

Pedoman Audit Sistem Informasi (PASI) Ikatan Audit Sistem Informasi Indonesia (IASII)

P-1 Penugasan Audit Sistem Informasi

1. Penugasan Audit Sistem Informasi dapat dituangkan dalam bentuk Piagam atau Surat Tugas Audit Sistem Informasi untuk auditor internal, dan Surat Tugas atau Surat Perintah Kerja untuk auditor eksternal.
2. Piagam atau Surat Tugas Audit Sistem Informasi harus menjelaskan tentang tujuan, lingkup, tanggung jawab, wewenang, akuntabilitas, periode atau jangka waktu, dan pelaporan dari Audit Sistem Informasi.
3. Piagam atau Surat Tugas Audit Sistem Informasi harus disetujui secara bersama oleh Auditor Sistem Informasi dan pemberi tugas.

P-2 Independensi dan Obyektifitas Auditor Sistem Informasi

1. Auditor Sistem Informasi harus membuat suatu surat pernyataan independensi, untuk memberikan suatu jaminan independensi dan obyektifitasnya dari organisasi atau hal yang diaudit, khususnya dalam berbagai hal yang berkaitan dengan Audit Sistem Informasi.
2. Auditor Sistem Informasi harus memperhatikan dan menghindari serta hal-hal yang dapat mengganggu independensi dan obyektifitasnya, yaitu antara lain :
 1. Hubungan struktural, profesional, pribadi, maupun finansial yang dapat mengakibatkan auditor membatasi pelaksanaan pengujian, membatasi informasi yang disampaikan, atau mengurangi temuan audit Sistem Informasi, dalam bentuk apapun;
 2. Anggapan atau pandangan terhadap sekumpulan individu, kelompok, organisasi atau tujuan dari suatu kegiatan tertentu yang dapat mengakibatkan tujuan maupun hasil audit Sistem Informasi menjadi bias;
 3. Tanggung jawab sebelumnya yang terkait dengan pengambilan keputusan atau pengelolaan dari sebuah entitas (organisasi, unit kerja, kelompok kerja, kepanitiaan, atau yang sejenis), dalam jangka waktu 2 (dua) tahun sebelumnya, yang dapat mempengaruhi operasional dari entitas atau kegiatan yang sedang diaudit;
 4. Berbagai hal yang dapat mengakibatkan bias, seperti adanya suatu keharusan politis atau sosial yang diakibatkan oleh keterlibatan dalam atau kewajiban kepada suatu kelompok, organisasi, atau jabatan pemerintahan tertentu.
 5. Kepentingan finansial, baik secara langsung maupun secara tidak langsung, terhadap entitas atau kegiatan yang sedang diaudit.
 6. Pelaksanaan audit Sistem Informasi berkelanjutan oleh individu yang sama yang sebelumnya terlibat dan menyetujui perancangan dan implementasi sistem informasi dari entitas atau kegiatan yang sedang diaudit.
 7. Adanya suatu penawaran atau pengajuan lamaran atas suatu posisi di entitas atau kegiatan yang diperiksa, dalam jangka waktu 1 (satu) tahun sebelumnya, termasuk jika penawaran atau pengajuan lamaran tersebut terjadi pada saat audit sedang berlangsung.
3. Auditor Sistem Informasi wajib mengungkapkan kondisi-kondisi yang dapat mengganggu independensi dan obyektifitasnya dalam pelaporan hasil pemeriksaan dan pengawasan.
4. Auditor Sistem Informasi wajib merahasiakan seluruh informasi yang terkait dengan Audit Sistem Informasi, kecuali ditentukan lain oleh peraturan perundang-undangan atau atas permintaan pengadilan.

P-3 Profesionalisme dan Kompetensi Auditor Sistem Informasi

1. Auditor Sistem Informasi harus memastikan bahwa dalam merencanakan, melaksanakan, mengawasi, dan melaporkan penugasannya, Auditor Sistem Informasi telah dan hanya menggunakan pendekatan dan metode yang sesuai dengan peraturan perundang-undangan, serta sesuai dengan kode etik dan standar profesi yang berlaku bagi Auditor Sistem Informasi.
2. Auditor Sistem Informasi dalam menerapkan prinsip kehati-hatian profesional dalam merencanakan, melaksanakan, mengawasi dan melaporkan penugasan auditnya, dengan memperhatikan hal-hal sebagai berikut :
 1. Lingkup pengujian audit yang diperlukan untuk menjamin pencapaian tujuan audit;
 2. Tingkat kompleksitas, materialitas dan signifikansi dari hal-hal yang diuji dalam audit;
 3. Kelayakan dan efektifitas manajemen resiko, pengendalian intern, dan tata kelola TI;
 4. Kemungkinan terdapatnya kesalahan, ketidakwajaran dan ketidakpatuhan yang signifikan;
 5. Keseimbangan sumber daya yang dibutuhkan untuk melakukan audit dengan manfaat keyakinan yang memadai yang akan diperoleh.
3. Auditor Sistem Informasi harus memiliki kompetensi yang didasarkan kepada dengan pengetahuan dan ketrampilan yang dibutuhkan oleh Auditor Sistem Informasi dalam merencanakan, melaksanakan, mengawasi dan melaporkan seluruh penugasannya, serta disesuaikan kepada situasi dan kondisi Sistem Informasi yang akan diaudit.
4. Auditor Sistem Informasi harus meningkatkan pengetahuan dan keahlian yang diperlukan untuk melaksanakan Audit Sistem Informasi, dengan menjadi anggota dari asosiasi profesi Auditor Sistem Informasi dan melakukan pendidikan profesi berkelanjutan yang memadai sesuai ketentuan dari asosiasi profesi.

P-4 Perencanaan Audit Sistem Informasi

1. Auditor Sistem Informasi harus merencanakan Audit Sistem Informasi dengan baik dengan terlebih dahulu mengidentifikasi hal-hal berikut :
 1. Sumber daya sistem informasi yang akan di audit;
 2. Tata kelola dan manajemen sistem informasi yang akan di audit;
 3. Peraturan perundang-undangan yang terkait dengan sistem informasi yang akan diaudit.
2. Auditor Sistem Informasi harus menyusun Rencana Audit Sistem Informasi secara rinci dan jelas, yang mencakup :
 1. Tujuan, lingkup, dan jenis Audit Sistem Informasi;
 2. Tahapan dan prosedur pengujian Audit Sistem Informasi yang harus dilakukan;
 3. Metodologi dan alat bantu Audit Sistem Informasi yang dapat digunakan oleh Auditor Sistem Informasi;
 4. Jangka waktu pelaksanaan setiap tahapan dan prosedur pengujian dalam Audit Sistem Informasi;
 5. Alokasi kepada Auditor Sistem Informasi yang harus melakukan prosedur pengujian tersebut.
3. Auditor Sistem Informasi dalam merencanakan Audit Sistem Informasi harus memperhatikan beberapa faktor berikut ini :
 1. Aspek materialitas dan signifikansi dari risiko dan kendali yang akan diuji;

2. Hak dan kewajiban serta batasan Auditor Sistem Informasi sesuai peraturan perundang-undangan;
3. Ketersediaan sumber daya audit, seperti jumlah hari audit, alat bantu audit, dan kompetensi tim auditor yang terlibat;
4. Berbagai keterbatasan dari aspek teknis dari lingkungan TI yang ada.

P-5 Pelaksanaan Audit Sistem Informasi

1. Auditor Sistem Informasi harus mendokumentasikan seluruh informasi yang terkait dengan pelaksanaan prosedur audit dan berbagai bukti yang diperolehnya di dalam seperangkat Kertas Kerja Audit Sistem Informasi, yang harus memenuhi ketentuan sebagai berikut :
 1. Disusun menggunakan Bahasa Indonesia, dengan lengkap, jelas, terstruktur, dan memiliki indeks, agar mudah untuk dipahami dan digunakan oleh Audit Sistem Informasi atau pihak lain yang akan melakukan review atas Kertas Kerja Audit tersebut.
 2. Memungkinkan dilakukannya pelaksanaan ulang seluruh kegiatan yang telah dilaksanakan selama penugasan Audit Sistem Informasi tersebut oleh pihak independen dan memperoleh hasil dan kesimpulan yang sama.
 3. Mencantumkan identitas pihak yang melaksanakan setiap tahapan dan pengujian Audit Sistem Informasi serta peranannya, serta telah diperiksa oleh pihak lain di dalam Tim Audit Sistem Informasi.
2. Auditor Sistem Informasi harus mengelola dokumentasi atau Kertas Kerja Audit Sistem Informasi atas suatu penugasan, yang antara lain mencakup catatan atau data mengenai :
 1. Perencanaan dan persiapan tujuan dan lingkup penugasan tersebut dan hasil telaahan atas dokumentasi audit sebelumnya atau yang terkait dengan penugasan tersebut;
 2. Hasil atau risalah rapat telaahan pimpinan, rapat manajemen, dan rapat-rapat lain yang terkait dengan penugasan tersebut;
 3. Pemahaman Auditor Sistem Informasi tentang entitas atau kegiatan yang diaudit, dan lingkungan pengendalian intern serta sistem pemrosesan informasi yang terkait;
 4. Daftar program audit dan prosedur audit lainnya untuk memenuhi tujuan penugasan tersebut;
 5. Prosedur audit yang telah dilaksanakan dan bukti audit yang diperoleh dalam rangka mengevaluasi kelayakan dan kelemahan pengendalian Sistem Informasi yang terkait dengan penugasan tersebut;
 6. Metode yang digunakan untuk menilai kelayakan pengendalian, adanya kelemahan atau kekurangan pengendalian, dan mengidentifikasi pengendalian pengganti;
 7. Pembuat dan sumber dari dokumentasi audit beserta tanggal penyelesaiannya;
 8. Hak akses yang dimiliki dan/atau digunakan oleh Auditor Sistem Informasi dalam pelaksanaan berbagai pengujian atas sumber daya Sistem Informasi yang terkait.
 9. Hasil Pengujian Pengendalian, seperti pengujian atas kebijakan, prosedur dan pemisahan fungsi;
 10. Hasil Pengujian Terinci, seperti prosedur analitis, pengujian atas perhitungan, dan pengujian terinci lainnya;
 11. Berbagai hasil pemeriksaan atau telaahan hasil pelaksanaan supervisi audit;
 12. Berbagai temuan, kesimpulan dan rekomendasi audit yang terkait dengan penugasan tersebut;
 13. Tanggapan atau komentar pihak yang diaudit atas rekomendasi dari Auditor Sistem Informasi.
 14. Berbagai laporan yang diterbitkan sebagai hasil dari pelaksanaan penugasan tersebut;
 15. Tanda terima dari pihak yang berhak untuk menerima laporan dan temuan audit;

3. Audit Sistem Informasi harus disupervisi untuk memberikan jaminan yang memadai bahwa :
 1. Seluruh prosedur audit yang telah dialokasikan telah dilaksanakan dan didokumentasikan;
 2. Tidak terdapat prosedur audit yang terkait dengan risiko dan kendali sistem informasi yang material dan signifikan yang tidak dilaksanakan oleh Tim Audit Sistem Informasi;
 3. Telah dilaksanakan pemeriksaan yang memadai atas seluruh dokumentasi pelaksanaan prosedur audit, kertas kerja audit serta bukti-bukti audit yang diperoleh.

P-6 Pelaporan Audit Sistem Informasi

1. Auditor Sistem Informasi, harus menyampaikan Temuan dan Rekomendasi Audit Sistem Informasi jika ditemukan adanya kelemahan atau kekurangan atas rancangan dan/atau pelaksanaan pengendalian intern, manajemen risiko, dan kelola TI, dimana Temuan dan Rekomendasi Audit Sistem Informasi paling sedikit mencakup informasi sebagai berikut :
 1. Temuan, yaitu berbagai fakta mengenai kelemahan atau kekurangan rancangan dan pelaksanaan atas rancangan dan/atau pelaksanaan pengendalian intern TI, manajemen risiko TI, dan tata kelola TI yang ditemukan oleh Auditor Sistem Informasi yang didasarkan kepada bukti-bukti audit yang diperoleh dari hasil pelaksanaan prosedur pengujian Audit Sistem Informasi;
 2. Risiko, yaitu dampak yang disebabkan oleh adanya kondisi tersebut diatas, yang secara aktual telah terjadi atau memiliki potensi untuk terjadi, yang telah atau akan dapat mempengaruhi pencapaian sebagian atau keseluruhan tujuan dari pengendalian intern TI, manajemen risiko TI dan tata kelola TI;
 3. Kriteria, yaitu berbagai peraturan perundang-perundangan dan/atau kebijakan, prosedur, dan instruksi kerja, serta standar dan praktik-praktik terbaik, yang digunakan oleh Auditor Sistem Informasi untuk melakukan evaluasi dan pengujian atas pengendalian intern TI, manajemen risiko TI dan tata kelola TI;
 4. Rekomendasi, yaitu berbagai tindakan perbaikan yang menurut Auditor Sistem Informasi dapat atau harus dilakukan oleh-oleh pihak yang terkait, untuk menghilangkan dan/atau mengendalikan berbagai hal yang menjadi penyebab, serta menghilangkan dan/atau mengendalikan berbagai dampak, dari adanya berbagai kelemahan atau kekurangan atas rancangan dan/atau pelaksanaan pengendalian intern TI, dan manajemen risiko TI serta tata kelola TI yang terkait;
 5. Tanggapan, yaitu klarifikasi atau penjelasan dan argumentasi atau tanggapan resmi dari pihak-pihak yang terkait dan/atau bertanggung jawab atas hal-hal yang terkait dengan temuan dan rekomendasi yang disampaikan oleh Auditor Sistem Informasi.
2. Auditor Sistem Informasi menyampaikan suatu Laporan Hasil Audit Sistem Informasi, yang disusun dalam Bahasa Indonesia, kepada pihak-pihak yang terkait dengan suatu penugasan segera setelah pelaksanaan sebuah penugasan audit selesai dilaksanakan, dimana Laporan Hasil Audit Sistem Informasi tersebut minimal mencakup informasi sebagai berikut:
 1. Identitas organisasi, pihak-pihak yang berhak menerima, dan pembatasan distribusi atau sirkulasi laporan tersebut;
 2. Tujuan, aspek dan periode yang dicakup, serta sifat, waktu, dan kedalaman audit;
 3. Hasil Audit Sistem Informasi berupa temuan, kesimpulan, dan rekomendasi Audit Sistem Informasi, serta, jika ada, pengecualian dan pembatasan terkait dengan lingkup audit;
 4. Tanggapan dan/atau komentar resmi atas Laporan Hasil Audit Sistem Informasi dari pihak-pihak yang bertanggung jawab atas entitas atau kegiatan yang diaudit;
 5. Tanggal pelaporan, serta nama, jabatan dan tanda tangan Ketua Tim Audit Sistem Informasi;
 6. Ringkasan Eksekutif, yang merupakan ringkasan dari Laporan Hasil Audit Sistem Informasi, khususnya mengenai hal-hal yang menurut Auditor Sistem Informasi cukup material dan

signifikan dan perlu mendapatkan perhatian dari pihak-pihak yang bertanggung jawab atas entitas atau kegiatan yang diaudit.

P-7 Pemantauan Tindak Lanjut Audit Sistem Informasi

1. Auditor Sistem Informasi dalam memantau tindak lanjut Audit Sistem Informasi, harus:
 1. Mencatat jangka waktu yang harus dipenuhi oleh satuan kerja yang bertanggungjawab untuk menindaklanjuti temuan dan rekomendasi Audit Sistem Informasi;
 2. Jika dipandang perlu, dapat melakukan penugasan khusus atau tambahan dalam rangka melakukan evaluasi dan verifikasi atas tindak lanjut yang telah dilaporkan;
 3. Apabila terdapat tindak lanjut yang belum dilaksanakan atau yang dipandang kurang memadai pelaksanaannya, Auditor Sistem Informasi harus menyampaikan atau mengeskalasikan hasil pemantauan tindak lanjut Audit Sistem Informasi tersebut kepada satuan kerja yang terkait atau kepada pejabat yang lebih tinggi.
2. Auditor Sistem Informasi dalam melakukan evaluasi dan verifikasi kelayakan tindak lanjut atas temuan dan rekomendasi Audit Sistem Informasi, harus memperhatikan faktor sebagai berikut :
 1. Signifikansi dari temuan dan rekomendasi Audit Sistem Informasi tersebut;
 2. Adanya perubahan terhadap lingkungan Sistem Informasi yang dapat mempengaruhi signifikansi permasalahan atau risiko yang terkait dengan temuan dan rekomendasi tersebut;
 3. Sumber daya dan kompleksitas serta jangka waktu yang dibutuhkan untuk melaksanakan tindak lanjut dari temuan dan rekomendasi Audit Sistem Informasi tersebut;
 4. Dampak yang mungkin ditimbulkan jika tindak lanjut dari temuan dan rekomendasi tersebut tidak atau gagal dilakukan;

Pedoman ini disusun oleh IASII sebagai bagian dari Rancangan Peraturan Menteri Komunikasi dan Informatika tentang Pedoman Audit Sistem Elektronik yang saat ini masih dalam proses persetujuan pihak-pihak terkait.

Untuk Saran dan Masukan atas Pedoman ini dapat disampaikan melalui surel ke sekretariat@iasii.id
Informasi lebih lanjut tentang IASII dapat dilihat pada situs web kami di www.iasii.id