ANALISIS DAN PERANCANGAN *SECURITY SYSTEM* DALAM RANCANGAN BERDASARKAN STANDAR EN506002-5 DENGAN METODE PPDIOO *LIFE-CYCLE APPROACH* STUDI KASUS : DISKOMINFO PEMERINTAH KABUPATEN BANDUNG

ANALYSIS AND DESIGN OF SECURITY SYSTEM IN DESIGN BASED ON EN506002-5 STANDARD WITH PPDIOO LIFE-CYCLE APPROACH METHOD CASE STUDY: DISKOMINFO GOVERNMENT OF BANDUNG REGENCY

Muhammad Ghazian[1], M Teguh Kurniawan[2], Umar Yunan Kurnia Septo Hediyanto[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[1]muhammadghazian@student.telkomuniversity.ac.id, [2]teguhkurniawan@telkomuniversity.ac.id, [3]umaryunan@telkomuniversity.ac.id

Abstrak

Pemerintahan Kabupaten Bandung adalah pembagian wilayah administratif yang merepresentatifkan sebuah lembaga pemerintah yang bertanggung jawab dalam segala urusan di bagian Teknologi Informasi dan Komunikasi di Kabupaten Bandung. Pada kondisi saat ini, di Pemerintahan Kabupaten Bandung memiliki data center yang berfungsi sebagai komponen penting dalam memberikan pelayanan teknologi informasi dan menjalankan segala proses bisnisnya, maka demi menjaga fungsi kerja dan penyimpanan data pada data center dibutuhkan keamanan fisik untuk menjaga keutuhannya. Maka dari itu dibutuhkan sebuah perancangan yang dapat menjaga aset institusi sehingga tidak menimbulkan kerugian yang cukup besar dikarenakan sistem keamanan yang lemah. Dibutuhkan perancangan security system physical yang sesuai dengan kebutuhan data center Pemerintahan Kabupaten Bandung. Dalam perancangan security system data center ini menggunakan metode PPDIOO Life-Cycle Approach pada tiga tahapan awal yaitu, Prepare, Plan, Design yang rancang sesuai pada standar EN50600-2-5. Metode PPDIOO Life-Cycle Approach digunakan untuk melakukan perancangan data center bertujuan untuk mencakupi semua kebutuhan layaknya data center dan memaksimalkan kemananan data untuk pengembangan jangka panjang data center Pemerintahan Kabupaten Bandung. Hasil keluaran dari penelitian ini adalah rancangan security system data center Pemerintahan Kabupaten Bandung yang sesuai dengan standar EN50600-2-5 menerapkan pada availability class 1 sebagai parameter. Hasil akhir pada class 1 berupa rekomendasi keamanan fisik memasuki area data center dikategorikan menjadi tiga yaitu akses untuk pegawai, akses untuk tamu, dan akses untuk pengantar. Dalam menjaga batas area tersebut diusulan penggunakan perangkat RFID Anti-passback door mencegah personal yang tidak memiliki wewenang memasuki ruangan. Untuk menjaga keutuhan perangkat yang ada pada data center diusulkan fire detection and suppresion system apabila terjadi kebakaran.

Kata kunci : Data Center, Security System, PPDIOO Life-Cycle Approach, EN50600-2-5.

Abstract

Bandung Regency Government is the division of administrative territory that represents a government agency responsible in all affairs in the Information and Communication Technology in Bandung Regency. In the current condition, in Bandung Regency Government has data center that serves as an important component in providing information technology services and run all business processes, so in order to maintain the work function and data storage in the data center needed physical security to maintain its integrity. Therefore required a design that can maintain the institutional assets so as not to cause significant losses due to weak security system. Required physical security system design in accordance with data center needs Bandung Regency Government. In designing this data center security system using PPDIOO Life-Cycle Approach method in the first three stages, Prepare, Plan, Design designed according to EN50600-2-5 standard. The PPDIOO Life-Cycle Approach method is used to design the data center aims to cover all needs like data center and maximize data security for long-term data center development Bandung Regency Government. The output of this study is the design of data system security center Bandung Regency Government in accordance with the standard EN50600-2-5 apply on the availability of class 1 as a parameter. The end result in class 1 in the form of physical security recommendations entering the data center area is categorized into three namely access for employees, access to guests, and access to the introduction. In maintaining the boundary of the area is proposed the use of RFID devices Anti-passback door to prevent personal who have no authority to enter the room. To maintain the integrity of existing devices in the data center is proposed fire detection and suppresion system in case of fire.

Keywords: Data Center, Security System, PPDIOO Life-Cycle Approach, EN50600-2-5.

1. Pendahuluan

Teknologi informasi (TI) berkembang sangat pesat dan telah merevolusi cara hidup kita, baik terhadap cara berkomunikasi maupun informasi [1]. Teknologi Informasi adalah sarana/prasarana, sistem dan metode untuk perolehan, pengiriman, penerimaan, pengolahan, penafsiran, penyimpanan, pengorganisasian, dan penggunaan data yang bermakna. TI juga dapat dikatakan suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan dan memanipulasi data.

Peran sebuah data sangat penting bagi sebuah organisasi. Karena data miliki suatu informasi yang sangat berguna bagi perkembangan sebuah organisasi tersebut. Semakin banyak informasi yang dibutuhkan, semakin banyak pula data yang harus diolah [2]. Oleh karena dibutuhkan suatu tempat yang bisa mengelola data dan meyimpan data-data dengan aman dari berbagai gangguan yaitu *data center*.

Data center merupakan tempat yang berisikan *server* serta perangkat komputer lainnya untuk melakukan pengelolaan data dan penyimpanan data. Pada dasarnya, proses bisnis sebuah perusahaan sangat berpengaruh terhadap tujuan perusahaan. Oleh karena itu *data center* menjadi salah satu komponen proses bisnis yang penting. *Data center* diharapkan mampu memberi keseimbangan pada proses bisnis perusahaan sehingga dapat memberikan keuntungan. Maka penting bagi sebuah perusahaan atau organisasi memiliki data center terutama perusahaan atau organisasi yang berbasis teknologi informasi dan sudah menerapkan internet, karena penting pengelolaan data-data yang dimiliki perusahaan [3]. Dalam pembangunan *data center*, keamanan merupakan aspek yang penting. Keamanan dalam *data center* sangat penting karena *data center* menyimpan data berupa aset yang berharga bagi perusahaan atau institusi. Maka dari itu keamanan pada *data center* harus diterapkan dengan ketat sehingga tidak terjadi kehilangan atau kerugian aset.

Pemerintah Kabupaten Bandung merupakan suatu instansi pemerintah yang memiliki kewajiban dalam mengurus segala keperluan masyarakat yang berada di wilayah Kabupaten Bandung. Dinas Komunikasi, Informatika, dan Statistik (DISKOMINFO) Kabupaten Bandung merupakan salah satu dinas yang ada di Pemerintah Kabupaten Bandung. Dinas Komunikasi, Informatika, dan Statistik memiliki tugas pokok, yaitu melaksanakan penyusunan dan pelaksanaan kebijakan daerah yang bersifat spesifik di bidang pengelolaan Informasi Publik, Komunikasi Publik, Teknologi Informasi dan Komunikasi, *Layanan e-Government*, Statistik dan Persandian [4]. Dinas Komunikasi, Informatika, dan Statistik merupakan dinas yang menangani dalam Sistem Informasi Manajemen (SIM) yang digunakan oleh Pemerintah Kabupaten Bandung. Sistem Informasi yang digunakan antara lain adalah SIM Daerah Keuangan, SIM Kepegawaian, dan SIM lainnya. Dengan begitu banyak Sistem Informasi Manajemen yang dimiliki Pemerintah Kabupaten Bandung tentunya harus memiliki *data center* yang dapat menjaga keamanan data dalam transaksi dan fungsi manajemennya.

Saat ini Pemerintahan Kabupaten Bandung memiliki *data center* yang dikelola oleh divisi DISKOMINFO. Akan tetapi masih kurang diterapkannya keamanan pada *data center* pemerintahan Kabupaten Bandung. Maka dari itu dibutuhkan sebuah standarisasi yang mencakupi kebutuhan dalam keamanan pada *data center*. Pada penelitian ini standar yang digunakan adalah EN50600. EN50600 Merupakan suatu standarisasi infrastruktur pada *data center*. Pada standar EN 50600 telah menetapkan semua ketentuan yang harus dipenuhi disetiap *availability class level* pada *data center* [5].

2. Dasar Teori dan Metodologi

2.1 Data Center

Data center dikenal sebagai kumpulan *server* atau ruang komputer, dimana *data center* merupakan ruangan sebagian besar *server* dan penyimpanan data perusahaan terletak, beroperasi, dan diatur [6].

2.2 Kriteria Sistem Kemanan *Data Center*

Dalam melakukan rancangan terhadap sebuah *data center* harus memenuhui beberapa kriteria, berikut kriteria-kriteria yang harus dimiliki sebuah *data center* [7]:

- *Confidentality* (kerahasiaan)
  Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang, dan menjamin kerahasiaan data yang dikirim, diterima serta disimpan.
- *Integrity* (integritas)
  Aspek yang menjamin bahwa data tidak di ubah tanpa ada ijin pihak yang berwenang
- *Authorized*
  Menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
- *Availability* (ketersediaan)
  Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperluka

2.3 *European Standard for Data Center* (EN50600)

2.3.1 Definisi *European Standard* (EN 50600)

Rangkaian standar EN 50600 merupakan standar Eropa yang dirancang untuk menjadi standar bagi pembuatan bangunan dan seluruh infrastruktur dari sebuah *data center*. Berbeda dengan standar lain yang pada umumnya berorientasi pada konsep ketahanan rancangan *data center*, rangkaian standar EN50600 dalam perancangannya menggunakan pendekatan rancangan yang berorientasi pada bisnis dengan menggunakan perspektif antara biaya dan rancangan. Karena pendekatannya yang berorientasi pada bisnis model, rangkaian standar EN 50600 tidak memiliki fokus perancangan layanan apa saja yang disediakan oleh *data center*, namun fokus kepada *availability* dari *data center* tersebut. Rancangan mengenai distribusi daya, pengendalian kondisi lingkungan, dan pengkabelan infrastruktur telekomunikasi, semuanya diklasifikasikan dalam sebuah model yang disebut *"Availability Class"* [5].

Pada rangkaian standar EN 50600, risiko paling tinggi yang dihadapi dari *availability* sebuah *data center* ialah masalah kegagalan pencatu daya dan kegagalan teknis ataupun administratif dari koneksi data yang disediakan oleh infrastruktur telekomunikasi. Hal-hal tersebut termasuk berisiko tinggi karena sedikit saja kegagalan dapat menyebabkan kekacauan pemrosesan data yang terjadi di data center terelepas dari ukuran data center tersebut. Sebagai perbandingan, kegagalan sistem kendali lingkungan berada pada tingkat "kronis", contohnya sedikit gangguan pada sistem pendinginan tidak akan menyebabkan hilangnya *availability* pada *data center*.

2.3.2 *Availability Class* pada EN50600

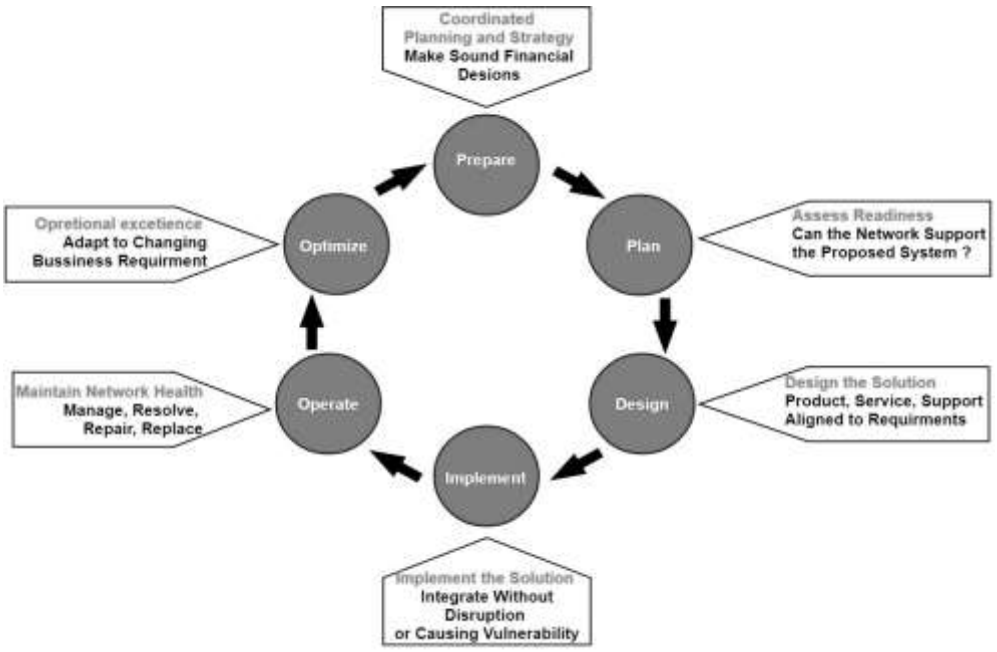
Berdasarkan standar EN50600-2-5 mengenai *Security System* setiap *data center* memiliki ruang bagian yang harus diperhatian dalam menjaga keamanannya [8]. Dalam menerapkan keamanan pada *data center* dibagi menjadi empat *class* masing – masing perancangan desain dalam keamanan *data center*. Berikut ini adalah bagian spesifikasi *class* yang ada pada standar EN50600-2-5 mengenai *Security System*:

Tabel 1 *Protection Class* Pada EN50600-2-5

Protection Class 1	*Protection Class 2*	*Protection Class 3*	*Protection Class 4*
Akses Pintu masuk personel ke bangunan atau struktur yang berisi ruang pusat data	Bangunan atau struktur yang mengandung akses ruang *data center* internal ke *docking bay* Ruang keamanan tempat eksternal Pintu masuk personel ke ruang pusat data Ruang penyimpanan Ruang pengujian Ruang kantor pusat data	Premises pintu masuk fasisitas Membangun fasilitas masuk Ruang komputer Ruang Kontrol Ruang keamanan pusat data	Lemari, kandang atau deretan lemari di ruang ruang komputer
a. berlaku untuk tempat fasilitas masuk yang berada dalam kendali pusat data. b. Pembatas akses yang berlaku untuk jalur pada area class yang lebih rendah.			

2.4 Metodologi Penelitian PPDIOO

PPDIOO merupakan metode analisis sampai pengembangan instalasi jaringan komputer yang dikembangkan oleh Cisco pada materi Designing for Cisco Internetwork Solution (DESGN) yang mendefinisikan secara terus menerus siklus hidup layanan yang dibutuhkan untuk pengembangan jaringan komputer atau teknologi terkait. Berikut tahapan analisis pada metode PPDIOO [9].



Gambar 1 Cisco PPDIOO

1. Tahap *Prepare*

Pada tahap ini dilakukan penetapan kebutuhan bisnis dan visi yang sesuai dengan perencanaan strategi dan mengidentifikasi teknologi yang digunakan untuk mendukung rencana pertumbuhan, serta mengusulkan arsitektur dengan desain tingkat tinggi melalui sebuah pengujian. Pada tahap *prepare* ini disusun rencana anggaran yang dibutuhkan dengan menyesuaikan kebutuhan dan kemampuan bisnis terhadap rancangan arsitektur yang diusulkan.

2. Tahap *Plan*

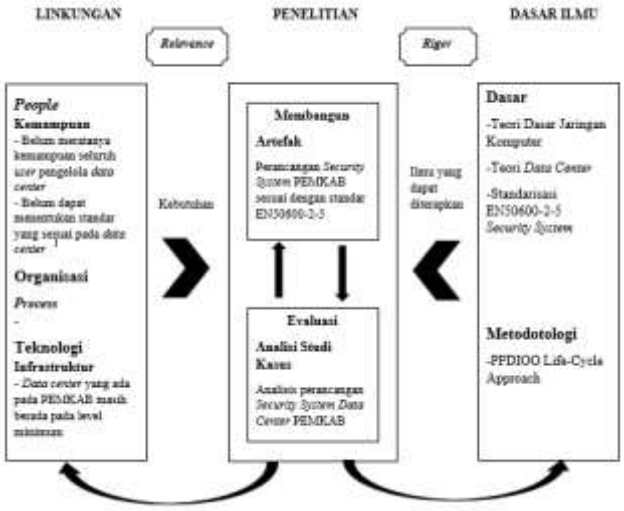
Pada tahap ini dilakukan penentuan apakah kondisi saat ini mampu mendukung sistem yang diusulkan dengan melakukan analisis gap, memastikan *resources* dari perusahaan tersedia untuk mengelola teknologi dari desain hingga implementasi. Tahapan ini meneruskan dari tahap *prepare* sebelumnya, dengan perencanaan yang baik maka akan membantu untuk mengatur pekerjaan, resiko yang mungkin muncul, permasalahan yang ditemui, dan menentukan sumber daya yang dibutuhkan.

3. Tahap *Design*

Pada tahap ini membahas tentang detail logis dari perancangan infrastruktur yang sesuai dengan mekanisme sistem, merancang mekanisme sistem yang akan berjalan sesuai dengan kebutuhan dan analisis. Dimana kebutuhan awal pada tahap perencanaan, antaralain : mengarahkan kegiatan spesialis desain jaringan dan infrastruktur. Sebuah desain yang dihasilkan harus selaras dengan tujuan bisnis dan persyaratan teknis yang dapat meningkatkan kinerja jaringan,

2.5 Model Konseptual

Model konseptual berfungsi untuk membantu peneliti dalam merumuskan pemecahan masalah dan membantu dalam perumusan solusi untuk permasalahan yang ada. Model ini juga berfungsi untuk membantu dalam penataan masalah, mengidentifikasi faktor-faktor yang relevan, serta memberikan penjelasan agar masalah yang ada dapat dipahami dengan mudah. Model konseptual ini menggambarkan kerangka penelitian tugas akhir Analisis dan Perancangan *Security System Data Center* Berdasarkan *Availability Class* 1 di Pemerintahan Kabupaten Bandung Menggunakan Standar EN50600-2-5 Dengan Metode PPDIOO *Life-Cycle Approach* yang betujuan untuk membuat rancangan *Security System Data Center* yang sesuai dengan standar dan *availability class*.

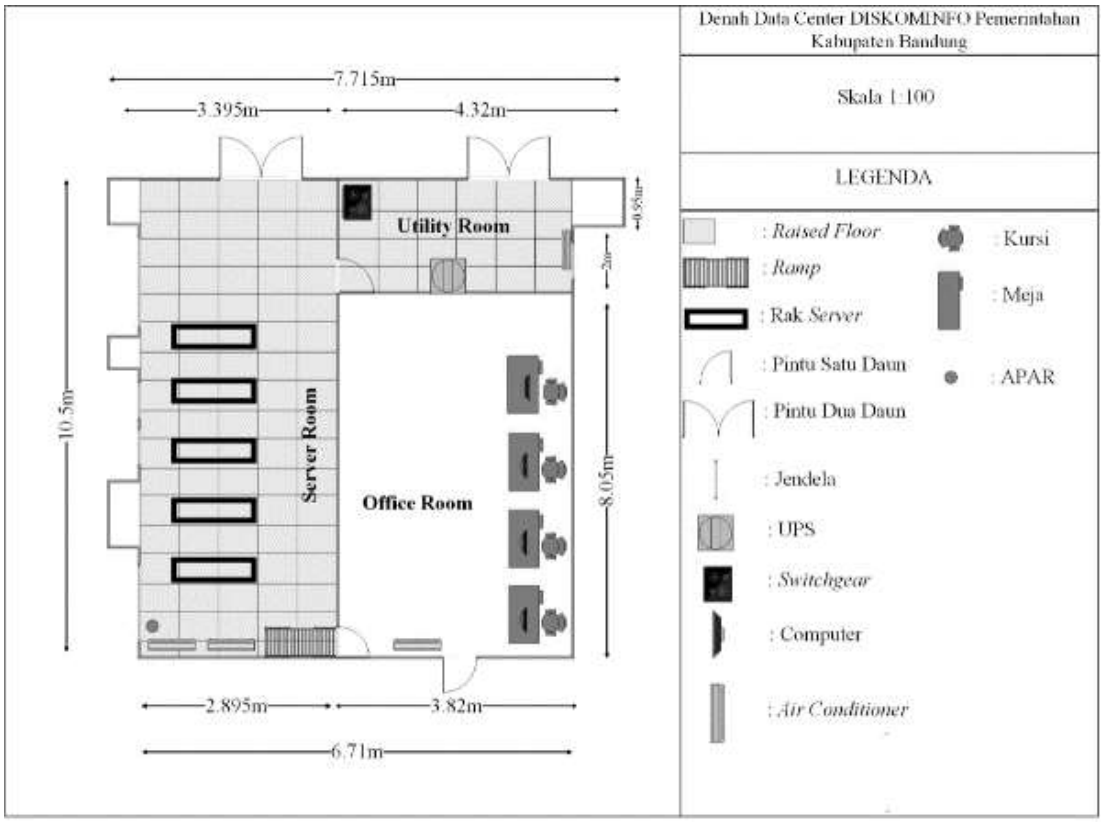


Gambar 2 Model Konseptual

Pada Gambar 2 menjelaskan bahwa permasalahan yang ada pada Pemerintah Kabupaten Bandung berada pada bagian lingkungan, dimana permasalahan yang ada dibagi menjadi tiga komponen, yaitu *People*, Organisasi, dan Teknologi. Berdasarkan hasil observasi langsung pada Dinas Komunikasi, Informatika, dan Statistik didapatkan sebuah data bahwa, permasalahan pada people terletak pada belum meratanya kemampuan *user* mengenai *data center*. Untuk membuat sebuah desain *security system data center* yang sesuai dengan standar yang ada, maka pada bagian dasar ilmu terdapat dasar dan metodologi yang dapat membantu dalam melakukan desain. Dasar yang digunakan antara lain teori jaringan komputer, teori *data center*, dan standar EN50600-2-5. Sedangkan pada bagian metodologi menggunakan metodologi PPDIOO *Life Cycle Approach.*

3. Pembahasan

3.1 Kondisi *Data Center* Saat Ini



Gambar 3 *Denah* Data Center Kondisi Saat Ini

Pada gambar 3 merupakan detail dari ruang data center DISKOMINFO Pemerintahan Kabupaten Bandung.

Berdasarkan hasil observasi DISKOMINFO memiliki 5 buah rak *server*, 1 buah UPS, dan 1 buah distribution panel. Pada ruang data center DISKOMINFO terdapat 1 APAR diletakan di ujung ruangan dekat pintu masuk. Di dalam ruang *data center* banyak sekali barang-barang yang tidak ada kaitannya dengan ruang *data center* diujung ruangan.

3.2 Denah Usulan Ruangan *Data Center*

Gambar 4 Denah Usulan Ruangan *Data Center*

Terdapat dua ruang tambahan yaitu *storage room* dan personal *entrence*. *Storage room* terletak di dalam ruang *server* dengan usulan ukuran 2 x 3 m dekat pintu keluar sebagai jalur evakuasi apabila terjadi bencana. Usulan penempatan ruangan ini bertujuan untuk memaksimalkan fungsi kapasitas pada ruang *server* yang belum terpakai dan dapat menyimpan barang-barang yang tidak dipakai. *Personal entrence* terletak dilaman *command room* dengan usuan ukuran 1,9 x 2.3m dekat dengan pintu masuk *command room* bertujuan untuk membatasi tamu memasuki ruang operasional tanpa wewenang.

3.3 Usulan Protection Class 1 Againts Unauthorized Access

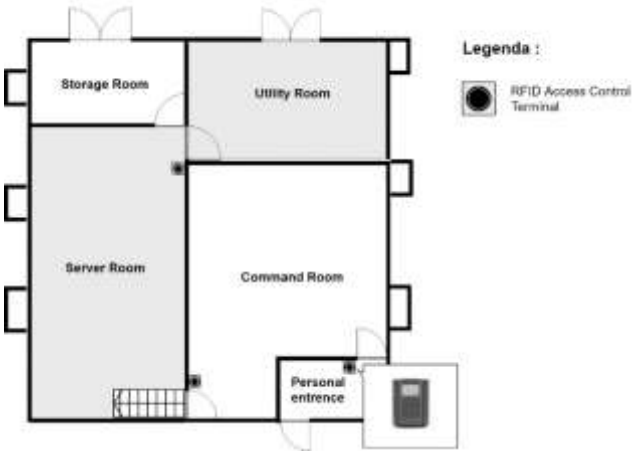
3.3.1 *Protection Class Accessible to* Persons

Berdasarkan hasil analisis gap kondisi saat ini menyesuaikan kebutuhan data center DISKOMINFO dengan standar EN50600-2-5 sebagai parameter sistem kemanan fisik. DISKOMINFO Pemerintahan Kabupaten Bandung memiliki alur prosedur pengunjung dan karyawan untuk memasuki ruangan pada *data center* namun tidak memiliki prosedur akses memasuki *data center* dengan membedakan jalur karyawan, pengunjung, dan pengantar. Selain itu *data center* DISKOMINFO tidak memliki batas area diluar bangunan dikhususkan untuk pejalan kaki, tempat parkir, dan pembatas bangunan DISKOMINFO dengan area luar sehingga dapat memprioritaskan pengguna berdasarkan kepentingannya dan tidak terjadi pengguna akses yang tidak diinzinkan memasuki area bangunan *data center*.

3.3.2 *Access Control Security Entrence*

Berdasarkan hasil analisis gap kondisi saat ini menyesuaikan kebutuhan data center DISKOMINFO dengan standar EN50600-2-5 sebagai parameter sistem kemanan fisik. Akses masuk ruang *data center* dibutuhkan sebuah kontrol akses sehingga dapat mengidentifikasi siapa saja yang masuk dan dan mencegah personal memasuki ruangan tanpa izin.

Pada usulan ini setiap pintu yang mengarah ke ruang *data center* dibutuhkan mekanisme akses personal penggunaan kontrol yaitu, *Anti-passback door* sehingga mencegah orang memasuki ruang data center tanpa wewenang, usulan perangkat kontrol akses dapat dilihat pada gambar V.5.

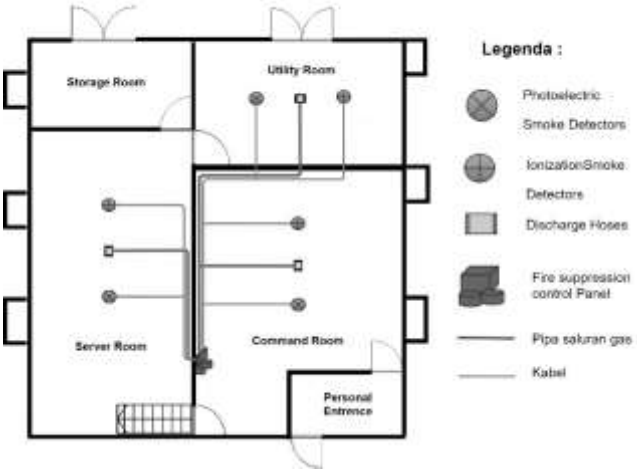


Gambar 5 Uusulan Rancangan RFID Anti-Passback

3.4 Usulan Protection Class 1 Against Fire Events

Berdasarkan hasil analisis gap kondisi saat ini menyesuaikan kebutuhan data center DISKOMINFO dengan standar EN50600-2-5 sebagai parameter sistem keamanan fisik, belum adanya perangkat untuk mendeteksi dan menangani ketika bencana kebakaran terjadi, maka perlu adanya *fire detection and suppression system* sebagai perangkat yang memberikan sinyal terindikasi dan penanganan terjadi kebakaran. Karena *data center* adalah aset yang sangat penting bagi institusi dan harus dijaga sebaik mungkin.

Untuk pencegahan dan penanganan terjadi kebakaran diperlukan perancangan *fire detection and suppression system* yang dibagi menjadi tiga bagian perangkat, yaitu perangkat *input, proccess*, dan *output*. Pada perangkat *input* mengidentifikasi sedang terjadi kebakaran. Perangkat *proccess* berfungsi sebagai menerima sinyal dari *detector* pada area yang terindikasi kebakaran. Dan memberikan *output* berupa sinyal terjadi kebakaran. Perangkat yang dibutuhkan untuk melakukan perancangan *fire detection system*.



Gambar 6 Usulan Perancangan Fire Suppression System

Pada perancangan FM200 system memiliki empat integrasi sistem dalam penanganan kebakaran. Pada usulan ini menggunakan integrasi *Multiple Room System* bertujuan untuk memproteksi dua ruangan atau lebih bila terjadi kebarakan. Berdasarkan hasil observasi ada beberapa ruangan yang memiliki resiko terjadi kebakaran yaitu *command room*, *server room*, dan *utility room*. FM200 berfungsi sebagai pemadam otomatis dengan melepaskan gas dengan bahan kimia HFC-227ea berebeda dengan sistem pemadam kebaran lain dengan menggunakan media air sehingga dapat meminimalisir kerusakan pada perangkat ketika pemadaman terjadi dan tidak berbahaya bagi manusia [10].

4. Kesimpulan

Setelah melakukan penelitian ini dapat disimpulkan bahwa :

1. Berdasarkan analisis kondisi saat ini pada data center DISKOMINFO Pemerintahan Kabupaten Bandung disimpulkan bahwa:

   A. Pengembangan keamanan fisik pada *data center* belum memenuhi dari standar EN50600-2-5. Pada ruang *data center* Pemerintahan Kabupaten Bandung masih banyak keamanan fisik yang belum diterapkan terutama akses untuk memasuki ruang *data center*. Prosedur yang dimiliki oleh DISKOMINFO perizinan

pegawai dan tamu untuk memasuki ruang *server* atau ruang *utility* namun hal ini belum mencukupi dalam otorisasi akses pada ruangan, diperlukan pembagian pengguna akses pada pegawai, tamu, dan pengantar untuk memasuki area *data center*. Selain itu belum disediakan tempat parkir khusus untuk ketiga kategori sehingga dapat mengidentifikasi kepentingan yang dilakukan pada *data center* DISKOMINFO. Dengan letak bangunan data center ditengah komplek Pemerintahaan Kabupaten Bandung terbuka belum memiliki pembatas fisik yang mengelilingi bangunan *data center*.

B. Menjaga keamanan fisik data center terhadap bencana kebakaran belum sesuai dengan standar EN50600-2-5. Pada ruang *data center* Pemerintahan Kabupaten Bandung sudah memiliki penanganan kebakaran dengan menyediakan dua buah APAR yang pertama diletakan didepan pintu masuk ruang *command room* dan satu lagi diletakan didalam ruang *server* dekat pintu masuk namun belum memiliki *fire detection system* dan *fire suppression system* untuk meengidentifikasi dan mencegah ketika terjadi kebakaran pada ruang *data center*.

C. Penanganan pada gangguan kerja perangkat belum diterapkan oleh DISKOMINFO sepenuhnya. Belum adanya penanganan gangguan perangkat terhadap elektromagnetik, getaran, banjir, bahaya gas, dan debu yang timbul pada dalam maupun dari luar data *center.*

2. Usulan Desain keamanan fisik pada data center DISKOMINFO Pemerintahan Kabupaten Bandung sesuai dengan standar EN50600-2-5 *availability class* 1 adalah sebagai berikut:

A. Membuat prosedur dalam hak akses yang dibagi menjadi beberapa kategori yaitu pegawai, tamu, dan pengantar dalam memasuki bangunan *data center*.

B. Merancang usulan dalam menjaga kemanan fisik *data center* apabila terjadi kebaran pada ruang *data center*. Memberikan penanganan dalam mendeteksi dan pencegahan sebelum terjadi kebakaran didalam ruang *data center.*

C. Memberikan rancangan usulan apabila kebakaran terjadi dengan *fire suppression system* pada *data center* DISKOMINFO Pemerintahan Kabupaten Bandung.

Daftar Pustaka:

[1] A. Ratnasari, Perkembangan Teknologi Komunikasi dan Kesenjangan Informasi, 2004.

[2] M. I. Padli, Urgensi Keamanan dalam Sistem Informasi, 2008.

[3] M. Arregoces and M. Portolani, Data Center Fundamentals, 2003.

[4] Pemerintah Kabupaten Bandung, "Profile Pemerinta Kabupaten Bandung," 2017. [Online].

[5] R. Cardigan, European Data Centre Infrastructure Standards, 2014.

[6] M. Bullock and C., Data Center Definitions and Solutions, 2009.

[7] D. E. Yulianti and H. B. Nanda, Best Practice Perancangan Fasilitas Data Center, 2008.

[8] Dansk, Informations teknologi – Faciliteter og infrastrukturer i datacentre – Del 2-5 : Sikkerhedssystemer, 2018.

[9] Cisco, Designing Cisco Network Service Architecture, 2007.

[10] FM200, "Fire Suppression System," 2016 [Online].