SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

PEDOMAN PENGAWASAN TEKNOLOGI INFORMASI

SPI

SATUAN PENGAWASAN INTERNAL
Universitas Islam Negeri Raden Fatah Palembang
Jl. Prof. K.H. Zainal Abidin Fikry KM.3,5 Palembang 30126
Telp. 0711-354668 Web : spi.radenfatah.ac.id
Email : spi_uin@radenfatah.ac.id Instagram : spiuinradenfatah

KATA PENGANTAR

Puji syukur kami panjatkan kepada Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga Satuan Pengawasan Internal (SPI) UIN Raden Fatah Palembang dapat menyusun Pedoman Pengawasan Teknologi Informasi dengan baik.

Kami bersyukur sepenuhnya atas tersusunnya Pedoman Pengawasan Teknologi Informasi ini. Pedoman ini merupakan salah satu wujud akuntabilitas dalam merespon lahirnya PMA Nomor 25 Tahun 2017 tentang Satuan Pengawasan Internal (SPI) pada Perguruan Tinggi Keagamaan Negeri dan Keputusan Menteri Agama RI Nomor 788 Tahun 2021 Tentang Pelaksanaan Sistem Pemerintahan Berbasis Elektronik Pada Kementerian Agama. Pedoman ini disusun sebagai wujud optimalisasi kelembagaan SPI dan fungsi SPI UIN Raden Fatah Palembang.

Dengan demikian, pedoman ini diharapkan mampu meningkatkan kinerja SPI dalam melaksanakan fungsi pengawasan dan evaluasi pengelolaan dan tata kelola layanan berbasis teknlogi infromasi di unit masing-masing UIN Raden Fatah Palembang. Sehingga terwujud tata kelola Lembaga yang profesional, transaparan dan akuntabel menuju terciptanya *Good University Governance* (GUG).

Kami ucapkan terima kasih kepada tim penyusun pedoman reviu/pemeriksaan dan semua pihak yang telah banyak memberikan masukan kepada SPI. Semoga pedoman ini memberikan manfaat bagi pihak-pihak yang berkepentingan khususnya SPI UIN Raden Fatah Palembang.

Palembang, 14 November 2022

Rektor,

Nyayu Khodijah

DAFTAR ISI

2022

SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

BAB I
PENDAHULUAN

BAB I
PENDAHULUAN

A. Pendahuluan

Pemanfaatan Teknologi Informasi di harapkan dapat menunjang pelaksanaan operasional organisasi dan pencapaian tujuan strategis organisasi. Pemanfaatan Teknologi Informasi memiliki beberapa Resiko yang sering terjadi, hilangnya atau rusaknya data, tidak lengkap atau ketidakakuratan data, inefisiensi penggunaan sumber daya Teknologi Informasi, tidak patuh terhadap peraturan perundang-undangan kepada tidak tercapainya tujuan organisasi.

Sehubungan dengan tujuan dan risiko pemanfaatan Teknologi Informasi tersebut, maka pemanfaatan Teknologi Informasi perlu dikendalikan dengan baik dan memadai, dimana pengendalian Teknologi Informasi umumnya dilakukan dan aspek tata kelola Teknologi Informasi. Pengendalian Teknologi Informasi dilakukan dalam suatu rangkaian aktivitas pengendalian yang mencakup kebijakan, struktur organisasi dan aktivitas pengendalian.

Untuk dapat memperoleh keyakinan yang memadai tantangan pengusaha dalam implementasi dari pengambilan Teknologi Informasi disebut sekolah independen oleh auditor Teknologi Informasi.

Auditor Teknologi Informasi yang dimaksud disini mencakup definisi yang luas auditor Teknologi Informasi di mana dalam interaksi sosial sistem informasi dan auditor infrastruktur Teknologi Informasi. Audit Teknologi atau Sistem Informasi merupakan suatu cara untuk menilai sejauhmana suatu teknologi atau sistem informasi telah mencapai tujuan organisasi.

UIN Raden Fatah Palembang bertekad untuk untuk lebih mengintensifkan penggunaan Teknologi Informasi kedalam setiap aspek yang memungkinkan keberadaannya, tidak hanya untuk peningkatan kualitas di bidang akademik, tapi juga di bidang administratif dan hal-hal lainnya. UIN Raden Fatah juga dituntut untuk menerapkan *Good University Governance (GUG)*, maka peran dan fungsi Teknologi Informasi dalam aktivitas perguruan tinggi harus di implementasikan baik dalam menerapkan tri dharma perguruan tinggi maupun dalam aktifitas non akademik atau administrasi maka tata kelola Teknologi Informasi menjadi bagian yang tak terpisahkan dari pengelolaan perguruan tinggi.

Audit Teknologi Informasi adalah bentuk pengawasan dan pengendalian dari infrastrutur teknologi dan sistem informasi secara menyeluruh. Audit Teknologi Informasi merupakan proses pengumpulan dan evaluasi bukti-bukti apakah sistem komputerisasi yang digunakan telah dapat melindungi aset milik UIN Raden Fatah Palembang, mampu menjaga integritas data, dan dapat membantu pencapaian tujuan organisasi secara efektif serta menggunakan sumber daya yang dimiliki secara efisien.

Dengan melaksanakan audit Teknologi Informasi suatu lembaga bisa dikatakan sudah memiliki kepedulian yang tinggi terhadap posisi Teknologi Informasi bagi perkembangan lembaganya. Audit Teknologi Informasi atau sistem informasi yang di rencanakan dengan baik akan memberikan beberapa hasil yang manfaatnya akan sangat signifikan bagi perjalanan dan pengembangan UIN Raden Fatah di kemudian hari.

Hasil-hasil tersebut antara lain; munculnya evaluasi terhadap praktik-praktik manajemen risiko terhadap kendali sistem internal dan terhadap kebijakan-kebijakan yang terkait dengan Teknologi

Informasi yang terjadi di UIN Raden Fatah Palembang, yang kompleksitas nya rendah atau yang tinggi.

Audit teknologi informasi ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset Teknologi informasi suatu institusi telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya. Beberapa alasan penting mengapa audit Teknologi Informasi perlu dilakukan, antara lain:

1. Kerugian Akibat Kehilangan Data

   Data telah menjadi salah satu aset terpenting bagi suatu institusi. Sehingga kehilangan data akan menjadi masalah yang sangat serius terhadap kelangsungan proses pada institusi tersebut. Jika terjadi kehilangan data, maka diperlukan waktu yang cukup lama untuk melakukan verifikasi manual atas dokumen yang dimiliki.

2. Kesalahan Dalam Pengambilan Keputusan

   Banyak institusi yang saat ini telah menggunakan bantuan Decision Support System (DSS) untuk mengambil keputusan-keputusan penting. Sehingga bagaimana validitas keputusan yang diambil jika data-data yang digunakan sebagai acuan tidak valid atau tidak tersedia. Dapat dipastikan akan terjadi kesalahan dalam pengambilan keputusan.

3. Risiko Kebocoran Data

   Data bagi suatu institusi merupakan sumber daya yang tidak ternilai harganya. Kebocoran data tidak saja berdampak teraksesnya data oleh orang/pihak yang tidak memiliki wewenang, akan tetapi lebih jauh lagi kebocoran data dapat mengganggu kelangsungan proses pada suatu institusi.

4. Penyalahgunaan Komputer

   Alasan lain perlunya dilakukan audit Teknologi Informasi adalah tingginya tingkat penyalahgunaan komputer. Pihak-pihak yang dapat melakukan kejahatan komputer sangat beraneka ragam. Kita mengenal adanya hackers dan crackers. Hackers merupakan orang yang dengan sengaja memasuki suatu sistem teknologi informasi secara tidak sah. Biasanya mereka melakukan aktivitas hacking untuk kebanggaan diri sendiri atau kelompoknnya, tanpa bermaksud merusak atau mengambil keuntungan atas tindakannya itu. Sedang, Crackers di sisi lain melakukan aktivitasnya dengan tujuan mengambil keuntungan sebanyak-banyaknya dari tindakannya tersebut, misalnya mengubah atau merusak atau, bahkan, menghancurkan sistem komputer. Tidak semua institusi siap mengantisipasi adanya risiko-risiko akibat adanya hackers dan crackers.

5. Kerugian Akibat Kesalahan Proses Perhitungan

   Seringkali, Teknologi Informasi digunakan untuk melakukan perhitungan yang rumit. Salah satu alasan digunakannya Teknologi Informasi adalah kemampuannya untuk mengolah data secara cepat dan akurat. Penggunaan Teknologi Informasi untuk mendukung proses penghitungan bukannya tanpa risiko kesalahan. Risiko ini akan semakin besar jika tanpa adanya mekanisme pengembangan sistem yang memadai. Kesalahan yang ditimbulkan oleh sistem baru ini akan sulit terdeteksi tanpa adanya audit terhadap sistem tersebut.

6. Tingginya Nilai Investasi Perangkat Keras dan Perangkat Lunak Komputer Investasi yang dikeluarkan untuk suatu proyek Teknologi Informasi seringkali sangat besar. Namun sulit mengukur manfaat yang dapat diberikan Teknologi Informasi.

Hasil audit Teknologi Informasi adalah temuan-temuan yang terbagi ke dalam dua kategori, yakni temuan negatif dan temuan positif. Di dalam temuan negatif, auditor mengungkapkan hal-hal yang menurutnya 'tidak seharusnya terjadi ' atau 'tidak seharusnya dikerjakan oleh user atau pengguna Teknologi Informasi di lingkungan UIN Raden Fatah Palembang terkait dengan keberadaan atau pemanfaatan Teknologi Informasi. Sementara dalam temuan positif, auditor menguraikan manfaat-manfaat atau keunggulan yang telah dicapai oleh UIN Raden Fatah Palembang dengan memanfaatkan fasilitas Teknologi Informasi yang sudah ada. Sebagai tindak lanjut dari temuan-temuan, maka auditor memberikan saran dan masukan. Saran ini nantinya dapat digunakan sebagai petunjuk bagi para pembuat kebijakan dalam hal penyusunan kebijakan Teknologi Informasi untuk masa kerja selanjutnya.

B. Tujuan

Adapun Tujuan Audit Teknologi Informasi di lingkungan UIN Raden Fatah Palembang ini adalah;

1. Untuk memberikan batasan dan panduan kepada Satuan Pengawasan Internal (SPI) dalam memeriksa tata kelola Teknologi Informasi di lingkungan UIN Raden Fatah Palembang dan untuk memberi keyakinan bahwa penggunaan Teknologi Informasi memiliki hubungan yang sangat erat bagi pencapaian tujuan organisasi.
2. Melakukan verifikasi terhadap efektifitas dari penerapan Teknologi Informasi.

3. Melakukan verifikasi apakah penerapan teknologi informasi sudah memenuhi aspek efisiensi, availability system, reliability, confidentiality, dan integrity, serta aspek keamanan.
4. Melaporkan hasil audit dengan data yang memadai dan memberikan masukan kepada bagian terkait agar dapat dilakukan perbaikan.

C. Pengertian

1. Audit Teknologi Informasi atau Audit Sistem Informasi dan Audit infrastruktur Teknologi Informasi adalah proses sistematis mengumpulkan dan mengevaluasi bukti untuk menentukan secara independen dan obyektif apakah suatu sistem informasi telah dapat melindungi aset, menjaga integritas data, dan memungkinkan tujuan organisasi tercapai secara efektif, dengan menggunakan sumber daya secara efisien, dan mematuhi peraturan yang berlaku.
2. Informasi meliputi keterangan, pernyataan, gagasan dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan Teknologi Informasi dan komunikasi secara elektronik ataupun non elektronik.
3. Aplikasi Teknologi Informasi merupakan komponen perangkat lunak sistem elektronik yang digunakan untuk menjalankan fungsi, proses dan mekanisme kerja yang mendukung penyelenggaraan sistem informasi yang diaudit.
4. Infrastruktur Teknologi Informasi meliputi Infrastruktur Teknologi Informasi utama dan pendukung yang terkait dengan penyelenggaraan sistem informasi yang diaudit.

5. Personil meliputi seluruh sumber daya manusia pada unit-unit kerja yang terkait dengan penyelenggaraan sistem informasi atau infrastruktur Teknologi Informasiyang diaudit.
6. Perencanaan Sistem Informasi meliputi seluruh ketentuan internal, standar, dan prosedur serta proses perencanaan strategis dan perencanaan serta pengorganisasian atas kegiatan dan anggaran yang terkait dengan sistem informasi yang diaudit.
7. Pengorganisasian Sistem Informasi meliputi seluruh ketentuan internal, standar, dan prosedur serta proses yang terkait dengan kelembagaan penyelenggaraan sistem informasi yang diaudit.
8. Pengembangan Sistem Informasi meliputi seluruh ketentuan internal, standar, dan prosedur serta proses yang terkait dengan perancangan, pengkodean, pengujian, instalasi, migrasi dan pelatihan sistem (sosialisai) atas sistem informasi yang diaudit.
9. Pengoperasian Sistem Informasi meliputi seluruh ketentuan internal, standar, dan prosedur serta proses yang terkait dengan pengoperasian sistem informasi yang diaudit.
10. Pemantauan meliputi seluruh ketentuan internal, standar, dan prosedur serta proses yang terkait dengan monitoring dan evaluasi penyelenggaraan sistem informasi yang diaudit.
11. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan Teknologi Informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE

D. Dasar Hukum

1. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Jo. Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008.

2. Undang-undang Nomor 14 Tahun 2008 Tentang Keterbukaan Informasi Publik.
3. Peraturan Pemerintah Nomor 60 Tahun 2008 Tentang Sistem Pengendalian Intern Pemerintah.
4. Peraturan Menteri Agama RI Nomor 55 Tahun 2022 Tentang Organisasi dan Tata Kerja UIN Raden Fatah Palembang
5. Peraturan Menteri Agama RI Nomor 25 Tahun 2017 Tentang Satuan Pengawas Internal Pada Perguruan Tinggi Keagamaan Negeri (PTKIN).
6. Peraturan Menteri Keuangan RI Nomor 200/PMK.05/2017 Tentang Sistem Pengendalian Internal Pada Badan Layanan Umum
7. Keputusan Menteri Agama RI Nomor 788 Tahun 2021 Tentang Pelaksanaan Sistem Pemerintahan Berbasis Elektronik Pada Kementerian Agama,

E. Ruang Lingkup

Pedoman pengawasan ini meliputi:

1. Perencanaan Strategis atau master plan Teknologi Informasi
2. Manajemen Risiko Teknologi Informasi
3. Manajemen Aset Teknologi Informasi
4. Security atau Keamanan Teknologi Informasi
5. Update atau Perubahan Teknologi Informasi

F. Pihak Atau Fungsi Terkait Pengawasan

1. Kepala Satuan Pengawasan Internal
2. Sekretaris Satuan Pengawasan Internal
3. Auditor pada Satuan Pengawasan Internal
4. Anggota Satuan Pengawasan Internal

2022

SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

BAB II

GAMBARAN UMUM PELAKSANAAN PEMERIKSAAN TEKNOLOGI INFORMASI

BAB II

GAMBARAN UMUM PELAKSANAAN PEMERIKSAAN TEKNOLOGI INFORMASI

A. Objek Pemeriksaan Teknologi Informasi

Berdasarkan Keputusan Menteri Agama RI Nomor 788 Tahun 2021 Tentang Pelaksanaan Sistem Pemerintahan Berbasis Elektronik Pada Kementerian Agama, Peraturan Menteri Keuangan RI Nomor 200/PMK.05/2017 Tentang Sistem Pengendalian Internal Pada Badan Layanan Umum dan merujuk pada Peraturan Menteri Komunikasi dan Informasi Nomor 41/Permen.Kominfo/11/2007 Tentang Panduan Tata Kelola Informasi dan Komunikasi Nasional, maka yang menjadi objek atau entitas pemeriksaan atau audit Teknologi Informasi adalah :

1. Unit pelayanan di semua fakultas, lembaga, unit dan bagian yang menggunakan Teknologi Informasi atau pelaksana teknis yang memiliki tugas pokok dan fungsi utama melaksanakan kegiatan atau pekerjaan atau layanan yang berbasis Teknologi Informasi.
2. Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPD) yang dalam pelaksanaan tugas pokok dan fungsi nya adalah membuat atau mengembangkan layanan berbasis TI baik bidang akademik maupun non akademik, memelihara, melayani, fungsi kontrol atau evaluasi serta mengamankan aset dan pengunaan Teknologi Informasi.

B. Metode Penilaian Hasil Pemeriksaan Teknologi Informasi

Hasil pemeriksaan dituangkan dalam bentuk penilaian. Setiap point pertanyaan yang disebutkan dalam daftar checklist

pemeriksaan diberi skor 0 sampai dengan 5. Terhadap skoring ini dilakukan laporan hasil pemeriksaan sebagai berikut:

1. Temuan

   Temuan hasil pemeriksaan disampaikan atas item-item pertanyaan dalam daftar checklist yang nilainya di bawah lima dan diberikan rekomendasi untuk mencapai nilai diatasnya atau nilai tertinggi (5).

Tabel 1. Contoh Temuan Hasil Pemeriksaan

No	Pemeriksaaan	Temuan	Saran dan tindak lanjut
1	Perencanaan Strategis atau Master Plan TI	- Perencanaan strategis masih dalam tahap perencanaan - Perencanaan strategis dan penyusunan master plan IT tidak menggunakan tools atau alat bantu analisa yang memadai	- Segera selesaikan penyusunan renstra atau master plan IT dan implementasikan rencana strategis dan planning yang sudah disusun - Perbaiki dan kaji ulang renstra dan master plan IT dengan menggunakan alat bantu yang cocok dan memadai

2. Penilaian Pemeriksaan

   Penilaian pemeriksaan (NP) adalah penghitungan jumlah skor hasil pemeriksaan (SP) di bagi skor maksimal (SM) yang harus dicapai dikalikan 100%.

   Dengan rumus penilaian :

   NP= SP/SM x 100% Contoh: Nilai Perencanaan Strategis :

   Skor Pemeriksaan = 30

   Skor Maksimal = 65

   Nilai Pemeriksaan (NP) = (30/65) x 100%

   Dari hasil nilai yang di peroleh kemudian diberikan rekomendasi sebagai berikut :

Tabel 2. Contoh Penilaian Pemeriksaan

No	Nilai Pemeriksaan (%)	Rekomendasi
1	0 - 50	Perbaikan/Revisi total Tata Kelola TI yang dinilai (dalam contoh di atas adalah revisi Perencanaan strategis dan Master Plan TI)
2	51 - 99	Perbaikan/Revisi sesuai dengan hasil temuan
3	100	Pertahankan

3. Evaluasi dan Penarikan kesimpulan Umum Tata Kelola TI

   Evaluasi Umum adalah penilaian yang diberikan atas pelaksanaan tata kelola teknologi informasi. Penilaian ini diperoleh dengan menjumlahkan nilai pemeriksaan (∑NP) di bagi total nilai yang harus diperoleh ((∑TN) dikali 100%.

Rumus evaluasi umum adalah:

$$\text{Evaluasi Umum} = \frac{\sum NP}{\sum TN} \times 100\%$$

Dari hasil evaluasi umum, selanjutnya di berikan rekomendasi sesuai dengan tingkat capaian penilaian, sebagai berikut:

Tabel 3. Contoh Hasil Penilaian Pemeriksaan

No	Penilaian Umum Tata Kelola TI (%)	Kesimpulan	Saran Rekomendasi
1	0 - 50	Tata Kelola belum dilaksanakan dengan baik	Segera menerapkan tata kelola Teknologi Informasisesuai dengan peraturan perundangan yang berlaku
2	51 – 79%	Tata Kelola telahdilaksanakan namun belum maksimal	Segera dilaksanakakan perbaikan pada bidang tata kelola sesuai hasil temuan pemeriksaan
3	80 – 100%	Tata Kelola teknologi Informasi telah dilaksanakan dengan baik	Sempurnakan pelaksanaan tata kelola TI sebagaimana hasil temuan dan pertahankan.

2022

SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

BAB III

PELAKSANAAN PEMERIKSAAN

BAB III PELAKSANAAN

PEMERIKSAAN

A. Pemeriksaan Perencanaan Strategis Teknologi Informasi

Pemeriksaan terhadap perencanaan strategis TI adalah proses yang dilakukan terhadap arah pengembangan dan penerapan TI.

✓ Prosedur Pemeriksaan

a. Dapatkan dokumen perencanaan strategis Teknologi Informasi
b. Dapatkan dokumen struktur organisasi UIN Raden Fatah Palembang
c. Dapatkan dokumen UIN Raden Fatah Palembang
d. Dapatkan dokumen, data atau informasi tentang pengembangan Teknologi Informasiyang telah dilaksanakan, dan komparasikan dengan dokumen Renstra TI, buat evaluasi atas pengembangan yang telah dilaksanakan.
e. Periksa ruang lingkup pengembangan TI pada dokumen Perencanaan Strategis TI dan komparasikan dengan Struktur Organisasi UIN Raden Fatah Palembang, buat catatan kesesuaian atau ketidaksesuaian.
f. Periksa inisiatif (rencana) kegiatan yang terdapat pada dokumen RKAKL dan komparasikan dengan Dokumen Renstra TI, buat catatan kesesuaian/ketidaksesuaian.
g. Tuangkan dalam hasil pemeriksaan, buat simpulan dan rekomendasi.

B. Pemeriksaan Manajemen Risiko Teknologi Informasi

Pemeriksaan terhadap manajemen resiko adalah pemeriksaan pengelolaan resiko yang timbul dalam operasionalisasi layanan TI. Sasaran pemeriksaan ini adalah pengelolaan dan resiko bawaan yang ditimbulkan oleh kelemahan-kelemahan perangkat keras dan perangkat lunak.

✓ Prosedur Pemeriksaan

a. Dapatkan dokumen penilaian resiko layanan Teknologi Informasi
b. Dapatkan dokumen tentang catatan resiko-resiko layanan Teknologi Informasi
c. Dapatkan dokumen standar operasional prosedur penanganan resiko
d. Periksa metode penilaian resiko dalam dokumen penilaian resiko
e. Periksa kelengkapan ruang lingkup manajemen resiko.
f. Tuangkan dalam laporan hasil pemeriksaan buat simpulan dan rekomendasi.

C. Pemeriksaan Manajemen Aset Teknologi Informasi

Pemeriksaan manajemen aset TI dilakukan terhadap tata kelola aset-aset yang berkaitan dengan pengelolaan aset Informasi, SDM, Fisik, Perangkat Lunak, Layanan dan Aset tak berwujud (*intangible*) menyangkut reputasi/kepercayaan terhadap layanan.

✓ Prosedur pemeriksaan.

a. Dapatkan dokumen Standar Operasional Prosedur Pengelolaan Aset.
b. Dapatkan dokumen catatan Aset yang meliputi: Aset Informasi, Aset Fisik, Aset Perangkat Lunak (*software*), Aset Layanan dan Aset tak berwujud (*intangible asset*).
c. Dapatkan dokumen pemantauan aset.
d. Dapatkan rencana perubahan/pembaharuan aset.
e. Dapatkan catatan perkembangan pembaharuan aset.
f. Periksa kelengkapan Standar Operasional Prosedur Pengelolaan Aset, yang meliputi keenam aset di atas.
g. Periksa kelengkapan catatan aset dalam dokumen pencatatan aset.
h. Periksa catatan pementauan kinerja aset.
i. Periksa perkembangan perubahan/pembaharuan aset.
j. Tuangkan dalam hasil pemeriksaan, buat simpulan dan buat

D. Pemeriksaan Keamanan Teknologi Informasi a.

Pemeriksaan Keamanan Perangkat TI

Pemeriksaan ini adalah pemeriksaan terhadap pengelolaan keamanan perangkat dari berbagai ancaman yang dapat mengakibatkan kerugian atau tidak optimalnya layanan TI.

✓ Prosedur Pemeriksaan

1. Dapatkan dokumen kebijakan layanan TI.

2. Dapatkan dokumen *Standard Operating Procedure* (SOP) pengamanan perangkat.
3. Dapatkan dokumen catatan akses ke fasilitas Teknologi Informasi.
4. Periksa setiap langkah dalam SOP pengamanan perangkat.
5. Periksa catatan akses ke fasilitas dan akses fisik perangkat yang dimiliki TI.
6. Periksa penempatan perangkat pengelola informasi yang sangat penting dan sensitif.
7. Periksa dokumen prosedur penghapusan dan penggunaan kembali perangkat yang sangat penting dan sensitif.
8. Periksa dokumen prosedur penggunaan media penyimpanan data dan informasi yang bersifat portabel. (misal Hardisk eksternal, CD, Flashdisk, dll)
9. Tuangkan hasil pemeriksaan, buat kesimpulan dan rekomendasi hasil pemeriksaan.

b. Pemeriksaan Keamanan Operasional TI

Pemeriksaan terhadap keamanan operasional TI dilakukan terhadap operasionalisasi data dan informasi yang terdapat dalam berbagai aplikasi sistem informasi manajemen.

✓ Prosedur Pemeriksaan

1. Dapatkan dokumen *Standard Operating Procedure* (SOP) layanan operasional sistem informasi manajemen (aplikasi).
2. Dapatkan dokumen perjanjian tingkat layanan (*Service Level Agreement / SLA)* yang telah di tandatangani oleh

setiap kepala satuan pemilik layanan aplikasi sistem informasi manajemen.

3. Dapatkan dokumen klasifikasi pengguna dan hak akses terhadap setiap sistem informasi manajemen yang ada.
4. Dapatkan dokumen klasifikasi tingkat keamanan setiap informasi pada setiap sistem informasi manajemen
5. Dapatkan dokumen manajemen risiko keamanan atas setiap aplikasi sistemn informasi manajemen
6. Pesriksa isi perjanjuan layanan (SLA) setiap layanan aplikasi sistem informasi manajemen
7. Periksa isi perjanjanjian tingkat layanan (SLA) setiap layanan aplikasi informasi manajemen
8. Periksa klasifikasi tingkat keamanan setiap pengguna (misal Admin: Kerahasiaan=3, Integritas=3, dan Ketersediaan=3, user level 1: Kerahasiaan=2, integritas=3, ketersediaan=3, user biasa: Kerahasiaan=1, integritas=1 dan ketersediaan=3, dst)
9. Periksa manajemen resiko atas tingkat keamanan pengguna.
10. Periksa dokumen pemantauan penggunaan setiap aplikasi sistem informasi manajemen (user log).

c. Pemeriksaan Keamanan Server dan Jaringan Pemeriksaan terhadap keamanan server dan jaringan merupakan kegiatan untuk memeriksa keamanan akses fisik dan non fisik ke server dan perangkat jaringan.

✓ Prosedur Pemeriksaan

1. Dapatkan dokumen kebijakan pengaman atau prosedur standar (SOP) pengamanan ruang server dan jaringan.

2. Dapatkan dokumen catatan sirkulasi orang yang memasuki ruang server
3. Dapatkan dokumen tentang perangkat lunak yang melindungi akses ke server dan jaringan.
4. Dapatkan dokumen catatan tentang aplikasi Sistem Informasi Manajemen yang dilayani.
5. Dapatkan dokumen akses ke server dari unit kerja pemilik aplikasi dan layanan internet.
6. Dapatkan prosedur backup data, informasi dan aplikasi sistem informasi manajemen.
7. Dapatkan dokumen pencatatan media backup dan sistematika backup.
8. Periksa prosedur pengamanan ruang server, pastikan bahwa prosedur tersebut memuat langkah-langkah pencatatan terhadap setiap personil yang memasuki ruang server.
9. Periksa catatan tentang akses masuk dan keluar ruang server, pastikan bahwa setiap personil yang memasuki ruang server telah dicatat, nama, asal, tanggal masuk, jam masuk hari masuk, tujuan (kepentingan), jam keluar dan perangkat yang di bawa saat masuk dan keluar.
10. Periksa sistem keamanan fisik server dan jaringan, pastikan ruang server telah dilengkapi dengan perangkat pengamanan yang maksimal (kunci/gembok) secara manual atau elektrik. Pastikan pula server dan jaringan telah diamankan dari bahaya bencana alam, seperti petir, kebakaran, banjir dan sejenisnya.

11. Periksa sistem keamanan jaringan, pastikan terdapat perangkat lunak firewall berikut versinya yang telah di update
12. Periksa catatan update perangkat lunak keamanan jaringan (firewall, antivirus).
13. Periksa dokumen catatan kendala dan permasalahan yang dihadapai pada jaringan lokal, pastikan bahwa setiap perangkat jaringan lokal (Modem, Switchub, akses point, kabel) selalu dipantau kinerjanya secara berkala.
14. Periksa dokumen catatan kendala dan permasalahan perangkat jaringan lokal, pastikan bahwa setiap kendala dan permasalahan tercatat.
15. Periksa solusi yang telah dilakukan terhadap permasalahan dan kendala pada jaringan lokal, pastikan bahwa solusi yang diberikan adalah yang terbaik, sementara, jangka waktu tertentu atau tidak memberi solusi berarti.
16. Periksa sistem pelaporan atas kendala dan permasalahan jaringan (lokal dan internet), pastikan bahwa pimpinan unit pelaksana teknis layanan TI selalu mengetahui dan memberikan rekomendasi yang tepat.
17. Periksa dokumen pencatatan akses log ke server, pastikan bahwa setiap orang yang mengakses ke server baik secara langsung maupun secara jarak jauh (remote) tercatat dengan baik: Nama, Jabatan, tanggal akses, jam login akses, jam logout akses, tujuan (kepentingan) akses.

18. Periksa konfigurasi sistem backup data server, pastikan bahwa setiap konfigurasi server dan basis data telah di backup.
19. Periksa bahwa data dan aplikasi (SIM) telah dibackup secara realtime (sistem backup data dilakukan sebagai redundansi dari apilkasi yang sedang berjalan)
20. Periksa prosedur backup data, pastikan bahwa data telah di backup secara periodik.
21. Periksa sistem pengamanan backup data, pastikan bahwa perangkat backup data tersimpan dengan aman dan baik
22. Periksa dokumen pakta integritas dan perjanjian kerahasiaan, atas personil yang memilki hak askes terhadap data dan informasi sensitif serta akses server.
23. Periksa sistem pengamanan akses aplikasi (SIM), pastikan setiap user menggunakan tingkat pengamanan maksimum (minimal 8 digit untuk password).
24. Periksa prosedur penghentian akses, pastikan bahwa terdapat mekanisme penghentian akses atas pergantian tugas personil, personil yang telah terbukti melakukan kesalahan fatal dengan sengaja, dan personil yang tidak dapat bertugas lagi.
25. Tuangkan dalam hasil pemeriksaan, buat simpulan hasil pemeriksaan dan rekomendasi

d. Pemeriksaan Perubahan Layanan TI

Pemeriksaan terhadap pengelolaan perubahan adalah pemeriksaan yang dilakukan terhadap tata kelola perubahan layanan TI. Perubahan-perubahan dapat berasal dari penyesuaian-penyesuaian yang harus dilakukan berkaitan dengan kualitas layanan, dapat pula berasal atas permintaan pengguna layanan TI dari unit kerja pemilik aplikasi. Pemeriksaan ini dilaksanakan setiap saat diperlukan atau atas permintaan.

✓ Prosedur Pemeriksaan

1. Dapatkan dokumen *Standard Operating Procedure* (SOP) perubahan layanan.
2. Dapatkan dokumen catatan perubahan yang telah dilaksanakan
3. Dapatkan dokumen permintaan perubahan yang berasal dari pengguna layanan
4. Dapatkan dokumen catatan keluhan/laporan berupa gangguan dan permasalahan layanan TI.
5. Periksa langkah-langkah dalam SOP perubahan.
6. Periksa catatan-catatan perubahan yang telah dilaksanakan
7. Periksa dokumen permintaan perubahan yang berasal dan bandingkan dengan catatan perubahan yang telah dilaksanakan.
8. Bandingkan catatan perubahan dan dokumen catatan keluhan pengguna dan permasalahan.

S

2022

SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

BAB IV

PELAPORAN HASIL PEMERIKSAAN

BAB IV
PELAPORAN HASIL PEMERIKSAAAN

Hasil Pemeriksaan dilaporkan kepada Rektor dan ditembuskan kepada unit kerja terkait agar ditindaklanjuti. Laporan tersebut disusun dengan sistematika sebagai berikut:

A. Pendahuluan

Bab ini memberikan gambaran tentang latar belakang, metode dan alasan lain sehingga pemeriksaan tata kelola Teknologi Informasi perlu dilaksanakan.

B. Hasil Pemeriksaan

Bab ini memaparkan hasil-hasil pemeriksaan yang diurutkan berdasarkan simpulan Umum Hasil Pemeriksaan, Penilaian Pemeriksaan dan Temuan pemeriksaan serta rekomendasi-rekomendasi hasil pemeriksaan.

C. Temuan dan Kesimpulan.

Bab ini memaparkan hasil temuan, kesimpulan dan rekomendasi hasil pemeriksaan TI

S

2022

SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

PENUTUP

BAB V

PENUTUP

Pedoman Pemeriksaan atau Audit Tata Kelola teknologi Informasi ini disusun daam rangka meletakkan dasar panduan di dalam merencanakan, melaksanakan dan melaporkan hasil pemeriksaan atau audit Tata Kelola Teknologi Informasi yang bertujuan untuk meningkatkan kualitas Tata Kelola TI dan menjamin kepatuhan terhadap ketentuan Tata Kelola TI sebagai sebuah *quality assurance* Tata Kelola TI di lingkungan Universitas Islam Negeri Raden Fatah Palembang.

S

2022

SATUAN PENGAWASAN INTERNAL
UIN Raden Fatah Palembang

LAMPIRAN

LAMPIRAN

Lampiran 1 : Checklist Pemeriksaan Renstra TI

No	Pemeriksaan	Kondisi				Dokumen Pendukung
		Tidak di terapkan	Dalam Perencanaan	Diterapkan Sebagian	Diterapkan Menyeluruh	
1	Terdapat dokumen perencaan strategis Teknologi Informasi yang masih berlaku					Dokumen Renstra TI
2	Dalam dokumen Renstra TI telah menggunakan alat bantu (tools) analisis SWOT, Value Chain (Rantai Nilai), Diagram Mc farlan (Mc Farlan Grid), Frame Work yang digunakan dan alat bantu lain yang di perlukan					sda
3	Di dalam Renstra TI telah memperhatikan stake holders					sda

	sebagai pengguna layanan TI di lingkungan UIN Raden Fatah Palembang					
4	Di dalam Renstra TI termuat capaian pengembangan TI sebelum sesudah (*acurrent analisys system/ as is*)					sda
5	Terdapat arsitektur bisnis organisasi UIN Raden Fatah dalam Renstra TI					sda
6	Terdapat arsitektur informasi dalam Renstra TI					sda
7	Terdapat arsitektur aplikasi dan data (sistem informasi)					sda
8	Terdapat arsitektur TI saat ini (*current*					sda

	condition/ as is) dan yang akan datang (*to be*)					
9	Arsitektur Informasi yang akan di kembangkan sesuai dengan mengacu pada organisasi bisnis (arsitektur bisnis) UIN Raden Fatah Palembang					sda
10	Rencana Pengembangan TI Perangkat Keras berdasarkan pada (untuk memenuhi) rencana pengembangan sistem informasi					sda
11	Renstra telah mengadopsi tren teknologi yang berkembang saat ini : - Trend Cloud Computing					sda

	- Tren Security System - Tren Media Sosial - Tren Teknologi Web (AI, Mobile, Broadnet) yang dapat diakses disemua perangkat atau gadget					
12	Terdapat tahapan-tahapan dalam rencana pengembangan aplikasi (*software*) dan teknologi perngkat keras (*hardware*) berbentuk *road map*					sda
13	Terdapat pemilihan prioritas pengembangan sistem informasi (aplikasi) dalam *road map* TI					sda

Lampiran 2. Checklist Pemeriksaan Manajemen Resiko

No	Pemeriksaan	Kondisi (Poin)				Dokumen Pendukung
		Tidak Ada (0)	Ada Belum di terapkkan (1)	Diterapkan Sebagian (3)	Diterapkan Menyeluruh (5)	
1	Ada prosedur pengelolaan risiko					SOP Pengelolaan Resiko
2	Risiko dikelola dengan metode penilaian yang konsisten					Dokumen *Risk Management*
3	Faktor dampak dari risiko diperhitungkan dalam metode penilaian risiko					sda
4	Faktor pengancam dari risiko terlibat dalam metode penilaian resiko					sda
5	Faktor kerentanan dari aset terlibat dalam metode penilaian risiko					sda
6	Faktor pengendalian yang sudah diterapkan terlibat dalam metode penilaian risiko					sda
7	Metode penilaian risiko mampu menggambarkan					sda

	tingkat risiko terkait dengan penyelenggaraan layanan					
8	Telah dilakukan langkah pengendalian terhadap risiko-risiko yang harus dikendalikan					sda
9	Telah dilakukan pemantauan Pada implementasi pengendalian terhadap risiko					sda
10	Identifikasi risiko dibuat berdasarkan aset yang terkait dengan penyelenggaraan layanan: - Resiko Aset Informasi - Resiko Aset Fisik - Resiko Aset SDM - Resiko Aset - Perangkat Lunak (*software*) - Aset Tak berwujud (*intangibel aset*)					sda
11	Daftar identifikasi risiko diperbaharui secara berkala					sda

	atau ketika terjadi perubahan atau penambahan aset					
12	Hasil identifikasi risiko dipantau untuk melihat kemungkinan perubahan risiko					sda

Lampiran 3. Checklist Pemeriksaan Manajemen Aset

No	Pemeriksaan	Kondisi (Poin)				Dokumen Pendukung
		Tidak Ada (0)	Ada Belum di terapkkan (1)	Diterapkan Sebagian (3)	Diterapkan Menyeluruh (5)	
1	Terdapat prosedur pengelolan aset					Dokumen SOP Pengelolaan Aset
2	Prosedur pengelolaan aset memuat aktifitas pendaftaran aset					sda
3	Aset didaftarkan sebagai Barang Milik Negera (BMN) dengan struktur atau format yang konsisten untuk setiap aset					Daftar Aset

4	Aset didaftarkan dengan pengklasifikasian jenis aset berupa Aset Informasi, Aset Pegawai, Aset Fisik, Aset Software, Aset Layanan dan Aset *Intangible*					sda
5	Daftar aset telah memuat deskripsi aset yang cukup sesuai dengan pengklasifikasian aset dan tercantum nama pemilik aset					sda
6	Daftar aset memuat sub klasifikasi dari aset yang merupakan pengelompokkan aset berdasarkan kesamaan ciri yang terkait dengan keamanan informasi					sda
7	Daftar aset dipantau secara berkala					Dokumen catatan perubahan aset
8	Daftar aset diperbaharui					sda

	setiap kali ada perubahan atau penambahan aset					
9	Prosedur pengelolaan aset memuat aktifitas pengklasifikasian aset berdasarkan aspek-aspek keamanan informasi					SOP Pengelolaan Aset
10	Pemberian nilai pada aset berdasarkan klasifikasi keamanan informasi dilakukan dengan konsisten untuk setiap jenis aset					Dokumen Daftar Aset

Lampiran 4. Checklist Pemeriksaan Keamanan

No	Pemeriksaan	Kondisi (Poin)				Dokumen Pendukung
		Tidak Ada (0)	Ada Belum di terapkkan (1)	Diterapkan Sebagian (3)	Diterapkan Menyeluruh (5)	
1	Kebijakan pengelolaan Keamanan perangkat					Dokumen kebijakan layanan TI
2	Terdapat prosedur pengelolaan					SOP Keamanan Perangkat

	keamanan perangkat					
3	Kebijakan atau prosedur pengelolaan keamanan perangkat telah diketahui oleh semua personil dalam penyelenggaraan layanan					Bukti sosialisasi
4	Perangkat pengolah informasi yang bersifat penting atau sensitif ditempatkan dengan aman dan dilindungi dengan perimeter keamanan yang cukup baik					Hasil observasi
5	Perlindungan perangkat pengolah informasi yang bersifat penting atau sensitif sudah sesuai atau sepadan dengan nilai risiko yang melekat pada perangkat tersebut					Sda

6	Perangkat pengolah informasi yang bersifat penting atau sensitif hanya boleh diakses oleh pegawai tertentu diletakkan pada tempat khusus atau pusat data (*data center*)					Dok, SOP akses *Data Center*
7	Tempat khusus untuk perangkat pengolah informasi penting atau sensitif telah dilindungi dari potensi gangguan secara fisik, misalnya pencurian, kebakaran, banjir, dan lain-lain					Hasil Observasi
8	Tempat khusus untuk perangkat pengolah informasi yang bersifat penting atau sensitif sudah memenuhi spesifikasi lingkungan yang dibutuhkan oleh perangkat untuk					sda

	bekerja, misalnya suhu dan tingkat kelembaban					
9	Tempat khusus untuk perangkat pengolah informasi yang bersifat penting sudah dilengkapi dengan alat penangkal petir					sda
10	Terdapat pengaturan tempat, lokasi atau posisi perangkat yang digunakan oleh pegawai ketika digunakan untuk mengakses informasi penting atau sensitif, misalnya komputer/laptop administrator sistem, dan lain-lain					Sda
11	Terdapat pengendalian akses fisik pada tempat khusus untuk perangkat pengolah informasi penting					Dokumen catatan akses *data center*

	atau sensistif, diantara nya pendaftaran hak akses dan prosedur pengaksesan					
12	Terdapat pencatatan terhadap setiap akses fisik yang dilakukan ke tempat khusus untuk perangkat pengolah informasi penting atau sensitif, diantaranya nama yang mengakses, waktu akses dan tujuan akses					Dokumen catatan akses ruangan
13	Pihak ketiga atau pihak lain Yang membutuhkan akses fisik ke tempat khusus perangkat pengolah informasi penting atau sensitif selalu didampingi oleh pegawai yang memiliki hak akses					sda
14	Terdapat pengaturan					sda

	pengamanan perangkat yang digunakan pegawai untuk bekerja, misalnya dengan penerapan autentikasi					
15	Terdapat pencatatan terhadap setiap akses fisik yang dilakukan oleh pengguna ke fasilitas-fasilitas layanan yang disediakan, misalnya akses ke ruang pelatihan, laboratorium, dan lain-lain					sda
16	Terdapat pencatatan akses fisik yang dilakukan oleh pengguna ke fasilitas-fasilitas layanan yang disediakan, sudah memuat nama pengguna, waktu akses dan tujuan mengakses					sda
17	Terdapat pengaturan pengamanan perangkat yang					Dokumen peraturan pengamanan fisik

	digunakan pegawai untuk bekerja, ketika di tinggalkan atau sedang tidak di gunakan, misal nya dengan mengunci layar komputer otomatis atau mematikan komputer					
18	Perangkat pengolah informasi penting atau sensitif sudah disanitasi sebelum dihapuskan, dibuang atau digunakan kembali					Dokumen catatan penghapusan data dan informasi
19	Ada pengaturan untuk penghapusan informasi yang disimpan pada media penyimpanan portable jika sudah tidak digunakan					sda
20	Terdapat pengaturan untuk membatasi penggunaan					Dokumen peraturan pengaman fisik

	media penyimpanan portable pada perangkat pengolah informasi penting atau sensitif					
21	Telah di terapkan pengendalian keamanan informasi yang sesuai untuk informasi penting atau sensitif yang disimpan pada media penyimpanan portable, misalnya informasi yang memiliki tingkat kerahasian tinggi harus di sandikan (enkripsi)					sda

Lampiran 5. Checklist Pemeriksaan Keamanan Operasional

No	Pemeriksaan	Kondisi (Poin)				Dokumen Pendukung
		Tidak Ada (0)	Ada Belum di terapkkan (1)	Diterapkan Sebagian (3)	Diterapkan Menyeluruh (5)	
1	Terdapat kebijakan pengelolaan keamanan operasional layanan					Dokumen kebijakan Pengelolaan Layanan
2	Terdapat prosedur untuk setiap proses dalam penyelenggaraan layanan					Dokumen SOP Layanan Umum
3	Terdapat prosedur-prosedur untuk setiap proses dalam penyelenggaraan layanan yang dibuat secara tertulis					Sda
4	Prosedur-prosedur untuk setiap proses dalam penyelenggaraan layanan sudah memperhatikan aspek-aspek risiko dan keamanan informasi					Dokumen *Risk Management*
5	Prosedur-prosedur untuk setiap proses dalam penyelenggaraan layanan ditinjau secara berkala untuk memastikan efektifitas dan efisiensinya					Dokumen Perubahan SOP
6	Prosedur-prosedur untuk setiap proses dalam					Bukti sosialisasi

	penyelenggaraan layanan diketahui dan dijalankan oleh semua unit yang terkait dalam penyelenggaraan layanan					
7	Semua personil atau unit yang terkait dalam penyelenggaraan layanan sudah bekerja sesuai prosedur					Log Sistem
8	Terdapat pengklasifikasian keamanan (kerahasian, integritas dan ketersedian) terhadap informasi yang terkait dengan penyelenggaraan layanan					Dokumen *Risk Management*
9	Klasifikasi keamanan terhadap informasi yang terkait dengan penyelenggaraan layanan dapat menjelaskan tingkat kepentingan atau sensitifitas dari informasi tersebut					sda
10	Klasifikasi keamanan terhadap informasi yang terkait dengan penyelenggaraan layanan dapat menjelaskan siapa yang boleh ataupun tidak mengakses informasi tersebut					Dokumen Hak Akses
11	Klasifikasi keamanan terhadap informasi yang					sda

	terkait dengan penyelenggaraan layanan dapat diketahui semua personil yang terlibat dalam penyelenggaraan layanan (dengan penggunaan label)					
12	Terdapat identifikasi tugas atau fungsi yang memiliki risiko keamanan tinggi jika dilakukan oleh personil atau unit yang sama dalam penyelenggaraan layanan					sda
13	Terdapat pemisahan tugas atau fungsi yang memiliki risiko keamanan tinggi jika dilakukan oleh personil atau unit yang sama dalam penyelenggaraan layanan					Dokumen Hask Akses dan *Risk Management*
14	Terdapat aktifitas pengawasan terhadap tugas atau fungsi yang memiliki risiko keamanan tinggi jika dilakukan oleh seorang personil atau satu unit dalam penyelenggaraan layanan					Log Akses
15	Terdapat pemisahan antara fisik yang diberikan untuk pengguna dan fasilitas yang digunakan oleh					Hak Akses Fisik (ruangan)

	personil atau unit penyelenggara layanan untuk bekerja					
16	Terdapat pengaturan perijinan dan hak akses untuk pekerjaan jarak jauh (*remote access*) pada perangkat pengolah informasi penting atau sensistif					Perjanjian Kerahasian
17	Terdapat perijinan dan hak akses pada perangkat pengolah informasi penting atau sensitif mempertimbangkan risiko terhadap layanan					sda
18	Terdapat pengendalian hak akses berupa otentikasi dan otorisasi terhadap perangkat pengolah infromasi penting atau sensitif diterapkan					Dokumen pengaturan password
19	Izin dan hak akses yang sudah diberikan, ditinjau secara berkala untuk melihat efektifitas penggunaannya					Log Akses

Lampiran 6. Chceklist Pemeriksaan Keamanan Server

No	Pemeriksaan	Kondisi (Poin)				Dokumen Pendukung
		Tidak Ada (0)	Ada Belum di terapkkan (1)	Diterapkan Sebagian (3)	Diterapkan Menyeluruh (5)	
1	Terapat kebijakan atau prosedur pengelolaan keamanan server dan jaringan					SOP Pengendalian Keamanan fisik dan non fisik
2	Penerapan kebijakan atau prosedur pengelolaan keamanan server dan jaringan dapat memberikan perlindungan berupa akses fisik maupun non fisik dari pihak yang tidak berwenang					sda
3	Akses terhadap server dan jaringan sudah dikendalikan sesuai dengan tingkat kepentingan akses dari pihak- pihak yang diijinkan					Data Hak Akses server, jaringan dan Sistem Informasi Manajemen
4	Pengendalian yang diterapkan untuk membatasi akses yang tidak					Catatan log data akses

	diijinkan selalu dipantau efektifitas dan efisiensinya					
5	Sistem pengendalian telah menggunakan perangkat lunak dinding api (*firewall*) untuk membatasi akses yang tidak diijinkan pada server dan jaringan					Data perangkat lunak *firewall*
6	Pengendalian keamanan server dan jaringan telah dilengkapi anti virus untuk menghindari serangan virus yang dapat mengganggu penyelenggaraan layanan					Data perangkat lunak antivirus dan jaringan
7	Pengendalian keamanan akses yang tidak dizinkan dilengkapi dengan pendeteksi/pencegah gangguan (*intrusion detection system/intrusion prevention system*) untuk menghindari serangan yang dapat mengganggu penyelenggaraan layanan					Data aktifitas *IDS (Intrusion Detection System)* dan *IPS (Intrusion Prevention System)*

8	Perangkat pengendalian yang diterapkan selalu diperbaharui untuk mengikuti tren keamanan informasi					Data catatan *update firewall,* antivirus dan IDS/IPS
9	Layanan-layanan (services) yang diberikan oleh server dan jaringan namun tidak dibutuhkan dalam penyelenggaraan layanan					Data catatan penghentian layanan Sistem Informasi Manajemen (SIM)
10	Layanan-layanan (*services*) yang diberikan oleh server dan jaringan sudah mencukupi kebutuhan penyelenggaraan layanan sudah dimatikan/non aktifkan. (jika ada)					Data catatan SIM dan kebutuhan layanan SIM
11	Terdapat kebijakan atau identifikasi terkait informasi- informasi yang harus di-backup					Dokumen kebijakan keamanan informasi
12	Kebijakan atau identifikasi terkait informasi-informasi yang harus di-backup dibuat tertulis					sda

13	Telah dilakukan identifikasi tingkatan kebutuhan backup terhadap informasi-informasi yang harus dibackup					Analisis kebutuhan *Backup* Data
14	Kegiatan backup yang sudah dilaksanan sesuai dengan identifikasi kebutuhan backup					Catatan identifikasi informasi yang perlu di *bcakup*
15	Kegiatan backup telah dilaksanan dengan penggunaan metode backup (*full backup, differential backup, incremental backup*) secara konsisten					Catatan realisasi *backup* data
16	Rentang waktu atau frekuensi backup sudah disetujui oleh unit kerja operasional SIM					Surat pernyataan persetujuan metode dan model *backup* data
17	Pemilihan metode backup dan frekuensi backup dapat mengendalikan risiko integritas dan ketersediaan dari informasi					Catatan metode dan kegiatan *backup* serta personil pelaksananya
18	Setiap media backup dan					sda

	perangkat pengolah informasi memiliki metode pengendalian kerahasiaan informasi yang sama					
19	Lokasi penyimpanan media backup sudah dianggap cukup untuk mengantisipasi kejadian kerusakan fisik secara bersamaan antara perangkat pengolah informasi dan media backup, misalnya kebakaran, gempa bumi, dll					Catatan lokasi tempat penyimpanan media *backup*
20	Log (catatan akses server) pada sistem aktif dan dipastikan dapat diakses sewaktu dibutuhkan					Catatan log data pada *server*
21	Data log ditinjau secara berkala sesuai dengan ketentuan pemisahan tugas, misalnya data log pengguna sistem ditinjau oleh administrator sistem dan log administrator sistem ditinjau					sda

	oleh pengawas administrator sistem					
22	Telah dilakukan pengendalian integritas data log hingga batas waktu retensinya, misalnya dengan backup					Catatan penghapusan dan pembaharuan *backup* data

Lampiran 7. Checlist Pemeriksaan Perubahan

No	Pemeriksaan	Kondisi (Poin)				Dokumen Pendukung
		Tidak Ada (0)	Ada Belum di terapkkan (1)	Diterapkan Sebagian (3)	Diterapkan Menyeluruh (5)	
1	Terdapat prosedur pengelolaan perubahan untuk memastikan perubahan yang dilakukan membawa dampak positif pada penyelenggaraan layanan					SOP layanan perubahan
2	Terdapat aktifitas alternatif pada prosedur (SOP) untuk pelaksanaan perubahan mendesak (*emergency change*) saat aktifitas perubahan biasa tidak dapat dilaksanakan					sda

	dengan segera					
3	Telah dilakukan identifikasi, perubahan yang akan di lakukan dengan memperhatikan skala prioritas yang bersifat mendesak atau tidak.					sda
4	Aktifitas alternatif untuk pelaksanaan perubahan mendesak disertai dengan pengendalian tambahan untuk memastikan agar tujuan dari perubahan tetap tercapai					Dokumen Rencana Perubahan
5	Setiap perubahan yang dilakukan berdasarkan analisa kebutuhan perubahan dengan memperhatikan sumber (permintaan perubahan), keluhan/laporan pengguna, latar belakang serta maksud dan tujuan dilakukannya perubahan					sda

6	Telah dilakukan analisa dampak dari perubahan terhadap komponen layanan					sda
7	Analisa dampak perubahan sudah memperhatikan keterkaitan perubahan dengan hasil analisa risiko layanan					Sda
8	Terlebih dahulu dilakukan ujicoba terhadap perubahan yang dilakukan, sebelum perubahan tersebut dirilis ke pengguna					Dokumen hasil uji coba perubahan
9	Pada prosedur (SOP) Perubahan terdapat aktifitas untuk pengembalian (*roolback*) ketika ujicoba terhadap perubahan menunjukkan hasil yang tidak sesuai					Dokumen SOP perubahan layanan
10	Semua aktitifas perubahan telah terdokumentasi					Dokumen catatan perubahan
11	Di dalam dokumentasi perubahan memuat waktu perubahan dilakukan					sda

12	Di dalam dokumentasi perubahan memuat informasi kebutuhan perubahan					sda
13	Di dalam dokumentasi perubahan memuat hasil identifikasi jenis perubahan					sda
14	Di dalam dokumentasi perubahan memuat tindakan yang diambil untuk menerapkan perubahan, baik perubahan mendesak maupun perubahan biasa					sda
15	Di dalam dokumentasi perubahan memuat hasil ujicoba terhadap perubahan beserta persetujan dari pengguna layanan					sda