ANALISIS DAN PERANCANGAN KEAMANAN FISIK DATA CENTER BERDASARKAN STANDAR TIA-942 MENGGUNAKAN PPDIOO LIFE-CYCLE APPROACH DI PEMERINTAHAN KABUPATEN BANDUNG BARAT

ANALYSIS AND DESIGN PHYSICAL SECURITY DATA CENTER BASED ON TIA-942 STANDARD USING PPDIOO LIFE-CYCLE APPROACH IN WEST BANDUNG DISTRICT GOVERNMENT

Salman Nuzuli[1], Avon Budiyono, S.T., M.T.[2], Almaarif, S.Kom., M.T [3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]salmannuzuli@student.telkomuniversity.ac.id, [2]avonbudi@telkomuniveristy.ac.id,
[3]ahmad.almaarif@gmail.com

Abstrak

***Data center* adalah suatu fasilitas khusus yang disusun untuk pengelolaan dan dukungan sumber daya komputer yang dikelola oleh organisasi untuk tujuan menangani data yang diperlukan untuk operasinya. Dikarenakan *data center* menjadi salah satu komponen yang paling penting dalam lingkungan bisnis, maka aspek keamanan fisik adalah salah satu faktor utama dalam kelancaran berjalannya *data center*. Keamanan fisik juga dapat mencegah terjadinya pencurian fisik data-data organisasi, kerusakan fisik *data center*, dan lain-lain.**

Objek pada penelitian ini adalah DISKOMINFO Kabupaten Bandung Barat. Berdasarkan dari kondisi saat ini, perangkat keamanan fisik pada ruangan *data center* masih tergolong sangat minim, hal ini dapat menyebabkan adanya celah keamanan terhadap *data center* tersebut. Berdasarkan hal tersebut, perlu dilakukan perancangan keamanan fisik *data center* sesuai dengan standarisasi TIA-942 serta menggunakan 3 tahapan awal PPDIOO *Network Life-Cycle Aproach*, yaitu *Implement*, *Operate*, *Design*. Hasil pada penilitan ini berupa rancangan desain keamanan fisik *data center* yang ideal pada DISKOMINFO Kabupaten Bandung Barat. Rancangan tersebut meliputi kontrol akses ruangan menggunakan perangkat card access dan perangkat intrusion detection, *monitoring* ruangan dengan perangkat CCTV, perangkat pendeteksi kebakaran menggunakan flame detector, penambahan personil staf untuk keamanan fisik, serta SOP untuk memasuki ruangan-ruangan *data center*.

Kata kunci : *Data Center*, Pemerintah Kabupaten Bandung Barat, keamanan fisik, TIA-942, PPDIOO *Network Life-Cycle Approach*.

Abstract

Data center is a facility that is arranged for the management and support of computer resources managed by the organization for the purpose of handling data needed for its operations. Because the data center is one of the most important components in the business environment, the physical security aspect is one of the main factors in the smooth running of the data center. Physical security can also prevent physical theft of organizational data, physical damage to data centers, and others.

The object of this research is* DISKOMINFO Pemerintah Kabupaten Bandung Barat. *Based on the current conditions, physical security devices in the data center room are still classified as very minimal, this can cause a security hole for the data center. Based on this, it is necessary to design the physical security of the data center according to the TIA-942 standard and use the 3 initial stages of the PPDIOO Network Life-Cycle Aproach, namely Implement, Operate, Design.

The results of this research are in the form of an ideal data center physical security design at DISKOMINFO, West Bandung Regency. The plan includes room access control using card access devices and intrusion detection devices, room monitoring with CCTV devices, fire detection devices using flame detectors, adding staff personnel for physical security, and SOPs to enter data center rooms.

Keywords: *Data Center*, Pemerintah Kabupaten Bandung Barat, *physical security, TIA-942, PPDIOO Network Life-Cycle Approach*.

1. Pendahuluan

Semakin berkembangnya teknologi pada zaman ini, kemajuan Teknologi Informasi (TI) semakin pesat, yang menjadikan TI sebagai aspek terpenting dalam pemenuhan kebutuhan perusahaan. Adanya TI dipandang dapat memberikan solusi terkait proses-proses bisnis perusahaannya [1]. Sejalan dengan laju pertumbuhan penggunaan teknologi informasi yang sangat cepat, semakin banyak juga data data yang dihasilkan dan perlu disimpan pada suatu wadah, oleh karena itu *data center* hadir sebagai tempat penampungan untuk data- data [2].

Data center adalah suatu fasilitas khusus yang disusun untuk pengelolaan dan dukungan sumber daya komputer yang dikelola oleh organisasi untuk tujuan menangani data yang diperlukan untuk operasinya [3]. *Data center* juga menjadi salah satu komponen penting dalam lingkungan bisnis yang ada saat ini. Sebagai inti dari layanan bisnis, *data center* diharapkan mampu memberikan pelayanan seoptimal mungkin, sekalipun dalam keadaan terjadinya suatu bencana sehingga bisnis dalam perusahaan atau lembaga tersebut tetap bertahan dan keuntungan bagi perusahaan akan terus mengalir [4]. Dikarenakan *data center* menjadi salah satu komponen yang paling penting dalam lingkungan bisnis, maka aspek keamanan fisik adalah salah satu faktor utama dalam kelancaran berjalannya *data center*. Pentingnya keamanan fisik data center bagi lembaga, khususnya pemerintahan, membuat peneliti berminat melakukan penelitian mengenai hal tersebut. Dalam penelitian ini, peneliti menentukan Pemerintah Kabupaten Bandung Barat sebagai lokasi untuk objek penelitian

Pada Pemerintah Kabupaten Bandung Barat terdapat Dinas Komunikasi, Informatika, dan Statistik yang biasa disebut DISKOMINFO. DISKOMINFO Bandung Barat merupakan perangkat daerah yang bertujuan untuk melaksanakan urusan pengelolaan dan layanan informasi publik, pengelolaan komunikasi publik, teknologi informatika, layanan *e-Government* serta statistik dan persandian [5].

Berdasarkan hasil observasi dan wawancara yang dilakukan dengan pihak DISKOMINFO Kabupaten Bandung Barat, kondisi keamanan fisik saat ini pada *data center* DISKOMINFO Kabupaten Bandung Barat masih tergolong sangat minim dan belum menerapkan standar keamanan fisik pada *data center*nya. Oleh karena itu peneliti memberikan solusi yang dapat diterapkan, yaitu dengan melakukan analisis dan perancangan keamanan fisik *data center* menggunakan standar internasional TIA-942 dan pendekatan PPDIOO *Life-cycle approach (Prepare*, *Plan*, *Design*, *Implement*, *Operate*, dan *Optimize)* dengan penggunaan tahapan sampai tahapan design.

2. Dasar Teori

2.1 Definisi *Data Center*

Data center adalah suatu fasilitas untuk menempatkan sistem komputer perangkat perangkat terkait, seperti sistem komunikasi data dan penyimpanan data, yang dikondisikan dengan pengaturan catu daya, pengatur udara, pencegah bahaya kebakaran dan biasanya dilengkapi pula dengan sistem pengamanan fisik [6]. Pengertian lain *data center* menurut [7] adalah bangunan atau bagian dari bangunan yang fungsi utamanya adalah sebagai ruang komputer dan area pendukungnya. Kemudian menurut [8] *data center* adalah tempat yang berisi sumber daya komputasi yang terletak di lingkungan yang terkendali dan di bawah kendali yang terpusat dengan memungkinkan organisasi menggunakannya sebagai pendukung kelangsungan bisnis.

2.2 Keamanan Fisik *Data Center*

Keamanan Fisik adalah keamanan untuk mencegah akses fisik oleh pihak yang tidak berwenang. Menurut [9] keamanan fisik adalah bagaimana menjaga sebuah keamanan fisikal dari *data center* agar *data center* dapat berjalan dengan baik tanpa ada gangguan dari fisikal seperti perusakan pada *data center*, pencurian komponen-komponen *hardware data center*, kebakaran, dan lain-lainnya.

2.3 Serangan Fisikal Pada *Data Center*

Serangan fisikal yang sering terjadi pada *data center*, yaitu [10]:

1. Faktor Lingkungan (*Environmental Factors*)
   Serangan fisikal yang disebabkan oleh faktor-faktor lingkungan seperti suhu ruangan, kelembapan, dan demo karyawan.
2. Bencana alam (*Acts of nature*)
   Serangan fisikal yang terjadi dikarenakan bencana alam ditempat *data center* berada dan tidak dapat diprediksi kejadiannya, contohnya tsunami, gempa bumi, gunung meletus, banjir, dan kebakaran.
3. Seorang yang tidak memiliki hak akses (*Uninvited guests*)
   Serangan fisikal yang terjadi dikarenakan minimnya kontrol akses pada ruangan *data center* yang menyebabkan masuknya orang yang tidak memiliki hak akses (tidak berkepentingan) ke ruangan *data center* yang dapat menimbulkan resiko terjadinya kerusakan infrastruktur dan kehilangan data sensitif pada organisasi.
4. Pencurian Infrastruktur (*infrastructure theft*)
   Serangan fisikal yang terjadi dikarenakan minimnya pengawasan pada ruangan *data center* yang menyebabkan pencurian pada infrastruktur *data center* seperti alat pemadam api, alat pendinginan, serta *server*.

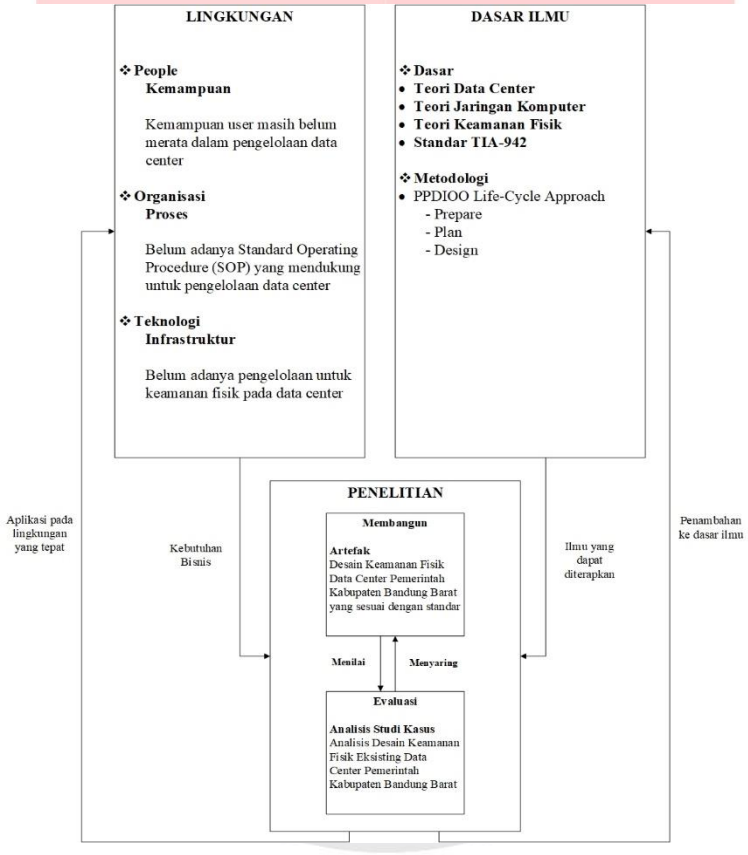
2.4 Standar TIA-942

Telecommunications Industry Association (TIA-942) adalah standar nasional Amerika yang menentukan persyaratan minimum untuk infrastruktur telekomunikasi dari *data center* dan ruang komputer. Topologi yang disiapkan dalam standar ini dimaksudkan untuk diterapkan di semua jenis *data center*. TIA-942 membahas prosedur untuk Jaringan arsitektur, desain listrik, penyimpanan *file*, cadangan dan pengarsipan, redundansi sistem, kontrol dan keamanan akses jaringan, manajemen basis data, hosting web, hosting aplikasi, distribusi konten, kontrol lingkungan, perlindungan terhadap bahaya fisik dan management daya [11].

3. Metodologi Penelitian

3.1 Model Konseptual

Model konseptual adalah representasi dari suatu sistem, terbuat dari komposisi konsep yang digunakan untuk membantu dalam memecahkan masalah. Model konseptual membantu peneliti dalam memberikan gambaran yang berguna untuk menentukan inti permasalahan yang ada lalu memberikan referensi untuk menyederhanakan permasalahan tersebut agar mudah dipahami [12]. Pada model konseptual ini digambarkan model dan sistematika penelitian dari Tugas Akhir tentang Analisis dan Perancangan Keamanan Fisik *Data Center* Berdasarkan Standar TIA-942 Menggunakan PPDIOO *Life-Cycle Approach* di Pemerintahan Kabupaten Bandung Barat. Berikut adalah model konseptual dari penelitian ini.



Gambar 1 Metodologi Penelitian

3.2 PPDIOO Life-Cycle Approach

Gambar 1 mendeskripsikan tentang permasalahan yang ada pada Pemerintah Kabupaten Bandung Barat. Dengan berbagai macam masalah yang terjadi pada *data center* DISKOMINFO Kabupaten Kota Bandung, penelitian ini akan menghasilkan artifak berupa desain keamanan fisik *data center* dengan menggunakan standar TIA-942 dan dengan menggunakan metode PPDIOO *Life-Cycle* yang hanya menggunakan tiga tahapan utama, yaitu *prepare*, *plan*, *design*.

4.Pembahasan

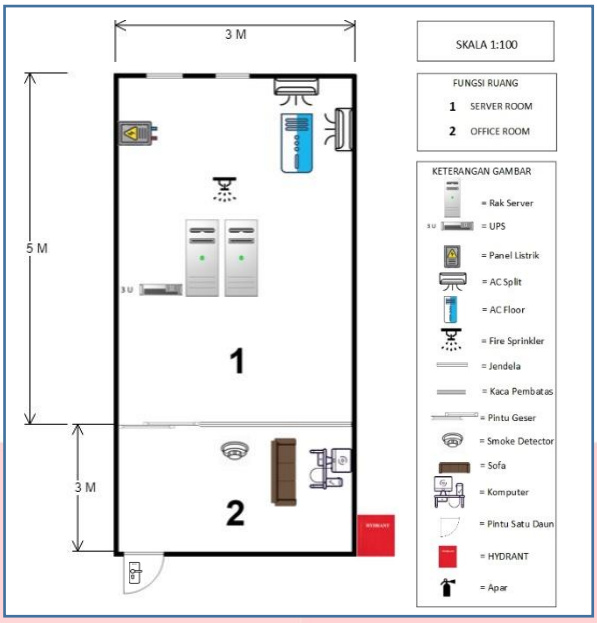
4.1 Rencana Jangka Panjang

Sesuai Peraturan Pemerintah, ditetapkan bahwa setiap daerah diwajibkan untuk menyusun Perencanaan Jangka Panjang (RJP), berikut merupakan rencana perencanaan jangka panjang (RJP) DISKOMINFO agar dapat meningkatkan kinerjanya:

1. Perluasan ruangan *data center.*
2. Peningkatan kualitas dan kuantitas perangkat *data center*.
3. Tersedianya CCTV pada ruang *data center* dan pintu akses menuju ruang *data center*.
4. Tersedianya perangkat kontrol akses pada pintu ruang *data center*.
5. Tersedianya SOP akses masuk ruang *data center*.

4.2 Desain Ruangan *Data Center* saat ini

Gambar 2 merupakan desain ruangan *data center* saat ini pada DISKOMINFO Kabupaten Bandung Barat



Gambar 2 Desain Ruangan Saat ini

Gambar diatas menunjukkan desain ruangan *data center* beserta perangkat-perangkatnya pada *data center* DISKOMINFO Kabupaten Bandung Barat.

4.3 Analisis Gap Kondisi Keamanan Fisik *Data Center* saat ini

Tabel 4.1 berikut ini menunjukkan hasil gap antara kondisi keamanan fisik *data center* saat ini dengan acuan standar TIA-942

Tabel 1 Analisis Gap

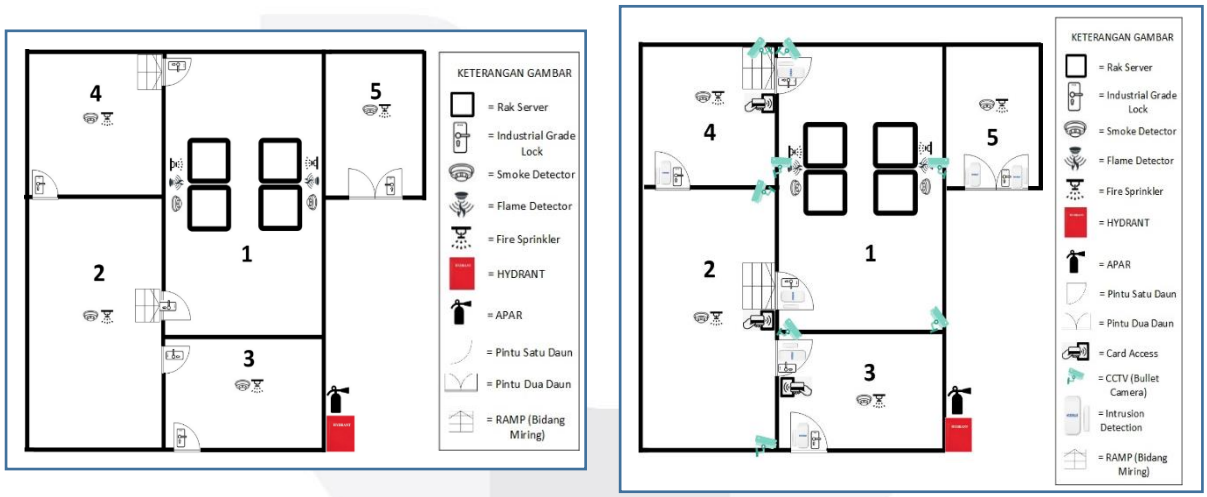
TIA-942		*Tier* 1			*Tier* 2		
No	Parameter	Tinjauan Kebutuhan	Kondisi Saat ini	*Cross/ Check*	Tinjauan Kebutuhan	Kondisi Saat ini	*Cross/ Check*
Architectural (Arsitektural)							
1	Keamanan						
1.1	Terdapat staf untuk keamanan fisik	Tidak ada persyaratan	Masih belum terdapat staf untuk keamanan fisik	✓	Dibutuhkan (Sesuai dengan jam kerja normal)	Masih belum terdapat staf untuk keamanan fisik	X
2	Keamanan Kontrol akses atau Pengawasan pada:						
2.1	Generator	*Industrial grade lock*	Belum menggunakan *industrial grade lock*	X	*Intrusion detection*	Belum menggunakan *Intrusion detection*	X
2.2	UPS	*Industrial grade lock*	Sudah menggunakan *industrial grade lock*	✓	*Intrusion detection*	Belum menggunakan *Intrusion detection*	X
2.3	Kelistrikan dan kabel *fiber optic*	*Industrial Grade lock*	Sudah menggunakan *industrial grade lock*	✓	*Intrusion detection*	Belum menggunakan *Intrusion detection*	X
2.4	Pintu masuk ruang *data center*	*Industrial Grade lock*	Sudah menggunakan *industrial grade lock*	✓	*Intrusion detection*	Belum menggunakan *Intrusion detection*	X

2.5	Pintu masuk ruang *server*	*Industrial Grade lock*	Sudah menggunakan *industrial grade lock*	✓	*Card access*	Masih menggunakan kunci	X
3	Pemantauan CCTV						
3.1	Pintu pintu akses masuk ruang *server*	Tidak dibutuhkan	Belum ada pemantauan CCTV	✓	Dibutuhkan CCTV	Belum ada pemantauan CCTV	X
4							
4.1	Semua CCTV merekam semua aktivitas yang berlangsung	Tidak dibutuhkan	Belum terdapat CCTV	✓	Tidak Dibutuhkan (Boleh diusulkan)	Belum terdapat CCTV	X
MECHANICAL (Mekanikal)							
5	*Fire Supression*						
1.1	Sistem deteksi kebakaran	Dibutuhkan	Belum tersedia sistem deteksi kebakaran	X	Dibutuhkan	Belum tersedia sistem deteksi kebakaran	X

Dapat dilihat pada tabel diatas, bahwa masih terdapat poin-poin yang masih belum memenuhi syarat standar TIA-942 *tier* 1 dan *tier* 2, sehingga perlu dilakukan perancangan untuk pengembangan keamanan fisik agar *data center* dapat terhindar dari risiko/ancaman.

4.4 Usulan Desain Ruangan dan Penempatan Perangkat Keamanan Fisik Tier 1 dan Tier 2

Gambar 3 merupakan desain usulan ruangan dan penempatan perangkat keamanan fisik untuk kebutuhan *tier* 1, dan desain usulan ruangan dan penempatan perangkat keamanan fisik untuk kebutuhan *tier* 2

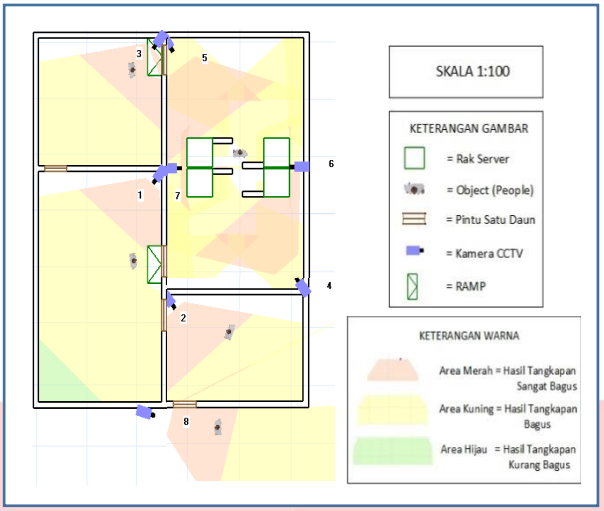


Gambar 3 Desain Usulan dan Penempatan Perangkat Keamanan Fisik

Untuk *tier* 1 (gambar sebelah kiri), diusulkan desain ruangan yang terdiri dari 6 bagian ruangan, dan untuk perangkat keamanan fisik diusulkan penambahan perangkat fisik lama yaitu *industrial grade lock*, *smoke detector*, dan *fire sprinkler*, lalu terdapat juga penambahan perangkat keamanan fisik baru yaitu *flame detector*. Untuk *tier* 2 (gambar sebelah kanan) usulan desain ruangan hanya berubah pada fungsi ruangan *office* yang menjadi ruangan *operations command*, dan untuk perangkat keamanan fisik diusulkan penambahan perangkat keamanan fisik baru yaitu *card access*, CCTV (*bullet camera*), dan *intrusion detection*.

4.5 Usulan CCTV

Perangkat CCTV diperlukan sebagai kamera pengawas yang dapat merekam semua aktivitas yang terjadi di ruang *data center* dan area sekelilingnya selama 24 jam. Berikut merupakan usulan penempatan perangkat kamera CCTV untuk kebutuhan *tier* 2 TIA-942:



Gambar 4 Penempatan CCTV

Dapat dilihat pada Gambar 4, terdapat 8 buah kamera CCTV (*bullet camera*) yang diletakan pada sudut-sudut ruangan. Kamera 1 diletakkan pada sudut ruangan *operations command* dekat pintu akses masuk ruang *server*. Kamera 2 diletakkan pada pada sudut kiri depan ruangan *entrance room* dekat pintu akses masuk operations command. Kamera 3 diletakan pada sudut ruangan *vendor and service area* dekat pintu akses masuk ruang *server*. Untuk kamera 1 dan 3 diletakan dekat pintu akses masuk ruang *server* agar bisa menangkap objek secara jelas, khususnya wajah dari setiap orang yang melalui pintu akses masuk ruang *server*. Kamera 4 diletakkan pada sudut kanan belakang ruang *server*. Kamera 5 diletakan pada sudut kiri depan ruang *server*. Kamera 4 dan 5 berfungsi sebagai pengawasan terhadap *data center* karena diletakan menghadap *data center*. Kamera 6 diletakan pada bagian kanan ruang *server*. Kamera 7 diletakan pada bagian kanan ruang *server*. Kamera 6 dan 7 berfungsi sebagai pengawasan jika kondisi rak *server* sedang keadaan terbuka, sehingga tidak terdapat blankspot pada area ruang *server*. Kamera 8 diletakan pada luar area ruangan *data center* dekat pintu akses masuk ruang *entrance room* sehingga dapat melakukan pemantauan pada area luar ruangan *data center*.

4.6 Usulan Perangkat Kontrol Akses

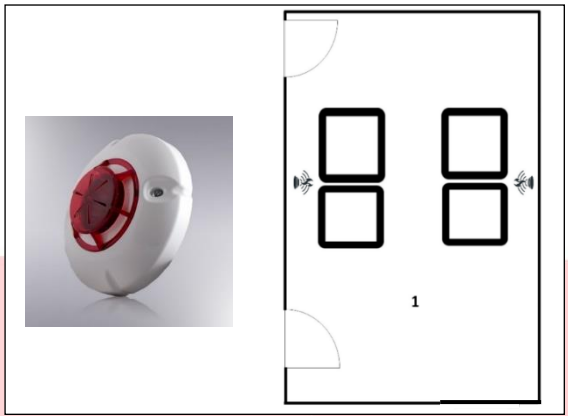
Perangkat kontrol akses diperlukan untuk membatasi pengguna untuk mengakses suatu ruangan dengan menempatkan sistem perangkat kontrol pada pintu, jadi hanya staf pegawai atau orang-orang yang mempunyai izin yang dapat keluar/masuk ke area ruangan *data center* dan ruang *server*. Berikut merupakan usulan perangkat akses kontrol yaitu berupa perangkat intrusion detection dan perangkat card access untuk kebutuhan *tier* 2 TIA-942:

Gambar 5 Perangkat Akses Kontrol dan Visualisasi Penempatan

Dapat dilihat pada gambar 5, terdapat penempatan perangkat *intrusion detection* berada di pintu dan kusen pintu. Untuk penempatan perangkat *card access* berada di tembok/dinding sebelah pintu, Untuk penempatan elektromagnet berada di kunsen pintu, namun untuk penempatan plat *armature* berada di pintu bagian atas. Untuk penempatan *exit button* berada di di tembok/dinding sebelah pintu

4.7 Usulan Perangkat Pendeteksi Api

Perangkat *flame detector* adalah alat pendeteksi kebakaran yang dapat memberikan *system warning* berupa *fire alarm*. Perangkat *flame detector* diperlukan sebagai langkah antisipasi bila sewaktu-waktu terjadi kebakaran dan dapat mengantisipasi kebakaran yang meluas/menyebar ke ruangan/area lainnya. Berikut merupakan usulan penempatan perangkat kamera CCTV untuk kebutuhan *tier* 2 TIA-942:



Gambar 6 Perangkat Flame Detector dan Penempatannya

Dapat dilihat pada gambar 6, perangkat *flame detector* mempunyai bentuk yang hampir mirip dengan *smoke detector* sehingga memudahkan perangkat ini ditempatkan pada atap ruangan *server*. Namun perangkat ini berbeda dengan perangkat *smoke detector*, karena perangkat ini berfungsi untuk mendeteksi api bukan sebagai pendeteksi asap. Dengan mudahnya perangkat ini dipasang pada bagian atap ruang *server*, maka penempatan yang diusulkan adalah pada atap bagian tengah di antara 2 rak *server*.

4.8 Usulan SOP

Standar Operasional Prosedur adalah langkah-langkah dan prosedur jika ada pengunjung yang ingin memasuki ruang *data center*, sehingga dapat mengurangi ancaman pada ruang *data center* untuk dimasuki oleh orang yang tidak memiliki izin. Maka dari itu, diusulkan 3 SOP yang mempunyai tingkatan/level hak aksesnya. Untuk level 1 (tingkatan terendah), terdapat SOP akses masuk ruang generator dan ruang *entrance*. Untuk level 2, terdapat SOP akses masuk ruang *office*/*operations command* dan ruang *vendor and service area*. Untuk level 3 (tingkatan tertinggi), terdapat SOP akses masuk ruang *server*,

5. Kesimpulan

Berdasarkan pada penelitian yang telah dilakukan pada objek *data center* DISKOMINFO Kabupaten Bandung Barat, maka dapat ditarik kesimpulan sebagai berikut:

1. Pada tahap identifikasi analisis kondisi *data center* saat ini dengan kesesuaian standar TIA-942, didapat hasil sebagai berikut:
   a. Untuk *tier* 1, kondisi keamanan fisik *data center* saat ini masih belum sepenuhnya memenuhi kebutuhan, dikarenakan belum adanya perangkat *flame detector* yang berfungsi sebagai alat pendeteksi kebakaran untuk ruang *data center* dan belum adanya perangkat *industrial grade lock* yang berfungsi sebagai kunci pengaman untuk ruangan generator.
   b. Untuk *tier* 2, terdapat poin-poin penambahan yang menjadi syarat untuk dapat memenuhi kebutuhan *tier* 2, yaitu perangkat CCTV untuk melakukan pengawasan pada pintu-pintu akses masuk ruang *server*, perangkat kontrol akses berupa perangkat *card access* pada pintu masuk ruang *server* dan perangkat *intrusion detection* pada pintu-pintu beberapa ruangan yang berfungsi untuk membatasi staf atau orang yang tidak memiliki izin untuk mengakses ruangan tersebut.
2. Rancangan desain usulan keamanan fisik *data center* adalah sebagai berikut:
   a. Rancangan desain usulan *data center tier* 1 :
      i. Terdapat usulan desain penempatan perangkat keamanan fisik berdasarkan kebutuhan *tier* 1 yang memudahkan untuk dilakukan pemasangan perangkat-perangkat keamanan fisik usulan.
      ii. Terdapat usulan penambahan perangkat keamanan fisik lama yang dibutuhkan untuk dapat menyesuaikan dengan usulan desain ruangan *tier* 1.
      iii. Terdapat usulan perangkat perangkat pendeteksi api berupa *flame detector* yang berjumlah 2 buah untuk pemenuhan kebutuhan *tier* 1. Perangkat tersebut digunakan untuk mengantisipasi kebakaran dan mencegah kebakaran yang meluas/menyebar ke ruangan/area lainnya.
   b. Rancangan desain usulan *data center tier* 2 :
      i. Terdapat usulan desain penempatan perangkat keamanan fisik berdasarkan kebutuhan *tier* 2 yang memudahkan untuk dilakukan pemasangan perangkat-perangkat keamanan fisik usulan.
      ii. Terdapat usulan perangkat keamanan fisik berupa kamera CCTV berjenis IP *camera* yang berjumlah 8 buah untuk pemenuhan kebutuhan *tier* 2. Usulan perangkat CCTV disimulasikan sehingga mendapatkan gambaran tangkapan kamera untuk pengawasan terhadap ruang *server*, pintu-pintu akses masuk ruang *server*, pintu masuk ruang *operations command*, dan pintu masuk *entrance room.* Pada usulan perangkat kamera CCTV juga terdapat spesifikasi dan harga yang direkomendasikan.
      iii. Terdapat usulan perangkat kontrol akses berupa perangkat *card access* yang berjumlah 3 buah dan perangkat *intrusion detection* yang berjumlah 7 buah untuk pemenuhan kebutuhan *tier* 2. Perangkat kontrol akses digunakan untuk membatasi pengguna yang tidak berwenang atau tidak

mempunyai izin untuk mengakses suatu ruangan. Perangkat kontrol akses tersebut divisualisasikan menggunakan gambar sehingga dapat melihat gambaran detail dari penempatan perangkat yang diusulkan.

c. Terdapat perbandingan harga usulan perangkat keamanan fisik untuk *tier* 1 dan *tier* 2 sebagai gambaran kebutuhan dana yang diperlukan untuk melakukan pengimplementasian, sehingga pihak DISKOMINFO Kabupaten Bandung Barat dapat melakukan pemilihan opsi *tier* 1 atau *tier* 2.
d. Terdapat standar operasional prosedur akses masuk ke ruang-ruang *data center* untuk kebutuhan rencana jangka panjang (RJP) yang berfungsi sebagai syarat dan prosedur untuk memasuki ruang-ruang *data center* bagi pengunjung.

Daftar Pustaka:

[1] Malik M, L. M., Arini, & Wardhani, L. K. (2017). Analisis Keamanan Informasi *Data Center* Menggunakan COBIT 5 . *Jurnal Teknik Informatika*.

[2] Wahyuddin, M. I., & Jauhari, F. (2008). Keamanan Jaringan Komputer Pada Sistem Pemerintahan Elektronik. *ICT Research Center*.

[3] Janpitak, N., & Sathitwiriyawong , C. (2012). *Data Center Physical Security* Ontology.

[4] Playbook, P*hysical Security Strategy and Process*. (2013).

[5] DISKOMINFOTIK KABUPATEN BANDUNG BARAT. (2018). *Diskominfotik Kab. Bandung Barat*. Diambil kembali dari diskominfotik.bandungbaratkab.go.id: http://diskominfotik.bandungbaratkab.go.id/

[6] Dewanannta. (2017). Pengantar Jaringan Komputer - *Data Center*.

[7] TIA. (2012). *Telecommunications Infrastructure Standard for Data Centers*.

[8] Arregoces, M. A., & Portolani. (2004). *Fundamentals Data Center*.

[9] Priatmoko, D. B., Astuti, E. S., & Riyadi. (2016). Analisis Penerapan Sistem Keamanan Fisik Pada *Data Center* Untuk Melindungi Data Organisasi. *Jurnal Administrasi Bisnis* .

[10] Kingsley, H. J. (2013). *Physical Security Strategy and Process Playbook*. *Oxford: Elsevier*.

[11] TIA. (2005). *Telecommunications Infrastructure Standard for Data Centers*.

[12] Hevner, A. R. (2004). *Design Science in Information System Research*.