KEBIJAKAN DAN PEDOMAN MANAJEMEN ASET TIK

PEMKAB PADANG PARIAMAN

KABUPATEN PADANG PARIAMAN

2023

DAFTAR ISI

DAFTAR GAMBAR

PEDOMAN MANAJEMEN ASET TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK)

Teknologi Informasi dan Komunikasi (TIK) telah menjadi bagian penting dan kritis dari bisnis. Begitu pentingnya bisnis sehingga perusahaanatau organisasiberlomba-lomba untukmemutakhirkan teknologi informasi dankomunikasi beserta proses-proses atau prosedur terkait teknologi informasi. Saat ini, sudah banyak perusahaan atau organisasi yang memiliki aset teknologi informasi. Fokus atau tujuan utama dari memiliki aset tersebut adalah agar bagaimana aset tersebut benar- benar memberikan nilai keuntungan bagi bisnis. Untuk mengaturnya, perusahaan atau organisasi mulai menerapkan tata kelola teknologi informasi dimana aset teknologi informasi dikelola guna mencapai keselarasan antara nilai yang disampaikan teknologi informasi dengan tujuan bisnis.

Aset daerah merupakan sumberdaya penting bagi pemerintah daerah sebagai penopang utama pendapatan asli daerah. oleh karena itu, penting bagi pemerintah daerah untuk dapat mengelola aset secara memadai. Dalam pengelolaan aset, pemerintah daerah harus menggunakan pertimbangan aspek perencanaan kebutuhan dan penganggaran, pengadaan, penerimaan, penyimpanan dan penyaluran, penggunaan, penatausahaan, pemanfaatan atau penggunaan, pengamanan dan pemeliharaan, penilaian, penghapusan, pemindahtanganan, pembinaan, pengawasan dan pengendalian, pembiayaan dan tuntutan ganti rugi agar aset daerah mampu memberika kontribusi optimal bagi pemerintah daerah yang bersangkutan.

Dokumen ini dibuat sebagai pedoman Manajemen Aset TIK pada Pemerintah Kabupaten Padang Pariaman. Aset TIK dikelola untuk setiap siklus hidup dari suatu aset teknologi informasi. Asetteknologi informasi dikelola untukmemastikan bahwa penggunaan dari aset teknologi informasi mampu menyampaikan nilai bagi bisnis pada biaya yangoptimal, sesuai dengan tujuan bisnis, terlindungi secara fisik maupun hukum, dan agar aset yang penting dalam mendukung kapabilitas suatu layanan selalu ada dan dapat digunakan pada saat yang dibutuhkan.

I. Siklus Manajemen Aset TIK

1.1 Perencanaan Aset TIK

1. Perencanaan aset TIK dilakukan pada anggaran tahun sebelumnya, kecuali untuk kebutuhan TIK yang bersif at mendesak dapat dibuat perencanaannya pada tahun anggaran yang berjalan dengan mendapat persetujuan Tim Pengarah SPBE.
2. Unit kerja di Sekretariat Jenderal yang menyelenggar ak an fungsi pengelolaan data, informasi, dan teknologi informasi membuat perencanaan aset TIK Kementer i anberdasarkan arsitektur SPBE dan peta rencana SPBE Kementerian.
3. Unit organisasi, unit kerja, dan unit pelaksana teknis membuat perencanaan aset TIK berdasarkan arsitektu r SPBE dan peta rencana SPBE unit organisasi.
4. Unit organisasi, unit kerja, dan unit pelaksana teknis melakukan koordinasi dengan unit kerja di Sekretar i at Jenderal yang menyelenggarakan fungsi-fun gs ipengelolaan data, informasi, dan teknologi informasi dalam membuat perencanaan aset TIK untuk menghind ar i duplikasi pengadaan aset TIK.
5. Unit kerja di Sekretariat Jenderal yang menyelenggar ak an fungsi pengelolaan data, informasi, dan teknologi informasi melakukan kompilasi seluruh perencanaan aset TIK di Kementerian, serta memastikan tidak terjadi duplikasi perencanaan aset TIK yang bisa berbagi-pakai di Kementerian sebelum menjadi rencana kerja TIK Kementerian tahun berikutnya dan menjadi Daftar Isian Pelaksanaan Anggaran (DIPA).
6. Sebelum ditetapkan menjadi DIPA, rencana kerja TIK unit organisasi, unit kerja, dan unit pelaksana teknis harus mendapatkan persetujuan dari unit kerja di Sekretariat Jenderal yang menyelenggarakan fungsi pengelolaan data, informasi, dan teknologi informasi.
7. Perencanaan aset TIK harus menjelaskan fungsi-fun gs i utama, justifikasi bisnis dan teknis dari aset yang akan diadakan, manfaat (*outcome*), keluaran (*output*), strategi pengadaan, perkiraan anggaran, serta sumber daya manusia dan waktu yang diperlukan, pada setiap Kerangka Acuan Kerja (KAK).

1.2. Pengadaan Aset TIK

a. Setiap kegiatan pengadaan aset TIK didahului dengan rencana kebutuhan aset TIK.
b. Pengadaan aset TIK dilakukan berdasarkan DIPA dan sesuai dengan ketentuan peraturan perundang- undangan.
c. Pengadaan aset TIK yang melibatkan pihak eksternal, baik badan usaha maupun individual, untuk tenaga ahli diwajibkan memiliki sertifikat keahlian yang sesuai dengan kebutuhan.
d. Pengadaan, penerimaan, verifikasi, pengujian, dan pencatatan semua aset TIK dilakukan dengan cara yang terkontrol, termasuk pelabelan fisik sesuai dengan ketentuan peraturan perundang-undangan.
e. Menyetujui pembayaran dan menyelesaikan proses dengan penyedia barang/jasa sesuai dengan kondisi kontrak yang disepakati.
f. Menyebarkan dan mengalokasikan aset TIK sesuai dengan standar siklus hidup pengelolaan barang milik negara, termasuk manajemen perubahan dan pengujia n penerimaan. Realokasi aset ketika tidak lagi diperlukan karena perubahan peran pengguna, redundansi dalam suatu layanan, ataupenghapusan/berhentinya suatu layanan.

1.3 Pengelolaan Aset

1.3.1. Pengelolaan Aset TIK Vital

a. Mengidentifikasi aset TIK vital dalam menyediaka n kapabilitas layanan dengan merujuk definisi layanan, *Service Level Agreement* (SLA), dan sistem manajemen konfigurasi.
b. Secara teratur, pertimbangkan risiko kegagalan atau kebutuhan untuk penggantian setiap aset TIK vital.
c. Berkomunikasi dengan pengguna yang terpengaruh (misalnya pembatasan kinerja) dari aktivitas pemeliharaan.
d. Menggabungkan downtime yang direncanaka n dalam jadwal produksi keseluruhan serta menjadwalkan kegiatan pemeliharaan untuk meminimalkan dampak buruk pada proses bisnis yang didukung oleh aset TIK vital.

e. Memelihara ketahanan aset TIK dengan menerapkan pemeliharaan preventif yang teratur serta memantau kinerja dan jika diperlukan, memberikan aset TIK alternatif dan/atau cadangan untuk meminima lk an kemungkinan kegagalan.
f. Menetapkan rencana pemeliharaan preventif untuk semua perangkat keras, mempertimbangkan analisis biaya/manf aat, rekomendasi pihak eksternal, risiko pemadaman, personel yang berkualifikasi, dan faktor-faktor terkait lainnya.
g. Menetapkan perjanjian pemeliharaan yang melibatkan akses pihak eksternal ke fasilitas TIK Kementerian untuk aktivitas di lokasi dan di
h. luar lokasi berupa kontrak layanan formal yang berisi atau merujuk pada semua kondisi keamanan dan privasi yang dipersyaratkan, termasuk prosedur otorisasi akses.
i. Memastikan bahwa layanan akses jarak jauh dan profil pengguna hanya aktif bila diperlukan.
j. Memantau kinerja aset TIK vital dengan memerik sa tren insiden dan jika diperlukan, pengelo la mengambil tindakan untuk memperbaiki atau mengganti.

1.3.2. Pengelolaan Nilai Aset TIK

a. Meninjau seluruh aset TIK secara berkala dan mempertimbangkan apakah aset TIK tersebut masih selaras dengan kebutuhan Kementerian.
b. Melakukan asesmen terkait biaya pemeliharaan, pertimbangkan kewajaran, dan identifikasi opsi biaya yang lebih rendah, termasuk penggantian dengan alternatif baru.
c. Mempertimbangkan nilai aset TIK dan strategi penggantian aset TIK untuk menentukan opsi biayaterendah.
d. Melakukan pengukuran kapasitas dan pemanf aatan aset TIK untuk mengidentif ikasi aset TIK yang kurang bermanfaat atau yang redundan sehingga dapat dipertimbangkan untuk dihapus atau diganti dalam rangka pengurangan biaya.
e. Meninjau seluruh aset TIK untuk mengidentif ikasi peluang yang dapat menurunkan biaya pengadaan, dukungan, dan pemeliharaan sesuai dengan ketentuan peraturan perundang-undangan.

f. Melakukan kajian untuk mengidentif ikasi peluang pemanfaatan teknologi baru.

1.3.3. Pengelolaan Lisensi

a. Mengelola daftar lisensi perangkat lunak yang dibeli beserta perjanjian lisensinya.
b. Secara berkala, melakukan audit untuk mengidentifikasi semua komponen (*instances*) perangkat lunak berlisensi yang diinstal.
c. Membandingkan jumlah *instances* perangkat lunak yang diinstal dengan jumlah lisensi yang dimiliki dan memastikan penggunaan lisensi sesuai dengan kontrak.
d. Ketika *instances* lebih rendah dari jumlah lisensi yang dimiliki, tentukan apakah mempertahankan atau menghentikan lisensi dengan, mempertimba n g k an pemeliharaan, pelatihan dan biaya lain yang tidak perlu.
e. Ketika *instances* lebih tinggi dari jumlah lisensi yang dimiliki, lakukan *uninstall instances* yang tidak lagi diperlukan, dan kemudian jika perlu beli lisensi tambahan untuk mematuhi perjanjian lisensi.
f. Secara teratur, pertimbangkan apakah nilai yang lebih baik dapat diperoleh dengan *upgrade* produk dan lisensi terkait.

1.4. Pencatatan Aset TIK

a. Mengidentifikasi semua aset TIK yang dimiliki dalam daftar aset TIK yang mencatat status saat ini dan melaporkan aset TIK sesuai dengan ketentuan peraturan perundang-undangan.
b. Mengidentifikasi persyaratan hukum, peraturan, atau kontrak yang perlu dipatuhi ketika mengelola aset TIK sesuai dengan ketentuan peraturan perundang-undangan.
c. Melakukan verifikasi untuk memastikan bahwa aset TIK sesuai dengan tujuannya.
d. Memastikan pertanggungjawaban untuk semua aset TIK.
e. Memverif ikasi keberadaan semua aset TIK yang dimiliki dengan melakukan pemeriksaan dan rekonsiliasi persediaan fisik dan logis secara teratur, termasuk penggunaan alat bantu untuk mengetahui status dan keberadaan perangkat lunak.

f. Memeriksa secara teratur untuk menetapkan apakah setiap aset TIK masih memberikan nilai dan memperkirak an masa umur aset TIKuntuk memberikan nilai sesuai dengan ketentuan peraturan perundang- undangan.

1.5. Penghapusan Aset TIK

a. Merencanakan, memberi wewenang dan menerapkan kegiatan terkait penghapusan aset TIK serta mengelola daftar aset TIK yang sesuai dengan kebutuhan layanan dan ketentuan peraturan perundang- undangan.
b. Menghapus aset TIK yang sudah tidak bermanfaat karena berhentinya/dihapusnya semua layanan terkait, teknolo gi yang sudah usang, atau kurangnya pengguna terkait dengan dampak lingkungan akibat penggunaan teknologi tersebut.
c. Menghapus aset TIK dengan aman, dengan mempertimbangkan, misalnya, penghapusan permanen semua data yang direkam padaperangkat media.
d. Penghapusan aset TIK dari daftar Barang Milik Negara (BMN) sesuai ketentuan peraturan perundan ga n-undangan.

II. Tata Kelola Teknologi Informasi & Komunikasi (TIK)

Tata kelola Teknologi Informasi & Komunikasi memiliki hubungan erat dengan Audit teknologi informasi. Audit Sistem informasi adalah proses pengumpulan dan evaluasi fakta untuk menentukan apakah sistem komputeryang digunakan telah dapat melindungi asset milik organisasi, mampu menjagga integritas data, dapat membantu pencapaian tujuan organisasi yang efektif, serta menggunakan sumber daya yang dimiliki secara efisien. Audit TIK akan memberikan gambarankondisi tertentuyang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap standar yang terdefinisi, dan hasil audit inilah yang digunakan suatu perusahaan atau organisasi untuk mendefinisikan tata kelolanya.

Tata kelola memiliki definisi yang mecakup sistem informasi, teknologi dan komunikasi, bisnis dan hokum, serta isu-isu lain yang melibatkan hampir seluruh stakeholder (direktur, manajemen eksekutif, pemilik proses, manajemen eksekutif, pemilik proses, supplier, pengguna TIbahkan auditor SI/TI). Berdasarkan ITGI, tata kelola TI adalah suatu struktur dan proses yang salingberhubungan serta mengarahkan dan mengendalikan perusahaan dalam pencapaian tujuan perusahaan melalui nilai tambah dan penyeimbangan antara risiko dan manfaat dari teknologi informasi serta prosesnya.

Tata kelola TI penting dilakukan karena saat ini teknologi sudah menjadi hal penting bagi suatu organisasi. TI akan memberikan nilai terhadap bisnis yang didorong oleh penyelarasan TI dengan bisnis. Tata kelola akan memberikan solusi untuk risiko terkait TI serta penentuan penanggungjawab untuk permasalahan tersebut.

Lebih detailnya, dalam tata kelola TI audit juga memiliki peran untuk menganalisasistem yang sedang berjalan dalam suatu perusahaan untuk mencegah terjadinya hal-hal berikut:

- **Kerugian akibat kehilangan data**

Dalam dokumen tata kelola sudah didefinisikan dengan jelas mengenai risiko yang mungkin terjadi, salah satunya kehilangan data. Perlunya definisi ini karena kehilangan data akan berakibat terhadap terhentinya aktivitas bisnis yang penting di organisasi atau aktivitas dapat berjalan namun membutuhkan waktu yang lama.

- **Kesalahan dalam pengambilan keputusan**

Tata kelola juga memuat prosedur pengerjaan suatu aktivitas dan pilhan untuk pengambilan keputusan. Pilihan yang ada sudah dari hasil rapat dan identifikasi proses bisnis organisasi. Saat dibutuhkan, dilakukan audit penyebab kesalahan yang ada dan pengambilan keputusan harus mengacu pada dokumen yang ada, untuk mencegah pengambilan keputusan yang lama dan salah

- **Risiko kebocoran data**

Kebocoran data tidak hanya berdampak terhadap kehilangan sejumlah pelanggan, akan tetapi lebih jauh lagi dapat mengganggu aktivitas bisnis perusahaan secara keseluruhan. Saat kebocoran data terjadi perlu dilakukan audit untuk menggali penyebab kebocoran. Setelah itu perbaikan dilakukan dengan dokumen tata kelola.

- **Penyalahgunaan asset TI**

Tata kelola mendefnisikan orang-orang yang bertanggung jawab atas keberlangsungan suatu proses dan keberadaan asset TI. Orang-orang inilah yang memastikan bahwa tiap bagian proses bisnis harus berjalan. Audit menjadi penting untuk bisa mengetahui kemungkinan penyalahgunaan aktivitas terkait dengan TI di organisasi.

- **Kerugian akibat kesalahan proses perhitungan**

Risiko tersebut akan mejadi semakin besar apabila tidak didukung dengan keberadaan mekanisme pengembangan yang memadai yang evaluasi implementasinya dapat diketahui melalui audit SI/TI

- **Tingginya nilai investasi perangkat keras dan perangkat lunak**

Keberadaan SI/TI membantu pihak manajemen dalam memastikan penggunaan TI sesuai standar pengelolaanyangbaik, kebijakan, hokum,dan regulasi yang berlaku sehingga dapat diarahkan untuk mendukung pencapaian tujuan bisnis.

Cakupan/fokus area tata kelola TIK ada 5 yakni:

1. Penyelarasan strategis (strategic alignment)

Tata kelola TI berfokus pada menyelaraskan strategi TI yang akan diimplementasi organisasi dengan strategi bisnis dan strategi operasional. yang sudah berjalan (sudah didefinisikan diawal pendrian perusahaan). Strategic alignment ini sendiri tidak hanya sekedar menyelaraskan strategi TI namun membuat bagaimana agar TI yang ada bisa meningkatkan nilai bisnis dan kinerja organisasi.

2. Penyampaian nilai (value delivery)

Untuk organisasi yang focus utama bisnisnya bukanlah TI (tidak bergerak di bidang TI), layanan TI tidak akan mampu memberikan manfaat langsung kepada bisnis, namun harus diimplementasikan bersama-sama dengan proses bisnis, kompetensi, dan prinsip kerja individu dalam perusahaan, serta perubahan-perubahan yang dilakukan dalam perusahaan itu sendiri. Prinsip dasar nilai TI adalah tepat waktu, sesuai anggaran/pengoptimalambiaya, sesuai manfaat, dan pembuktiannilai keberadaan IT. Oleh karena itu, proses TI harus dirancang dan dioperasikan dengan cara yang efisien dan efektif untuk memenuhi tujuan dan harapan perusahaan yang ditentukan oleh business value driver yang dipengaruhi oleh faktor lingkungan.

3. Pengelolaan sumber daya (resource management)

Berkaitan dengan pengoptimalan investasi yang dilakukan dan pengelolaan secara tepat dari sumber daya TI yang kritis mencakup:

- Perangkat lunak
- Perangkat keras
- Informasi
- Infrastruktur TI
- Sumber daya manusia, dll

4. Pengelolaan risiko (risk management)

Manajemen risiko menitikberatkan pada hal-hal yang berkenaan dengan

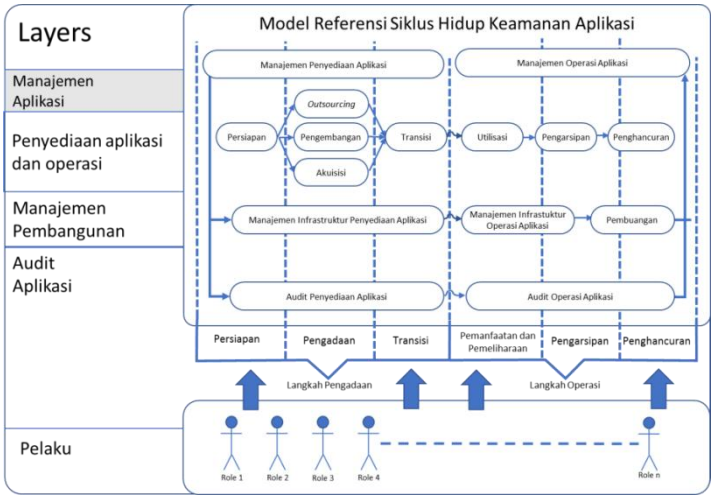
pengendalian internal dan hubungan antara organisasi dengan pelanggan, stakeholder, dan shareholder. Segala kemungkinan risiko harus dapat diidentifikasi sehingga dapat dilakukan langkah-langkah antisipasi untuk menghindari terjadinya dan mengurangi dampak terjadinya risiko. Untuk melakukan manajemen risiko, dibutuhkan kesadaran stakeholder akan adanya risiko, pemahaman yangjelas akan perhatian perusahaan atas keberadaan risiko, pemahaman kebutuhan dan kepatutan, transparasi akan risiko , pengenalan risiko apa saja yang bisa terjadi, cara penanggulangan risiko, dan menanamkan tanggung jawab untuk mengelola risiko di organisasi.

5. Pengukuran kinerja (performance measurement)

Pengukuran kinerja menjadi tolok ukur keberhasilan tata kelola TI. Hal ini dapat memberikan gambaran apakah hasil kerja tiap domain domain tata kelola TI sudah sesuai dengan tujuan dan tanggungjawab masing-masing. Berjalannya tiap bagian proses bisnis tentu memiliki seorang penanggungjawab. Investasi TI harus dapat dipertanggungjawabkan dengan satuan ukuran tertentu, dengan kinerja yang dihasilkan oleh TI terhadap proses bisnis dan tujuan perusahaan. Hal-hal yang perlu diukur adalah penelusuran dan pengawasan implementasi dari strategi, pemenuhan proyek yang berjalan, penggunaan sumber daya, kinerja proses dan penyampaian layanan.

III. Studi Kasus : Manajemen Aset Aplikasi SPBE

Siklus manajemen aset aplikasi (perangkat lunak) pada SPBE meliputi persiapan, pengadaan, transisi, pemanfaatan dan pemeliharaan, pengarsipan dan penghancuran. Masing-masing tahap tersebut dijelaskan untuk empat layer yang berbeda yaitu manajemen aplikasi, penyediaan aplikasi dan operasi, manajemen pembangunan dan audit aplikasi seperti dijelaskan pada Gambar 1. berikut ini.



Gambar 1. Manajemen Aset Aplikasi SPBE

3.1. Deskripsi

a. Manajemen Penyediaan aplikasi SPBE

Kegiatan manajemen penyediaan aplikasi SPBE dilakukan oleh manajer proyek dan Kepala pada instansi Pusat/Daerah, selama tahap penyediaan siklus hidup aplikasi. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah. Proses di dalamnya antara lain, Proses Manajemen Sumber Daya Manusia, Proses Perencanaan Proyek, Penilaian Proyek dan Proses Kontrol, dan Proses Manajemen Keputusan.

b. Manajemen Operasional aplikasi SPBE

Aktivitas manajemen operasi aplikasi terkait dengan manajemen dan penggunaan aplikasi SPBE selama tahap operasional. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah. Proses di dalamnya antara lain, Proses Manajemen Keputusan dan Proses Manajemen Informasi . Aplikasi berada dibawah tanggungjawab pemiliknya yangdapat memilih untuk membagikan sebagian dari ini tanggung jawab dengan aktor lain seperti manajer pengguna. Perubahan pada aplikasi selama tahap operasi, seperti perubahan yang berasal dari peraturan baru persyaratan atau ancaman, harus diprakarsai oleh pemilik aplikasi, yang bertanggung jawab memastikan bahwa aplikasi dengan benar dan terus menerus memenuhi kebutuhan keamanan instansi Pusat/Daerah yang berubah. Melalui proses ini, pemilik aplikasi akan memberikan Sistem Manajemen Keamanan Informasi (SMKI) instansi Pusat/Daerah yang dibutuhkan oleh aplikasi SPBE.

c. Persiapan

Selama tahap persiapan, tim penyediaan melakukan kegiatanpersiapan atau persiapan. Seperti itu kegiatan harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah.

d. Outsourcing

Selama tahap realisasi, jika outsourcing melakukan kegiatan implementasi, mungkin perlu ditambahkan ASC (Application Security Control) tertentu untuk kegiatan implementasinya untuk mencapai Target Level of Trust yangditargetkan aplikasi SPBE. Untuk alasan ini, Life Cycle Reference Model Keamanan Aplikasi

SPBE menyajikan area aktivitas spesifik untuk outsourcing Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah. Proses di dalamnya antaralain Proses Akuisisi, Dokumentasi Perangkat Lunak Proses Manajemen, Proses Manajemen Konfigurasi Perangkat Lunak dan Proses Manajemen Risiko.

e. Pengembangan

Kegiatan yang berkaitan dengan implementasi perangkat lunak dilakukan oleh tim penyedia selama tahap realisasi. Jika instansi Pusat/Daerah melakukan beberapa kegiatan implementasi secara internal, ASC menambahkan untuk pelaksanaannya kegiatan mungkin berbeda dari yang ditambahkan saat membeli atau outsourcing komponen implementasi atau aplikasi. Untuk alasan ini, Life Cycle Reference Model Keamanan Aplikasi menyajikan area spesifik untuk kegiatan pembangunan yang menghasilkan implementasi internal perangkat lunak yang dikembangkan. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh organisasi. Proses di dalamnya antara lain, Proses Manajemen Risiko, Desain Arsitektur Sistem, Proses Perancangan Arsitektur Perangkat Lunak, Proses Perancangan Perangkat Lunak, Proses Konstruksi Perangkat Lunak, Proses Manajemen Dokumentasi Perangkat Lunak, Proses Manajemen Konfigurasi Perangkat Lunak, Proses Verifikasi Perangkat Lunak, Proses Validasi Perangkat Lunak, Proses Tinjauan Perangkat Lunak, Proses Rekayasa Domain dan Proses Penggunakan Kembali Manajemen Aset.

f. Akuisisi

Kegiatan akuisisi dapat dilakukan oleh tim penyedia untuk tujuan memperoleh secara eksternal atau membeli produk dan / atau layanan yang dikebutuhan instansi Pusat/Daerah. ASC spesifik mungkin ditambahkan ke aktivitas tersebut. Life Cycle Reference Model Keamanan Aplikasi menyajikan area spesifik untuk kegiatan akuisisi yang menghasilkan implementasi komponen aplikasi yang diperoleh. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh isntansi Pusat/Daerah. Proses di dalamanya antara lain, Proses Akuisisi, Dokumentasi Perangkat Lunak Proses Manajemen, Proses Manajemen Konfigurasi Perangkat Lunak, Proses Manajemen Risiko dan Proses Implementasi.

g. Transisi

Area ini dalam tahap Transisi mencakup aktivitas yang dilakukan oleh tim penyedia untuk persiapan, mengkonfigurasi, menguji, dan menggunakan aplikasi di lingkungan operasional yang ditentukan oleh instansi Pusat/Daerah. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah. Proses di dalamnya antara lain, Proses Manajemen Konfigurasi Perangkat Lunak, Sistem Proses Integrasi danProses Pengujian Kualifikasi Sistem.

h. Utilization

Selama tahap Utilisasi dan pemeliharaan, aktivitas yang terlibat dalam penggunaan aktual aplikasi dalam lingkungan operasional oleh semua pengguna termasuk pengguna akhir. Aktivitas tersebut termasuk manajemen pengguna dan akses, logging, pemantauan, pelatihan keamanan, dll. Kegiatan lain dilakukan untuk pemeliharaan perangkat lunak dan manajemen perubahan, termasuk pembaruan perangkat lunak aplikasi untuk memenuhi perubahan persyaratan informasi, seperti menambahkan fungsi baru dan mengubah format data. Ini juga termasuk memperbaiki bug dan mengadaptasi perangkat lunak ke perangkat perangkat keras baru. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah. Proses di dalamnya antara lain, Proses Operasi Perangkat Lunak dan Pemeliharaan Perangkat Lunak Proses.

i. Archive

Kegiatan pengarsipan dilakukan oleh tim operasi ketika aplikasi tidak dalam kondisi aktif. Mereka menyertakan arsip semua informasi aplikasi, termasuk arsip semua alat dan proses untuk melindungi akses informasi ini dengan aman bahkan jika aplikasi tidak berjalan di environtment operasional. Kegiatan semacam itu biasanya dilakukan sebagai bagian dari proses di seluruh organisasi.

j. Penghancuran

Aktivitas penghancuran termasuk penghancuran semua informasi aplikasi, pengguna data, informasi instansi Pusat/Daerah, log pengguna, parameter aplikasi, dll. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh organisasi.

k. Manajemen Penyediaan Infrastruktur Aplikasi

Area kegiatan ini dalam tahap penyediaan meliputi aktivitas yang terlibat dalam menyediakan dan memelihara keamanan infrastruktur teknologi dalam

mendukung kegiatan tim penyediaan. Ini termasuk layanan, fasilitas, alat, dan aset teknologi komunikasi dan informasi dalam lingkungan pengembangan dan berbagai lingkungan pengujian. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah.

l. Manajemen Operasional Infrastruktur Aplikasi

Area kegiatan ini dalam tahap penyediaan meliputi aktivitas yang terlibat dalam menyediakan dan memelihara keamanan infrastruktur teknologi untuk tahap operasional dari siklus hidup aplikasi. Ini termasuk layanan, fasilitas, alat, dan aset teknologi komunikasi dan informasi dalam pengoperasian aplikasi lingkungan Hidup. Kegiatan lain juga harus dilakukan selama tahap operasonal untuk pemeliharaan yang aman infrastruktur yang mendukung aplikasi. Pemeliharaan infrastruktur mencakup perangkat keras sistem dan jaringan pemeliharaan, pencadangan dan pemulihan, pemulihan bencana, dll. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh instansi Pusat/Daerah.

m. Pembuangan

Kegiatan pembuangan dilakukan untuk memberikan jaminan bahwa semua informasi disimpan di server, sistem dan komponen teknologi lainnya yang digunakan oleh suatu aplikasi dihapus dengan aman. Ini memungkinkan untuk pembuangan atau daur ulang komponen- komponen ini tanpa risiko keamanan yang tidak semestinya bagi instansi Pusat/Daerah. Kegiatan semacam itu biasanya dilakukan sebagai bagian dari proses di seluruh organisasi.

n. Audit Penyediaan Aplikasi

Kegiatan audit dilakukan pada semua kegiatan, aktor, proses, artefak, dan komponen aplikasi yang digunakan atau diproduksi selama siklus hidup aplikasi. Kegiatan ini dapat dilakukan sekali atau secara berkala oleh tim audit internal atau eksternal, tergantung pada Level of Trust yang ditargetkan dari aplikasi SPBE. Mereka menyediakan aplikasi dengan yang membutuhkan jaminan dan bukti bahwa persyaratan keamanan untuk aplikasi dipenuhi seperti yang diharapkan. Kegiatan audit yang dilakukan selama tahap penyediaan biasanya berbeda dengan yang dilakukan selama tahap operasi. Instansi Pusat/Daerah yang mengembangkan tetapi tidak mengoperasikan aplikasi (seperti vendor perangkat lunak) mungkin tidak perlu mengaudit aplikasi dalam tahap operasi.

Untuk alasan ini, Siklus Life Cycle Reference Model Keamanan Aplikasi menyajikan area spesifik untuk kegiatan audit yang dilakukan selama tahap penyediaan. Kegiatan semacam itu harus dilakukan sebagai bagian dari proses di seluruh Instansi Pusat/Daerah. Proses di dalamnya contohnya Proses Audit Perangkat Lunak.

o. Audit Operasional Aplikasi

Kegiatan audit yang dilakukan selama tahap operasi biasanya berbeda dari yang dilakukan selama tahap penyediaan. Organisasi yang hanya mengoperasikan aplikasi yang diperoleh mungkin tidak perlu mengaudit aplikasi dalam tahap penyediaan. Untuk alasan ini, Life Cycle Reference Model Keamanan Aplikasi menyajikan area spesifik untuk aktivitas audit yang dilakukan selama tahap operasional.

3.2. Kegiatan

a. Manajemen Penyedia Aplikasi

Kegiatan manajemen penyediaan aplikasi dilakukan oleh manajer proyek dan organisasi manajer, selama tahap penyediaan siklus hidup aplikasi. Kegiatan semacam itu biasanya dilakukan sebagai bagian dariproses di seluruh organisasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi area kegiatan ini ke dalam sub area seperti memulai, merencanakan, melaksanakan, memantau dan kontrol, dan penutupan.

b. Manajemen Operasi Aplikasi

Aktivitas manajemen operasi aplikasi terkait dengan manajemen dan penggunaan aplikasi selama tahap operasi. Perubahan pada aplikasi selama tahap operasi, seperti perubahan yang berasal dari peraturan baru persyaratan atau ancaman, harus diprakarsai oleh pemilik aplikasi,yang bertanggung jawab untuk memastikan bahwa aplikasi dengan benar dan terus-menerus menangani perubahan kebutuhan keamanan organisasi. Melalui proses ini, pemilik aplikasi akan memberikan keamanan informasi organisasi sistem manajemen dengan jaminan yang dibutuhkan dan bukti bahwa tata kelola aplikasi proyek sedang ditangani. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi areakegiatan ini ke dalam sub area seperti memulai, merencanakan, melaksanakan, memantau dan kontrol, dan penutupan.

c. Persiapan

Selama tahap persiapan, tim penyediaan melakukan kegiatan persiapan atau persiapan. Kegiatan semacam itu biasanya dilakukan sebagai bagian dari proses di seluruh organisasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut bagikan bidang kegiatan ini ke dalam sub bidang seperti inisiasi dan perencanaan.

d. Outsourcing

Selama tahap realisasi, kegiatan yang berkaitan dengan implementasi perangkat lunak dilakukan oleh tim penyediaan. Jika organisasi outsourcing beberapa kegiatan implementasi, mungkin perlu menambahkan ASC tertentu ke aktivitas implementasinya untuk mencapai Tingkat Target aplikasi Kepercayaan. Untuk alasan ini, Model Referensi Siklus Hidup Keamanan Aplikasi menyajikan kegiatan tertentu area untuk outsourcing. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi wilayah kegiatan ini ke dalam sub bidang seperti realisasi dan transisi.

e. Pengembangan

Kegiatan yang terkait dengan implementasi perangkat lunak dilakukan oleh tim penyedia selama tahap realisasi. Jika organisasi melakukan secara internal beberapa kegiatan implementasi, maka ASC yang ditambahkan ke aktivitas implementasinya mungkin berbeda dari yang ditambahkan saat membeli atau outsourcing komponen implementasi atau aplikasi. Untuk alasan ini, Aplikasi Model Referensi Siklus HidupKeamanan menyajikan area spesifik untuk kegiatan pengembangan yang menghasilkan implementasi perangkat lunak yang dikembangkan secara internal. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat selanjutnya membagi area kegiatan ini menjadi beberapa sub area seperti permulaan, elaborasi, konstruksi dan penerapan.

f. Akuisisi

Kegiatan akuisisi dapat dilakukan oleh tim penyedia untuk tujuan memperoleh secara eksternal atau membeli produk dan / atau layanan yang memuaskan kebutuhan organisasi. Spesifik ASC dapat ditambahkan ke aktivitas-aktivitas tersebut. Untuk alasan ini, Referensi Siklus Hidup Keamanan Aplikasi Model menyajikan area spesifik untuk kegiatan akuisisi yang menghasilkan

implementasi yang diperoleh komponen aplikasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lanjut membagi wilayah kegiatan ini ke dalam sub bidang seperti rencana dan tutup.

g. Transisi

Area ini dalam tahap Transisi mencakup aktivitas yang dilakukan oleh tim penyedia untuk menyiapkan, mengkonfigurasi, menguji, dan menggunakan aplikasi dalam lingkungan operasi yang ditentukan oleh organisasi Kegiatan semacam itu biasanya dilakukan sebagai bagian dari proses di seluruh organisasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut bagikan bidang kegiatan ini ke dalam beberapa sub bidangseperti perencanaan, pengembangan, dan pengujian.

h. Pemanfaatan

Area ini dalam tahap Transisi mencakup aktivitas yang dilakukan oleh tim penyedia untuk menyiapkan, mengkonfigurasi, menguji, dan menggunakan aplikasi dalam lingkungan operasi yang ditentukan oleh organisasi Kegiatan semacam itu biasanya dilakukan sebagai bagian dari proses di seluruh organisasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut bagikan bidang kegiatan ini ke dalam beberapa sub bidangseperti perencanaan, pengembangan, dan pengujian.

i. Arsip

Kegiatan pengarsipan dilakukan oleh tim operasi ketika aplikasi tidak lagi diperlukan di keadaan aktifnya. Mereka menyertakan arsip semua informasi aplikasi, termasuk arsip semua alat dan proses untuk melindungi dan mengakses informasi ini dengan aman bahkan jika aplikasi tidak berjalan di lingkungan operasi lagi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut bagikan bidang kegiatan ini ke dalam sub bidang seperti perencanaan, pelaksanaan, dan verifikasi.

j. Penghancuran

Aktivitas penghancuran terlibat dalam penghancuran semua informasi aplikasi secara aman, termasuk data pengguna, informasi organisasi, log pengguna, parameter aplikasi, dll. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut bagikan bidang kegiatan ini ke dalam sub bidang seperti perencanaan, pelaksanaan, dan verifikasi.

k. Manajemen Infrastruktur Apikasi Penyediaan

Aktivitas manajemen infrastruktur penyediaan provisi terlibat dalam menyediakan dan memelihara infrastruktur teknologi yang aman untuk mendukung kegiatan tim penyediaan. Ini termasuk layanan, fasilitas, alat, dan aset teknologi komunikasi dan informasi di Indonesia lingkungan pengembangan dan berbagai lingkungan pengujian. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi area aktivitas ini kedalam sub area seperti instalasi, operasi, pemeliharaan, dukungandanarsip.

l. Manajemen Infrastruktur Aplikasi Operasional

Kegiatan manajemen infrastruktur operasi aplikasi terlibat dalam menyediakan dan memelihara infrastruktur teknologi yang aman untuk tahap operasi dari siklus hidup aplikasi. Ini termasuk layanan, fasilitas, alat, dan aset teknologi komunikasi dan informasi di dalam aplikasi lingkungan operasi. Kegiatan lain juga harus dilakukan selama tahap operasi untuk pemeliharaan yang aman infrastruktur yang mendukung aplikasi. Pemeliharaan infrastruktur mencakup sistem dan jaringan pemeliharaan perangkat keras, cadangan dan pemulihan, pemulihan bencana, dll. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi wilayah kegiatan ini ke dalam sub bidang seperti dukungan, operasi, pemeliharaan, dan arsip.

m. Pembuangan

Kegiatan pembuangan dilakukan untuk memberikan jaminan bahwa semua informasi disimpan diserver, sistem, dan komponen teknologi lainnya yang digunakan oleh suatu aplikasi dihapus dengan aman. Ini memungkinkan pembuangan atau daur ulang komponen-komponen ini tanpa risiko keamanan yang tidak semestinya untuk organisasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut bagikan bidang kegiatan ini ke dalam sub bidang seperti perencanaan, pelaksanaan, dan verifikasi.

n. Audit Penyediaan Aplikasi

Kegiatan audit dapat dilakukan pada semua kegiatan, aktor, proses, artefak, dan aplikasi komponen yangdigunakan atau diproduksi selama siklus hidup aplikasi.

Kegiatan-kegiatan ini dapat dilakukan sekali atau secara berkala oleh tim audit internal atau eksternal, tergantung pada Tingkat Target Kepercayaan dari proyek aplikasi. Mereka menyediakan pemilik aplikasi dengan diperlukan jaminan dan bukti bahwa persyaratan keamanan untukaplikasi dipenuhi seperti yang diharapkan. Kegiatan audit yang dilakukan selama tahap penyediaan biasanya berbeda dari yang dilakukan selama tahap operasi. Organisasi mengembangkan tetapi tidak mengoperasikan aplikasi (seperti perangkat lunak vendor) mungkin tidak perlu mengaudit aplikasi pada tahap operasi. Untuk alasan ini, Aplikasi Model Referensi Siklus HidupKeamanan menyajikan area spesifik untuk aktivitas audit yang dilakukan selama tahap penyediaan. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi area aktivitas ini ke dalam sub area seperti merencanakan, memperoleh, mengimplementasikan, memberikan, mendukung, memantau dan mengevaluasi.

o. Audit Operasional Aplikasi

Kegiatan audit yang dilakukan selama tahap operasi biasanya berbeda dari yang dilakukan selama tahap penyediaan. Organisasi yang hanya mengoperasikan aplikasi yang diperoleh mungkin tidak perlu aplikasi audit dalam tahap penyediaan. Untuk alasan ini, Referensi Siklus Hidup Keamanan Aplikasi Model menyajikan area spesifik untuk aktivitas audit yang dilakukan selama tahap operasi. Untuk spesifikasi yang lebih tepat tentang kapan kegiatan keamanan harus dilakukan, organisasi dapat lebih lanjut membagi area aktivitas ini ke dalam sub area seperti merencanakan, memperoleh, mengimplementasikan, memberikan, mendukung, memantau dan mengevaluasi