Coding : Jurnal Komputer dan Aplikasi
Volume 10, No. 02 (2022), hal 237-248

p-ISSN : 2338-493X
e-ISSN : 2809-574X

ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN *NIST CYBERSECURITY FRAMEWORK* DAN *ISO/IEC 27001:2013* (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)

[1]Tasha Safira Putri , [2]Nurul Mutiah, [3]Dian Prawira
[1,2,3] Jurusan Sistem Informasi, Fakultas MIPA Universitas Tanjungpura
Jalan Prof Dr. H. Hadari Nawawi Pontianak
Telp/Fax.: (0561)577963
e-mail: [1]tashasafiraa25@student.untan.ac.id, [2]nurul@sisfo.untan.ac.id,
[3]dianprawira@sisfo.untan.ac.id

Abstrak

Penerapan teknologi informasi yang tepat dapat memberikan dampak baik pada proses bisnis perusahaan maupun instansi pemerintah. Teknologi informasi membuat proses bisnis menjadi efektif dan efisien, sehingga menghasilkan keuntungan lebih besar, salah satu instansi pemerintah yang menerapkan teknologi informasi sebagai kegiatan operasional sehari-hari adalah Badan Pusat Statistik (BPS) Kalimantan Barat. BPS Kalimantan Barat berperan sebagai penyedia data dan informasi lengkap, berkualitas, akurat dan relevan bagi pengguna data, namun BPS Kalimantan Barat belum melakukan manajemen risiko pada setiap aset informasi dan belum mempunyai dokumen perancangan sistem manajemen keamanan informasi untuk memantau dan menanggapi ancaman risiko. Maka dari itu, penelitian ini dilakukan guna menganalisis dan menilai risiko keamanan informasi serta kesenjangan pengamanan aset informasi menggunakan metode NIST Cybersecurity Framework Dan ISO/IEC 27001:2013. Metode NIST Cybersecurity berfokus ke business drivers untuk memandu kegiatan keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian manajemen risiko. ISO/IEC 27001:2013 terkandung persyaratan untuk mengontrol keamanan informasi yang disesuaikan dengan kebutuhan. Hasil penelitian berupa pemaparan gap keamanan informasi, gap tertinggi dari perwakilan setiap fungsi NIST Cybersecurity, yaitu: penilaian risiko, keamanan data, anomali dan peristiwa, mitigasi, dan perencanaan pemulihan. Berdasarkan identifikasi dan penilaian risiko, terdapat 36 ancaman memiliki kriteria Tinggi, 29 ancaman kriteria risiko Sedang dan 21 ancaman dengan kriteria risiko Rendah. Penelitian ini juga memberikan rekomendasi kontrol keamanan terhadap risiko yang teridentifikasi yang dijelaskan dalam dokumen Sistem Manajemen Keamanan Informasi (SMKI).

Kata kunci : Manajemen Risiko, Keamanan Informasi, *NIST Cybersecurity*, ISO/IEC 27001:2013.

1. PENDAHULUAN

Penggunaan teknologi informasi hampir merambah ke semua aspek penunjang kehidupan, mulai dari aspek kesehatan, transportasi, lingkungan, pendidikan, terutama bisnis perusahaan. Dalam dunia bisnis, penerapan teknologi dan sistem informasi merupakan bagian dari keberlangsungan bisnis suatu perusahaan. Penerapan teknologi informasi dalam mengelola data dapat memberikan dampak baik pada proses bisnis perusahaan [1]. Salah satu instansi pemerintah yang menerapkan teknologi informasi adalah Badan Pusat Statistik (BPS) Kalimantan Barat. BPS Kalimantan Barat berperan sebagai penyedia data dan informasi lengkap, berkualitas, akurat dan relevan bagi pengguna data. Sebagai instansi yang bergerak dalam bidang penyedia data, BPS Kalimantan Barat memiliki ketergantungan yang tinggi terhadap teknologi informasi. Berdasarkan observasi dan wawancara, masih terdapat serangan virus maupun *malware* yang diakibatkan oleh kurangnya pengetahuan pegawai mengenai keamanan informasi sehingga mempengaruhi aset lainnya, seperti data, jaringan, perangkat lunak dan perangkat keras yang menyebabkan terjadinya gap

p-ISSN : 2338-493X
e-ISSN : 2809-574X

(kesenjangan) pada pengamanan informasi yang ingin dicapai serta belum memiliki dokumen kontrol keamanan untuk menangani risiko keamanan informasi.

Pada dasarnya, BPS Kalimantan Barat dapat menghindari atau mengurangi risiko keamanan informasi yaitu dengan merencanakan, mengantisipasi dan melakukan rencana peningkatan keamanan informasi kedepannya melalui manajemen risiko keamanan yang berpotensi menyebabkan kerugian bisnis. Salah satu kerangka kerja untuk meminimalkan dampak risiko dan peningkatan keamanan informasi BPS Kalimantan Barat adalah *National Institute of Standards and Technology Cybersecurity Framework.* Kerangka ini berfokus pada business drivers untuk memandu kegiatan keamanan siber dan mempertimbangkan risiko keamanan siber sebagai bagian proses manajemen risiko perusahaan [2]. Kerangka NIST *Cybersecurity* didukung oleh standar ISO/IEC 27001:2013 sebagai mitigasi risiko yang memberikan langkah rekomendasi kontrol untuk menangani risiko yang dirancang dalam dokumen Sistem Manajemen Keamanan Informasi (SMKI) sehingga dapat meningkatkan keamanan informasi pada tingkat yang ingin dicapai.

Dalam hal ini, pengamanan informasi tidak cukup dilakukan dari sisi teknis saja, tetapi juga diperlukan suatu analisis dan manajemen risiko untuk memperoleh gambaran terhadap berbagai kemungkinan risiko yang muncul di dalam organisasi. Untuk itu, peneliti melakukan manajemen risiko keamanan informasi menggunakan kerangka NIST Cybersecurity dan ISO/IEC 27001:2013 pada BPS Kalimantan Barat diharapkan dapat membantu meminimalkan risiko dan melakukan peningkatan keamanan informasi menjadi efektif dan efisien.

2. LANDASAN TEORI

2.1 Aset Informasi

Aset informasi berupa kombinasi terorganisir dari software, hardware, people, data dan network yang saling berhubungan. Pengertian hardware, software, people, data, dan network, yaitu [3]:

1. *Hardware* atau perangkat keras adalah suatu perangkat yang dapat menerima, memproses program, dan menampilkan data dan informasi.
2. *Software* adalah kumpulan program yang memungkinkan hardware untuk memproses dan mengelola data.
3. Data memuat sekumpulan fakta dari suatu hal yang diperoleh dari pengamatan sumber tertentu, dapat berupa angka, huruf, angka, suara, dan gambar.
4. *Network* ialah sistem koneksi yang menghubungkan perangkat komputer yang berbeda untuk berbagi sumber daya.
5. *People* merupakan individu atau pengguna yang menggunakan hardware dan software, berinteraksi, dan memanfaatkan hasil keluaran dari perangkat tersebut.

2.2 Manajemen Risiko

International Organization for Standardization mengemukakan manajemen risiko adalah sebuah aplikasi sistematik dalam kebijakan ketentuan, konsultasi, pengelolaan, langkah-langkah dalam aktivitas komunikasi, ruang lingkup, mengidentifikasi, mengevaluasi, menganalisa, memantau, dan meninjau suatu risiko [4].

2.3 Keamanan Informasi

Gambar 1 Triad CIA[5]

Berdasarkan Gambar 1, terdapat 3 prinsip utama dari keamanan informasi, yaitu[5]:

1. Kerahasiaan (*Confidentiality*), adalah mencegat adanya akses dari pihak yang tidak berwenang serta memproteksi informasi bersifat rahasia.
2. Ketersediaan (*Availability*), adalah memastikan kelengkapan informasi bisa diakses dan digunakan setiap saat diperlukan tanpa adanya gangguan.
3. Integritas atau (*Integrity*), adalah menjaga informasi dan melindunginya dari korupsi, kerusakan dan perubahan serta

p-ISSN : 2338-493X
e-ISSN : 2809-574X

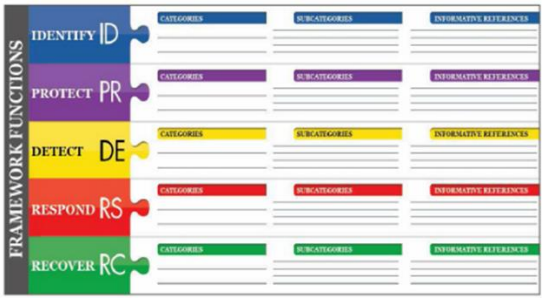
memastikan informasi tidak berubah dari bentuk dari aslinya.

2.4 *National Institute of Standards and Technology Cybersecurity Framework*

NIST *Cybersecurity Framework* adalah kerangka kerja untuk melindungi organisasi atau instansi terhadap ancaman siber. NIST *Cybersecurity* menyediakan bahasa yang umum untuk memahami, mengelola, serta mengungkapkan risiko keamanan siber baik kepada pemangku kepentingan internal maupun eksternal[2]. Terdapat tiga komponen utama dalam *Cybersecurity Framework*, antara lain[2]:

1. *Framework Core*

Pada kerangka inti terdiri dari aktifitas dan kontrol keamanan siber organisasi dengan menyesuaikan hasil yang dinginkan dan tindakan yang akan dilakukan untuk mengurangi risiko yang akan dialami pada sistem yang sudah berjalan. Gambar 2 berikut merupakan struktur dari kerangka inti, yaitu:



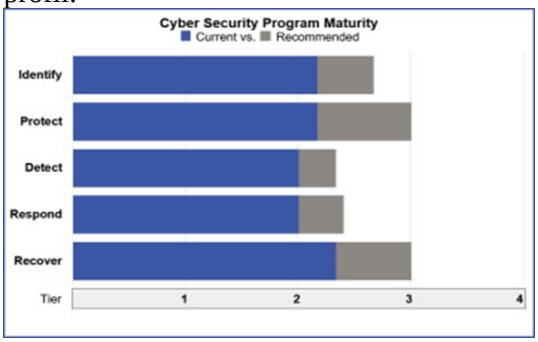
Gambar 2 *Framework Core Structure*[2]

2. *Framework Implementation Tier*

Pada kerangka implementasi tier (tingkatan) menggambarkan bagaimana proses mengukur keamanan siber untuk mengurangi risiko pada sistem yang ada. Tiers juga memberikan gambaran tentang karakteristik tingkat kematangan pada manajemen risiko. Adapun empat tingkatan dalam kerangka, yaitu: partial (Tingkatan 1), risk-informed (Tingkatan 2), repeatable (Tingkatan 3), adaptive (Tingkatan 4).

3. *Framework Profile*

Profil menggambarkan bagaimana keamanan informasi ditangani dalam organisasi, baik *current profile* dan *target profile*. Kerangka ini dapat menyediakan hasil keamanan informasi organisasi, serta kewajiban dan persyaratan keamanan, sehingga organisasi memerlukan pemahaman yang kuat terkait *current profile* dan *target profile* sebelum dapat mencapai tujuan keamanan informasinya. Perbandingan profil (Profil Saat Ini dan Profil Target) secara menunjukkan kesenjangan yang ada untuk memenuhi tujuan manajemen risiko keamanan informasi. Berikut Gambar 3, merupakan gambaran dari perbandingan profil.



Gambar 3 Perbandingan *Current* dan *Target Profile*[6]

2.5 Langkah-langkah Implementasi NIST *Cybersecurity Framework*

Dalam mengimplementasikan program keamanan informasi tersedia tujuh langkah yang dapat diulang untuk terus meningkatkan kemampuan keamanan siber, yaitu[2]:

1. Prioritas dan cakupan

Organisasi menentukan tujuan, misi bisnis dan prioritas organisasi. Setelah informasi didapat, maka organisasi dapat membuat strategi keputusan terkait implementasi kemananan dan menentukan ruang lingkup sistem dan aset yang mendukung proses bisnis.

2. Orientasi

Dalam fase ini organisasi juga dapat mengidentifikasi ancaman dan kerentanan berlaku untuk sistem dan aset tersebut. Berikut Tabel 1 merupakan peninjauan kemungkinan skenario terjadi[7].

Tabel 1 Kriteria Kemungkinan

Score	Kemungkinan	Deskripsi
1	Sangat Jarang (*Rare*)	Hampir tidak pernah terjadi
2	Jarang (*Unlikely*)	Jarang Terjadi
3	Mungkin (*Possible*)	Mungkin Bisa Terjadi
4	Sering (*Likely*)	Sering Terjadi
5	Sangat Sering (*Almost Certain*)	Hampir Sering Terjadi

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Pada Tabel 2,pemetaan kriteria terhadap perkiraan dampak bisnis[7].

Tabel 2 Kriteria Dampak (*impact*) Risiko

Score	Dampak	Deskripsi
1	Sangat Rendah (*Insignificant*)	Dampak diabaikan dan tidak mengganggu aktifitas.
2	Kecil (*Minor*)	Dampak kecil dan dapat diatasi dengan prosedur sederhana.
3	Sedang (*Moderate*)	Dampak tergolong sedang, dapat dikelola dengan prosedur tertentu.
4	Besar (*Major*)	Dampak besar, berpotensi pada biaya finansial dan terhambatnya kinerja.
5	Sangat Tinggi (*Catastrophic*)	Dampak ekstrim, berpotensi besarnya biaya finansial dan terhentinya kinerja.

3. Membuat profil saat ini

Organisasi mengembangkan *current profile* dengan memaparkan hasil kategori dan subkategori dari kerangka kerja NIST *Cybersecurity* saat ini tercapai.

4. Melakukan penilaian risiko

Setelah aset dan risiko atau kerentanan yang menyertainya telah diidentifikasi, akan ditentukan skala atau skor risiko. Risiko dapat diukur dengan menggabungkan dampak dengan kemungkinan risiko yang mungkin terjadi. Skor risiko divisualisasikan dalam matriks kemungkinan atau dampak pada perusahaan. Berikut Tabel 3, pemetaan skor risiko berdasarkan matriks resiko[7].

Tabel 3 Matriks Risiko

LIKEHOOD						
	5	Moderate	Moderate	High	High	High
	4	Low	Moderate	High	High	High
	3	Low	Low	Moderate	High	High
	2	Low	Low	Moderate	Moderate	Moderate
	1	Low	Low	Low	Moderate	Moderate
		1	2	3	4	5
		IMPACT				

Kemungkinan skenario terjadi diberikan oleh ancaman yang mengeksploitasi kerentanan dengan kemungkinan tertentu. Adapun rumus untuk menghitung level risiko, yaitu:

Level Risiko = Dampak x Kemungkinan (1)

Pada Tabel 4, menjelaskan level pada risiko[7].

Tabel 4 Level Risiko

Level Risiko	Keterangan
High Risk – Risiko Tinggi	Termasuk risiko kategori berbahaya yang harus diatasi sesegera mungkin.
Moderate Risk – Risiko Sedang	Risiko yang harus dimonitor dan memerlukan penanganan berkelanjutan.
Low Risk – Risiko Rendah	Risiko yang tidak berbahaya dan memiliki tingkat pengaruh paling kecil terhadap perusahaan.

Adapun Tabel 4 dijelaskan terkait level risiko yang didapat melalui pemetaan dari matriks risiko, level risiko dibagi menjadi tiga, yaitu: *High*, *Moderate* dan *Low*. Setelah risiko dianalisis dan dinilai maka selanjutnya adalah mitigasi risiko.

5. Membuat profil target

Profil untuk status manajemen keamanan siber apa adanya didirikan, dalam langkah ini keadaan yang akan datang didefinisikan. Organisasi membuat dan menetapkan profil target yang berfokus pada penilaian kategori dan subkategori dalam inti kerangka yang memaparkan hasil keamanan siber yang diinginkan.

6. Menentukan, menganalisis, dan memprioritaskan kesenjangan

Organisasi membandingkan current profile dan target profile untuk menentukan kesenjangan (gap). Analisis Gap merupakan alat evaluasi bisnis berfokus pada kesenjangan keamanan perusahaan saat ini dengan keamanan perusahaan yang ditargetkan [8]. Perhitungan Gap dilakukan dengan rumus:

Gap = Current Profile – Target Profile (2)

Setelah Gap ditemukan, dapat mendorong organisasi untuk membuat keputusan yang

p-ISSN : 2338-493X
e-ISSN : 2809-574X

tepat tentang aktivitas keamanan dan mendukung manajemen risiko.

7. Implementasikan rencana aksi

Ketika rencana dibuat dan sumber daya ditentukan, langkah terakhir adalah untuk melaksanakan rencana itu. Organisasi menentukan tindakan mana yang harus diambil untuk mengatasi kesenjangan.

2.6 ISO/IEC 27001:2013

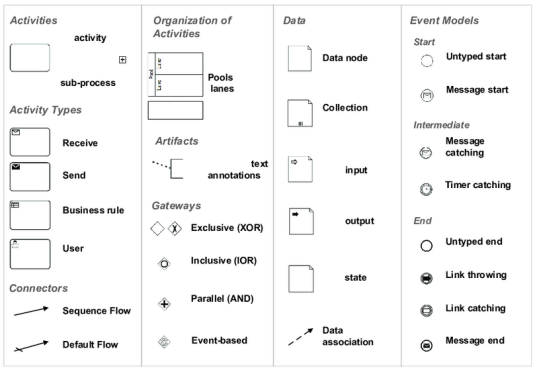
Memuat persyaratan yang harus dipenuhi dalam upaya untuk menggunakan konsep keamanan informasi yang berlaku secara internasional untuk suatu organisasi. Standar ini menetapkan persyaratan untuk pembentukan, implementasi, pemeliharaan dan peningkatan Sistem Manajemen Keamanan Informasi (SMKI) dalam konteks organisasi secara berkelanjutan[9].

2.7 ISO/IEC 27002:2013

Berisikan panduan yang memaparkan dan menjelaskan berbagai contoh penerapan keamanan informasi dengan menggunakan bentuk gambaran kontrol yang tersedia agar organisasi dapat mencapai sasaran kontrol. Bentuk kontrol yang tersedia seluruhnya melibatkan 14 area klausul kontrol seperti mana ditetapkan dalam ISO/IEC 27001[10].

2.8 *Business Process Modelling Natation*

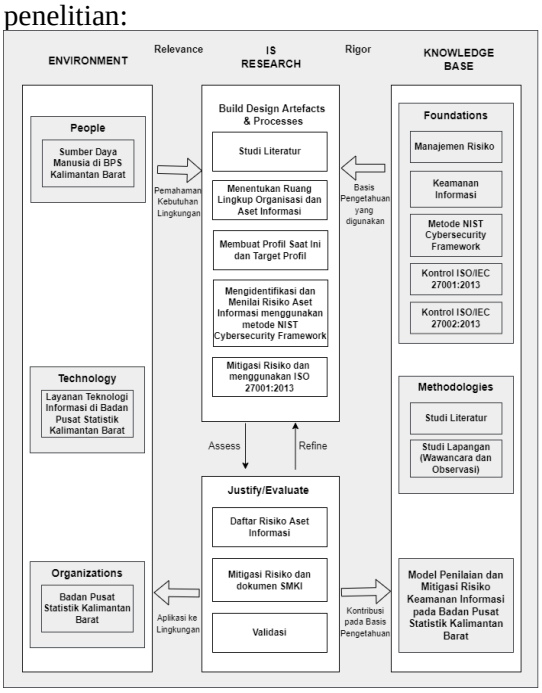
BPMN merupakan sebuah standar yang memodelkan proses bisnis perusahaan dengan menyajikan notasi grafis dalam mememaparkan suatu proses bisnis. Pada Gambar 4, menunjukkan beberapa kategori elemen pada BPMN [11].



Gambar 4 Elemen-Elemen BPMN[11]

3. METODE PENELITIAN

Metodologi penelitian menggunakan kerangka penelitian *IS Research* yang memaparkan tahapan pelaksanaan penelitian. Berikut Gambar 5, merupakan metodologi penelitian:



Gambar 5 Metodologi Penelitian

Langkah awal penelitian ini adalah menentukan ruang lingkup organisasi, yakni proses bisnis secara umum pada BPS Kalimantan Barat. Proses bisnis diidentifikasi melalui wawancara dan observasi yang digambarkan melalui diagram BPMN. Setelah proses bisnis diketahui, maka akan teridentifikasi aset informasi. Langkah selanjutnya adalah menentukan current dan target profile untuk mengetahui kesenjangan penanganan keamanan informasi. Apabila sudah mengetahui nilai kesenjangan pada kategori NIST *Cybersecurity*, maka dilakukan analisis untuk mengidentifikasi kerentanan dan ancaman yang akan ditimpulkan dari kesenjangan tersebut terhadap aset informasi. Selanjutnya, penilaian risiko yang dapat dilaksanakan setelah kemungkinan dan dampak ditentukan. Risiko dapat diukur dengan menggalikan nilai dampak dengan kemungkinan risiko sehingga menghasilkan skor risiko. Kemudian, penentuan level risiko dengan menyesuaikan hasil dari skor risiko pada matriks risiko. Level risiko pada masing-masing aset diketahui, dilakukan tindakan mitigasi dan pembuatan SMKI berdasarkan kontrol keamanan ISO/IEC 27001:2013 serta

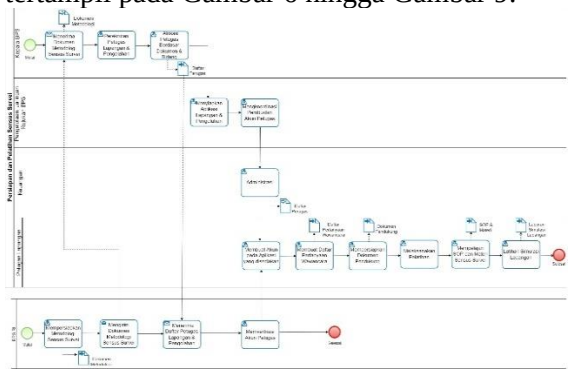
p-ISSN : 2338-493X
e-ISSN : 2809-574X

ISO/IEC 27002:2013 sebagai pedoman penerapan kontrol keamanan informasi.

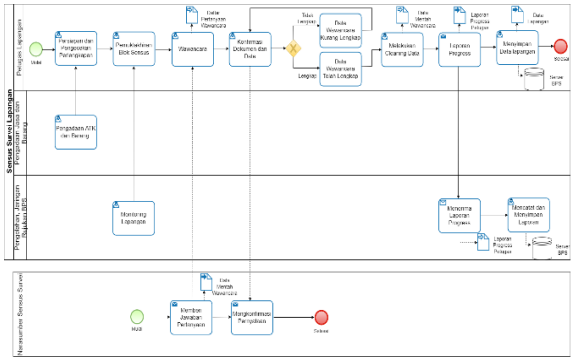
4. HASIL DAN PEMBAHASAN

4.1 Proses Bisnis BPS Kalimantan Barat

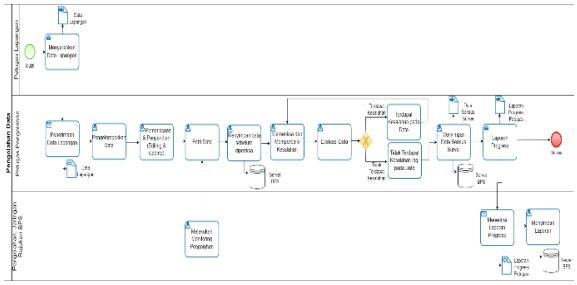
Untuk mengetahui proses bisnis yang ada pada BPS Kalimantan Barat, dilakukan wawancara, *brainstorming* mengenai proses bisnis secara umum dan mempelajari dokumen pendukung lainnya. Dalam menguraikan proses bisnis, akan dilakukan menggunakan pemodelan *Business Process Modelling Notation* (BPMN) untuk mengidentifikasi setiap aset informasi, tertampil pada Gambar 6 hingga Gambar 9.



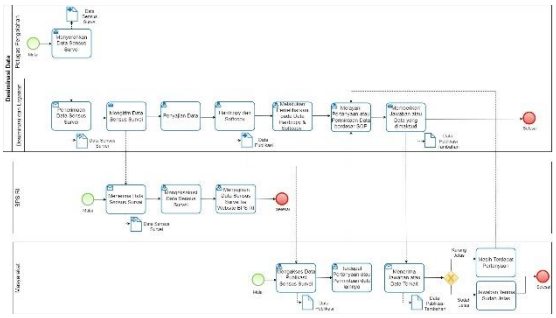
Gambar 6 Persiapan dan Pelatihan Sensus Survei



Gambar 7 Sensus Survei Lapangan



Gambar 8 Pengolahan Data



Gambar 9 Desiminasi Data

4.2 Mengidentifikasi Aset Informasi Berdasarkan Proses Bisnis BPMN

Proses bisnis BPS Kalimantan Barat secara umum telah diuraikan menggunakan BPMN, maka akan teridentifikasi aset informasi pada setiap aktivitas, masukkan, keluaran maupun teknologi informasi dapat dilihat pada Tabel 5.

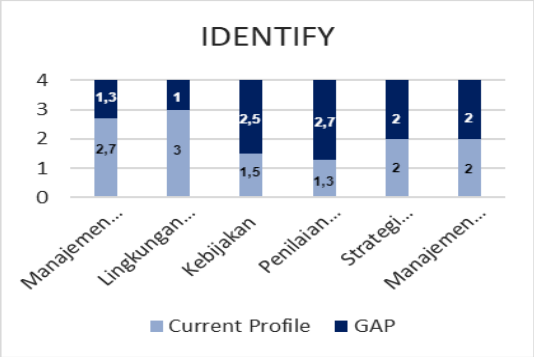
Tabel 5 Pemetaan Aset Informasi

Hardware	Software	People	Network	Data
PC, Server, UPS	Simitra	Kepala BPS, Keuangan Jaringan Rujukan, Petugas Sensus Survei	Internet ,Router, VPN, *Access Point*, UTP	Dokumen Metodologi Data Petugas, Daftar Wawancara
PC, Server, UPS	E-learning BPS	Jaringan Rujukan, Petugas Sensus Survei	Internet ,Router ,*Access Point*, UTP	SOP dan Materi
Laptop	ICS	Petugas Lapangan	Internet	Data Lapangan
PC, Server, Scanner, UPS	Coolsis	Petugas Pengolahan	Internet, VPN, Router, *Access Point*, UTP	Data Sensus Survei
PC, Server, UPS	Monitoring BPS	Jaringan Rujukan	Internet, VPN, *Access Point*, Router	Laporan Sensus Survei
PC, Server, UPS, Printer	Website BPS Kalbar	Desiminasi dan Layanan	Internet, VPN, Router, *Access Point*, UTP	Data Publikasi Sensus Survei

p-ISSN : 2338-493X
e-ISSN : 2809-574X

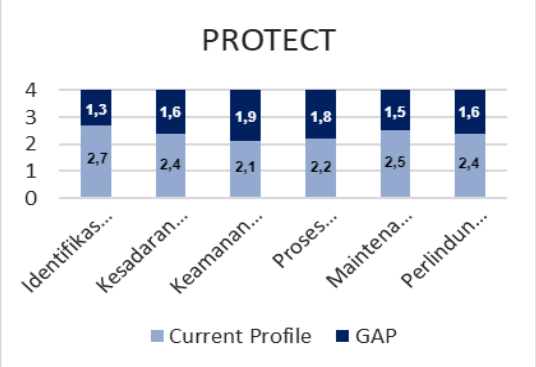
4.3 Menentukan Current Profile dan Target Profile

Dengan mengombinasikan ketiga komponen kerangka (*core, tier, profile*) akan membantu BPS Kalimantan Barat mengetahui kesenjangan penanganan keamanan informasi dalam aktivitas keseharian. Kerangka inti pada NIST *Cybersecurity* terdapat 5 fungsi, 23 kategori dan 108 subkategori. Masing-masing subkategori akan dinilai dengan menggunakan tingkatan pencapaian berdasarkan keadaan perusahaan saat ini (*current profile*) serta target kedepannya (*target profile*). Untuk melihat lebih jelas gap pada BPS Kalimantan Barat di setiap fungsi kategori NIST *Cybersecurity*, akan divisualisasi menggunakan diagram berikut:



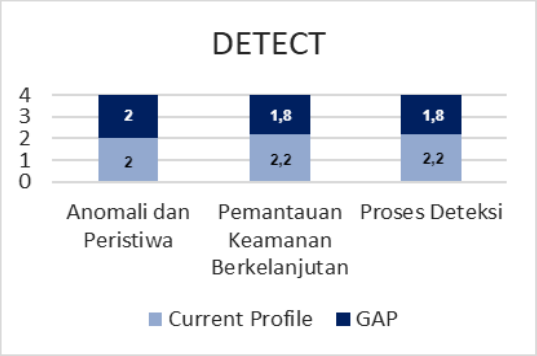
Gambar 10 Gap pada Fungsi *Identify*

Berdasarkan Gambar 10, kategori penilaian risiko memiliki nilai kesenjangan tertinggi sebesar 2,7 dibandingkan kategori lainnya pada fungsi *Identify*. Kesenjangan tersebut diakibatkan BPS Kalimantan Barat tidak mempunyai kebijakan terkait penilaian risiko terhadap aset informasi sehingga BPS tidak memiliki persiapan ketika risiko terjadi.



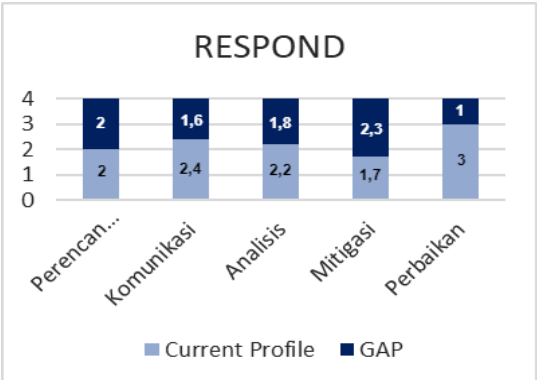
Gambar 11 Gap pada Fungsi *Protect*

Berdasarkan Gambar 11, kategori keamanan data memiliki nilai kesenjangan tertinggi sebesar 1,9 dibandingkan kategori lainnya pada fungsi *Protect.* Kesenjangan tersebut diakibatkan masih minimnya pengetahuan pengamanan data dari sisi pegawai pada BPS Kalimantan Barat, baik data perusahaan maupun data pribadi sehingga kategori keamanan data memiliki kesenjangan tertinggi walaupun sudah ditetapkan kebijakan keamanan data.



Gambar 12 Gap pada Fungsi *Detect*

Berdasarkan Gambar 12, kategori anomali dan peristiwa memiliki nilai kesenjangan tertinggi sebesar 2 dibandingkan kategori lainnya pada fungsi *Detect*. Kesenjangan tersebut diakibatkan kurangnya BPS Kalimantan Barat untuk menganalisis dan memahami peristiwa keamanan sehingga instansi BPS tidak mengetahui sumber ancaman maupun metode serangan yang dilakukan oleh penyusup walaupun sudah memasang firewall pada jaringan.



Gambar 13 Gap pada Fungsi *Respond*

Berdasarkan Gambar 13, kategori mitigasi memiliki nilai kesenjangan tertinggi sebesar 2,3 dibandingkan kategori lainnya pada fungsi *Respond*. Kesenjangan tersebut diakibatkan proses mitigasi risiko saat ini pada BPS Kalimantan Barat tidak dijalankan secara menyeluruh sehingga jika risiko

p-ISSN : 2338-493X
e-ISSN : 2809-574X

terjadi dan hanya memiliki dampak yang kecil, maka tidak dilakukan penanganan yang berarti.

Gambar 14 Gap pada Fungsi *Recover*

Berdasarkan Gambar 14, kategori perencanaan pemulihan memiliki nilai kesenjangan tertinggi sebesar 2 dibandingkan kategori lainnya pada fungsi *Recover*. Kesenjangan tersebut diakibatkan BPS Kalimantan Barat tidak memiliki kebijakan perencanan pemulihan setelah peristiwa risiko terjadi secara yang matang sehingga BPS tidak rencana untuk memulihkan apa yang dirusak atau diganggu oleh risiko tersebut.

4.4 Identifikasi Risiko

Melihat hasil penilaian gap sebelumnya, masih terdapat nilai kesenjangan yang tinggi pada beberapa kategori NIST *Cybersecurity* yaitu penilaian risiko, keamanan data, anomali dan peristiwa, mitigasi dan perencanaan pemulihan, maka diperlukan analisis untuk mengidentifikasi risiko yang akan ditimpulkan dari kesenjangan tersebut terhadap aset informasi BPS Kalimantan Barat. Berikut Tabel 6 merupakan identifikasi risiko pada setiap aset informasi.

Tabel 6 Identifikasi Risiko

Aset	Risiko	Kode
PC	Terhambat mengakses PC	R1
	Terinfeksi virus	R2
	Terinfeksi virus/malware dan tidak berfungsinya PC	R3
	Pencurian informasi dan eksploitasi pada PC	R4
	PC tidak beroperasi dengan maksimal dan menghapus data penting	R5
Laptop	Terhambat mengakses laptop	R6
	Terinfeksi virus	R7
	Terinfeksi virus/malware dan tidak berfungsinya laptop	R8
	Pencurian informasi dan eksploitasi laptop	R9
	Laptop tidak beroperasi dengan maksimal dan menghapus data penting	R10
	Menggangu lalu lintas jaringan dan mencuri data pribadi	R11
	Hilangnya aset laptop	R12
Server	Server down	R13
	Backup failure	R14
	Terinfeksi virus/malware	R15
	Pencurian informasi dan merusak database server	R16
Printer	Kerusakan pada printer	R17
	Printer tidak berfungsi dengan masimal	R18
	Pencurian Informasi dan data terekspos	R19
Scanner	Kerusakan pada scanner	R20
	Pencurian Informasi	R21
UPS	Backup daya failure	R22
	Kerusakan pada UPS	R23
	Merusak dan menganggu kinerja dari UPS	R24
Monitoring BPS	Adanya akses tidak diketahui dan pencurian informasi	R25
	Kerusakan dan modifikasi database	R26
	Penyusup mengambil ahli akun dan akses tak sah	R27
	Mengambil dan mengubah data	R28
	Meninjeksi malware dan mengeksploitasi informasi sensitive	R29
E-learning BPS	Adanya akses tidak diketahui dan pencurian informasi	R30

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Aset	Risiko	Kode
	Kerusakan dan modifikasi database	R31
	Server Down	R32
	Penyusup mengambil ahli akun dan akses tak sah	R33
	Mengambil dan mengubah data	R34
	Meninjeksi malware dan mengeksploitasi informasi sensitive	R35
Website BPS Kalimantan Barat	Adanya akses tidak diketahui dan pencurian informasi	R36
	Kerusakan dan modifikasi database	R37
	Server Down	R38
	Penyusup mengambil ahli akun dan akses tak sah	R39
	Mengambil dan mengubah data	R40
	Meninjeksi malware dan mengeksploitasi informasi sensitive	R41
Integrated Collection System (ICS)	Adanya akses tidak diketahui dan pencurian informasi	R42
	Server Down	R43
	Penyusup mengambil ahli akun dan akses tak sah	R44
	Error pada aplikasi dan database serta pencurian data	R45
	Mengambil dan mengubah data	R46
	Meninjeksi malware dan mengeksploitasi informasi sensitive	R47
Coolsis	Adanya akses tidak diketahui dan pencurian informasi	R48
	Kerusakan dan modifikasi database	R49
	Penyusup mengambil ahli akun dan akses tak sah	R50
	Mengambil dan mengubah data	R51
	Meninjeksi malware dan mengeksploitasi informasi sensitive	R52
Simitra	Adanya akses tidak diketahui dan pencurian informasi	R53
	Kerusakan dan modifikasi database	R54
	Server Down	R55
	Penyusup mengambil ahli akun dan akses tak sah	R56
	Mengambil dan mengubah data	R57
	Meninjeksi malware dan mengeksploitasi informasi	R58
Internet	Kecepatan internet lambat	R59
	Eksploitasi ke sistem dan jaringan perusahaan	R60
	Pencurian informasi dan menyalahgunakannya	R61
	Kinerja perangkat yang melambat, mencuri dan merusak data	R62
Kabel UTP	Kerusakan kabel	R63
	Terhambatnya aktifitas operasional dan pencurian informasi	R64
Router	Kerusakan Router	R65
	Pencurian informasi dan eksploitasi jaringan	R66
	Adanya akses tidak diketahui dan jaringan tidak stabil	R67
	Menganggu proses perutean perusahaan dan terinfeksi virus/malware	R68
Access Point	Kerusakan *Access Point*	R69
	Koneksi jaringan tidak stabil	R70
	Menganggu proses perutean perusahaan	R71
VPN	Terhambatnya akses ke sistem	R72
	Membobol dan eksploitasi jaringan	R73
	Pencurian informasi dan akses tidak dikenal pada sistem yang terhubung ke VPN	R74
Data Pegawai	Pencurian data pribadi	R75
Data Berkaitan dengan Sensus Survei	Kerusakan data	R76
	Redudansi Data	R77
	Data tidak relevan	R78
	Kebocoran data	R79
	Pencurian data dan menyalahgunakannya	R80

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Aset	Risiko	Kode
	Data tidak sesuai dan relevan	R81
Pegawai BPS Kalimantan Barat	Membuka celah keamanan informasi	R82
	Pengungkapan dan pencurian data pribadi	R83
	Kinerja perangkat terhambat dan pengungkapan data	R84
	Mencuri dan menyabotase database	R85
	Sistem atau perangkat tidak berfungsi dengan semestinya	R86

4.5 Penilaian Risiko

Penilaian risiko dapat dilaksanakan setelah kemungkinan dan dampak ditentukan. Risiko diukur dengan menggalikan nilai dampak dengan kemungkinan sehingga menghasilkan skor risiko. Pada Tabel 7, penilaian risiko yang menghasilkan skor pada setiap aset informasi, yaitu:

Tabel 7 Penilaian Risiko

Kode	Kemungkinan	Dampak	Skor
R1	5	3	15
R2	5	4	20
R3	5	4	20
R4	4	4	16
R5	5	4	20
R6	5	3	15
R7	5	4	20
R8	5	4	20
R9	4	4	16
R10	5	4	20
R11	5	4	20
R12	3	4	12
R13	2	2	4
R14	2	4	8
R15	2	5	10
R16	3	5	15
R17	4	2	8
R18	1	2	2
R19	1	2	2
R20	2	4	8
R21	2	2	4
R22	5	2	10
R23	2	1	2
R24	2	1	2
R25	2	2	4
R26	1	2	2
R27	3	2	6
R28	1	2	2
R29	3	2	6
R30	5	3	15
R31	1	4	4
R32	5	3	15
R33	3	2	6
R34	2	4	8
R35	3	4	12
R36	5	4	20
R37	3	4	12
R38	1	4	4
R39	3	4	12
R40	3	4	12
R41	4	4	16
R42	5	3	15
R43	3	3	9
R44	5	3	15
R45	5	3	15
R46	4	3	12
R47	3	3	9
R48	2	4	8
R49	2	5	10
R50	2	4	8
R51	2	4	8
R52	2	4	8
R53	5	2	10
R54	3	2	6
R55	4	2	8
R56	3	2	6
R57	3	2	6
R58	3	2	6
R59	5	4	20
R60	4	4	16
R61	3	3	9
R62	3	3	9
R63	4	1	4
R64	1	1	1
R65	4	3	12
R66	3	3	9
R67	3	3	9
R68	3	3	9
R69	4	2	8
R70	5	1	5
R71	1	3	3
R72	1	3	3
R73	1	3	3
R74	2	3	6
R75	5	3	15
R76	3	5	15
R77	3	3	9
R78	4	5	20
R79	2	5	10
R80	2	4	8
R81	3	4	12
R82	5	3	15
R83	4	3	12
R84	4	3	12

p-ISSN : 2338-493X
e-ISSN : 2809-574X

Kode	Kemungkinan	Dampak	Skor
R85	5	3	15
R86	3	3	9

Setelah semua skor risiko diketahui, selanjutnya pada Tabel 8 skor risiko akan dipetakan berdasarkan matriks risiko, sebagai berikut.

Tabel 8 Pemetaan Skor Risiko

LIKEHOOD						
	5	R70	R22, R53	R1,R6, R30, R32,R42,R44, R45,R75,R82, R85	R2,R3,R5, R7,R8,R10, R11, R36, R	
	4	R63	R17,R55, R69	R46,R65,R83, R84	R4,R9,R41, R60	R59, R78
	3		R27,R29,R33, R54,R56,R57, R58	R43,R47,R61, R62,R66,R67, R68,R77, R86	R12, R35, R37, R39, R40, R81	R16, R76
	2	R23, R24	R13,R21,R25	R74	R14, R20, R34, R48, R50, R51, R52, R80,	R15, R49, R79
	1	R64	R18,R19,R26, R28	R71,R72,R73	R31, R38	
		1	2	3	4	5
		IMPACT				

Hasil Tabel 8 memperlihatkan bahwa dari 86 ancaman risiko, sebanyak 36 ancaman memiliki kriteria risiko Tinggi, 29 ancaman dengan kriteria risiko Sedang dan 21 ancaman dengan kriteria risiko Rendah. Maka dari itu, selanjutnya akan dilakukan penanganan risiko berupa mitigasi setiap ancaman yang telah dinilai untuk mencegah dan mengurangi risiko keamanan.

4.6 Mitigasi Risiko Menggunakan ISO/IEC 27001:2013

Mitigasi risiko bertujuan untuk dan menentukan pemilihan mitigasi yang tepat serta sesuai sehingga ketika risiko tersebut muncul, hal tersebut dapat ditangani sesuai dengan kesepaktan mitigasi yang dipilih. Strategi mitigasi risiko pada Kantor Badan Pusat Statistik Kalimantan Barat dilakukan berdasarkan pada kontrol ISO/IEC 27001:2013.

4.7 Sistem Manajemen Keamanan Informasi (SMKI)

Setelah pemilihan klausul dan penyesuaian dengan risiko yang dimitigasi, selanjutnya adalah melakukan perancangan dokumen SMKI dengan menguraikan tujuan, referensi, ruang lingkup, kebijakan sesuai dengan ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 sebagai pedoman penerapan keamananan.

5. KESIMPULAN

Kesimpulan berdasar hasil penelitian yang telah dilaksanakan terhadap analisis kesenjangan dan penilaian risiko keamanan informasi pada BPS Kalimantan Barat maka disimpulkan sebagai berikut:

1. Berdasarkan hasil analisis dan penilaian gap menggunakan NIST *Cybersecurity*, terdapat beberapa kategori yang memiliki gap tertinggi dari perwakilan setiap fungsinya, yaitu:
   a. Fungsi *Identify* pada kategori penilaian risiko yang memiliki nilai kesenjangan tertinggi sebesar 2,7.
   b. Fungsi *Protect* pada kategori keamanan data yang memiliki nilai kesenjangan tertinggi sebesar 1,9.
   c. Fungsi *Detect* pada kategori anomali dan peristiwa yang memiliki nilai kesenjangan tertinggi sebesar 2.
   d. Fungsi *Respond* pada kategori mitigasi yang memiliki nilai kesenjangan tertinggi sebesar 2,3
   e. Fungsi *Recover* pada kategori perencanaan pemulihan yang memiliki nilai kesenjangan tertinggi sebesar 2.
2. Berdasarkan hasil analisis risiko terdapat sebanyak 86 ancaman yang tersebar dimasing-masing aset informasi, dimana terdapat 36 ancaman kriteria risiko Tinggi, 29 ancaman kriteria risiko Sedang dan 21 ancaman dengan kriteria risiko Rendah.
3. Rancangan dokumen SMKI dibuat dengan menentukan klausul ISO/IEC 27001:2013 dalam mitigasi risiko dan diperlukan 14 klausul pengendalian keamanan serta ISO/IEC 27002:2013 sebagai prosedur penerapan dan dari ke-14 klausul tersebut.

p-ISSN : 2338-493X
e-ISSN : 2809-574X

6. SARAN

Berdasarkan hasil kajian dan analisis yang telah dilaksanakan dalam penelitian ini, maka terdapat saran sebagai berikut:

1. Bagi Badan Pusat Statistik Kalimantan Barat

   BPS Kalimantan Barat belum pernah melaksanakan penilaian risiko dan belum mempunyai dokumen SMKI sehingga hasil penelitian dapat menjadi kerangka acuan untuk mitigasi risiko.
2. Bagi Jurusan Sistem Informasi

   Penelitian dapat dijadikan literasi dan bahan ajaran terkait Analisis Manajemen Risiko Keamanan Informasi menggunakan metode NIST Cybersecurity Framework dan ISO/IEC 27001:2013 sebagai mitigasi risiko. Dokumen SMKI juga dapat memberikan referensi dan gambaran terkait tahapan perancangan dokumen SMKI.
3. Bagi Peneliti Selanjutnya

   Penelitian ini dapat dijadikan acuan untuk peneliti seterusnya saat melaksanakan analisis dan penilaian risiko keamanan informasi mengkombinasikan kontrol ISO lainnya serta melakukan penilaian tidak terbatas pada bidang IT namun juga ke seluruh bidang agar menjadi perbandingan hasil efektifitas dari penilaian risiko.

DAFTAR PUSTAKA

[1] F. Febrianto and D. I. Sensuse, "Evaluasi keamanan informasi menggunakan ISO / IEC 27002 : studi kasus pada Stimik Tunas Bangsa Banjarnegara," *Infokam*, vol. 2, no. 2013, pp. 21–27, 2017.

[2] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018.

[3] R. Kelly Rainer, Brad Prince, Casey G. Cegielski, "Introduction to Information Systems_ Supporting and Transforming Business-Wiley", 2013.

[4] R. E. Izzaty, B. Astuti, and N. Cholimah, "済無No Title No Title No Title," *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 2013, pp. 5–24, 1967.

[5] M. Syafrizal, "ISO 17799 : Standar Sistem Manajemen Keamanan Informasi," *Semin. Nas. Teknol. 2007 (SNT 2007)*, vol. 2007, no. November, pp. 1–12, 2007.

[6] L. Johnson, "Cybersecurity framework," *Secur. Control. Eval. Testing, Assess. Handb.*, pp. 537–548, 2020, doi: 10.1016/b978-0-12-818427-1.00012-4.

[7] F. L. Nice, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *JUISI*, vol. 02, no. 02, 2016.

[8] A. Sekarwati, T. Gantini, and S. K. Yefta, "Penerapan Domain DSS Cobit 5 pada Analisis GAP dan Kecukupan Layanan Teknologi Informasi," *J. Tek. Inform. dan Sist. Inf.*, vol. 3, no. 3, pp. 609–617, 2017, doi: 10.28932/jutisi.v3i3.703.

[9] British Standard Institution., "ISO/IEC 27001:2013 (2013). Information Tecnology-Security Techniques-Information Security Management Systems-Requirements," *BSI Stand. Limited.*, vol. 27001, no. 2, p. ISO/IEC 27000:2009(E), 2013.

[10] E. Kurniawan and I. Riadi, "Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM," *INTENSIF J. Ilm. Penelit. dan Penerapan Teknol. Sist. Inf.*, vol. 2, no. 1, p. 12, 2018, doi: 10.29407/intensif.v2i1.11830.

[11] E. Bazhenova, "Discovery of Decision Models Complementary to Process Models," no. May, p. 234, 2018.