PENGUKURAN TINGKAT KAPABILITAS

Nama :

Jabatan :

|  |
| --- |
| Kolom pencapaian diisi dengan menimbang pencapaian aktivitas dengan:* 0 untuk aktivitas yang tidak/belum diimplementasikan
* 1 untuk aktivitas yang telah diimplementasikan
 |

EDM03

EDM03.01 Evaluasi manajemen risiko

|  |
| --- |
| Praktik Tata Kelola |
| Secara terus menerus memeriksa dan mengevaluasi efek risiko penggunaan IT di perushaan pada saat ini dan masa mendatang. Mempertimbangkan apakah selera risiko perusahaan sesuai dan memastikan bahwa risiko pada nilai perusahaan mengenai penggunaan IT teridentifikasi dan terkendali. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Memahami perusahan dan konteksnya yang berhubungan deng T&I | 2 |  |  |
| 2. | Menentukan cakupan risiko dari organisasi tersebut, yaitu tingkat risiko terkait T&I yang bersedia diambil oleh perusahaan dalam mengejar tujuan perusahaan  |  |  |
| 3. | Menentukan level toleransi risiko terhadap selera/cakupan risiko, yaitu penyimpangan semetara dari selera/cakupan risiko. |  |  |
| 4.  | Menentukan sejauh mana *alignment* strategi risiko TI terhadap strategi risiko perusahaan dan memastikan selera risiko di bawah kapasitas risiko organisasi |  |  |
| 5.  | Secara proaktif mengevaluasi faktor risiko I&T sebelum dan memastikan bahwa pertimbangan risiko adalah bagian dari proses keputusan strategis perusahaan | 3 |  |  |
| 6. | Mengevaluasi aktifias manajemen risiko untuk memastikan keselarasan dengan kapasitass perusahaan untuk kerugian menyangkut T&I dan toleransi kepemimpinan terhadapnya. |  |  |
| 7.  | Memikat dan mempertahankan *skill* personel yang diperlukan untuk Manajemen Risiko I&T |  |  |

EDM03.02 Mengarahkan manajemen risiko

|  |
| --- |
| Praktik Tata Kelola |
| Mengarahkan penetapan praktik manajemen risiko untuk menyediakan jaminan yang masuk akal bahwa praktik manajemen risiko TI sudah sesuai dan bahwa risiko TI yang sesungguhnya tidak melebihi selera risiko dewan. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan kegiatan operasional. | 2 |  |  |
| 2. | Mengarahkan perkembangan dari rencana komunikasi risiko (mencakup seluruh level di perusahaan) |  |  |
| 3.  | Implementasi langssung dari mekanisme yang baik untuk merespon secara cepat untuk mengubah risiko dan melaporkan  |  |  |
| 4. | Mengarahkan bahwa risiko, peluang adalah masalah dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa saja kepada pihak yang tepat setiap saat. risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan diteruskan kepada pengambil keputusan yang relevan. |  |  |
| 5. | Mengidentifikasi tujuan dan metrik utama dari proses tata kelola dan manajemen risiko yang akan dipantau, dan menyetujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran. | 3 |  |  |

EDM03.03 Mengawasi manajemen risiko

|  |
| --- |
| Praktik Tata Kelola |
| Meninjau tujuan utama dan matriks dari proses manajemen risiko. Menentukan bagaimana penyimpangan atau masalah akan diidentifikasi, dilacak dan dilaporkan untuk perbaikan. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Melaporkan semua kendala manajemen risiko kepada komite eksekutif. | 2 |  |  |
| 2. | Memantau sejauh mana profil risiko dikelola dalam ambang batas toleransi risiko perusahaan. | 3 |  |  |
| 3.  | Memantau tujuan utama dan metrik proses tata kelola dan manajemen risiko terhadap target, menganalisis penyebab penyimpangan, dan memulai tindakan perbaikan untuk mengatasi penyebab yang mendasarinya | 4 |  |  |
| 4. | Memungkinkan *stakehoder* untuk meninjau kemajuan perusahaan menuju tujuan tertentu/diidentifikasi. |  |  |

APO12

APO12.01 Mengumpulkan data

|  |
| --- |
| Praktik Manajemen |
| Mengidentifikasi dan mengumpulkan data yang relevan untuk memungkinkan identifikasi, analisis, dan pelaporan risiko terkait TI yang efektif. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Menetapkan dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko TI. | 2 |  |  |
| 2. | Merekam data terkait risiko TI yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan. |  |  |
| 3. | Mengadopsi atau menentukan taksonomi/pengelompok risiko untuk definisi skenario risiko dan kategori dampak dan kemungkinan yang konsisten. | 3 |  |  |
| 4.  | Merekam data tentang kejadian risiko yang telah menyebabkan atau dapat menyebabkan dampak bisnis sesuai dengan kategori dampak yang ditentukan dalam taksonomi risiko. Menangkap data yang relevan dari kendala, insiden, masalah, dan investigasi terkait. |  |  |
| 5.  | Mensurvei dan menganalisis riwayat data risiko IT dan *loss experience* dari data eksternal yang tersedia dan tren, rekan industri berdasarkan *event logs* berbasis industri, database, dan penjanjian/kesepakat industri untk pengungkapan peristiwa/kejadian umum. | 4 |  |  |
| 6. | Untuk kejadian dengan kelas serupa, menususn data yang sudah terkumpul dan menyorot faktor yang berkontribusi. Menetukan faktor umum yang berkontribusi di berbagai kejadian. |  |  |
| 7.  | Menentukan kondisi spesifik yang ada maupun yang tidak ketika peristiwa/kejadian risiko terjadi dan bagaimana kondisi tersebut mempengaruhi frekuensi peristiwa/kejadian dan besarnya kerugian. |  |  |
| 8. | Melaksanakan analisis peristiwa/kejadian dan faktor risiko secara berkala untuk mengidentifikasi kendala risiko baru atau yang akan timbul untuk mendapatkan pemahaman mengenai faktor-faktor risiko internal dan eksternal yang terkait. |  |  |

APO12.02 Menganalisis risiko

|  |
| --- |
| Praktik Manajemen |
| Mengembangkan pandangan yang kuat pada risiko TI yang sebenarnya., untuk mendukung keputusan risiko. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Menentukan ruang lingkup yang tepat dari upaya analisis risiko, dengan mempertimbangkan semua faktor risiko dengan/atau kekritisan bisnis aset. | 3 |  |  |
| 2. | Membangun dan memperbarui skenario risiko TI secara teratur; paparan kerugian terkait TI; dan skenario mengenai risiko reputasi, termasuk skenario gabungan dari peristiwa ancaman yang benjenjang dan/atau kebetulan.mengembangkan ekspektasi untuk aktivitas kontrol spesifik dan kemampuan untuk mendeteksi. |  |  |
| 3. | Memperkirakan frekuensi (kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI. Memperhitungkan seluruh faktor risiko yang berlaku dan mengevaluasi kontrol operasional yang diketahui. |  |  |
| 4.  | Membandingkan risiko saat ini (paparan kerugian terkait TI) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko tinggi atau tidak dapat diterima. |  |  |
| 5.  | Mengusulkan respon risiko untuk risiko yang melebihi selera serta tingkatan toleransi. |  |  |
| 6. | Menspesifikasi persyaratan tingkat tinggi proyek atau program yang akan menerapkan respon risiko yang dipilih. Mengidentifikasi persyaratan dan ekspektasi untuk kontrol kunci/utama yang sesuai. |  |  |
| 7.  | Memvalidasi hasil analisis risiko dan hasil analisis dampak bisnis sebelum menggunakannya dalam pengambilan keputusan. Mengkonfirmasi bahwa analisis sejalan dengan persyaratan perusahaan dengan memverifikasi bahwa estimasi telah disesuaikan dan diteliti untuk bias/prasangka. | 4 |  |  |
| 8. | Menganalisis biaya/manfaat dari opsi respon risiko potensial seperti menghindari, mengurangi, mentransfer/membagikan, dan menerima serta mengeksploitasi/merebut. Mengkonfirmasi respon risiko yang optimal | 5 |  |  |

APO12.03 Menjaga profil risiko

|  |
| --- |
| Praktik Manajemen |
| Memelihara inventaris risiko yang diketahui dan atribut-atribut risiko, termasuk sebeerapa sering, dampak potensial dan responnya. Sumber daya terkait dokumen, kapabilitas dan aktivitas kontrol saat ini yang terkait dengan item risiko. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Inventarisasi proses bisnis dan dokumen tentang proses manajemen informasi TI dan sumber daya TI. | 2 |  |  |
| 2. | Menentukan dan menyetujui layanan TI dan infrastruktur TI mana yang esensial untuk mempertahankan operasi proses bisnis. Menganalisis ketergantungan dan mengidentifikasi link yang lemah. |  |  |
| 3. | Mengumpulkan skenario risiko saat ini berdasarkan kategori, jalur bisnis dan area fungsional. |  |  |
| 4.  | Merekam profil informasi seluruh risiko secara berkala/reguler. | 3 |  |  |
| 5.  | Merekam informasi tentang status tindakan risiko. |  |  |
| 6. | Berdasarkan seluruh data profil risiko, mendefinisikan satu set indikator risiko yang memungkinkan pemantauan serta cepat teridentifikasinya risiko saat ini maupun kecenderungan risiko. | 4 |  |  |
| 7.  | Merekam informasi mengenai kejadian risiko TI yang telah termaterialisasi guna penyertaan dalam profil risiko TI. |  |  |

APO12.04 Mengartikulasikan risiko

|  |
| --- |
| Praktik Manajemen |
| Mengkomunikasikan informasi tentang paparan terkait TI pada kondisi/keadaan/status saat ini dan peluang pada waktu yang tepat untuk mendapatkan respon yang baik pada seluruh *stakeholder* yang bersangkutan. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Melaporkan hasil analisis risiko kepada seluruh *stakeholder* yang terkena dampak dalam ketentuan dan format yang berguna untuk mendukung keputusan perusahaan. Bila memungkinkan, tambahkan probabilitas dan kisaran untung rugi bersama dengan tingkat kepercayaan untuk memungkinkan manajemen untuk menyeimbangkan *risk-return.* | 3 |  |  |
| 2. | Menyediakan pembuat keputusan pemahaman mengenai *worse-case* dan skenario yang paling memungkinkan, paparan kerugian mengenai TI dan reputasi yang signifikan, regulasi yang legal dan sudah dipertimbangkan, mapun kategori dampak mana saja per taksonomi risiko. |  |  |
| 3. | Melaporkan profil risiko saat ini pada seluruh *stakeholder*.Tambahkan informasi mengenai keefektifan dari proses manajemen risiko. Kefektifan kontrol, *gaps*, ketidak-konsistenan, perbaikan status dan damaknya pada profil risiko. |  |  |
| 4.  | Pada basis berkala, untuk area/wilayah dengan risiko relatif dan keseimbangan kapasitas risiko, identifikasi peluang yang berkaitan dengan TI yang memungkinkan penerimaan risiko yang lebih besar dan meningkatkan pertumbuhan dan laba. |  |  |
| 5.  | Meninjau hasil penilaian objektif dari pihak ketiga dan *internal audit* serta tinjauan jaminan kualitas. Sertakan mereka dalam profil risiko. Meninjau *gaps*  yang teridentifikasi dan paparan kerugian terkait TI untuk menentukan apakah analisis risiko tambahan dibutuhkan. | 4 |  |  |

APO12.05 Menentukan portfolio tindakan manajemen risiko

|  |
| --- |
| Praktik Manajemen |
| Mengelola peluang untuk mengurangi risiko ke tingkat yang dapat diterima sebagai portfolio. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Memelihara inventarisasi aktivitas pengendalian yang ada untuk memitigasi risiko dan yang memungkinkan risiko diambil sesuai dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas kontrol dan memetakannya ke skenario risiko TI. | 2 |  |  |
| 2. | Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portfolionya. | 3 |  |  |
| 3. | Menentukan satu set proposal proyek seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang strategis perusahaan, dengan mempertimbangkan biaya, manfaat, efek pada profil risiko dan peraturan saat ini. |  |  |

APO12.06 Respon kepada risiko

|  |
| --- |
| Praktik Manajemen |
| Merespon secara tepat waktu terhadap peristiwa risiko yang terwujud dengan langkah-langkah efektif untuk membatasi besarnya kerugian. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika peristiwa risiko dapat menyebabkan insiden operasional maupun pengembangan yang signifikan dengan dampak bisnis yang serius. Memastikan bahwa rencana tersebut mencakup jalur peningkatan/pengembangan di seluruh perusahaan. | 3 |  |  |
| 2. | Menerapkan rencana reespon yang tepat untuk meminimalkan dampak bisnis ketika insiden risiko terjadi. |  |  |
| 3. | Mengkategorikan insiden dan membandingkan paparan kerugian terkait TI dengan ambang batas toleransi risiko. Mengkomunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari pelaporan dan melakukan pengkinian profil risiko. | 4 |  |  |
| 4.  | Memeriksa kejadian buruk/kerugian masa lalu dan peluang yang terlewatkan dan menentukan akar penyebabnya. |  |  |
| 5.  | Mengkomunikasikan akar penyebab, persyaratan respon risiko tambahan dan perbaikan prosess kepada pembuat keputusan yang tepat. Memastikan bahwa penyebab, persyarata respon, dan peningkatan proses disertakan dalam proses tata kelola risiko. | 5 |  |  |

DSS03

DSS03.01 Mengidentifikasi dan mengklasifikasi masalah

|  |
| --- |
| Praktik Manajemen |
| Menentukan dan mengimplementasikan kriteria serta prosedur untuk mengidentifikasi dan melaporkan masalah. Sertakan klasifikasi masalah dan, pengkategorisasian dan prioritasnya. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Mengenali masalah melalui korelasi laporan masalah, *error logs*, dan identifikasi masalah sumber daya lainnya. | 2 |  |  |
| 2. | Secara formal menangani semua masalah dengan akses ke seluruh data relevan.termasuk informasi dari manajemen perubahan sistem TI dan konfigurasi TI/aset serta detail-detail kejadian. |  |  |
| 3. | Menentukan grup pendukung yang tepat untuk membantu dalam pengidentifikasian masalah, analisa akar masalah dan penentuan solusi untuk mendukung manajemen masalah. Menentukan grup pendukung bersadarkan kategori yang sudah ditentukan, seperti perangkat keras, jaringan, *network*, perangkat lunak, aplikasi dan perangkat lunak pendukung. |  |  |
| 4.  | Menentukan tingkatan prioritas melalui konsultasi bisnis untuk memastikan bahwa identifikasi masalah dan analisis akar masalah ditangani secara tepat waktu menurut SLA. Berdasarkan tingkat prioritas pada dampak dan kepentingan bisnis. |  |  |
| 5.  | Melaporkan status dari masalah yang teridentifikasi ke meja layanan sehingga baik *customer* maupun manajemen TI tetap terinformasi. |  |  |
| 6. | Mempertahankan satu katalog manajemen masalah untuk didaftarkan serta melaporkan masalah yang teridentifikasi. Menggunakan katalog tersebut untuk membuat jejak audit dari proses manajemen masalah, termasuk status dari tiap-tiap masalah (contoh: buka, buka ulalng, dalam pengerjaan atau ditutup). |  |  |

DSS03.02 Menginvestigasi dan mendiagnosa masalah

|  |
| --- |
| Praktik Manajemen |
| Menyelidiki dan mendiagnosa masalah menggunakan ahli materi yang relevan untuk menilai dan menganalisa akar masalah |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1.  | Mengenali masalah yang mungkin adalah error yg telah diketahui dengan membandingkan data kejadian dengan basis data dari error yang diketahui dan dicurigai (misal : yang dikomunikasikan oleh vendor - vendor eksternal). Klasifikasikan masalah sebagai error yang diketahui. | 3 |  |  |
| 2. | Mengelompokkan item konfigurasi yang terpengaruh ke error yang telah ditetapkan/diketahui. |  |  |
| 3. | Membuat laporan untuk memberitahukan kemajuan dalam penyelesaian masalah dan memantau dampak berkelanjutan dari masalah yang belum diselesaikan. Memantau status dari proses penanganan masalah melalui siklus hidupnya, termasuk input dari manajemen perubahan dan konfigurasi IT. |  |  |

DSS03.03 Meningkatkan eror yang diketahui

|  |
| --- |
| Praktik Manajemen |
| Segera setelah akar masalah dikenali, buat catatan error yang diketahui, dokumentasikan solusi yang sesuai dan kenali solusi yang potensial. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Segera setelah akar sebab dari masalah dikenali, buat catatan error yang diketahui dan kembangkan solusi yang cocok. | 2 |  |  |
| 2. | Kenali, evaluasi, prioritaskan dan proses (melalui Manajemen perubahan IT) solusi untuk error yang diketahui, berdasarkan biaya/keuntungan kasus bisnis dan dampak dan urgensi bisnis. | 3 |  |  |

DSS03.04 Menyelesaikan dan menutup masalah

|  |
| --- |
| Praktik Manajemen |
| Kenali dan menginisiasi solusi berkelanjutan untuk mengatasai akar masalah. Tingkatkan permintaan pengubahan melalui proses manajamen perubahan yang sudah didirikan. , jika diperlukan,untuk menyelesaikan masalah. Pastikan bahwa personel yang terlibat sadar dengan tindakan yang diambil dan merencanakan pengembangan untuk mencegah insiden terjadi di masa depan. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Tutup rekaman/catatan masalah, baik setelah konfirmasi keberhasilan eliminasi masalah yang diketahui atau setelah persetujuan dengan pihak bisnis tentang cara alternatif penanganan masalah. | 2 |  |  |
| 2. | Memberitahukan meja layanan tentang jadwal penutupan masalah (misal : Jadwal perbaikan masalah yang diketahui, kemungkinan solusi atau fakta bahwa masalah akan tetap ada hingga pengubahan diterapkan) dan konsekuensi dari pendekatan yang diambil. Menjaga pengguna dan pelanggan yang terlibat tetap terinformasi dengan sesuai. |  |  |
| 3. | Melalui proses resolusi, peroleh catatan berkala dari manajemen perubahan IT tentang kemajuan dalam penyelesain masalah dan error. | 3 |  |  |
| 4. | Memantau dampak berkelanjutan atas masalah dan error yang diketahui dalam layanan. | 4 |  |  |
| 5. | Meninjau dan mengkonfirmasi keberhasilan resolusi dari masalah utama. |  |  |
| 6 | Memastikan ilmu yang dipelajari dari ulasan dimasukkan ke dalam rapat tinjauan layanan dengan pelanggan bisnis | 5 |  |  |

DSS03.05 Melakukan manajemen masalah proaktif

|  |
| --- |
| Praktik Manajemen |
| Mengumpulkan dan menganalisa data operasional (khususnya catatan insiden dan perubahan) untuk mengidentifikasi tren baru yang muncul yang mungkin mengindikasikan masalah. *Log* (catat) rekaman masalah untuk memungkinkan penilaian. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Merekam informasi masalah yang terkait dengan perubahan dan insiden I&T serta mengkomunikasikannya kepada *stakeholders* utama. Mengkomunikasikan melalui laporan dan pertemuan/rapat berkala antara, insiden, masalah, perubahan, dan konfigurasi pemilik proses manajemen untuk mempertimbangkan masalah terkini dan tindakan korektif yang potensial. | 3 |  |  |
| 2. | Pastikan bahwa pemilik proses dan manajer dari insiden, masalah, perubahan, dan manajemen konfigurasi bertemu secara teratur untuk mendiskusikan masalah yang diketahui dan rencana perubahan di masa depan. |  |  |
| 3. | Mengidentifikasi dan menginisiasi solusi berkelanjutan (perbaikan permanen) untuk mengatasi akar penyebab utama. Tingkatkan permintaan melalui proses manajemen perubahan yang stabil/mapan. |  |  |
| 4. | Untuk memungkinkan perusahaan memantau total biaya dari masalah-masalah, rekam/catat upaya perubahan yang dihasilkan dari aktivitas proses manajemen masalah (misalnya, perbaikan masalah dan kesalahan yang diketahui) dan melaporkannya pada perusahaan. | 4 |  |  |
| 5. | Membuat laporan untuk memantau penyelesaian masalah terhadap persyaratn bisnis dan SLA. Memastikan peningkatan masalah yang tepat, seperti peningkatan ke level manajemen yang lebih tinggi sesuai dengan kriteria yang disepakati, menghubungi vendor eksternal, atau mengacu pada dewan penasihat perubahan untuk meningkatkan prioritas permintaan mendesak untuk perubahan (RFC) untuk menerapkan solusi sementara.  |  |  |
| 6 | Untuk mengoptimalkan penggunaan sumber daya dan mengurangi celah, melacak tren masalah. |  |  |

DSS05

DSS05.01 Melindungi dari software berbahaya

|  |
| --- |
| Praktik Manajemen |
| Menerapkan dan memelihara tindakan pencegahan, pendeteksian, dan korektif (terutama patch keamanan terbaru dan pengendalian virus) di selruh perusahaan untuk melindungi sistem dan teknologi informasi dari perangkat lunak berbahaya (Contoh; *ransomware, malware, virus, worm, spyware, spam*). |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Menginstall dan mengaktifkan alat perlindungan perangkat lunak berbahaya di semua fasilitas pemrosesan, dengan file defiisi perangkat lunak berbahaya yang diperbarui sesuai kebutuhan (otomatis atau semi otomatis). | 2 |  |  |
| 2. | Menyaring lalu lintas, seperti email dan unduhan untuk melindungi dari informasi yang tidak diminta (misalnya, *spyware*, email *phising*). |  |  |
| 3. | Mengkomunikasikan kesadaran perangkat lunak berbahaya dan menegakkan prosedur dan tanggung jawab penegahan. Melakukan pelatihan berkala tentang malware dalam penggunaan email dan internet. Melatih pengguna untuk tidak membuka, tapi melaporkan, email yang mencurigakan dan untuk tidak menginstall perangkat lunak yang dibagikan/tidak disetujui. | 3 |  |  |
| 4. | Mendistribusikan perangkat lunak perlindungan secara terpusat (versi dan tingkat patch) menggunakan konfigurasi terpusat dan manajemen perubahan TI. |  |  |
| 5. | Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau produk vendor dan saran layanan keamanan). | 4 |  |  |

DSS05.02 Mengelola keamanan jaringan dan konektivitas

|  |
| --- |
| Praktik Manajemen |
| Menggunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi melalui seluruh metode konektifitas. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Hanya mengizinkan perangkat yang berwenang untuk memiliki akses ke informasi perubahan dan jaringan perusahaan. Mengkonfigurasi perangkat ini untuk memaksa entri kata sandi. | 2 |  |  |
| 2. | Menerapkan mekanisme penerapan jaringan, seperti firewall dan perangkat lunak pendeteksi gangguan. Melaksanakan kebijakan yang tepat untuk mengontrol lalu lintas masuk dan keluar. |  |  |
| 3. | Menereapkan protokol keamanan yang disetujui ke konektivitas jaringan. |  |  |
| 4. | Mengkonfigurasikan peralatan jaringan dengan cara yang aman. |  |  |
| 5. | Mengenkripsi informasi dalam perjalanan sesuai dengan klasifikasinya. | 3 |  |  |
| 6. | Berdasarkan penilasan risiko dan persyaratan bisnis, buat dan pertahankan kebijakan untuk keamanan konektivitas. |  |  |
| 7. | Membangun mekanisme terpercaya untuk mendukung transmisi dan penerimaan informasi yang aman. |  |  |
| 8. | Melakukan pengujian penetrasi berkala untuk menentukan perlindungan jaringan yang memadai. | 4 |  |  |
| 9. | Melakukan pengujian keamanan sistem secara berkala untuk menentukan perlindungan sistem yang memadai. |  |  |

DSS05.03 Mengelola keamanan endpoint

|  |
| --- |
| Praktik Manajemen |
| Memastikan bahwa *endpoints* (misalnya, laptop, desktop, server, perangkat seluler dan jaringan lainnya atau perangkat lunak) diamankan pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditentukan untuk informasi yang diproses, disimpan, atau dikirim. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Mengkonfigurasi dengan cara yang aman. | 2 |  |  |
| 2. | Menerapkan mekanisme penguncian perangkat. |  |  |
| 3. | Mengelola *remote access* dan kontrol (contoh, perangkat lunak, teleworking). |  |  |
| 4. | Mengelola konfigurasi jaringan dengan cara yang aman. |  |  |
| 5. | Menerapkan penyaringan lalu lintas jaringan pada perangkat *endpoint*. |  |  |
| 6. | Melindungi integritas sistem. |  |  |
| 7. | Menyediakan perlindungan fisik pada perangkat *endpoint*. |  |  |
| 8. | Membuang perangkat *endpoint* dengan aman. |  |  |
| 9. |  Mengelola akses berbahaya melalui email dan browser web. Misalnya, memblokir situs tertentu dan menonaktifkan klik-tayang pada tautan untuk *smartphone*. |  |  |
| 10. | Mengenkripsi informasi dalam penyimpanan berdasarkan klasifikasinya. | 3 |  |  |

DSS05.04 Mengelola identitas pengguna dan *logical access*

|  |
| --- |
| Praktik Manajemen |
| Memastikan bahwa semua pengguna memiliki hak akses informasi sesuai dengan persyaratan bisnis. Berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Menjaga hak akses pengguna sesuai dengan fungsi bisnis, persyaratan proses dan kebijakan keamanan, menyelaraskan pengelolaan identitas dan hak akses dengan peran serta tanggung jawab yang ditentukan, berdasarkan pada prinsip *least-privilege*, *need-to-have* *need-to-know* (hak istimewa paling rendah, wajib dimiliki, wajib tahu). | 2 |  |  |
| 2. | Mengelola semua perubahan hak akses (pembuatan, modifikasi, dan penghapusan) secara tepat waktu, berdasarkan hanya pada transaksi yang telah disetujui dan didokumentasikan serta diotorisasi oleh individu manajemen yang dituju.  | 3 |  |  |
| 3. | Memisahkan, kurangi hingga jumlah minimum yang diperlukan dan secara aktif mengatur akun pengguna dengan *privilege*. Memastikan pemantauan di semua aktivitas pada akun ini.  |  |  |
| 4. | Secara unik mengidentifikasi semua aktivitas pemrosesan informasi berdasarkan peran fungsional. Berkoordinasi edngan unit bisnis untuk memastikan bahwa seluruh peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam penerapan proses bisnis. |  |  |
| 5. | Mengotentifikasi semua akses ke aset informasi berdasarkan peran individu ataupun aturan bisnis. Berkoordinasi dengan unit bisnis yang mengelola otentifikasi aplikasi yang digunakan dalam proses bisnis untuk memastikan bahwa kontrol otentifikasi telah dikelola dengan benar. |  |  |
| 6. | Memastikan bahwa semua pengguna (internal, eksternal, dan sementara) dan aktivitasnya pada sistem TI (aplikasi bisnis, infrastruktur TI, sistem operasi, pengembangan dan pemeliharaan) dapat diidentifikasi dengan unik. |  |  |
| 7. | Mempertahankan jejak audit akses ke informasi tergantung dengan sensitivitas dan persyaratan peraturannya. | 4 |  |  |
| 8. | Melakukan tinjauan manajemen reguler pada semua akun dan *privilege* terkait. |  |  |

DSS05.05 Mengelola physical access sampai ke aset TI

|  |
| --- |
| Praktik Manajemen |
| Menentukan dan menerapkan prosedur (termasuk prosedur darurat) untuk diberikan, membatasi dan mencabut akses ke wilayah, bangunan dan area, menurut kebutuhan bisnis. Akses ke wilayah, bangunan dan area harus dijustifikasi, diotorisasi/disahkan, dicatat dan diawasi. Persyaratan ini berlaku untuk setiap orang yang masuk ke wilayah, termasuk staf, staf sementara, klien, vendor, pengunjung atau pihak ketiga manapun. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Mencatat dan memantau seluruh *entry points* pada lokasi. Meregistrasi seluruh pengunjung, termasuk kontraktor dan vendor, pada lokasi tersebut. | 2 |  |  |
| 2. | Memastikan seluruh personel menunjukkan/menampakkan identifikasi dengan benar setiap saat. |  |  |
| 3. | Mengharuskan pengunjung untuk dikawal/diiringi setiap saat ketika ada di lokasi. |  |  |
| 4. | Membatasi dan meninjau akses pada lokasi TI yang sensitif dengan menetapkan batasan-batasan perimeter, seperti pagar, dinding dan perangkat keamanan pada pintu interior dan eksterior. |  |  |
| 5. | Mengelola permintaan untuk mengijinkan akses terotorisasi dengan benar pada fasilitas komputasi. | 3 |  |  |
| 6. | Memastikan profil akses tetap terkini. Akses dasar pada lokasi TI (ruang, bangunan, area, zona server) pada fungsi tugas dan tanggung jawab.ntuk |  |  |
| 7. | Mengadakan pelatihan kesadaran keamanan informasi fisik secara berkala. |  |  |

DSS05.06 Mengelola dokumen sensitif dan output perangkat

|  |
| --- |
| Praktik Manajemen |
| Menempatkan *safeguard* yang baik, praktik akuntansi dan manajemen inventaris terkait aset TI sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer dengan tujuan khusus atau token keamaan. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Membuat prosedur untuk mengendalikan tanda terima, menggunakan, menghapus dan membuang dokumen sensitif, dan perangkat *output* pada, di dalam, dan diluar dari perusahaan. | 2 |  |  |
| 2. | Memastikan pengendalian kriptografi tersedia untuk melindungi informasi sensitif yang disimpan elektronik. |  |  |
| 3. | Tetapkan hak akses untuk dokumen sensitif dan perangkat *output* berdasarkan prinsip *least-privilege*, menyeimbangkan risiko dan kebutuhan bisnis. | 3 |  |  |
| 4. | Membangun invtaris untuk dokumen sensitif dan perangkat *output*, dan mengadakan rekonsiliasi berkala. |  |  |
| 5. | Membangun *safeguard* fisik yang baik terhadap dokumen sensitif. |  |  |

DSS05.07 Mengelola kerentanan dan memonitor infrastruktur untuk kejadian terkait keamanan

|  |
| --- |
| Praktik Manajemen |
| Menggunakan portfolio peralatan dan teknologi (Contoh, alat pendeteksi intrusi), mengelola kerentanan dan meninjau infrastruktur untuk akses yang tidak sah/tidak berwenang. Memastikan bahwa peralatan keamanan, teknologi dan pendeteksi terintegrasi dengan pemantauan kejadian umum dan manajemen insiden. |
| No. | Aktivitas | Level | Pencapaian |
| 0 | 1 |
| 1. | Secara kontinu menggunakan portfolio teknologi yang didukung, pelayanan dan aset (contohnya, scanner kerentanan, fuzzer dan sniffer, penganalisis protokol) untuk mengidentifikasi kerentanan keamanan informasi. | 2 |  |  |
| 2. | Menentukan dan mengkomunikasikan skenario risiko, sehingga mereka bisa dengan cepat di kenali, serta kemungkinan terjadi dan dampaknya dapat dipahami. |  |  |
| 3. | Meninjau *event logs* secara teratur untuk menemukan insiden potensial. |  |  |
| 4. | Memastikan bahwa tiket insiden tekait keamanan dibuat secara tepat waktu ketika peninjauan mengidentifikasi insiden potensial. |  |  |
| 5. | *Log* kejadian terkait keamanan dan simpan catatan untuk periode yang sesuai. | 3 |  |  |