LAMPIRAN-LAMPIRAN

Lampiran 1. Surat Ijin Penelitian

129
24/02

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI
UNIVERSITAS PENDIDIKAN GANESHA
FAKULTAS TEKNIK DAN KEJURUAN
Alamat Jalan Udayana Nomor 11, Singaraja 81116
Telepon (0362) 25571 Fax. (0362) 25571
Laman http://ftk.undiksha.ac.id

Nomor : 438/UN48.11.1/DT/2022 Singaraja, 25 Pebruari 2022
Lampiran : -
Hal : Permohonan Data

Yth. Ketua UPT. TIK Undiksha
di tempat

Dengan hormat, dalam rangka melengkapi persyaratan penyusunan Skripsi, bersama ini dimohon bantuannya untuk memberikan informasi yang diperlukan terkait data mengenai "Keamanan Informasi", kepada mahasiswa berikut.

Nama : Putu Risma Widharini
NIM : 1815091017
Program Studi : Sistem Informasi
Semester : VIII (delapan)

Demikian surat ini disampaikan, atas perkenaan dan kerjasamanya diucapkan terima kasih.

a.n. Dekan,
Wakil Dekan I,

Dr. Ketut Agustini, S.Si., M.Si.
NIP 197408012000032001

Lampiran 2. Transkrip Wawancara Awal

Hasil Wawancara Awal

Hari/Tanggal	Jumat, 11 Maret 2022
Jam Wawancara	10:00 WITA-selesai
Tempat	UPA TIK Universitas Pendidikan Ganesha
Nama Responden	Made Agus Januharsa, S.Kom., M.Kom
Jabatan Responden	Anggota Devisi Infrastruktur, Jaringan dan Keamanan
Tanda Tangan	

Pertanyaan : Apakah pernah terjadi serangan keamanan informasi di UPA TIK ? jika pernah, serangan seperti apa yang terjadi ?
Jawaban : Pernah terjadi serangan di website Undiksha yang mana ada oknum yang mencoba untuk membobol website dan sempat mengganti beberapa tampilan antar muka website namun sebelum oknum tersebut bertindak lebih jauh, serangan itu sudah diatasi. Serangan lainnya yang pernah terjadi adalah DDoS yang menyebabkan *traffic* internet melampaui batas maksimalnya sehingga perangkat sempat mengalami *heng*. Sedangkan, serangan untuk bagian sistem informasi seperti SIAK dan yang lainnya belum pernah terjadi karena UPA TIK sudah menerapkan *firewall* yang bisa mendeteksi ancaman akan terjadinya serangan keamanan sebelum hal tersebut bisa terjadi.
Pertanyaan : Apakah pernah terjadi pencurian data pada sistem di UPA TIK ?
Jawaban :

Selama ini belum pernah terjadi kasus pencurian data
Pertanyaan : Apakah bapak mengetahui kemungkinan apa yang menyebabkan pernah terjadinya serangan ?
Jawaban : Kemungkinan serangan terjadi karena oknum iseng dan coba – coba ingin coba mengubah-ubah tampilan website dan mencoba masuk ke website. Kalau mengambil data mungkin mereka belum bisa menembusnya karena UPA telah mengantisipasi hal tersebut dan UPA memiliki DMZ yang berarti ada area tertentu yang tidak bisa diakses oleh pihak luar
Pertanyaan : Saat terjadinya serangan, apa yang dilakukan oleh pihak UPA TIK ?
Jawaban : Waktu itu serangan bisa terjadi karena php belum di update ke versi terbaru, wordpress juga belum di update yang menyebabkan adanya celah kemanan yang bisa ditembus oleh karena itu, saat terjadi serangan dilakukan update yang masih versi lama ke versi terbaru. Untuk serangan DDoS juga pada saat itu belum dilakukan update pada sistem operasinya sehingga saat itu juga dilakukan update pada sistem operasi ke yang terbaru
Pertanyaan : Apakah ada dokumen yang mendokumentasikan terkait versi perangkat lunak yang digunakan untuk mempermudah mengetahui apakah perangkat sudah versi terbaru atau masih versi lama ?
Jawaban : Untuk masalah update, dilakukan oleh tim pengembang. Pada saat terjadinya serangan, devisi infrastruktur dan jaringan dan bagian multimedia juga mengecek adanya serangan yang mana informasi mengenai serangan yang didapat dilanjutkan

ke devisi sistem informasi dan dicek oleh mereka dan ditemukan bahwa belum dilakukan update pada perangkat lunak yang digunakan.
Pertanyaan : Saat terjadinya serangan, apakah kejadian tersebut didokumentasikan dengan cara sepertu dibuatkan laporan ?
Jawaban : Biasanya akan dibuatkan dokumentasinya oleh devisi sistem informasi. Devisi infrastruktur dan jaringan hanya melaporkan dulu adanya "hal yang aneh" yang ditemkan pada saat monitoring ke devisi sistem informasi untuk mengeceknya lebih lanjut
Pertanyaan : Terkait keamanan informasi apakah devisi infrastruktur dan jaringan hanya bertugas untuk mengetahui adanya serangan keamanan?
Jawaban : Iya, devisi infrastruktur dan jaringan hanya berada di ranah jaringan dan infrastruktur dalam artian seperti server, perangkat keras, infrastruktur jaringannya, dan topologi jaringan tidak sampai ke ranah sistem informasi karena untuk masalah penanganan di bagian sistem informasi sudah ada devisi sendiri yang menangani

Lampiran 3. Daftar Narasumber

Hasil Wawancara Indeks KAMI

No	Narasumber	Tanggal Wawancara	Pertanyaan Area Indeks KAMI	Tanda Tangan
1	Ir. Gede Arna Jude Saskara, S.T., M.T	5 Juli 2023, 15 November 2023, dan 14 Desember 2023	sistem elektronik, area tata kelola; risiko keamanan informasi; kerangka kerja; pengelolaan aset; teknologi; suplemen (pengamanan layanan infrastruktur awan (*cloud service*))	
2	Ir. I Made Dendi Masanjaya, S.Pd., M.Eng	16 Januari 2024	area tata kelola (2.11), area pengelolaan aset dan suplemen (perlindungan data pribadi)	
3	Ir. I Made Ardwi Pradnyana, S.T., M.T	9 November 2023 dan 15 November 2023	Area pengelolaan aset informasi dan suplemen (layanan)	
4	Ida Komang Widhiarjaya, S.T., M.Pd.	16 Januari 2024	sistem elektronik, suplemen	
5	I Nyoman Yoga Satyawan, S.ST., M.Kom	1 Februari 2024	area kerangka kerja dan area pengelolaan aset	

No.	Pertanyaan Indeks KAMI Sistem Elektronik	Jawaban
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	B

Lampiran 4. Rangkuman Transkrip Wawancara

Pertanyaan	Jawaban
2.1; Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Bertanggung jawab secara prinsip dan resmi
2.2; Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Terdapat divisi yang menangani hal tersebut yaitu divisi infrastruktur & keamanan informasi yang ada pada bagan struktur organisasi walaupun dalam penerapan belum ada unit khusus yang memiliki tugas dan tanggung jawab dalam mengelola keamanan informasi dan menjaga kepatuhannya
2.3; Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Belum didefinisikan wewenang terkait penerapan dan menjamin kepatuhan program keamanan informasi
2.4; Apakah penanggung jawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola	Sumber daya manusia untuk bagian keamanan informasi yang disediakan masih kurang

dan menjamin kepatuhan program keamanan informasi?	
2.5; Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi (pemisahan) kewenangan?	Belum ada pemetaan dan belum pernah dilakukan audit internal terkait keamanan informasi
2.6; Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Belum adanya syarat kompetensi dan keahlian untuk pelaksana pengamanan informasi yang berlaku secara tertulis
2.7; Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Kompetensi yang dimiliki sudah cukup baik namun sesuai dengan pernyataan 2.6 terkait belum adanya syarat yang berlaku secara tertulis
2.8; Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Belum ada sosialisasi secara resmi namun untuk semua pihak di UPA TIK sudah paham dan sadar akan keamanan informasi di instansi. Pernah melakukan *sharing* terkait data pribadi kepada mahasiswa
2.9; Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan	Belum ada

petugas pelaksana pengelolaan keamanan informasi?	
2.10; Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Integrasi dilakukan di bagian internet dan intranet.
2.11; Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Sudah dikategorikan bagian mana yang bersifat publik dan terbatas.
2.12; Apakah tanggung jawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Ada koordinasi dengan pihak lain yang terkait dengan infrastruktur (provider wifi) namun belum ada dokumen resminya. Untuk keamanan informasi masih seluruhnya dilakukan sendiri oleh pihak UPA (koordinasi antar divisi)
2.13; Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang	Koordinasi dilakukan proaktif antar divisi.

berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	
2.14; Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sudah didefinisikan dan dialokasikan?	Belum didefinisikannya business continuity dan disaster recovery plans. Yang baru dilakukan adalah backup data saja
2.15; Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Belum adanya pelaporan secara rutin. Biasanya pelaporan dilakukan saat terjadi insiden keamanan informasi saja
2.16; Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Menjadi bagian dari proses pengambilan Keputusan. Misalnya, dilakukan rapat peningkatan keamanan dan antisipasi kebocoran data pada sistem
2.17; Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi,	Belum ada

khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	
2.18; Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Belum ada
2.19; Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Belum ada
2.20; Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Belum ada
2.21; Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Belum ada

2.22; Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Belum ada
3.1; Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Belum ada program kerja pengelolaan risiko keamanan informasi
3.2; Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Belum ada yang berperan sebagai penanggung jawab manajemen risiko keamanan informasi
3.3; Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Belum ada kerangka kerja pengelolaan risiko keamanan informasi
3.4; Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Belum ada

3.5; Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Belum didefiniskan terkait penetapan ambang batas tingkat risiko keamanan informasi yang dapat diterima
3.6; Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Ada dokumen aset informasi
3.7; Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Belum dilakukan identifikasi
3.8; Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Belum ada
3.9; Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Belum ada

3.10; Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Belum dilakukan penyusunan langkah mitigasi penanggulangan risiko
3.11; Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Belum dilakukan penyusunan karena langsung dilakukan saat itu juga ketika terjadi suatu insiden keamanan informasi. Belum dibuatkan dokumen
3.12; Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Belum ada
3.13; Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Belum ditetapkan
3.14; Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau	Belum ada

keperluan penerapan bentuk pengamanan baru?	
3.15; Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Belum dilakukan
3.16; Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Belum ada
4.1; Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Belum adanya kebijakan dan prosedur terkait keamanan informasi secara tertulis
4.2; Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Belum dibuatnya dokumen kebijakan keamanan informasi
4.3; Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan	Belum ada mekanisme pengalolaan dokumen kebijakan dan prosedur keamanan informasi secara tertulis

daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	
4.4; Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Belum ada
4.5; Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	Belum ada
4.6; Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Insiden dapat langsung diidentifikasi karena rutin dilakukan scanning pada sistem dan juga adanya sistem missu sebagai sistem yang mendokumentasikan pengaduan dalam pengelolaan laporan insiden
4.7; Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK	Belum ada, tidak ada kerjasama untuk keamanan informasi dengan pihak ketiga

tercantum dalam kontrak dengan pihak ketiga?	
4.8; Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Belum didefinisikan secara tertulis
4.9; Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	Belum ada prosedur resmi
4.10; Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya?	Belum adanya kebijakan dan prosedur khusus terkait pengelolaan implementasi *security patch*
4.11; Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	belum
4.12; Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi	Sudah dilakukan evaluasi risiko pembelian sistem baru dan masalah

risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	yang muncul. Sebelum membeli sistem baru dievaluasi risikonya seperti apa saja. Dilakukan pendokumentasian (yang mengetahui secara detail kepala devisinya). (dukumen evaluasi)
4.13; Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Proses pengembangan secara umum belakangan sekarang yg baru sudah diterapkan pengembangan yang aman menggunakan SDLC. Ada dokumentasi. Perencanaan, apa yang digunakan, sudah terdukumentasi ada di masing-masing. Proses bisnis, perancangan semuanya per masing-masing sistem (dukumen nama sistemnya)
4.14; Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Ada proses pengulangan. Jika sistem mengalami kebocoran data sudah ditangani. Tim pengembang sistem harus menggunakan tunel yang sesuai sudah dilakukan penanggulangan. Tidak dibuatkan jadwal karena serangan ditangani saat itu juga. Secara rutin dilakukan scaning sistem (scanning hampir setiap hari dilakukan oleh devisi infrastruktur, jaringan dan keamanan informasi tapi tidak semua sistem)

4.15; Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Belum adanya dokumentasi business continuity plan yang mendefinisikan persyaratan/konsiderans keamanan informasi namun uji coba pengeloaan perancanaan kelangsungan layanan TIK pernah dilakukan
4.16; Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Belum ada *disaster recovery plan* hanya baru dilakukan backup untuk datanya saja
4.17; Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak ada
4.18; Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	belum ada perencanaan pemulihan bencana sehingga belum pernah dilakukan evaluasi

4.19; Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Belum dilakukan evaluasi kelayakan
4.20; Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Belum ada
4.21; Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Belum
4.22; Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Belum
4.23; Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Belum pernah dilakukan audit internal terkait keamanan informasi
4.24; Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi	Belum

dan efektivitas penerapan keamanan informasi?	
4.25; Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Belum
4.26; Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Belum
4.27; Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Belum ada kebijakan atau prosedur untuk bagian keamanan informasi
4.28; Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan	Belum pernah dilakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi secara rutin

yang diperlukan, telah diterapkan secara efektif?	
4.29; Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Untuk rencana ada tapi belum dilakukan
5.1; Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Ada dokumen inventaris aset informasi
5.2; Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak ada klasifikasi aset
5.3; Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Belum ada
5.4; Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Belum ada

5.5; Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Ada pengelolaan perubahan terhadap sistem dan konfigrasi namun tidak ada dokumennya
5.6; Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Ada,tidak didokumentasikan dan belum dilakukan secara konsisten
5.7; Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Belum ada
5.8; Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Belum dilakukan untuk semua personil di instansi
5.9; Tata tertib penggunaan komputer, email, internet dan intranet	Hanya ada tata tertib penggunaan komputer
5.10; Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Belum ada
5.11; Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Belum ada
5.12; Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak ada peraturan yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
5.13; Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya	Tergantung risiko dari pemegang akun itu sendiri. Tidak ada kebijakan terkait pelanggaran yang ditentukan

5.14; Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Ada prosedur. Pemantauan secara berkala. Dilakukan pemantauan secara berkala 1 tahun minimal dilakukan 2 kali. Prosedur tertulisnya tidak lengkap. IK Layanan Data Dan Informasi (pemetaan data dan dokumen data)
5.15; Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dilakukan secara berkala. Ada beberapa data yang dipilah untuk dihapus. Pengelolaan data yang disimpan dan dihapus belum ada (dokumen syarat dan ketetapannya) perhapusan permanen masih belum dilakukan. Datanya masih tersimpan tapi akses ke sistem dihilangkan (penghapusan masih sekedar ini saja)
5.16; Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Hanya dilakukan pertukaran data kepada kementerian atau data dosen mealui website belum ada dokumen dan ketetapannya
5.17; Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dilakukan penyidikan namun tidak dibuatkan dokumen tertulisnya
5.18; Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	Sudah dilakukan backup secara otomatis belum pernah dilakukan restore (IK Proses *Backup* dan *Restore*)

5.19; Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Belum ada ketentuan pengamanan fisik
5.20; Proses pengecekan latar belakang SDM	Ada, ketika perekrutan karyawan misal bagian *programmer*
5.21; Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Insiden keamanan informasi hanya didiskusikan kepada pihak internal saja biasanya
5.22; Prosedur penghancuran data/aset yang sudah tidak diperlukan	Tidak ada prosedur tapi dilakukan ketika data sudah tidak diperlukan
5.23; Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku	Tidak ada prosedur secara tertulis
5.24; Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Tidak ada prosedur secara tertulis
5.25; Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Data di *backup* namun daftar datanya dan laporan kepatuhan tidak ada
5.26; Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak ada
5.27; Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan	Tidak ada

aspek HAKI dan pengamanan akses yang digunakan?	
5.28; Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Semua pihak bisa masuk ke UPA TIK namun untuk tempat - tempat tertentu akses masuknya sudah dibatasi dan terdapat passlock pada masing-masing pintunya
5.29; Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Menggunakan *passcode* dan kunci
5.30; Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Ada tabung gas pemadam kebakaran, serta untuk suhu dan kelembaban sendiri dilakukan dengan dipasang AC disetiap ruang
5.31; Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Ada penangkal petir yang dipasang diatap gedung
5.32; Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Tidak ada
5.33; Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Tidak ada

5.34; Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Ada fasilitas pendukung yaitu AC pada tiap-tiap ruang dan tabung gas pemadam kebakaran yang terletak di depan meja helpdesk
5.35; Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Tidak dilakukan perawatan komputer secara khusus. Biasanya dilakukan pada jaringan
5.36; Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Tidak ada
5.37; Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	Tidak ada peraturan khusus
5.38; Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang	Tidak ada

bekerja untuk kepentingan instansi/perusahaan anda?	
6.1; Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Belum
6.2; Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Dari sisi kepentingan belum.segmentasi hanya dilakukan dari sisi servernya saja. Server front end dan server back end
6.3; Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Ada, menggunakan firewall. Dokumen panduan instalasi server (firewall)
6.4; Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Belum dilakukan
6.5; Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Ada beberapa sistem yang sudah dipindai secara rutin dan dokumentasinya sudah ada berupa dokumentasi konfigurasi dan dokumentasi hasil pemindaian
6.6; Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Iya, dilakukan perancangan
6.7; Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk	Ada pemantauan dan monitoring secara berkala

memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	
6.8; Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Ada capture log
6.9; Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Untuk ke sistem belum namun untuk ke server dilakukan perekaman log secara otomatis
6.10; Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Tidak ada
6.11; Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak dilakukan enskripsi, hanya berupa *password*
6.12; Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Tidak ada standar enskripsi untuk *password*
6.13; Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Semua password dikelola dan disimpan oleh sistem. Diperbaharui setiap 6 bulan sekali. Belum ada panduan tertulis
6.14; Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password,	Masih diganti secara manual

mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?	
6.15; Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Ya, pengembang hanya bisa sampai GIT dan dilanjutkan oleh tim develop untuk ke bagian server
6.16; Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses?	Sudah diterapkan ke semua pengguna
6.17; Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Belum ada
6.18; Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Tidak ada pengamanan khusus
6.19; Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Untuk server belum pernah dimutakhirkan namun ada rencana untuk diperbaharui ke versi terkini
6.20; Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	Untuk desktop sudah
6.21; Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa	tidak ada

antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	
6.22; Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak ada laporan karena belum pernah terkena serangan malware
6.23; Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Standarnya belum ada namun sinkronisasi terus berjalan secara otomatis. Data dengan apk saling sinkron
6.24; Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Selalu dilakukan spesifikasi dan fungsi keamanan dalam proses pengembangan dan uji coba. Dibuatkan dokumentasi hasil pengujian secara black box sudah ada dokumentasinya.
6.25; Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	Sudah menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar
6.26; Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak ada, semua dikerjakan oleh pihak internal UPA TIK
7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Tidak ada

7.1.1.2 Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Tidak ada
7.1.1.3 Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Tidak ada
7.1.1.4 Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Tidak ada
7.1.1.5 Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Tidak ada Kerjasama dengan pihak ke-3 terkait keamanan informasi
7.1.1.6 Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Tidak ada
7.1.1.7 Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga?	Tidak ada

Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	
7.1.2.1 Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	Sudah. tidak ada dokumennya
7.1.2.2 Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Ada surat kontrak kerjasama dengan UPA TIK ada tapi yang terkait dengan risiko keamanan informasi tidak ada.
7.1.2.3 Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Dilakukan pemantauan atau/evaluasi untuk infrastruktur. Tiap minggu dilakukan secara rutin. Diberikan laporan setiap bulan.
7.1.3.1 Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	Ada proses dan prosedur. Prosedur dengan pihak ketiga tidak ada tapi untuk internal ada
7.1.3.2 Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah	Tidak menggunakan pihak ketiga untuk melakukan pemantauan dalam melaksanakan audit keamanan

ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	informasi. Belum pernah dilakukan audit keamanan informasi
7.1.3.3 Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	Ada dokumen SLA dari pihak ke-3 tapi bukan tentang keamanan
7.1.3.4 Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Tidak dilakkan rapat. Dipelajari saja laporan yang diberikan selama sebulan sekali.
7.1.3.5 Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	Iya, ada dokumen laporannya
7.1.3.6 Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Tidak ada
7.1.3.7 Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	Tidak ada
7.1.3.8 Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah	Sudah ada dokumentasi kontraknya. Sejauh ini belum pernah ada pelanggaran yang menyebabkan denda dari pihak ke 3

didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	
7.1.4.1 Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	Iya. Melaksanakan spesifikasi ulang, risiko tiap tahun deivaluasi, perosedur dilakukan perbaikan (tiap tahun)
7.1.4.2 Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Tiap tahun dilakukan untuk mempengaruhi kebijakan pada tahun berikutnya
7.1.5.1 Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?	Kemungkinan ada prosedur formal dari pihak ke-3 tapi pihak UPA TIK tidak mengetahui bagaimana prosedurnya. Kalo data tidak ada
7.1.5.2 Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	Tidak ada
7.1.6.1 Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	Ada prosedur pelaporan terkait insiden yang terjadi pada internet dan manajemen wifi saja karena tidak ada kerjasama terkait keamanan informasi ke pihak ketiga
7.1.6.2 Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Setiap insiden yang terkait dengan internet dan manajemen *wifi* dilaporkan ke *email*

7.1.7.1 Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	Belum dilakukan
7.1.7.2 Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Belum
7.1.7.3 Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Ada tim khusus yang ditugaskan di UPA dari pihak ke-3. Kontraknya jadi 1 antara pihak ke-3 dengan orang yang ada di UPA dari pihak ke-3
7.2.1; Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	Tidak pernah dilakukan kajian tapi digunakan cloud untuk penyimpanan
7.2.2; Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	Tidak ada
7.2.3; Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?	Tidak ada
7.2.4; Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan	Tidak ada

memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	
7.2.5; Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	Tidak ada
7.2.6; Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Tidak ada
7.2.7; Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Tidak ada
7.2.8; Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Tidak ada
7.2.9; Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	Untuk insiden, masih dilakukan pelaporan berupa screenshot
7.2.10; Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Belum ada kebijakan/aturan pemberhentian layanan

7.3.1 Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Belum ada. Keamanan data pribadi masih dibebankan kepada pemilik data itu sendiri
7.3.2 Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	Belum ada
7.3.3 Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Belum ada
7.3.4 Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Disesuaikan dengan milik BSSN
7.3.5 Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	Sudah ada pembagian tugas per orang di tiap devisi. Penangung jawab ke masing-masing
7.3.6 Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	Risiko data pribadi merupakan risiko sendiri

7.3.7 Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Iya
7.3.8 Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Tidak ada
7.3.9 Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Tidak ada
7.3.10 Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?	Tidak ada
7.3.11 Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Lewat helpdesk missiu lalu disalurkan ke devisi. SOP dari pihak helpdesk (sudah ada sopnya) untuk pelaporan insiden.
7.3.12 Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Pemilik data pribadi dapat mengakses data mereka

7.3.13 Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Dulu diwajibkan pergantian misal kata sandi dan username penting jika ada pergantian staff tapi sekarang belum dilakukan lagi dan dokumennya belum ada juga
7.3.14 Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	Dilakukan peghapusan data berdasarkan kriteria tertentu/ saat data sudah tidak tidak diperlukan lagi tapi tidak memerlukan perjanjian dengan pemilik data. Belum ada dokumen tertulis
7.3.15 Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?	Belum ada dokumen tertulis untuk penghapusan data
7.3.16 Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Belum ada untuk secara resmi pedomannya tapi sudah dilakukan

Lampiran 5. Hasil Perhitungan Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi				
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			**Status**	Skor
#	**Fungsi/Organisasi Keamanan Informasi**			
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Perencanaan	1
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Perencanaan	1
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan	0
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0

2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan	0
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Perencanaan	1
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Perencanaan	2
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Dalam Perencanaan	2
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Dalam Perencanaan	2
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk	Tidak Dilakukan	0

			menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?		
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Perencanaan	2
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Dalam Perencanaan	2
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Dalam Perencanaan	2
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak Dilakukan	0
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan	0
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi	Tidak Dilakukan	0

			individu (pejabat & petugas) pelaksananya?		
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Tidak Dilakukan	0
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak Dilakukan	0
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
			Total Nilai Evaluasi Tata Kelola	**21**	

Lampiran 6. Hasil Perhitungan Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi					
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Kajian Risiko Keamanan Informasi**		
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Tidak Dilakukan	0
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan	0
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Tidak Dilakukan	0
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Perencanaan	1

3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Diterapkan Secara Menyeluruh	3
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Perencanaan	1
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Tidak Dilakukan	0
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Tidak Dilakukan	0
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Perencanaan	1
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Perencanaan	2
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak Dilakukan	0

3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan	0
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	Tidak Dilakukan	0
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan	0
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan	0
			Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	**8**	

Lampiran 7. Hasil Perhitungan Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#	**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Tidak Dilakukan	0
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Tidak Dilakukan	0
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Tidak Dilakukan	0
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Tidak Dilakukan	0
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari	Tidak Dilakukan	0

			hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?		
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh	3
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Tidak Dilakukan	0
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Perencanaan	2
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?	Tidak Dilakukan	0
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan	0
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Tidak Dilakukan	0

4.12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Perencanaan	2
4.13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Dalam Perencanaan	2
4.14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	Dalam Perencanaan	2

4.15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Dalam Perencanaan	2
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan	0
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak Dilakukan	0
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	Tidak Dilakukan	0
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan	0
#	**Pengelolaan Strategi dan Program Keamanan Informasi**				
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Tidak Dilakukan	0
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan	Tidak Dilakukan	0

			pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?		
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Tidak Dilakukan	0
4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Tidak Dilakukan	0
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Tidak Dilakukan	0
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan	0
4.27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Tidak Dilakukan	0
4.28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak Dilakukan	0

4.29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Tidak Dilakukan	0
			Total Nilai Evaluasi Kerangka Kerja	**13**	

Lampiran 8. Hasil Perhitungan Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi					
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengelolaan Aset Informasi**		
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	3
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Tidak Dilakukan	0
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Tidak Dilakukan	0
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Perencanaan	1
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Perencanaan	1
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Tidak Dilakukan	0
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai		

			kelanjutan dari proses penerapan mitigasi risiko?		
5.8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dalam Perencanaan	1
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Penerapan / Diterapkan Sebagian	2
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Tidak Dilakukan	0
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Dalam Perencanaan	1
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak Dilakukan	0
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Perencanaan	1
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian	2
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Dalam Perencanaan	1
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan	0
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Perencanaan	1
5.18	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	Dalam Penerapan / Diterapkan Sebagian	2
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Tidak Dilakukan	0

5.20	III	2	Proses pengecekan latar belakang SDM	Diterapkan Secara Menyeluruh	6
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Tidak Dilakukan	0
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Dalam Perencanaan	2
5.23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Dalam Perencanaan	2
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Perencanaan	2
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan	0
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan	0
5.27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/*vendor*) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan	0
#		**Pengamanan Fisik**			
5.28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Diterapkan Secara Menyeluruh	3
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	3

5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Diterapkan Secara Menyeluruh	3
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Diterapkan Secara Menyeluruh	3
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Tidak Dilakukan	0
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Tidak Dilakukan	0
5.34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Diterapkan Secara Menyeluruh	6
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Perencanaan	2
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Tidak Dilakukan	0
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi)	Tidak Dilakukan	0

			yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)		
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Tidak Dilakukan	0
			Total Nilai Evaluasi Pengelolaan Aset	**48**	

Lampiran 9. Hasil Perhitungan Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
#			**Pengamanan Teknologi**		
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Diterapkan Secara Menyeluruh	3
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Dalam Perencanaan	1
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dalam Perencanaan	1
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Tidak Dilakukan	0
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Penerapan / Diterapkan Sebagian	2
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Dalam Perencanaan	1
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan	Dalam Perencanaan	1

			kapasitas yang cukup untuk kebutuhan yang ada?		
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Diterapkan Secara Menyeluruh	3
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Tidak Dilakukan	0
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak Dilakukan	0
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan	0
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Perencanaan	2
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	Tidak Dilakukan	0
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Diterapkan Secara Menyeluruh	6
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	Diterapkan Secara Menyeluruh	6
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan	Tidak Dilakukan	0

			akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?		
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Tidak Dilakukan	0
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	2
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Penerapan / Diterapkan Sebagian	2
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak Dilakukan	0
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan	0
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	4
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Dalam Perencanaan	2
6.25	III	3	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?	Dalam Perencanaan	3

6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan	0
			Total Nilai Evaluasi Teknologi dan Keamanan Informasi	**42**	

Lampiran 10. Hasil Perhitungan Suplemen

Bagian VII: Suplemen					
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.					
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	Skor
7,1			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**		0,63
7.1.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**		
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Tidak Dilakukan	0
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Tidak Dilakukan	0
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Tidak Dilakukan	0
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Tidak Dilakukan	0
7.1.1.5		1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?	Tidak Dilakukan	0
7.1.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan	Tidak Dilakukan	0

			persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?		
7.1.1.7		1	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	Tidak Dilakukan	0
7.1.2			**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**		
7.1.2.1		1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	Dalam Perencanaan	1
7.1.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Tidak Dilakukan	0
7.1.2.3		1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Dalam Perencanaan	1
7.1.3			**Pengelolaan Layanan dan Keamanan Pihak Ketiga**		
7.1.3.1		1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	Tidak Dilakukan	0
7.1.3.2		1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	Tidak Dilakukan	0
7.1.3.3		1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan	Dalam Perencanaan	1

			(SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?		
7.1.3.4		1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Tidak Dilakukan	0
7.1.3.5		1	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	Dalam Perencanaan	1
7.1.3.6		1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Tidak Dilakukan	0
7.1.3.7		1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	Tidak Dilakukan	0
7.1.3.8		1	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	Dalam Perencanaan	1
7.1.4			**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**		
7.1.4.1		1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	Dalam Perencanaan	1
7.1.4.2		1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Dalam Perencanaan	1
7.1.5			**Penanganan Aset**		

7.1.5.1		1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?	Tidak Dilakukan	0
7.1.5.2		1	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	Tidak Dilakukan	0
7.1.6			**Pengelolaan Insiden oleh Pihak Ketiga**		
7.1.6.1		1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	Tidak Dilakukan	0
7.1.6.2		1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Tidak Dilakukan	0
7.1.7			**Rencana Kelangsungan Layanan Pihak Ketiga**		
7.1.7.1		1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	Tidak Dilakukan	0
7.1.7.2		1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Tidak Dilakukan	0
7.1.7.3		1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Tidak Dilakukan	0
7,2			**Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**		0,10
7.2.1		1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	Dalam Perencanaan	1
7.2.2		1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?	Tidak Dilakukan	0

7.2.3		1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?	Tidak Dilakukan	0
7.2.4		1	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?	Tidak Dilakukan	0
7.2.5		1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?	Tidak Dilakukan	0
7.2.6		1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud,* termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Tidak Dilakukan	0
7.2.7		1	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Tidak Dilakukan	0
7.2.8		1	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Tidak Dilakukan	0
7.2.9		1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?	Tidak Dilakukan	0
7.2.10		1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Tidak Dilakukan	0
7,3			**Perlindungan Data Pribadi**		0,69
7.3.1		1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Tidak Dilakukan	0

7.3.2		1	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	Tidak Dilakukan	0
7.3.3		1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Tidak Dilakukan	0
7.3.4		1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Dalam Perencanaan	1
7.3.5		1	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	Tidak Dilakukan	0
7.3.6		1	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	Dalam Perencanaan	1
7.3.7		1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Dalam Perencanaan	1
7.3.8		1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Tidak Dilakukan	0
7.3.9		1	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Tidak Dilakukan	0
7.3.10		1	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut	Tidak Dilakukan	0

			dan menyimpan catatan persetujuan tersebut ?		
7.3.11		1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Dalam Perencanaan	1
7.3.12		1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Diterapkan Secara Menyeluruh	3
7.3.13		1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Tidak Dilakukan	0
7.3.14		1	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	Dalam Perencanaan	1
7.3.15		1	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?	Diterapkan Secara Menyeluruh	3
7.3.16		1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Tidak Dilakukan	0

Lampiran 11. Bukti Validasi Data

BERITA ACARA VERIFIKASI, VALIDASI DATA, DAN REKOMENDASI PENELITIAN

Pada hari ini, , bertempat di UPA TIK Undiksha, kami yang bertanda tangan di bawah ini:

1. **Nama Peneliti** : Putu Risma Widharini
   NIM : 1815091017
   Program Studi : Sistem Informasi
   Fakultas : Fakultas Teknik dan Kejuruan
   Universitas : Universitas Pendidikan Ghanesa
2. **Nama Pembimbing 1** : I Ketut Resika Arthana, S.T., M.Kom
3. **Nama Pembimbing 2** : Ir. I Made Ardwi Pradnyana, S.T., M.Kom

Dengan ini menyatakan bahwa telah dilakukan verifikasi dan validasi terhadap data yang diperoleh dalam penelitian skripsi yang berjudul **"Pengukuran Tingkat Kematangan Keamanan Informasi UPA TIK Universitas Pendidikan Ganesha Menggunakan Indeks Kami Berbasis ISO/IEC 27001:2013"**

Proses Verifikasi dan Validasi Data:

Verifikasi data dilakukan untuk memastikan bahwa data yang dikumpulkan sesuai dengan metode dan instrumen yang telah dirancang, serta validitas data diuji untuk memastikan bahwa data yang diperoleh benar-benar menggambarkan fenomena yang diteliti. Proses ini melibatkan pengecekan keakuratan dan kesesuaian data dengan sumber yang ada.

Deskripsi Data yang Diverifikasi dan Divalidasi:

1. **Jenis Data** : Kualitatif
2. **Sumber Data** : Sumber data didapatkan dari pernyataan narasumber, dokumen-dokumen terkait, serta observasi kondisi langsung pada tempat penelitian.
3. **Jumlah Narasumber** : Narasumber berjumlah 6 orang.
   - Ir. Gede Arna Jude Saskara, S.T., M.T selaku ketua devisi infrastruktur, jaringan dan keamanan
   - Ir. I Made Dendi Masanjaya, S.Pd., M.Eng selaku ketua devisi pusat data dan informasi

- Ir. I Made Ardwi Pradnyana, S.T., M.T selaku ketua devisi helpdesk dan dokumentasi
- Ida Komang Widhiarjaya, S.T., M.Pd. selaku sekretaris UPA TIK
- I Nyoman Yoga Satyawan, S.ST., M.Kom selaku anggota devisi sistem informasi
- Made Agus Januharsa, S.Kom., M.Kom selaku anggota devisi infrastruktur, jaringan dan keamanan

4. **Metode Pengumpulan Data** :

- Observasi

  Observasi dilakukan untuk mengetahui kondisi tempat dilakukannya penelitian dengan cara pengamatan langsung dan memberikan beberapa pertanyaan terkait.

Aktivitas	Keterangan
Observasi dan Wawancara awal	Dilakukan pada tanggal : 11 maret 2022 Waktu : 10:00 WITA-selesai Lokasi : UPA TIK Undiksha Narasumber : Made Agus Januharsa, S.Kom., M.Kom Objek : Kondisi dan proses penanganan keamanan informasi yang terdapat di UPA TIK Tujuan : Mengetahui apakah pernah terjadi serangan atau ancaman terkait keamanan informasi dan bagaimana proses yang dilakukan untuk menanganinya sehingga dapat melakukan pemetaan perumusan masalah dalam penelitian berdasarkan kondisi awal yang didapat. Hasil : Pernah terjadi serangan pihak ketiga yang mengubah tampilan website milik Undiksha dan adanya serangan DdoS dan proses penanganan dilakukan secara spontan atau langsung saat itu juga.

- Wawancara

Aktivitas	Keterangan
Wawancara narasumber 1	Dilakukan pada tanggal : 5 Juli 2023, 15 November 2023, dan 14 Desember 2023 Lokasi : UPA TIK Undiksha Narasumber : Ir. Gede Arna Jude Saskara, S.T., M.T Objek : Pertanyaan yang terdapat pada intrumen indeks KAMI untuk sistem elektronik, area tata kelola; risiko keamanan informasi; kerangka kerja; pengelolaan aset; teknologi; suplemen (pengamanan layanan infrastruktur awan (*cloud service*)) Tujuan : Mengetahui kondisi pengamanan informasi untuk area tata kelola; risiko keamanan informasi; kerangka kerja; pengelolaan aset; teknologi; suplemen (pengamanan layanan infrastruktur awan (*cloud service*)) Hasil : Status dan skor tiap pertanyaan yang terdapat pada instrument indeks KAMI untuk area tata kelola; risiko keamanan informasi; kerangka kerja; pengelolaan aset; teknologi; suplemen (pengamanan layanan infrastruktur awan (*cloud service*))
Wawancara narasumber 2	Dilakukan pada tanggal : 16 Januari 2024 Lokasi : UPA TIK Undiksha Narasumber : Ir. I Made Dendi Masanjaya, S.Pd., M.Eng Objek : Pertanyaan yang terdapat pada intrumen indeks KAMI untuk area tata kelola, area pengelolaan aset dan suplemen (perlindungan data pribadi) Tujuan : Mengetahui kondisi pengamanan informasi untuk area tata kelola, area pengelolaan aset dan suplemen (perlindungan data pribadi)

	Hasil : Status dan skor tiap pertanyaan yang terdapat pada instrument indeks KAMI untuk area tata kelola, area pengelolaan aset dan suplemen (perlindungan data pribadi)
Wawancara narasumber 3	Dilakukan pada tanggal : 9 November 2023 dan 15 November 2023 Lokasi : UPA TIK Undiksha Narasumber : Ir. I Made Ardwi Pradnyana, S.T., M.T Objek : Pertanyaan yang terdapat pada intrumen indeks KAMI untuk area pengelolaan aset informasi dan suplemen (layanan) serta dokumen bukti/prosedur Tujuan : Mengetahui kondisi pengamanan informasi untuk area pengelolaan aset informasi dan suplemen (layanan) serta meminta dokumen bukti/prosedur Hasil : Status dan skor tiap pertanyaan yang terdapat pada instrument indeks KAMI untuk area pengelolaan aset informasi dan suplemen (layanan) serta dokumen bukti/prosedur
Wawancara narasumber 4	Dilakukan pada tanggal : 16 Januari 2024 Lokasi : UPA TIK Undiksha Narasumber : Ida Komang Widhiarjaya, S.T., M.Pd. Objek : Pertanyaan yang terdapat pada intrumen indeks KAMI untuk sistem elektronik, suplemen, dan kerjasama dengan pihak ketiga Tujuan : Mengetahui tingkat kepentingan penggunaan sistem elektronik di Undiksha, kondisi pengamanan informasi untuk suplemen dan kerjasama dengan pihak ketiga Hasil : Tingkat kepentingan penggunaan sistem elektronik di Undiksha, status dan skor tiap pertanyaan yang terdapat pada instrument indeks KAMI untuk suplemen dan tidak ada kerjasama dengan pihak ketiga terkait dengan keamanan informasi

Wawancara narasumber 5	Dilakukan pada tanggal : 1 Februari 2024 Lokasi : UPA TIK Undiksha Narasumber : I Nyoman Yoga Satyawan, S.ST., M.Kom Objek : Pertanyaan yang terdapat pada intrumen indeks KAMI untuk area kerangka kerja dan area pengelolaan aset Tujuan : Mengetahui kondisi pengamanan informasi untuk area kerangka kerja dan area pengelolaan aset Hasil : Status dan skor tiap pertanyaan yang terdapat pada instrument indeks KAMI untuk area kerangka kerja dan area pengelolaan aset yang mencakup pengembangan sistem dan uji cobanya

- Dokumentasi

Aktivitas	Keterangan
Dokumentasi hasil wawancara	Dilakukan pada tanggal : 6 Mei 2024 Waktu : 11:45 WITA Media : Melalui media foto Objek : Dokumen dan bukti yang mendukung hasil wawancara Tujuan : Melakukan validasi ketersediaan dokumen
Dokumentasi hasil wawancara	Dilakukan pada tanggal : 29 Mei 2024 Waktu : 10:00 WITA Media : Melalui media Google drive dengan format file word Objek : Dokumen yang mendukung hasil wawancara Tujuan : Melakukan validasi ketersediaan dokumen.

5. **Periode Pengumpulan Data** : Pengumpulan data dilakukan selama penelitian dilakukan.

Demikian berita acara verifikasi, validasi data, dan rekomendasi ini dibuat untuk dapat digunakan sebagaimana mestinya.

REKOMENDASI PENELITIAN

Form Validasi dan verifikasi Hasil Rekomendasi Pengukuran Tingkat Kematangan Keamanan Informasi UPA TIK Universitas Pendidikan Ganesha Menggunakan Indeks KAMI Berbasis ISO/IEC 27001:2013

Verifikasi Hasil Analisis Indeks KAMI

Petanyaan	Pernyataan
1. Apakah bapak/ibu setuju dengan hasil analisis Indeks KAMI yang dilakukan terkait keamanan infromasi di UPA TIK?	☑ Iya ☐ Tidak
2. Jika tidak setuju, bagian mana dari analisis yang perlu diperbaiki atau diperjelas?	
3. Apakah analisis Indeks KAMI masih relevan dengan kondisi di UPA TIK saat ini ?	☑ Iya ☐ Tidak
4. Jika tidak, bagian mana yang tidak relevan atau perlu diperbaiki?	

Verifikasi Penyusunan Rekomendasi

Pertanyaan	Pernyataan
1. Apakah rekomendasi yang disusun sudah sesuai dengan kebutuhan di UPA TIK ?	☑ Iya ☐ Tidak

2. Jika tidak, bagian mana yang perlu disesuaikan? —	
3. Apakah rekomendasi ini sudah mencakup perbaikan yang dapat dilakukan oleh UPA TIK dalam upaya meningkatkan kesiapan kamanan informasi dan kematangannya ?	☑ Iya ☐ Tidak
4. Jika tidak, apa yang perlu ditambah? —	
5. Apakah hasil rekomendasi ini mudah dipahami dan bisa diterima untuk menunjang pengamanan informasi di UPA TIK ?	☐ Sangat Jelas ☑ Jelas ☐ Cukup Jelas ☐ Tidak Jelas
6. Sejauh mana rekomendasi ini sesuai dengan kebutuhan di UPA TIK Undiksha?	☐ Sangat Sesuai ☑ Sesuai ☐ Cukup Sesuai ☐ Tidak Sesuai
7. Apakah rekomendasi ini sudah mencakup pengelolaan keamanan infromasi yang baik di UPA TIK Undiksha?	☑ Iya ☐ Tidak ☐ Perlu Penyesuaian

Mengetahui,

Daftar Hadir

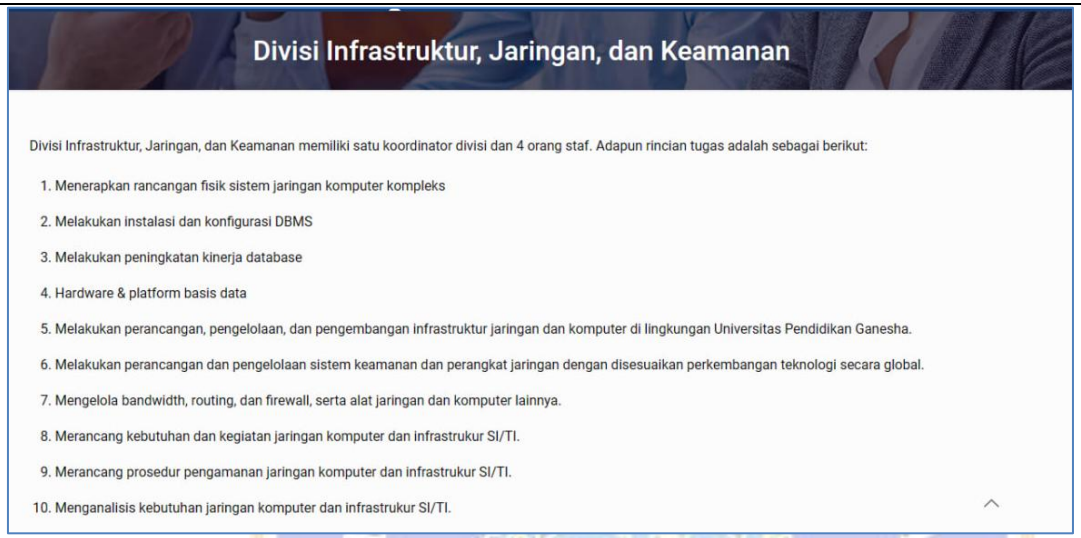
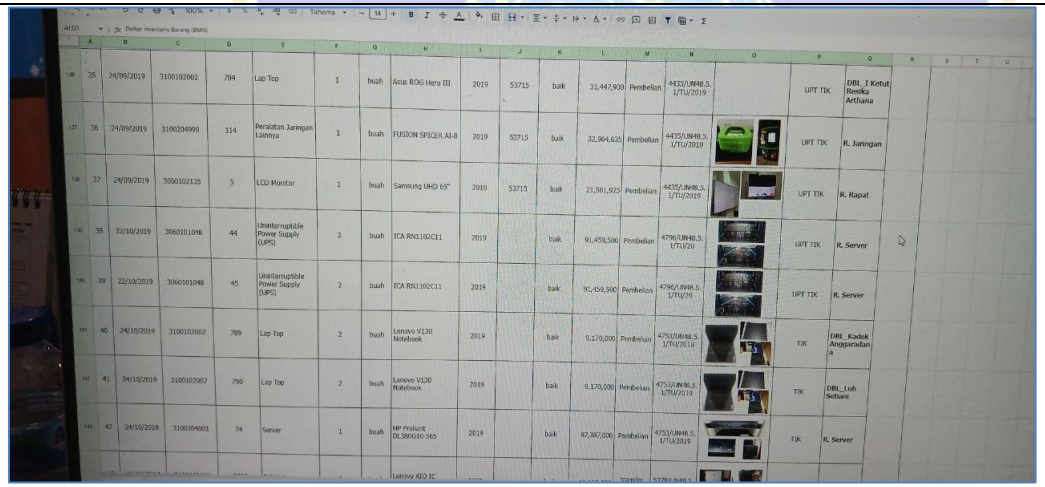
No	Nama	Ttd
1.	I Ketut Resika Arthana, S.T., M.Kom	
2.	I Made Ardwi Pradnyana.	
3.		
4.		
5.		
6.		

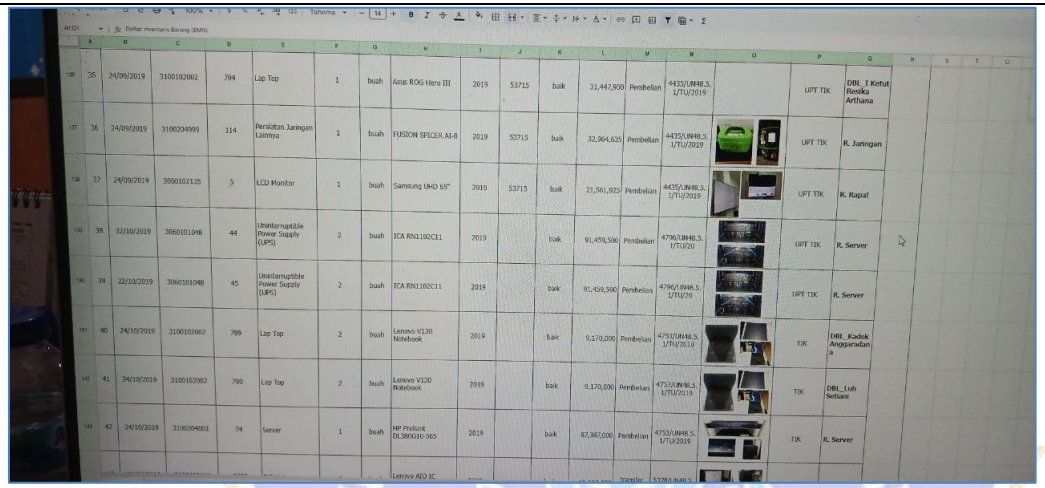
Peneliti

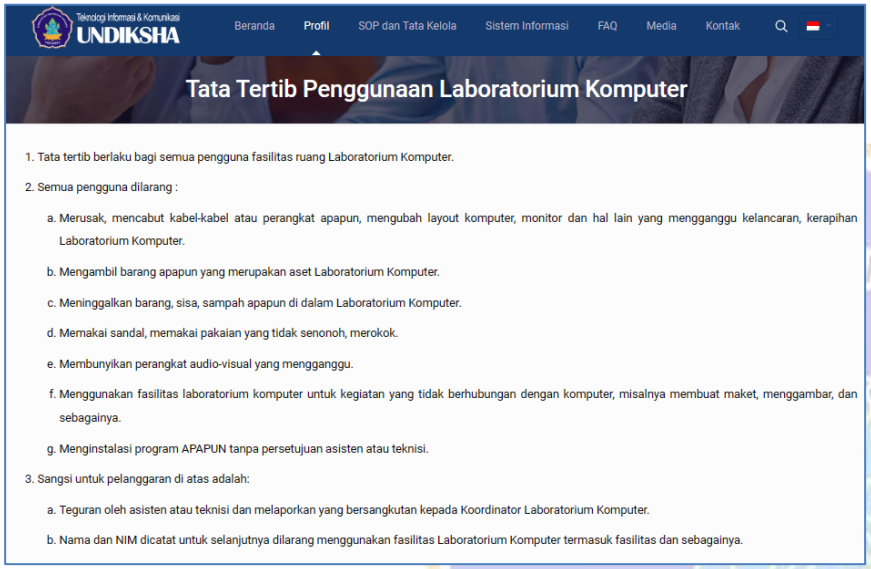
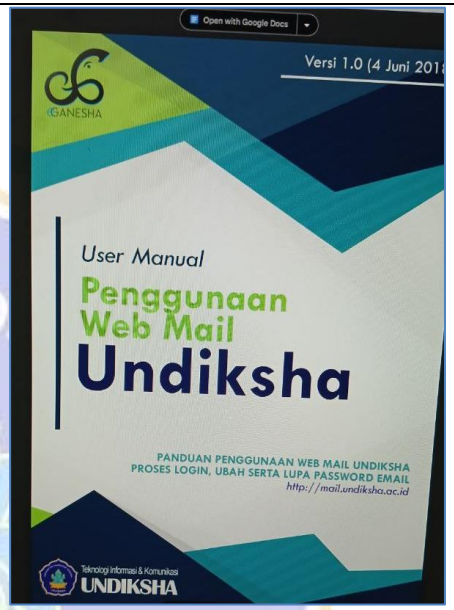
Putu Risma Widharini

Lampiran 12. Bukti Dokumen Indeks KAMI

No. Pertanyaan di Indeks KAMI	Bukti	Keterangan
2.2		Struktur Organisasi

2.3		Tupoksi
3.6		Dokumen aset informasi

5.1		Dokumen daftar inventaris aset informasi

5.9			Dokumen tata tertib penggunaan komputer, email, internet dan intranet

5.14	GANESHA **UNIT PELAKSANA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI**	**JUDUL IK**	NIP 198412012012121002 Manajemen Akun Single Sign On (SSO)

INSTRUKSI KERJA (IK)

TUJUAN DAN RUANG LINGKUP
Tujuan dibuatnya instruksi kerja ini adalah memberikan gambaran tentang apa saja yang wajib diketahui dan dilakukan oleh Staff Divisi Pusat Data dan Informasi untuk melakukan manajemen Akun Single Sign On (SSO). Instruksi kerja ini mencakup langkah-langkah mulai dari mendapatkan permintaan Akun SSO sampai pada proses pembuatan (*create*), pembaharuan (*update*), dan penghapusan (*delete*) akun SSO selesai.

ACUAN/ REFERENSI
-

DEFINISI/ ISTILAH/ SINGKATAN
-

SISTEM, PERALATAN dan DOKUMEN
Peralatan yang digunakan Staff Divisi Pusat Data dan Informasi dalam melaksanakan instruksi kerja ini adalah perangkat komputer, koneksi internet dan beberapa aplikasi pendukung untuk melakukan untuk Manajemen Akun SSO (*Create, Update, Delete*).

PELAKSANA/ PENANGGUNG JAWAB
Staff Divisi Pusat Data dan Informasi

Dokumen persyaratan dan prosedur pengelolaan/ pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi

	UNIT PELAKSANA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI	JUDUL IK	Layanan Data dan Informasi

INSTRUKSI KERJA (IK)

TUJUAN DAN RUANG LINGKUP
Tujuan dibuatnya instruksi kerja ini adalah memberikan gambaran tentang apa saja yang wajib diketahui dan dilakukan oleh Staff Divisi Pusat Data dan Informasi dalam memberikan layanan kebutuhan data dan informasi.

ACUAN/ REFERENSI
-

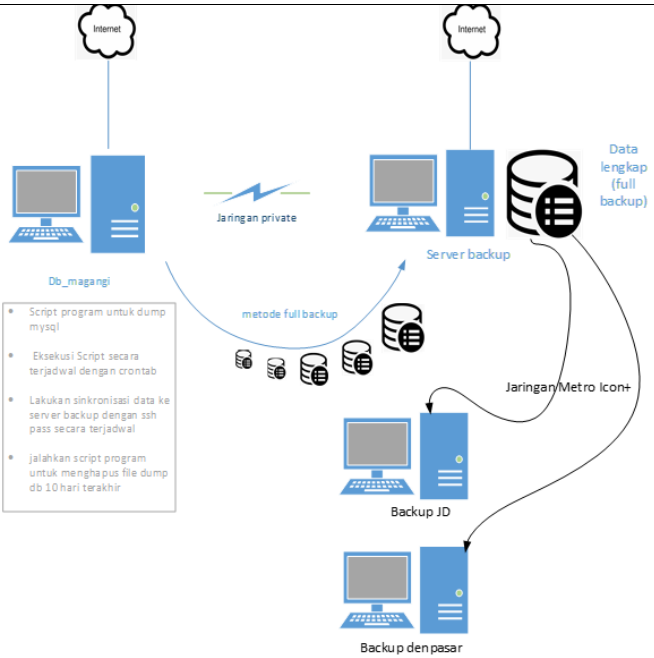
DEFINISI/ ISTILAH/ SINGKATAN
-

SISTEM, PERALATAN dan DOKUMEN
Peralatan yang digunakan Staff Divisi Pusat Data dan Informasi dalam melaksanakan instruksi kerja ini adalah perangkat komputer atau laptop, koneksi internet dan beberapa aplikasi pendukung untuk melakukan akses data.

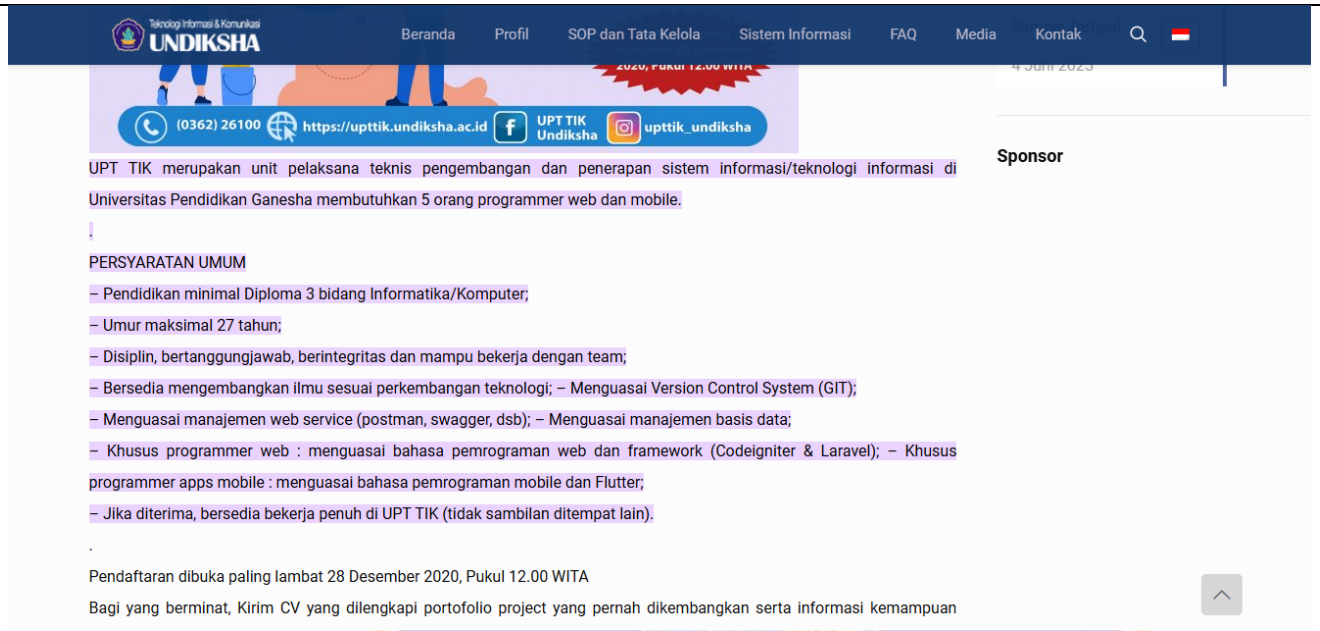
PELAKSANA/ PENANGGUNG JAWAB
Staff Divisi Pusat Data dan Informasi

KUALIFIKASI
a. Mampu melakukan analisis data yang diperlukan ke sistem sumber.
b. Mampu mengimplementasikan database dalam manajemen sistem.

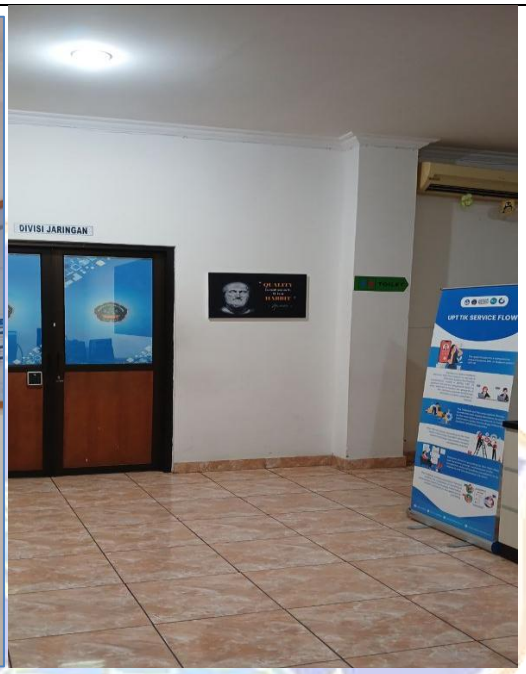
5.15	GANESHA **UNIT PELAKSANA TEKNIS TEKNOLOGI INFORMASI DAN KOMUNIKASI** **JUDUL IK**: Manajemen Akun Single Sign On (SSO) NIP 198412012012121002 **INSTRUKSI KERJA (IK)** **TUJUAN DAN RUANG LINGKUP** Tujuan dibuatnya instruksi kerja ini adalah memberikan gambaran tentang apa saja yang wajib diketahui dan dilakukan oleh Staff Divisi Pusat Data dan Informasi untuk melakukan manajemen Akun Single Sign On (SSO). Instruksi kerja ini mencakup langkah-langkah mulai dari mendapatkan permintaan Akun SSO sampai pada proses pembuatan (*create*), pembaharuan (*update*), dan penghapusan (*delete*) akun SSO selesai. **ACUAN/ REFERENSI** - **DEFINISI/ ISTILAH/ SINGKATAN** - **SISTEM, PERALATAN dan DOKUMEN** Peralatan yang digunakan Staff Divisi Pusat Data dan Informasi dalam melaksanakan instruksi kerja ini adalah perangkat komputer, koneksi internet dan beberapa aplikasi pendukung untuk melakukan untuk Manajemen Akun SSO (*Create, Update, Delete*). **PELAKSANA/ PENANGGUNG JAWAB** Staff Divisi Pusat Data dan Informasi	Dokumen atau ketentuan pengelolaan data yang disimpan dan dihapus

5.18		Dokumen prosedur back-up dan uji coba pengembalian data (restore), screen capture backup data

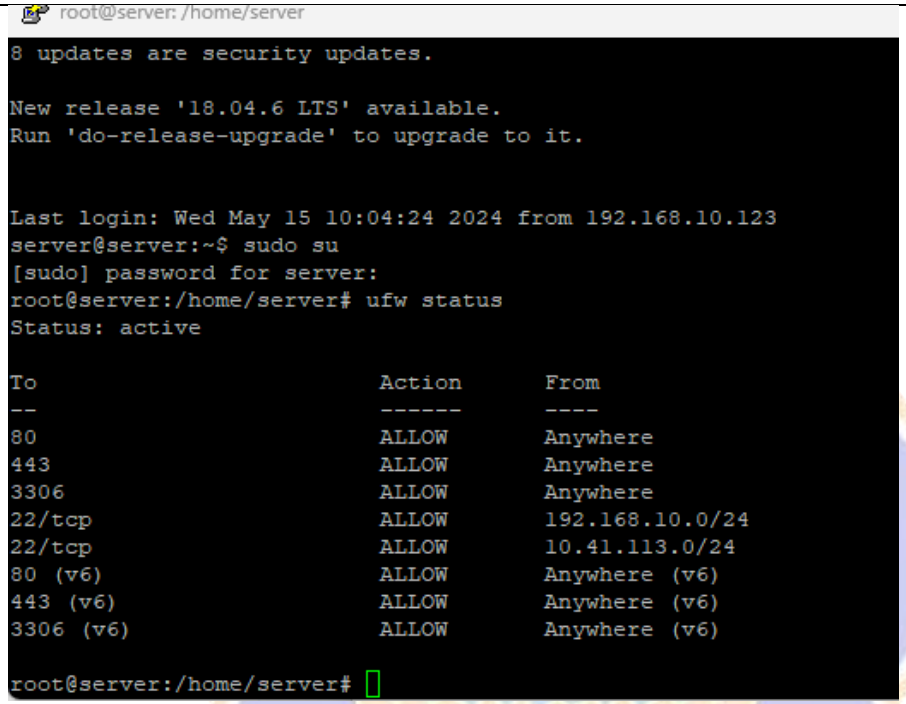
	Backup Data 1. Buat script untuk melakukan dumping data dengan perintah sql dan disimpan dalam bentuk file *.sh 2. Lakukan atau jalankan peritah sql tersebut secara terjadwal dengan crontab yang sudah tersedia di sistem operasi ubuntu server 3. Buat script untuk menghapus file hasil dumping sql 30 hari terakhir (hal ini dilakukan untuk antisipasi penuhnya server db_magang) 4. Lakukan atau jalankan perintah untuk hapus file backup 30 hari terakhir secara terjadwal pada crontab. 5. Buat script untuk sinkronisasi data-data yang akan dibackup dari server db_sistensi ke server tujuan dengan sshpass atau aplikasi sejenis 6. Jalankan script sinkronisasi secara terjadwal dengan crontab. 7. File hasil sinkronisasi akan tersimpan pada server backup dengan tambahan nama sesuai tanggal backup. 8. Untuk melakukan restore data, kita dapat mengcopy file-file yang ada di server backup dengan komunikasi port 22 SSH. 9. Setelah file-file dicopy kita dapat melakukan pengembalian data sesuai data yang kita inginkan. Penentuan waktu dan periode backup dan pemulihan data. Waktu untuk backup data kita lakukan setiap hari dari senin sampai jumat pada pukul 24.00 Wita. Untuk waktu pemulihan data dapat kita lakukan jika terjadi kehilangan data atau kesalahan prosedur dari pengguna sistem.	

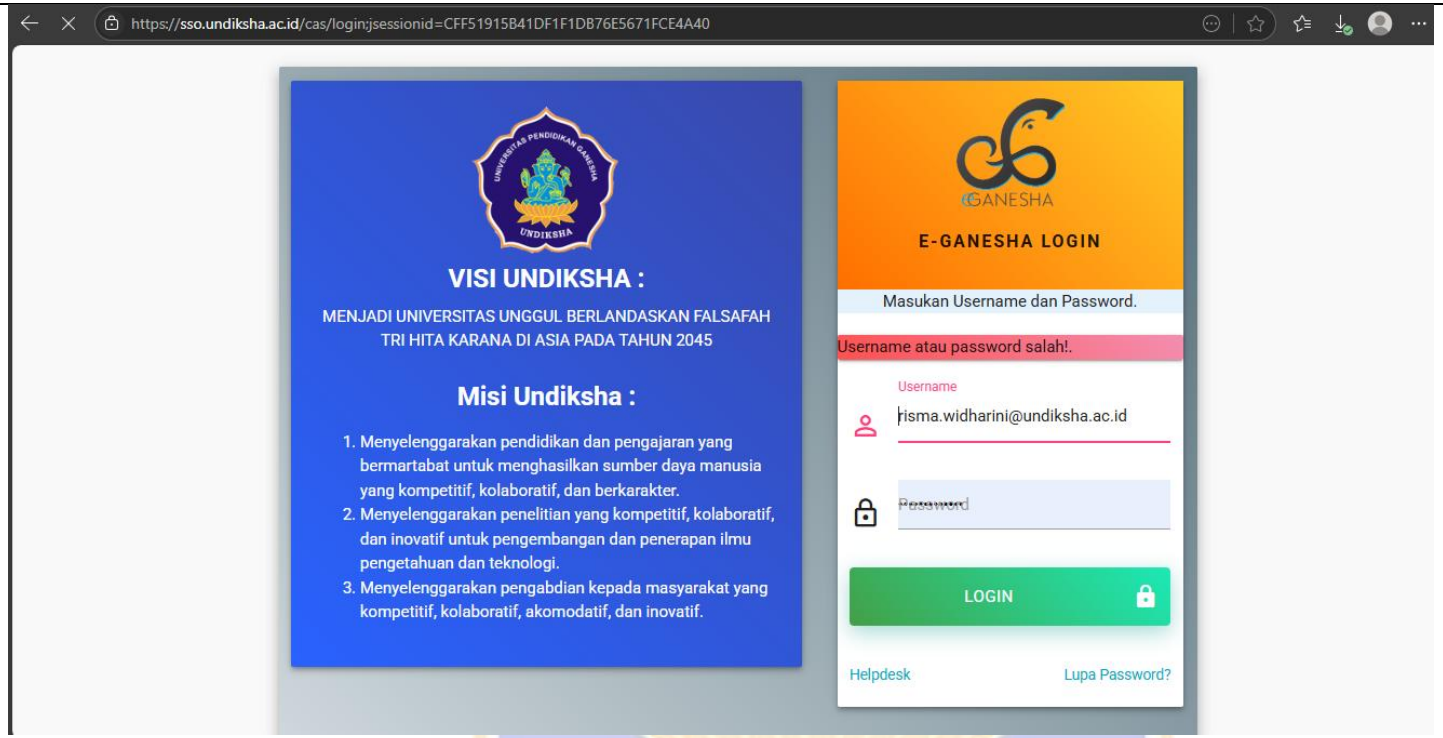
5.20		Kebijakan pengecekan latar belakang SDM petugas UPA TIK

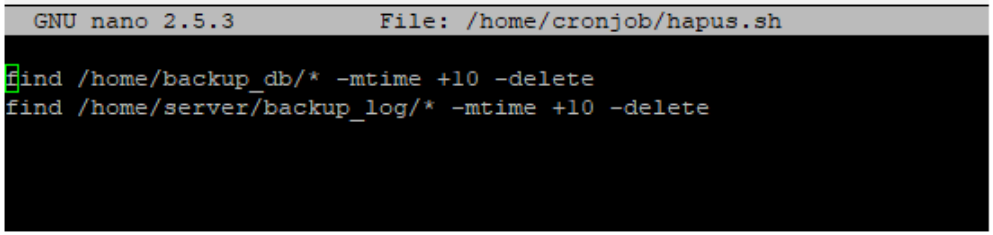
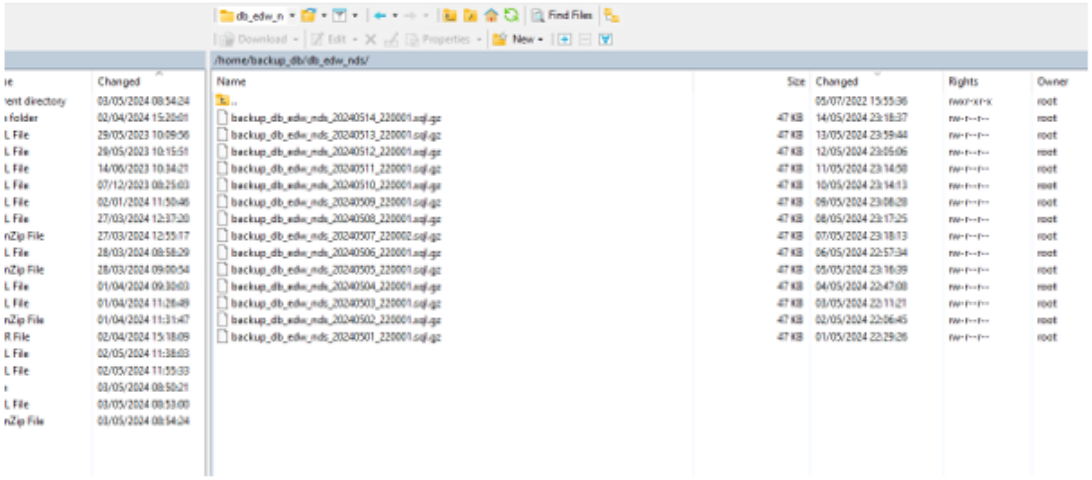
5.29		Bukti foto pengamanan kunci masuk (fisik dan elektronik) ke fasilitas fisik

5.30	 	Bukti pengelolaan infrastruktur TI, Foto infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban

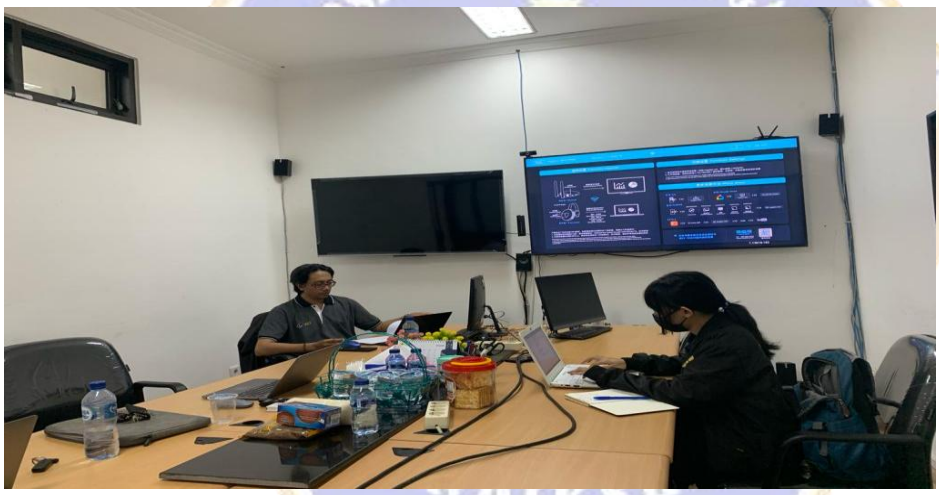
5.31		Bukti pengelolaan infrastruktur TI, infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir

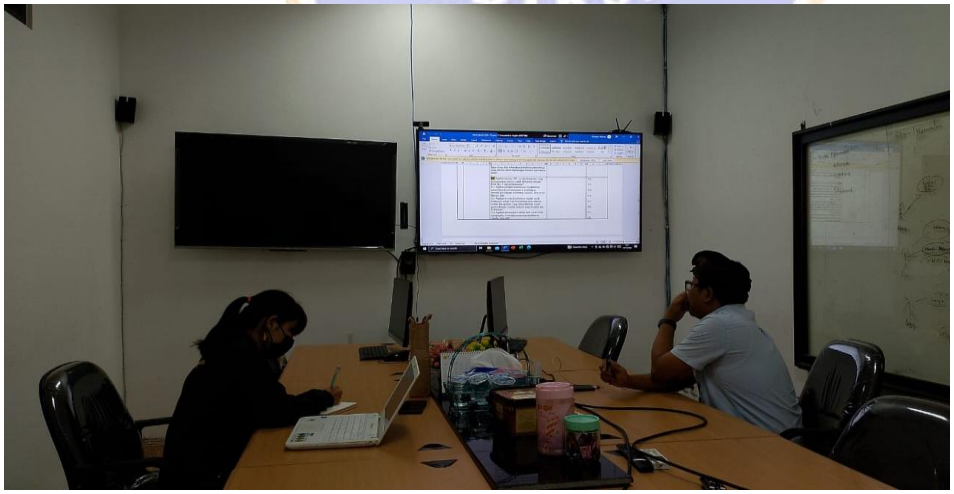
6.1			Screen capture penggunaan firewall

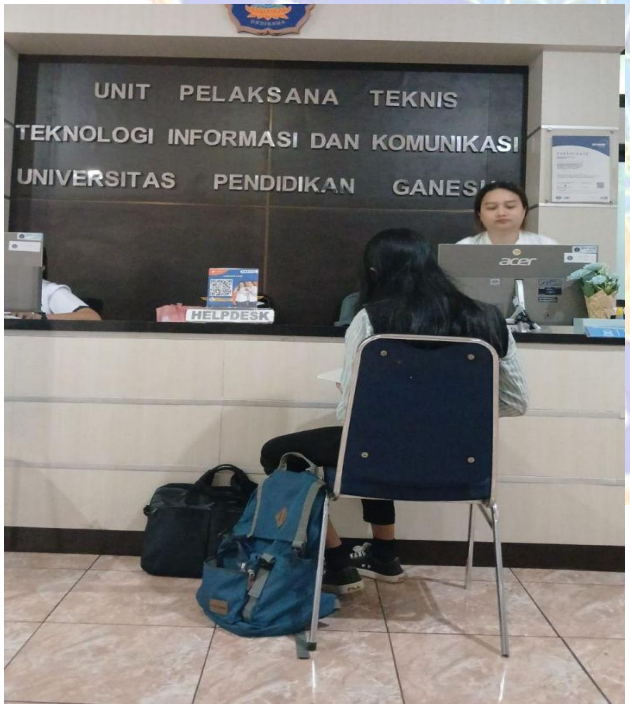
6.16		Screen capture pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses pada sistem

7.3.15	 	Screen capture penghapusan data

Lampiran 13. Dokumentasi






UNIT PELAKSANA TEKNIS
TEKNOLOGI INFORMASI DAN KOMUNIKASI
UNIVERSITAS PENDIDIKAN
HELPDESK
acer

Lampiran 14. Riwayat Hidup

RIWAYAT HIDUP

Putu Risma Widharini adalah nama Penulis Skripsi ini. Penulis merupakan anak pertama dari kedua orang tuanya. Penulis lahir di Singaraja, 01 November 2000. Penulis menempuh pendidikan dasar di SD Negeri 1 Banjar Jawa dan lulus pada tahun 2012. Pendidikan selanjutnya dilanjutkan di SMP Negeri 1 Singaraja dan diselesaikan pada tahun 2015. Penulis lulus dari SMA Negeri 4 Singaraja pada tahun 2018, kemudian melanjutkan studi ke jenjang S1 pada Program Studi Sistem Informasi, Jurusan Teknik Informatika di Universitas Pendidikan Ganesha.