BAB III
METODOLOGI PENELITIAN

3.1 Tempat dan Waktu

Peneliti melakukan penelitian di Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera. Waktu penelitian dilakukan mulai bulan November 2019 sampai bulan Agustus 2020, seperti yang dijabarkan dalam tabel 3.1 berikut.

Tabel 3. 1 Waktu Penelitian

No.	Aktivitas	Bulan ke-										Keterangan
		1	2	3	4	5	6	7	8	9	10	
1.	Perumusan Masalah											
2.	Studi Literatur											
3.	Pengumpulan data dan *Mapping*											
4.	Pengumpulan data											
5.	Penulisan Laporan											

3.2 Data

Data yang akan digunakan dalam penelitian ini berupa informasi tentang keadaan infrastruktur teknologi informasi di Institut Teknologi Sumatera, khususnya pada bagian sistem informasi, implementasi dan pengembangan teknologi informasi, serta tata kelolanya. Data-data tersebut akan didapatkan dari wawancara kepada beberapa narasumber dari UPT TIK ITERA dan Rencana Strategis (Renstra) UPT TIK ITERA.

3.3 Metodologi

Pada bagian ini, penulis membahas metode pengumpulan data serta tahap-tahap penelitian. Metode penelitian yang digunakan pada penelitian ini adalah metode kualitatif, dengan menggunakan studi kasus, yaitu suatu cara yang sistematis dalam melihat suatu kejadian, mengumpulkan data, menganalisa informasi dan melaporkan

hasilnya. Metodologi kualitatif ialah prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati [21]. Pendekatan ini diarahkan pada latar dan individu tersebut secara utuh, sehingga kita tidak dapat mengisolasikan individu atau organisasi ke dalam variabel atau hipotesis, melainkan dipandang sebagai dari suatu keutuhan [22]. Dalam studi kasus ini, pengumpulan data utama dilakukan dengan wawancara dan analisa dokumen-dokumen organisasi terkait penelitian.

3.3.1 Metode pengumpulan data

Metode yang digunakan dalam pengumpulan data-data untuk penulisan penelitian ini adalah sebagai berikut:

1. Studi literatur

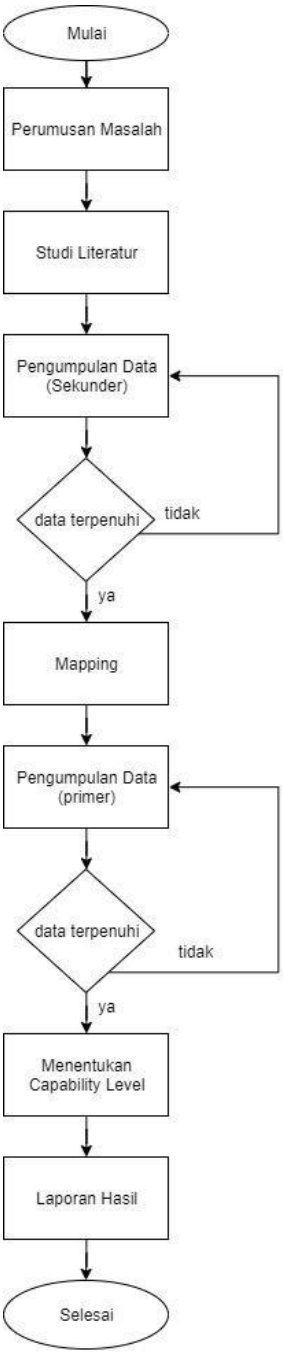
   Penelitian ini dilakukan dengan cara mencari dan mengumpulkan data, sumber informasi dan bahan-bahan yang diperoleh dari buku, literatur, artikel terkait COBIT, tata kelola IT, metode penelitian yang digunakan, dan penelitian sebelumnya yang berkaitan dengan topik penelitian.

2. Wawancara semi terstruktur

   Melakukan tanya jawab dengan pihak yang terkait untuk mendapatkan informasi dan data-data yang dibutuhkan. Teknik wawancara dalam penelitian ini dilakukan dengan menggunakan metode semi terstruktur, yaitu proses wawancara yang berpedoman pada daftar pertanyaan dan peneliti dapat mengembangkan pertanyaan-pertanyaan penelitian sesuai dengan kebutuhan informasi yang diinginkan. Partisipan dalam penelitian ini adalah *staff* Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera

3.3.2 Tahap – tahap penelitian

Adapun tahapan penelitian yang dilakukan, di ilustrasikan pada Gambar 3.1 berikut :



Gambar 3. 1 Langkah-langkah penelitian

1. Perumusan Masalah

   Mengumpulkan permasalahan yang ditemukan untuk digunakan sebagai pedoman, penentu fokus dari penelitian. Pada tahap ini, peneliti mengumpulkan permasalahan yang ada dengan mengambil topik keamanan informasi pada Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera, dan didapatkan permasalahan tentang belum dilakukannya penilaian keamanan pada sistem.

2. Studi Literatur

   Studi literatur ini dilakukan dengan cara mencari dan mengumpulkan data, sumber informasi dan bahan-bahan yang diperoleh dari buku, literatur, artikel terkait COBIT, tata kelola IT, metode penelitian yang digunakan, dan sebagainya.

3. Pengumpulan Data Sekunder

   Pada tahap ini, peneliti melakukan pengumpulan data sekunder yang berupa informasi tentang gambaran umum (visi, misi, rencana strategis Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera) yang diperoleh dari hasil analisis dokumen dan wawancara pra-penelitian.

4. *Mapping*

   Pada tahap ini, peneliti melakukan COBIT 5 *mapping*, peneliti menganalisa kebijakan keamanan informasi dari rencana strategis Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera dan hasil wawancara dengan pihak TIK untuk kemudian disesuaikan dengan kerentanan pada sistem informasi yang diambil dari OWASP.

5. Pengumpulan Data Primer

   Peneliti melakukan pengumpulan data primer secara kualitatif dengan metode observasi, dan wawancara dengan narasumber dari pihak Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera. Pertanyaan yang diajukan seputar implementasi dan tata kelola IT di Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera.

6. Menentukan *Capability Level*

   Pada tahap ini dilakukan penentuan tingkat kemampuan (*Capability Level*) yang didapatkan dari hasil observasi dan wawancara dengan pihak Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera. Pada tahap ini juga akan dijabarkan temuan-temuan berkaitan dengan keamanan informasi, dan membuat rekomendasi hasil penentuan tingkat kemampuan.

7. Laporan Hasil

   Peneliti melakukan penarikan kesimpulan berdasarkan hasil penelitian penilaian menggunakan *Process Assessment Model*. Pada tahap ini peneliti juga memberikan saran yang nantinya dapat diterapkan untuk meningkatkan maupun memperbaiki keamanan informasi pada Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi Institut Teknologi Sumatera.

3.4 Mapping

Pada tahap ini dilakukan COBIT 5 *mapping*, peneliti menganalisa kerentanan pada sistem informasi untuk kemudian disesuaikan dengan COBIT 5.

a. *Mapping IT Related Goal*

Pada tahap ini dilakukan *mapping IT related goal*, peneliti menganalisa kebijakan keamanan informasi dari rencana strategis TIK dan hasil wawancara dengan pihak TIK untuk disesuaikan dengan *IT related goal* pada COBIT 5 [15].

Tabel 3. 2 *Mapping IT Related Goal*

Sumber	**Isi pernyataan**	***IT Related Goal***		
Kebijakan keamanan informasi (renstra TIK)	Aspek keamanan elektronis meliputi proses input data ke dalam sistem, penyimpanan, pengelolaan, penggunaan dan transmisi data dan informasi.	08		
	Aspek keamanan fisik mencakup keamanan ruangan tempat penyimpanan data atau informasi dan aplikasi, tata letak fiber optik, pemilihan jalur pemasangan kabel UTP (*Unshielded Twisted Pair*), sistem pasokan listrik, kamera pemantau, pendingin ruangan, *Disaster Recovery Center* (DRC) sistem penangkal petir.	10		
	Keamanan prosedur yang meliputi hak, kewajiban dan kewenangan pengelolaan sistem informasi, klasifikasi informasi rahasia, pelatihan, pengawasan dan sistem *reward and punishment* dan kebijakan *definition of done.*	14	15	17
Wawancara	Gangguan yang terjadi lebih dari sekali seperti internet bermasalah, listrik mati, sistem *down*, *hardware* rusak	04		

Adapun penjelasan dari *IT goals* COBIT yang teridentifikasi adalah sebagai berikut :

Tabel 3. 3 *IT goals* yang teridentifikasi

04	*Managed IT-related business risk*
08	*Adequate use of applications, information and technology solutions*
10	*Security of information, processing infrastructure and applications*
14	*Availability of reliable and useful information for decision making*
15	*IT compliance with internal policies*
17	*Knowledge, expertise and initiatives for business innovation*

b. Mapping IT Related Goal to IT Process

Pada tahap ini dilakukan *mapping IT related goal to IT process*, peneliti menganalisa *IT goals* COBIT yang teridentifikasi untuk disesuaikan dengan *IT process* pada COBIT 5 [15].

Tabel 3. 4 *Mapping IT Related Goal to IT Process*

IT related goal		***IT process***						
04	*Managed IT-related business risk*	EDM03	APO10	APO12	APO13	BAI01	BAI06	DSS01
		DSS01	DSS02	DSS03	DSS04	DSS05	DSS06	MEA01
		MEA02	MEA03					
08	*Adequate use of applications, information and technology solutions*	APO04	BAI05					
10	*Security of information, processing infrastructure and applications*	EDM03	APO12	APO13	BAI06	DSS05		
14	*Availability of reliable and useful information for decision making*	APO09	APO13	BAI04	BAI10	DSS03	DSS04	
15	*IT compliance with internal policies*	EDM03	APO01	MEA01	MEA02			
17	*Knowledge, expertise and initiatives for business innovation*	EDM02	APO01	APO02	APO04	APO07	APO08	BAI05
		BAI08						

c. Mapping OWASP

Pada tahap ini dilakukan COBIT 5 *mapping*, peneliti menganalisa kebijakan keamanan informasi dari rencana strategis TIK dan hasil wawancara dengan pihak TIK untuk kemudian disesuaikan dengan kerentanan pada sistem informasi yang diambil dari OWASP.

Tabel 3. 5 *Mapping OWASP*

Sumber	**Isi pernyataan**	**Keterkaitan dengan OWASP**
Kebijakan keamanan informasi	Aspek keamanan elektronis meliputi proses input data ke dalam sistem, penyimpanan, pengelolaan, penggunaan dan transmisi data dan informasi.	*Injection*
		Broken authentication
		Sensitive Data Exposure
		XML *External Entities (*XXE)
		Broken Access Control
		Security Misconfiguration
		Cross-Site Scripting (XSS)
		Insecure Deserialization
		Using Components with Known Vulnerabilities
		Insufficient Logging & Monitoring
	Aspek keamanan fisik mencakup keamanan ruangan tempat penyimpanan data atau informasi dan aplikasi, tata letak fiber optik, pemilihan jalur pemasangan kabel UTP (*Unshielded Twisted Pair*), sistem pasokan listrik, kamera pemantau, pendingin ruangan, *Disaster Recovery Center* (DRC) sistem penangkal petir.	*Insufficient Logging & Monitoring*

	Keamanan prosedur yang meliputi hak, kewajiban dan kewenangan pengelolaan sistem informasi, klasifikasi informasi rahasia, pelatihan, pengawasan dan sistem *reward and punishment* dan kebijakan *definition of done.*	*Injection*
		Broken authentication
		Sensitive Data Exposure
		XML *External Entities (*XXE)
		Broken Access Control
		Security Misconfiguration
		Cross-Site Scripting (XSS)
		Insecure Deserialization
		Using Components with Known Vulnerabilities
		Insufficient Logging & Monitoring
wawancara	Gangguan yang terjadi lebih dari sekali seperti internet bermasalah, listrik mati, sistem *down*, *hardware* rusak	*Insufficient Logging & Monitoring*

d. Tabel *mapping* OWASP dengan COBIT 5

Pada tahap ini dilakukan COBIT 5 *mapping*, peneliti menganalisa kerentanan pada sistem informasi yang diambil dari OWASP untuk kemudian disesuaikan dengan COBIT 5.

Tabel 3. 6 *Mapping* OWASP dengan COBIT 5

Kerentanan (OWASP)	**COBIT 5**			
Injection	APO13.01	APO13.03	DSS05.02	DSS05.04
Broken authentication	APO13.01	APO13.03	DSS05.01	DSS05.02
Sensitive Data Exposure	APO13.01	APO13.03	DSS05.02	DSS05.03
XML *External Entities* (XXE)	APO13.01	APO13.03	DSS05.02	
Broken Access Control	APO13.01	APO13.03	DSS05.04	
Security Misconfiguration	APO13.01	APO13.03	DSS05.04	DSS05.05
Cross-Site Scripting (XSS)	APO13.01	APO13.03	DSS05.02	DSS05.03
Insecure Deserialization	APO13.01	APO13.03	DSS05.03	
Using Components with Known Vulnerabilities	APO13.01	APO13.03	DSS05.03	
Insufficient Logging & Monitoring	APO13.01	APO13.03	DSS05.03	DSS05.04

Fokus pada penelitian ini adalah dalam hal keamanan informasi, sehingga domain APO pada proses APO13 dan domain DSS pada proses DSS05 dipilih karena menangani masalah keamanan. Proses APO13 (*Manage Security*) mendefinisikan, mengoperasikan dan mengawasi sistem untuk manajemen keamanan informasi. Tujuan dari proses tersebut adalah menjaga agar dampak dan kejadian dari insiden masih berada dalam batas resiko yang dapat diterima organisasi. Sub proses pada APO13 sebagai berikut:

1. APO13.01 *Establish and maintain an information security management system* (ISMS) (Menetapkan dan memelihara sistem manajemen keamanan informasi) Menetapkan dan memelihara ISMS yang menyediakan pendekatan standar, formal, dan berkelanjutan untuk manajemen keamanan untuk informasi, memungkinkan teknologi aman dan proses bisnis yang selaras dengan persyaratan bisnis dan manajemen keamanan organisasi. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :
   a. Menentukan ruang lingkup dan batasan sistem manajemen keamanan informasi (SMKI) dalam hal karakteristik organisasi, lokasinya, aset dan teknologinya.
   b. Sertakan detail, dan alasan untuk, pengecualian apa pun dari cakupan.
   c. Mendefinisikan SMKI sesuai dengan kebijakan organisasi dan sejalan dengan organisasi, lokasi, aset dan teknologinya.
   d. Sejajarkan SMKI dengan pendekatan perusahaan secara keseluruhan untuk manajemen keamanan.
   e. Dapatkan otorisasi manajemen untuk menerapkan dan mengoperasikan atau mengubah SMKI.
   f. Menyiapkan dan memelihara pernyataan penerapan yang menggambarkan ruang lingkup SMKI.
   g. Mendefinisikan dan mengkomunikasikan peran dan tanggung jawab manajemen keamanan informasi.
   h. Mengkomunikasikan pendekatan SMKI.

   Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen kebijakan SMKI dan pernyataan ruang lingkup SMKI.

2. APO13.02 *Define and manage an information security risk treatment plan* (Menentukan dan mengelola rencana perawatan risiko keamanan informasi)

Mempertahankan rencana keamanan informasi yang menjelaskan bagaimana risiko keamanan informasi dikelola dan diselaraskan dengan strategi organisasi dan arsitektur organisasi. Memastikan bahwa rekomendasi untuk mengimplementasikan peningkatan keamanan didasarkan pada kasus bisnis yang disetujui dan diimplementasikan sebagai bagian integral dari pengembangan layanan dan solusi, kemudian dioperasikan sebagai bagian integral dari operasi bisnis. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

a. Merumuskan dan memelihara rencana perlakuan risiko keamanan informasi selaras dengan tujuan strategis dan arsitektur organisasi. Pastikan bahwa rencana tersebut mengidentifikasi praktik manajemen dan solusi keamanan yang tepat dan optimal, dengan sumber daya, tanggung jawab, dan prioritas terkait untuk mengelola risiko keamanan informasi yang teridentifikasi.
b. Menjaga sebagai bagian dari arsitektur organisasi inventaris komponen solusi yang ada untuk mengelola risiko terkait keamanan.
c. Menyusun proposal untuk melaksanakan rencana perlakuan risiko keamanan informasi, didukung oleh kasus bisnis yang sesuai, yang meliputi pertimbangan pendanaan dan alokasi peran dan tanggung jawab.
d. Memberikan masukan untuk desain dan pengembangan praktik manajemen dan solusi yang dipilih dari rencana perlakuan risiko keamanan informasi.
e. Menentukan bagaimana mengukur keefektifan praktek pengelolaan yang dipilih dan tentukan bagaimana pengukuran ini akan digunakan untuk menilai keefektifan untuk menghasilkan hasil yang sebanding dan dapat direproduksi.
f. Merekomendasikan pelatihan keamanan informasi dan program kesadaran.
g. Mengintegrasikan perencanaan, desain, implementasi dan pemantauan prosedur keamanan informasi dan kontrol lain yang mampu memungkinkan pencegahan yang cepat, deteksi kejadian keamanan dan respon terhadap insiden keamanan.

Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen rencana penanganan risiko keamanan informasi dan *business cases* keamanan informasi.

3. APO13.03 *Monitor and review the ISMS* (Meninjau dan mengkaji sistem manajemen keamanan informasi)

   Menjaga dan secara teratur mengomunikasikan kebutuhan, dan manfaat, peningkatan keamanan informasi yang berkelanjutan. Kumpulkan dan analisis data tentang ISMS, dan tingkatkan efektivitas ISMS. Mendorong budaya keamanan dan peningkatan berkelanjutan. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a Melakukan tinjauan berkala atas keefektifan SMKI termasuk memenuhi kebijakan dan tujuan SMKI, dan meninjau praktik keamanan. Mempertimbangkan hasil audit keamanan, insiden, hasil dari pengukuran efektivitas, saran dan umpan balik dari semua pihak yang berkepentingan.
   b Melakukan audit SMKI internal pada interval yang direncanakan.
   c Melakukan tinjauan manajemen SMKI secara teratur untuk memastikan bahwa ruang lingkup tetap memadai dan perbaikan dalam proses SMKI diidentifikasi.
   d Memberikan masukan untuk pemeliharaan rencana keamanan dengan mempertimbangkan temuan kegiatan pemantauan dan peninjauan.
   e Mencatat tindakan dan peristiwa yang dapat berdampak pada efektivitas atau kinerja SMKI.

   Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen laporan audit SMKI dan rekomendasi untuk meningkatkan SMKI.

Domain DSS pada proses DSS05 mengenai melindungi informasi organisasi untuk mempertahankan tingkatan dari keamanan informasi yang dapat diterima oleh organisasi sesuai dengan kebijaksanaan keamanan. Menetapkan dan mempertahankan peran keamanan informasi dan hak akses dan melakukan pengawasan keamanan. Domain proses yang digunakan yaitu DSS05 *Manage Security Service*. Berikut merupakan deskripsi sub proses DSS05:

1. DSS05.01 *Protect against malware* (Melindungi terhadap malware) Menerapkan dan memelihara pencegahan, dan langkah-langkah perbaikan di tempat (terutama *up-to-date patch* keamanan dan kontrol virus) di organisasi untuk melindungi sistem informasi dan teknologi dari *malwar*e (misalnya, virus, *worm*, *spyware*, *spam*). Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :
   a. Mengkomunikasikan kesadaran perangkat lunak berbahaya dan menerapkan prosedur pencegahan dan tanggung jawab.
   b. Menginstal dan mengaktifkan alat perlindungan perangkat lunak berbahaya di semua fasilitas pemrosesan, dengan file definisi perangkat lunak berbahaya yang diperbarui sesuai kebutuhan (secara otomatis atau semi-otomatis).
   c. Mendistribusikan semua perangkat lunak perlindungan secara terpusat (versi dan tingkat patch) menggunakan konfigurasi terpusat dan manajemen perubahan.
   d. Secara teratur meninjau dan mengevaluasi informasi tentang potensi ancaman baru (misalnya, meninjau produk vendor).
   e. Filter lalu lintas masuk, seperti email dan unduhan, untuk melindungi dari informasi yang tidak diminta (misalnya, *spyware*, *email phishing*).
   f. Melakukan pelatihan berkala tentang malware dalam penggunaan email dan Internet. Melatih pengguna untuk tidak menginstal perangkat lunak yang dibagikan atau tidak disetujui.

   Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen kebijakan pencegahan perangkat lunak berbahaya dan evaluasi potensi ancaman.

2. DSS05.02 *Manage network and connectivity security* (Mengelola jaringan dan konektivitas keamanan)

   Gunakan langkah-langkah keamanan dan prosedur manajemen terkait untuk melindungi informasi atas semua metode konektivitas. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a. Berdasarkan penilaian risiko dan kebutuhan bisnis, tetapkan dan pelihara kebijakan untuk keamanan konektivitas.
   b. Izinkan hanya perangkat yang diizinkan untuk memiliki akses ke informasi perusahaan dan jaringan perusahaan. Konfigurasi perangkat ini untuk memaksa memasukkan kata sandi.
   c. Menerapkan mekanisme penyaringan jaringan, seperti *firewall* dan perangkat lunak pendeteksi intrusi, dengan kebijakan yang sesuai untuk mengontrol lalu lintas masuk dan keluar.
   d. Mengenkripsi informasi dalam perjalanan sesuai dengan klasifikasinya.
   e. Terapkan protokol keamanan yang disetujui ke konektivitas jaringan.
   f. Konfigurasi peralatan jaringan dengan cara yang aman.
   g. Menetapkan mekanisme tepercaya untuk mendukung transmisi dan penerimaan informasi yang aman.
   h. Melakukan *penetration testing* secara berkala untuk mengetahui kecukupan proteksi jaringan.
   i. Melakukan pengujian keamanan sistem secara berkala untuk menentukan kecukupan perlindungan sistem.

   Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen kebijakan keamanan konektivitas dan hasil *penetration testing*.

3. DSS05.03 *Manage endpoint security* (Mengelola keamanan titik akhir)
   Memastikan bahwa titik akhir (misalnya, laptop, desktop, server dan perangkat *mobile* dan jaringan lainnya atau perangkat lunak) dijamin pada tingkat yang sama dengan atau lebih besar dari persyaratan keamanan didefinisikan dari informasi yang diproses, disimpan atau dikirimkan. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a. Konfigurasi sistem operasi dengan cara yang aman.
   b. Menerapkan mekanisme penguncian perangkat.

c. Mengenkripsi informasi dalam penyimpanan sesuai dengan klasifikasinya.
d. Kelola akses dan kontrol jarak jauh.
e. Kelola konfigurasi jaringan dengan cara yang aman.
f. Menerapkan pemfilteran lalu lintas jaringan pada perangkat titik akhir.
g. Lindungi integritas sistem.
h. Memberikan perlindungan fisik perangkat titik akhir.
i. Buang perangkat titik akhir dengan aman.

Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen kebijakan keamanan untuk perangkat *end point*.

4. DSS05.04 *Manage user identity and logical access* (Mengelola identitas pengguna dan akses logis)

   Memastikan bahwa semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan koordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a. Menjaga hak akses pengguna sesuai dengan fungsi bisnis dan persyaratan proses. Sejajarkan pengelolaan identitas dan hak akses dengan peran dan tanggung jawab yang ditentukan, berdasarkan pada prinsip-prinsip yang paling tidak memiliki hak istimewa, yang perlu dimiliki, dan yang perlu diketahui.
   b. Secara unik mengidentifikasi semua aktivitas pemrosesan informasi berdasarkan peran fungsional, berkoordinasi dengan unit bisnis untuk memastikan bahwa semua peran didefinisikan secara konsisten, termasuk peran yang ditentukan oleh bisnis itu sendiri dalam aplikasi proses bisnis.
   c. Mengautentikasi semua akses ke aset informasi berdasarkan klasifikasi keamanannya, berkoordinasi dengan unit bisnis yang mengelola otentikasi dalam aplikasi yang digunakan dalam proses bisnis untuk memastikan bahwa kontrol otentikasi telah diatur dengan benar.
   d. Mengelola semua perubahan pada hak akses (pembuatan, modifikasi dan penghapusan) agar berlaku pada waktu yang tepat hanya berdasarkan transaksi yang disetujui dan didokumentasikan yang disahkan oleh individu manajemen yang ditunjuk.

e. Pisahkan dan kelola akun pengguna dengan hak istimewa.
f. Lakukan tinjauan manajemen rutin semua akun dan hak istimewa terkait.
g. Memastikan bahwa semua pengguna (internal, eksternal dan sementara) dan aktivitas mereka pada sistem TI (aplikasi bisnis, infrastruktur TI, sistem operasi, pengembangan dan pemeliharaan) dapat diidentifikasi secara unik. Secara unik mengidentifikasi semua aktivitas pemrosesan informasi oleh pengguna.
h. Menjaga jejak audit dari akses ke informasi yang diklasifikasikan sebagai sangat sensitif.

Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen hak akses pengguna yang disetujui dan hasil tinjauan akun pengguna dan hak istimewa.

5. DSS05.05 *Manage physical access to IT assets* (Mengelola akses fisik ke aset TI)

   Mendefinisikan dan menerapkan prosedur untuk memberikan, batas dan mencabut akses ke lokasi, bangunan dan daerah sesuai dengan kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, dan area harus dibenarkan, disahkan, dicatat, dan dipantau. Ini harus berlaku untuk semua orang yang memasuki lokasi, termasuk staf, staf sementara, klien, *vendor*, pengunjung atau pihak ketiga lainnya. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a. Mengelola permintaan dan pemberian akses ke fasilitas komputasi. Permintaan akses formal harus diselesaikan dan disahkan oleh manajemen situs TI, dan catatan permintaan disimpan. Formulir harus secara spesifik mengidentifikasi area di mana individu diberikan akses.
   b. Pastikan profil akses tetap terkini. Akses dasar ke situs TI (ruang server, gedung, area atau zona) pada fungsi dan tanggung jawab pekerjaan.
   c. Masuk dan pantau semua titik masuk ke situs TI. Daftarkan semua pengunjung, termasuk kontraktor dan vendor, ke situs.
   d. Perintahkan semua personel untuk menampilkan identifikasi yang terlihat setiap saat. Cegah penerbitan kartu identitas atau lencana tanpa otorisasi yang tepat.

e. Mengharuskan pengunjung untuk didampingi setiap saat saat berada di lokasi. Jika teridentifikasi seseorang tanpa pendamping dan tidak dikenal yang tidak mengenakan identitas staf, peringatkan personel keamanan.
f. Batasi akses ke situs TI yang sensitif dengan menetapkan batasan perimeter, seperti pagar, dinding, dan perangkat keamanan di pintu interior dan eksterior. Pastikan perangkat merekam entri dan memicu alarm jika terjadi akses yang tidak sah. Contoh perangkat tersebut termasuk lencana atau kartu kunci, keypad, televisi sirkuit tertutup, dan pemindai biometric.
g. Lakukan pelatihan kesadaran keamanan fisik secara teratur.

Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen permintaan akses yang disetujui dan akses log.

6. DSS05.06 *Manage sensitive documents and output devices* (Mengelola dokumen sensitif dan perangkat output)

   Menetapkan pengamanan fisik yang sesuai, praktik akuntansi, dan manajemen inventaris atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer tujuan khusus, atau token keamanan. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a. Tetapkan prosedur untuk mengatur penerimaan, penggunaan, pemindahan dan pembuangan bentuk khusus dan perangkat keluaran ke dalam, di dalam dan di luar perusahaan.
   b. Tetapkan hak istimewa akses ke dokumen sensitif dan perangkat keluaran berdasarkan prinsip hak paling rendah, seimbangkan risiko dan persyaratan bisnis.
   c. Buat inventarisasi dokumen sensitif dan perangkat keluaran, dan lakukan rekonsiliasi secara teratur.
   d. Tetapkan pengamanan fisik yang sesuai atas bentuk khusus dan perangkat sensitif.
   e. Hancurkan informasi sensitif dan lindungi perangkat keluaran (misalnya, degaussing media elektronik, perusakan fisik perangkat memori, sediakan penghancur atau keranjang kertas yang terkunci untuk menghancurkan formulir khusus dan kertas rahasia lainnya).

Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen inventaris dokumen dan perangkat sensitif dan hak akses.

7. DSS05.07 *Monitor the infrastructure for security-related events* (Memantau infrastruktur untuk acara yang berhubungan dengan keamanan)
   Menggunakan alat deteksi gangguan, memantau infrastruktur untuk akses yang tidak sah dan memastikan bahwa setiap peristiwa yang terintegrasi dengan pemantauan kejadian umum dan manajemen insiden. Untuk mendukung proses ini ada beberapa aktifitas yang harus dilakukan, yaitu :

   a. Catat kejadian terkait keamanan yang dilaporkan oleh alat pemantauan keamanan infrastruktur, dengan mengidentifikasi tingkat informasi yang akan dicatat berdasarkan pertimbangan risiko. Pertahankan selama jangka waktu yang sesuai untuk membantu penyelidikan di masa mendatang.
   b. Mendefinisikan dan mengkomunikasikan sifat dan karakteristik potensi insiden terkait keamanan sehingga dapat dengan mudah dikenali dan dampaknya dipahami untuk memungkinkan tanggapan yang sepadan.
   c. Tinjau log peristiwa secara teratur untuk mengetahui potensi insiden.
   d. Menjaga prosedur pengumpulan bukti sejalan dengan aturan bukti forensik lokal dan memastikan bahwa semua staf diberi tahu tentang persyaratan tersebut.
   e. Memastikan bahwa tiket insiden keamanan dibuat tepat waktu saat pemantauan mengidentifikasi potensi insiden keamanan.

   Setelah melakukan aktifitas-aktifitas tersebut, selanjutnya melengkapi dokumen log peristiwa keamanan, karakteristik insiden keamanan, dan tiket insiden keamanan.