PERANCANGAN TATA KELOLA KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE) MENGGUNAKAN STANDAR ISO 27001:2013 (STUDI KASUS: DISKOMINFOTIK KABUPATEN BANDUNG BARAT)

DESIGN OF INFORMATION SECURITY GOVERNANCE FOR E-GOVERNMENT USING ISO 27001:2013 STANDARD (CASE STUDY: DISKOMINFOTIK OF WEST BANDUNG REGENCY)

Hikam Haikal Radya Hans Ananza[1], Irfan Darmawan[2], Rahmat Mulyana[3]

[1,2,3] Prodi S1 Sistem Informasi, Universitas Telkom
[1]hikamhaikal@student.telkomuniversity.ac.id, [2]irfandarmawan@telkomuniversity.ac.id, [3]rahmatmoelyana@telkomuniversity.ac.id

Abstrak

Pemerintah telah menjalankan program dalam skala nasional untuk menyelenggarakan Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE berjalan dengan beberapa lingkup, salah satunya adalah lingkup pemerintah daerah. Pemerintah Kabupaten Bandung Barat juga merupakan penyelenggara dari SPBE. Pemerintah Kabupaten Bandung Barat memiliki pelaksana teknis untuk menyelenggarakan SPBE. Pelaksana tersebut adalah Dinas Komunikasi, Informatika, dan Statistik. Mengingat ketergantungan penyelenggaraan SPBE pada penggunaan teknologi yang tinggi, peraturan perundang-undangan yang berlaku mengenai SPBE dan keamanan informasi, dan risiko yang berhubungan dengan keamanan informasi, maka perlu diperhatikan kondisi keamanan informasi organisasi terkait. Untuk itu, diperlukan evaluasi agar dapat mengetahui kondisi tata kelola keamanan informasi pada saat ini dan merekomendasikan pengelolaan tata kelola keamanan informasi agar dapat menjadi lebih baik. Alat yang digunakan untuk mengevaluasi dan merekomendasikan adalah standar ISO 27001:2013. Proses yang dilakukan adalah menganalisis kesenjangan terhadap ISO 27001:2013, memetakan kesenjangan tersebut kepada risiko, menganalisis risiko tersebut, memprioritaskan risiko, dan memberikan rekomendasi sesuai dengan risiko terkait. Rekomendasi yang dihasilkan berupa kontrol personel, kontrol proses, dan kontrol teknologi. Kontrol personel akan menghasilkan pembagian tugas, fungsi, dan kompetensi. Kontrol proses menghasilkan kebijakan keamanan informasi dan *Standard Operating Procedure* (SOP). Kontrol teknologi menghasilkan penggunaan aplikasi untuk mempermudah pekerjaan yang sudah ada. Ketiga control tersebut disusun untuk menangani risiko keamanan informasi dan meningkatkan kualitas tata kelola keamanan informasi.

Kata kunci : Tata Kelola Keamanan Informasi, SPBE, Evaluasi, Analisis Risiko, Kepatuhan.

Abstract

Government has decided to execute a nation-wide program to work on Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE works in several scope, one of the scopes is in region/city scope. West Bandung Regency is one of the executors of SPBE. Within the SPBE execution of West Bandung Regency there is a technical implementer. That technical implementer named as Dinas Komunikasi, Informatika, dan Statistik. Reckoning that there is a high dependency of SPBE towards information technology, the needs to comply with regulations about SPBE and Information Security, and risks about information security, thus there is a need to concern about organization's information security state. Therefore, an evaluation is necessary to discover the current state of information security governance and to recommend a set of information security governance management to make a better information security governance. The tools that is used to evaluate and to recommend is ISO 27001:2013 standard. The processes are to analise the conformity towards ISO 27001:2013, mapping gaps toward risk, risk analysis, risk prioritization, and give a set of recommendation correspond with the risks. The forms of recommendation will be control of people, process, and technology. People control produces a set of job description and competencies. Process control produces information security policy and Standard Operating Procedure (SOP). Technology control produces application usage to ease the work. These controls are built to mitigate risks of information security and improve the quality of information security governance.

Keywords: Information Security Governance, SPBE, *Evaluation, Risk Analysis, Conformity.*

1. Pendahuluan

Pemerintah Indonesia mencanangkan penyelenggaraan pemerintahan berbasis teknologi informasi dan komunikasi atau yang biasa disebut sebagai Sistem Pemerintahan Berbasis Elektronik (SPBE). SPBE perlu diselenggarakan baik oleh Instansi Pusat maupun Pemerintah Daerah, termasuk di dalamnya adalah Pemerintah Kabupaten Bandung Barat. Pemerintah Kabupaten Bandung Barat memiliki Dinas Komunikasi, Informatika, dan Statistik (Diskominfotik) sebagai koordinator dan pelaksana teknis SPBE.

Pelaksanaan SPBE perlu memerhatikan tentang tata kelola keamanan informasi dari SPBE. Terdapat kebijakan yang sudah menjelaskan lebih lanjut, bagaimana seharusnya keamanan informasi dikelola. Kebijakan tersebut adalah Peraturan Menteri Komunikasi dan Informatika No. 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Dalam peraturan ini, disebutkan bahwa terdapat dua jenis pedoman yang dapat digunakan untuk melakukan pengamanan informasi yaitu standar SNI ISO/IEC 27001 atau kerangka kerja Indeks Keamanan Informasi (KAMI) yang disusun oleh Badan Siber dan Sandi Negara.

Peraturan perundang-undangan yang mengatur tentang keamanan informasi telah dibuat untuk menghadapi perkembangan tren ancaman dalam keamanan informasi. Sebagaimana survei yang dilakukan oleh European Union Agency for Network and Information Security (ENISA)[1] yang menunjukkan tentang tentang 15 ancaman terbanyak yang terjadi pada bidang keamanan informasi. Ancaman-ancaman tersebut berurutan dari jumlah tertinggi berupa malware, serangan berbasis web, serangan aplikasi web, botnets, denial of service, serangan fisik atau kehilangan, ancaman dari dalam, phising, spam, exploit kits, pelanggaran hak akses data, pencurian identitas, kebocoran informasi, ransomware, dan spionase.

Dampak yang mungkin muncul ketika terjadi ancaman terhadap keamanan informasi dapat berupa hilangnya data, pengaksesan sistem dan informasi oleh pihak yang tidak berwenang, pengambilan data dan informasi oleh pihak yang tidak berwenang, berhentinya sistem aplikasi dan tidak dapat memberikan layanan yang semestinya, atau bahkan kerusakan pada infrastruktur yang digunakan untuk menjalankan sistem aplikasi. Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat sendiri sudah mengalami beberapa risiko seperti yang sudah disebutkan sebelumnya. Risiko-risiko keamanan informasi yang terjadi pada Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat adalah serangan berbasis web, denial of service, dan malware.

Untuk membantu Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat dalam menghadapi regulasi yang perlu dipatuhi terutama dalam bidang pengelolaan keamanan informasi serta untuk mengetahui dan meminimalkan risiko-risiko keamanan informasi yang ada pada dinas tersebut, dilakukan penggunaan standar ISO 27001:2013 untuk melakukan penilaian dan perancangan rekomendasi mengenai pengelolaan keamanan informasi SPBE Pemerintah Kabupaten Bandung Barat yang penyelenggaraannya dilakukan oleh Dinas Komunikasi, Informatika, dan Statistik.

2. Studi Literatur

2.1. Keamanan Informasi

Keamanan informasi adalah suatu kegiatan atau proses untuk melindungi aspek *Confidentiality* (Kerahasiaan), *Integrity* (Keutuhan), dan *Availability* (Ketersediaan) daripada suatu aset informasi[2]. Perlindungan ketiga aspek dari aset informasi ini dilakukan di semua elemen, baik pada perangkat penyimpanan informasi, perangkat pengolahan informasi, ataupun perangkat keras yang digunakan untuk pemindahan atau transmisi informasi.

Terdapat aspek-aspek yang menjadi fungsi utama dalam pembahasan keamanan informasi. Aspek tersebut adalah aspek kebijakan keamanan informasi, aspek keamanan organisasi, aspek pengklasifikasian aset, aspek keamanan personel, aspek keamanan fisik, aspek komunikasi dan manajemen operasi, aspek kontrol akses, aspek pengembangan dan perawatan sistem, aspek Business Continuity Planning (BCP), dan aspek kepatuhan[3].

2.2. Risiko

Risiko adalah hasil dari Kemungkinan (Probability) suatu kejadian untuk terjadi dan dikombinasikan dengan Dampak (Impact) dari kejadian tersebut[4]. Risiko ditulis dan didokumentasikan dalam bentuk skenario risiko. Skenario risiko adalah deskripsi dari kejadian-kejadian yang mungkin terjadi bersama dengan ketidakpastian dampak yang dibawa. Skenario risiko umumnya mengandung beberapa unsur di dalamnya. Unsur tersebut adalah aktor atau pelaku yang menyebabkan risiko tersebut terjadi, tipe terjadinya risiko, penjabaran dari kejadian yang terjadi, aset atau sumber daya yang terkena dampak dari kejadian tersebut, dan waktu terjadinya risiko.

2.3. ISO 27001:2013

Standar ISO 27001:2013 adalah pedoman yang berisikan tentang klausa-klausa yang perlu dipenuhi dalam rangka penyelenggaraan Sistem Manajemen Keamanan Informasi (SMKI) yang baik. Standar ini memiliki dua bagian, yaitu bagian PDCA (Plan – Do – Check – Act) dan bagian Kontrol Annex.

Kontrol Annex dari ISO 27001:2013 memiliki 14 area untuk dilakukan assessment. Area-area tersebut adalah Kebijakan Keamanan Informasi, Organisasi Keamanan Informasi, Keamanan Sumber Daya Informasi, Manajemen Aset, Kontrol Akses, Kriptografi, Pengamanan Fisik dan Lingkungan, Keamanan Operasi, Keamanan Komunikasi, Akuisisi, Pengembangan, dan Pemeliharaan Sistem, Relasi dengan Supplier, Manajemen Insiden Keamanan Informasi, Aspek Keamanan Informasi dalam Manajemen Kontinuitas Bisnis, dam Kepatuhan

3. Metodologi Penelitian

3.1. Model Konseptual

Model konseptual berguna dalam merumuskan masalah serta rumusan solusi dari permasalahan yang dihadapi. Model ini membantu untuk melakukan penataan masalah ke dalam faktor-faktor yang bersesuaian, serta mempermudah penjelasan mengenai masalah yang ada pada obyek penelitian. Model konseptual yang digunakan adalah analisis kepatuhan terhadap standar ISO 27001:2013, dengan menggunakan tahap analisis penelitian berupa studi literatur, wawancara, dan observasi.

Hasil dari model konseptual tersebut adalah rekomendasi yang disusun berdasarkan profil risiko. Rekomendasi tersebut berada pada tiga aspek, yaitu:

1) Personel, menghasilkan rancangan struktur organisasi, rancangan analisis jabatan, dan kompetensi
2) Proses: menghasilkan rancangan kebijakan dan *Standar Operating Procedure* (SOP), serta
3) Teknologi: menghasilkan penggunaan aplikasi beserta instruksi penggunaannya.

3.2. Sistematika Penelitian

Sistematika penelitian yang digunakan sistematika penelitian *waterfall*, dimana langkah-langkah yang dilakukan dalam penelitian dilakukan secara teratur, bertahap, berkelanjutan, dan menjadi satu siklus utuh penelitian. Adapun tahapan di sistematika penelitian tersebut dapat dilihat pada gambar dan penjelasan di bawah ini.

1) Tahap Inisiasi
   Pada tahap ini terdapat aktivitas yang bertujuan untuk memahami masalah yang ada melalui studi lapangan dan studi pustaka. Hal ini dilakukan untuk dapat memahami masalah yang dialami oleh obyek penelitian serta kesesuaian keadaan obyek penelitian kepada peraturan perundang-undangan yang berlaku. Pemahaman masalah secara studi pustaka dan studi lapangan akan menghasilkan masalah yang sudah diidentifikasi.
2) Tahap Perencanaan
   Aktivitas pertama pada tahapan ini adalah untuk memahami kondisi Sistem Manajemen Keamanan Informasi sebagai obyek penelitian. Pemahaman ini didapatkan dengan melakukan penilaian dengan pencocokan terhadap klausa-klausa yang ada dari standar yang digunakan. Aktivitas selanjutnya adalah penentuan kondisi saat ini. Kondisi yang ada pada saat penelitian ini dilaksanakan perlu disetujui dan disahkan oleh pihak pengelola obyek penelitian.
3) Tahap Analisis
   Dilakukan analisis kesenjangan dari hal-hal yang belum dipenuhi oleh obyek penelitian apabila disesuaikan dengan klausa-klausa yang disediakan dari standar yang digunakan. Aktivitas selanjutnya adalah memetakan hasil analisis kesenjangan kepada risiko keamanan informasi. Pemetaan ini juga termasuk pemetaan kerentanan risiko, pemetaan ancaman risiko, pemetaan kemungkinan risiko, pemetaan dampak risiko, dan pemetaan tingkat risiko. Selanjutnya, risiko akan dianalisis dan diberi kontrol atau rekomendasi yang sesuai sehingga kontrol tersebut dapat digunakan untuk menanggulangi risiko terkait.
4) Tahap Perancangan
   Kontrol yang telah dibuat pada tahap sebelumnya selanjutnya diprioritaskan sesuai dengan tingkat kritikalitas risiko terkait, dampak yang terjadi ketika kontrol tersebut diterapkan, dan cakupan yang terkena dampak kontrol tersebut. Rekomendasi dirancang sesuai dengan kontrol-kontrol yang telah ditetapkan sebelumnya. Rekomendasi ini dirancang untuk dapat digunakan sebagai pedoman atau acuan

agar kondisi Sistem Manajemen Keamanan Informasi dari obyek penelitian dapat ditingkatkan sesuai dengan kekurangan yang dimilikinya.

4. Analisis Data

Data diolah untuk dapat mengetahui kondisi eksisting dari Sistem Manajemen Keamanan Informasi SPBE Kabupaten Bandung Barat yang berada dalam pengelolaan Dinas Komunikasi, Informatika, dan Statistik.

4.1 *Assessment* Kesesuaian terhadap Standar ISO 27001:2013

Dalam tahapan ini, dilakukan *assessment* mengenai kondisi kesesuaian Sistem Manajemen Keamanan Informasi yang dikelola oleh Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat terhadap Standar ISO 27001:2013. *Assessment* ini diperlukan untuk memahami kondisi sistem manajemen keamanan informasi milik Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat. Berikut merupakan hasil dari *assessment* kesesuaian kondisi sistem manajemen keamanan informasi milik Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat terhadap Standar ISO 27001:2013:

Tabel 1 Kepatuhan terhadap ISO 27001:2013

Area dalam Standar	Persyaratan	Keterpenuhan	Tingkat Kesesuaian
A.5 Kebijakan Keamanan Informasi	2	0	0%
A.6 Organisasi Keamanan Informasi	7	3	43%
A.7 Keamanan Sumber Daya Manusia	6	2	33%
A.8 Manajemen Aset	10	6	60%
A.9 Kontrol Akses	14	8	57%
A.10 Kriptografi	2	0	0%
A.11 Pengamanan Fisik Dan Lingkungan	15	5	33%
A.12 Keamanan Operasi	14	4	29%
A.13 Keamanan Komunikasi	7	4	57%
A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem	13	6	46%
A.15 Relasi Dengan Supplier	5	1	20%
A.16 Manajemen Insiden Keamanan Informasi	7	3	43%
A.17 Aspek Keamanan Informasi Dalam Manajemen Kontinuitas Bisnis	4	0	0%
A.18 Kepatuhan	8	4	50%

4.2 Pemetaan Kesenjangan terhadap Risiko

Pada tahap ini, kesenjangan yang belum terpenuhi dari klausa-klausa ISO 27001:2013 dipetakan kepada risiko keamanan informasi. Berikut adalah kategori risiko yang digunakan dan hasil pemetaan risiko:

1. Kriteria Kemungkinan Risiko
   Kemungkinan risiko menggolongkan seberapa mungkin risiko tersebut terjadi pada organisasi tersebut. Berikut pada Tabel 2 adalah kriteria kemungkinan terjadinya risiko yang digunakan:

Tabel 2 Kemungkinan Risiko

	Kriteria Kemungkinan Risiko
Sangat Tinggi	Kemungkinan terjadinya risiko per tahun adalah x > 26
Tinggi	Kemungkinan terjadinya risiko per tahun adalah 18 < x <= 26
Sedang	Kemungkinan terjadinya risiko per tahun adalah 10 < x <= 18
Rendah	Kemungkinan terjadinya risiko per tahun adalah 3 < x <= 10

Sangat Rendah	Kemungkinan terjadinya risiko per tahun adalah x <= 2

2. Kriteria Dampak Risiko
Dampak dari terjadinya risiko digolongkan menjadi beberapa golongan. Pada penelitian ini, dampak risiko dapat dinilai menggunakan dua sudut pandang, yaitu dampak risiko terhadap finansial atau dampak risiko terhadap waktu yang membuat layanan dan informasi tidak dapat digunakan. Berikut adalah kriteria dampak terjadinya risiko yang digunakan:

Tabel 3 Dampak Risiko

Tingkat	Dampak Finansial	Dampak Waktu
Sangat Tinggi	x > 500 Jt	x > 7 Hari
Tinggi	200 Jt <= x <= 500 Jt	3 Hari < x <= 7 Hari
Sedang	50 Jt <= x < 200 Jt	1 Hari < x <= 3 Hari
Rendah	10 Jt <= x < 50 Jt	5 Jam < x <= 1 Hari
Sangat Rendah	x < 10 Jt	x <= 5 Jam

3. Matriks Risiko
Kriteria kemungkinan risiko dan kriteria dampak risiko perlu dikombinasikan untuk dapat mengetahui matriks risiko secara utuh. Selain itu matriks risiko juga dibutuhkan untuk mengklasifikasikan kuadran risiko dimana risiko tersebut berada dan tingkatan pada kuadran tersebut. Berikut merupakan matriks risiko yang digunakan:

Tabel 4 Matriks Risiko

Kuadran Risiko		**Dampak Risiko**				
		Sangat Rendah	**Rendah**	**Sedang**	**Tinggi**	**Sangat Tinggi**
Kemungkinan Risiko	**Sangat Tinggi**	9	15	18	23	25
	Tinggi	6	12	16	19	24
	Sedang	4	10	14	17	22
	Rendah	2	7	11	13	21
	Sangat Rendah	1	3	5	8	20

4. Tingkat Risiko
Terdapat kuadran yang menunjukkan tempat risiko secara tepat pada matriks risiko. Namun selain itu, kuadran juga digunakan untuk mengklasifikasikan tingkatan risiko. Berikut tingkatan risiko yang digunakan:

Tabel 5 Tingkat Risiko

Kategori	Kuadran
Sangat Rendah	1-6
Rendah	7-11
Sedang	12-15
Tinggi	16-19
Sangat Tinggi	20-25

5. Hasil Rangkuman Risiko
   Hasil dari penilaian risiko tersebut dapat adalah penilaian risiko. Penilaian risiko tersebut dapat dirangkum seperti berikut ini:

Tabel 6 Rangkuman Risiko

Kategori	Jumlah Risiko	Persentase
Sangat Rendah (1-6)	0	0%
Rendah (7-11)	2	8%
Sedang (12-15)	4	17%
Tinggi (16-19)	12	50%
Sangat Tinggi (20-25)	6	25%

5. Perancangan Solusi

5.1 Perancangan Solusi Personel

Rekomendasi Personel adalah rekomendasi mengenai struktur organisasi yang ada pada Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat. Rekomendasi Personel ini disusun dengan mengacu pada analisis risiko yang dilakukan sebelumnya. Penyusunan rekomendasi Personel dapat menghasilkan perubahan pada struktur organisasi, tanggung jawab, kompetensi, dan kualifikasi. Perubahan tersebut perlu dilakukan untuk dapat meminimalkan risiko-risiko keamanan informasi yang tidak dapat diterima dan meningkatkan kualitas dan kemampuan dalam mengelola Sistem Manajemen Keamanan Informasi.

Berikut adalah perancangan solusi personel, yaitu dengan melakukan pembagian tugas dan fungsi kepada personel Diskominfotik dalam melakukan:

1) Proses pengamanan informasi yang berkaitan dengan SPBE
2) Pengklasifikasian, pelabelan, peninjauan, dan pengamanan informasi
3) Pengembangan sistem, pengujian sistem, operasional sistem, dan pengelolaan *password* dan kriptografi.
4) Pengamanan area aman, tempat informasi, dan fasilitas pengolah informasi.
5) Pengamanan perangkat secara fisik.
6) *Backup*, peninjauan *event-log*, dan instalasi perangkat lunak.
7) Pendokumentasian proses.
8) Klasifikasi, dokumentasi, dan peninjauan insiden keamanan informasi.
9) Tindakan pengamanan perangkat dan pemulihan layanan.
10) Pengawasan perangkat keras.

5.2 Perancangan Solusi Process

Tugas tiap Personel telah dibagi pada bagian sebelumnya untuk menentukan partisipasinya masing-masing dalam penyelenggaraan Sistem Manajemen Pengamanan Informasi. Tentunya dalam melakukan tugas-tugas tersebut diperlukan adanya pedoman dalam pelaksanaan, sehingga pengamanan informasi bisa dilakukan dengan efektif. Pedoman tersebut bisa dalam bentuk payung hukum maupun pedoman teknis berupa *Standard Operating Procedure* (SOP)

Berikut adalah perancangan solusi berupa kebijakan yang mencantumkan adanya pengaturan mengenai:

1) Pelaksanaan proses SMKI untuk SPBE.
2) Klasifikasi informasi yang terkait dengan SPBE.
3) Penggunaan, pengamanan, dan peninjauan hak akses terhadap informasi sesuai klasifikasi dan aset yang terkait dengan fasilitas pengolahan informasi beserta dengan peninjauan berkala.
4) Penggunaan, proteksi, dan *lifetime* kunci kriptografi dan proses penggunaan *password*.
5) Pemisahan pelaksana dan lingkungan pengembangan sistem, pengujian sistem, dan operasional sistem
6) Area aman dan perimeter pengamanan untuk tempat informasi dan pengolahan informasi.
7) Pengamanan perangkat, pengamanan fisik dari bencana alam dan serangan fisik.

8) *Backup* program dan informasi secara berkala
9) Instalasi perangkat lunak pada sistem
10) Penjagaan informasi yang berkaitan dengan SPBE
11) Pelatihan keamanan informasi bagi pegawai dan kontraktor yang berhubungan dengan SPBE
12) Melarang pegawai menyebarkan informasi atau kredensial terhadap pihak lain
13) Kewajiban pelaksanaan uji aplikasi oleh pengguna aplikasi sebelum dirilis
14) Klasifikasi, dokumentasi, dan peninjauan insiden keamanan informasi.

Berikut adalah perancangan solusi berupa pedoman teknis/*Standard Operating Procedure* (SOP), yang mengatur tentang:

1) Bekerja dalam area aman.
2) Pengawalan untuk pengunjung.
3) Klasifikasi, dokumentasi, dan peninjauan insiden keamanan informasi.
4) Pengamanan diri ketika terjadi bencana alam/kebakaran.

5.3 Perancangan Solusi Teknologi

Rekomendasi aplikasi berguna untuk mempermudah perkerjaan yang sudah ada atau melakukan otomatisasi terhadap proses-proses yang sudah berjalan.

Penggunaan aplikasi mengenai:

1) Password Policy untuk pengharusan penggunaan password yang rumit
2) Pemantauan kondisi server.

6. Kesimpulan

Berdasarkan hasil analisis dan rekomendasi pada Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat dapat ditarik kesimpulan bahwa:

1. Kondisi tata kelola keamanan informasi SPBE yang dikelola oleh Dinas Komunikasi, Informatika, dan Statistik Kabupaten Bandung Barat masih sangat jauh untuk dapat memenuhi persyaratan standar ISO 27001:2013. Hal ini dibuktikan dari kepatuhan yang masih jauh dari 100% dan profil risiko yang masih banyak yang belum dimitigasi.
2. Kondisi tata kelola keamanan informasi mebuktikan diperlukannya rekomendasi. Rekomendasi yang dapat digunakan untuk meningkatkan kualitas tata kelola keamanan informasi pada Dinas Komunikasi, Informatika, dan Statistik adalah sebagai berikut:
    a. Personel : Aspek ini menambahkan staf Sandiman yang berada di bawah Seksi Persandian, menambahkan deskripsi kerja kepada staf Pengelola Sistem dan Jaringan dan Teknisi Alat Elektro dan Alat Komunikasi. Serta, penambahan rekomendasi untuk melakukan perekrutan pegawai tetap dan secara reguler memeriksa capaian tugas yang telah dibebankan
    b. Proses : Aspek ini memberikan rancangan kebijakan Keamanan Informasi sesuai dengan rekomendasi yang disebutkan sebelumnya.
    c. Teknologi : Aspek ini memberikan rekomendasi *tools Password Policy* dan Aplikasi pemantauan kondisi *server*

Daftar Pustaka

[1] ISACA. (2017). Cybersecurity Fundamentals 2nd Edition. Illinois: ISACA.
[2] Whitman, M. E., & Mattord, H. J. (2012). Principles of Information Security (Fourth Edition). Boston: Cengage Learning.
[3] Peltier, T. R., Peltier, J., & Blackley, J. (2005). Information Security Fundamentals. Florida: CRC Press LLC.
[4] ISACA. (2013). COBIT 5 for Risk. Illinois: ISACA.