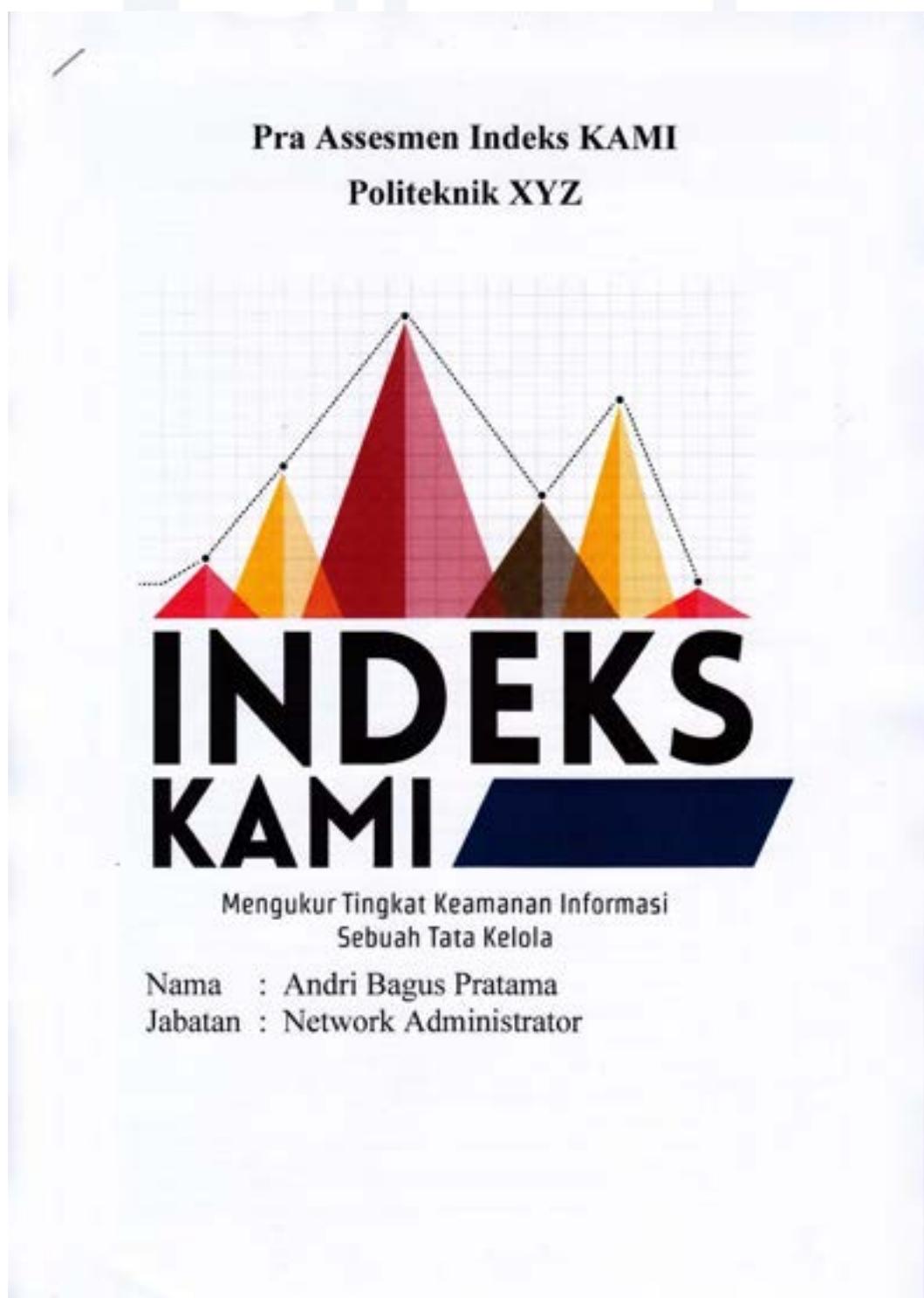


Lampiran

1. Network Administrator Pra Instalasi Asesmen



Babak II: Kategori Sistem Elektronik				
Babak I: Integrasi dan Implementasi Sistem Elektronik yang Efektif				
[Kategori Sistem Elektronik] Standar Tingkat Strategis				
	Karakteristik Internasionalisasi	Status		
	A	B	C	
1.1	Nilai investasi sistem elektronik yang tepatang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar sd Rp.30 Miliar [C] Kurang dari Rp.3 Miliar			✓
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar sd Rp.10 Miliar [C] Kurang dari Rp.1 Miliar			✓
1.3	Mempunyai kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus		✓	
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi		✓	
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna		✓	
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	✓		
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman spesies penyerangan atau penyebarluasan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa		✓	
1.8	Tingkat korelikasi proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman spesies penyerangan atau penyebarluasan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berisiko pada bisnis perusahaan	✓		
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berkala nasional atau memihayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih			✓
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Mengimbasikan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)		✓	

Bagian II: Tata Kelola Keamanan dan Tergantung				
Bogor, Jawa Barat, 10 September 2019 Dalam rangka evaluasi kelayakan berikutnya untuk kerjasama antara Dinas Kepolisian Perairan dan Uang, Bogor dan Daerah Istimewa Tangerang Selatan				
Penilaian: Tidak Dilakukan (A), Dulu Perencanaan (B), Didalam Perencanaan (C), Diketahui Seoarai Merujuk (D)		Skor		
Fungsi/Organisasi Keamanan Informasi		A	B	C
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?				✓
2.2 Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab 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?				✓
2.4 Apakah perangkingan/tanggungjawab pelaksana pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan meningkatkan kepatuhan program keamanan informasi?				✓
2.5 Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan suatu interval dan persyaratan segerangsi kewajibannya?				✓
2.6 Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan kualitas pelaksana pengelolaan keamanan informasi?				✓
2.7 Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan kualitas yang memadai sesuai persyaratan/standar yang berlaku?				✓
2.8 Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?				✓
2.9 Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan kualitas untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?				✓
2.10 Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?		✓		
2.11 Apakah instansi/pemahaman anda sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?				✓
2.12 Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkaitan, untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang membutuhkan informasi penting) dan menyelesaikan permasalahan yang ada?				✓
2.13 Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan sektor terkait (SDM, Legal/Hukum, Umum, Keuangan dkk) dan pihak eksternal yang berkaitan (misal: regulator, aparat keamanan) untuk menerapkan dan meningkatkan 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 plan) sudah didefinisikan dan diajukan?		✓		
2.15 Apakah tanggungjawab pengelolaan keamanan informasi mempertimbangkan kondisi, kinerja/efektifitas dan kepuasan pengguna keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?				✓
2.16 Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsideran atau bahan dari proses pengambilan keputusan strategis di instansi/perusahaan anda?		✓		
2.17 Apakah pimpinan suatu kerja di instansi/perusahaan anda menerapkan program khusus untuk memenuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?				✓
2.18 Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporan?				✓
2.19 Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaannya?				✓
2.20 Apakah instansi/perusahaan anda sudah memerlukan 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?		✓		
2.21 Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, peraturan hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan mengalihkan tingkat kepatuhannya?				✓
2.22 Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah tanggungjawab melindungi keamanan informasi yang menyajikan pelanggaran hukum (pidana dan perdata)?				✓

8

Bagian III: Pengelolaan Risiko Keamanan Informasi				
Batasan informasi kerja pengelolaan risiko keamanan informasi terhadap daerah penggunaan strategi kerahaman informasi				Status
[Penilaian]: Tidak Dilakukan (A); Dalam Perencanaan (B); Dalam Penerapan atau Diterapkan Setengah (C); Diterapkan Secara Matang/tuntas (D)				
Kajian Risiko Keamanan Informasi				A B C D
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?			✓
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓
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?			✓
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko 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?			✓
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?			✓
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang 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)?			✓
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?			✓
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?			✓
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?			✓
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?			✓
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memantau akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?			✓
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?			✓
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan?			✓

8

Bab IV: Kesiagaan Kejayaan Pengelolaan Keamanan Informasi		Status
Pertanyaan	Jawaban	
Penyelesaian dasar Pengelolaan Kejayaan & Prosedur Keamanan Informasi		
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?	✓
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?	✓
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan 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?	✓
4.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	✓
4.6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	✓
4.7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata terib penggunaan dan pengamanan asset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	✓
4.8	Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	✓
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk merindak lanjuti konsekuensi dari kondisi ini?	✓
4.10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya nilai security patch baru, memastikan pemasangannya dan melaporkannya?	✓
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	✓
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	✓
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?	✓
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?	✓

8

4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	<input checked="" type="checkbox"/>		
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	<input checked="" type="checkbox"/>		
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?	<input checked="" type="checkbox"/>		
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	<input checked="" type="checkbox"/>		
Evaluasi Strategi dan Program Keamanan Informasi		A	B	C D
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?		<input checked="" type="checkbox"/>	
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirananya disesuaikan dengan kebutuhan dan perubahan profil risiko?	<input checked="" type="checkbox"/>		
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	<input checked="" type="checkbox"/>		
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)?	<input checked="" type="checkbox"/>		
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	<input checked="" type="checkbox"/>		
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pemberahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>		
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>		
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?	<input checked="" type="checkbox"/>		
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 yang diperlukan, telah diterapkan secara efektif?	<input checked="" type="checkbox"/>		
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	<input checked="" type="checkbox"/>		

Bab V: Pengelolaan Aset Informasi				
	Penilaian: Tidak Dilakukan (A); Dalam Persepsi (B); Dalam Penerapan atau Dilakukan Seperti (C); Dilakukan Secara Mengintimidasi (D)			
	Pengelolaan Aset Informasi			
	A	B	C	D
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)			✓
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?			✓
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?		✓	
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut		✓	
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?		✓	
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?		✓	
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkannya inventaris aset informasi?		✓	
5.8	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?			
5.9	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda		✓	
5.10	Tata tertib penggunaan komputer, email, internet dan intranet		✓	
5.11	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI		✓	
5.12	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan		✓	
5.13	Pengelolaan identitas elektronik dan proses otentifikasi (<i>username & password</i>) termasuk kebijakan terhadap pelanggarannya		✓	
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentifikasi dan otorisasi untuk menggunakan aset informasi		✓	
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data		✓	
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya		✓	
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi		✓	
5.18	Prosedur <i>back-up</i> dan uji coba pengembalian data (<i>restore</i>) secara berkala		✓	
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya		✓	
5.20	Proses pengecekan latar belakang SDM		✓	
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.		✓	
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan		✓	
5.23	Prosedur kajian penggunaan akses (<i>user access review</i>) dan hak aksesnya (<i>user access rights</i>) berikut langkah pemberhanan apabila terjadi ketidaksesuaian (<i>non-conformity</i>) terhadap kebijakan yang berlaku		✓	

L

5.24	Prosedur untuk aset yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.			✓
5.25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?			✓
5.26	Apakah tersedia daftar rekanan pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?			✓
5.27	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?			✓
	Pengamanan Fisik	A	B	C
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?			✓
5.29	Apakah tersedia proses untuk mengelola akses kunci masuk (fisik dan elektronik) ke fasilitas fisik?			✓
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelenjaran yang sesuai dengan prasyarat pabrikannya?			✓
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?			✓
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?			✓
5.33	Apakah tersedia proses untuk memindahkan aset TIK (peranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?			✓
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendekung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?			✓
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?			✓
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?			✓
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 telp gerggam di dalam ruang server, menggunakan kamera dll)			✓
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?			✓

Babagan VI: Teknologi dan Keamanan Informasi					
Babagan VI: Keamanan Informasi				Status	
	[Pembalas] Tidak Dilakukan (A); Diketahui Perluas atau Ditingkatkan (B); Diumpan (C); Sama/Menyekuhkan (D)	A	B	C	
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	✓			
6.2	Apakah jaringan komunikasi disegmenasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?			✓	
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan asset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?			✓	
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?			✓	
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelelahan atau perubahan/keutuhan konfigurasi?	✓			
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?			✓	
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?		✓		
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terakam di dalam log?			✓	
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terakam di dalam log?	✓			
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	✓			
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi asset informasi penting sesuai kebijakan pengelolaan yang ada?			✓	
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?			✓	
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?			✓	
6.14	Apakah semua sistem dan aplikasi secara otomatis mendekripsi dan menerapkan penggantian password secara otomatis, termasuk menonaktifkan password, 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?			✓	
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses?			✓	
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	✓			
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	✓			
6.19	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?			✓	

S

6.20	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	✓		
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	✓		
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	✓		
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?			✓
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	✓		
6.25	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yg dibangun?			✓
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	✓		

Bab VII: Sajaman			
Bab VII: Sajaman		Status	
	Persilakan [Tidak Diketahui] (A), Dalam Proses (B), Dalam Penyelesaian (C) atau Selesai (Mengakhiri) (D)	A	B
7.1 Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan			
7.1.1 Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga		A B C D	
7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	✓		
7.1.1.2 Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	✓		
7.1.1.3 Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	✓		
7.1.1.4 Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	✓		
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?	✓		
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?	✓		
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? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	✓		
7.1.2 Pengelolaan Layanan dan Keamanan Pihak Ketiga			
7.1.2.1 Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	✓		
7.1.2.2 Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	✓		
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?	✓		
7.1.3 Pengelolaan Layanan dan Keamanan Pihak Ketiga			
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 asset informasi dan infrastruktur milik instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	✓		
7.1.3.2 Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	✓		
7.1.3.3 Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?		✓	
7.1.3.4 Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?		✓	

7.1.3.3	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuanya kepada instansi/perusahaan?	<input checked="" type="checkbox"/>
7.1.3.4	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	<input checked="" type="checkbox"/>
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	<input checked="" type="checkbox"/>
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	<input checked="" type="checkbox"/>
Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga		
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?	<input checked="" type="checkbox"/>
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	<input checked="" type="checkbox"/>
Pengelolaan Aset		
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?	<input checked="" type="checkbox"/>
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	<input checked="" type="checkbox"/>
Pengelolaan Insiden oleh Pihak Ketiga		
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, pengamanan, dan analisis insiden keamanan informasi?	<input checked="" type="checkbox"/>
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	<input checked="" type="checkbox"/>
Rencana Kelangsungan Layanan Pihak Ketiga		
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	<input checked="" type="checkbox"/>
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	<input checked="" type="checkbox"/>
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	<input checked="" type="checkbox"/>
Pengamanan Layanan Infrastruktur Awan (Cloud Service)		
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	<input checked="" type="checkbox"/>
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	<input checked="" type="checkbox"/>
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?	<input checked="" type="checkbox"/>
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	<input checked="" type="checkbox"/>
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	<input checked="" type="checkbox"/>

8

7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	<input checked="" type="checkbox"/>	
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	<input checked="" type="checkbox"/>	
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?	<input checked="" type="checkbox"/>	
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	<input checked="" type="checkbox"/>	
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	<input checked="" type="checkbox"/>	
Perlindungan Data Pribadi			
7.3			
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?		<input checked="" type="checkbox"/>
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?		<input checked="" type="checkbox"/>
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?		<input checked="" type="checkbox"/>
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?		<input checked="" type="checkbox"/>
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (<i>Data Protection Officer</i> , <i>Data Controller</i> , <i>Data Processor</i>) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?		<input checked="" type="checkbox"/>
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?		<input checked="" type="checkbox"/>
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?		<input checked="" type="checkbox"/>
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?		<input checked="" type="checkbox"/>
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?		<input checked="" type="checkbox"/>
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 menyimpulkan persetujuan tersebut?		<input checked="" type="checkbox"/>
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?		<input checked="" type="checkbox"/>
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?		<input checked="" type="checkbox"/>
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termatahkan?		<input checked="" type="checkbox"/>

8

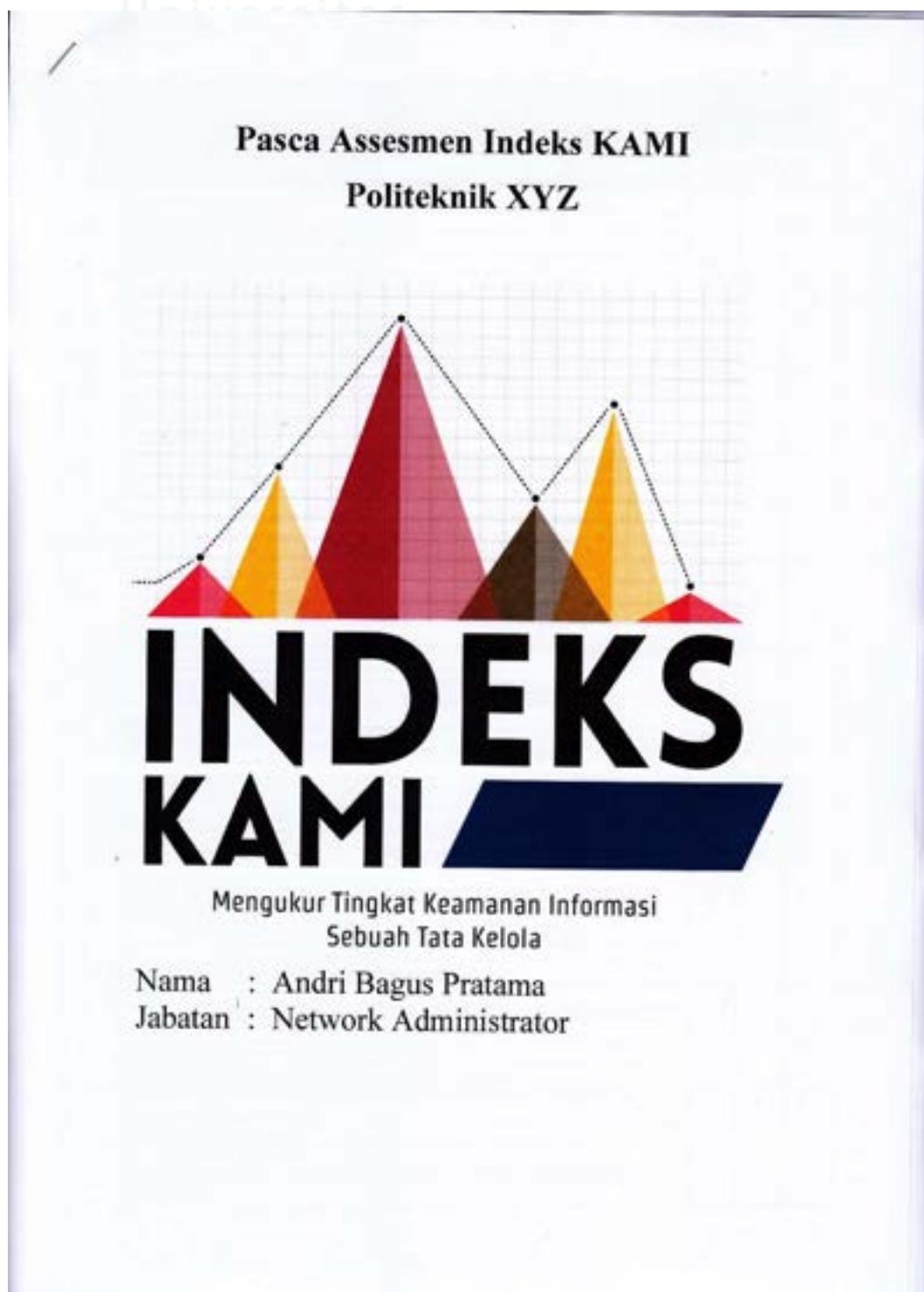
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahan sesuai dengan peraturan atau perjanjian dengan pemilik data?	<input checked="" type="checkbox"/>		
7.3.15	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atas dasar permintaan pemilik data dan menyimpan catatan proses tersebut?		<input checked="" type="checkbox"/>	
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?			<input checked="" type="checkbox"/>

Tanggal 1/8/2022


Andri Bagus Pratama

8

2. Network Administrator Pasca Instalasi Asesmen



#	Karakteristik Sistem Elektronik	Status		
		A	B	C
1.1	Misi investasi sistem elektronik yang terpenuhi [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar			✓
1.2	Total anggaran operasional tahunan yang disediakan untuk pengembangan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar			✓
1.3	Memiliki kewajiban kewajiban terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus		✓	
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi		✓	
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna		✓	
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan keperluan badan usaha [C] Tidak ada data pribadi	✓		
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyiraman atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa		✓	
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyiraman atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	✓		
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersebarluas layanan publik berbasis nasional atau membebaskan pertahanan keamanan negara [B] Tidak tersebarluas layanan publik dalam 1 propinsi atau lebih [C] Tidak tersebarluas layanan publik dalam 1 kabupaten/kota atau lebih			✓
1.10	Potensi kerugian atau dampak negatif dari insiden dilaluiannya keamanan informasi Sistem Elektronik (substansi, terorisme) [A] Mengakibatkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)		✓	

Bab II. TINJAUAN KONSEP DAN REFERENSI		Status
[Prestasi] Tidak Dilakukan (A); Dalam Perbaikan (B); Dalam Penyatuan dan Diterapkan Setiap Hari (C); Diterapkan Secara Sistematis (D)	Fungsi/Organisasi Keamanan Informasi	
	A B C D	
2.1 Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (instal yang termasuk dalam ITSP), termasuk penetapan kebijakan terkait?		
2.2 Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga keparahamannya?	✓	
2.3 Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjalankan kebijakan program keamanan informasi?	✓	
2.4 Apakah pesanggarjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjalin keteralihan program keamanan informasi?	✓	
2.5 Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan diperlukan dengan lengkap, termasuk keterlibatan audit internal dan pemeriksaan sebagaimana keharusannya?	✓	
2.6 Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan kualitas pelaksana pengelolaan keamanan informasi?	✓	
2.7 Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan kualitas yang memadai sesuai persyaratan/standar yang berlaku?	✓	
2.8 Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk keperluan kreativitasnya bagi semua pihak yang terkait?	✓	
2.9 Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan kualitas untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	✓	
2.10 Apakah instansi/perusahaan anda sudah menerapkan integrasi keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	✓	
2.11 Apakah instansi/perusahaan anda sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundang-undang yang berlaku?	✓	
2.12 Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak luar yang berkepentingan, untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	✓	
2.13 Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, agensi keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	✓	
2.14 Apakah tanggungjawab untuk menyiapkan, menanggulangi, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plan) sudah difinisikan dan dialokasikan?	✓	
2.15 Apakah pesanggarjawab pengelolaan keamanan informasi meliputi kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	✓	
2.16 Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	✓	
2.17 Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk memastikan tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	✓	
2.18 Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup risiko/kemungkinan, waktu pengukuran, pelaksanaanya, permaianannya dan etiket pelaporannya?	✓	
2.19 Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaannya?	✓	
2.20 Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengelusuri perspektivanya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	✓	
2.21 Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan mengawasi tingkat kepatuhannya?	✓	
2.22 Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah peranggangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdamaian)?	✓	

8

Bagan III: Pengelolaan Risiko Keamanan Informasi					Status
Dalam hal mengidentifikasi kerusakan/pemecahan pengelolaan risiko keamanan informasi dalam pelaksanaan tugas dan tanggung jawab instansi/perusahaan					
	[Penilaian] Tidak Dilakukan (A); Dalam Perencanaan (B); Dalam Pelaksanaan/Dilengkapi (C); Dilengkapi Secara Mempadai (D)	A	B	C	D
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓	
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelapecehan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?			✓	
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓	
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?			✓	
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko 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?			✓	
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?			✓	
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/bergangguannya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang 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)?			✓	
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?			✓	
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?			✓	
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?			✓	
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?			✓	
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?			✓	
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?			✓	
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan?			✓	

Bagian IV: Kewajiban Kerja Pengelolaan Keamanan Informasi				
Babuan ini mengakali, kinerjakan dan kelembutan kerja kebijakan & prosedur pengelolaan keamanan informasi dan strategi peningkatannya				Status
[Pertama] Tidak Diketahui (A); Diketahui Perluas (B); Diketahui Implementasi atau Dilengkapi Sebagian (C); Dilengkapi Sosial Masyarakat (D)	A	B	C	
Persyaratan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi				
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?				✓
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?				✓
4.3 Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan 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?				✓
4.5 Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?				✓
4.6 Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?				✓
4.7 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?				✓
4.8 Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?				✓
4.9 Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi ini?				✓
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?				✓
4.11 Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?				✓
4.12 Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?				✓
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?				✓
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?				✓

4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	<input checked="" type="checkbox"/>	
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	<input checked="" type="checkbox"/>	
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	<input checked="" type="checkbox"/>	
4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pemberian yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	<input checked="" type="checkbox"/>	
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	<input checked="" type="checkbox"/>	
Pengelolaan Strategi dan Program Keamanan Informasi		A	B
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	<input checked="" type="checkbox"/>	
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirananya disesuaikan dengan kebutuhan dan perubahan profil risiko?	<input checked="" type="checkbox"/>	
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	<input checked="" type="checkbox"/>	
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)?	<input checked="" type="checkbox"/>	
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	<input checked="" type="checkbox"/>	
4.25	Apakah hasil audit internal tersebut diujicobakan/dievaluasi untuk mengidentifikasi langkah pemberian dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>	
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>	
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?	<input checked="" type="checkbox"/>	
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 pemberian yang diperlukan, telah diterapkan secara efektif?	<input checked="" type="checkbox"/>	
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	<input checked="" type="checkbox"/>	

8

Bab V: Pengelolaan Aset Informasi				
				Standar
	Pengelolaan Aset Informasi	A	B	C
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)			✓
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangannya yang berlaku?			✓
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	✓		
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut		✓	
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	✓		
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	✓		
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkannya inventaris aset informasi?		✓	
	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?			
5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda		✓	
5.9	Tata tertib penggunaan komputer, email, internet dan intranet		✓	
5.10	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI		✓	
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan		✓	
5.12	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi		✓	
5.13	Pengelolaan identitas elektronik dan proses otentikasi ('username & password') termasuk kebijakan terhadap pelanggarannya		✓	
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	✓		
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	✓		
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya		✓	
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi		✓	
5.18	Prosedur back-up dan uji coba pengembalian data ('restore') secara berkala	✓		
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya		✓	
5.20	Proses pengecekan latar belakang SDM		✓	
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.		✓	
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan		✓	
5.23	Prosedur kajian penggunaan akses ('user access review') dan hak aksesnya ('user access rights') berikut langkah pemberhan apabila terjadi ketidaksesuaian ('non-conformity') terhadap kebijakan yang berlaku			✓

8

5.24	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.				✓
5.25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?				✓
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamatan yang sesuai dengan klasifikasinya?				✓
5.27	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?				✓
Pengamanan Fisik					
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?				✓
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?				✓
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?				✓
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?				✓
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?				✓
5.33	Apakah tersedia proses untuk memindahkan aset TIK (peranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?				✓
5.34	Apakah kompleksi 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?				✓
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?				✓
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?				✓
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)				✓
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?				✓

8

Bab VI: Teknologi dan Keamanan Infrastruktur		Penilaian	Status		
#	Pengamatan Teknologi	A	B	C	D
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?			✓	
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?			✓	
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan asset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?			✓	
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?			✓	
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?			✓	
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?			✓	
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?			✓	
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis tercatat di dalam log?			✓	
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis tercatat di dalam log?			✓	
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?			✓	
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?			✓	
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?			✓	
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?			✓	
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian <i>password</i> secara otomatis, termasuk menon-aktifkan <i>password</i> , mengatur kompleksitas/panjangnya dan penggunaan kembali <i>password</i> lama?			✓	
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?			✓	
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses <i>timeouts</i> , <i>lockout</i> setelah kegagalan <i>login</i> , dan penarikan akses?			✓	
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?			✓	
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?			✓	
6.19	Apakah sistem operasi untuk setiap perangkat <i>desktop</i> dan <i>server</i> dimutakhirkan dengan versi terkini?			✓	

8

6.20	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	✓
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	✓
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	✓
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	✓
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	✓
6.25	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamanahkan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?	✓
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	✓

Tabel VIII: Sistem Pengelolaan Keamanan Informasi				
Batasan pengujian dan kriteria pengujian dalam perbaikan keamanan informasi				
(Penilaian) Tidak Dicakup (A), Dicakup Penilaian (B), Dari Penilaian atau Diving Audit Sebagian (C), Dicakup Secara Melayang (D)				
7.1 Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan				A B C D
7.1.1 Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga				
7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?				✓
7.1.1.2 Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?				✓
7.1.1.3 Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatah oleh pihak ketiga?				✓
7.1.1.4 Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?				✓
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?				✓
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?				✓
7.1.1.7 Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dari 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?				✓
7.1.2 Pengelolaan Layanan dan Keamanan Pihak Ketiga				
7.1.2.1 Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?				✓
7.1.2.2 Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?				✓
7.1.2.3 Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap keamanan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?				✓
7.1.3 Pengelolaan Layanan dan Keamanan Pihak Ketiga				
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 instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?				✓
7.1.3.2 Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau dilakukan dalam unit organisasi tertentu?				✓
7.1.3.3 Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang diharapkan dalam perjanjian komersil (kontrak)?				✓
7.1.3.4 Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?				✓

8

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?	<input checked="" type="checkbox"/>
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melaksanakan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	<input checked="" type="checkbox"/>
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	<input checked="" type="checkbox"/>
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	<input checked="" type="checkbox"/>
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga	
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?	<input checked="" type="checkbox"/>
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	<input checked="" type="checkbox"/>
7.1.5	Penanganan Aset	
7.1.5.1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perbaikan, dan penghapusan / penghancuran aset?	<input checked="" type="checkbox"/>
7.1.5.2	Apakah per untuk penghapusan (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	<input checked="" type="checkbox"/>
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga	
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	<input checked="" type="checkbox"/>
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	<input checked="" type="checkbox"/>
7.1.7	Rencana Kelangsungan Layanan Pihak Ketiga	
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	<input checked="" type="checkbox"/>
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	<input checked="" type="checkbox"/>
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	<input checked="" type="checkbox"/>
7.2	Pengamanan Layanan Infrastruktur Awan (Cloud Service)	
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis <i>cloud</i> dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	<input checked="" type="checkbox"/>
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis <i>cloud</i> ?	<input checked="" type="checkbox"/>
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan <i>cloud</i> ?	<input checked="" type="checkbox"/>
7.2.4	Apakah instansi/perusahaan sudah mengkaji, merisetakan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis <i>cloud</i> ?	<input checked="" type="checkbox"/>
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan <i>cloud</i> terkait reputasi penyelenggaranya?	<input checked="" type="checkbox"/>

8

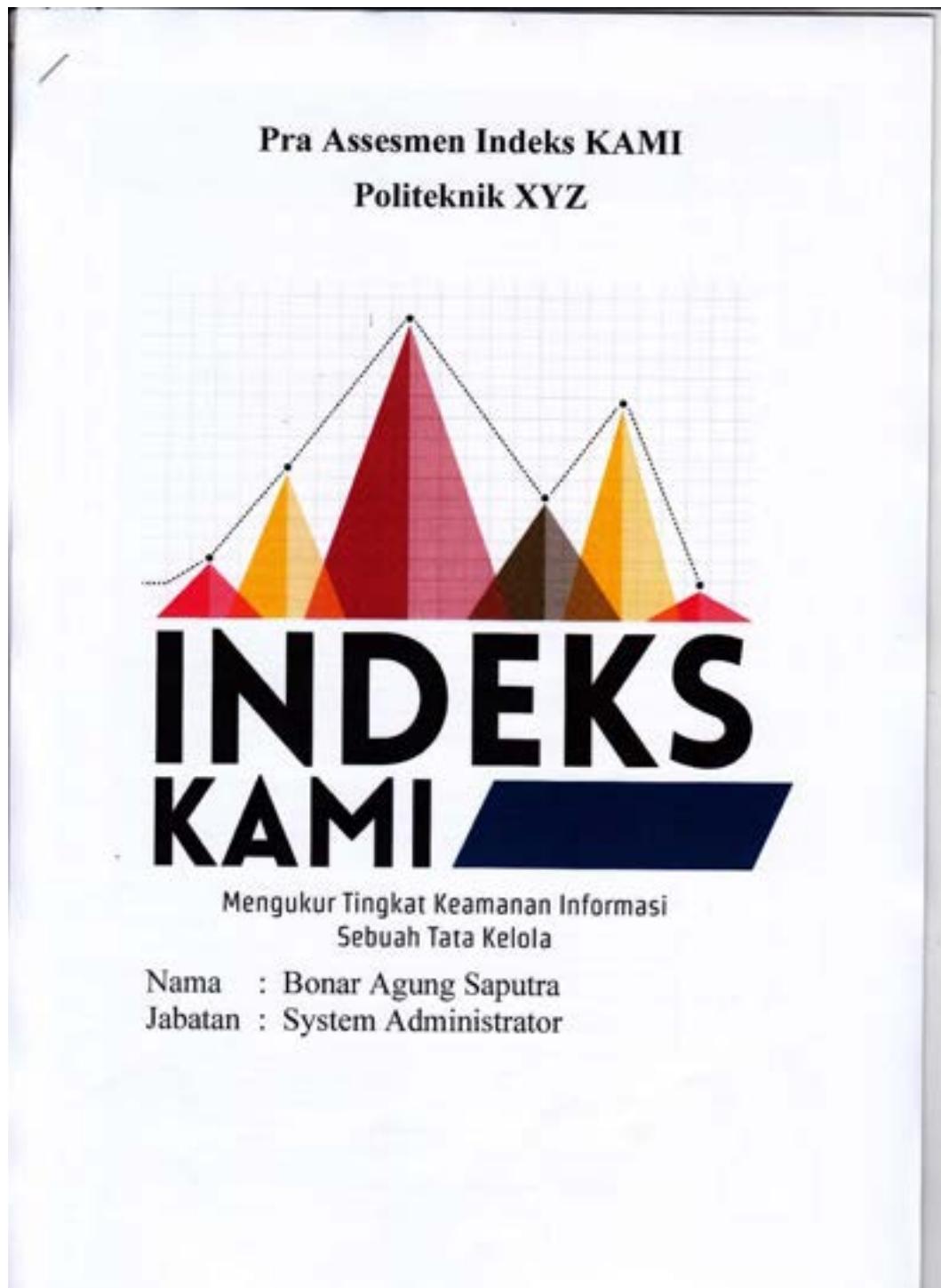
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	<input checked="" type="checkbox"/>
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemerluhan sertifikasi layanan berbasis ISO 27001?	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	<input checked="" type="checkbox"/>
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	<input checked="" type="checkbox"/>
Perlindungan Data Pribadi		
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/eletronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	<input checked="" type="checkbox"/>
7.3.2	Apakah instansi/perusahaan sudah memetakan alir pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	<input checked="" type="checkbox"/>
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	<input checked="" type="checkbox"/>
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundang-undang yang berlaku?	<input checked="" type="checkbox"/>
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (<i>Data Protection Officer, Data Controller, Data Processor</i>) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	<input checked="" type="checkbox"/>
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	<input checked="" type="checkbox"/>
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	<input checked="" type="checkbox"/>
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundang-undang yang berlaku?	<input checked="" type="checkbox"/>
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundang-undang yang berlaku?	<input checked="" type="checkbox"/>
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 menyimpulkan catatan persetujuan tersebut?	<input checked="" type="checkbox"/>
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melacakkan insiden terkait terungkapnya data pribadi?	<input checked="" type="checkbox"/>
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	<input checked="" type="checkbox"/>
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	<input checked="" type="checkbox"/>

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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Tanggal 7/11/2022


Andri Bagus Pratama

3. System Administrator Pra Instalasi Asesmen



Tabel 1. Kategori Sistem Elektronik			
Bagian ini mengidentifikasi tingkat atau kategori sistem elektronik yang dianalisa			
[Kategori Sistem Elektronik] Rendah, Tinggi, Strategis			
#	Karakteristik Testcase / Perbaikan	Status	
		A	B
1.1	Nilai investasi sistem elektronik yang terpiong		✓
	[A] Lebih dari Rp.30 Miliar		
	[B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar		
1.2	[C] Kurang dari Rp.3 Miliar		
	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik		✓
	[A] Lebih dari Rp.10 Miliar		
1.3	[B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar		
	[C] Kurang dari Rp.1 Miliar		
	Miliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu		
1.4	[A] Peraturan atau Standar nasional dan internasional		✓
	[B] Peraturan atau Standar nasional		
	[C] Tidak ada Peraturan khusus		
1.5	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik		✓
	[A] Teknik kriptografi khusus yang disertifikasi oleh Negara		
	[B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri		
1.6	[C] Tidak ada penggunaan teknik kriptografi		
1.7	Jumlah pengguna Sistem Elektronik		✓
	[A] Lebih dari 5.000 pengguna		
	[B] 1.000 sampai dengan 5.000 pengguna		
1.8	[C] Kurang dari 1.000 pengguna		
1.9	Data pribadi yang dikelola Sistem Elektronik		✓
	[A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya		
	[B] Data pribadi yang bersifat individu dan/tapi data pribadi yang terkait dengan kepemilikan badan usaha		
1.10	[C] Tidak ada data pribadi		
1.11	Tingkat klasifikasi/kelarituan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyiraman atau penyerobosan keamanan informasi		✓
	[A] Sangat Rahasia		
	[B] Rahasia dan/ atau Terbatas		
1.12	[C] Biasa		
1.13	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyiraman atau penyerobosan keamanan informasi		✓
	[A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik		
	[B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung		
1.14	[C] Proses yang hanya berdampak pada bisnis perusahaan		
1.15	Dampak dari kugagalan Sistem Elektronik		✓
	[A] Tidak tersedianya layanan publik berikala nasional atau membahayakan pertahanan keamanan negara		
	[B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih		
1.16	[C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih		
1.17	Potensi kerugian atau dampak negatif dari insiden disterbunya keamanan informasi Sistem Elektronik (substansi, teorisme)		✓
	[A] Mengintensifkan korban jiwa		
	[B] Terbatas pada kerugian finansial		
1.18	[C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)		

Bab III: Tata Kelola Keamanan Informasi				
Bab III: Tata Kelola Keamanan Informasi			Status	
#	Fungsi/Organisasi Keamanan Informasi	A	B	C
2.1	Apakah pimpinan instansi/persaudaraan anda secara prinsip dan resmi berenggajawab terhadap pelaksanaan program keamanan informasi (misal yang termuat dalam ITSP), termasuk penetapan kibijakan terkait?			✓
2.2	Apakah instansi/persaudaraan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepuhannya?			✓
2.3	Apakah instansi/persaudaraan pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjalankan program keamanan informasi?			✓
2.4	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan diperlukan dengan lengkap, termasuk keterhadap audit internal dan persyaratan sebagaimana kewajiban?			✓
2.5	Apakah instansi/persaudaraan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?			✓
2.6	Apakah instansi/persaudaraan anda mempunyai kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?			✓
2.7	Apakah semua pelaksana pengamanan informasi di instansi/persaudaraan anda memiliki kompetensi dan keahlian yang memadai bersifat persyaratan/standar yang berlaku?			✓
2.8	Apakah instansi/persaudaraan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepuhannya bagi semua pihak yang terkait?			✓
2.9	Apakah instansi/persaudaraan anda menerapkan program pengembangan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?			✓
2.10	Apakah instansi/persaudaraan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?			✓
2.11	Apakah instansi/persaudaraan anda sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?			✓
2.12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna akses informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasi persyaratan/kelulusan pengamanan (misal: perlakuan informasi atau korjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?			✓
2.13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan setiap terkait (SDM, Legal/Hukum, Umroh, Keuangan dkk) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjalankan kepuhannya pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?			✓
2.14	Apakah tanggungjawab untuk menutarkan, merancang, melaksanakan dan mengelola langkah krlangsungan layanan TIK (business continuity dan disaster recovery plan) sudah didefinisikan dan dialokasikan?			✓
2.15	Apakah pengelola keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepuhannya program keamanan informasi kepada pimpinan instansi/persaudaraan secara rutin dan resmi?			✓
2.16	Apakah kondisi dan permasalahan keamanan informasi di instansi/persaudaraan anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di instansi/persaudaraan anda?			✓
2.17	Apakah pimpinan satuan kerja di instansi/persaudaraan anda menerapkan program khusus untuk memahami tujuan dan sifat kepuhannya pengamanan informasi, khususnya yang mencakup akses informasi yang menjadi tanggungjawabnya?			✓
2.18	Apakah instansi/persaudaraan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaanya, pemantauannya dan etiket pelaporannya?			✓
2.19	Apakah instansi/persaudaraan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaanya?			✓
2.20	Apakah instansi/persaudaraan anda sudah mempunyai target dan sifat pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sifat yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/persaudaraan?			✓
2.21	Apakah instansi/persaudaraan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menjalankannya tingkat kepuhannya?			✓
2.22	Apakah instansi/persaudaraan anda sudah mendefinisikan kibijakan dan langkah penanggolongan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdana)?			✓

Rujukan III: Pengelolaan Risiko Keamanan Informasi		Status			
#	Kajian Risiko Keamanan Informasi	A	B	C	D
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓	
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?			✓	
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓	
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?			✓	
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko 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?			✓	
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?			✓	
3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?			✓	
3.9	Apakah instansi/perusahaan anda sudah mewujudkan 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)?			✓	
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?			✓	
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?			✓	
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?			✓	
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?			✓	
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?			✓	
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?			✓	
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?			✓	

Bab IV: Kerangka Kerja Pengelolaan Keamanan Informasi		Status
[Prestasi] Tidak Dicapai (A); Dalam Perbaikan (B); Dalam Penerapan atau Ditetapkan Sebagian (C), Diterapkan Secara Meryatah (D)		
Prinsip dasar Pengelolaan Kebijakan & Prosedur Keamanan Informasi		
	A B C D	
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?		✓
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?		✓
4.3 Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan 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?		✓
4.5 Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun satuan/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?		✓
4.6 Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?		✓
4.7 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?		✓
4.8 Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?		✓
4.9 Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi ini?		✓
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?		✓
4.11 Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?		✓
4.12 Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?		✓
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?		✓
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?		✓

4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (<i>business continuity planning</i>) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (<i>disaster recovery plan</i>) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (<i>disaster recovery plan</i>) sudah dilakukan sesuai jadwal?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (<i>disaster recovery plan</i>) 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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Programe Strategi dan Program Keamanan Informasi		A	B
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirananya disesuaikan dengan kebutuhan dan perubahan profil risiko?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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)?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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 yang diperlukan, telah diterapkan secara efektif?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Bagian VI: Pengelolaan Aset Informasi					
Situs ini mengidentifikasi kelengkapan pengamanan aset informasi, termasuk kesiapan dan alat pengamanan aset tersebut				Status	
[Penilaian] Tidak Dibuktikan (A); Dalam Permencahan (B); Dalam Pengembangan; Diterapkan Seligam (C); Diterapkan Secara Melanjutkan (D)					
#	Pengelolaan Aset Informasi	A	B	C	D
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)				✓
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundang-undang yang berlaku?				✓
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?				✓
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut				✓
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?				✓
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?				✓
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkannya inventaris aset informasi?				✓
	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?				
5.8	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda				✓
5.9	Tata tertib penggunaan komputer, email, internet dan intranet				✓
5.10	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI				✓
5.11	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan				✓
5.12	Peraturan penggunaan data pribadi yang memerlukan pemberian ijin tertulis oleh pemilik data pribadi				✓
5.13	Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya				✓
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi				✓
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data				✓
5.16	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya				✓
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi				✓
5.18	Prosedur back-up dan uji coba pengembalian data (restore) secara berkala				✓
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya				✓
5.20	Proses pengecekan latar belakang SDM				✓
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.				✓
5.22	Prosedur penghancuran data/aset yang 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				✓

5.24	Prosedur untuk aset yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.			<input checked="" type="checkbox"/>
5.25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?			<input checked="" type="checkbox"/>
5.26	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamatan yang sesuai dengan klasifikasinya?			<input checked="" type="checkbox"/>
5.27	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?			<input checked="" type="checkbox"/>
5.28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset infoemasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?			<input checked="" type="checkbox"/>
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?			<input checked="" type="checkbox"/>
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?			<input checked="" type="checkbox"/>
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?			<input checked="" type="checkbox"/>
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?			<input checked="" type="checkbox"/>
5.33	Apakah tersedia proses untuk memindahkan aset TIK (peranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?			<input checked="" type="checkbox"/>
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, pesugat suhu dan kelembaban) yang sesuai?			<input checked="" type="checkbox"/>
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?			<input checked="" type="checkbox"/>
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?			<input checked="" type="checkbox"/>
5.37	+ Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, mang 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)			<input checked="" type="checkbox"/>
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?			<input checked="" type="checkbox"/>

Bab 6: Teknologi dan Keamanan Informasi				
[Penilaian] Tidak Dilakukan (A); Dalam Persepsi (B); Dalam Pengetahuan atau Dibayangkan Sebagian (C); Diterapkan Secara Mulyasandi (D)				Skor
#	Pengamanan Teknologi	A	B	C
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	✓		
6.2	Apakah jaringan komunikasi disegmenasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	✓		
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?	✓		
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	✓		
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	✓		
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	✓		
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	✓		
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	✓		
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	✓		
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk keperluan jejak audit dan forensik)?	✓		
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	✓		
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	✓		
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengejota kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	✓		
6.14	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?	✓		
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khasus yang berlapis?	✓		
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses <i>timeout</i> , <i>lockout</i> setelah kegagalan login, dan penarikan akses?	✓		
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	✓		
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	✓		
6.19	Apakah sistem operasi untuk setiap perangkat <i>desktop</i> dan <i>server</i> dimutakhirkan dengan versi terkini?	✓		

6.20	Apakah setiap <i>desktop</i> dan <i>server</i> dilindungi dari penyerangan virus (<i>malware</i>)?	✓	
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - <i>audit trail</i>) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	✓	
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukces ditindaklanjuti dan diselesaikan?	✓	
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?		✓
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	✓	
6.25	Apakah instansi/perusahaan ada menerapkan lingkaran pengembangan dan uji coba yang sudah diamanahkan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yg dibangun?		✓
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	✓	

Bab VII: Kelembagaan		Bab VIII: Keamanan			
		Bab IX: Pengelolaan Layanan			
		Bab X: Pengelolaan Keamanan Layanan			
		Bab XI: Pengelolaan Keamanan Layanan			
[Penilaian] Tidak Dibuktikan (A), Dibuktikan (B), Dibuktikan Dengan Kekurangan (C), Dibuktikan Secara Mengilustrasi (D)		Bab XII: Pengelolaan Keamanan Layanan			
		Bab XIII: Pengelolaan Keamanan Layanan			
7.1 Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan		A	B	C	D
7.1.1 Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga					
7.1.1.1 Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?		✓			
7.1.1.2 Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?			✓		
7.1.1.3 Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatah oleh pihak ketiga?			✓		
7.1.1.4 Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?			✓		
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?			✓		
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?			✓		
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? Terkait dengan akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?			✓		
7.1.2 Pengelolaan Layanan dan Keamanan Pihak Ketiga					
7.1.2.1 Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?			✓		
7.1.2.2 Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?			✓		
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?			✓		
7.1.3 Pengelolaan Layanan dan Keamanan Pihak Ketiga					
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 instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?			✓		
7.1.3.2 Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?			✓		
7.1.3.3 Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang diwajibkan dalam perjanjian komersial (kontrak)?			✓		
7.1.3.4 Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?			✓		

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?	<input checked="" type="checkbox"/>
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemerlukan pernyataan keamanan informasi oleh pihak ketiga?	<input checked="" type="checkbox"/>
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	<input checked="" type="checkbox"/>
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	<input checked="" type="checkbox"/>
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga	
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?	<input checked="" type="checkbox"/>
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	<input checked="" type="checkbox"/>
7.1.5	Penanganan Aset	
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?	<input checked="" type="checkbox"/>
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	<input checked="" type="checkbox"/>
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga	
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	<input checked="" type="checkbox"/>
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	<input checked="" type="checkbox"/>
7.1.7	Rencana Kelangsungan Layanan Pihak Ketiga	
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	<input checked="" type="checkbox"/>
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	<input checked="" type="checkbox"/>
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	<input checked="" type="checkbox"/>
7.2	Pengamanan Layanan Infrastruktur Awan (Cloud Service)	
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud/ dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	<input checked="" type="checkbox"/>
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	<input checked="" type="checkbox"/>
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?	<input checked="" type="checkbox"/>
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	<input checked="" type="checkbox"/>
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?	<input checked="" type="checkbox"/>

7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3 Perlindungan Data Pribadi			
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/eletronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (<i>Data Protection Officer, Data Controller, Data Processor</i>) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insides lain?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
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 ?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

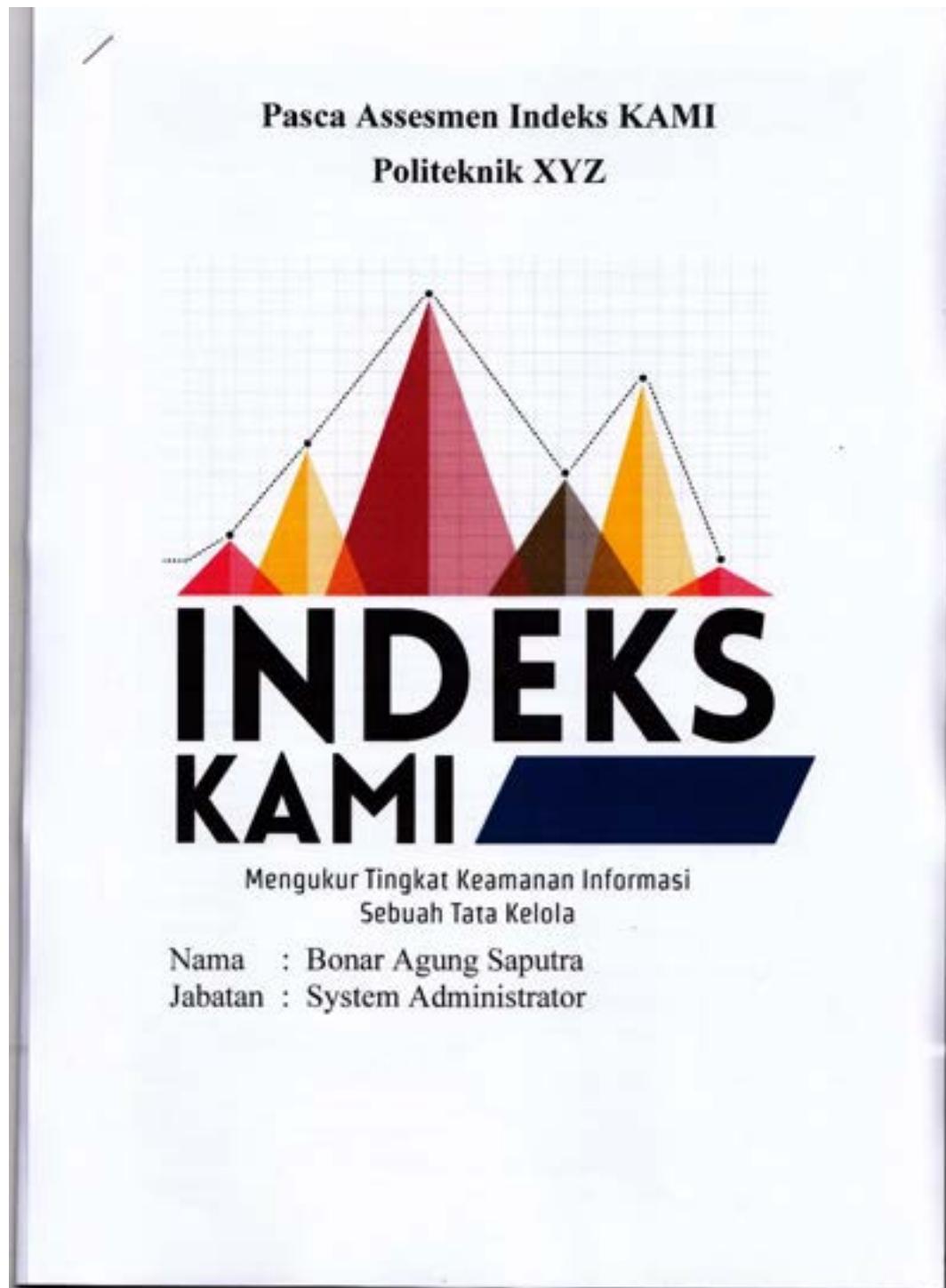
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	<input checked="" type="checkbox"/>		
7.3.15	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahannya apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?		<input checked="" type="checkbox"/>	
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?			<input checked="" type="checkbox"/>

Tanggal 01 - 04 - 2012



Bonar Agung Saputra

4. System Administrator Pasca Instalasi Asesmen



Bagian I: Kategori Sistem Elektronik		
Bagian II: Pengembangan Tingkat dan Karakter Sistem Elektronik yang diwujudkan		
(Kategori Sistem Elektronik) (rendah/Tinggi/Singkat)		
	Karakteristik Sistemat Periode 4	Status
		A B C
1.1	Nilai investasi sistem elektronik yang terpasang	
	[A] Lebih dari Rp.30 Miliar	
	[B] Lebih dari Rp.3 Miliar sd Rp.30 Miliar	
	[C] Kurang dari Rp.3 Miliar	✓
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik	
	[A] Lebih dari Rp.10 Miliar	
	[B] Lebih dari Rp.1 Miliar sd Rp.10 Miliar	
	[C] Kurang dari Rp.1 Miliar	✓
1.3	Mempunyai kewajiban kepatuhan terhadap Peraturan atau Standar tertentu	
	[A] Peraturan atau Standar nasional dan internasional	
	[B] Peraturan atau Standar nasional	✓
	[C] Tidak ada Peraturan khusus	
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik	
	[A] Teknik kriptografi khusus yang disertifikasi oleh Negara	
	[B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri	✓
	[C] Tidak ada penggunaan teknik kriptografi	
1.5	Jumlah pengguna Sistem Elektronik	
	[A] Lebih dari 5.000 pengguna	
	[B] 1.000 sampai dengan 5.000 pengguna	
	[C] Kurang dari 1.000 pengguna	✓
1.6	Data pribadi yang diketahui Sistem Elektronik	
	[A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya	
	[B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha	
	[C] Tidak ada data pribadi	✓
1.7	Tingkat klasifikasi/kekritisitas Data yang ada dalam Sistem Elektronik, relatif terhadap aksi/cara upaya penyerangan atau penerobosan keamanan informasi	
	[A] Sangat Rahasia	
	[B] Rahasia dan/ atau Terbatas	
	[C] Biasa	✓
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap aksi/cara upaya penyerangan atau penerobosan keamanan informasi	
	[A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik	
	[B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung	
	[C] Proses yang hanya berdampak pada bisnis perusahaan	
1.9	Dampak dari kregagalan Sistem Elektronik	
	[A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara	
	[B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih	
	[C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih	✓
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, tembosi)	
	[A] Merintahkan korban jiwa	
	[B] Terbatas pada kerugian finansial	
	[C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	✓

Bagan II: Tata Kelola Keamanan Informasi				
Bagian ini mengawali kisi-kisi berdasarkan kriteria keamanan informasi berdasarkan perusahaan yang terdiri dari bagian-bagian pengelolaan keamanan informasi.				
(Penilaian) Total Dikujok (A); Dalam Penilaianan (B); Dalam Pertemuan atau Diterangkan Sebagian (C); Diterangkan Secara Melayanthi (D)				
	Fungsi/Organisasi Keamanan Informasi			
	A	B	C	D
2.1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penciptaan kebijakan terkait?			✓
2.2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepastiannya?		✓	
2.3	Apakah pejabat/pengawas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menempak dan menjamin kepatuhan program keamanan informasi?		✓	
2.4	Apakah penganggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?		✓	
2.5	Apakah per pelaksana pengamanan informasi yang mencakup semua keperluan dipersiapkan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kerwamahan?		✓	
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan kualitas pelaksana pengelolaan keamanan informasi?		✓	
2.7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan kualitas yang memadai sesuai persyaratan/standar yang berlaku?		✓	
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepastiannya bagi semua pihak yang terkait?		✓	
2.9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan kualitas untuk pejabat dan pegawai pelaksana pengelolaan keamanan informasi?		✓	
2.10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	✓		
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan mensyaratkan pengamanan sesuai dengan peraturan perundangan yang berlaku?		✓	
2.12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna acet informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyusulkan perbaikan/potongan yang ada?		✓	
2.13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan sektor terkait (SDM, Legal/Hukum, Usoor, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, asuransi keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?		✓	
2.14	Apakah tanggungjawab untuk memusatkan, merencanakan, melaksanakan dan mengelola langkah kesiangan/tujuan layanan TIK (business continuity dan disaster recovery plan) sudah didefinisikan dan dilaksanakan?	✓		
2.15	Apakah penganggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerjanya/efektivitas dan kognitif program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?		✓	
2.16	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi koridor/ruang atau bagian dari proses pengembangan keputusan strategis di instansi/perusahaan anda?		✓	
2.17	Apakah pimpinan unit kerja di instansi/perusahaan anda menerapkan program khusus untuk memahami tujuan dan sasaran keputusan pengamanan informasi, khususnya yang mencakup acet informasi yang menjadi tanggungjawabnya?		✓	
2.18	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporannya?		✓	
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kriteria pengelolaan keamanan informasi bagi individu (pejabat & pegawai) melaksananya?		✓	
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 statutnya kepada pimpinan instansi/perusahaan?	✓	✓	
2.21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepastiannya?		✓	
2.22	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah peranggulangan insiden keamanan informasi yang menyengkut pelanggaran hukum (pidana dan perdamaian)?			✓

Bab III: Pengelolaan Risiko Keamanan Informasi		Penilaian Tidak Dapatkan (A), Dapat Perbaikan (B), Dapat Penilaian atau Ditentukan Sebagian (C), Dapat (L)	Status		
#	Kajian Risiko Keamanan Informasi	A	B	C	D
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓	
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?			✓	
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			✓	
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?			✓	
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko 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?			✓	
3.7	Apakah ancaman dan kelemahan yang berkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?			✓	
3.8	Apakah dampak kerugian yang berkait dengan hilangnya/tenggungnya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang 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)?			✓	
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?			✓	
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menarikkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?			✓	
3.12	Apakah status penyelesaian langkah mitigasi risiko dipastur secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?			✓	
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan komitensi dan efektifitasnya?			✓	
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?			✓	
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?			✓	
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?			✓	

9

Bagian IV: Kesiagaan Kepada Pengelola Keamanan Informasi								
Bapak/Ibu mengeluarkan ketegangan dan ketidaknyamanan terhadap kebijakan dan prosedur pengelolaan keamanan informasi dan cara kerjanya								
(Pilihlah) Tidak Dirasakan (A), Dalam Persepsi (B), Diduga Pembenaran Dikenakan Seperti (C), Diketahui Secara Mampu (D)				Status				
Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi					A	B	C	D
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?						<input checked="" type="checkbox"/>	
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?						<input checked="" type="checkbox"/>	
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?						<input checked="" type="checkbox"/>	
4.4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasaranannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?						<input checked="" type="checkbox"/>	
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?						<input checked="" type="checkbox"/>	
4.6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?						<input checked="" type="checkbox"/>	
4.7	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?						<input checked="" type="checkbox"/>	
4.8	Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?						<input checked="" type="checkbox"/>	
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi ini?						<input checked="" type="checkbox"/>	
4.10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya nilai security patch baru, memastikan pemasangannya dan melaporkannya?						<input checked="" type="checkbox"/>	
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?						<input checked="" type="checkbox"/>	
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?						<input checked="" type="checkbox"/>	
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?						<input checked="" type="checkbox"/>	
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?						<input checked="" type="checkbox"/>	

4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	<input checked="" type="checkbox"/>
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	<input checked="" type="checkbox"/>
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah dilakukan sesuai jadwal?	<input checked="" type="checkbox"/>
4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) dievaluasi untuk menerapkan langkah perbaikan atau pemberian yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	<input checked="" type="checkbox"/>
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	<input checked="" type="checkbox"/>
Penerapan Strategi dan Program Keamanan Informasi		A B C D
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	<input checked="" type="checkbox"/>
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhiran disesuaikan dengan kebutuhan dan perubahan profil risiko?	<input checked="" type="checkbox"/>
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	<input checked="" type="checkbox"/>
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)?	<input checked="" type="checkbox"/>
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	<input checked="" type="checkbox"/>
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pemberian dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>
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 pemberian yang diperlukan, telah diterapkan secara efektif?	<input checked="" type="checkbox"/>
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	<input checked="" type="checkbox"/>

Bagian V: Pengelolaan Aset Informasi					
	[Penilaian] Tidak Dilakukan (A); Dalam Perbaikannya (B); Dalam Pelaksanaan atau Diterapkan Seligat (C); Diterapkan Secara Almoyaknya (D)				Status
#	Pengelolaan Aset Informasi				A B C D
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)				✓
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?				✓
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?				✓
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut				✓
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?				✓
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?				✓
5.7	Apakah tersedia proses untuk merilis suatu aset buku ke dalam lingkungan operasional dan memutakhirkann inventaris aset informasi?				✓
5.8	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?				
5.9	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda				✓
5.10	Tata tertib penggunaan komputer, email, internet dan intranet				✓
5.11	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI				✓
5.12	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan				✓
5.13	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi				✓
5.14	Persyaratan dan prosedur pengelolaan/pemberian akses, otentifikasi dan otorisasi untuk menggunakan aset informasi				✓
5.15	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data				✓
5.16	Ketetapan terkait perlakuan data dengan pihak eksternal dan pengamanannya				✓
5.17	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi				✓
5.18	Prosedur back-up dan uji coba pengembalian data (<i>restore</i>) secara berkala				✓
5.19	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya				✓
5.20	Proses pengecekan latar belakang SDM				✓
5.21	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.				✓
5.22	Prosedur penghancuran data/aset yang sudah tidak diperlukan				✓
5.23	Prosedur kajian penggunaan akses (<i>user access review</i>) dan hak aksesnya (<i>user access rights</i>) berikut langkah pemberhentian apabila terjadi ketidaksesuaian (<i>non-conformity</i>) terhadap kebijakan yang berlaku				✓

5.24	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.			✓
5.25	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?			✓
5.26	Apakah tersedia daftar rekomendasi pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?			✓
5.27	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?			✓
	Pengamanan Fisik	A	B	C
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?			✓
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?			✓
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat publikannya?			✓
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?			✓
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?			✓
5.33	Apakah tersedia proses untuk memindahkan aset TIK (peranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk penutupan lokasinya dalam daftar inventaris)?			✓
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?			✓
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan memerlukan: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?			✓
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?			✓
5.37	Apakah tersedia peraturan untuk mengamanakan 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 telepon genggam di dalam ruang server, menggunakan kamera dll)			✓
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?			✓

Bab 5.3 Teknologi dan Keamanan Informasi					
Bagian ini memperbaiki kelengkapan/kompleksitas dan efektivitas pengamanan dalam log dalam pengamanan informasi				Status	
Penilaian: Tidak Dilakukan (A); Dalam Perbaikan (B); Dalam Pengembangan/Diterapkan Sebagian (C); Dilakukan Secara Mempadankan (D)					
#	Pengamanan Teknologi	A	B	C	D
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?			✓	
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?			✓	
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan asset jaringan, sistem dan aplikasi, yang dimatahirkas sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?			✓	
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?			✓	
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?			✓	
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rasongan redundan) sesuai kebutuhan/persyaratan yang ada?			✓	
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?			✓	
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?			✓	
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?			✓	
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?			✓	
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?			✓	
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?			✓	
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?			✓	
6.14	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?			✓	
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?			✓	
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses?			✓	
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?			✓	
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?			✓	
6.19	Apakah sistem operasi untuk setiap perangkat desktop dan server dimatahirkas dengan versi terkini?			✓	

6.20	Apakah setiap <i>desktop</i> dan <i>server</i> dilindungi dari penyerangan virus (<i>malware</i>)?		✓
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - <i>audit trail</i>) yang mengkonfirmasi bahwa antivirus/antimalware telah diinstal secara rutin dan sistematis?		✓
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?		✓
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?		✓
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?		✓
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?		✓
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?		✓

Bab VII: Sistem Pengelolaan Keamanan Informasi			
Bagian II: Pengelolaan Keamanan Informasi yang dilakukan oleh pihak ketiga			
[Pertanyaan] Tidak Diketahui (A), Dalam Proses (B) Data: Penyelesaian Ditemui (C) Sebagian Dilengkapi Secara Mempadai (D)			
Status			
7.1 Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan			
Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga			
7.1.1.	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	<input checked="" type="checkbox"/>	
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	<input checked="" type="checkbox"/>	
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	<input checked="" type="checkbox"/>	
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	<input checked="" type="checkbox"/>	
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?	<input checked="" type="checkbox"/>	
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?	<input checked="" type="checkbox"/>	
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? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	<input checked="" type="checkbox"/>	
7.1.2	Pengelolaan Layanan dan Keamanan Pihak Ketiga		
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	<input checked="" type="checkbox"/>	
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	<input checked="" type="checkbox"/>	
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?	<input checked="" type="checkbox"/>	
7.1.3	Pengelolaan Layanan dan Keamanan Pihak Ketiga		
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 instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	<input checked="" type="checkbox"/>	
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	<input checked="" type="checkbox"/>	
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	<input checked="" type="checkbox"/>	
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	<input checked="" type="checkbox"/>	

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 kemajuananya kepada instansi/perusahaan?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga		
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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.5	Penanganan Aset		
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?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.5.2	Apakah peraturan penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga		
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.7	Rencana Kelangsungan Layanan Pihak Ketiga		
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2	Pengamanan Layanan Infrastruktur Awan (Cloud Service)		
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud' dan menyelesaikan kebijakan keamanan informasi terkait layanan ini?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud'?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud'?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dasar menastikas aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud'?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud' terkait reputasi penyelenggaranya?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	<input checked="" type="checkbox"/>
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan penerapan sertifikasi layanan berbasis ISO 27001?	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	<input checked="" type="checkbox"/>
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	<input checked="" type="checkbox"/>
7.3	Perlindungan Data Pribadi	
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	<input checked="" type="checkbox"/>
7.3.2	Apakah instansi/perusahaan sudah menetapkan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	<input checked="" type="checkbox"/>
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	<input checked="" type="checkbox"/>
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundang-undangan yang berlaku?	<input checked="" type="checkbox"/>
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (<i>Data Protection Officer, Data Controller, Data Processor</i>) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	<input checked="" type="checkbox"/>
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	<input checked="" type="checkbox"/>
7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	<input checked="" type="checkbox"/>
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundang-undangan yang berlaku?	<input checked="" type="checkbox"/>
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemberhan/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundang-undangan yang berlaku?	<input checked="" type="checkbox"/>
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?	<input checked="" type="checkbox"/>
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	<input checked="" type="checkbox"/>
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	<input checked="" type="checkbox"/>
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	<input checked="" type="checkbox"/>

7.3.14	Apaakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahan sesuai dengan peraturan atau perjanjian dengan pemilik data?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7.3.15	Apaakah 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?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
7.3.16	Apaakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Tanggal 07 - 11 - 2022
-
Bonar Agung Saputra