dan terlibat baik secara langsung maupun tidak langsung dalam pengendalian intern. Di samping itu, dibentuk pula seorang/tim fasilitator yang akan memimpin dan mengarahkan jalannya diskusi. Dalam konteks penilaian PIPK, tugas fasilitator dilaksanakan oleh Tim Penilai yang telah

www.peraturan.go.id

dibentuk. Diskusi dapat dilaksanakan dalam bentuk *Focused Group Discussion* (FGD) maupun bentuk lainnya.

2) Survei/wawancara/kuesioner Manajemen (dhi. Tim Penilai) melakukan survei dengan teknik wawancara maupun membuat kuesioner untuk diisi oleh seluruh pejabat/pegawai yang terkait dengan pengendalian intern. Pertanyaan yang diajukan melalui wawancara atau kuesioner sebaiknya disusun sesederhana mungkin sehingga mudah dipahami dan dijawab tanpa menimbulkan persepsi yang berbeda-beda, misalnya dalam bentuk pertanyaan "ya/tidak". Selanjutnya hasil survei dianalisis oleh Tim Penilai untuk memperoleh kesimpulan.

2. Perencanaan adalah langkah yang penting dalam setiap kegiatan, termasuk dalam proses penilaian PIPK. Dalam tahap ini, manajemen harus memutuskan ruang lingkup penilaian (meliputi: periode pelaporan keuangan dan komponen laporan keuangan mana yang akan dinilai pengendalian internnya), tingkat materialitas, dan jadwal penilaian beserta keputusan atau kebijakan penting lainnya. Penentuan ruang lingkup yang terlalu luas atau tingkat materialitas yang terlalu rendah akan berakibat pada pekerjaan penilaian pengendalian dan proses yang tidak perlu dan tidak penting bagi organisasi secara keseluruhan. Sebaliknya, penentuan ruang lingkup terlalu sempit atau menentukan tingkat materialitas terlalu tinggi akan berakibat minimnya pengujian dan ketidakmampuan menilai pengendalian intern secara memadai.

a. Struktur Organisasi Penilaian Pengendalian Intern Dukungan dari Menteri/Pengguna Anggaran dan Kuasa Pengguna Anggaran serta Penanggung Jawab Unit Akuntansi sangat penting dalam kesuksesan penilaian PIPK. Tim Penilai dibentuk pada Entitas Akuntansi dan Entitas Pelaporan sesuai dengan tingkat manajemen yang memberi pernyataan tanggung jawab. Pada Kemhan dan TNI, susunan Tim Penilai meliputi:

1) Tim Penilai Tingkat UAKPA;
2) Tim Penilai Tingkat UAPPA-W;
3) Tim Penilai Tingkat UAPPA-El; dan
4) Tim Penilai Tingkat UAPA. Tim Penilai Tingkat UAPA diketuai

www.peraturan.go.id

oleh Dirjen Renhan Kemhan (atas nama Menteri Pertahanan RI). Tim Penilai di bawahnya (selanjutnya disebut Tim Penilai) diketuai oleh Pejabat yang secara struktural berada satu tingkat di bawah dan ditunjuk langsung oleh pimpinan Entitas Akuntansi dan/atau Entitas Pelaporan yang membuat pernyataan tanggung jawab atas laporan keuangan.

b. Tugas dan Tanggung Jawab Tim Penilai

Tugas dan tanggung jawab Tim Penilai Tingkat UAPA dan Tim Penilai adalah membantu Menteri/ Pengguna Anggaran dan Kuasa Pengguna Anggaran untuk memantau implementasi PIPK dan meningkatkan kesadaran akan pengendalian intern dalam pelaporan keuangan. Proses penilaian ini tidak hanya berlangsung di tiap akhir semester atau pada saat penyusunan dan penyampaian laporan keuangan. Akan tetapi, kegiatan ini merupakan upaya terus menerus sepanjang tahun untuk mendokumentasikan, menilai, dan memantau pengendalian intern dan memperbaiki kelemahannya. Secara singkat, pemantauan dan peningkatan pengendalian intern merupakan proses yang terus menerus dan dilakukan secara paralel dengan penyusunan laporan keuangan. Meskipun demikian, unit kerja diharuskan melaporkan hasilnya secara tahunan.

Tanggung jawab Tim Penilai Tingkat UAPA setidaknya adalah:

1) menentukan lingkup penilaian yaitu laporan keuangan yang akan dinilai dan proses yang mempengaruhi laporan keuangan tersebut;
2) melakukan kompilasi dan menarik kesimpulan atas penilaian efektivitas pengendalian intern tingkat UAPA;
3) melaksanakan pemantauan tindak lanjut atas rekomendasi;
4) mengkoordinasikan kegiatan penilaian oleh Tim Penilai di bawahnya; dan
5) menyampaikan laporan kompilasi kepada pimpinan, APIP Kemhan, dan TNI.

Tanggung jawab Tim Penilai Tingkat UAPPA-El setidaknya adalah:

1) memetakan rancangan pengendalian;
2) menyusun desain penilaian pengendalian intern dan

www.peraturan.go.id

metodologinya;

3) menentukan batas materialitas pos yang akan diuji;
4) menyusun jadwal dan kebutuhan sumber daya penilaian;
5) melaksanakan penilaian pengendalian intern di unit kerjanya;
6) melakukan kompilasi dan menarik kesimpulan atas penilaian efektivitas pengendalian intern pada tingkat tersebut;
7) melaksanakan pemantauan tindak lanjut atas rekomendasi;
8) mengoordinasikan kegiatan penilaian oleh Tim Penilai di bawahnya;
9) menyampaikan laporan kepada pimpinan, APIP Kemhan, dan TNI; dan
10) memantau perkembangan tindakan perbaikan PIPK.

Tanggung jawab Tim Penilai Tingkat UAPPA-W setidaknya adalah:

1) menyusun jadwal dan kebutuhan sumber daya penilaian;
2) melaksanakan penilaian pengendalian intern di unit kerjanya;
3) melaksanakan pemantauan tindak lanjut atas rekomendasi;
4) mengoordinasikan kegiatan penilaian oleh Tim Penilai bawahnya;
5) menyampaikan laporan kepada Tim Penilai tingkat UAPPA-El; dan
6) memantau perkembangan tindakan perbaikan PIPK.

Tanggung jawab Tim Penilai Tingkat UAKPA setidaknya adalah:

1) menyusun jadwal dan kebutuhan sumber daya penilaian;
2) melaksanakan penilaian pengendalian intern di unit kerjanya;
3) melaksanakan pemantauan tindak lanjut atas rekomendasi;
4) menyampaikan laporan kepada Tim Penilai tingkat UAPPA-W sebagai dasar pembuatan pernyataan tanggungjawab; dan
5) memantau perkembangan tindakan perbaikan PIPK.

c. Keanggotaan Tanggung jawab penilaian PIPK tingkat UAPA berada pada Dirjen Renhan Kemhan, namun proses yang akan dinilai berada pada seluruh organisasi. Manajemen harus menggunakan pertimbangan profesionalnya dalam memilih anggota Tim Penilai dan harus mempertimbangkan untuk mengikutsertakan perwakilan dari seluruh bagian organisasi seperti bagian akuntansi/keuangan, bagian TIK, bagian umum, bagian sumber

www.peraturan.go.id

daya manusia, dan/atau APIP sebagai penasihat atau pemberi asistensi. Agar dapat melaksanakan penilaian dengan baik, diperlukan kualifikasi Tim Penilai sebagai berikut:

1) memiliki kompetensi teknis yang memadai (pemahaman yang baik terhadap proses bisnis yang dipantau, konsep pengendalian intern, dan teknik pemantauan);
2) memiliki sikap mental (kepribadian) yang baik, tercermin dari kejujuran, objektivitas, ketekunan, loyalitas, bijaksana, dan bertanggung jawab terhadap profesinya;
3) memiliki kemampuan berinteraksi dan berkomunikasi secara efektif baik lisan maupun tertulis dengan berbagai pihak di lingkungan unit organisasinya; dan
4) memiliki keinginan untuk maju dan menambah pengetahuan/ meningkatkan kemampuan profesionalnya.

Sumber Daya Manusia Tim Penilai harus memperoleh pelatihan yang cukup terkait teknis penilaian dan proses bisnis unit yang dinilai. Dalam kaitan dengan teknis penilaian, program pengembangan kompetensi yang diperlukan diantaranya meliputi pelatihan tentang:

1) konsep dasar pengendalian intern secara umum dan PIPK;
2) perancangan dan pengembangan perangkat penilaian PIPK;
3) mekanisme pelaksanaan tugas penilaian PIPK; dan
4) simulasi pelaksanaan tugas penilaian PIPK berdasarkan perangkat yang telah disusun.

d. Pendekatan Umum Penilaian Untuk dapat memberikan pernyataan tanggung jawab atas laporan keuangan berupa pernyataan bahwa laporan keuangan telah disusun berdasarkan sistem pengendalian intern yang memadai, manajemen harus menilai efektivitas PIPK untuk mendukung pernyataan tersebut. Agar dapat melakukan penilaian tersebut, pendekatan dari atas ke bawah (*Top-Down Approach*) harus digunakan dalam merencanakan penilaian PIPK. Penilaian PIPK dilakukan untuk memberikan jaminan pada tingkat entitas unit kerja. Pendekatan dari atas ke bawah dalam perencanaan, pengujian, dan pendokumentasian PIPK dimulai dengan laporan keuangan yang

www.peraturan.go.id

signifikan di level entitas dan ditelusuri sampai ke proses utama pengendalian, dan dokumen pendukungnya. Tim Penilai Tingkat UAPA akan menentukan ruang lingkup pelaporan keuangan, desain penilaian pengendalian intern dan metodologinya, serta penentuan batas materialitas pos yang akan diuji. Manajemen memiliki fleksibilitas dalam menentukan laporan keuangan signifikan yang akan diuji pengendaliannya. Tim Penilai Tingkat UAPA akan mengkomunikasikan prosedur tersebut ke seluruh unit organisasi dan memantau kemajuan Entitas Akuntansi atau Entitas Pelaporan dalam menjalankan strategi yang telah ditetapkan.

e. Koordinasi dengan unit lain di dalam dan luar organisasi satuan kerja di pemerintahan memiliki ketentuan dan peraturan yang mendukung implementasi pengendalian intern yang efektif. Sebagai contoh, beberapa reviu dan/atau pemantauan juga dilakukan oleh manajemen atau atas nama manajemen sepanjang tahun. Tim Penilai dalam setiap tingkatan harus mempertimbangkan penggunaan hasil reviu atau pemantauan yang telah dilakukan manajemen agar tidak tumpang tindih. Tim Penilai dalam setiap tingkatan juga harus mempertimbangkan hasil asurans dari pemberi asurans lainnya baik dari APIP maupun auditor eksternal. Tim Penilai dan Manajemen harus:

   1) memahami perspektif APIP/auditor eksternal untuk mengetahui apakah penentuan akun signifikan, proses/transaksi utama, dan asersi tertentu sejalan dengan hasil identifikasi APIP/auditor eksternal. Perbedaan mungkin saja terjadi, seperti perbedaan karena tingkat materialitas. Pada umumnya, materialitas yang ditetapkan manajemen atau Tim Penilai akan lebih rendah dari materialitas yang ditetapkan oleh APIP/auditor eksternal.
   2) memfasilitasi pertukaran informasi jika memungkinkan antara manajemen dan APIP/auditor eksternal berkenaan dengan pemahaman bersama terhadap PIPK sehingga diperoleh pemahaman yang komprehensif.
   3) mengoordinasikan waktu pengujian pengendalian untuk

www.peraturan.go.id

mencegah tumpang tindih dengan pengujian pengendalian oleh APIP/auditor eksternal dalam rangka reviu/ audit.

4) membandingkan hasil penilaian PIPK dengan hasil pengujian pengendalian intern dalam laporan hasil audit atas laporan keuangan oleh auditor eksternal.

f. Penentuan ruang lingkup pelaporan keuangan tim penilai tingkat UAPA harus merekomendasikan kepada manajemen ruang lingkup laporan keuangan yang akan dinilai pengendalian internnya termasuk pemilihan akun-akun signifikan. Manajemen memutuskan ruang lingkup berupa periode dan komponen-komponen laporan keuangan termasuk akun-akun signifikan. Periode penilaian minimal adalah laporan keuangan semesteran. Sedangkan komponen laporan keuangan yang akan dinilai dan kedalaman penilaiannya diserahkan kepada manajemen sesuai dengan risiko proses dan pengendalian intern yang akan diuji. Untuk Entitas Pelaporan yang melakukan proses konsolidasi atas laporan keuangan unit-unit di bawahnya, maka proses konsolidasi dan laporan keuangan konsolidasian juga harus dinilai oleh Tim Penilai.

g. Penentuan Materialitas dalam pelaporan keuangan adalah risiko kesalahan atau salah saji yang dapat terjadi dalam laporan keuangan yang akan berpengaruh terhadap keputusan atau kesimpulan yang diambil berdasarkan laporan keuangan tersebut. Manajemen harus mempertimbangkan sejauh mana suatu kesalahan akan mempengaruhi manajemen atau proses pelaporan keuangan. Penentuan tingkat materialitas merupakan kewenangan dan pertimbangan profesional manajemen. Oleh karena itu, manajemen harus mempertimbangkan proses bisnis utama yang akan berpengaruh terhadap pelaporan keuangan. Manajemen harus mempertimbangkan kemungkinan dari salah saji laporan keuangan secara individual atau gabungan. Nilai materialitas yang diperoleh merupakan besarnya kesalahan yang mempengaruhi pertimbangan pengguna laporan keuangan. Penetapan nilai materialitas secara kuantitatif meliputi tahapan sebagai berikut:

www.peraturan.go.id

1) Penentuan Dasar (Basis) Penetapan Materialitas Dalam memutuskan nilai yang akan dijadikan dasar, Tim Penilai sebaiknya mempertimbangkan beberapa hal, antara lain:
   a) karakteristik (sifat, besar dan tugas pokok) dan lingkungan entitas yang diperiksa;
   b) area dalam laporan keuangan yang akan lebih diperhatikan oleh pengguna laporan keuangan; dan
   c) kestabilan atau keandalan nilai yang akan dijadikan dasar.

   Dasar penetapan materialitas yang dapat digunakan oleh Tim Penilai adalah sebagai berikut:
   a) Total Aktiva, untuk entitas yang berbasis aktiva.
   b) Nilai aset bersih atau ekuitas, untuk entitas yang berbasis aset.
   c) Total pendapatan, untuk entitas yang fungsinya sebagai pusat penerimaan (*revenue center*); dan
   d) Total belanja, untuk entitas yang fungsinya sebagai pusat belanja (*cost center*).
2) Penentuan Tingkat (*Rate*) Materialitas, Contoh tingkat materialitas adalah sebagai berikut:
   a) Untuk entitas *revenue center* sebesar 0,5% (nol koma lima persen) sampai dengan 5% (lima persen) dari total penerimaan;
   b) Untuk entitas *cost center* sebesar 0,5% (nol koma lima persen) sampai dengan 5% (lima persen) dari total belanja; dan
   c) Untuk entitas yang berbasis aset sebesar 0,5% (nol koma lima persen) sampai 1 % (satu persen) dari total aset.

h. Penentuan Proses Bisnis Utama (*Key Business Processes*) yang Mendukung Akun Signifikan. Proses bisnis adalah dasar penilaian pengendalian intern dan mendukung saldo yang material di laporan keuangan. Proses bisnis merupakan serangkaian peristiwa, yang terdiri dari metode dan pencatatan yang digunakan untuk mengidentifikasi, mengelompokkan, menganalisis, dan

www.peraturan.go.id

mencatat transaksi-transaksi seperti penerimaan dan pengeluaran kas, penerimaan piutang dan Penerimaan Negara Bukan Pajak, pembelian barang persediaan, dan lain-lain. Ketika menentukan proses bisnis utama, manajemen harus mereviu laporan keuangan dan pengungkapan lainya baik melalui bagan alur (*flowchart*) proses maupun dokumen lain yang tersedia. Sementara itu, terdapat pula proses atau aplikasi yang digunakan untuk mencatat transaksi untuk memelihara akuntabilitas aset dan kewajiban. Proses tersebut biasanya berupa metode untuk melaporkan dan menunjukkan akuntabilitas seperti proses akuntansi piutang, persediaan, aset tetap, dan lain-lain. Manajemen harus memiliki pemahaman yang baik atas kedua jenis proses yang bermuara pada pelaporan keuangan tersebut di atas.

i. Asersi Pelaporan Keuangan.

Manajemen harus mengidentifikasi asersi laporan keuangan yang relevan pada akun signifikan. Asersi manajemen merupakan pernyataan manajemen tentang berbagai transaksi dan akun yang terkait dengannya dalam laporan keuangan. Asersi manajemen secara langsung terkait dengan prinsip-prinsip akuntansi yang berlaku umum. Asersi-asersi ini merupakan bagian dari kriteria yang digunakan oleh manajemen untuk mencatat serta mengungkapkan informasi akuntansi dalam laporan keuangan.

Terdapat beberapa macam asersi, yaitu:

1) Keberadaan atau keterjadian (*existence or occurrence*). Asersi tentang keberadaan atau keterjadian berhubungan dengan apakah aset, kewajiban, dan ekuitas yang tercantum dalam neraca memang benar-benar ada pada tanggal neraca. Berbagai asersi tentang keterjadian berkaitan dengan apakah berbagai transaksi yang tercatat dalam suatu laporan keuangan memang benar-benar terjadi selama periode akuntansi tersebut. Sebagai contoh, manajemen membuat asersi bahwa persediaan alat tulis kantor yang tercantum dalam neraca adalah tersedia untuk digunakan. Begitu pula, manajemen membuat asersi Penerimaan Negara Bukan Pajak

www.peraturan.go.id

dalam laporan operasional menunjukkan bahwa telah terjadi pertukaran barang atau jasa dengan kas atau aset bentuk lain (misalnya piutang) dengan pihak lain.

2) Kelengkapan (*completeness*). Asersi manajemen ini menyatakan bahwa seluruh transaksi dan akun yang seharusnya disajikan dalam laporan keuangan telah disajikan seluruhnya. Sebagai contoh, manajemen membuat asersi bahwa seluruh Penerimaan Negara Bukan Pajak telah dicatat dan dicantumkan dalam laporan keuangan. Demikian pula, manajemen membuat asersi bahwa piutang pajak di neraca telah mencakup semua piutang pajak yang dimiliki oleh entitas tersebut. Asersi kelengkapan berhubungan dengan berbagai masalah yang berlawanan dengan berbagai masalah yang terkait dengan asersai keberadaan atau keterjadian. Asersi kelengkapan berkaitan dengan kemungkinan adanya sejumlah item yang seharusnya tersaji, hilang sehingga tidak tercatat dalam laporan keuangan. Sementara asersi keberadaan atau keterjadian berkaitan dengan pencatatan sejumlah nilai yang seharusnya tidak tersaji dalam laporan keuangan. Berbagai pelanggaran atas asersi keterjadian ini banyak berhubungan dengan pencatatan nilai akun yang terlalu tinggi, sementara pelanggaran atas asersi kelengkapan banyak berhubungan dengan pencatatan nilai akun yang terlalu rendah. Sebagai contoh, pencatatan sebuah transaksi Penerimaan Negara Bukan Pajak yang fiktif merupakan suatu pelanggaran atas asersi keterjadian sedangkan kegagalan mencatat suatu transaksi Penerimaan Negara Bukan Pajak merupakan pelanggaran atas asersi kelengkapan.

3) Hak dan kewajiban (*right and obligation*). Asersi tentang hak dan kewajiban berhubungan dengan apakah pada tanggal tertentu, aset yang tercantum dalam laporan keuangan merupakan hak entitas dan utang merupakan kewajiban entitas. Sebagai contoh manajemen membuat asersi bahwa jumlah Penerimaan Negara Bukan Pajak telah mencerminkan nilai perolehan hak entitas atas pemberian jasa kepada pihak

www.peraturan.go.id

lain dan jumlah utang jangka panjang pemerintah mencerminkan suatu kewajiban pemerintah kepada pihak lain.

4) Penilaian atau alokasi (*valuation or allocation*). Asersi tentang penilaian atau alokasi berhubungan dengan apakah nilai-nilai yang tersaji pada akun aset, kewajiban, pendapatan dan beban dalam laporan keuangan merupakan nilai yang tepat. Sebagai contoh, manajemen membuat asersi bahwa aset tetap dicatat berdasarkan harga perolehannya dan perolehan semacam itu secara sistematis dialokasikan ke dalam periode-periode akuntansi yang semestinya. Demikian pula manajemen membuat asersi bahwa piutang PNBP yang tercantum di neraca dinyatakan berdasarkan nilai bersih yang dapat direalisasikan.

5) Penyajian dan pengungkapan (*presentation and disclosure*). Asersi tentang penyaJian dan pengungkapan berhubungan dengan apakah berbagai komponen dalam laporan keuangan telah digabungkan atau dipisahkan, diuraikan, dan diungkapkan dengan tepat. Misalnya, manajemen membuat asersi bahwa kewajiban-kewajiban yang diklasifikasikan sebagai utang jangka panjang di neraca merupakan utang yang jatuh temponya lebih dari satu tahun. Dari uraian di atas, hubungan akun signifikan dengan asersi laporan keuangan dapat dilihat contohnya pada tabel berikut:

No	Akun	Asersi yang relevan
1	Kas	*Existence* *completeness*
2	Penerimaan PNBP	*Existence* *completeness*
3	Utang Pemerintah	*Existence* *Right and obligation* *presentation and* *disclosure*
4	Piutang PNBP	*Existence* *Right and obligation*

www.peraturan.go.id

		Presentation and disclosure
5	Aset Tetap	*Existence* *Valuation or allocation*

Akun-akun yang lain dapat ditentukan asersi yang relevan sesuai dengan karakteristiknya.

j. Penilaian Risiko.

Penilaian risiko adalah proses intern dari manajemen untuk mengidentifikasi, menganalisis dan mengelola risiko untuk mencapai tujuan keandalan pelaporan keuangan. Manajemen harus menyiapkan ikhtisar risiko atas salah saji akun tertentu yang akan digunakan untuk merencanakan penilaian pengendalian internnya. Ikhtisar risiko tersebut setidaknya memuat daftar akun signifikan, saldonya, asersi laporan keuangannya dan risiko yang mungkin terjadi. Manajemen harus menilai pengendalian atau risiko dari setiap asersi, mendokumentasikan penilaian risiko, dan menyiapkan rencana pengujian.

k. Dokumentasi Pendokumentasian atau pemutakhiran proses utama dan pengendalian intern atas proses pelaporan keuangan harus disiapkan, termasuk proses yang menggunakan Teknologi Informasi dan Komunikasi. Pendokumentasian proses utama dan pengendaliannya merupakan awal proses pengambilan keputusan untuk menentukan proses penilaian selanjutnya.

1) Dokumentasi Rencana dan Metodologi

Tim Penilai harus mendokumentasikan metodologi penilaian, termasuk:

a) Penetapan kewenangan Tim Penilai dan anggotanya;
b) Metode komunikasi dengan manajemen dan pegawai selama penilaian; dan
c) Komponen penting dari metodologi penilaian.

2) Dokumentasi Hasil Penilaian Tim Penilai harus memiliki dokumentasi untuk mendukung hasil penilaian yang dilakukan. Tim Penilai harus secara jelas mengomunikasikan

www.peraturan.go.id

kepada seluruh pegawai prosedur yang dilakukan, bukti yang diperoleh, dan kesimpulan yang diambil berkenaan dengan PIPK.

Dokumentasi tersebut setidaknya memuat:

a) Informasi tentang bagaimana transaksi signifikan diidentifikasi, dicatat, diproses dan dilaporkan.
b) Informasi yang memadai tentang risiko salah saji dan kecurangan yang mungkin timbul dari proses/transaksi.
c) Pengendalian yang dirancang untuk mencegah dan mendeteksi kecurangan termasuk siapa yang melaksanakan pengendalian tersebut.
d) Pengendalian proses pelaporan keuangan pada akhir periode.
e) Pengendalian atas pengamanan aset.
f) Hasil penilaian PIPK.

3. Pengujian Pengendalian Intern Tingkat Entitas

a. Tujuan

Pengujian Pengendalian Intern Tingkat Entitas dilakukan terhadap pengendalian-pengendalian yang mempunyai pengaruh luas/menyebar ke seluruh kegiatan/proses pelaporan keuangan dalam suatu organisasi. Tujuan penilaian dimaksud adalah untuk menentukan efektivitas Pengendalian Intern Tingkat Entitas dalam menciptakan lingkungan yang mendukung efektivitas Pengendalian Intern Tingkat Proses/Transaksi.

b. Pelaksana dan Lingkup.

Pelaksana pengujian Pengendalian Intern Tingkat Entitas beserta lingkup objek yang dinilai adalah sebagai berikut:

1) Tim Penilai tingkat UAKPA menilai Pengendalian Intern Tingkat Entitas unit kerja UAKPA.
2) Tim Penilai tingkat UAPPA-W menilai Pengendalian Intern Tingkat Entitas unit kerja UAPPA-W.
3) Tim Penilai tingkat UAPPA-El menilai Pengendalian Intern Tingkat Entitas unit kerja UAPPA-El.

www.peraturan.go.id

4) Tim Penilai tingkat UAPA mengompilasi hasil penilaian pengendalian intern Tim Penilai di bawahnya dan menyimpulkan tingkat keandalan efektivitas Pengendalian Intern Tingkat Entitas K/L secara keseluruhan.

c. Waktu dan Proses Penilaian Pengendalian Intern Tingkat Entitas dilakukan setiap tahun namun pada tahun berikutnya dapat menggunakan hasil penilaian tahun sebelumnya apabila entitas dipandang tidak mengalami perubahan signifikan. Penggunaan hasil penilaian tahun sebelumnya ini hanya berlaku satu kali saja. Penilaian Pengendalian Intern Tingkat Entitas juga dilakukan apabila terdapat kondisi-kondisi yang dapat mempengaruhi Pengendalian Intern Tingkat Entitas, seperti perubahan kepemimpinan, perubahan proses bisnis yang strategis, perubahan struktur organisasi. Langkah-langkah penilaian Pengendalian Intern Tingkat Entitas adalah sebagai berikut:

1) Menyusun program kerja.

Program kerja harus mendefinisikan dengan jelas mengenai tujuan, ruang lingkup, teknik evaluasi, waktu pelaksanaan, dokumen/laporan yang dibutuhkan, Sumber Daya Manusia yang terlibat, serta cara penarikan simpulan.

2) Melaksanakan evaluasi.

Evaluasi dilakukan terhadap setiap faktor dari kelima unsur pengendalian intern dengan menggunakan salah satu atau kombinasi dari beberapa teknik sebagai berikut:

a) Reviu Dokumen

Reviu dokumen dilakukan dengan mempelajari dokumen-dokumen yang berhubungan dengan pelaksanaan unsur-unsur pengendalian intern.

b) Wawancara

Wawancara dilakukan melalui diskusi dengan

www.peraturan.go.id

pegawai yang bertanggung jawab terhadap rancangan atau implementasi pengendalian dalam rangka mengumpulkan bukti mengenai efektivitas pengendalian tingkat entitas. Wawancara dapat menjadi sarana mengumpulkan informasi kesesuaian pelaksanaan kebijakan dengan target yang diharapkan.

c) Survei

Survei dilakukan dengan mengajukan serangkaian pertanyaan tertulis untuk mendapatkan tanggapan dari pegawai/pejabat mengenai hal-hal terkait lima unsur pengendaian intern di dalam suatu unit kerja. Untuk menjaga keandalan dan validitas hasil survei, perlu diperhatikan beberapa hal yaitu:

1) uji coba dan perbaikan pertanyaan survei berdasarkan hasil uji coba;
2) banyaknya responden akan mempengaruhi keandalan hasil survei;
3) sampel yang distratifikasi akan menghasilkan hasil yang lebih bagus;
4) perlu pertimbangan matang ketika manajemen mengeluarkan suatu grup uji petik dari populasi.

d) Observasi.

Observasi dilakukan dengan mengamati secara cermat pegawai, kondisi lingkungan, dan pelaksanaan kegiatan di suatu unit kerja terkait dengan lima unsur pengendalian intern.

Penggunaan teknik tersebut di atas bersifat saling melengkapi sesuai dengan kebutuhan di lapangan. Tim Penilai dapat menggunakan salah satu atau kombinasi beberapa teknik sesuai dengan tingkat keyakinan yang

www.peraturan.go.id

dihasilkan dari penerapan teknik tersebut. Pengujian Pengendalian Intern Tingkat Entitas sebagaimana Tabel B.1 berikut ini:

Tabel B.1 Pengujian Pengendalian Intern Tingkat Entitas (Tim Penilai)

Nama Entitas Akuntansi/Pelaporan:

Faktor-Faktor yang Dinilai Tingkat Entitas			Reviu Dokumen (Y/T)	Wawancara (Y/T)	Survei (Y/T)	Observasi (Y/T)	Skor	Hasil Penelitian Lanjutan
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
Jumlah							(10)	
Total faktor relevan							(11)	
Persentase							(12)	

Keterangan:

(1) Diisi huruf besar atau angka

(2) Diisi huruf kecil

(3) Diisi faktor-faktor yang dinilai.

(4) Diisi Y jika hasil reviu dokumen menunjukkan faktor yang dinilai ada, diisi T faktor yang dinilai tidak ada, atau diisi N/A jika faktor yang dinilai tidak relevan dengan kondisi yang ada.

(5) Diisi Y jika hasil wawancara menunjukkan faktor yang dinilai ada, diisi T faktor yang dinilai tidak ada, atau diisi N/A jika faktor yang dinilai tidak relevan dengan kondisi yang ada.

(6) Diisi Y jika hasil survei menunjukkan faktor yang dini lai ada, diisi T faktor yang dinilai tidak ada, atau diisi N/A jika faktor yang dinilai tidak relevan dengan kondisi yang ada.

(7) Diisi Y jika hasil observasi menunjukkan faktor yang dinilai ada, diisi T faktor yang dinilai tidak ada atau diisi N/A jika factor yang dinilai tidak relevan dengan kondisi yang ada.

(8) Diisi 1 jika simpulannya faktor yang dinilai ada atau diisi 0 jika simpulannya faktor yang dinilai tak ada, atau diisi

www.peraturan.go.id

N/A jika faktor yang dinilai tidak relevan dengan kondisi yang ada.

(9) Penelitian Lanjutan hanya dilakukan bila skor bernilai 0. Penelitian Lanjutan dilakukan dengan memperhatikan ketiadaan *compensating control* terkait dan/atau adanya bukti bahwa kelemahan tersebut telah dieksploitasi yang mendukung simpulan adanya Kelemahan Signifikan.
Diisi dengan "Tidak Ada Kelemahan/Kelemahan Tidak Signifikan/Kelemahan Signifikan/Kelemahan Material"

(10) Diisi dengan jumlah faktor-faktor yang memiliki skor "l"

(11) Diisi dengan total -faktor yang relevan.

(12) Diisi dengan jumlah faktor-faktor yang memiliki skor "l" dibagi total faktor yang relevan dikali 100%.

Faktor - Faktor yang Dinilai Tingkat Entitas		
(1)	(2)	(3)
A		LINGKUNGAN PENGENDALIAN
1		Integritas, nilai etika, dan perilaku etis
	a	Apakah telah dilakukan sosialisasi yang memadai tentang kewajiban, larangan, dan sanksi dalam kode etik dan/atau aturan perilaku lainnya, termasuk kepada pegawai baru?
	b	Apakah pimpinan unit kerja memberi keteladanan dengan menerapkan integritas dan nilai-nilai etika dan mendorong bawahan untuk menerapkannya pula?
	c	Apakah pimpinan unit kerja memberikan sanksi kepada pegawai yang melanggar kode etik dan/atau aturan perilaku lainnya?
	d	Apakah pegawai mengetahui kewajiban dan larangan serta sanksi pelanggaran kode etik dan/atau aturan perilaku lainnya?
2		Kesadaran pimpinan unit kerja atas pengendalian dan gaya operasi yang dimiliki oleh pimpinan unit kerja
	a	Apakah pimpinan unit kerja memiliki sikap yang selalu mempertimbangkan risiko dalam pengambilan keputusan?

www.peraturan.go.id

	b	Apakah pimpinan unit kerja mendorongpenerapan pengendalian intern di unit kerjanya?
	c	Apakah pimpinan unit kerja memiliki sikap yang positif dan *responsive* terhadap pencapaian tujuan kegiatan/organisasi?
	d	Apakah pimpinan unit kerja memandang penting dan menindaklanjuti hasil pengawasan aparat pengawas intern, pengaduan, keluhan, pertanyaan dari pegawai dan masyarakat?
3		Komitmen terhadap kompetensi
	a	Apakah terdapat proses untuk memastikan bahwa pegawai yang terpilih untuk menduduki suatu jabatan telah memiliki pengetahuan, keahlian , dan kemampuan yang diperlukan?
	b	Apakah unit kerja menyelenggarakan pelatihan dan pembimbingan untuk mempertahankan dan meningkatkan kompetensi pegawai?
4		Struktur organisasi serta penetapan wewenang dan tanggung jawab
	a	Apakah pimpinan dan pegawai mengetahui dan melaksanakan tugas, wewenang dan tanggung jawabnya?
	b	Apakah wewenang diberikan kepada pegawai yang tepat sesuai dengan tingkat tanggung jawabnya dalam rangka pencapaian tujuan unit kerja?
	c	Apakah pimpinan dan pegawai mengetahui dan bertanggung jawab atas pengendalian intern yang menjadi tanggung jawabnya?
	d	Apakah jumlah pejabat/pegawai dalam suatu unit kerja telah sesuai dengan analisis beban kerja?
5		Kebijakan dan oraktik yang berkaitan dengan Sumber Daya Manusia
	a	Apakah kebijakan dan praktik pembinaan sumber daya manusia pada unit kerja telah disosialisasikan dan diperbaharui secara terus menerus?
	b	Apakah pimpinan unit kerja memberikan panduan, penilaian, dan pelatihan kepada pegawai untuk memastikan ketepatan pelaksanaan pekerjaan, mengurangi kesalahpahaman, serta mendorong berkurangnya tindakan pelanggaran?
	c	Apakah sudah dilaksanakan pemilihan diklat yang mengacu pada pedoman pelaksanaan diklat berbasis kompetensi?
	d	Apakah sudah ada keterkaitan diklat yang dilaksanakan dengan

www.peraturan.go.id

		pembinaan karir dan kinerja pegawai?
	e	Apakah pemberian sanksi telah dijalankan sesuai dengan kebijakan dan prosedur yang berlaku
B		PENILAIAN RISIKO
1		Sasaran unit kerja telah disusun dan dikomunikasikan
		Apakah sasaran unit kerja telah dikomunikasikan kepada
		seluruh pegawai?
2		Telah dilakukan penilaian risiko yang meliputi perkiraan signifikansi dari suatu risiko, penilaian kemungkinan terjadinya, dan penanganannya
	a	Apakah unit kerja telah mengidentifikasi risiko dalam pencapaian tujuan?
	b	Apakah unit kerja telah menganalisis dan mengevaluasi risiko dalam pencapaian tujuan?
	c	Apakah unit kerja telah melakukan penanganan risiko dalam pencapaian tujuan?
3		Adanya mekanisme untuk mengantisipasi, mengidentifikasi, dan bereaksi terhadap perubahan yang dapat menghasilkan dampak besar dan menyebar pada unit keria
		Apakah ada mekanisme untuk mengantisipasi, mengidentifikasi, dan bereaksi terhadap perubahan yang dapat menghasilkan dampak besar dan menyebar pada unit kerja?
C		KEGIATAN PENGENDALIAN
1		Kebijakan dan prosedur yang dibutuhkan untuk pengendalian setiap kegiatan telah diterapkan secara tepat
	a	Apakah telah dilakukan perbandingan antara kinerja yang direncanakan dengan kinerja yang dicapai setiap pegawai?
	b	Apakah laporan pencapaian kinerja telah disampaikan tepat waktu kepada pimpinan?
2		Evaluasi atas perbedaan capaian kinerja dan pelaksanaan tindakan perbaikan yang tepat serta tepat waktu
	a	Apakah unit kerja telah melaksanakan evaluasi atas pencapaian

www.peraturan.go.id

		Indikator Kinerja Utama?
	b	Apakah ada tindak lanjut atas perbedaan capaian kinerja dengan kineria yang direncanakan?
3		Adanya pemisahan atau pembagian tugas kepada pihak yang berbeda untuk mengurangi risiko kecurangan atau tindakan yang tidak layak
		Apakah pimpinan unit kerja telah memperhatikan pemisahan tugas *(segregation of duties)* untuk mengurangi risiko terjadinya kecurangan atau tindakan yang tidak layak?
4		Pembatasan akses terhadap dokumen, catatan, asset, data, dan aplikasi
		Apakah unit kerja telah mengatur pembatasan akses atas aset dan aplikasi yang dimiliki?
5		Adanya mekanisme otorisasi dan persetujuan terhadap transaksi dan kejadian penting
		Apakah unit kerja telah memiliki mekanisme otorisasi dan Persetujuan (*approval)* atas transaksi dan kejadian penting?
6		Dokumentasi yang baik atas kegiatan
		Apakah pelaksanaan kegiatan telah didukung dengan dokumentasi yang cukup dan tepat waktu?
D		INFORMASI DAN KOMUNIKASI
1		Sistem menyediakan informasi yang dibutuhkan oleh unit kerja terkait baik informasi yang berasal dari dalam dan luar unit kerja secara akurat
		Apakah informasi yang diperlukan dalam pelaksanaan kegiatan telah tersedia secara tepat waktu, akurat dan disampaikan kepada pihak yang tepat?
2		Informasi tersedia bagi orang yang tepat dalam rincian yang cukup dan tepat waktu
		Apakah informasi yang diperlukan bagi orang yang tepat dalam rincian yang cukup dan tepat waktu?
3		Sistem informasi dikembangkan atau diperbaiki dengan berdasar pada rencana strategis unit keria

www.peraturan.go.id

		Apakah unit kerja mengelola, mengembangkan, dan memperbarui sistem informasi untuk meningkatkan kegunaan dan keandalan komunikasi informasi secara terus menerus?
4		Unit kerja memastikan dan mengawasi keterlibatan pengguna dalam pengembangan, perbaikan, dan pengujian program/sistem informasi
	a	Apakah seluruh pegawai telah menggunakan program/sistem informasi terkait dengan tugasnya?
	b	Apakah pegawai sebagai *end user* telah diminta masukan dalam pengembangan, perbaikan dan pengujian program/sistem informasi?
	c	Apakah unit kerja menindaklanjuti saran dan masukan dari pegawai terkait pengembangan, perbaikan, dan pengujian program/sistem informasi?
5		Telah disusun rencana pemulihan pusat data utama apabila terjadi bencana
		Apakah data yang penting dalam sistem informasi *di backup* secara rutin?
6		Terdapat komunikasi yang efektif mengenai tugas dan tanggung jawab pengendalian yang dimiliki oleh masing-masing pihak
		Apakah terdapat saluran komunikasi baik ke atas maupun kepada seluruh bagian organisasi mengenai: hal yang tidak diharapkan terjadi dalam pelaksanaan tugas beserta penyebab dan usulan perbaikannya, informasi yang negatif, perilaku yang tidak benar, atau penyimpangan?
7		Terdapat saluran komunikasi untuk melaporkan adanya dugaan pelanggaran/ketidaktepatan dan informasi negatif
	a	Apakah terdapat perlindungan bagi pegawai yang menyampaikan informasi yang negatif, perilaku yang tidak benar, atau penyimpangan ?
	b	Apakah ada alat komunikasi efektif yang menginformasikan hal-hal penting kepada seluruh pegawai?
8		Adanya respon yang tepat waktu terhadap komunikasi yang diterima dari pengguna, rekanan, dan pihak eksternal lainnya

www.peraturan.go.id

	a	Apakah terdapat saluran komunikasi yang terbuka dan efektif dengan masyarakat, rekanan, konsultan, dan aparat pengawasan intern pemerintah serta kelompok lainnya yang bisa memberikan masukan yang signifikan terhadap kualitas pelayanan unit kerja?
	b	Apakah ada strategi pelaksanaan dan jadwal kegiatan komunikasi dan informasi? *(workplan,* jadwal detail setiap tahun)
E		PEMANTAUAN
1		Terdapat mekanisme reviu atas pelaksanaan kegiatan pengendalian
		Apakah terdapat prosedur yang mewajibkan pimpinan unit kerja untuk mereviu pelaksanaan pengendalian?
2		Telah diambil tindakan perbaikan terhadap kesalahan atau sebagai tanggapan atas rekomendasi dan saran perbaikan bagi unit kerja

Setelah melaksanakan pengujian terhadap Pengendalian Intern Tingkat Entitas, Tim Penilai melakukan pengujian terhadap PUTIK. Untuk meningkatkan akurasi penilaian PUTIK, Tim Penilai dapat melibatkan pejabat/pegawai di bagian Teknologi Informasi dan Komunikasi atau pihak ketiga yang kompeten di bidang Teknologi Informasi dan Komunikasi. PUTIK dilakukan pengujian efektivitas sebagaimana Tabel B.2 berikut ini:

Tabel B.2 Pengujian PUTIK

Nama Entitas Akuntansi/Pelaporan :

Nama Aplikasi-Aplikasi :

Akun Signifikan: (diisi dengan akun-akun signifikan terkait)

No	Pengendalian Utama	Pengujian yang dilakukan	Hasil Pengujian	Hasil Penelitian Lanjutan
(1)	(2)	(3)	(4)	(5)

Keterangan:

(1) Diisi nomor

(2) Diisi nama Pengendalian Utama dengan tipe PUTIK.

(3) Diisi dengan menguji manajemen risiko Teknologi Informasi dan Komunikasi, manajemen perubahan Teknologi Informasi

www.peraturan.go.id

dan Komunikasi, akses logikal, dan operasional Teknologi Informasi dan Komunikasi. Pengujian terhadap unsur-unsur pengendalian umum Teknologi Informasi dan Komunikasi bergantung pada lingkungan Teknologi Informasi dan Komunikasi terkait, sehingga suatu lingkungan Teknologi Informasi dan Komunikasi dapat hanya terdiri dari satu unsur saja. Situasi terkait lingkungan Teknologi Informasi dan Komunikasi tersebut perlu dijelaskan dalam suatu kertas kerja. Misalnya dalam situasi lingkungan Teknologi Informasi dan Komunikasi tertentu, hanya dilakukan pengujian asersi pemisahan fungsi atas *user role* beserta akses logikalnya terutama program sosialisasi *security awareness* ke pengguna, pemantauan terhadap penggunaan hak akses serta kewajiban dan larangan pengguna, reviu secara berkala atas pengaktivan jejak audit (*audit trail*), serta pengujian konsistensi implementasi prosedur *backup* dan/*restore*.

(4) Dalam hal hasilnya tidak sesuai dengan kriterianya maka simpulkan tidak efektif. Bila sesuai, simpulkan efektif.

(5) Penelitian Lanjutan hanya dilakukan bila simpulan efektivitasnya "Tidak Efektif'.

Penelitian Lanjutan dilakukan dengan memperhatikan ketiadaan *compensating control* terkait dan/atau adanya bukti bahwa kelemahan tersebut telah dieksploitasi yang mendukung simpulan adanya Kelemahan Signifikan.

Diisi dengan "Tidak Ada Kelemahan/Kelemahan Tidak Signifikan/Kelemahan Signifikan/Kelemahan Material".

Berikut adalah beberapa pengendalian utama PUTIK yang dapat dipertimbangkan untuk dilakukan pengujian:

No	PENGENDALIAN UTAMA
AREA MANAJEMEN RISIKO	
1	Penerapan Manajemen Risiko Teknologi Informasi dan Komunikasi Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa pengelolaan Teknologi Informasi dan Komunikasi telah berpeduli risiko, yaitu risiko kegagalan dukungan dan layanan Teknologi Informasi dan Komunikasi terhadap organisasi telah diidentifikasi, dievaluasi, dan dimitigasi dengan memadai.

www.peraturan.go.id

a)	Terdapat kebijakan dan prosedur umum terkait dengan manajemen risiko Teknologi Informasi dan Komunikasi.
b)	Kebijakan dan prosedur manajemen risiko TIK (jika ada) telah memuat hal-hal sebagai berikut: pemilik risiko, identifikasi risiko, penilaian risiko, dan mitigasi risiko.
c)	Terdapat rencana penerapan manajemen risiko Teknologi Informasi dan Komunikasi.
d)	Rencana penerapan manajemen risiko (jika ada) tersebut telah memuat tahapan identifikasi, evaluasi, dan rencana mitigasi atas risiko-risiko utama Teknologi Informasi dan Komunikasi Organisasi.
e)	Terdapat dokumentasi terkait implementasi manajemen risiko TIK seperti formulir risiko, notulen rapat, dan bahan-bahan sosialisasi manajemen risiko Teknologi Informasi dan Komunikasi.
f)	Manajemen risiko TIK telah diterapkan sesuai dengan kebijakan dan prosedur manajemen risiko yang ditetapkan.
g)	Penerapan manajemen risiko Teknologi Informasi dan Komunikasi telah memadai dalam menjaga pencapaian tujuan Teknologi Informasi dan Komunikasi sebagai pendukung proses bisnis.
h)	Terdapat sosialisasi/internalisasi budaya risiko dan risiko TIK yang dihadapi kepada pegawai.
AREA MANAJEMEN PERUBAHAN	
2	Analisis kebutuhan bisnis dilakukansebelum memberlakukan perubahan sistem. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa perubahan system yang diimplementasikan sesuai dengan kebutuhan organisasi.
a)	Terdapat kebijakan mengenai perubahan sistem.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan analisis kebutuhan bisnis sebelum melakukan perubahan sistem.
c)	Terdapat dokumentasi perubahan sistem.
d)	Dokumentasi perubahan sistem (jika ada) telah memuat: 1) permintaan dan alasan perubahan; 2) analisis dan evaluasi dampak perubahan terhadap kebutuhan bisnis pengguna; 3) persetujuan oleh pemilik proses bisnis.
3	Perubahan sistem diuji sebelum diimplementasikan ke dalam lingkungan produksi. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa perubahan sistem tidak berdampak pada terjadinya gangguan pada sistem yang berialan di lingkungan produksi.
a)	Terdapat kebijakan mengenai pengembangan sistem dan kebijakan pengelolaan perubahan sistem.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan pengujian sebelum perubahan system diimplementasikan ke dalam lingkungan produksi.
c)	Terdapat definisi tugas dan tanggung jawab yang jelas dari para pihak yang terlibat dalam proses perubahan sistem.

www.peraturan.go.id

d)	Terdapat dokumentasi perubahan sistem (log, dokumen sistem, dll).
e)	Proses perubahan yang diimplementasikan telah memenuhi kebijakan pengembangan sistem, terutama memenuhi kriteria berikut: 1) telah diuji di lingkungan non-produksi; dan 2) hasil uji telah disetujui secara teknis untuk diterapkan di lingkungan produksi.
4	Kontrol versi *(version control)* dalam aktivitas pemrograman diimplementasikan yang memuat dokumentasi konfigurasi dan dokumentasi *program code*. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa dokumentasi teknis atas sistem dipelihara untuk memastikan kelangsungan sistem setelah perubahan, maupun dalam hal terjadi kegagalan perubahan.
a)	Terdapat kebijakan mengenai pengembangan sistem dan kebijakan pengelolaan perubahan sistem.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan dokumentasi dan reviu berjenjang atas kontrol versi terhadap perubahan sistem.
c)	Kewajiban dokumentasi kontrol versi (jika ada) telah memuat informasi penting seperti dokumentasi konfigurasi dan *program code*.
d)	Terdapat dokumentasi kontroversi terhadap perubahan sistem.
e)	Proses perubahan yang diimplementasikan telah memenuhi kebijakan pengembangan sistem, terutama memenuhi kriteria berikut: 1) telah diuji di lingkungan non-produksi; dan 2) hasil uji telah disetujui secara teknis untuk diterapkan di lingkungan produksi.
5	Terdapat rencana implementasi serta pemantauan aktivitas implementasi atas perubahan sistem yang dimigrasi ke lingkungan produksi, termasuk *rollback plan*. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa implementasi sistem direncanakan dengan memadai yang mencakup definisi tugas dan tanggung jawab, tahapan implementasi, serta rencana *rollback* (dalam hal terjadi kegagalan implementasi).
a)	Terdapat kebijakan mengenai pengembangan sistem dan kebijakan pengelolaan perubahan sistem.
b)	Kebijakan tersebut (jika ada) telah mencakup kewajiban penyusunan rencana implementasi yang terutama memuat: 1) definisi tugas dan tanggung jawab para pihak yang terlibat; 2) tahapan implementasi yang jelas; 3) *rollback plan;* dan 4) mekanisme pemantauan atas implementasi sistem.
c)	Terdapat dokumentasi implementasi perubahan sistem.
d)	Dokumen implementasi sistem telah memuat: 1) tugas dan tanggung jawab para pihak yang terlibat; 2) target dan realisasi jadwal; 3) persetujuan pihak berwenang; dan

www.peraturan.go.id

	4) memuat *rollback plan*.
6	Perubahan sistem dalam konfigurasi sistem, aplikasi, *interface, database, OS,* dan *patches/*peningkatan sistem telah disetujui sebelum dimigrasikan dan diimplementasikan di lingkungan produksi. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa perubahan terhadap sistem atau konfigurasi sistem diterapkan berdasarkan otorisasi yang sah dari pihak berwenang.
a)	Terdapat kebijakan mengenai pengembangan sistem dan kebijakan pengelolaan perubahan sistem.
b)	Kebijakan tersebut (jika ada) telah memuat: 1) definisi tugas dan tanggung jawab yang jelas dari para pihak yang terlibat dalam proses perubahan sistem; dan 2) mekanisme persetujuan sebelum perubahan sistem diimplementasikan ke dalam lingkungan produksi.
c)	Terdapat dokumentasi implementasi perubahan sistem.
d)	Terdapat persetujuan sebelum perubahan sistem diimplementasikan ke dalam lingkungan produksi.
7	Lingkungan pengembangan dan pengujian terpisah dari lingkungan produksi. Akses fisik maupun logis terhadap lingkungan tersebut dibatasi berdasarkan fungsi *(role)* dan tanggungjawab pengguna. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa perubahan data pada lingkungan produksi merupakan perubahan yang sah.
a)	Terdapat kebijakan mengenai pengembangan sistem dan kebijakan pengelolaan perubahan sistem.
b)	Kebijakan tersebut (jika ada) telah memuat: 1) kewajiban pemisahan antara lingkungan pengembangan , pengujian, dan produksi; dan 2) definisi yang jelas mengenai tugas dan tanggung jawab para pihak yang terlibat pada lingkungan tiap-tiap lingkungan tersebut.
c)	Lingkungan pengembangan, pengujian, dan produksi telah dipisahkan dalam pengembangan dan pengujian sistem.
d)	Terdapat perangkat yang dikhususkan untuk digunakan sebagai lingkungan pengembangan, pengujian, dan produksi.
e)	Dalam hal terdapat lingkungan pengembangan, pengujian, dan produksi: 1) terdapat daftar pengguna beserta hak akses atas perangkat pada tiap-tiap lingkungan tersebut; dan 2) pemisahan *IP address* tiap lingkungan.
f)	Ada pengguna *(user)* pada lingkungan produksi yang memiliki *responsibility/role* sebagai *"Application Developer"*
AREA AKSES LOGIKAL	
8	Program *security awareness* disosialisasikan ke pengguna, termasuk pengguna sementara. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa pengguna sistem aplikasi memahami tanggung jawab penggunaan sistem.

www.peraturan.go.id

a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat: 1) kewajiban diadakan nya program *security awareness* kepada pegawai, termasuk pengguna sementara; dan 2) materi program mencakup rincian tanggung jawab dan konsekuensi bagi pengguna.
c)	Terdapat rencana jadwal sosialisasi *security awareness*.
d)	Terdapat dokumentasi program *security awareness* .
e)	Terdapat *security awareness team*, yang bertugas untuk mengembangkan, menyampaikan, dan memelihara program *security awareness* .
g)	Program *security awareness* (jika ada) telah disosialisasikan melalui berbagai jalur komunikasi.
9	Pemantauan terhadap penggunaan hak akses. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai akuntabilitas penggunaan akun oleh pengguna sistem.
a)	Terdapat kebiiakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban dilakukannya pemantauan terhadap penggunaan hak akses, termasuk pemantauan terhadap kewaiiban dan larangan pengguna.
c)	Terdapat prosedur/rencana pemantauan terhadap penggunaan hak akses.
d)	Terdapat dokumentasi pelaksanaan pemantauan hak akses.
e)	Pemantauan tersebut (jika ada) menilai kepatuhan pemenuhan kewajiban dan larangan pengguna.
f)	Terdapat dokumentasi tindak lanjut atas pemantauan kepatuhan tersebut (jika ada).
10	Matriks akses pengguna *(User Access Matrix/DAM)* di setiap lapisan, baik aplikasi, OS, DB , dan layanan jaringan disusun dan divalidasi secara berkala. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai pengendalian hak akses pada aplikasi maupun infrastruktur terkait .
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi dan matriks akses pengguna
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban penyusunan dan validasi matriks akses pengguna secara berkala
c)	Terdapat matriks akses pengguna
d)	Akun pengguna telah divalidasi dan proses validasi diketahui dan disetujui oleh pemilik proses bisnis yang terkait
e)	Tidak terdapat: 1) pegawai yang telah keluar/mengundurkan diri masih berstatus pengguna aktif di aplikasi; 2) pegawai yang telah dimutasi/promosi namun masih memiliki fungsi dan tanggung jawab di posisi mereka sebelumnya; dan

www.peraturan.go.id

	3) pengguna yang tidak digunakan (tidak aktif lebih dari 90 hari) masih berstatus aktif.
11	Hak akses dari pegawai yang dimutasi/mengundurkan diri, pihak ketiga yang kontraknya telah habis, dan individu yang melanggar standar keamanan informasi dan tengah menjalani proses hukum dicabut sesegera mungkin. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa akses terhadap sistem dilakukan oleh pengguna yang sah.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi dan matriks akses pengguna.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban penonaktifan pegawai yang dimutasi/mengundurkan diri, pihak ketiga yang kontraknya telah habis, dan individu yang melanggar standar keamanan informasi dan tengah menialani proses hukum.
c)	Terdapat matriks akses pengguna.
d)	Terdapat pegawai yang dimutasi/mengundurkan diri, pihak ketiga yang kontraknya telah habis, dan individu yang melanggar standar keamanan informasi dan tengah menjalani proses hukum.
e)	Tanggal perolehan dan penonaktifan hak akses pegawai tersebut (jika ada) telah sesuai.
12	Akun pengguna (umum maupun khusus) didefinisikan secara individual untuk memastikan akuntabilitasnya. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai akuntabilitas penggunaan akun oleh pengguna sistem.
	Terdapat kebijakan mengenai sistem manajemen keamanan informasi dan pengelolaan hak akses.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai akun khusus (dengan pengguna umum/lebih dari satu personil).
c)	Pengaturan akun khusus tersebut memuat definisi yang jelas mengenai tanggung jawab pengguna umum.
d)	Terdapat prosedur/rencana pemantauan terhadap penggunaan hak akses, terutama oleh akun khusus.
e)	Terdapat daftar pengguna yang memiliki akses ke aplikasi.
f)	ID pengguna yang unik untuk tiap pengguna dan akun umum tidak diberikan kepada suatu departemen atau kelompok.
g)	Terdapat standar penamaan untuk ID pengguna .
h)	Terdapat ID pengguna umum yang digunakan oleh departemen/kelompok dalam aplikasi.
13	Akses *remote* dan jaringan nirkabel diamankan dengan pengendalian secara teknis (misal segmentasi jaringan) dan administratif. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa akses terhadap sistem dilakukan melalui perangkat yang terotorisasi oleh pihak yang terotorisasi.

www.peraturan.go.id

a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi khususnya terkait akses remote dan jaringan nirkabel, serta segmentasi jaringan.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai: 1). akses remote dan jaringan nirkabel; dan 2). Segmentasi jaringan berdasarkan kriteria aset, unit/fungsi yang menggunakan jaringan, dan pemisahan jaringan internal dan eksternal.
c)	Jaringan nirkabel diakses melalui mekanisme yang aman (misalnya menggunakan metode enkripsi WPA2).
d)	Terdapat laporan yang berhubungan dengan pengujian keamanan jaringan nirkabel.
e)	Pemberian akses ke jaringan nirkabel kepada pihak eksternal yang didasarkan atas kebutuhan dan telah dilakukan pemantauan.
f)	Terdapat dokumentasi topologi jaringan.
g)	Jaringan internal (yang mencakup segmentasi untuk lingkup pengembangan, pengujian, dan produksi) dan jaringan eksternal/tamu telah dipisahkan secara tepat.
h)	Terdapat pembatasan terhadap akses ke lingkungan tertentu sesuai dengan kebiiakan atau prosedur yang berlaku.
14	Kata sandi default untuk akun-akun *default* (misalnya, SYSADMIN, GUEST) di *database, server* , dan aplikasi telah diubah. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa akses melalui akun *default* telah diantisipasi
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai: 1) penggunaan akun dan kata sandi *default;* atau *2)* prosedur standar penerimaan dan penggunaan perangkat TIK yang mencakup pengubahan akun dan konfigurasi *default.*
c)	*User* dan kata sandi *default* pada perangkat terkait aplikasi telah dinonaktifkan .
15	*Penetration testing / vulnerability assessment* dilakukan pada segmen sistem/jaringan yang sesuai berdasarkan profil risikonya dan segala kelemahan ditindaklanjuti berdasarkan rekomendasi yang telah disetujui. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa kerentanan sistem telah diantisipasi.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban dan pengaturan mengenai *penetration testing vulnerability assessment,* termasuk area utama *testing/assessment* dan periodisasi pengujian (misal : setahun sekali).
c)	Terdapat dokumentasi hasil *penetration testing / vulnerability assessment.*

www.peraturan.go.id

d)	*Penetrationtesting/ vulnerability assessment* (jika dilakukan) telah mencakup aktivitas berikut: *pre-penetration, identification entry points, host scanning, scanning, implementation security hardening.*
e)	Kerentanan yang ditemukan dari pengujian *penetration testing/ vulnerability assessment* (jika ada) telah diperbaiki/dimitigasi/ dilakukan pengendalian tambahan.
16	Jejak audit *(audit trail)* di aplikasi diaktifkan dan direviu secara berkala. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa terdapat pemantauan dan langkah perbaikan atas akses yang tidak terotorisasi.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi khususnya terkait *audit trail.*
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai *audit trail* dan kewajiban untuk melakukan reviu *audit trail* secara *periodic.*
c)	Terdapat kebijakan dan prosedur terkait dengan pemantauan pelanggaran akses.
d)	Kebijakan dan prosedur pemantauan pelanggaran akses mencakup definisi tujuan dan periodisasi pemantauan, serta jenis tindakan yang dipantau.
e)	Terdapat dokumentasi konfigurasi dan pemantauan penggunaan akun (*audit trail* serta laporan analisis atas *audit trail)*
f)	Dokumentasi pemantauan penggunaan akun (jika ada) memuat analisis atas aktivitas mencurigakan seperti: login yang tidak berhasil, termasuk profil akun yang bersangkutan *(Audit Trail: Activate Profile Option).*
AREA OPERASIONAL TIK DAN KELANGSUNGAN LAYANAN	
17	Implementasi prosedur *backup* dan *restore* secara konsisten. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai ketersediaan data untuk mendukung sistem/layanan.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan *backup* dan *restore.*
c)	Kebijakan/prosedur tersebut (jika ada) telah memuat pengaturan kritis antara lain mengenai: 1) periodisasi *backup*, dan periodisasi uji *restore;* 2) definisi tugas dan tanggung jawab para pihak yang terlibat; 3) mekanisme penanganan kegagalan pada proses *backup* dan uji coba *restore.*
d)	Terdapat dokumentasi pelaksanaan *backup* dan *restore.*
e)	*Log backup* (jika ada) minimal telah mencakup informasi mengenai: 1) Tanggal dan waktu *backup*; 2) Status *backup;* dan 3) Deskripsi mengenai data *backup.*
f)	Jika terjadi kegagalan pada proses *backup* dan uji coba *restore* (jika dilakukan) telah sesuai dengan prosedur.

www.peraturan.go.id

18	*Service-level Agreement* atau *Operational-level Agreement* secara formal didefinisikan antara pihak-pihak terkait. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai keselarasan dan konsistensi kapasitas layanan TIK dengan kebutuhan proses bisnis.
a)	Terdapat kebijakan mengenai sistem manajemen layanan TIK.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai: 1) penyusunan *Service-level Agreement* dan *Operational-level Agreement*; 2) pemantauan pencapaian *Service-level Agreement* dan *Operational-level Agreement*; dan 3) penanganan kegagalan pencapaian target layanan.
c)	Terdapat dokumentasi *Service-level Agreement* dan *Operational-level Agreement*; laporan pemantauan pencapaian *Service-level Agreement/ Operational-level Agreement*; dan dokumentasi tindaklanjut penanganan kegagalan pencapaian target layanan.
d)	*Service-level Agreement* dan *Operational-level Agreement* (jika ada) telah disusun dengan memperkirakan kebutuhan proses bisnis.
e)	*Service-level Agreement* dan *Operational-level Agreement* (jika ada) telah sesuai dengan kebutuhan proses bisnis pada saat ini.
19	implementasi dan uji berkala atas *Disaster Recovery Planning*. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai kemampuan pemulihan aplikasi/layanan ketika terjadi bencana.
a)	Terdapat kebijakan mengenai sistem manajemen layanan Teknologi Informasi dan Komunikasi.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai DRP yang mencakup: kewajiban penyusunan *Disaster Recovery Planning*; informasi penting, misalnya daftar kontak dan wewenang masing-masing; mekanisme/prosedur uji dan reviu hasil uji serta mekanisme sosialisasi .
c)	Terdapat dokumentasi: *Disaster Recovery Planning*, laporan uji *Disaster Recovery Planning* (termasuk reviu hasil uji, jika ada), dan laporan sosialisasi/pelatihan implementasi *Disaster Recovery Planning*.
d)	Terdapat mekanisme eskalasi yang ditempuh atas permasalahan yang terjadi pada saat pengujian *Disaster Recovery Planning*, serta tindak lanjut penyelesaian permasalahan tersebut.
20	Perencanaan kapasitas dan pemantauan utilisasi infrastruktur dan kinerja sistem yang kritis secara konsisten (termasuk performa, beban/utilisasi jaringan, deteksi gangguan, virus, performa *helpdesk*, dll). Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai kapasitas dan kinerja infrastruktur (dan penunjangnya) dalam mendukung layanan dan proses bisnis.
a)	Terdapat kebijakan mengenai sistem manajemen layanan Teknologi Informasi dan Komunikasi.
b)	Kebijakan tersebu (jika ada) telah memuat kewajiban untuk melakukan pemantauan secara berkala terhadap: l).utilisasi

www.peraturan.go.id

	infrastruktur mencakup kapasitas pemrosesan, penyimpanan data, komunikasi data; 2).keandalan infrastruktur dalam mengatasi serangan *malware*; 3).kinerja perangkat secara umum; 4).kinerja layanan dukungan operasional (*helpdesk*).
c)	Terdapat dokumentasi perencanaan kapasitas infrastruktur.
d)	Terdapat dokumentasi pemantauan atas kinerja infrastruktur sistem.
e)	Dokumentasi pemantauan atas kinerja infrastruktur sistem (jika ada) telah memuat: 1) lingkup pemantauan; 2) kesesuaian periodisasi, pencatatan, dan mekanisme penanganan dengan kebijakan/ prosedur yang ditetapkan; 3) tindak lanjut/penyelesaian atas gangguan/insiden yang terjadi; dan 4) eskalasi permasajahan (gangguan/insiden) dan penyelesaiannya kepada pimpinan unit pengelola TIK maupun jajaran pimpinan organisasi.
f)	Realisasi kinerja dan kapasitas infrastruktur telah sesuai dengan yang direncanakan.
21	Gangguan atau insiden operasional TI diidentifikasi, ditangani, direviu, dan dianalisa dengan tepat waktu. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa gangguan dan insiden terhadap sistem dan layanan TIK telah diantisipasi.
a)	Terdapat kebijakan mengenai sistem manajemen layanan TIK.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan: 1) pemantauan terhadap gangguan dan insiden terhadap sistem; 2) prioritisasi penanganan gangguan/insiden berdasarkan dampak; 3) mekanisme penanganan gangguan dan insiden tersebut; dan 4) mekanisme eskalasi.
c)	Terdapat dokumentasi pemantauan berkala terhadap gangguan dan insiden operasional terhadap sistem dan infrastrukturnya.
d)	Dokumentasi pemantauan berkala terhadap gangguan dan insiden operasional terhadap sistem dan infrastrukturnya (jika ada) telah memuat: 1) jenis gangguan/insiden yang dipantau; 2) kesesuaian periodisasi, pencatatan, dan mekanisme penanganan dengan kebijakan/prosedur yang ditetapkan; 3) tindak lanjut/ penyelesaian atas gangguan/insiden yang terjadi; dan 4) eskalasi permasalahan (gangguan/insiden) dan penyelesaiannya kepada jajaran pimpinan organisasi
22	Pengendalian fisik diimplementasikan secara memadai pada lingkungan data center dan fasilitas pemrosesan lainnya. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai keamanan fisik perangkat.

www.peraturan.go.id

a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai keamanan fisik dan lingkungan yang antara lain mencakup: 1) pengaturan atas akses fisik dengan mekanisme otentifikasi akses dengan sidik jari pada pintu masuk data *center*, otentifikasi akses sidik jari ganda pada *main trap data center*, dan *logbook* pada lobi gedung dan pintu utama *data center*, serta 2) mekanisme pengaturan kelistrikan, dan pendinginan.
c)	Terdapat dokumentasi pemantauan berkala terhadap fasilitas pengolah informasi *(Data Center)*.
d)	Mekanisme akses, penanganan terhadap insiden fisik, perlindungan kelistrikan, dan pendinginan telah sesuai dengan kebijakan/standar/prosedur yang berlaku.
e)	Terdapat dokumentasi pemeliharaan fasilitas *(Data Center)* dengan penyedia/pihak ketiga yang terkait.
f)	Aktivitas pemeliharaan fasilitas *(Data Center)* dengan penyedia/ pihak ketiga telah sesuai dengan kontrak/SLA yang ditetapkan.
g)	Aktivitas pemeliharaan fasilitas *(Data Center)* telah sesuai dengan dengan kebutuhan.

Pengujian PUTIK secara menyeluruh dilakukan pada lingkungan aplikasi terkait pelaporan keuangan yang PUTIK terdapat pada Kementerian Keuangan. Pengujian pada Entitas Akutansi/Pelaporan pada masing-masing Kementerian/Lembaga dilasanakan atas 2 (dua) area, yaitu area akses logikal serta area operasional TIK dan kelangsungan layanan dengan pengendalian utama sebagaimana tabel di bawah ini. Dalam hal terdapat ketidaksesuaian dengan kondisi di lapangan, butir-butir pengendalian utama tersebut dapat dimodifikasi, baik ditambah atau dikurangi dengan menyebutkan alasannya yang dijelaskan dalam suatu pernyataan terpisah yang ditandatangani oleh Tim Penilai.

AREA AKSES LOGIKAL	
No	**PENGENDALIAN UTAMA**
1	Program *security awareness* disosialisasikan ke pengguna, termasuk pengguna sementara. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa pengguna sistem aplikasi memahami tanggung jawab penggunaan sistem.

www.peraturan.go.id

a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat: 1) kewajiban diadakannya program *security awareness* kepada pegawai , termasuk pengguna sementara; dan 2) materi program mencakup rincian tanggung jawab dan konsekuensi bagi pengguna.
c)	Terdapat rencana jadwal sosialisasi *security awareness*.
d)	Terdapat dokumentasi program *security awareness* .
e)	Terdapat *security awareness team*, yang bertugas untuk mengembangkan, menyampaikan, dan memelihara program *security awareness*.
f)	Program *security awareness* (jika ada) menyediakan referensi bagi organisasi untuk melatih personil dalam tingkatan yang sesuai dengan tugas dan fungsinya .
g)	Program *security awareness* (jika ada) telah disosialisasikan melalui berbagai jalur komunikasi .
2	Pemantauan terhadap penggunaan hak akses. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai akuntabilitas penggunaan akun oleh pengguna sistem.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban dilakukannya pemantauan terhadap penggunaan hak akses, termasuk pemantauan terhadap kewajiban dan larangan pengguna.
c)	Terdapat prosedur/rencana pemantauan terhadap penggunaan hak akses.
d)	Terdapat dokumentasi pelaksanaan pemantauan hak akses.
e)	Pemantauan tersebut (jika ada) menilai kepatuhan pemenuhan kewajiban dan larangan pengguna.
f)	Terdapat dokumentasi tindak lanjut atas pemantauan kepatuhan tersebut (jika ada).

www.peraturan.go.id

3	Matriks akses pengguna (*user Access Matrix/ UAM)* di setiap lapisan, baik aplikasi, OS, DB, dan layanan jaringan disusun dan divalidasi secara berkala. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai pengendalian hak akses pada aplikasi maupun infrastruktur terkait.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi dan matriks akses pengguna.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban penyusunan dan validasi matriks akses pengguna secara berkala.
c)	Terdapat matriks akses pengguna.
d)	Akun pengguna telah divalidasi dan proses validasi diketahui dan disetujui oleh pemilik proses bisnis yang terkait.
e)	Tidak terdapat: 1) pegawai yang telah keluar/mengundurkan diri masih berstatus pengguna aktif di aplikasi; 2) pegawai yang telah dimutasi/promosi namun masih memiliki fungsi dan tanggung jawab di posisi mereka sebelumnya; dan 3) pengguna yang tidak digunakan (tidak aktif lebih dari 90 hari) masih berstatus aktif.
4	Hak akses dari pegawai yang dimutasi/mengundurkan diri, pihak ketiga yang kontraknya telah habis, dan individu yang melanggar standar keamanan informasi dan tengah menjalani proses hukum dicabut sesegera mungkin. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa akses terhadap sistem dilakukan oleh penerima yang sah.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi dan matriks akses pengguna.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban penonaktifan pegawai yang dimutasi/mengundurkan diri, pihak ketiga yang kontraknya telah habis, dan individu yang melanggar standar keamanan informasi dan tengah menjalani proses hukum.

www.peraturan.go.id

c)	Terdapat matriks akses pengguna.
d)	Terdapat pegawai yang dimutasi/ mengundurkan diri, pihak ketiga yang kontraknya telah habis, dan individu yang melanggar standar keamanan informasi dan tengah menjalani proses hukum.
e)	Tanggal perolehan dan penonaktifan hak akses pegawai tersebut (jika ada) telah sesuai.
5	Akun pengguna (umum maupun khusus) didefinisikan secara individual untuk memastikan akuntabilitasnya. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai akuntabilitas penggunaan akun oleh pengguna sistem.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi dan pengelolaan hak akses.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai akun khusus (dengan pengguna umum/lebih dari 1 (satu) personil).
c)	Pengaturan akun khusus tersebut memuat definisi yang jelas mengenai tanggung jawab pengguna umum.
d)	Terdapat prosedur/rencana pemantauan terhadap penggunaan hak akses, terutama oleh akun khusus.
e)	Terdapat daftar pengguna yang memiliki akses ke aplikasi.
f)	ID pengguna yang unik untuk tiap pengguna dan akun umum tidak diberikan kepada suatu departemen atau kelompok.
g)	Terdapat standar penamaan untuk ID pengguna.
h)	Terdapat ID pengguna umum yang digunakan oleh departemen/kelompok dalam aplikasi.
6	Akses remote dan jaringan nirkabel diamankan dengan pengendalian secara teknis (misal segmentasi jaringan) dan administratif. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa akses terhadap sistem dilakukan melalui perangkat yang terotorisasi oleh pihak yang terotorisasi.

www.peraturan.go.id

a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi khususnya terkait akses remote dan jaringan nirkabel, serta segmentasi jaringan.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai: 1). akses remote dan jaringan nirkabel; dan 2). segmentasi jaringan berdasarkan kriteria aset, unit/ fungsi yang menggunakan jaringan, dan pemisahan jaringan internal dan eksternal.
c)	Jaringan nirkabel diakses melalui mekanisme yang aman.
d)	Terdapat laporan yang berhubungan dengan pengujian keamanan jaringan nirkabel.
e)	Pemberian akses ke jaringan nirkabel kepada pihak eksternal yang didasarkan atas kebutuhan dan telah dilakukan pemantauan.
f)	Terdapat dokumentasi topologi jaringan.
g)	Jaringan internal yang mencakup segmentasi untuk lingkup pengembangan, pengujian, dan produksi) dan jaringan eksternal/tamu telah dipisahkan secara tepat.
h)	Terdapat pembatasan terhadap akses ke lingkungan tertentu sesuai dengan kebijakan atau prosedur yang berlaku.
7	Kata sandi *default* untuk akun-akun *default* (misalnya, SYSADMIN, GUEST) di *database, server,* dan aplikasi telah diubah. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa akses melalui akun *default* telah diantisipasi.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai: 1) penggunaan akun dan kata sandi *default*; atau 2) prosedur standar penerimaan dan penggunaan perangkat Teknologi Informasi dan Komunikasi yang mencakup pengubahan akun dan konfigurasi *default*.

www.peraturan.go.id

c)	*User* dan kata sandi *default* pada perangkat terkait aplikasi telah dinonaktifkan.
8	*Penetration testing / vulnerability assessment* dilakukan pada segmen sistem/jaringan yang sesuai berdasarkan profil risikonya dan segala kelemahan ditindaklanjuti berdasarkan rekornendasi yang telah disetujui. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa kerentanan sistem telah diantisipasi.
a)	Terdapat kebijakan mengenai sistem manajernen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban dan pengaturan mengenai penetration testing/*vulnerability assessment*, termasuk area utama testing/*assessment* dan periodisasi (misal : setahun)
c)	Terdapat dokumentasi hasil *penetration testing/ vulnerability assessment.*
d)	*Penetration testing/ vulnerability assessment* Uika dilakukan) telah mencakup aktivitas berikut: *pre-penetration, identification entry points, host scanning, scanning, implementation security hardening.*
e)	Kerentanan yang ditemukan dari pengujian *penetration testing/vulnerability assessment* (jika ada) telah diperbaiki/ dimitigasi/dilakukan pengendalian tambahan.
9	Jejak audit (*audit trail*) di aplikasi diaktifkan dan direviu secara berkala. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa terdapat pemantauan dan langkah perbaikan atas akses yang tidak terotorisasi.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi khususnva terkait *audit trail.*
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai *audit trail* dan kewajiban untuk melakukan reviu *audit trail* secara periodik.

www.peraturan.go.id

c)	Terdapat kebijakan dan prosedur terkait dengan pemantauan pelanggaran akses.
d)	Kebijakan dan prosedur pemantauan pelanggaran akses mencakup definisi tujuan dan periodisasi pemantauan, serta jenis tindakan yang dipantau.
e)	Terdapat dokumentasi konfigurasi dan pemantauan penggunaan akun (*audit trail* serta laporan analisis atas *audit trail).*
f)	Dokumentasi pemantauan penggunaan akun (jika ada) memuat analisis atas aktivitas mencurigakan seperti: *login* yang tidak berhasil, termasuk profil akun yang bersangkutan *(Audit Trail: Activate Profile Option)*
AREA OPERASIONAL TIK DAN KELANGSUNGAN LAYANAN	
10	Implementasi prosedur *backup* dan r*estore* secara konsisten. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai ketersediaan data untuk mendukung sistem/layanan.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan *backup* dan *restore.*
c)	Kebijakan/prosedur tersebut (jika ada) telah memuat pengaturan kritis antara lain mengenai: 1) periodisasi *backup,* dan periodisasi uji *restore;* 2) definisi tugas dan tanggung jawab para pihak yang terlibat; dan 3) mekanisme penanganan kegagalan pada proses backup dan uji coba *restore.*
d)	Terdapat dokumentasi pelaksanaan *backup* dan *restore.*
e)	*Log backup* Uika ada) minimal telah mencakup informasi mengenai: 1) tanggal dan waktu *backup;* 2) *status backup;* dan 3) deskripsi mengenai data *backup.*

www.peraturan.go.id

f)	Jika terjadi kegagalan pada proses *backup* dan uji coba *restore* jika dilakukan) telah sesuai dengan prosedur.
11	*Service-level Agreement* (SLA) atau *Operational-level Agreement* (OLA) secara formal didefinisikan antara pihak-pihak terkait. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai keselarasan dan konsistensi kapasitas layanan TIK dengan kebutuhan proses bisnis.
a)	Terdapat kebijakan mengenai sistem manajemen layanan TIK.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai: 1) penyusunan *Service-level Agreement* dan *Operational-level Agreement*; 2) pemantauan pencapaian *Service-level Agreement* dan *Operational-level Agreement*; dan 3) penanganan kegagalan pencapaian target layanan.
c)	Terdapat dokumentasi *Service-level Agreement* dan *Operational-level Agreement*; laporan pemantauan pencapaian *Service-level Agreement / Operational-level Agreement*; dan dokumentasi tindak lanjut penanganan kegagalan pencapaian target layanan.
d)	*Service-level Agreement* dan *Operational-level Agreement* (jika ada) telah disusun dengan memperkirakan kebutuhan proses bisnis.
e)	*Service-level Agreement* dan *Operational-level Agreement* (jika ada) telah sesuai dengan kebutuhan proses bisnis pada saat ini.
12	Implementasi dan uji berkala atas *Disaster recovery planning* Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai kemampuan pemulihan aplikasi/layanan ketika terjadi bencana.
a)	Terdapat kebijakan mengenai sistem manajemen layanan TIK.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai mengenai *Disaster recovery planning* yang mencakup: kewajiban penyusunan *Disaster recovery planning*; Informasi

www.peraturan.go.id

	penting, misalnya daftar kontak dan wewenang masing-masing; mekanisme / prosedur uji dan reviu hasil uji serta mekanisme sosialisasi.
c)	Terdapat dokumentasi: *Disaster recovery planning*; laporan uji *Disaster recovery planning* (termasuk reviu hasil uji, jika ada); dan laporan sosialisasi/pelatihan implementasi *Disaster recovery planning*.
d)	Terdapat mekanisme eskalasi yang ditempuh atas permasalahan yang terjadi pada saat pengujian *Disaster recovery planning*, serta tindak lanjut/penyelesaian permasalahan tersebut.
13	Perencanaan kapasitas dan pemantauan utilisasi infrastruktur dan kinerja sistem yang kritis secara konsisten (termasuk performa, beban/utilisasi jaringan, deteksi gangguan, virus, performa *helpdesk*, dll). Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai kapasitas dan kinerja infrastruktur (dan penunjangnya) dalam mendukung layanan dan proses bisnis.
a)	Terdapat kebijakan mengenai sistem manajemen layanan Teknologi Informasi dan Komunikasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan pemantauan secara berkala terhadap: 1) utilisasi infrastruktur mencakup kapasitas pemrosesan, penyimpanan data, komunikasi data; 2) keandalan infrastruktur dalam mengatasi serangan *malware*; 3) kinerja perangkat secara umum; dan 4) kineria layanan dukungan operasional *(help desk)*.
c)	Terdapat dokumentasi perencanaan kapasitas infrastruktur.
d)	Terdapat dokumentasi pemantauan atas kinerja infrastruktur sistem.
e)	Dokumentasi pemantauan atas kinerja infrastruktur sistem (jika ada) telah memuat: 1) lingkup pemantauan; 2) kesesuaian periodisasi, pencatatan, dan mekanisme penanganan dengan kebijakan/ prosedur yang ditetapkan;

www.peraturan.go.id

	3) tindak lanjut/ penyelesaian atas gangguan/insiden yang terjadi; dan 4) eskalasi permasalahan (gangguan/insiden) dan penyelesaiannya kepada pimpinan unit pengelola Teknologi Informasi dan Komunikasi maupun jajaran pimpinan organisasi.
	Realisasi kinerja dan kapasitas infrastruktur telah sesuai dengan yang direncanakan.
14	Gangguan atau insiden operasional Teknologi Informasi diidentifikasi, ditangani, direviu, dan dianalisa dengan tepat waktu. Pengendalian ini bertujuan untuk memberikan keyakinan memadai bahwa gangguan dan insiden terhadap sistem dan layanan Teknologi Informasi dan Komunikasi telah diantisipasi.
a)	Terdapat kebijakan mengenai sistem manajemen layanan Teknologi Informasi dan Komunikasi.
b)	Kebijakan tersebut (jika ada) telah memuat kewajiban untuk melakukan: 1) pemantauan terhadap gangguan dan insiden terhadap sistem; 2) prioritisasi penanganan gangguan/insiden berdasarkan dampak; 3) mekanisme penanganan gangguan dan insiden tersebut; dan 4) mekanisme eskalasi.
c)	Terdapat dokumentasi pemantauan berkala terhadap gangggguan dan insiden operasional terhadap sistem dan infrastrukturnva.
d)	Dokumentasi pemantauan berkala terhadap gangguan dan insiden operasional terhadap sistem dan infrastrukturnya (jika ada) telah memuat:
	1) jenis gangguan/insiden yang dipantau; 2) kesesuaian periodisasi, pencatatan, dan mekanisme penanganan dengan kebijakan/prosedur yang ditetapkan; 3) tindak lanjut/ penyelesaian atas gangguan/insiden yang terjadi; dan

www.peraturan.go.id

	4) eskalasi permasalahan (gangguan/insiden) dan penyelesaiannya kepada jajaran pimpinan organisasi.
15	Pengendalian fisik diimplementasikan secara memadai pada lingkungan data *center* dan fasilitas pemrosesan lainnya. Pengendalian ini bertujuan untuk memberikan keyakinan memadai mengenai keamanan fisik perangkat.
a)	Terdapat kebijakan mengenai sistem manajemen keamanan informasi.
b)	Kebijakan tersebut (jika ada) telah memuat pengaturan mengenai keamanan fisik dan lingkungan yang antara lain mencakup: 1) pengaturan atas akses fisik dengan mekanisme otentifikasi akses dengan sidik jari pada pintu masuk data center, otentifikasi akses sidik jari ganda pada *main trap data center,* dan *logbook* pada lobi gedung dan pintu utama *data center,* dan 2) mekanisme pengaturan kelistrikan, dan pendinginan.
c)	Terdapat dokumentasi pemantauan berkala terhadap fasilitas pengolah informasi *(Data Center).*
d)	Mekanisme akses, penanganan terhadap insiden fisik, perlindungan kelistrikan, dan pendinginan telah sesuai dengan kebijakan/standar/prosedur yang berlaku.
e)	Terdapat dokumentasi pemeliharaan fasilitas *(Data Center)* dengan penyedia/pihak ketiga yang terkait.
f)	Aktivitas pemeliharaan fasilitas *(Data Center)* dengan penyedia/pihak ketiga telah sesuai dengan kontrak yang ditetapkan.
g)	Aktivitas pemeliharaan fasilitas *(Data Center)* telah sesuai dengan dengan kebutuhan.

Kelemahan-kelemahan pengendalian yang diperoleh dalam pengujian PUTIK akan dipertimbangkan dalam penyusunan simpulan penilaian efektivitas pengendalian intern secara keseluruhan.

www.peraturan.go.id

3) Menarik simpulan

Dari hasil pengujian ini akan diperoleh simpulan mengenai keandalan Pengendalian Intern Tingkat Entitas, kelemahan, dan rekomendasi untuk perbaikan. Simpulan diperoleh dari persentase skor terhadap jumlah faktor yang dinilai dan dikategorikan ke dalam 3 (tiga) tingkatan sebagai berikut:

a) Rendah, yaitu apabila nilai akhir kurang dari 34% (tiga puluh empat persen);

b) Sedang, yaitu apabila nilai akhir sebesar 34%(tiga puluh empat persen) s.d. 63% (enam puluh tiga persen); atau

c) Tinggi, yaitu apabila nilai akhir lebih dari 63% (enam puluh tiga persen).

Simpulan hasil penilaian tersebut digunakan sebagai bahan pertimbangan untuk kelanjutan dalam melakukan penilaian Pengendalian Intern Tingkat Proses/Transaksi. Kelemahan penilaian Pengendalian Intern Tingkat Entitas akan dipertimbangkan dalam penyusunan simpulan penilaian efektivitas pengendalian intern secara keseluruhan. Kelemahan tersebut menguraikan kondisi pelanggaran dan/atau penyimpangan terhadap penerapan pengendalian intern, akibat, dan penyebabnya. Rekomendasi menguraikan saran-saran perbaikan dan rencana aksi yang diperlukan.

4. Pengujian Pengendalian Intern Tingkat Proses/Transaksi Setelah seluruh risiko terkait proses utama dan pengendaliannya diidentifikasi, didokumentasikan, serta langkah pengujiannya disusun pada tahap perencanaan, langkah berikutnya adalah melaksanakan penilaian Pengendalian Intern Tingkat Proses/Transaksi.

a. Tujuan

Penilaian Pengendalian Intern Tingkat Proses/Transaksi bertujuan untuk memberikan keyakinan memadai bahwa pengendalian telah dilaksanakan secara efektif untuk mencegah dan mendeteksi "apa yang bisa salah" atau tidak tercapainya tujuan keandalan pelaporan keuangan.

b. Pelaksana dan Lingkup

Pelaksana penilaian Pengendalian Intern Tingkat Proses/Transaksi

www.peraturan.go.id

beserta lingkup objek yang dinilai adalah sebagai berikut:

1) Tim Penilai tingkat UAKPA menilai Pengendalian Intern Tingkat Proses/Transaksi unit kerja UAKPA.
2) Tim Penilai tingkat UAPPA-W menilai Pengendalian Intern Tingkat Proses/Transaksi unit kerja UAPPA-W.
3) Tim Penilai tingkat UAPPA-El menilai Pengendalian Intern Tingkat Proses/Transaksi unit kerja UAPPA-El.
4) Tim Penilai tingkat UAPA mengompilasi hasil penilaian pengendalian intern Tim Penilai di bawahnya dan menyimpulkan tingkat keandalan Pengendalian Intern Tingkat Proses/Transaksi Kemhan dan TNI secara keseluruhan.

c. Proses Proses penilaian Pengendalian Intern Tingkat Proses/Transaksi dilaksanakan melalui dua tahap yaitu penilaian efektivitas rancangan pengendalian dan penilaian efektivitas implementasi pengendalian. Penjelasan setiap tahapan dapat diuraikan sebagai berikut:

1) Penilaian Efektivitas Rancangan Pengendalian Menilai efektivitas rancangan pengendalian dapat dilakukan dengan pendekatan asersi manajemen atas laporan keuangan. Pendekatan ini berguna untuk menilai efektivitas rancangan pengendalian pada tingkat transaksi. Hasil pada tahap perencanaan dapat dimanfaatkan untuk menilai apakah pengendalian yang dirancang sudah efektif.

   Apabila pengendalian yang ada dianggap telah cukup dan tepat untuk menjamin asersi yang terkait maka kesimpulannya adalah rancangan telah memadai. Apabila pengendalian yang ada tidak tepat maka kesimpulan rancangan tidak memadai sehingga perlu diuraikan kelemahan dan rekomendasinya. Kelemahan ini akan dipertimbangkan dalam penyusunan kesimpulan efektivitas pengendalian intern secara keseluruhan.

   Prosedur uji efektivitas rancangan pengendalian meliputi: wawancara personel terkait, observasi operasional satker, serta inspeksi dokumen yang relevan. *Walkthrough* juga dapat

www.peraturan.go.id

dilakukan dalam melakukan uji rancangan pengendalian ini. Untuk melakukan penilaian efektivitas rancangan pengendalian dapat menggunakan Tabel A yang telah disusun oleh lini manajemen pada saat Penerapan PIPK (kolom 1 sampai dengan 9) dan melengkapinya dengan melakukan penilaian pada kolom 10 dan isian Simpulan serta isian Usulan Koreksi (*feedback*).

Dalam melakukan penilaian efektivitas rancangan pengendalian, Tim Penilai mempertimbangkan apakah terdapat risiko atas asersi terhadap akun signifikan. Dalam hal terdapat risiko atas asersi terhadap akun-akun signifikan maka Tim Penilai harus memastikan adanya pengendalian utama terhadap risiko tersebut. Dalam hal seharusnya terdapat risiko atas asersi terhadap akun-akun signifikan namun tidak diungkapkan oleh pemilik pengendalian, Tim Penilai harus menyampaikan usulan koreksi (*feedback*) terkait risiko tersebut beserta rancangan pengendalian utamanya. Tidak terdapatnya risiko atas asersi terhadap akun-akun signifikan tidak mempengaruhi rancangan pengendalian. Dalam hal isian Simpulan berisi "Tidak Cukup" maka Tim Penilai memberikan usulan koreksi (*feedback*) kepada manajemen untuk melakukan perbaikan yang bila dilaksanakan maka Tim Penilai dapat melengkapi Tabel A tersebut dengan Tabel A.1 Perbaikan Identifikasi Risiko dan Pengendaliannya khusus untuk proses/transaksi utama yang diperbaiki atau yang baru. Pembuatan Tabel A.1 dilaksanakan dengan langkah-langkah sebagai berikut yaitu:

a) penentuan akun signifikan;
b) mengidentifikasi proses/transaksi utama pelaporan keuangan;
c) mengidentifikasi risiko utama;
d) mengidentifikasi pengendalian utama;
e) mendokumentasikan proses utama dan pengendalian utama yang berkaitan; dan
f) memahami infrastruktur TIK dan risiko-risikonya.

www.peraturan.go.id

Penjelasan lebih rinci dari setiap langkah dapat diuraikan sebagai berikut:

a) Penentuan akun signifikan. Langkah awal identifikasi proses utama pelaporan keuangan adalah mengidentifikasi akun yang signifikan pada laporan keuangan. Akun atau kelompok akun merupakan akun signifikan apabila memiliki kemungkinan salah saji yang material, atau menurut pertimbangan manajemen perlu dievaluasi karena alasan tertentu. Faktor-faktor yang harus dipertimbangkan dalam menentukan apakah suatu akun merupakan akun signifikan antara lain:
   (1) Ukuran dan komposisi akun termasuk kerentanannya terhadap kecurangan.
   (2) Jumlah dan nilai serta kompleksitas dan keseragaman proses transaksi atas akun tersebut.
   (3) Sejauh mana subjektivitas dan pertimbangan dalam menentukan saldo akun tersebut.
   (4) Sifat akun tersebut (misalnya akun *suspen* pada umumnya memperoleh perhatian yang lebih besar).
   (5) Kompleksitas perlakuan akuntansi dan pelaporan yang berkenaan dengan akun tersebut.

b) Mengidentifikasi proses/transaksi utama pelaporan keuangan. Setelah menentukan akun yang signifikan, Tim Penilai selanjutnya mengidentifikasi proses/ transaksi utama dan aktivitas akuntansi yang mempengaruhi akun tersebut. Aktivitas akuntansi termasuk aktivitas membuat dan mencatat estimasi akuntansi atau untuk menyelesaikan pelaporan keuangan pada akhir periode akuntansi.

   Hal penting yang harus diperhatikan berkenaan dengan proses utama adalah tingkat ketergantungannya pada Teknologi Informasi dan Komunikasi. Tim Penilai pada umumnya harus mendokumentasikan Sistem Teknologi Informasi dan Komunikasi yang digunakan untuk memproses transaksi utama. Dalam kondisi

www.peraturan.go.id

ketidakcukupan sumber daya yang memahami Teknologi Informasi dan Komunikasi, keterlibatan konsultan dapat dipertimbangkan.

c) Mengidentifikasi risiko utama.

Langkah selanjutnya adalah mengidentifikasi risiko atau "apa yang bisa salah" pada proses/transaksi. Dengan mengidentifikasi risiko, Tim Penilai akan dapat memusatkan perhatian pada pengendalian yang relevan dan efektif dalam mencegah dan mendeteksi kesalahan penyajian atau kecurangan.

Tim Penilai harus menentukan risiko pelaporan keuangan yang akan dievaluasi dan pengaruhnya terhadap kewajaran laporan keuangan. Dalam mengidentifikasi jenis kesalahan yang dapat terjadi, Tim Penilai harus mempertimbangkan asersi laporan keuangan atas akun signifikan. Untuk setiap proses utama, Tim Penilai harus mengidentifikasi titik-titik dalam aliran proses/transaksi saat data diinisiasi, dikirimkan, atau diubah yang memungkinkan terjadinya kesalahan. Pada titik-titik tersebut, pengendalian dibutuhkan untuk menjamin tercapainya asersi atas laporan keuangan yang wajar. Identifikasi apa yang bisa salah akan membantu Tim Penilai menemukan titik-titik dalam aliran transaksi yang mungkin terjadi kesalahan mencapai tujuan pelaporan keuangan dan mengidentifikasikan pengendalian yang sesuai. Contohnya risiko pada pengeluaran kas antara lain pengeluaran kas dan transfer tidak dicatat pada periode yang tepat, pengeluaran kas tidak diberi kode untuk menjamin kelengkapan, dua kali posting pengeluaran kas ke Buku Besar (*Ledger*), pengeluaran kas yang tidak riil, dan jumlah yang dikeluarkan tidak sama dengan yang seharusnya dibayar.

d) Mengidentifikasi pengendalian utama. Pengendalian utama mengacu pada akun yang signifikan atau risiko

www.peraturan.go.id

yang signifikan. Pengendalian utama pada umumnya memiliki karakteristik sebagai berikut:

(1) kegagalan pengendalian tersebut akan mempengaruhi tujuan kegiatan dan tidak dapat dideteksi secara tepat waktu oleh pengendalian-pengendalian yang lain; dan/ atau

(2) pelaksanaan pengendalian tersebut akan mencegah atau mendeteksi kegagalan sebelum kegagalan tersebut memiliki pengaruh material terhadap tujuan kegiatan.

Pada proses ini, Tim Penilai mengidentifikasi pengendalian yang memberikan keyakinan memadai bahwa kesalahan terkait asersi laporan keuangan dapat dicegah atau kesalahan selama proses transaksi dapat dideteksi dan diperbaiki. Proses transaksi tersebut meliputi inisiasi, pencatatan, pemrosesan, dan pelaporan transaksi.

Pada umumnya, pengendalian dibagi menjadi dua yaitu pengendalian preventif (*preventive control*) dan pengendalian detektif (*detective control*). Pengendalian preventif adalah prosedur yang dirancang untuk mencegah kesalahan atau kecurangan. Pengendalian preventif ini biasa diterapkan pada satu transaksi. Pengendalian detektif adalah kebijakan dan prosedur yang dirancang untuk memantau pencapaian tujuan proses tertentu termasuk mengidentifikasi kesalahan atau kecurangan. Pengendalian detektif dapat diterapkan pada sekelompok transaksi. Pengendalian utama dapat diidentifikasi dari rancangan pengendalian yang ada. Rancangan pengendalian tersebut dapat berupa SOP, Peraturan, Pedoman, atau kebijakan lainnya.

e) Mendokumentasikan proses utama dan pengendalian utama yang berkaitan.

Tim Penilai harus mendokumentasikan proses utama pelaporan keuangan dan pengendalian utamanya.

www.peraturan.go.id

Dokumentasi tersebut dapat berupa bagan alur, kuesioner, kebijakan atau pedoman akuntansi, dsb. Untuk penilaian pengendalian intern yang pertama kali, Tim Penilai harus memanfaatkan dokumen yang tersedia dalam organisasi. Meskipun demikian, dokumen dalam bentuk bagan alur disarankan untuk digunakan karena lebih memudahkan dan mempercepat pemahaman.

Bila perlu Tim Penilai dapat melakukan peninjauan (*walkthrough*) untuk memastikan bahwa proses signifikan yang didokumentasikan masih sesuai dan mutakhir.

Memahami infrastruktur TI dan risiko-risikonya. Dengan semakin berkembangnya TIK, perannya pun semakin meningkat dalam pengembangan PIPK. Tim Penilai harus menilai pengendalian intern berbasis TIK. Meskipun penilaian pengendalian intern yang berbasis TIK membutuhkan keahlian khusus, penilaian pengendalian intern ini harus dilakukan bersamaan dengan penilaian atas pengendalian intern yang dilakukan secara manual. Tim Penilai harus memahami proses pelaporan keuangan dan sejauh mana proses ini dipengaruhi oleh TIK. Aplikasi-aplikasi utama harus diperhatikan dalam menilai PIPK. Setelah memahami operasi penyiapan laporan keuangan, Tim Penilai harus menilai risiko inheren dan risiko pengendalian berkaitan dengan sistem informasi.

f) Penyusunan Tabel A.1 Hasil dari langkah-langkah di atas dituangkan dalam Tabel A. l sebagai berikut:

www.peraturan.go.id

Tabel A.1.Perbaikan Identifikasi Risiko dan Pengendaliannya

Nama Entitas Akuntansi/Pelaporan:

Akun Signifikan: (diisi dengan akun-akun signifikan terkait)

No	Proses/ Transaksi Utama	Risiko Utama	Nama Pengendalian Utama	Aplikasi pendukung	Pelaksana Pengendalian	Dokumen Pendukung	Tipe Pengendalian	Asersi	Memadai Ya/Tidak
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Tanggal Penyusunan:									
Paraf Tim Penilai/Tanggal:									

Keterangan:

Berisi hanya Proses/Transaksi Utama yang kolom (10) Tabel A berisi "Tidak" serta Proses/Transaksi Utama baru hasil dari Tim Penilai dan hanya dibuat bila Tim Penilai telah meyakini bahwa pengendalian utamanya telah memadai sehingga dapat mengisi kolom (10) Tabel A. 1 dengan isian "Ya".

(1) : Diisi nomor urut sebagaimana Tabel A. Bila terdapat rekomendasi identifikasi baru, nomor urut merupakan nomor setelah nomor terakhir dari Tabel A.

(2) : Diisi proses/transaksi utama yang terkait akun signifikan tersebut.

(3) : Diisi risiko utama pada proses atau transaksi.

(4) : Diisi dengan Nomor pada kolom (1) diikuti tanda hubung (-) diikuti bentuk aktivitas pengendalian seperti pengendalian akses, pemeriksaan fisik, persetujuan, reviu atas persetujuan, validasi, monitoring, inventarisasi, penelitian lebih lanjut, klarifikasi, verifikasi keakuratan akun, rekonsiliasi, pengendalian input (aplikasi). Contoh: 1-Validasi, 2-Rekonsiliasi, 3-Validasi, 4-Monitoring, 5-Klarifikasi, 6-Rekonsiliasi, 7-Validasi, 8-Pengendalian input (aplikasi) dll.

Catatan: Perhatikan contoh terdapat 3 (tiga) validasi yang dibedakan satu sama lain dengan nomor sehingga terdapat Nama Pengendalian Utama 1-Validasi, 3-Validasi, dan 7-Validasi.

www.peraturan.go.id

(5) : Diisi aplikasi yang khusus, misal: SIMAK BMN, SPAN, dll.

(6) : Diisi pemilik pengendalian.

(7) : Diisi dokumen terkait, misal: kuitansi, kontrak, SPM, SP2D, dll.

(8) : Diisi dengan tipe pengendalian dengan rincian:

a. Manual

b. Aplikasi

c. ITDM (IT *Dependent Manual*)

d. Pengendalian Umum TIK

(9) : Diisi jenis asersi terkait: *Completeness, Existence and Occurance, Valuation and Allocation, Rights and Obligation, Presentation and Disclosure*.

(10) : Diisi dengan "Ya" bila ada pengendalian utama (5) yang memitigasi risiko utama (3).

Dalam hal isian simpulan berisi "Tidak Cukup" dan usulan koreksi (*feedback*) kepada manajemen untuk melakukan perbaikan tidak dilaksanakan maka terhadap Proses/ Transaksi Utama yang tidak memadai (kolom 10 terisi "Tidak") dilakukan penelitian lebih lanjut dampak dari ketidak memadaiannya. Kelemahan tersebut dinyatakan sebagai "Kelemahan Tidak Signifikan" bila basil penelitian lebih lanjut salah saji teridentifikasi di bawah 0,1 % (nol koma satu persen) dari Total aktiva/penerimaan/pembiayaan, dinyatakan "Kelemahan Signifikan" bila salah saji teridentifikasi 0,1%-0,5% dari total aktiva/penerimaan/ pembiayaan, dinyatakan "Kelemahan Material" bila salah saji teridentifikasi melewati batas materialitas 0,5% (nol koma lima persen) dari Total Aktiva/ penerimaan/pembiayaan.

2) Penilaian Efektivitas Implementasi Pengendalian

Penilaian efektivitas implementasi pengendalian di antaranya dilakukan dengan pengujian atribut pengendalian. Atribut pengendalian dibagi menjadi dua, yaitu atribut pengendalian berupa aktivitas dan berupa kriteria. Atribut pengendalian berupa kriteria merupakan jenis pengendalian yang

www.peraturan.go.id

menggunakan sistem atau kriteria khusus dalam rangka menghasilkan output tertentu. Pengujian untuk jenis pengendalian ini dilakukan dengan melihat apakah kriteria yang ditetapkan telah berjalan sebagaimana mestinya. Contohnya salah satu bentuk pengendalian dalam penerbitan Surat Perintah Membayar (SPM) melalui aplikasi adalah penomoran secara otomatis untuk mencegah adanya nomor SPM yang sama atau tidak urut. Prosedur pengujian terhadap atribut pengendalian ini dilakukan dengan mengecek kolom input nomor SPM apakah dapat dirubah secara manual. Contoh lainnya adalah pengendalian berupa pemisahan fungsi antara fungsi penyimpanan uang dan fungsi pencatatannya sehingga kita hanya menguji satu kali saja apakah pemisahan fungsi tersebut berjalan sebagaimana mestinya. Atribut pengendalian berupa aktivitas merupakan Jenis pengendalian yang dilakukan secara manual dan berulang dalam rangka menghasilkan output tertentu. Pengujian terhadap aktivitas dilakukan untuk melihat konsistensi pelaksanaan pengendalian. Contohnya pelaksanaan pengujian terhadap pengendalian verifikasi dengan melihat ada tidaknya atribut pengendalian tanda tangan. Untuk mendukung pengujian atribut pengendalian dilakukan *reperformance* (reviu ulang suatu pekerjaan) terutama dalam rangka melihat dampak terhadap salah saji yang diakibatkan pengendalian yang tidak andal.

Pengujian keandalan PIPK jenis aktivitas dapat dilakukan dengan Tabel C. 1 berikut ini:

Tabel C. 1. Pengujian Atribut Pengendalian

Nama Entitas Akuntansi/Pelaporan:

Akun Signifikan: (diisi dengan akun-akun signifikan terkait)

No	Nama Pengendalian Utama	Nomor sampel/ Dokumen	Atribut utama Pengendalian (V/-)	Hasil Reperformance
(1)	(2)	(3)	(4)	(5)
*Pengendalian Utama yang Tidak Andal:				

www.peraturan.go.id

Keterangan:

(1) : Diisi nomor.

(2) : Diisi Nama Pengendalian Utama dengan tipe pengendalian manual/ITDM.

(3) : Diisi nomor sampel/ dokumen

(4) : Diisi "V" bila atribut pengendalian utama ada, diisi "-" bila atribut pengendalian utamanya tidak ada.

Dalam hal menggunakan sensus dan terdapat lebih dari 5% (lima persen) dari kolom (4) berisi "-" maka disimpulkan "Tidak Andal" Dalam hal menggunakan uji petik, bila dari 77 atau 93 sampel (tergantung ARO) untuk setiap pengendalian utama terdapat lebih dari 1 pada kolom (4) yang berisi "-" maka disimpulkan "Tidak Andal"

(5) : *Reperformance* hanya dilakukan bila simpulan keandalannya "Tidak Andal". *Reperformance* dilakukan terhadap dokumen yang tidak ada atribut pengendaliannya. Diisi dengan "Tidak Ada Kelemahan/Kelemahan Tidak Signifikan/Kelemahan Signifikan/Kelemahan Material"

* : Diisi Nama Pengendalian Utama yang Tidak Andal.

Pengujian keandalan PIPK Jems aktivitas secara sensus maupun secara uji petik dengan ketentuan sebagai berikut:

a) Sensus dilakukan ketika jumlah populasi yang diuji kurang dari 100 (seratus). Untuk populasi dengan jumlah 100 (seratus) hingga 499 (empat ratus sembilan puluh sembilan) dapat dipilih dilakukan pengujian secara sensus atau secara uji petik. Jika jumlah populasi 500 (lima ratus) atau lebih, maka dilakukan pengujian secara uji petik.

b) Tingkat Penyimpangan yang Ditoleransi (*Tolerable Deviation Rate*/TDR), dengan mempertimbangkan Tingkat Risiko Pengendalian dinilai yang Direncanakan (*Planned Assessed Level of Control Risk*/PALCR) berada pada tingkat rendah, ditetapkan 5% (lima persen).

www.peraturan.go.id

c) Pada pengujian secara sensus, ketidakpatuhan dapat disajikan dalam bentuk Tingkat Penyimpangan (*Deviation Rate*/DR), yaitu jumlah ketidakpatuhan dibagi populasi dikalikan 100% (seratus persen), yang kemudian dibandingkan dengan TDR (5% (lima persen)). Jika DR < 5% (lima persen) yang berarti DR < TDR maka pengendalian intern disimpulkan teruji keandalannya dan berpeluang menjadi pengendalian intern yang efektif. Jika DR > 5% (lima persen) yang berarti DR > TDR maka pengendalian intern disimpulkan tidak teruji keandalannya dan berarti tidak efektif.

d) Pada pengujian secara uji petik, sampel ditentukan dengan tabel ukuran sampel atribut (*Attributes Sample Size Table*). Sampel tersebut dipengaruhi oleh Risiko terhadap Ketergantungan kepada Pengendalian Intern yang Diterima (*Acceptable Risk of Overreliance*/ARO), TDR, dan Tingkat Penyimpangan Populasi yang Diharapkan (*Expected Population Deviation Rate*/EPDR). Penentuan sampel untuk menguji keandalan PIPK dalam peraturan ini, dengan didasarkan atas pertimbangan tertentu, ditentukan sebagai berikut:

   (1) ARO ditetapkan sebesar 10% (sepuluh persen) apabila hasil Penilaian Pengendalian Intern Tingkat Entitas-nya tinggi, dan 5% (lima persen) apabila hasil Penilaian Pengendalian Intern Tingkat Entitas-nya sedang dan rendah;

   (2) TDR, dengan mempertimbangkan Tingkat Risiko Pengendalian dinilai yang direncanakan (*Planned Assessed Level of Control Risk*/PALCR) berada pada tingkat rendah, ditetapkan 5% (lima persen); dan

   (3) EPDR ditetapkan rendah sebesar 1 % (satu persen).

Tahapan pengujiannya adalah sebagai berikut:

a) Uji pengendalian, baik menggunakan sensus atau uji petik, tergantung jumlah populasi dan hasil penilaian Pengendalian Intern Tingkat Entitas.

www.peraturan.go.id

Jika hasil penilaian Pengendalian Intern Tingkat Entitasnya tinggi, maka:

(1) Untuk populasi dengan jumlah kurang dari 100 (seratus), pengujian dilakukan secara sensus.

(2) Untuk populasi dengan jumlah 100 (seratus) hingga 499 (empat ratus sembilan puluh sembilan), pengujian dapat dilakukan secara sensus atau secara uji petik. Apabila menggunakan uji petik, maka jumlah sampel minimal diperoleh dengan rumus n definitif = 77'1(1 - (77 /N)).

(3) Untuk populasi dengan jumlah 500 (lima ratus) atau lebih, pengujian dilakukan secara uji petik dengan jumlah sampel minimal 77 (tujuh puluh tujuh).

b) Jika hasil penilaian Pengendalian Intern Tingkat Entitasnya sedang atau rendah, maka:

(1) Untuk populasi dengan jumlah kurang dari 100 (seratus), pengujian dilakukan secara sensus.

(2) Untuk populasi dengan jumlah 100 (seratus) hingga 499 (empat ratus sembilan puluh sembilan), pengujian dapat dilakukan secara sensus atau secara uji petik. Apabila menggunakan uji petik, maka jumlah sampel minimal diperoleh dengan rumus n definitif = 93-V(l - (93/N)).

(3) Untuk populasi dengan jumlah 500 (lima ratus) atau lebih, pengujian dilakukan secara uji petik dengan jumlah sampel minimal 93 (sembilan puluh tiga).

c) Simpulkan keandalan pengendalian utama dengan ketentuan sebagai berikut:

(1) Untuk pengujian secara sensus, bila ketidakpatuhan atas populasi tersebut tidak melebihi 5% (lima persen), maka disimpulkan andal. Bila di atas 5% (lima persen), disimpulkan tidak andal.

(2) Untuk pengujian secara uji petik, jika ketidakpatuhan atas sampel tidak melebihi 1 (CUDR >5% (lima persen)), maka disimpulkan andal. Bila

www.peraturan.go.id

ketidakpatuhan lebih dari 1 (CUDR>5% (lima persen)), maka disimpulkan tidak andal.

(3) Tuangkan keterandalan pengendalian utama ke dalam Tabel C.1

Pengujian keandalan PIPK Jenis kriteria diantaranya pengujian pengendalian aplikasi. Pengujian pengendalian aplikasi dilakukan dengan menggunakan Tabel C.2 berikut ini:

Tabel C.2 Pengujian Pengendalian Aplikasi

Nama Entitas Akuntansi/Pelaporan:

Nama Aplikasi:

Akun Signifikan: (diisi dengan akun-akun signifikan terkait)

No	Nama Pengendalian Utama	Pengujian yang dilakukan	Hasil Pengujian	Hasil Penelitian Lanjutan
(1)	(2)	(3)	(4)	(5)
*Pengendalian Utama yang Tidak Andal:				

Keterangan:

(1) : Diisi nomor

(2) : Diisi nama pengendalian utama dengan tipe pengendalian aplikasi.

(3) : Diisi dengan menguji asersi keakuratan input atas field-field pada *form* aplikasi dan menguji asersi kelengkapan atas *field-field* yang wajib diisi pada *form* aplikasi.

(4) : Dalam hal hasilnya tidak sesuai dengan rancangannya maka simpulkan tidak andal, bila sesuai disimpulkan andal.

(5) : Penelitian Lanjutan hanya dilakukan bila simpulan keandalannya "Tidak Andal". Penelitian Lanjutan dilakukan dengan meneliti kesalahan data-data yang telah direkam. Diisi dengan "Tidak Ada Kelemahan/ Kelemahan Tidak Signifikan/Kelemahan Signifikan/ Kelemahan Material"

5. Penilaian Efektivitas Pengendalian dan Kelemahan Pengendalian.

Dari pengujian pengendalian intern tingkat entitas (Tabel B.1),

www.peraturan.go.id

pengujian PUTIK (Tabel B.2), pengujian atribut pengendalian (Tabel C.1), dan pengujian pengendalian aplikasi (Tabel C.2), dihasilkan simpulan efektivitas implementasi dan penilaian kelemahan pengendalian. Tingkatan kelemahan diklasifikasikan sebagai berikut:

a. Kelemahan tidak signifikan (*inconsequentian*). Suatu kelemahan, atau kombinasi dari beberapa kelemahan, yang pengaruhnya tidak material terhadap pelaporan keuangan. Secara umum, diklasifikasikan Kelemahan Tidak Signifikan bila hasil penilaian "TL Tuntas" atau hasil penilaian "TL Tidak Tuntas" tapi salah saji teridentifikasi di bawah 0,1 % (nol koma satu persen) dari total aktiva atau 0,1 % (nol koma satu persen) dari total penerimaan atau total pembiayaan tergantung dari relevansinya dengan akun signifikan. Dalam hal hanya terdapat informasi berupa total aktiva maka salah saji diidentifikasi 0,1 % (nol koma satu persen) dari total aktiva.

b. Kelemahan signifikan (*significant deficiency*). Suatu kelemahan, atau kombinasi dari beberapa kelemahan, yang berpengaruh cukup material terhadap pelaporan keuangan. Secara umum diklasifikasikan Kelemahan Signifikan bila hasil penilaian "TL Tidak Tuntas" dan salah saji teridentifikasi berkisar 0,1 %-0,5% dari total aktiva atau 0,1 %-0,5% dari total penerimaan atau total pembiayaan tergantung dari relevansinya dengan akun signifikan. Dalam hal hanya terdapat informasi berupa total aktiva maka salah saji diidentifikasi 0,1 %-0,5% dari total aktiva.

c. Kelemahan material (*material weakness*). Suatu kelemahan, atau kombinasi dari beberapa kelemahan signifikan, yang berpengaruh material terhadap pelaporan keuangan. Secara umum diklasifikasikan Kelemahan Material bila hasil penilaian "TL Tidak Tuntas" dan salah saji teridentifikasi melewati batas materialitas 0,5% (nol koma lima persen) dari total aktiva atau melewati batas materialitas 0,5% (nol koma lima persen) dari total penerimaan atau total pembiayaan tergantung dari relevansinya dengan akun signifikan. Dalam hal hanya terdapat informasi berupa total aktiva maka salah saji diidentifikasi melewati batas materialitas 0,5% (nol koma lima persen) dari total aktiva.

www.peraturan.go.id

Selain pengklasifikasian secara umum seperti tersebut di atas. Tim Penilai dapat mempertimbangkan 5 (lima) faktor lain berikut ini:

a. memiliki indikasi adanya kecurangan (*fraud*);
b. tingkat pertimbangan subjektif dan kompleksitas dalam menentukan nilai akun;
c. kemungkinan kelemahan terjadi secara berulang;
d. besarnya saldo akun termasuk besarnya nilai kelemahan secara relatif terhadap saldo akun, dan transaksi yang terpengaruh serta asersi laporan keuangan yang terlibat; dan
e. kelemahan Pengendalian Intern Tingkat Entitas yang secara signifikan mempengaruhi laporan keuangan.

Dalam hal Tim Penilai menggunakan pertimbangan faktor-faktor lain dalam pengklasifikasian kelemahan pengendalian, Tim Penilai harus menjelaskan pertimbangan faktor-faktor lain yang digunakan dalam pengklasifikasian kelemahan pengendalian tersebut. Hasil tersebut dituangkan pada Tabel D Penilaian Efektivitas Implementasi Pengendalian dan Kelemahan Pengendalian berikut ini:

Tabel D Penilaian Efektivitas lmplementasi Pengendalian dan Penilaian Kelemahan Pengendalian

Nama Entitas Akuntansi/Pelaporan:

Akun Signifikan: (diisi dengan akun-akun signifikan terkait)

No	Nama Pengendalian Utama	Simpulan Efektifitas Implementasi	Usulan koreksi *(feed back)*	TL (Tindak Lanjut)	Hasil Penilaian Kelemahan
(1)	(2)	(3)	(4)	(5)	(6)
*Keterangan : **Total salah saji teridentifikasi: **"Simpulan PIPK:					

Keterangan:

(1) : Diisi nomor urut.

(2) : Diisi nama Faktor-faktor dinilai tingkat entitas yang tidak efektif berdasarkan Tabel B. 1 dan B.2 dan Nama Pengendalian Utama yang ada di Tabel C. 1 dan C.2.

www.peraturan.go.id

(3) : Diisi dengan "Efektif/ Tidak Efektif' berdasarkan data dari Tabel B. l, B.2, C. l, dan C.2.

Efektif bila tidak ada kelemahan atau ada kelemahan tidak signifikan.

Tidak Efektif bila ada kelemahan signifikan atau kelemahan material.

(4) : Diisi dengan ketentuan: Berasal dari Tabel B.l, B.2, dan C.2, maka:

a. Diisi dengan "-" bila hasil penelitian lanjutan pada Tabel B .1 menunjukkan tidak ada kelemahan atau ada kelemahan tidak signifikan.

b. Diisi dengan usulan koreksi (*feed back*) yang diperlukan untuk mengoreksi kelemahan yang ditimbulkan bila hasil penelitian lanjutan Tabel B.1 menunjukkan ada kelemahan signifikan.

Berasal dari Tabel C.1:

a. Diisi dengan "-" bila hasil *reperformance* Tabel C.1 menunjukkan tidak ada kelemahan atau ada kelemahan tidak signifikan.

b. Diisi dengan usulan koreksi (*feed back*) yang diperlukan untuk mengoreksi kelemahan yang ditimbulkan bila hasil *reperformance* Tabel C.1 menunjukkan ada kelemahan signifikan.

(5) : Diisi TL (Tindak Lanjut) dengan "TL Tuntas" apabila dilakukan sesuai usulan koreksi (feedback) atau "TL Tidak Tuntas" disertai identifikasi salah sajinya: di bawah 0,1 %, 0,1%-0,5%, atau lebih dari 0,5% dari Total Aktiva/ penerimaan/pembiayaan, diisi "Kelemahan Tidak Signifikan" bila hasil penilaian "TL Tuntas" atau hasil penilaian "TL Tidak Tuntas" tapi salah saji teridentifikasi di bawah 0,1% dari Total aktiva/penerimaan/pembiayaan.

(6) : Diisi "Kelemahan Signifikan" bila hasil penilaian "TL Tidak Tuntas" dan salah saji teridentifikasi 0,1%-0,5% dari total aktiva/penerimaan/pembiayaan.

diisi "Kelemahan Material" bila hasil penilaian "TL Tidak

www.peraturan.go.id

Tuntas" dan salah saji teridentifikasi melewati batas materialitas 0,5% dari Total Aktiva/penerimaan/ pembiayaan.

(*) : Dalam hal digunakan lima faktor lain dalam pertimbangan, maka pada Keterangan dijelaskan penggunaan pertimbangan atas faktor lain yang digunakan untuk mengklasifikasikan kelemahan.

(**) : Diisi salah saji keseluruhan teridentifikasi) atau "-" bila tidak terdapat salah saji yang teridentifikasi.

(***) : Diisi simpulan PIPK

Pengendalian Intern Efektif (PIE) bila terdapat tidak terdapat Kelemahan Material atau Kelemahan Signifikan.

Pengendalian Intern Efektif dengan Pengecualian (PIEDP) bila tidak terdapat Kelemahan Signifikan. Pengendalian Intern Mengandung Kelemahan Material (PIMKM) bila terdapat Kelemahan Material. Simpulan PIPK ini juga harus mempertimbangkan salah saji keseluruhan yang telah teridentifikasi.

6. Kompilasi Simpulan Pengendalian Intern Secara Keseluruhan Simpulan pengendalian intern dapat dijadikan dasar bagi manajemen dalam membuat pernyataan efektivitas pengendalian intern secara berjenjang dari tingkat Entitas Akuntansi sampai dengan UAPA. Simpulan-simpulan pengendalian intern dikompilasi secara berjenjang termasuk dikompilasi pada Entitas Akuntansi yang melakukan kompilasi seperti UAPPA-El.

Kompilasi simpulan didasarkan pada hasil penilaian efektivitas implementasi pengendalian yang terdapat pada kolom (6) Tabel D Penilaian Efektivitas Implementasi Pengendalian dan Kelemahan Pengendalian.

Pelaksanaan kompilasi penilaian pengendalian intern pada tingkat Entitas Pelaporan UAPA menggunakan Tabel E Penilaian Kelemahan Gabungan sebagai berikut:

www.peraturan.go.id

- 76 -

Tabel E Penilaian Kelemahan Gabungan

(Nama Entitas Akuntansi yang Melakukan Kompilasi/Entitas Pelaporan)

Uraian Kelemahan	UAPA/ Unit Terkait	Entitas Akuntansi di bawahnya	Entitas Akuntansi di bawahnya	Rata-rata	Simpulan Sebelum Penyesuaian	Penyesuaian	Simpulan menurut Tim (Penilai UAPA/ Unit Terkait
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Keterangan: * Total salah saji teridentifikasi gabungan: **Simpulan PIPK gabungan:							

Keterangan:

(1) : Diisi deskripsi kelemahan;

(2) s.d (4) : (1) Diisi tingkatan kelemahan yang sama pada unit terkait, yaitu:

Angka "l" bila kelemahan tidak signifikan /*inconsequential*;

Angka "2" bila kelemahan signifikan/*significant deficiency*;

Angka "3" bila kelemahan material/material *weakness*;

Kolom (3) dan (4) dapat diperbanyak sesuai kondisi

(5) : Diisi nilai rata-rata kolom (2) s.d. (4);

(6) : Diisi dengan tingkatan kelemahan rata-rata seluruh unit kerja yaitu:

Angka "O" bila nilai kolom (5) adalah tidak ada kelemahan (kelemahan tereliminasi)

Angka "l" bila nilai kolom (5) adalah 1,0 s.d. 1,5 -> kelemahan tidak signifikan/*inconsequential*;

Angka "2" bila nilai kolom (5) adalah 1,6 s.d. 2,5 ->kelemahan signifikan/*significant deficiency*;

Angka "3" bila nilai kolom (5) adalah 2,6 s.d. 3,0 ->kelemahan material/ material *weakness*;

(7) : Diisi nilai penyesuaian oleh Tim Penilai tingkat wilayah/eselon I, yaitu:

Angka "l" untuk penyesuaian satu tingkat di atas simpulan awal;

www.peraturan.go.id

Angka "1" untuk penyesuaian di tingkat bawah simpulan awal;
Angka "O" bila tidak ada penyesuaian;
Penyesuaian terutama didasarkan atas persentase nilai saji teridentifikasi terhadap nilai Aktiva atau pertimbangan lainnya dengan ketentuan:
Dapat berubah menjadi Kelemahan Tidak Signifikan bila salah saji teridentifikasi di bawah 0,1 % dari Total Aktiva dari seluruh unit kompilasi.
Dapat berubah menjadi Kelemahan Signifikan bila salah saji teridentifikasi berkisar 0,1%-0,5% dari Total Aktiva dari seluruh unit kompilasi.
Dapat berubah menjadi Kelemahan Material bila

www.peraturan.go.id