PERANCANGAN MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN KONTROL ISO 27001 PADA PT. XYZ

DESIGN INFORMATION SECURITY MANAGEMEN USING CONTROL ISO 27001 METHOD FOR PT. XYZ

Amellia Briliant Oktavia[1], Rokhman Fauzi[2], Ryan Adhitya Nugraha[3]

[1]Prodi S1 Sistem Informasi Fakultas Rekayasa Industri, Universitas Telkom
[2]Prodi S1 Sistem Informasi Fakultas Rekayasa Industri, Universitas Telkom
[3]Prodi S1 Sistem Informasi Fakultas Rekayasa Industri, Universitas Telkom
[1]amelliabriliant@student.telkomuniversity.ac.id, [2]rokhmanfauzi@telkomuniveristy.co.id,
[3]ranugraha@telkomuniversity.ac.id

ABSTRAK

PT. XYZ adalah Instansi milik Daerah yang bertanggung jawab atas pengolahan informasi dalam lingkungan Pemerintahan daerah setempat. Menurut Peraturan Wali Kota Bandung No. 195 tahun 2018 Setiap Pemerintahan Daerah yang mengatur Sistem Pemerintahan Berbasis Elektronik. Tujuan dari adanya aturan tersebut adalah untuk pengaturan Tata Kelola pemerintahan. Adapun diperlukan keamanan informasi yang perlu diperhatikan Pemerintahan Daerah. Pada penelitian ini, analisis risiko dilakukan dengan metode OCTAVE-S karena metode ini lebih sistematis dan menyeluruh ke Organisasi, sedangkan untuk perancangan kontrol risiko mengikuti Standar ISO 27001. Hasil dari penelitian ini adalah penyusunan kebijakan mengenai kesadaran keamanan informasi.

Kata kunci : manajemen keamanan informasi, ISO 27001, Analisis risiko OCTAVE-S, SPBE, dll

ABSTRACT

PT. XYZ is a regional agency responsible for processing information in the local government environment. According to Bandung Mayor Regulation No. 195 in 2018 Every Regional Government Needs an Electronic-Based Government System. The purpose of this rule is to regulate governance. Information security is needed that needs to be considered by the Regional Government. In this study, risk analysis is carried out by the OCTAVE-S method because this method is more complete and comprehensive for the organization, while for risk control design follows ISO 27001 Standard. The results of this study are regarding information security policies regarding information security.

Keywords: managing information's security, ISO 27001, Risk Analysis OCTAVE-S, ISMS, etc

1. PENDAHULUAN

Teknologi Informasi telah mengalami perkembangan yang pesat saat ini. Perkembangan teknologi Informasi mengubah budaya dalam kehidupan Manusia. Dengan adanya Teknologi Informasi, Manusia dituntut untuk bertindak praktis dan efisien. Seiring dengan berkembangnya Teknologi Informasi, berbagai Organisasi berlomba lomba untuk menerapkan Teknologi Informasi untuk mempermudah pekerjaan. Saat ini, sudah hampir semua sector sudah menerapkan Teknologi Informasi untuk efisiensi pekerjaan.

Adapun kendala yang dihadapi dalam pengelolaan Aset TI yang dimiliki oleh Pemerintah Daerah, seperti Data hilang, *Corrupt*, serangan *Virus* dan ancaman terhadap Aset TI lainnya (Setyawan & Wijaya, 2018). Masalah keamanan menjadi permasalahan yang penting bagi sebuah Organisasi. Bagaimanapun, semua Organisasi berlomba lomba untuk merancang Infrastruktur yang memiliki keamanan yang cukup kuat. Untuk menanggulangi hal tersebut, perlu dilakukan *Risk Assesment* pada semua Aset TI yang dimiliki. Sebelum melakukan perancangan Manajemen Keamanan, perlu diketaui hasil penelitian Risiko yang dimana Risiko tersebut dapat dilakukan mitigasi untuk penanggulangannya (Alberts & Dorofee, 2001).

Dengan melakukan perancangan Manajemen Keamanan Informasi dengan metode OCTAVE-S memiliki manfaat untuk menangani Risiko terjadinya ancaman pada semua Aset TI yang dimiliki. Penggunaan Metode OCTAVE-S dikarenakan metodenya yang telah didesain dengan baik dan tersedia secara bebas. Metode ini juga bekerja secara kolaboratif pada semua unit bisnis untuk membentuk unit bisnis yang lebih koperatif. Metode ini juga melihat segala aspek Informasi keamanan Risiko TI dari sudut pandang fisik, teknis, dan orang.

Untuk mengatasi permasalahan yang terjadi di PT. XYZ akan dilakukan perancangan tentang manajemen keamanan informasi. Analisis Risiko TI akan dilakukan untuk menjadi pondasi dalam Analisis digunakan yang menjadi pondasi dalam melakukan perancangan Manajemen Kemanan Informasi pada PT. XYZ. Metode yang digunakan dalam penelitian ini adalah OCTAVE-S Framework. Dengan penelitian ini, Penulis merekomendasikan perancangan dengan Framework OCTAVE-S yang diharapkan metode ini bisa menjadi pertimbangan untuk penanganan risiko pada PT. XYZ.

2. TINJAUAN PUSTAKA

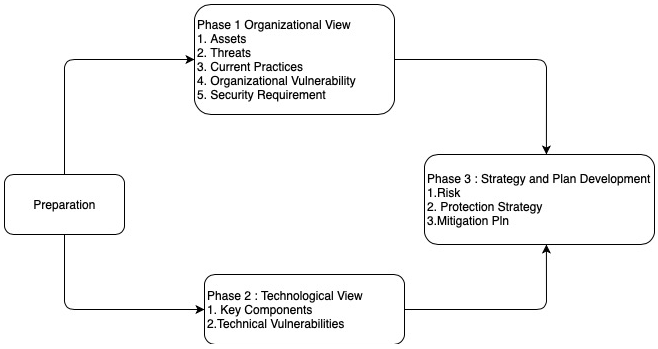
2.1 Aspek Keamanan

Dalam merancang sistem keamanan sistem informasi terdapat aspek-aspek keamanan informasi yang perlu diperhatikan, yaitu :

1. Confidentiality
   Confidentiality merupakan Aspek yang menjamin kerahasiaan informasi atau data dan memastikan informasi hanya dapat diakses oleh pihak yang berwenang.
2. Integrity
   Integrity merupakan Aspek yang menjamin data tidak dapat dirubah tanpa ada ijin pihak yang berwenang, menjaga kelengkapan informasi dan menjaga dari kerusakan atau ancaman lain yang bisa menyebabkan perubahan pada informasi atau data asli.
3. Availability
   Availability merupakan Aspek yang menajamin bahwa data akan tersedia pada saat dibutuhkan dan menjamin user dapat mengakses informasi tanpa adanya gangguan.

2.2 Metode OCTAVE-S

Metode OCTAVE-S menggunakan tiga fase pendekatan untuk menguji isu teknologi, menyusun sebuah gambaran komprehensif keamanan informasi yang dibutuhkan oleh organisasi. Metode ini melakukan diskusi dan pertukaran informasi mengenai asset, praktek keamanan informasi dan strategi kemanan informasi.



Gambar 1 Fase pada Metode OCTAVE-S

Sesuai dengan Gambar 1 dapat dijelaskan bahwa dalam metode OCTAVE-S terdapat 4 fase yang perlu dilakukan. Dimana setiap Fase memiliki fokus masing masing dalam penilaiannya. Pada Fase Pertama dan Kedua dapat dilakukan beriringan sebelum melakukan Fase Ketiga.

2.3 Kontrol ISO 27001

Pada ISO 27001 adapaun model proses atau yang sering disebut dengan *PDAC (Plan, Do , Act, Check)* yang memiliki fungsi berbeda, sebagaimana dengan penjelasannya, sebagai berikut :

- *Plan*
  merupakan tahap dari perancangan dan penerapan Sistem Manajemen Keamanan Informasi, pada tahap ini implementasinya berupa pembangunan komitmen, kebijakan, kontrol, prosedur, instruktur kerja dan yang mendukung terciptanya Sistem Manajemen Keamanan Informasi agar Sistem Manajemen Keamanan Informasi tercipta sesuai yang diinginkan. Sehingga dilakukan analisis kebutuhan untuk menunjang kelengkapan dalam penelitian.

- *Do*
  merupakan implementasi dan operasi dari kebijakan kontrol, proses dan prosedur Sistem Manajemen Keamanan Informasi yang telah dibuat pada tahap *plan*. *Do* meliputi pembuatan kuesioner yang nantinya akan diserahkan kepada bagian TI dan sistem informasi.

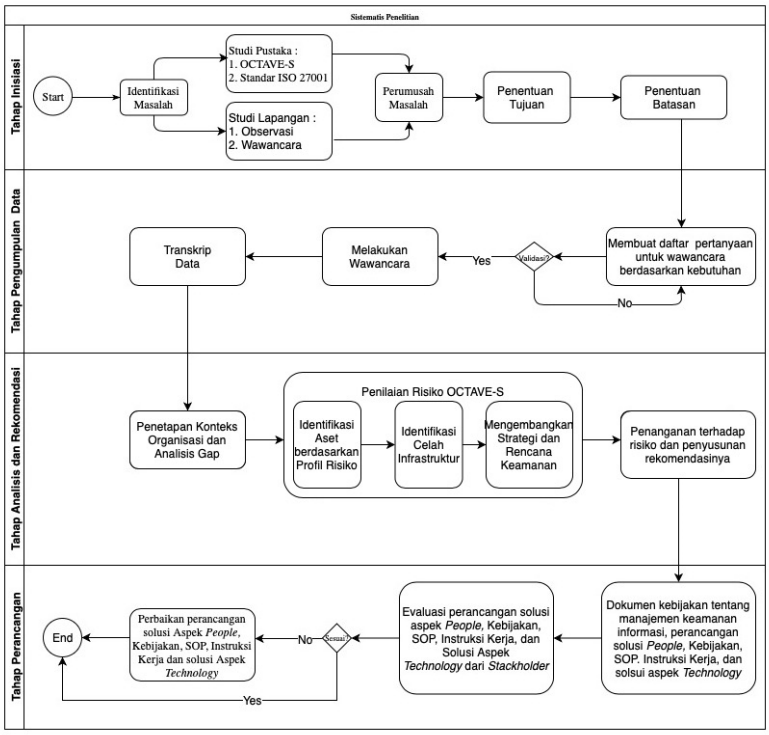
- *Check*

merupakan tahap monitoring pelaksanaan Sistem Manajemen Keamanan Informasi, termasuk pada pelaksanaan pada audit terhadap SMKI. Tahap *Check* meliputi pengolahan kuisoner yang telah dibuat sesuai pada standar ISO 27001.

- *Act*
  merupakan peningkatan serta pemeliharaan Sistem Manajemen Keamanan Informasi, dengan mengambil tindakan pencegahan dan korektif dengan berdasarkan hasil dari internal audit Sistem Manajemen Keamanan Informasi.

3. METODOLOGI PENELITIAN

Pada penelitian ini, langkah awal yang dilakukan adalah studi literature. Lalu melakukan studi kasus yang terjadi di Organisasi dengan menggunakan metode Observasi langsung dengan metode Questioner dan Wawancara. Kemudian Data akan diolah sesuai dengan metode OCTAVE-S untuk menilai risiko aset kritis dan penerapan praktik keamanan di Organisasi.



Gambar 2 Metode Penelitian

Dalam melakukan penilaian risiko dengan metode OCTAVE-S, adapun 3 fase yang diperlu dilakukan, yaitu :

1. Fase 1 – Identifikasi Aset berdasarkan Profil Risiko: Dalam fase pertama memiliki tujuan untuk mengevaluasi terhadap aspek-aspek yang dimiliki oleh perusahaan. Dalam fase ini, tim analisis akan melakukan evaluasi terhadap semua aset yang dimiliki oleh organisasi dan mengkategorikan asset tersebut sesuai dengan prosil risiko.
2. Fase 2 – Identifikasi Celah Infrastruktur : Dalam fase ini memiliki fungsi untuk melakukan Analisa Infrastruktur Informasi. Pada fase ini akan melakukan analisis tingkat keamanan mana yang perlu dipertimbangkan infrastrukturnya untuk dipelihara.
3. Fase 3 – Mengembangkan Strategi dan Rencana Keamanan : Selama fase 3, tim analisis mengidentifikasi risiko aset kritis organisasi dan menentukan apa yang harus dilakukan terhadap risiko aset kritis tersebut.

4. ANALISIS RISIKO

Objek penelitian ini berbentuk Pemerintahan Daerah yang berfokus dalam pengolahan data Pemerintahan di lingkungan setempat. Visi dari Instansi adalah Mewujudnya efektifitas dan efisiensi komunikasi dan informatika penyelenggaraan pemerintah daerah dalam rangka mewujudkan kota bandung sebagai kota jasa bermartabat. Dalam melaksanakan penelitian ini, Analisis Risiko dilakukan dengan metode OCTAVE-S yang terdiri dari 3 Fase.

Table 1 Evaluasi Dampak

Tipe Dampak	Dempak Rendah	Dampak Sedang	Dampak Tinggi
Reputasi	Reputasi Organisasi bisa di perbaiki tanpa memerlukan biaya.	Reputasi Organisasi rusak lalu diperlukan biaya untuk memperbaiki Reputasi.	Reputasi Organisasi rusak atau hancur.
Biaya Operasional	Meningkat kurang dari 5% dalam biaya operasional setiap tahun	Biaya Operasional Meningkat 5-10% setiap tahun.	Biaya Operasional meningkat hingga lebih dari 10% setiap tahun.
Kehilangan Pendapatan Rutin	Lebih dari 5% kehilangan pendapatan pertahun.	Antara 5% sampai 15% kehilangan pendapatan pertahun.	Lebih dari 15% kehilangan pendapatan pertahun.
Kesehatan/Keamanan	Adanya ancaman kesehatan yang memerlukan waktu pemulihan dibawah 1 Minggu.	Adanya ancaman kesehatan yang memerlukan waktu 2-4 Minggu pemulihan	Adanya ancaman kesehatan yang fatal sehingga waktu pemulihan yang diperlukan waktu lebih lama atau bahkan permanen karena tidak dapat di sembuhkan.
Keselamatan	Keselamatan Karyawan di pertanyakan.	Keselamatan Karyawan terpengaruh	Keselamatan Karyawan terlanggar
Denda	Denda yang dikenakan kurang dari Rp 100.000	Denda yang dikenakan antara Rp 100.000 sampai dengan Rp 300.000	Denda yang dikenakan lebih dari Rp 300.000

Table 2 Aset sesuai Kategori

System	Information	Application & Services	Other Assets
• PC • Jaringan • Data Centre • Aplikasi Absensi • Aplikasi Surat Online	• Data Organisasi Perangkat Daerah (OPD) • Data Kepegawaian • Data Keuangan • Data Aset • Data Absensi Pegawai	• Database MySQL, POSTGRE • Server Linux, Sentos, Ubuntu • Microsoft Office • Email	Internet Service Provider

Pada Fase 1 terdapat Proses 1 dan Proses 2 dimana S2 mengidentifikasi informasi keorganisasi. Pada Table 1 menjelaskan mengenai Dampak apa saja yang dimiliki oleh PT. XYZ berdasarkan kategori dampaknya. Kemudian pada Table 2 menjelskan mengenai Aset apa saja yang berhasil di identifikasi berdasarkan Kategori Asetnya.

Table 3 Evaluasi Praktik Keamanan

No.	Area Praktik Keamanan	Spotlight Area
1.	Kesadaran Keamanan dan Pelatihan	Yellow
2.	Strategi Keamanan	Yellow
3.	Manajemen Keamanan	Yellow
4.	Peraturan dan Kebijakan Keamanan	Yellow
5.	Manajemen Keamanan Kolaboratif	Yellow
6.	Rencana Kemungkinan/Pemulijam dari bencana	Yellow
7.	Pengendalian Akses Fisik	Red
8.	Memantau dan mengaudit keamanan fisik	Yellow
9.	Manajemen sistem dan jaringan	Yellow
10.	Pemantauan dan Audit Keamanan TI	Red
11.	Pengesahan dan Otoritas	Red
12.	Manajemen Kerentanan	Yellow
13.	Enkripsi	Yellow
14.	Desain dan Arsitektur	Red
15.	Manajemen Insiden	Red

Keterangan :
Green : Praktik Keamanan telah diimplementasikan dengan Baik
Yellow : Praktik Keamanan telah diimplementasikan Cukup Baik

Red : Praktik Keamanan Belum diimplementasikan.

sedangkan untuk Proses S2 adalah membuat profil ancaman, hasil S2 terdapat pada Table 3 yang menjelaskan mengenai Hasil Evaluasi yang dilakukan dengan Kuesioner yang diisi oleh Responden, dimana hasil ini menjadi acuan dalam penyusunan Fase selanjutnya. Kemudian untuk Fase 2 terdapat proses S3 yaitu melakukan identifikasi terhadap celah Infrastruktur terhadap aset yang dimiliki, Selanjutnya pada Fase terakhir yaitu Fase 3 proses S4 akan dilakuakn evaluasi terhadap profil risiko yang pernah terjadi.

Table 4 Evaluasi Ancaman

No.	Potensi Ancaman	Tipe Ancaman Terkait
1.	Tidak sengaja memasukkan data sehingga terjadi redudansi data, menggunakan computer milik staff lain.	pihak Internal yang bertindak secara tidak sengaja dapat menggunakan akses fisik
2	Membagikan Lisensi Software milik perusahaan.	pihak Internal yang bertindak secara sengaja dapat menggunakan akses fisik
3.	Bencana Alam seperti Banjir yang terjadi, dapat menyebabkan kerusakan pada hardware dan gangguan jaringan.	pihak Eksternal yang bertindak secara tidak sengaja dapat menggunakan akses fisik
4.	Terjadinya Transfer Data sehingga Virus juga ikut Transfigurasi.	pihak Internal yang bertindak secara tidak sengaja dapat menggunakan akses jaringan
5.	Karyawan yang ingin mengambil data perusahaan.	pihak Internal yang bertindak secara sengaja dapat menggunakan akses jaringan

Pada tabel 4 adalah hasil identifikasi dari profil risiko yang dilakukan pada Fase 3. Kemudian untuk Proses terakhir yaitu S5 akan dilakukan evaluasi mengenai rencana mitigasi yang perlu di pertimbangkan oleh PT. XYZ kedepannya. Pada Tabel 5 adalah hasil evaluasi mengenai langkah mitigasi apa yang perlu di terapkan PT. XYZ berdasarkan dengan hasil analisis risiko yang telah di lakukan.

Table 5 Evaluasi Langkah Selanjutnya

Manajemen Sponsorship For Security Improvement Apa yang harus dilakukan manajemen untuk mendukung implementasi hasil OCTAVE-S?	Organisasi harus memprioritaskan keamanan yang di perlukan oleh Organisasi dan mampu mengalokasikan dana untuk pelaksanaan mitigasi. Dan semua staf memiliki kesadaran untuk berpartisipasi dalam pelatihan terhadap aktivitas terkait keamanan
Monitoring Implementation Apa yang akan organisasi lakukan untuk melacak kemajuan dan memastikan bahwa hasil pengukuran ini dilaksanakan	Untuk mengontrol keamanan di perlukan laporan bulanan yang di dapat dipertanggung jawab kan oleh Subbidang keamanan.
Expanding the Current Information Security Risk Evaluation Akankah Anda mengembangkan pengukuran risiko dengan metode OCTAVE-S saat ini untuk menambahkan aset-aset penting?	Untuk saat ini, aset kritis tidak mengalami penambahan jika aktivitas mitigasi belum di terapkan dengan optimal.
Net Information Security Risk Evaluation Kapan sebuah organisasi akan melakukan pengukuran risiko dengan metode OCTAVE-S selanjutnya?	Organisasi dianjurkan untuk melakukan evaluasi OCTAVE-S setiap 1 (satu) tahun sebanyak sekali.

5. HASIL PERANCANGAN

5.1 Identifikasi Risiko

Berdasarkan hasil Analisis terdapat 18 Potential Risk yang berhasil di Identifikasi. Risiko yang berhasil di temukan ini kemudian akan dinilai risikonya berdasarkan Dampak dan Kemungkinana risiko tersebut dapat terjadi. Kemudian hasil ini akan menjadi acuan dalam pemilihan kontrol keamanan sesuai dengan standar ISO 27001.

5.2 Hasil Peranangan

Kemudian setelah Kontrol di tetapkan untuk masing masing risiko, Rekomendasi akan di usulkan berdasarkan degan Tipe Respon Risiko. pada Tabel 6 akan menjelaskan mengenai Kontrol apa saja yang di terapkan dan rekomendasi apa yang di usulkan untuk menangani risiko yang telah di tetapkan.

Table 6 Evaluasi Rekomendasi Kontrol

No.	Klausul	Kontrol Objektif	Kontrol Keamanan	Tipe Respons Risiko	Rekomendasi
1.	A.6 – Organisasi Keamanan Informasi	A.6.1 Organisasi Internal	A.6.1.1 Peran dan tanggung jawab keamanan informasi	*People*	Penambahan Job Deskripsi dalam penanganan tanggung jawab pada Keamanan *Cyber*.
		A.6.2 Perangkat seluler dan *teleworking*	A.6.2.1 Kebijakan perangkat seluler	*Process*	Penambahan kebijakan mengenai standar minimal perangkat yang di gunakan di organisasi.
2.	A.7 – Keamanan SDM	A.7.1 Sebelum Bekerja	A.7.1.2 Syarat dan ketentuan dari pekerjaan	*Process*	Membuat dokumentasi aturan kepegawaian secara legal yang berisi informasi mengenai apa saja yang perlu diperhatikan untuk menjaga keamanan informasi.
		A.7.2 Selama Bekerja	A.7.2.1 Tanggung jawab manajemen	*Process*	Menambahkan pada dokumen kebijakan mengenai hal tentang praktik keamanan untuk menjadi tanggung jawab setiap karyawan.
			A.7.2.2 Kesadaran keamanan informasi, pendidikan serta pelatihan	*People*	Pemberian pelatihan pada karyawan secara rutin untuk meningkatkan kompetensi mengenai Kesadaran pada Keamanan Data Organisasi.
			A.7.2.3 Proses pendisiplinan	*Process*	Menambahkan kebijakan mengenai pendisiplinan karyawan terhadap keamanan dan menerapkan kebijakan tersebut sebelum merekrut karyawan tetap.
3.	A.8 - Manajemen Aset	A.8.2 Klasifikasi Informasi	A.8.2.3 Penanganan Aset	*People*	Memberikan pelatihan terhadap Karyawan mengenai penanganan aset yang menjadi tanggung jawab setiap User di Organisasi.
4.	A.9 – Kontrol Akses	A.9.2 Manajemen akses	A.9.2.4 Manajemen informasi	*Technology*	Penambahan fitur Authentikasi yang berupa pengiriman OTP

No.	Klausul	Kontrol Objektif	Kontrol Keamanan	Tipe Respons Risiko	Rekomendasi
		pengguna	Otentikasi rahasia pengguna		(*One Time Passcode*) pada nomor ponsel/email pengguna untuk validasi saat Login.
		A.9.4 Kontrol akses sistem dan aplikasi	A.9.4.2 Prosedur *log-on* yang aman	*People*	Menambahkan Kompetensi Karyawan terhadap praktik keamanan *cyber.*
			A.9.4.3 Sistem Manajemen *Password*	*Technology*	Mengaktifkan fitur *2 Factor Authentication* untuk memvalidasi pengguna saat login.
5.	A.11 - Fisik dan Keamanan Lingkungan	A.11.2 Peralatan	A.11.2.3 Keamanan kabel	*Process*	Menerapkan aturan tertulis mengenai manajemen *Data Centre* sesuai dengan acuan Kebijakan yang di gunakan.
6.	A.13 - Keamanan Komunikasi	A.13.1 Manajemen keamanan jaringan	A.13.1.1 Kontrol Jaringan	*Technology*	Melakukan kontrol jaringan dengan rekomendasi Tools seperti *Wireshark,* dan *Nagios* untuk mempermudah dalam memantau performa jaringan.
			A.13.1.2 Keamanan dari layanan jaringan	*Technology*	Mengaktifkan *firewall* agar layanan tidak dapat diakses dari jaringan publik.
7.	A.14 - Akuisisi, pengembangan dan pemeliharaan sistem	A.14.3 Pengujian data	A.14.3.1 Perlindungan data pengujian	*Technology*	Menggunakan Enkripsi *salt* di mana data yang disimpan ada penambahan karakter acak saat proses *hashing*.
8.	A.15 – Hubungan Supplier	A.15.2 Manajemen pengiriman layanan pemasok	A.15.2.1 Pemantauan dan peninjauan layanan pemasok	*Process*	Membuat dokumen audit secara rutin secara legal antara Pemasok layanan dan PT.XYZ untuk audit layanan.
9.	A.17 - Aspek keamanan informasi dari manajemen kelangsungan bisnis	A.17.2 Redudansi	A.17.2.1 Ketersediaan fasilitas pengolahan informasi	*Technology*	Menggunakan teknologi *Cloud Computing* untuk penyimpanan dan pengolahan data.

6. KESIMPULAN

Hasil dari perancangan Manajemen Keamanan Infformasi pada PT. XYZ yang menggunakan Kontrol sesuai standar ISO 27001 telah dilaksanakan di penelitian ini. Hasil penelitian ini adalah analisis risiko dengan metoide OCTAVE-S, dimana hasil risiko yang berhasil di identifikasi akan dilakukan kontrol yang mengacu pada ISO 270001. Kontrol yang di terapkan ini mencakup pada Aspek *People, Process,* dan *Technology.* Berdasarkan hasil perancangan,

Usulan prioritas ditujukan pada : (1) Penambahan Deskripsi Kerja dan Kompetensi, (2) Penambahan Kebijakan mengenai Praktik Keamanan pada SDM, dan (3) Usulan Tools, Fitur keamanan.

Daftar Pustaka:

[1] A. R. Prabawati, Via Aprilia; Rachmadi, Aditya; Perdanakusuma, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan Kerangka Kerja OCTAVE-S Pada Unit Pengelola Sistem Informasi Dan Kehumasan (PSIK) Fakultas Ilmu Komputer Universitas Brawijaya," *Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 3, pp. 2829–2836, 2019.

[2] C. dkk Alberts, *OCTAVE-S Implementation Guide, Version 1.0 Volume 1: Introduction to OCTAVE-S.* Pittsburgh: Carnegie Mellon University, 2005.

[3] I. P. Putra, Anggi Anugraha; Nurhayati, Oky Dwi; Windasari, "Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071," *Teknol. dan Sist. Komput.*, vol. 4, no. 1, pp. 60–66, 2016.

[4] ISO, *Information Technology- Security Techniques-Information Security Management Systems-Requirements*, 2nd ed. Switzerland: ISO, 2013.

[5] T. I. ASSOCIATION, *Telecommunications Infrastructure Standard for Data Centers*. Arlington, U.S.A: TELECOMMUNICATIONS INDUSTRY ASSOCIATION, 2005.

LAMPIRAN

Hasil Rekomendasi People

<table>
<tr><td>No.</td><td>Item</td><td>Keterangan</td></tr>
<tr><td>1.</td><td>Jabatan</td><td>Pengelola Keamanan Sistem Informasi</td></tr>
<tr><td>2.</td><td>Pimpinan</td><td>Kepala Seksi Persandian dan Keamanan Sistem Informasi</td></tr>
<tr><td>3.</td><td>Kewenangan</td><td>1. Membuat usulan mengenai kebijakan yang perlu di tambahkan.
2. Membuat laporan hasil audit keamanan untuk di serahkan kepada Kepala Persandian dan Aplikasi Informatika.</td></tr>
<tr><td>4.</td><td>Profil Kompetensi Jabatan</td><td>
<table>
<tr><td>No.</td><td>Soft Skill</td><td>Level (5)</td><td>Hard Skill</td><td>Level (5)</td></tr>
<tr><td>1.</td><td>Komunikasi</td><td>3</td><td>Manajemen Kualitas TI</td><td>3</td></tr>
<tr><td>2.</td><td>Kepemimpinan</td><td>3</td><td>Keamanan Informasi</td><td>3</td></tr>
<tr><td>3.</td><td>Manajemen</td><td>3</td><td></td><td></td></tr>
<tr><td>4.</td><td>Decision Making</td><td>3</td><td></td><td></td></tr>
<tr><td>5.</td><td>Negosiasi</td><td>3</td><td></td><td></td></tr>
<tr><td>6.</td><td>Team Work</td><td>3</td><td></td><td></td></tr>
<tr><td>7.</td><td>Problem Solving</td><td>3</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>5.</td><td>Pelatihan dan Sertifikasi Terkait</td><td>
<table>
<tr><td>No.</td><td>Pelatihan</td><td>Sertifikasi</td></tr>
<tr><td>1.</td><td>Manajemen Proyek TI</td><td>PMP (Project Management Professional)</td></tr>
<tr><td>2.</td><td>Keamanan Informasi</td><td>ISO 27001 atau ISO 27002</td></tr>
</table>
</td></tr>
</table>

Hasil Rekomendasi Process

Hal	Pengelolaan Keamanan Informasi Sumber Daya Manusia
Tujuan	Kebijakan Pengelolaan Keamanan Informasi Sumber Daya Manusia ini bertujuan untuk memberi acuan dalam: *1.1 Memastikan bahwa pegawai dan pihak ketiga memahami tanggung jawabnya yang sesuai dengan peran terkait penugasannya, dan untuk mengurangi risiko pencurian, penyalahgunaan dan kesalahan pemanfaatan aset informasi.* *1.2 Memastikan bahwa pegawai dan pihak ketiga mengetahui ancaman maupun hal-hal yang utama dari keamanan, tanggung jawab dan perannya, serta telah dibekali pelatihan untuk mendukung kebijakan keamanan DJP dan mengurangi kesalahan dalam pekerjaannya.*

	1.3 Memastikan bahwa pegawai dan pihak ketiga menjalani prosedur terkait keamanan informasi sebelum, selama, dan saat akan mengakhiri tugas di DJP.
Ruang Lingkup	Kebijakan Pengelolaan Keamanan Informasi Sumber Daya Manusia ini mencakup pengelolaan keamanan informasi terhadap pegawai dan pihak ketiga dan pekerjaan di DJP.
Kebijakan	1. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi mereka yang memiliki akses terhadap aset informasi yang bersifat sangat rahasia dan berharga 2. Seluruh pegawai DJP dan pihak ketiga harus mematuhi kebijakan, pedoman, dan tata cara keamanan informasi yang berlaku 3. Seluruh pegawai DJP harus mendapatkan pendidikan, pelatihan, dan sosialisasi pengelolaan keamanan informasi secara berkala sesuai dengan tingkat tanggung jawabnya masing-masing; 4. Masing-masing pegawai harus melindungi kepemilikan dan kerahasiaan data pribadinya selama yang bersangkutan bekerja di DJP. Data pribadi pegawai tersebut hanya boleh digunakan untuk kepentingan yang diperbolehkan oleh peraturan dan ketentuan perundang-undangan;