**Kuisioner Penelitian**

|  |  |  |  |
| --- | --- | --- | --- |
| **Klausula 1 : Kebijakan Keamanan** | | | |
| **Kebijakan Kemanan Informasi** | | | |
| Pengarahan manajemen dan dukungan untuk keamanan informasi harus disusun secara jelas. | | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 1.1 | Apakah dokumen kebijakan keamanan informasi sudah disusun? |  |  |
| 1.2 | Apakah dokumen kebijakan keamanan informasi sudah diterbitkan? |  |  |
|  |  |  |  |
| **Klausula 2 : Pengorganisasian Keamanan** | | | |
| **2.1** | **Infrastruktur Kemanan Informasi** |  |  |
|  | Kerangka kerja manajemen harus disusun untuk memprakarsai dan mengendalikan implementasi keamanan informasi di dalam organisasi. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 2.1.1 | Apakah sudah dibentuk forum untuk mengawasi dan mendukung keamanan informasi? |  |  |
| 2.1.2 | Apakah sudah ada proses yang ditetapkan untuk mengkoordinasikan pelaksanaan langkah-langkah keamanan informasi? |  |  |
| 2.1.3 | Apakah tanggung jawab untuk memenuhi persyaratan keamanan informasi sudah didefinisikan dengan jelas? |  |  |
| 2.1.4 | Apakah proses persetujuan manajemen sudah ditetapkan untuk memberi izin pada fasilitas TI baru baik dari sudut pandang bisnis maupun teknis? |  |  |
| 2.1.5 | Apakah sudah ditetapkan sebuah kemampuan yang memberi nasihat keamanan informasi yang khusus? (*Has a capability been established that provides specialized information security advice?)* |  |  |
| 2.1.6 | Apakah ada hubungan dengan petugas dan organisasi keamanan informasi di luar termasuk industri dan/atau spesialis keamanan pemerintah; otoritas penegakan hukum; penyedia layanan TI; otoritas telekomunikasi? |  |  |
| 2.1.7 | Apakah tinjauan independen atas praktik keamanan informasi sudah dijalankan untuk memastikan kelayakan, keefektivan, dan kepatuhan pada kebijakan-kebijakan tertulis? |  |  |
| **2.2** | **Keamanan Akses Pihak Ketiga** |  |  |
|  | Fasilitas-fasilitas TI organisasi dan aset-aset informasi yang mengendalikan akses pihak ketiga yang non-organisasi harus dijaga agar tetap aman. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 2.2.1 | Apakah resiko-resiko hubungan pihak ketiga sudah dianalisis? |  |  |
| 2.2.2 | Apakah langkah-langkah keamanan yang khas sudah diidentifikasi untuk memerangi resiko koneksi pihak ketiga? |  |  |
| 2.2.3 | Apakah persyaratan keamanan dimasukkan dalam kontrak-kontrak resmi pihak ketiga? |  |  |
| **2.3** | **Mengalihdayakan (*Outsourcing*)** |  |  |
|  | Keamanan informasi harus dipertahankan bahkan ketika tanggung jawab untuk pemrosesan dialihdayakan kepada organisasi lain. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 2.3.1 | Apakah persyaratan keamanan pemilik informasi sudah diatur dengan sebuah kontrak antara para pemilik dan organisasi outsource? |  |  |
|  |  |  |  |
| **Klausula 3 : Klasifikasi dan Kontrol Aset** | | | |
| 3.1 | **Akuntansi Aset** |  |  |
|  | Akuntansi yang memadai atas akses organisasi harus disusun | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 3.1.1 | Apakah penginventarisasian aset-aset utama yang berhubungan dengan setiap sistem informasi sudah diciptakan? |  |  |
| 3.2 | **Klasifikasi Informasi** |  |  |
|  | Klasifikasi keamanan harus digunakan untuk menunjukkan keperluan akan, dan prioritas untuk, perlindungan keamanan aset informasi. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 3.2.1 | Apakah panduan klasifikasi keamanan sudah ditetapkan untuk menunjukkan keperluan akan, dan prioritas untuk, perlindungan keamanan? |  |  |
| 3.2.2 | Apakah suatu proses sudah diimplementasikan untuk memberi label informasi yang mensyaratkan perlindungan keamanan? |  |  |
|  |  |  |  |
| **Klausula 4 : Keamanan Personil** | | | |
| **4.1** | **Keamanan dalam Definisi Kerja dan Pensumberdayaan** |  |  |
|  | Keamanan sudah perlu ditangani sejak tahapan perekrutan, termasuk yang menyangkut deskripsi tugas dan kontrak, dan dipantau selama seseorang dipekerjakan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 4.1.1 | Apakah tanggung jawab keamanan tercakup dalam deskripsi tugas pegawai? |  |  |
| 4.1.2 | Apakah lamaran kerja diteliti untuk pekerjaan-pekerjaan yang memerlukan akses terhadap informasi yang peka? |  |  |
| 4.1.3 | Apakah perjanjian untuk menjaga kerahasiaan menjadi persyaratan? |  |  |
| 4.1.4 | Apakah syarat dan ketentuan kerja mencakup tanggung jawab pegawai untuk keamanan informasi, termasuk lama waktu sesudah bekerja dan akibat-akibat dari kegagalan untuk memenuhi syarat-syarat ini? |  |  |
| **4.2** | **Pelatihan Pengguna** |  |  |
|  | Para pengguna harus dilatih dalam hal prosedur keamanan dan penggunaan fasilitas TI yang benar. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 4.2.1 | Sebelum memperoleh akses terhadap fasilitas TI, apakah para pengguna mendapat pelatihan dalam kebijakan dan prosedur keamanan informasi, persyaratan keamanan, pengawasan bisnis dan penggunaan fasilitas TI yang benar? |  |  |
| **4.3** | **Menanggapi Kejadian dan Salah Fungsi Keamanan** |  |  |
|  | Kejadian-kejadian yang mempengaruhi keamanan seharusnya secepat mungkin dilaporkan melalui jalur manajemen. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 4.3.1 | Apakah pelaporan dan prosedur tanggapan kejadian resmi tersedia untuk mengidentifikasi tindakan yang diambill ketika menerima laporan kejadian? |  |  |
| 4.3.2 | Apakah para pengguna diwajibkan untuk mencatat dan melaporkan semua kelemahan keamanan yang diamati atau diduga ada di dalam atau mengancam sistem atau pelayanan? |  |  |
| 4.3.3 | Apakah para pengguna diwajibkan untuk mencatat dan melaporkan peranti lunak apa saja yang tidak berfungsi secara benar kepada bagian pendukung TI? |  |  |
| 4.3.4 | Apakah tersedia mekanisme untuk memantau jenis, volume, dan biaya kejadian-kejadian dan salah fungsi? |  |  |
| 4.3.5 | Apakah proses penegakan disiplin resmi tersedia untuk menindak para pegawai yang melanggar kebijakan dan prosedur keamanan? |  |  |
|  |  |  |  |
| **Klausula 5 : Keamanan Fisik & Lingkungan** | | | |
| **5.1** | **Wilayah yang Diamankan** |  |  |
|  | Fasilitas TI yang mendukung kegiatan yang sangat penting atau peka merupakan bagian dari wilayah yang diamankan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 5.1.1 | Apakah perlindungan keamanan fisik tersedia, berdasarkan batas-batas yang sudah ditetapkan melalui penghalang yang ditempatkan secara strategis di seluruh organisasi? |  |  |
| 5.1.2 | Apakah kendali pintu masuk digunakan pada wilayah-wilayah yang diamankan untuk memastikan hanya petugas yang mendapat izin yang dapat memperoleh akses? |  |  |
| 5.1.3 | Apakah keamanan fisik untuk pusat-pusat data dan ruang-ruang komputer sebanding dengan ancaman-ancaman? |  |  |
| 5.1.4 | Apakah kendali tambahan digunakan untuk petugas atau pihak ketiga yang bekerja di wilayah yang diamankan? |  |  |
| 5.1.5 | Apakah wilayah tempat penyerahan dan pemuatan di ruang komputer/pusat data terpisah untuk mencegah akses tanpa izin? |  |  |
| **5.2** | **Keamanan Peralatan** |  |  |
|  | Peralatan harus dilindungi secara fisik dari ancaman keamanan dan bahaya lingkungan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 5.2.1 | Apakah ada perlengkapan yang ditempatkan untuk mengurangi resiko bahaya lingkungan dan akses tanpa izin? |  |  |
| 5.2.2 | Apakah peralatan elektronik dilindungi dari kegagalan pasokan daya dan ketidakteraturan listrik lainnya? |  |  |
| 5.2.3 | Apakah sambungan kabel daya dan telekomunikasi dilindungi dari putus atau kerusakan sambungan? |  |  |
| 5.2.4 | Apakah prosedur sudah ditetapkan untuk memelihara peralatan TI dengan benar untuk memastikan ketersediaan dan keterpaduannya? |  |  |
| 5.2.5 | Apakah peralatan yang dipakai di luar lokasi, siapa pun pemiliknya, memberikan perlindungan sama besarnya dengan yang diberikan peralatan TI di lokasi? |  |  |
| **5.3** | **Kendali Umum** |  |  |
|  | Informasi dan fasilitas pemrosesan informasi harus dilindungi dari pengungkapan pada, perubahan oleh, atau pencurian oleh pihak-pihak yang tidak diziinkan, dan kendali harus tersedia untuk meminimalkan kerugian atau kerusakan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 5.3.1 | Apakah kebijakan meja bersih/layar bersih terhadap bahan yang peka sudah diadopsi untuk mengurangi resiko akses tanpa izin, kerugian, atau kerusakan di luar jam kerja biasa? |  |  |
| 5.3.2 | Apakah petugas diwajibkan untuk memperoleh izin manajemen yang didokumentasi untuk mengambil peralatan, data, atau peranti lunak di luar lokasi? |  |  |
|  |  |  |  |
| **Klausula 6 : Manajemen Komunikasi dan Operasi** | | | |
| **6.1** | **Prosedur dan Tanggung Jawab Operasional** |  |  |
|  | Tanggung jawab dan prosedur harus ditetapkan untuk manajemen dan operasi semua komputer dan jaringan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.1.1 | Apakah prosedur operasi dengan jelas didokumentasikan untuk semua sistem komputer operasi untuk memastikan sistem itu adalah operasi yang benar, yang aman? |  |  |
| 6.1.2 | Apakah ada proses untuk perubahan kendali pada fasilitas-fasilitas TI dan sistem-sistem untuk memastikan kendali yang memuaskan atas semua perubahan pada peralatan, peranti lunak atau prosedur? |  |  |
| 6.1.3 | Apakah tanggung jawab dan prosedur manajemen kejadian tersedia untuk memastikan tanggapan yang cepat, efektif, teratur terhadap kejadian-kejadian keamanan? |  |  |
| 6.1.4 | Apakah tugas-tugas atau wilayah-wilayah tanggung jawab dipilah-pilah untuk mengurangi terjadinya modifikasi tanpa izin atau penyalahgunaan data atau layanan? |  |  |
| 6.1.5 | Apakah fasilitas-fasiltas pengembangan dan operasional dipisahkan untuk mengurangi resiko perubahan tak direncanakan atau akses tanpa izin terhadap peranti operasional dan data bisnis? |  |  |
| **6.2** | **Perencanaan dan Penerimaan Sistem** |  |  |
|  | Perencanaan dan persiapan sebelumnya dapat memastikan ketersediaan kemampuan dan sumber daya yang memadai. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.2.1 | Apakah persyaratan kapasitas dipantau, dan persyaratan di masa depan diproyeksikan, untuk mengurangi resiko beban lebih pada sistem? |  |  |
| 6.2.2 | Apakah kriteria penerimaan untuk sistem baru sudah ditetapkan, dan apakah ujicoba yang sesuai sudah dilakukan sebelum penerimaan? |  |  |
| **6.3** | **Perlindungan dari Peranti Lunak yang Berbahaya** |  |  |
|  | Menerapkan prinsip kehati-hatian untuk mencegah dan mendeteksi peranti lunak yang berbahaya dapat mengamankan keterpaduan peranti lunak dan data. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.3.1 | Apakah deteksi virus dan langkah-langkah pencegahan dan prosedur kesadaran pengguna sudah dijalankan? |  |  |
| **6.4** | **Pemeliharaan** |  |  |
|  | Prosedur rutin harus disusun untuk membuat salinan data cadangan, mencatat peristiwa-peristiwa dan kesalahan-kesalahan, dan jika sesuai, memantau lingkungan peralatan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.4.1 | Apakah sudah ditetapkan sebuah proses untuk membuat salinan cadangan secara teratur atas data bisnis yang penting dan peranti lunak untuk memastikan bahwa data itu bisa ditemukan kembali menyusul bencana komputer atau kegagalan media? |  |  |
| 6.4.2 | Apakah operator komputer diwajibkan untuk menyimpan rekaman semua pekerjaan yang dilakukan? |  |  |
| 6.1.3 | Apakah tersedia prosedur untuk merekam kesalahan-kesalahan yang dilaporkan oleh para pengguna yang menyangkut masalah-masalah dengan sistem komputer atau komunikasi? |  |  |
| **6.5** | **Manajemen Jaringan** |  |  |
|  | Keamanan jaringan komputer yang dapat menjangkau batas-batas organisasi harus diatur untuk mengamankan informasi dan untuk melindungi infrastruktur pendukung. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.5.1 | Apakah kendali yang memadai memastikan keamanan data dalam jaringan, dan perlindungan pada layanan terhubung dari akses tanpa izin? |  |  |
| **6.6** | **Penanganan dan Keamanan Media** |  |  |
|  | Media komputer harus dikendalikan dan secara fisik dilindungi untuk mencegah kerusakan pada aset dan gangguan pada kegiatan bisnis. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.6.1 | Apakah tersedia prosedur untuk pengaturan media komputer yang dapat dihapus seperti tape, cakram, kaset, dan laporan dalam bentuk cetak? |  |  |
| 6.6.2 | Apakah tersedia proses untuk memastikan bahwa media komputer dapat dihilangkan dengan pasti dan aman ketika tidak lagi dibutuhkan? |  |  |
| 6.6.3 | Apakah prosedur-prosedur untuk menangani data yang peka tersedia untuk melindungi data semacam itu dari pengungkapan tanpa izin atau salah penggunaan? |  |  |
| 6.6.4 | Apakah dokumentasi sistem dilindungi dari akses tanpa izin? |  |  |
| **6.7** | **Pertukaran Informasi dan Peranti Lunak** |  |  |
|  | Pertukaran data dan peranti lunak antarorganisasi harus dikendalikan untuk mencegah penghilangan, perubahan, atau penyalahgunaan data. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 6.7.1 | Apakah ada perjanjian resmi, termasuk perjanjian wasiat peranti lunak jika diperlukan, untuk pertukaran data dan peranti lunak (apakah secara elektronik atau manual) antar-organisasi? |  |  |
| 6.7.2 | Apakah kendali yang diterapkan untuk mengamankan media komputer yang dipindahkan antara lokasi untuk untuk meminimalkan kerentanannya atas akses tanpa izin, penyalahgunaan, atau korupsi selama pemindahan? |  |  |
| 6.7.3 | Apakah kendali keamanan diterapkan bila perlu untuk melindungi perdagangan elektronik (saling tukar data elektronik, surat elektronik, dan transaksi on-linemelalui jaringan publik seperti Internet) terhadap pemutusan atau perubahan tanpa izin? |  |  |
| 6.7.4 | Apakah kendali diterapkan jika diperlukan untuk mengurangi bisnis dan resiko keamanan yang berhubungan dengan surat elektronik untuk mencakup pemutusan, perubahan, dan kesalahan? |  |  |
| 6.7.5 | Apakah kebijakan dan panduan yang jelas tersedia untuk mengendalikan bisnis dan resiko keamanan yang berhubungan dnegan sistem kantor elektronik? |  |  |
| 6.7.6 | Apakah ada proses izin resmi sebelum informasi tersedia untuk umum? |  |  |
| 6.7.7 | Apakah prosedur dan kendali tersedia untuk melindungi pertukaran informasi melalui penggunaan fasilitas komunikasi suara, faksimili, dan video? |  |  |
|  |  |  |  |
| **Klausula 7 : Pengontrolan Akses** | | | |
| **7.1** | **Persyaratan Bisnis untuk Akses Sistem** |  |  |
|  | Kebijakan untuk penyebarluasan dan pemilikanhak atas informasi harus mengendalikan akses terhadap layanan komputer dan data berdasarkan persyaratan bisnis. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.1.1 | Apakah persyaratan bisnis didefinisikan dan didokumentasi untuk kendali akses? |  |  |
| **7.2** | **Manajemen Akses Pengguna** |  |  |
|  | Prosedur resmi diperlukan untuk mengendalikan alokasi hak-hak akses terhadap layanan TI. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.2.1 | Apakah ada prosedur untuk mendaftar dan tidak mendaftar lagi bagi pengguna resmi untuk akses terhadap semua layanan TI multiguna? |  |  |
| 7.2.2 | Apakah ada pembatasan dan kendali atas penggunaan fitur atau fasilitas multi pengguna sistem TI yang memungkinkan seorang pengguna untuk menghalangi sistem atau kendali aplikasi? |  |  |
| 7.2.3 | Apakah proses manajemen kata sandi resmi sudah ditetapkan untuk mengendalikan kata sandi? |  |  |
| 7.2.4 | Apakah sebuah proses resmi tersedia untuk tinjauan berkala atas hak-hak akses pengguna? |  |  |
| **7.3** | **Tanggung Jawab Pengguna** |  |  |
|  | Pengguna harus disadarkan atas tanggung jawab mempertahankan kendali akses yang efektif, khususnya menyangkut penggunaan kata sandi dan keamanan peralatan pengguna. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.3.1 | Apakah para pengguna diajari praktik keamanan yang baik dalam pemilihan dan penggunaan kata sandi? |  |  |
| 7.3.2 | Apakah semua pengguna dan kontraktor sudah disadarkan tentang persyaratan dan prosedur keamanan untuk melindungi peralatan tanpa penjaga? |  |  |
| 7.3.3 | Apakah semua pengguna dan kontraktor sudah disadarkan tentang tanggung jawab mereka untuk melaksanakan perlindungan seperti itu? |  |  |
| **7.4** | **Kendali Akses Jaringan** |  |  |
|  | Koneksi pada layanan-layanan jaringan harus dikendalikan untuk memastikan bahwa para pengguna atau layanan komputer yang terhubung tidak /berkompromi dalam soal keamanan dengan layanan jaringan lainnya. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.4.1 | Apakah sebuah proses tersedia untuk memastikan bahwa jaringan dan layanan komputer yang dapat diakses oleh satu pengguna atau dari terminal tertentu sejalan dengan kebijakan kendali akses bisnis? |  |  |
| 7.4.2 | Apakah sudah dimasukkan kendali yang membatasi jalur antara terminal pengguna dan layanan komputer yang penggunanya diberi izin akses? |  |  |
| 7.4.3 | Apakah koneksi oleh pengguna dari jarak jauh melalui jaringan umum atau non-organisasi diautentikasi untuk mencegah akses terhadap aplikasi bisnis? |  |  |
| 7.4.4 | Apakah koneksi dengan sistem komputer jarak jauh diautentikasi untuk mencegah akses tanpa izin terhadap aplikasi bisnis? |  |  |
| 7.4.5 | Apakah ada proses untuk mengendalikan akses terhadap porta-porta diagnostik yang dirancang untuk penggunaan jarak jauh oleh teknisi pemelihara? |  |  |
| 7.4.6 | Apakah jaringan yang besar dipilah menjadi wilayah-wilayah terpisah untuk mengurangi resiko akses tanpa izin terhadap sistem komputer yang ada yang memakai jaringan tersebut? |  |  |
| 7.4.7 | Apakah kendali dimasukkan untuk membatasi kemampuan koneksi para pengguna, dalam mendukung persyaratan kebijakan akses atas aplikasi bisnis sampai ke batas-batas organisasi? |  |  |
| 7.4.8 | Apakah kendali perutean sudah dimasukkan dalam jaringan bersama di semua batas organisasi untuk memastikan bahwa koneksi komputer dan arus informasi mematuhi kebijakan akses unit-unit bisnis? |  |  |
| 7.4.9 | Apakah penyedia jaringan dengan jelas menggambarkan atribut keamanan dari semua layanan yang digunakan, dan menetapkan implikasi keamanan untuk kerahasiaan, keterpaduan, dan ketersediaan aplikasi bisnis? |  |  |
| **7.5** | **Kendali Akses Sistem Operasi** |  |  |
|  | Akses terhadap komputer harus sangat terbatas melalui penggunaan:  ● Identifikasi terminal otomatis;  ● Prosedur log masuk terminal;; ● Identitas pengguna:  ● Manajemen kata sandi;  ● Tanda bahaya yang mengancam; ● Jeda terminal; dan ● Waktu koneksi terbatas. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.5.1 | Apakah identifikasi terminal otomatis digunakan untuk melakukan autentikasi koneksi dengan lokasi-lokasi tertentu? |  |  |
| 7.5.2 | Apakah prosedur-prosedur sudah dirancang untuk masuk ke sistem komputer untuk meminimalkan kesempatan akses tanpa izin? |  |  |
| 7.5.3 | Apakah semua pengguna memiliki tanda identifikasi (userID) untuk penggunaan pribadi mereka dan satu-satunya, untuk memastikan bahwa kegiatan mereka dapat ditelusuri kepada mereka? |  |  |
| 7.5.4 | Apakah sistem manajemen kata sandi digunakan untuk autentikasi para pengguna? |  |  |
| 7.5.5 | Apakah program-program utilitas yang dapat digunakan untuk mengganggu sistem dan kendali aplikasi dikendalikan secara ketat dan penggunaannya dibatasi? |  |  |
| 7.5.6 | Berdasarkan penilaian resiko, apakah tanda peringatan mengancam disediakan bagi para pengguna yang mungkin menjadi sasaran intimidasi? |  |  |
| 7.5.7 | Apakah sudah ada definisi tanggung jawab untuk menanggapi tanda bahaya yang mengancam? |  |  |
| 7.5.8 | Apakah terminal di lokasi beresiko tinggi diatur untuk jeda ketika sedang tidak aktif untuk mencegah akses oleh pihak-pihak tanpa izin? |  |  |
| 7.5.9 | Apakah batas waktu sudah ditetapkan untuk terminal dapat dihubungkan dengan sistem aplikasi yang peka? |  |  |
| **7.6** | **Kendali Akses Aplikasi** |  |  |
|  | Kendali akses logis harus didukung untuk melindungi sistem-sistem aplikasi dan data dari akses tanpa izin.. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.6.1 | Apakah akses terhadap data dan fungsi sistem aplikasi bersifat terbatas sesuai dengan kebijakan akses dan berdasarkan persyaratan individual? |  |  |
| 7.6.2 | Menurut resiko-resiko yang diidentifikasi, apakah sistem aplikasi yang peka beroperasi dalam lingkungan pemrosesan yang terisolasi? |  |  |
| **7.7** | **Akses dan Penggunaan Sistem Pemantauan (*Monitoring*)** |  |  |
|  | Sistem-sistem harus dipantau untuk memastikan kepatuhan pada kebijakan dan standar akses, untuk mendeteksi kegiatan tanpa izin, dan untuk menentukan keefektivan langkah-langkah keamanan yang diambil. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 7.7.1 | Apakah jejak audit yang merekam pengecualian dan peristiwa terkait keamanan lainnya dibuat dan dijaga untuk membantu penelitian di masa depan dan dalam pemantauan kendali akses? |  |  |
| 7.7.2 | Apakah prosedur-prosedur sudah disusun untuk penggunaan sistem pemantauan untuk memastikan bahwa para pengguna sudah secara eksplisit mendapat izin? |  |  |
| 7.7.3 | Untuk memastikan keakuratan catatan audit, apakah jam komputer atau alat komunikasi sudah diatur menurut standar yang sudah disepakati? |  |  |
|  |  |  |  |
| **Klausula 8 : Pengembangan dan Pemeliharaan Sistem** | | | |
| **8.1** | **Persyaratan Keamanan Sistem-Sistem** |  |  |
|  | Untuk memastikan bahwa keamanan dibangun di dalam sistem TI, persyaratan keamanan harus diidentifikasi, dibenarkan, disetujui, dan didokumentasi sebagai bagian dari tahapan definisi persyaratan dari semua proyek pengembangan sistem TI. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 8.1.1 | Apakah analisis persyaratan keamanan menjadi bagian dari tahapan analisis persyaratan dari setiap proyek pembangunan? |  |  |
| **8.2** | **Keamanan dalam Sistem Aplikasi** |  |  |
|  | Kendali keamanan yang mematuhi standar industri praktik keamanan yang baik yang umumnya diterima harus dirancang ke dalam sistem aplikasi untuk mencegah penghilangan, perubahan, atau penyalahgunaan data pengguna. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 8.2.1 | Apakah data yang dimasukkan dalam sistem aplikasi divalidasi untuk memastikan bahwa data itu benar dan sesuai? |  |  |
| 8.2.2 | Apakah pemeriksaan validasi sudah dimasukkan ke dalam sistem untuk mendeteksi korupsi yang disebabkan oleh pemrosesan kesalahan atau melalui tindakan yang disadari? |  |  |
| 8.2.3 | Apakah autentikasi pesan sudah dipertimbangkan untuk aplikasi yang melibatkan transmisi data yang peka? |  |  |
| 8.2.4 | Apakah data yang menjadi keluaran sistem aplikasi divalidasi untuk memastikan bahwa data itu benar dan cocok? |  |  |
| **8.3** | **Kendali Kriptografis** |  |  |
|  | Untuk melindungi kerahasiaan, autentisitas, atau keterpaduan informasi, sistem kriptografis dan teknik harus digunakan untuk melengkapi perlindungan informasi yang dianggap beresiko. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 8.3.1 | Apakah manajemen sudah mengembangkan sebuah kebijakan tentang penggunaan kendali kriptografis, termasuk manajemen kunci-kunci enkripsi, dan implementasi yang efektif? |  |  |
| 8.3.2 | Apakah enkripsi data dipakai untuk melindungi data yang sangat peka selama pemindahan atau dalam penyimpanan? |  |  |
| 8.3.3 | Apakah tersedia layanan non-penyangkalan ketika perselisihan mungkin muncul akibat penggunaan enkripsi atau tanda tangan digital? |  |  |
| 8.3.4 | Apakah sistem manajemen tersedia untuk mendukung penggunaan teknik kriptografis organisasi, termasuk teknik kunci yang rahasia dan teknik kunci yang umum? |  |  |
| **8.4** | **Keamanan Arsip-Arsip Sistem** |  |  |
|  | Untuk memastikan bahwa proyek-proyek TI dan kegiatan pendukung dilakukan dengan cara aman, tanggung jawab untuk mengendalikan akses terhadap arsip-arsip sistem aplikasi harus diberikan pada dan dilakukan oleh fungsi pengguna pemilik atau kelompok pengembang.. | | |
| 8.4.1 | Apakah kendali ketat diterapkan pada implementasi peranti lunak pada sistem operasi? |  |  |
| 8.4.2 | Apakah semua data tes sistem aplikasi dilindungi atau dikendalikan? |  |  |
| 8.4.3 | Untuk mengurangi potensi korupsi program-program komputer, apakah akses untuk memrogram perpustakaan sumber dikendalikan secara ketat? |  |  |
| **8.5** | **Keamanan dalam Lingkungan Pengembangan dan Dukungan** |  |  |
|  | Lingkungan proyek dan dukungan harus secara ketat dikendalikan untuk menjaga keamanan peranti lunak dan data sistem aplikasi. | | |
| 8.5.1 | Apakah prosedur kendali perubahan resmi sudah diimplementasikan? |  |  |
| 8.5.2 | Apakah sistem aplikasi ditinjau ketika perubahan-perubahan sistem operasi terjadi? |  |  |
| 8.5.3 | Apakah modifikasi terhadap peranti yang dipasok penjual dihalangi, dan ketika modifikasi sedemikian diperlukan, apakah modifikasi itu dikendalikan secara ketat? |  |  |
| 8.5.4 | Untuk menghindari kanal terlindung atau kode-kode Trojan, apakah organisasi:  ● Membeli program hanya dari sumber yang dikenal;  ● Membeli program yang kode sumbernya dapat diperiksa;  ● Hanya menggunakan produk-produk yang dievaluasi;  ● Memeriksa semua kode sumber sebelum digunakan;  ● Mengendalikan akses terhadap, dan perubahan pada, kode yang dipasang  ● Mempekerjakan staf yang dipercaya untuk mengurusi sistem kunci |  |  |
| 8.5.5 | Ketika pengembangan peranti lunak dialihdayakan, apakah hal-hal rinci sudah diatur untuk melindungi proyek dari kepemilikan intelektual untuk pra-pengujian sebelum pemasangan? |  |  |
| **Klausula 9 : Manajemen Kelangsungan Bisnis** | | | |
| **9.1** | **Aspek-Aspek Perencanaan Keberlanjutan Bisnis** |  |  |
|  | Rencana-rencana keberlanjutan bisnis harus tersedia untuk menghadapi gangguan terhadap aktivitas bisnis. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 9.1.1 | Apakah ada proses yang ditata untuk mengembangkan/memelihara rencana keberlanjutan bisnis di seluruh organisasi? |  |  |
| 9.1.2 | Apakah sebuah strategi sudah dikembangkan untuk menentukan keseluruhan pendekatan terhadap keberlanjutan usaha, dan didukung oleh manajemen? |  |  |
| 9.1.3 | Apakah proses perencanaan keberlanjutan bisnis mencakup identifikasi dan kesepakatan atas semua tanggung jawab dan prosedur kedaruratan? |  |  |
| 9.1.4 | Apakah kerangka kerja rencana keberlanjutan bisnis dipertahankan untuk memastikan bahwa semua tingkatan rencana itu konsisten? |  |  |
| 9.1.5 | Apakah rencana keberlanjutan bisnis diuji secara teratur untuk memastikan bahwa rencana-rencana itu mutakhir dan efektif? |  |  |
|  |  |  |  |
| **Klausula 10 : Kepatuhan** | | | |
| **10.1** | **Kepatuhan Pada Persyaratan Hukum** |  |  |
|  | Semua persyaratan terkait untuk setiap sistem TI harus didefinisikan dan didokumentasikan. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 10.1.1 | Apakah semua hukum terkait, peraturan, dan persyaratan kontrak secara khusus didefinisikan dan didokumentasikan untuk setiap sistem informasi? |  |  |
| 10.1.2 | Apakah ada kepatuhan pada pembatasan hukum menyangkut penggunaan materi hak cipta yang memastikan bahwa hanya peranti lunak yang dikembangkan oleh organisasi, atau dilisensi atau disediakan oleh pengembang untuk organisasi, yang digunakan? |  |  |
| 10.1.3 | Apakah rekaman organisasi yang penting disimpan secara aman untuk memenuhi persyaratan perundangan, maupun untuk mendukung kegiatan bisnis yang penting? |  |  |
| 10.1.4 | Apakah aplikasi yang memroses data pribadi seseorang mematuhi peraturan perlindungan data terkait? |  |  |
| 10.1.5 | Apakah fasilitas-fasilitas TI hanya digunakan untuk tujuan bisnis? |  |  |
| 10.1.6 | Apakah sudah pernah meminta nasihat mengenai kepatuhan organisasi pada hukum nasional dan internasional tentang kendali kriptografis? |  |  |
| 10.1.7 | Ketika tindakan terhadap seseorang melibatkan hukum, apakah peraturan-peraturan untuk bukti sudah dipatuhi untuk keberterimaan, kualitas, dan kelengkapan? |  |  |
| **10.2** | **Tinjauan Kebijakan Keamanan dan Kepatuhan Teknis** |  |  |
|  | Untuk memastikan kepatuhan sistem TI pada kebijakan dan standar keamanan organisasi, tinjauan terhadap kepatuhan harus dilakukan secara teratur. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 10.2.1 | Apakah semua hukum terkait, peraturan, dan persyaratan kontrak secara khusus didefinisikan dan didokumentasikan untuk setiap sistem informasi? |  |  |
| 10.2.2 | Apakah ada kepatuhan pada pembatasan hukum menyangkut penggunaan materi hak cipta yang memastikan bahwa hanya peranti lunak yang dikembangkan oleh organisasi, atau dilisensi atau disediakan oleh pengembang untuk organisasi, yang digunakan? |  |  |
| **10.3** | **Pertimbangan Audit Sistem** |  |  |
|  | Harus ada kendali atas sistem operasional dan perangkat audit sepanjang dilakukannya audit sistem untuk mengurangi gangguan pada dan dari proses audit sistem, dan untuk melindungi keterpaduan dan mencegah penyalahgunaan perangkat audit. | | |
| **No.** | **Pertanyaan** | **Jawaban** | |
| **Ya** | **Tidak** |
| 10.3.1 | Apakah audit dan kegiatan menyangkut pemeriksaan atas sistem operasional direncanakan dan diatur secara cermat? |  |  |
| 10.3.2 | Apakah akses terhadap perangkat audit sistem dikendalikan? |  |  |