

**EVALUASI TINGKAT KEAMANAN SISTEM INFORMASI
DI PT MAJU BERKAH ADIKARYA MENGGUNAKAN INSTRUMEN
AUDIT KEAMANAN INDEKS KAMI 4.2**



Disusun Oleh:

- | | |
|-------------------------|--------------|
| 1. Adnan Fatoni | (21.01.4707) |
| 2. Herly Chaya putra | (21.01.4658) |
| 3. Yanuar Ardhi Pratama | (21.01.4683) |
| 4. Muh Irvan Hakim | (21.01.4703) |

Dosen Pembimbing:

Pramudhita Ferdiansyah, M.Kom

**PROGRAM STUDI D3 TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM
YOGYAKARTA
2023**

DAFTAR ISI

DAFTAR ISI.....	i
DAFTAR GAMBAR.....	ii
A. Latar Belakang.....	1
B. Objek Penelitian.....	1
C. Hasil dan Pembahasan.....	1
1. Kategori Sistem Elektronik.....	1
2. Tata Kelola.....	1
3. Risiko.....	2
4. Kerangka Kerja.....	2
5. Pengelolaan Aset.....	2
6. Teknologi.....	3
D. Kesimpulan.....	3
E. Lampiran.....	3

A. Latar Belakang

PT. Maju Berkah Adikarya adalah perusahaan yang bergerak dalam bidang multipayment di Indonesia, dengan fokus pada pengembangan software berbasis aplikasi Android & iOS, SMS, WhatsApp, Telegram, dan media komunikasi lainnya. Mereka menawarkan berbagai layanan seperti pulsa, data, voucher fisik, tiket transportasi, pembayaran utilitas, dan masih banyak lagi. Keamanan sistem informasi merupakan hal penting bagi perusahaan tersebut, mengingat mereka menangani data sensitif dan transaksi keuangan pelanggan.

Dalam rangka menjaga keamanan sistem informasi mereka, PT. Maju Berkah Adikarya memutuskan untuk melakukan evaluasi menggunakan instrumen audit keamanan Indeks KAMI 4.2. Instrumen ini dirancang untuk mengukur dan mengevaluasi tingkat keamanan sistem informasi, mencakup aspek kebijakan keamanan, manajemen risiko, pengendalian akses, perlindungan data, serta pemantauan dan respons terhadap insiden keamanan.

Evaluasi tingkat keamanan sistem informasi menggunakan Indeks KAMI 4.2 akan membantu PT. Maju Berkah Adikarya mengidentifikasi kelemahan dan celah keamanan yang ada dalam sistem mereka. Dengan demikian, mereka dapat mengambil langkah-langkah perbaikan yang diperlukan untuk meningkatkan keamanan sistem informasi mereka.

Tingkat keamanan yang optimal pada sistem informasi sangat penting bagi PT. Maju Berkah Adikarya, karena hal ini akan memperkuat kepercayaan klien mereka. Dalam persaingan bisnis yang ketat dan ancaman keamanan yang semakin kompleks, evaluasi rutin terhadap keamanan sistem informasi menjadi langkah yang strategis bagi perusahaan untuk tetap menjadi pilihan utama bagi klien yang mengutamakan keamanan dan kehandalan dalam layanan multipayment.

B. Objek Penelitian

PT. MAJU BERKAH ADIKARYA bergerak dalam bidang multipayment, khususnya pengembangan software berbasis Aplikasi Android & IOS, SMS, whatsapp, telegram, dan media komunikasi lainnya untuk segala kebutuhan Pulsa, data, voucher fisik, voucher makan/ laundry, tiket kereta/ pesawat / hotel, PLN, PDAM, etoll, emoney, ecommers, spp sekolah, samsat. Sebagai Perusahaan pengembangan dibidang multipayment di Indonesia dengan menitikberatkan produknya lewat pilihan program aplikasi yang handal dan didukung dengan desain antar muka (interface) yang dinamik, simple dan menarik. Produk unggulan kami E-Commerce telah mendapat pengakuan luas dari para klien yang sejauh ini telah mempercayakan pengembangan sistem informasi untuk institusi atau lembaganya kepada kami.

C. Hasil dan Pembahasan

1. Kategori Sistem Elektronik

Evaluasi kategori sistem elektronik menunjukkan bahwa PT. Maju Berkah Adikarya memiliki tingkat ketergantungan yang tinggi terhadap sistem elektronik dengan skor 17. Dalam kegiatan operasional dan manajemen, perusahaan sangat mengandalkan sistem elektronik. Untuk meningkatkan efisiensi dan keandalan, diperlukan upaya dalam pengembangan dan optimalisasi sistem elektronik yang

digunakan. Detail hasil evaluasi kategori sistem elektronik dapat ditemukan pada Gambar 2.

1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	B
Skor penetapan Kategori Sistem Elektronik		17
Tingkat Ketergantungan		Tinggi

Gambar 2 Hasil Evaluasi Kategori Sistem Elektronik

2. Tata Kelola

Evaluasi tata kelola PT. Maju Berkah Adi Karya mendapatkan skor 22 dengan tingkat kematangan tingkat 1+. Meskipun telah ada kemajuan, masih ada ruang untuk perbaikan lebih lanjut. Perusahaan perlu mengembangkan praktik pengelolaan yang lebih efektif dan efisien untuk memastikan keputusan dan kebijakan sesuai dengan standar dan tujuan yang ditetapkan. Lihat Gambar 3 untuk hasil evaluasi tata kelola.

Total Nilai Evaluasi Tata Kelola		22
Jumlah pertanyaan Tahap 1	8	
Jumlah pertanyaan Tahap 2	8	
Jumlah pertanyaan Tahap 3	6	
Batas Skor Min untuk Skor Tahap Penerapan 3	48	
Total Skor Tahap Penerapan 1 & 2	22	
Status Penilaian Tahap Penerapan 3	Tidak Valid	

Gambar 3 Hasil Tata Kelola

3. Risiko

Evaluasi risiko PT. Maju Berkah Adi Karya mendapatkan skor 20 dengan tingkat kematangan tingkat 1. Skor ini menunjukkan bahwa pengelolaan risiko perusahaan masih dalam tahap awal. Penting untuk meningkatkan pemahaman dan penerapan praktik pengelolaan risiko yang efektif guna mengurangi potensi kerugian dan memastikan kelangsungan operasional yang lebih baik. Lihat Gambar 4 untuk hasil evaluasi risiko.

Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi		20
Jumlah pertanyaan Tahap 1	10	
Jumlah pertanyaan Tahap 2	4	
Jumlah pertanyaan Tahap 3	2	
Batas Skor Min untuk Skor Tahap Penerapan 3	36	
Total Skor Tahap Penerapan 1 & 2	20	
Status Penilaian Tahap Penerapan 3	Tidak Valid	

Gambar 4 Hasil Evaluasi Risiko

4. Kerangka Kerja

Evaluasi kerangka kerja menunjukkan PT. Maju Berkah Adi Karya memperoleh skor 85 dengan tingkat kematangan tingkat 2. Perusahaan perlu memperhatikan dan memperkuat kerangka kerja yang ada untuk memenuhi standar dan persyaratan yang berlaku. Melalui perbaikan dalam perencanaan dan

implementasi kerangka kerja yang lebih kuat, perusahaan dapat mencapai tujuan pendidikan dengan lebih baik. Lihat Gambar 5 untuk hasil evaluasi kerangka kerja.

Total Nilai Evaluasi Kerangka Kerja	85
Jumlah pertanyaan Tahap 1	12
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	7
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	64
Status Penilaian Tahap Penerapan 3	Valid

Gambar 5 Hasil Evaluasi Kerangka Kerja

5. Pengelolaan Aset

Evaluasi mengenai pengelolaan aset memperoleh skor 62 dengan tingkat kematangan tingkat 1+. Skor ini menunjukkan bahwa pengelolaan aset di PT. Maju Berkah Adi Karya telah mencapai tingkat yang baik. Namun, tetap diperlukan pemantauan dan perawatan yang baik untuk memastikan aset tetap berfungsi dengan baik dan efisien. Hasil evaluasi pengelolaan aset yang dilakukan dapat dilihat pada gambar 6 berikut.

Total Nilai Evaluasi Pengelolaan Aset	62
Jumlah pertanyaan Tahap 1	24
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	4
Batas Skor Min untuk Skor Tahap Penerapan 3	88
Total Skor Tahap Penerapan 1 & 2	62
Status Penilaian Tahap Penerapan 3	Tidak Valid

Gambar 6 Hasil Evaluasi Pengelolaan Aset

6. Teknologi

Evaluasi bagian teknologi dan keamanan informasi diperoleh skor 51 dengan tingkat kematangan tingkat 2. Skor ini menunjukkan bahwa PT. Maju Berkah Adi Karya telah mengadopsi teknologi dan keamanan informasi yang baik. Hal ini sangat penting dalam era digital untuk melindungi data sensitif dan memastikan sistem informasi yang aman. Hasil evaluasi teknologi dan keamanan informasi yang dilakukan dapat dilihat pada gambar 7 berikut.

Total Nilai Evaluasi Teknologi dan Keamanan Informasi	51
Jumlah pertanyaan Tahap 1	14
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	68
Total Skor Tahap Penerapan 1 & 2	51
Status Penilaian Tahap Penerapan 3	Tidak Valid

Gambar 7 Hasil Evaluasi Teknologi dan Keamanan Informasi

D. Kesimpulan

Berdasarkan skor kategori SE dan evaluasi akhir yang diberikan, dapat disimpulkan bahwa tingkat kematangan penerapan standar ISO27001 tidak mencapai standar yang diharapkan. Hasil evaluasi menunjukkan bahwa organisasi atau sistem yang dievaluasi tidak layak.

Berikut adalah ringkasan tingkat kematangan dalam berbagai kategori:

Tata Kelola: Skor 22, tingkat kematangan I+ (Kondisi Awal)

Pengelolaan Risiko: Skor 20, tingkat kematangan I (Kondisi Awal)

Kerangka Kerja Keamanan Informasi: Skor 85, tingkat kematangan II (Penerapan Kerangka Kerja Dasar)

Pengelolaan Aset: Skor 62, tingkat kematangan I+ (Kondisi Awal).

Teknologi dan Keamanan Informasi: Skor 51, tingkat kematangan II (Penerapan Kerangka Kerja Dasar).

Pengamanan Keterlibatan Pihak Ketiga: Skor 35% (Strategis)

Pengamanan Layanan Infrastruktur Awan: Skor 47% (Strategis).

Perlindungan Data Pribadi: Skor 40% (Strategis).

Dari skor di atas, terlihat bahwa kategori dengan tingkat kematangan tertinggi adalah Kerangka Kerja Keamanan Informasi dengan tingkat kematangan II. Namun, kategori lainnya belum mencapai tingkat kematangan yang sama. Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastruktur Awan, dan Perlindungan Data Pribadi memiliki tingkat kematangan yang lebih rendah.

Dengan demikian, perlu dilakukan perbaikan dan peningkatan dalam berbagai aspek penerapan standar ISO27001 untuk mencapai tingkat kematangan yang diinginkan.

E. Lampiran

1. Lampiran hasil bagian kategori sistem elektronik

Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
[Kategori Sistem Elektronik] Rendah, Tinggi, Strategis		Status
#	Karakteristik Instansi/Perusahaan	
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	B
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan 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	C
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	B
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	C
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	B
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	B
1.7	Tingkat klasifikasi/kekritisn Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	B
1.8	Tingkat kekritisn proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman 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	C
1.9	Dampak dari kegagalan 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	B
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)	B
Skor penetapan Kategori Sistem Elektronik		17

Gambar 8 Lampiran 1

2. Lampiran hasil bagian tata kelola

Bagian II Tata Kelola Keamanan Informasi				
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status
#	Fungsi/Organisasi Keamanan Informasi			
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Perencanaan
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Perencanaan
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Perencanaan
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Dalam Perencanaan
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Perencanaan
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Tidak Dilakukan
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Diterapkan Secara Menyeluruh
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Tidak Dilakukan
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan stakeholder terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	Dalam Perencanaan
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (<i>business continuity</i> dan <i>disaster recovery plans</i>) sudah didefinisikan dan dialokasikan?	Dalam Perencanaan
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	Dalam Perencanaan
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi pertimbangan atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	Dalam Perencanaan
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak Dilakukan
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaanya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaanya?	Tidak Dilakukan
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	Tidak Dilakukan
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak Dilakukan
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanganan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan
Total Nilai Evaluasi Tata Kelola				22

Gambar 9 Lampiran 2

3. Lampiran hasil bagian risiko

Bagian III: Pengelolaan Risiko Keamanan Informasi				
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status
#	Kajian Risiko Keamanan Informasi			
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Dalam Perencanaan
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	Tidak Dilakukan
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Diterapkan Secara Menyeluruh
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (<i>custodian</i>) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Perencanaan
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Penerapan / Diterapkan Sebagian
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	Dalam Perencanaan
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Perencanaan
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	Dalam Penerapan / Diterapkan Sebagian
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak Dilakukan
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan
3.14	IV	2	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?	Dalam Penerapan / Diterapkan Sebagian
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan
Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi				20

Gambar 10 Lampiran 3

4. Lampiran hasil bagian kerangka kerja

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			Status
#	Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi		
4.1	I	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?	Dalam Penerapan / Diterapkan Sebagian
4.2	I	1 Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	Diterapkan Secara Menyeluruh
4.3	I	1 Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Dalam Perencanaan
4.4	I	1 Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	Tidak Dilakukan
4.5	I	1 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?	Dalam Penerapan / Diterapkan Sebagian
4.6	I	1 Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkan sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?	Diterapkan Secara Menyeluruh
4.7	I	1 Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
4.8	I	2 Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Penerapan / Diterapkan Sebagian
4.9	I	2 Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi ini?	Dalam Penerapan / Diterapkan Sebagian
4.10	II	2 Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi <i>security patch</i> , alokasi tanggung jawab untuk memonitor adanya rilis <i>security patch</i> baru, memastikan pemasangannya dan melaporkannya?	Dalam Penerapan / Diterapkan Sebagian
4.11	II	2 Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Dalam Penerapan / Diterapkan Sebagian
4.12	II	2 Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Penerapan / Diterapkan Sebagian
4.13	II	2 Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman (<i>Secure SDLC</i>) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	Diterapkan Secara Menyeluruh
4.14	II	2 Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (<i>compensating control</i>) dan jadwal penyelesaiannya?	Dalam Perencanaan
4.15	II	2 Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (<i>business continuity planning</i>) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Dalam Penerapan / Diterapkan Sebagian
4.16	II	3 Apakah perencanaan pemulihan bencana terhadap layanan TIK (<i>disaster recovery plan</i>) sudah mendefinisikan komposisi, peran, wewenang dan tanggung jawab tim yang ditunjuk?	Dalam Perencanaan
4.17	II	3 Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (<i>disaster recovery plan</i>) sudah dilakukan sesuai jadwal?	Dalam Perencanaan
4.18	IV	3 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?	Dalam Perencanaan
4.19	IV	3 Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Penerapan / Diterapkan Sebagian
#	Pengelolaan Strategi dan Program Keamanan Informasi		
4.20	I	1 Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian
4.21	I	1 Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Penerapan / Diterapkan Sebagian
4.22	II	1 Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Diterapkan Secara Menyeluruh
4.23	II	1 Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Diterapkan Secara Menyeluruh
4.24	II	1 Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Diterapkan Secara Menyeluruh
4.25	II	2 Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Perencanaan
4.26	II	2 Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
4.27	IV	3 Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	Dalam Perencanaan
4.28	V	3 Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	Tidak Dilakukan
4.29	V	3 Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	Dalam Perencanaan
Total Nilai Evaluasi Kerangka Kerja			85

Gambar 11 Lampiran 4

5. Lampiran hasil bagian pengelolaan aset

Bagian V: Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			Status
#		Pengelolaan Aset Informasi	
5.1	II	1 Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara? (termasuk kepemilikan aset)	Dalam Perencanaan
5.2	II	1 Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan
5.3	II	1 Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Tidak Dilakukan
5.4	II	1 Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	Tidak Dilakukan
5.5	II	1 Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian
5.6	II	1 Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Diterapkan Secara Menyeluruh
5.7	II	1 Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian
		Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	
5.8	II	1 Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	Dalam Penerapan / Diterapkan Sebagian
5.9	II	1 Tata tertib penggunaan komputer, email, internet dan intranet	Diterapkan Secara Menyeluruh
5.10	II	1 Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Dalam Perencanaan
5.11	II	1 Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Dalam Penerapan / Diterapkan Sebagian
5.12	II	1 Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak Dilakukan
5.13	II	1 Pengelolaan identitas elektronik dan proses otentikasi (<i>username & password</i>) termasuk kebijakan terhadap pelanggaran	Dalam Penerapan / Diterapkan Sebagian
5.14	II	1 Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Perencanaan
5.15	II	1 Ketentuan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak Dilakukan
5.16	II	1 Ketentuan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Tidak Dilakukan
5.17	II	1 Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Diterapkan Secara Menyeluruh
5.18	II	1 Prosedur <i>back-up</i> dan uji coba pengembalian data (<i>restore</i>) secara berkala	Dalam Penerapan / Diterapkan Sebagian
5.19	II	2 Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Perencanaan
5.20	III	2 Proses pengecekan latar belakang SDM	Dalam Penerapan / Diterapkan Sebagian
5.21	III	2 Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib	Dalam Penerapan / Diterapkan Sebagian
5.22	III	2 Prosedur penghancuran data/aset yang sudah tidak diperlukan	Tidak Dilakukan
5.23	III	2 Prosedur kajian penggunaan akses (<i>user access review</i>) dan hak aksesnya (<i>user access rights</i>) berikut langkah pembenahan apabila terjadi ketidaksesuaian (<i>non-conformity</i>) terhadap kebijakan yang berlaku	Dalam Perencanaan
5.24	III	2 Prosedur untuk <i>user</i> yang mutasi/keluar atau tenaga kontrak/ <i>outsourcing</i> yang habis masa kerjanya	Dalam Penerapan / Diterapkan Sebagian
5.25	III	3 Apakah tersedia daftar data/informasi yang harus di- <i>back-up</i> dan laporan analisa kepatuhan terhadap prosedur <i>back-up</i> -nya?	Tidak Dilakukan
5.26	III	3 Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan
5.27	III	3 Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/ <i>vendor</i>) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	Tidak Dilakukan
#		Pengamanan Fisik	
5.28	II	1 Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	Dalam Perencanaan
5.29	II	1 Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Tidak Dilakukan
5.30	II	1 Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	Dalam Penerapan / Diterapkan Sebagian
5.31	II	1 Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Dalam Penerapan / Diterapkan Sebagian
5.32	II	1 Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Perencanaan
5.33	II	1 Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Tidak Dilakukan
5.34	II	2 Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	Dalam Penerapan / Diterapkan Sebagian
5.35	II	2 Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	Dalam Penerapan / Diterapkan Sebagian
5.36	II	2 Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
5.37	II	2 Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telepon genggam di dalam ruang server, menggunakan kamera dll)	Dalam Penerapan / Diterapkan Sebagian
5.38	III	3 Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Tidak Dilakukan
Total Nilai Evaluasi Pengelolaan Aset			62

Gambar 12 Lampiran 5

6. Lampiran hasil bagian teknologi

Bagian VI: Teknologi dan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			Status
#	Pengamanan Teknologi		
6.1	II	1 Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Dalam Perencanaan
6.2	II	1 Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Dalam Penerapan / Diterapkan Sebagian
6.3	II	1 Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?	Dalam Penerapan / Diterapkan Sebagian
6.4	II	1 Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Perencanaan
6.5	II	1 Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Diterapkan Secara Menyeluruh
6.6	II	1 Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Diterapkan Secara Menyeluruh
6.7	II	1 Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Diterapkan Secara Menyeluruh
6.8	II	1 Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian
6.9	II	1 Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian
6.10	II	1 Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Penerapan / Diterapkan Sebagian
6.11	II	1 Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Penerapan / Diterapkan Sebagian
6.12	III	2 Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Dalam Perencanaan
6.13	III	2 Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Perencanaan
6.14	III	2 Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?	Dalam Penerapan / Diterapkan Sebagian
6.15	III	2 Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Dalam Penerapan / Diterapkan Sebagian
6.16	III	2 Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login dan penarikan akses?	Tidak Dilakukan
6.17	III	2 Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Penerapan / Diterapkan Sebagian
6.18	II	1 Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian
6.19	II	1 Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian
6.20	II	1 Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	Dalam Penerapan / Diterapkan Sebagian
6.21	III	2 Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	Tidak Dilakukan
6.22	III	2 Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Perencanaan
6.23	III	2 Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian
6.24	III	2 Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Tidak Dilakukan
6.25	III	3 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 yang dibangun?	Tidak Dilakukan
6.26	IV	3 Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Diterapkan Secara Menyeluruh
Total Nilai Evaluasi Teknologi dan Keamanan Informasi			51

Gambar 13 Lampiran 6

7. Lampiran hasil bagian suplemen

Bagian VII: Suplemen			
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.			
(Perilaian) Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			Status
7.1	Pencapaian Keterlibatan Pihak Ketiga Penyedia Layanan		
7.1.1	Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga		
7.1.1.1	1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau kanvasan kontrak?	Dalam Penerapan / Diterapkan Sebagian
7.1.1.2	1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Dalam Penerapan / Diterapkan Sebagian
7.1.1.3	1	Apakah instansi/perusahaan mengidentifikasi persyaratan mitigasi risiko instansi/perusahaan dan eksploitasi mitigasi risiko yang harus dipenuhi oleh pihak ketiga?	Tidak Dilakukan
7.1.1.4	1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau kanvasan kontrak?	Tidak Dilakukan
7.1.1.5	1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penanganan informasi, manajemen risiko?	Dalam Penerapan / Diterapkan Sebagian
7.1.1.6	1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	Dalam Penerapan / Diterapkan Sebagian
7.1.1.7	1	Apakah hak audit IT secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
		Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	
7.1.2	Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga		
7.1.2.1	1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layannya?	Dalam Perencanaan
7.1.2.2	1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Dalam Perencanaan
7.1.2.3	1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	Dalam Perencanaan
7.1.3	Pengelolaan Layanan dan Keamanan Pihak Ketiga		
7.1.3.1	1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	Dalam Perencanaan
7.1.3.2	1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau diwujudkan dalam unit organisasi tertentu?	Tidak Dilakukan
7.1.3.3	1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disampaikan dalam perjanjian komersial kontrak?	Dalam Penerapan / Diterapkan Sebagian
7.1.3.4	1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Tidak Dilakukan
7.1.3.5	1	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan keamanannya kepada instansi/perusahaan?	Dalam Perencanaan
7.1.3.6	1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
7.1.3.7	1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terakumulasi dalam pemenuhan rencana tersebut?	Dalam Penerapan / Diterapkan Sebagian
7.1.3.8	1	Apakah kondisi terkait dengan / peran/ kanvasan keddapatannya pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	Dalam Penerapan / Diterapkan Sebagian
7.1.4	Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga		
7.1.4.1	1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain: - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	Tidak Dilakukan
7.1.4.2	1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi lainnya?	Tidak Dilakukan
7.1.5	Penanganan Aset		
7.1.5.1	1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftran, perubahan, dan penghapusan / penghauran aset?	Tidak Dilakukan
7.1.5.2	1	Apakah per untuk penghauran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	Tidak Dilakukan
7.1.6	Pengelolaan Insiden oleh Pihak Ketiga		
7.1.6.1	1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
7.1.6.2	1	Apakah pihak ketiga memiliki buku-buku penerapan yang memadai dalam menangani insiden keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
7.1.7	Rencana Kelangkaan Layanan Pihak Ketiga		
7.1.7.1	1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangkaan layanan pihak ketiga dalam keadaan darurat/bencana?	Tidak Dilakukan
7.1.7.2	1	Apakah kebijakan, prosedur atau rencana kelangkaan layanan tersebut telah diuji/boba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Tidak Dilakukan
7.1.7.3	1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang drugaskan untuk mengelola proses kelangkaan layannya?	Dalam Perencanaan
7.2	Keperluan Perilaku Restitusi Layanan (Cloud Service)		
7.2.1	1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan mengevaluasi kebijakan keamanan informasi terkait layanan ini?	Diterapkan Secara Menyeluruh
7.2.2	1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?	Diterapkan Secara Menyeluruh
7.2.3	1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?	Diterapkan Secara Menyeluruh
7.2.4	1	Apakah instansi/perusahaan sudah menguji, menetapkan kriteria dan memastikan aspek hukum (yurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?	Dalam Perencanaan
7.2.5	1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi dan kepercayaannya?	Dalam Perencanaan
7.2.6	1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Dalam Perencanaan
7.2.7	1	Apakah instansi/perusahaan sudah mengevaluasi kelakuan keamanan layanan cloud termasuk aspek ketersediaan dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Dalam Perencanaan
7.2.8	1	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	Dalam Perencanaan
7.2.9	1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?	Tidak Dilakukan
7.2.10	1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Tidak Dilakukan
7.3	Perlindungan Data Pribadi		
7.3.1	1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	Dalam Penerapan / Diterapkan Sebagian
7.3.2	1	Apakah instansi/perusahaan sudah menetapkan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?	Dalam Penerapan / Diterapkan Sebagian
7.3.3	1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Tidak Dilakukan
7.3.4	1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Diterapkan Secara Menyeluruh
7.3.5	1	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	Dalam Perencanaan
7.3.6	1	Apakah instansi/perusahaan sudah menganalisa dampak terkait tenunglanya data pribadi yang disimpan, diolah dan dipertukarkan secara legal atau karena insiden lain?	Tidak Dilakukan
7.3.7	1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Tidak Dilakukan
7.3.8	1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Dalam Perencanaan
7.3.9	1	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Tidak Dilakukan
7.3.10	1	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan dibertukarkan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut?	Dalam Penerapan / Diterapkan Sebagian
7.3.11	1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait tenunglanya data pribadi?	Dalam Penerapan / Diterapkan Sebagian
7.3.12	1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Dalam Penerapan / Diterapkan Sebagian
7.3.13	1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan terakumulasi?	Dalam Penerapan / Diterapkan Sebagian
7.3.14	1	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/burnsuhannya sesuai dengan peraturan atau penilaian dengan pemilik data?	Tidak Dilakukan
7.3.15	1	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/burnsuhannya data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengadanya lebih lanjut atau atas permintaan pemilik data dan menyingkir catatan proses tersebut?	Tidak Dilakukan
7.3.16	1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Dalam Penerapan / Diterapkan Sebagian

Gambar 14 Lampiran 7

8. Lampiran hasil bagian ringkasan

