Data Center Infrastructure (DCI) - Assignment

Research · May 2018

DOI: 10.13140/RG.2.2.32032.43522

2 authors, including:

Abdurraouf Fathi Sawehli
Asia Pacific University of Technology & Innovation
21 PUBLICATIONS **3** CITATIONS

SEE PROFILE

Module Code	**:**	CT109-3-2-DCI
Intake Code	**:**	UC2F1708IT(NC)
Lecturer Name	**:**	DR YASEEIN SOUBHI HUSSEIN
Hand in Date	**:**	25 MAY 2018

Student ID	**Student Name**
TP043185	Benedict Loh
TP042816	Abdurraouf Fathi Ali
TP047430	Beh Wei Xiang

Contents

1. Introduction to Data Center

Tamanix data centers is a company that provides installation and technical support services for companies' applications and networks. Those companies are various from small-medium enterprises to multinational companies that require reliable, high touch and network neutral data center. We are employed by them to implement a new data center that offers state-of-the-art security and compliance features for one of their clients which is Panadox. Panadox is a healthcare company located in Malaysia serving over 10 million patients nation-wide and provide a Customer Relationship Management (CRM) platform which requires a tremendous amount of data to be stored to maintain the highest level of service to customers and their patients.

Besides that, appropriate planning of the data center infrastructure design is vital where several aspects need to be cautiously well-thought-out such as performance, resiliency, scalability and flexibility in fast deploying and supporting new services. Such a design requires solid planning and consideration as well as justification to achieve the predefined requirements.

1.1 Data center definition

The IT field and the whole world are moving at an exponential pace and with this growth, the changing of the IT business is necessary to adopt them in a way that the brain of an enterprise and most critical processes are running in one place.

A data center consists of hardware such as server racks and power distribution units, software such as server operating systems and network monitoring tools.

The responsibilities of a data center are to provide computational power, network of computers, storage devices, cooling system and applications that are essential to aid an enterprise business. Data center plays a pivotal role in most big companies since their business depends on the services that they provide.

2. Data Center Requirements

This section will explain the basic requirements of a data center. To understand the components of a data center, the level of service expected from the data center must be determined. In the scenario, the proposed data center will house a customer relations management (CRM) system with an electronic health record (EHR). The requirements of the data center are as follows.

2.1 Security:

The EHR will be stored in a data warehouse collocated with the CRM. The type of data that is expected to be processed by the data center is patient health records. Therefore, it is important that the proposed data center has the highest level of data security. Data security must include cybersecurity measures and physical security to safeguard against both internal and external threats. Benefits of a high security data center will guarantee data integrity and maintain the turst between Panadox customers.

2.2 Scalability:

Panadox is an organization that may expand their operations in the future. Thus, the proposed data center must be able to support ongoing scalability as well as provide colocation services. It is the most significant requirement of building up data center as the ability of growth and handling the increase in number of data or users is needed and that might affect the data center design in long term operation if scalability is not taken into consideration. Any changes in the data center that require additional space, devices or other technical aspects in the future has to be managed in an efficient way that does not affect main existing elements of the data center.

2.3 Manageability:

There must be ease of access for maintenance, while meeting stringent physical security needs. Location security is an important aspect of data center design that must be taken into consideration when choosing the location of the data center. Additionally, manageability also includes data manageability. For instance, data stored in the data center should be able to be analyzed by Panadox management in an effective and efficient manner.

2.4 Cost:

The cost of running a data center is an important factor to consider. The costs involved in running the data center are the Total Cost of Ownership (TCO) which include the Operational Expenditure (OPEX) and Capital Expenditure (CAPEX). Ideally, Panadox data center will keep the TCO low to ensure that the datacenter is not too expensive to operate.

2.5 Availability:

This is so that Panadox can have confidence in the services provided by the data center, to be able to provide its service to their customers. The availability target of Panadox is a 99.995% availability.

The data center will be evaluated according the data center tier hierarchy. The data center tier hierarchy is a guideline to assign each data center a tier rating based on uptime standards. The data center tier hierarchy requirements are shown in the table below.

Tier requirements	TIER I	TIER II	TIER III	TIER IV
Distribution paths power and cooling	1	1	1 active / 1 alternate	2 active
Redundancy active components	N	N+1	N+1	2 (N+1)
Redundancy backbone	no	no	yes	yes
Redundancy horizontal cabling	no	no	no	optional
Raised floors	12"	18"	30"-36"	30"-36"
UPS / generator	optional	yes	yes	dual
Concurrently maintainable	no	no	yes	yes
Fault tolerant	no	no	no	yes
Availability	**99.671%**	**99.749%**	**99.982%**	**99.995%**

Figure 1 shows the availability description(Bendict,2018)

3. Data center design overview

This section will explain the considerations and justifications when implementing a data center. The factors that are taken into considerations when designing a data center are:

3.1 Location:

A report from the National Centers for Environmental Information states that weather and climate disasters in 2014 amounted to losses exceeding $1 billion across the United States. (National centers for environmental information, 2015)

Therefore, the data center must be in a place that is sheltered from weather and natural disasters. Weather patterns in the area should be analyzed to determine factors such as flooding tendencies, rainfall and seismic activity.

The figures below show examples of data that must be collected when choosing a data center location. FIGURE1 shows rainfall at a given time. FIGURE2 shows earthquake activity in the region. Analysis of this data shows that earthquake prone areas such as Sabah should be avoided. Additionally, areas of heavy rainfall such as the Klang Valley should also be avoided.

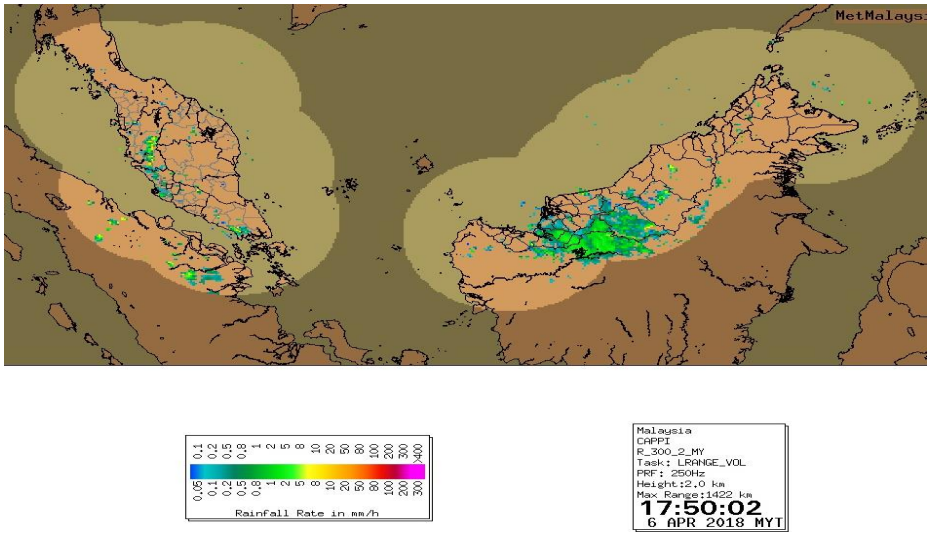

Figure shows the location (Bendict, 2018)

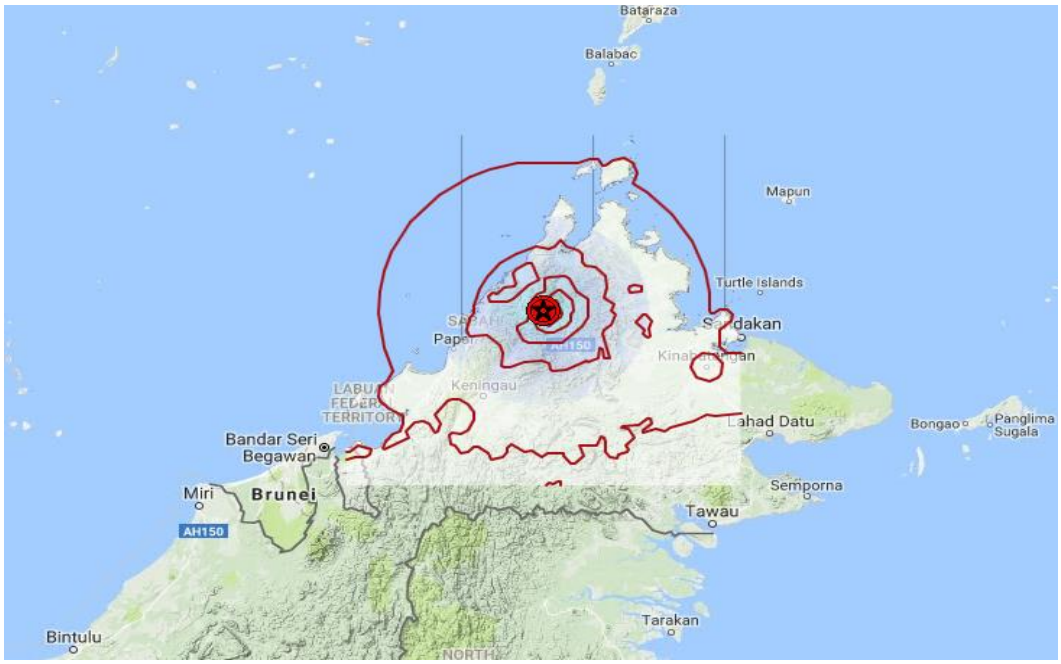

Figure shows the location (Bendict, 2018)

3.2 Network Services:

Network services should be considered. The optimal location of a data center should be in a location that has access to high speed networking that services the geographical location and has links to other locations. This is done to reduce latency when accessing the data center, which is beneficial to availability and accessibility.

The figure below shows the internet backbone of Malaysia. This internet backbone is the foundation that many Internet Service Providers use to provide internet access. Analysis of this map shows that optimally, the data center should be located in one of the nodes shown in the figure. Doing so will provide accessibility to the data center from all locations in Malaysia.

Figure shows the location (Bendict, 2018)

3.3 Security:

Security is an important aspect when choosing a location for a data center. Physical security can include active deterrents such as guards and passive deterrents such as CCTV monitoring. A Defense-in-Depth model should be taken to safeguard the compound against threats.

3.4 Additional Considerations:

3.4.1 Raised floor and dropped ceiling:

A raised floor and dropped ceiling is Many reasons influence the decision to adopt a raised floor and dropped ceiling.

Firstly, the raised floor and dropped ceiling effectively reduces the size of the room the data center is housed in. This is done because a smaller room is easier to cool than a large room. By adopting a raised floor and dropped ceiling approach, the area of the room that needs to be cooled becomes smaller.

Second, many current data center cooling techniques involve venting either cold or hot air through the raised floor or dropped ceiling. By implementing a raised floor and dropped ceiling approach, the options to implement cold or hot aisle cooling techniques are viable in the data center.

Third, adding raised floor and dropped ceilings enable many cable management options. With raised floors, it is possible to run cables under the floor. With dropped ceilings, it is possible to run overhead cabling.

Lastly, to comply with the tier 4 data center standards, the raised floor must be at least 30-36 inches high. Compliance to standards are important to provide confidence in the service provided by the data center and to attract other organizations to use the data center as a colocation solution.

3.4.2 Insulated Walls:

Because of the difference of temperature between inside and outside of the datacenter, condensation may occur, leading to increased humidity that can damage sensitive equipment. Thus, it is important to insulate the walls to form a vapor barrier between the inside and outside of the data center.

The figure below shows the design of a vapor barrier that can control the condensation that occurs during datacenter operation.

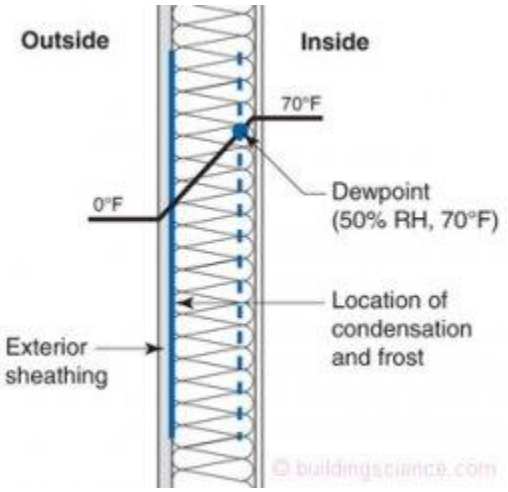

Figure shows the Insulated Walls (Bendict, 2018)

4. Hardware overview

4.1 Rack Standard

Standardization is the main factor that must be taken into consideration when choosing the best type of server rack to implement in the data center. This is to enable a predictability in the size and weight of each rack and to enable ease of maintenance after implementation.

The EIA (Electronic Industries Alliance) standard server rack is a 19-inch-wide rack enclosure with rack mount rails which are 17 3/4″ (450.85 mm) apart and whose height is measured in 1.75″ (44.45 mm) unit increments. A 42U rack would have an internal rack unit height dimension of 73.5 inches (1.8669 m). The figure below shows the specifications for a EIA compliant rack.

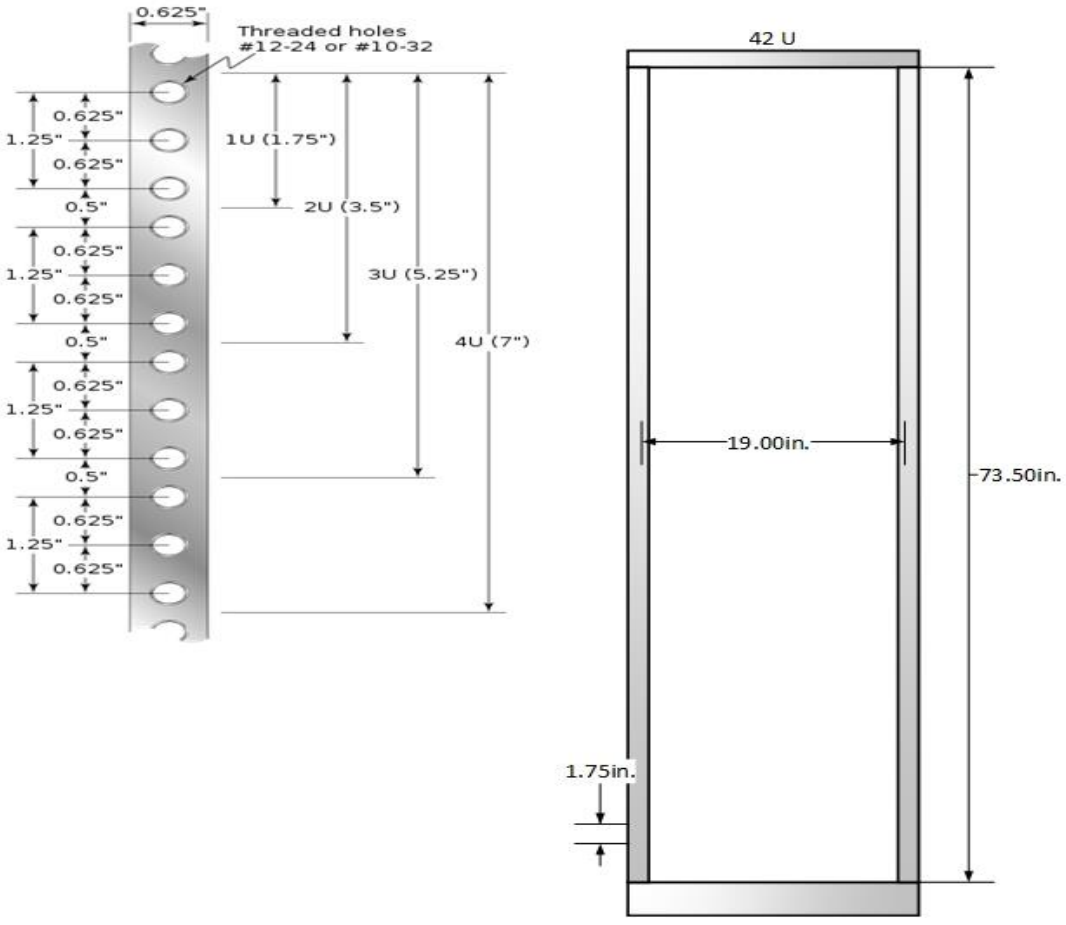

Figure shows the rack(Beh,2018)

4.2 Rack Comparisons

Four types of racks have been found to be compliant with the above-mentioned standards were researched to determine which is the best type of rack to implement in the data center. Rack data was obtained from the Rackmount Solutions website (Rackmountsolutions.net, 2018).

Rack Name	4 Post Rack	Colo Cabinets	AcoustiQuiet Soundproof Rack	Server Enclosure
Image				
Rack Units (U)	44	42 (2 x 21U)	42	42
Internal Width (in.)	19.00 (EIA Compliant)			
Material	Steel	Steel	Extruded Aluminum	Extruded Aluminum
Door Style	None (Open Frame)	Vented	Solid	Perforated
Price	$396.78	$2,699.99	$5,211.02	$1,962.32
Model Number	DC4R4429F	CLC2B42BK	AQ732042-2	RSP732030

Comparison table(Beh,2018)

4.3 Rack Recommendation

All 4 researched racks are compliant with the EIA standard outlined in the previous section. The differences in the racks are the design of the housing to accommodate different hardware setups.

The 4-post rack is the cheapest rack. However, it does not have any enclosure around the rack itself. This can lead to dust and other harmful substances gathering on the hardware housed within the rack.

The Colo cabinets are made to have two (2) 21U cabinets in a single rack. The cabinets can be individually opened without having to affect the other cabinet.

The soundproof rack has built in noise reduction and heat dissipation. The manufacturer specifications show that this rack can reduce up to 20.7 dBA of noise while dissipating 3.0KW of heat. This rack is the most expensive rack of the four (4) racks researched.

The server cabinet is the cheapest closed server rack researched. The server cabinet does not have any value-added features.

In conclusion, the Colo cabinet rack is the recommended rack to be used in the Panadox data center. This is because the rack provides sufficient space for hardware, being a 42U rack, and provides more options for colocation solutions. Lastly, the price is suitable for a server rack with the listed features.

4.4 Cabling:

The two main types of cabling to be used in a data center are the UTP cables and optical fiber cables. Fiber cables are split into single-mode and multi-mode fiber. The figure below shows the comparison between multimode and single mode fiber in terms of cost, speed, and distance. (Optical Communication, 2018)

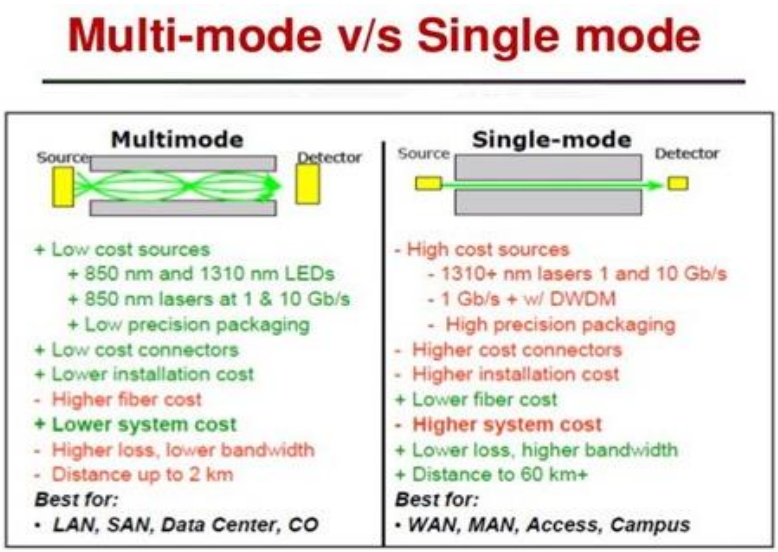

Figure shows the rack (Optical Communication,2016)

The same considerations are applied to UTP cables. Currently, UTP cables are split into 3 major standards, CAT5, CAT5e, and CAT6. The figure below shows the comparison between each standard respectively.

UTP Categories - Copper Cable

UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Figure shows the rack (Optical Communication,2016)

The figure above compares between five UTP categories of cables. The comparison made is between data rate, maximum length, and application. The proposed data center should ideally be using the highest bandwidth cable available.

5. Physical Design Overview:

5.1 Power:

5.1.1 Rated Electrical Voltage Supply for Data Center:

The PUE that shows in the calculation is 1.63, which is below average in the PUE table. As the data center that is locate in Malaysia which has no four seasons. This PUE is at the good efficient level for the data center. Unlike other country, where there has winter season, the PUE will be lower and more efficient because the use of cooling system can be decrease due to the environment of the country.

The power that has been use in this PUE majority is supply to IT devices because the need of 24 hours uptime. Also for the charging of the backup battery, it is to prevent the downtime of the cooling system and the server. The power that provide to the IT equipment need to be adjust because if the power is overload in the IT equipment, it may slow down the performance of the IT equipment. This will cause the dissatisfaction of customer where the service of the server is slow due to overload of the power.

When there is a power failure in the data center, the first thing that need to maintain is the cooling system. The temperature in the server room is a must to maintain because the server rack temperature can increase minimum up to 60 degrees Celsius within 18 seconds. If the server room is not maintaining in a low temperature, the heat may burn the server rack and cause fire, the sprinkler system will go off to put out the fire. This will cause damage to the IT equipment.

The PUE also helps the data center to calculate the bill of the power use. In Malaysia, the cost of the power that use in this data center is RM 332,377.21 include with 6% Government Service Tax (GST). With the help of PUE, we can manage the use of power in data center and understand the efficiency of the power that are using for every equipment in the data center.

5.1.2 Electrical Distribution System

Equipment	Power
IT Device	
10 Rack = 80 server	4600W x 10 (4600w per rack)
10 rack – 10 Ethernet Switch	204W x 10 (204W per rack)
4 routers = whole data center	240W x 4 (240W per router)
1 Computer	250W
Desktop/Printer	300W x 9(300w per device)
Total	**51,950W**
Non-It Device	
Cooling System	30kW
Lighting	100W x 20 (100W per bulb)
Smoke detector	0.4W x 15 (0.4W per detector)
Coffee Maker	850W
Total	**32,856W**
Total for all	**84,806W**
Kilowatt per hour	Kilowatt x hours
	= 84,806W x (24 hours x 30 Days)
	= 84,806W x 720
	= 61,060kWH

As we can see the calculation above, has include both IT and Non-IT equipment that use in the data center. For the monthly power usage of the data center will be 61,060kWh. The data center is expected to be 24 hours uptime. So, the power consumption of the data center will be as shown as above, of cause there is some situation where the lights and fans or computers are off when the workers are going home. But the majority of the power was use on the IT equipment and the cooling system, so the power consumption will not drop much.

Moreover, the cooling system takes 40%-50% of the power in the data center, because the environment in the cabinet has to be maintain in a correct temperature. Besides that, the server rack has the second higher power usage in the data center. As if there is a blackout, the first thing that has to maintain is the cooling system. Because they have to maintain the temperature of the rack as the temperature of the rack can be up to 60 degrees Celsius within seconds. It is also to prevent fire to breakout due to the high temperature.

5.1.3 Power Distribution in IT Space

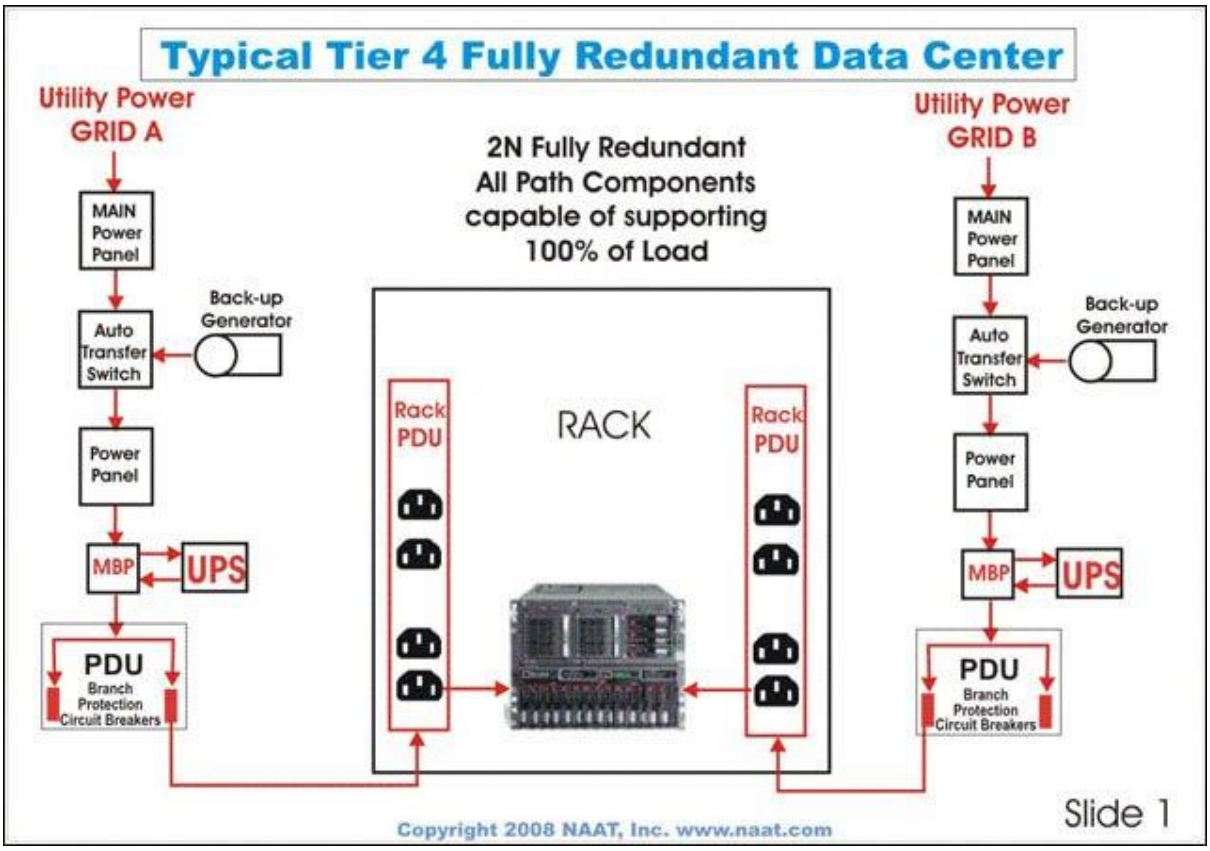

Figure shows power distribution in IT space(Beh,2018)

For the data center, we will be implement a tier 4 data center for Panadox. This is produce a very efficient power usage for the data center. It contains 2N redundancy which ensure 100% uptime for the IT equipment. 2N redundancy means 2 times the amount of capacity required to the power, backup and cool the load. This works well for co-location server, because there will be no unscheduled server shutdown due to power loss. The chance of total failure is extremely low and nearly non-existent.

So, for the data center is good to use 2N redundancy in order to maintain the uptime of the service. With proper maintenance of the system, there should never be both A and B side unavailable, means there should always power available for normal operations. With two power supply from different utility, this can prevent the blackout and the loss service for the customer.

Power from the electric utility delivered at voltage anywhere from 480V to 21kV or higher. First step in the distribution process is to transform this voltage to a level that is usable by the building and data center equipment. This process is to reduce the overload of power that distribute to the equipment and maintain the voltage in the data center.

Second process is use switchgear and distribution boards to safely distribute from the utility to the data center floor. The switchgear includes circuit breakers and switches for managing medium and low voltages and they are typically used to distribute large amounts of power to various locations within datacenters and buildings. The purpose of this process is to interrupt and disconnect the load from the power source in the event of abnormally high current conditions that could damage the electrical system or create unsafe operating conditions

Third process is the power distribution unit (PDU) will control the power that distribute by the switchgear and provide the power to the equipment. It can monitor the use of the power supply in the data center in order to assist in balancing the power loads. Lastly, rack power distribution which is a rack-mounted power distribution that distributes the power to the IT equipment that installed in the rack. It monitors the power supply to each of the IT equipment to prevent overload of power in the IT equipment.

5.2 Cooling Solutions

The purpose of data center cooling system is to maintain the environment condition suitable for the equipment to operate (Sasser, 2018). There are two types of cooling system that is commonly use in data center, hot aisle containment system and cold aisle containment system.

5.2.1 Hot Aisle Containment System

A hot aisle containment system (HACS) encases the hot aisle to gather the IT equipment's hot fumes air, permitting whatever is left of the data center to wind up an expansive frosty air return plenum. By containing the hot aisle, the hot and cold air streams are isolated. Note at this regulation technique requires the columns of racks be set up in a reliable hot aisle or cold aisle course of action. Images below show how the hot aisle containment unit works (Niemann, 2018).

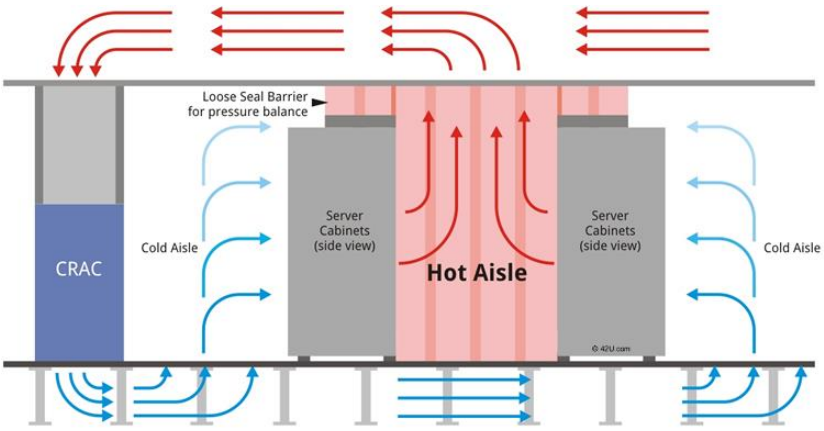

Figure show the hot Aisle (Beh,2018)

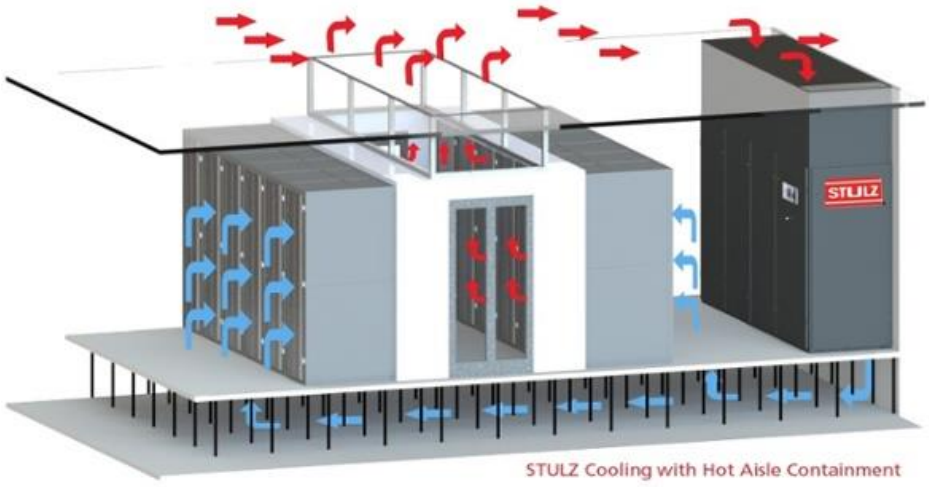

Figure show the hot Aisle (Beh,2018)

5.2.2 Cold Aisle Containment System

Cold aisle expands its antecedent's (hot aisle/cold aisle) plan by encasing the cold aisle. The path at that point turns into a room unto itself, fixed with boundaries made of metal, plastic, or plexiglass. A cold aisle containment system (CACS) encases the cold aisle, permitting whatever is left of the data center to wind up an expansive hot air return plenum. By containing the cold aisle, the hot and cold air streams are isolated. Note at this regulation technique requires the columns of racks be set up in a reliable hot aisle or cold aisle course of action. Images below show how the cold aisle containment unit works (Niemann, 2018) .

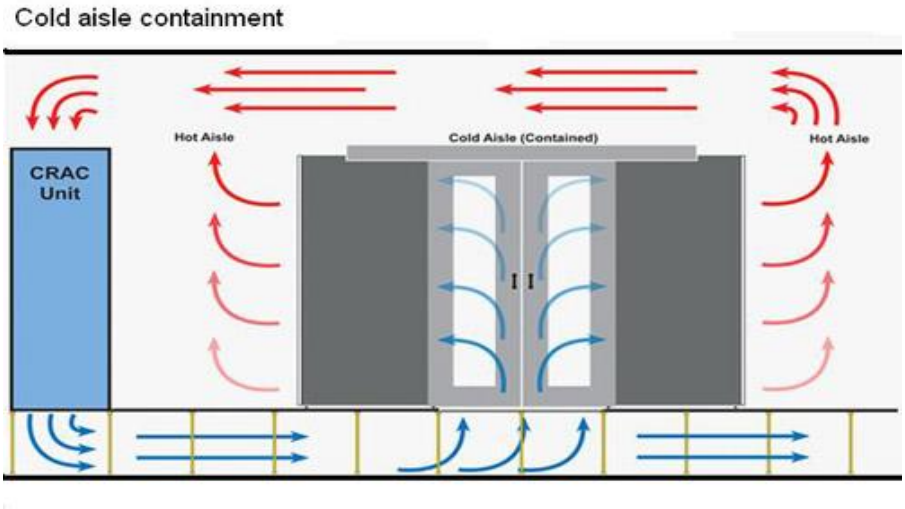

Figure show the cold Aisle (Beh,2018)

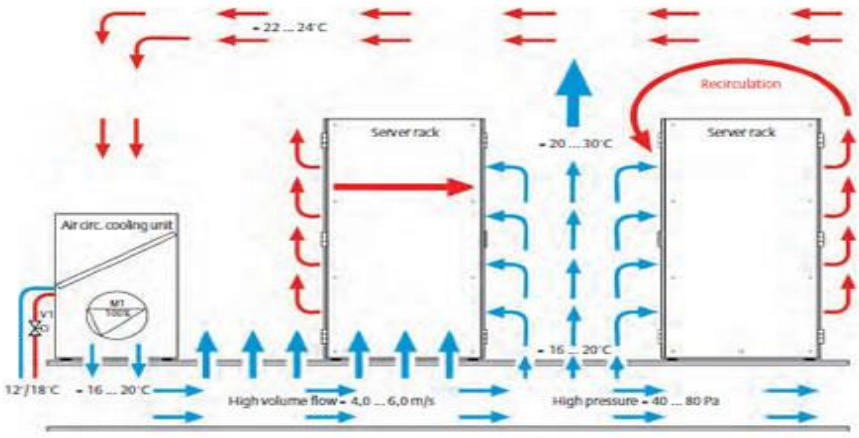

Figure show the hot Aisle (Beh,2018)

5.3 Advantages

1. Hot Aisle Containment System

Hot Aisle Containment is that the general data center space stays cool, killing the recognition by visitors that the IT equipment isn't being cooled adequately and taking into consideration some low-thickness areas to be un-contained if wanted. Having the hot air contained as opposed to being depleted around likewise causes for the employees to work ordinarily without feeling uncomfortable. Additionally, the precise dissemination of supply air all through the space is less basic. For whatever length of time that the cool air is brought into the general space, even a long way from the server admissions, and hot air is legitimately returned, costly raised floor supply dispersion frameworks and broad supply ventilation work can be avoided. (Travis Steinmetz & Thomas Squillo, 2018)

2. Cold Aisle Containment System

Cold Aisle Containment can be utilized with raised floor supply plenums or overhead ducted supply with no raised floor. In the event that controls are planned accurately, it might offer some effectiveness points of interest by giving more noteworthy capacity to control supply air to coordinate server wind stream. Cold Aisle Containment does not require an arrangement of air pipes and is for the most part more affordable to run. You fundamentally just need to close off the highest point of the cabinets and include doors. This likewise makes it less demanding to switch to older data center over to this system. (Travis Steinmetz & Thomas Squillo, 2018)

5.4 Disadvantages

Hot Aisle Containment System

Since the system requires an arrangement of ducts and interfaces with the roof, hot aisle containment is regularly the costlier option to be choose. Additionally, given its name, this system makes the hot aisle significantly hotter, which can make an uncomfortable workplace for technicians. (Travis Steinmetz & Thomas Squillo, 2018)

Cold Aisle Containment System

Disadvantage of Cold Aisle Containment System is allowing the release air from the hot aisle to fill the room brings the temperatures somewhere in the range of 80 to 100 degrees F all through most of the data center. This can make recognition issues for organization officials or for occupants of a co-location data center. It may cause operational issues if any non-contained hardware, for example, low-density storage or communication racks, is installed in the general data center space. Additionally, by and large, cold aisle has middle of the road roofs over the aisle. This may influence the general fire protection and lighting outline, particularly when added to a current data center. (Travis Steinmetz & Thomas Squillo, 2018)

5.5 Recommendation

Looking into all the considerations that has been made, the recommended cooling system that will be used by Panadox is hot aisle containment system. It is a more proficient approach than cold aisle containment system since it permits higher workplace temperatures and expanded chilled water temperatures which brings about expanded economizer hours and noteworthy electrical cost investment funds. Cooling set options can be set higher while still keep up an agreeable workplace temperature.

6. Equipment Racking

6.1 Recommendation for rack model

Equipment Racking is a important part in the way to create a well-designed data center. It comprises of where and how the equipment is housed in the facility itself. While considering the way that data center will encounter development in the future, they need to prepare for the overhaul or extension that may happen. With a legitimate equipment racking arrangement, this can be accomplished. (Rackmountsolutions, 2018)

Before proceeding to the racking model, first is to do a proper evaluation about cooling system and power supply. After the necessary steps has been done, the installation of the server racks can begin. Consider the connections of the network and power, a large space is needed for the connections to be done, as server is tending to be deep. The most suitable rack model for this is a 42U Universal Server Rack, it is 42-inch deep cabinet, with 83.02 inches height, 24 inches width for the external and internal about 19 inches width, which can help the cabling and power management. (Rackmountsolutions, 2018)

Another important thing to be concerned is the type of rails that is suitable with the servers. Current age servers at first touch base with square opening style vertical rack rails on their rack mounts. Without the required rails and mounts implies using, separate connectors which is bother. This is on the grounds that it makes the equipment and servers hard to oversee and furthermore incomprehensible now and again without taking out other hardware or immolate space. The rails for the recommended rack is adjustable which makes the placement for the servers easy to manage and easy work for the technician to do maintenance when there is a problem occur. (Rackmountsolutions, 2018)

This rack is rated up to 3000 pounds of IT equipment. It is also RoHS compliant which means that the materials that use to make this rack is approve by the community where the materials will not cause hard to human body. If the use of material is not approved by the community from the country that created the rack, it may cause harm to human health and cause hazardous to the data center. This may result the loss of trust from the customer who want to buy the server rack.

In the end, equipment rack is a very important factor to consider with when designing a data center. It has blueprint which can ensure that the physical environmental requirements are met. These also involve the easy maintenance, scalability, and efficiency of power supply.

6.2 Advantage

- **Hot Aisle Containment System**

Hot Aisle Containment is that the general data center space stays cool, killing the recognition by visitors that the IT equipment isn't being cooled adequately and taking into consideration some low-thickness areas to be un-contained if wanted. Having the hot air contained as opposed to being depleted around likewise causes for the employees to work ordinarily without feeling uncomfortable. Additionally, the precise dissemination of supply air all through the space is less basic. For whatever length of time that the cool air is brought into the general space, even a long way from the server admissions, and hot air is legitimately returned, costly raised floor supply dispersion frameworks and broad supply ventilation work can be avoided.

- **Cold Aisle Containment System**

Cold Aisle Containment can be utilized with raised floor supply plenums or overhead ducted supply with no raised floor. In the event that controls are planned accurately, it might offer some effectiveness points of interest by giving more noteworthy capacity to control supply air to coordinate server wind stream. Cold Aisle Containment does not require an arrangement of air pipes and is for the most part more affordable to run. You fundamentally just need to close off the highest point of the cabinets and include doors. This likewise makes it less demanding to switch to older data center over to this system.

6.3 Disadvantage

-Hot Aisle Containment System:

Since the system requires an arrangement of ducts and interfaces with the roof, hot aisle containment is regularly the costlier option to be choose. Additionally, given its name, this system makes the hot aisle significantly hotter, which can make an uncomfortable workplace for technicians. (Travis Steinmetz & Thomas Squillo, 2018)

- Cold Aisle Containment System:

Disadvantage of Cold Aisle Containment System is allowing the release air from the hot aisle to fill the room brings the temperatures somewhere in the range of 80 to 100 degrees F all through most of the data center. This can make recognition issues for organization officials or for occupants of a co-location data center. It may cause operational issues if any non-contained hardware, for example, low-density storage or communication racks, is installed in the general data center space. Additionally, by and large, cold aisle has middle of the road roofs over the aisle. This may influence the general fire protection and lighting outline, particularly when added to a current data center. (Travis Steinmetz & Thomas Squillo, 2018)

6.4 Recommendation

Looking into all the considerations that has been made, the recommended cooling system that will be used by Panadox is hot aisle containment system. It is a more proficient approach than cold aisle containment system since it permits higher workplace temperatures and expanded chilled water temperatures which brings about expanded economizer hours and noteworthy electrical cost investment funds. Cooling set options can be set higher while still keep up an agreeable workplace temperature.

7. Equipment Racking

7.1 Recommendation for rack model:

Equipment Racking is a important part in the way to create a well-designed data center. It comprises of where and how the equipment is housed in the facility itself. While considering the way that data center will encounter development in the future, they need to prepare for the overhaul or extension that may happen. With a legitimate equipment racking arrangement, this can be accomplished.

Before proceeding to the racking model, first is to do a proper evaluation about cooling system and power supply. After the necessary steps has been done, the installation of the server racks can begin. Consider the connections of the network and power, a large space is needed for the connections to be done, as server is tending to be deep. The most suitable rack model for this is a 42U Universal Server Rack, it is 42-inch deep cabinet, with 83.02 inches height, 24 inches width for the external and internal about 19 inches width, which can help the cabling and power management.

Another important thing to be concerned is the type of rails that is suitable with the servers. Current age servers at first touch base with square opening style vertical rack rails on their rack mounts. Without the required rails and mounts implies using, separate connectors which is bother. This is on the grounds that it makes the equipment and servers hard to oversee and furthermore incomprehensible now and again without taking out other hardware or immolate space. The rails for the recommended rack is adjustable which makes the placement for the servers easy to manage and easy work for the technician to do maintenance when there is a problem occur.

This rack is rated up to 3000 pounds of IT equipment. It is also RoHS compliant which means that the materials that use to make this rack is approve by the community where the materials will not cause hard to human body. If the use of material is not approving by the community from the country that created the rack, it may cause harm to human health and cause hazardous to the data center. This may result the loss of trust from the customer who want to buy the server rack.

In the end, equipment rack is a very important factor to consider with when designing a data center. It has blueprint which can ensure that the physical environmental requirements are met. These also involve the easy maintenance, scalability, and efficiency of power supply.

8. Network Security

8.1 Physical Security Guidelines:

The purpose of physical data center security is to restrict people who can access to the data center building, and in the event that they do, they need to be identified as soon as they enter. There are a lot of assets to direct the procedure of outlining an extremely secure data center. Below is a few essential rules and guidelines that any data center should have (Barker, 2016).

1. The data center should be kept away form a populated territory and not known to everyone and it should have no signs that relates to “data center”.
2. The data center should be disconnected from the company’s main office.
3. The data center should have limited entering points and they need to be controlled and guarded by security, and all these points should be observed by CCTVs.
4. Visitors can enter only from one point, so they can be identified easily.
5. Unauthorized people are denied form entering the data center room and man-traps where allow only one person goes in at a time should be applied.
6. The data center should be guaranteed with physical safety efforts, for example, monitors, fingerprint and intrusion detection.
7. Server rooms should have a programmed entryway door that closes after a timeframe and having an alarm if it is being opened for a long time.
8. The data center should have CCTV cameras as much as possible to cover all areas in it and all the records should be saved digitally and archived offsite.
9. security staff should be hired meticulously and trained to be familiar with the whole site.
10. the data center construction should be able to keep it away from any harms such as water, fire, and any harms.

8.2 Network Security Guidelines:

Network Security becomes a significant aspect in data centers and some guidelines and measures should be considered to confirm the accessibility and security of the shared network resources. Below some of them are discussed (Secretariat-yorku 2015).

1. All access points or any network device in the data center should have an authorization and authentication process so only who has the right permission can access and get the full services.
2. Use an efficient network management system that monitors all the traffic in the network to detect unauthorized activity or intrusion attempts and deliver reports and statistics. This system should have bandwidth management and load balancing features to ensure that efficient use of the network resource is used.
3. The data center administrators should perform vulnerability analysis and provide training to the staff make them aware of any threats such as Social Engineering.
4. Admins only have the permission to install, update or upgrade any application in the network.
5. A proper encryption method of data should be implemented to ensure the data integrity and secure the exchange of data between networks.
6. Data back-up is necessary to restore them easily in anytime and it should be accessible from anywhere.
7. Accounting or auditing should be considered to check the data back if any threat happens.

8.3 Firewall and IPS:

Data centers have grown rapidly and become widely used solution to overcome the expanding requests for network connectivity in the past few years. Thus, guaranteeing those connections stay secure is vital. Most of the large networks battle to stay aware of mobile workforce where every point needs to be connected via Internet, so the need of solution that combines a firewall and Intrusion Prevention system is necessary (Cisco.com, 2017).

Firewall is device or software or both that stops unapproved access to your datacenter and its main function is to scan access from or toward the network and to make those unapproved access not gaining access to the datacenter. Example of these scenarios are Denial of Service attack where the attacker is trying to take down your network by overwhelming it with too many traffic and the second one is Intrusion where the attacker is trying to gain access to the data center by using a correct username and password to get some data from your network without your knowledge (Fortinet, 2016).

Intrusion Prevention System IPS is used to keep away from undesirable access in the network. IPS is installed in the network to secure the client activity from cybercriminal attacks by dynamically looking for and denying external threats before they can reach possibly vulnerable network hosts (Fortinet, 2016).

The recommended firewall and IPS is The Cisco ASA 5585-X series which can maintain a high level of security by providing unique scalability, greater performance and leading-edge security – in a small and 2RU frame factor. The Cisco ASA 5585-X consolidates a demonstrated firewall with a complete IPS and a superior VPN. This series of device more powerful by 8X performance density of other firewalls as it supports the maximum VPN session totals, twice the same number of connection every second, and 4X the connection capacity of other firewalls to encounter the developing needs of the present most unique organizations – all in a minimal 2RU frame. The Cisco ASA 5585-X runs data centers with the best-of-breed firewall, IPS and VPN as it essentially decreases introductory obtainment costs by 80%, power consumption costs by 85% and the rack space prerequisites by 88% compared to other solutions, moreover, it reduces significantly the overall integration and management difficulty and prices. Large data centers will likewise profit by decreasing cooling costs with reducing 80% of power consumption. As opposed to bringing about extra management and deployment costs by requiring two different devices from two different sellers, the Cisco ASA 5585-X can provide a demonstrated firewall and a full IPS. In addition, the ASA 5585-X gives the alternative a completely incorporated chassis or to coordinate extra administrations as the necessities of the business growth. All of them make Cisco ASA 5585-X is the most suitable solution for the data center compared to any competitive firewall and IPS where most of them not integrated (Cisco.com, 2017).

8.3 Fire Suppression System:

In the past, the temporary interruption and interference of business was inexpensive to overcome, and the operation of the data center will not be affected that much. Yet, with the expanding of IT infrastructure and technologies, the downtime of the data center can carry out a serious effect of any business which will affect its customers, providers and the whole enterprise. The downtimes in modern data center is perilous as according a 2013 Ponemon Institute report, the cost of data center downtime is higher than the past where from 2010 to 2013, the normal cost per minute of data center downtime enlarged 41%, from $5617 per minute in 2010 to $7908 per minute in 2013. Therefore, fire suppression has become a vital element of data center risk assessment (L. Robin, 2015).

There are several ways of protecting our data center from fire. The first one is the sprinkler system which is water based and used to control the fire by preventing it from spreading and avoid any structural harm. Sprinkler system is considered as inexpensive and an easy solution that uses around 25 gallons of water per minute. That leads to some disadvantages in which the electrical conductivity of data center equipment and in some cases, can be worse than the fire harm, moreover, the place where fire occurred needs to be immensely cleaned and that will cost the business more (L. Robin, 2015).

Another way that based on water is the Water mist systems which a new entrant in the water-based fire suppression. It needs good pressure pumps and specific nozzles to spread the water mist in the designated area and it is recommended on large areas only as it resulted a bad performance on small fires in terms of not fully flooding the area especially in the obstructed fires. Further, the mist systems leave residual water after the suppression and it costs and the equipment damages still a dilemma (L. Robin, 2015).

Another way of protecting our data center from fire is the clean agent which can extinguish the fire very fast and bound the fire harm to the data center equipment in its place and it has no need for water. The main purpose of implementing this type is to protect the valued, complex and critical resources. It is distinguished from the other types as it does not require any extinguishment cleaning and no corrosive or residues are left behind, thus, no additional costs are needed. It can extinguish protected, blocked or three-dimensional fires in complex areas (L. Robin, 2015).

Moreover, clean agent can be classified into two types. The first one is halocarbon agents that contains the elements of carbon, hydrogen, and halogen such as fluorine, thus, it carries out some dangerous effects for people who are in the fire place as the carbon will be flooded and that causes a ventilation issue. The second one is the inert gas agents which is prepared on gases like nitrogen, argon and carbon dioxide and less risky to humans than the first type and also less damage to the resources. The two agents are considered as non-conductive in terms of electricity and recommended to be used in typically covered spaces. To add on that, both have a high concern of safety as they are categorized and prepared by low chemical reactivity and low toxicity (L. Robin, 2015).

8.4 Recommendation

From the previous discussion and many real-world tests that have been done before such as a test was held by Kidde which is a world leader in the development and manufacture of fire detection and protection systems between clean agent -inert gas type- and water sprinkler where inert gas performed very well, quickly and with less damage compared to the water sprinkler (YouTube, 2018). We are as a Tamanix team would suggest the clean agent -inert gas type- system to be implemented in Panadox data center as the many advantages and features it has such as it can extinguish the fire quickly and restrict the damage in a specific area as well as it does not require any major cleaning after the fire occurs. Moreover, the cost of its implementation is inexpensive and finally it is quite easy to install and maintain and has no harm for either people's health or the environment. Additionally, we still need to use sprinkler system outside of data center's core such as the entrance and place some halocarbon agents to be as assistance in some situations.

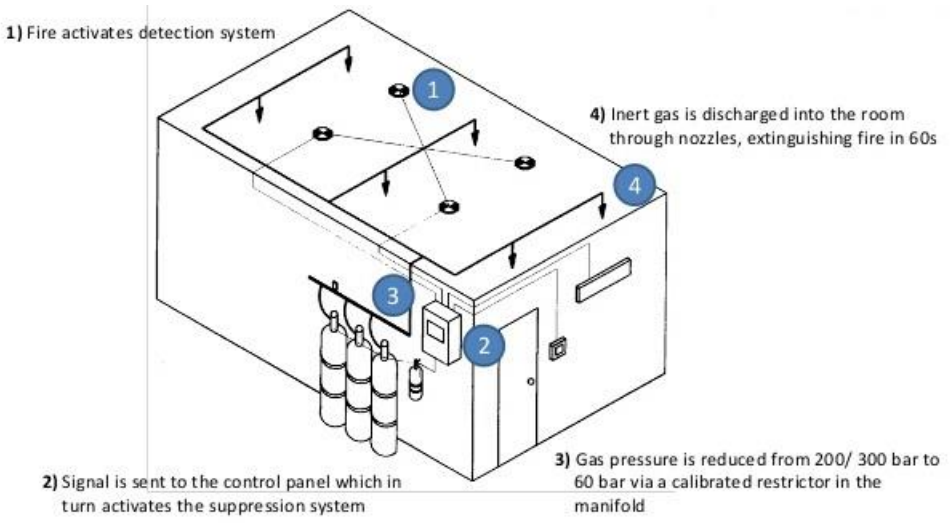

Figure 1 shows how inert is implemented in the data center (Worldwide, 2016)

Figure 2 shows the halocarbon agents (Brickwood.co, 2015)

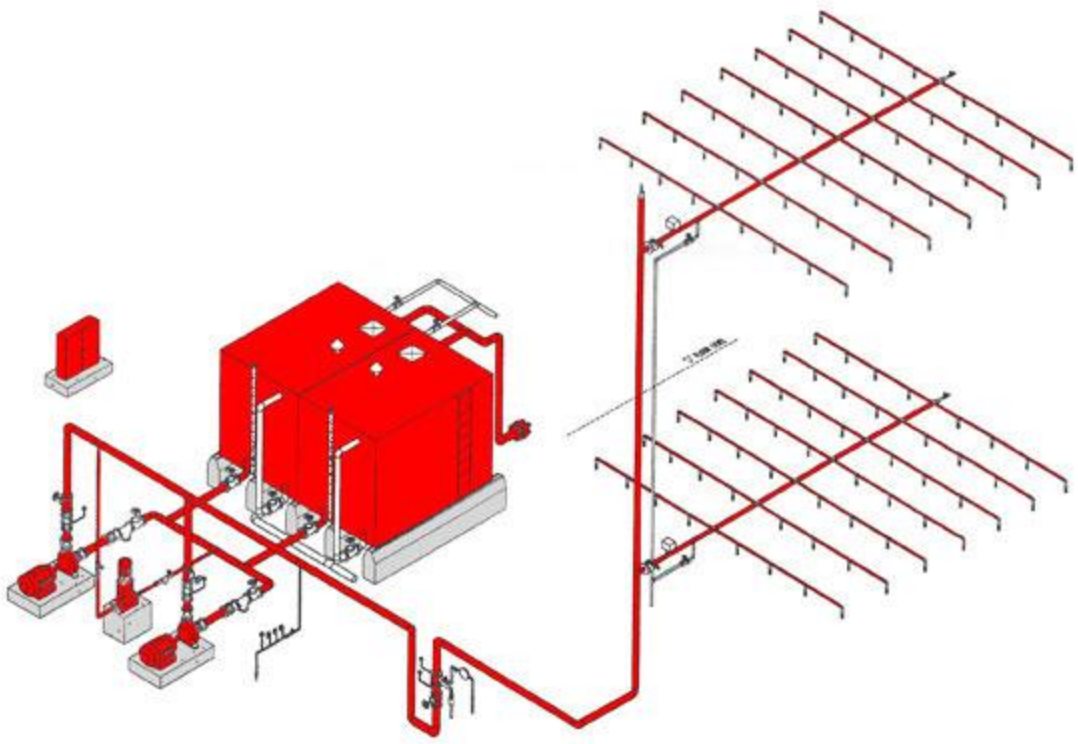

Figure 3 shows how Sprinkler system is implemented outside of the data center (Rajyogfire.com, 2016)

9 Physical Security

Physical security is an important thought when it comes to securing the information of our data center. Physical security should be employed properly as it is used to stop attacks that try to gain access to our data center. The need of applying physical security measures is more necessary now than in the past as all the data center devices store vital data that can be damaged or stolen.

The main objectives of deploying physical security is to protect the data center information, devices and IT infrastructure from any threat that might disrupts the operation of it by causing any illegal activities such as theft, data leaks or damage anything in the data center by physical involvement. Statistics show that about 74,000 workers, providers, and contractors in 2014 were victims of a data breach as by stealing their devices (Scott, 2014).

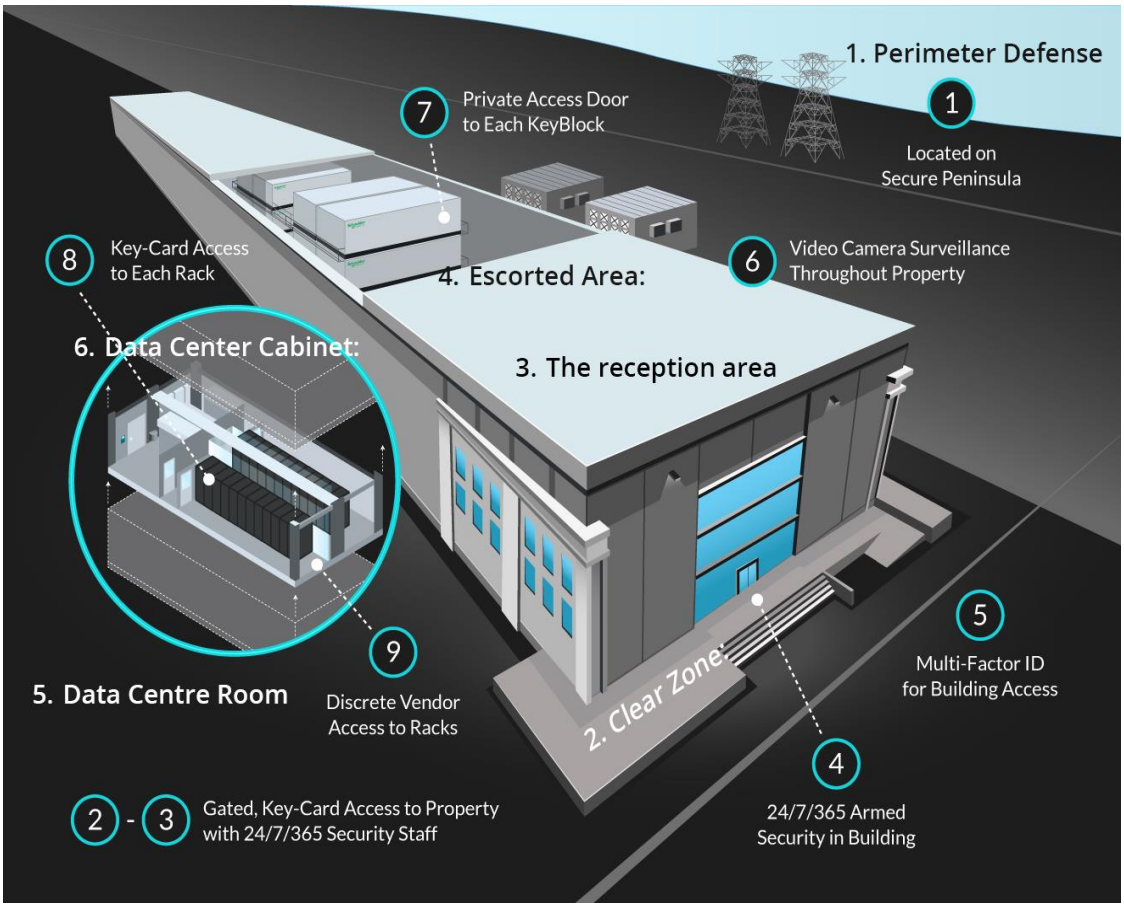

Figure 1 show layers and its features of the physical security layers (Keystone NAP, 2017)

A defense in depth approach is recommended for a data center. The security architecture consists of several layers of physical security need to be considered to ensure a whole guard of our data center and to conform with the data center protection guidelines (Datacenterdynamics.com, 2015).

9.1 Perimeter Defense:

The initial layer of physical security is the perimeter defense which controls and restricts the access of the data center property. It is very essential layer as it could lessen the expense of the data center security plan and improve the efficiency of it by controlling the admission of individuals into the data center. The first need of this stage is to use fencing which is the first line of the data center protection that separates it from the environment. Another thing is using security

sensors in the fences or the walls to vibrate and disturb by detecting if anyone is trying to enter the perimeter defense. Perimeter Lighting and Thermal Cameras may be applied also.

9.2 Clear Zone

The second layer of physical security is clear zone which is essential as it is the next point after entering the perimeter where all the critical and mechanical are placed like the main power suppliers and wires and the backups. This level needs to be equipped with an active video monitoring system to guard the area in case of any harm. These surveillance cameras should be a high-resolution and cover the whole area. Other aids can be security alarm and access cards or controlled keys as well as implementing multipoint locking systems for the doors.

9.3 The reception area

The third layer of physical security is the reception area and facility façade where guest control begins by providing them with a guest badge to be identified with. The badge should have the visitor's photo and its expiration time and date. Video surveillance is also important in this level to capture and monitor what is happing as well as using card readers to access for the other facilities is needed.

9.4 Escorted Area:

The next layer of physical security is the escorted area or the gray space which is the way that we can go to the data center with and it is significant as much as the previous levels. It is used often by the guests to take a look of the data center equipment and devices, so some measures need to be taken to protect it as using a proper access control method and restrict who can access by the card readers. Another way is by letting people to enter individually which is more secure than letting them in groups and using secure the doors in the facility. Lastly which is the main requirement is using the surveillance cameras to monitor and safeguard the area.

9.5 Data Centre Room:

The fifth layer of physical security is the data center room or the while space which is the room that has all the data center racks and servers and the need to deny or prevent any unauthorized people to access into our data center room is really pivotal. Cages to divide the customer's cabinets may be applied to improve the protection as well as providing them with video surveillance, intrusion detection and access control that uses biometrics.

9.6 Data Center Cabinet:

The last layer of physical security is the data center cabinet which the core of our data center and holds all the IT infrastructure and resources. It is very sensitive area as it is vulnerable to insider attacks. Access control to the servers and devices is necessary by restricting and locking them and provide video surveillance should keep away from ant threat.

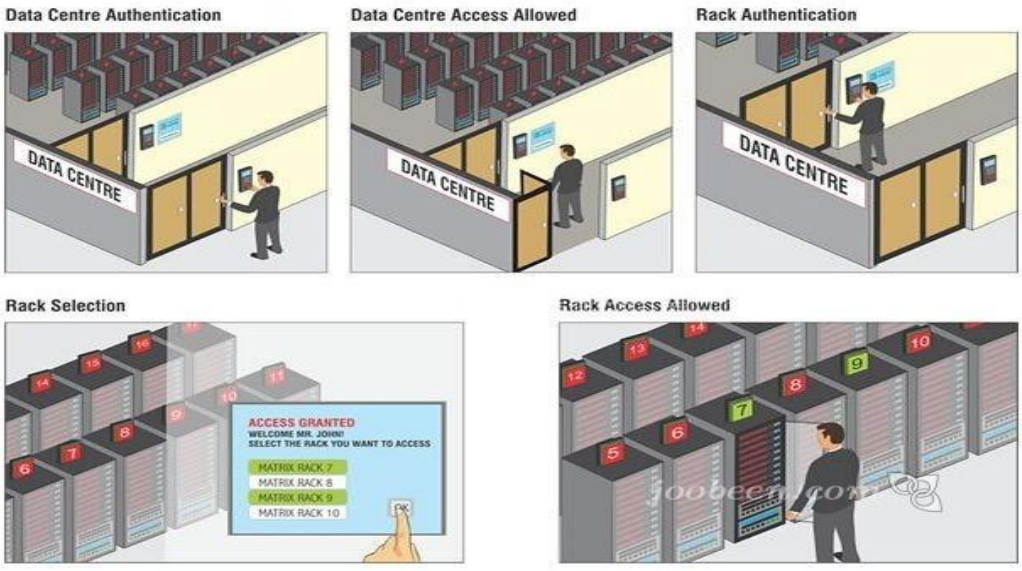

Figure 1 show an overall of the physical security layers (Joobeen.ir, 2017)

10.Conclusion:

To summer up, information technology field is continually advancing and the interest for more up to date and better solutions will never stop. The solutions and equipment decided for this assignment are unquestionably future confirmation on it its own. The proposed datacenter is well thoroughly considered from security to execution astute. In addition, Co-location seriver which allow clients to co-locate their data by renting a space in the datacenter and determining what devices they want to choose. What has been highlighted in this task should turn out to be exceptionally solid if executed. We likewise trusted that we have met every one of the necessities of Panadox.

Workload Matrix:

Task	Abdurraouf Fathi (TP042816)	Beh Wei Xiang (TP047430)	Benedict Loh TP047430
1.Introduction to Data Center	100%		
2.Data Center Requirements	50%	-	50%
3.Data center design overview chapter	-	-	100%
4.Hardware overview chapter	-	-	100%
5.Physical Design Overview chapter	-	100%	-
6.Equipment Racking chapter	-	100%	-
7.Network Security chapter	100%	-	-
8.Physical Security chapter	100%	-	-
9.Conclsuion	100%	-	-

References

Barker, D. (2016). A Guide to Physical Security for Data Centers. [online] The Data Center Journal. Available at: http://www.datacenterjournal.com/a-guide-to-physical-security-for-data-centers/ [Accessed 23 Apr. 2018].

Brickwood.co. (2018). Halon Fire Extinguishers | BrickwooD®. [online] Available at: http://brickwood.co/halon-fire-extinguishers-in-bangalore/ [Accessed 7 Apr. 2018].

Cisco.com. (2017). Cisco ASA 5585-X. [online] Available at: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-730903.pdf [Accessed 23 Apr. 2018].

Datacenterdynamics.com. (2015). RISK MANAGEMENT BEST PRACTICES. [online] Available at: http://www.datacenterdynamics.com/download?ac=14079 [Accessed 7 Apr. 2018].

Fortinet. (2016). Enterprise Firewall - DCIPS. [online] Available at: https://www.fortinet.com/solutions/enterprise-midsize-business/data-center-security-sdn/dcips.html [Accessed 23 Apr. 2018].

Joobeen.ir. (2017). Data Center Access Control | JOOBEEN. [online] Available at: https://joobeen.ir/solutions/data-center-access-control/ [Accessed 7 Apr. 2018].

Keystone NAP. (2017). Advanced Security - Keystone NAP. [online] Available at: http://www.keystonenap.com/advanced-security/ [Accessed 23 Apr. 2018].

L. Robin, M. (2015). Fire Protection Options for Data Centres. [online] Chemours.com. Available at: https://www.chemours.com/FE/en_US/assets/downloads/pdf/201501-FireBuyerArticle.pdf [Accessed 6 Apr. 2018].

National centers for environmental information, 2015. *NCDC Releases 2014 U.S. Climate Report.* [Online] Available at: https://www.ncdc.noaa.gov/news/ncdc-releases-2014-us-climate-report [Accessed 1 April 2018].

Niemann, J., 2018. Hot Aisle Vs Cold Aisle. [Online]

Available at:https://www.missioncriticalmagazine.com/ext/resources/MC/Home/Files/PDFs/WP-APC-Hot_vs_Cold_Aisle.pdf

[Accessed 15 April 2018].

Optical Communication. (2018). Twisted Pair Cable VS. Coaxial Cable VS. Fiber Optic Cable. [online] Available at: http://opticalcommunication.fomsn.com/2016/11/23/twisted-pair-cable-vs-coaxial-cable-vs-fiber-optic-cable/ [Accessed 24 May 2018].

Rajyogfire.com. (2018). Automatic Sprinkler System, Sprinkler Heads, Flow Switches, Mumbai, India. [online] Available at: http://www.rajyogfire.com/fire-sprinkler-system-1.html [Accessed 7 Apr. 2018].

Rackmountsolutions, 2018. Rack Mount Solutions. [Online]
Available at: https://www.rackmountsolutions.net/hammond-clc2b42bk-42u-2-bay-colocation-cabinet/[Accessed 17 March 2018].

Sasser, J., 2018. UptimeInstitute. [Online] Available at: https://journal.uptimeinstitute.com/a-look-at-data-center-cooling-technologies/[Accessed 08 04 2018].

Secretariat-policies.info.yorku.ca. (2015). Network Security and Management (Guidelines and Procedures) | Secretariat Policies. [online] Available at: http://secretariat-policies.info.yorku.ca/policies/network-security-and-management-guidelines-and-procedures/ [Accessed 23 Apr. 2018].

Travis Steinmetz & Thomas Squillo, 2018. The ADvantage and Disadvantage of Hot Ails, Cold Aisle Containment Strategies. [Online]
Available at: https://www.facilitiesnet.com/datacenters/article/The-Advantages-And-Disadvantages-Of-Hot-Aisle-Cold-Aisle-Containment-Strategies-Facilities-Management-Data-Centers-Feature--14486
[Accessed 24 March 2018].

Worldwide (2018). AIRFIRE WORLDWIDE Inert Fire Suppression Systems. [online] Slideshare.net. Available at: https://www.slideshare.net/StefanoMuttoni/03-afww-inert-gases-eng [Accessed 7 Apr. 2018].

L. Robin, M. (2015). Fire Protection Options for Data Centres. [online] Chemours.com. Available at: https://www.chemours.com/FE/en_US/assets/downloads/pdf/201501-FireBuyerArticle.pdf [Accessed 6 Apr. 2018].

YouTube. (2018). Kidde Fire Systems – Fire Detection and Suppression Systems. [online] Available at: https://www.youtube.com/watch?v=SjZKsKXL-hI [Accessed 7 Apr. 2018].

Worldwide (2018). AIRFIRE WORLDWIDE Inert Fire Suppression Systems. [online] Slideshare.net. Available at: https://www.slideshare.net/StefanoMuttoni/03-afww-inert-gases-eng [Accessed 7 Apr. 2018].

Brickwood.co. (2018). Halon Fire Extinguishers | BrickwooD®. [online] Available at: http://brickwood.co/halon-fire-extinguishers-in-bangalore/ [Accessed 7 Apr. 2018].

Rajyogfire.com. (2018). Automatic Sprinkler System, Sprinkler Heads, Flow Switches, Mumbai, India. [online] Available at: http://www.rajyogfire.com/fire-sprinkler-system-1.html [Accessed 7 Apr. 2018].

Datacenterdynamics.com. (2015). RISK MANAGEMENT BEST PRACTICES. [online] Available at: http://www.datacenterdynamics.com/download?ac=14079 [Accessed 7 Apr. 2018].

Joobeen.ir. (2017). Data Center Access Control | JOOBEEN. [online] Available at: https://joobeen.ir/solutions/data-center-access-control/ [Accessed 7 Apr. 2018].

Barker, D. (2016). A Guide to Physical Security for Data Centers. [online] The Data Center Journal. Available at: http://www.datacenterjournal.com/a-guide-to-physical-security-for-data-centers/ [Accessed 23 Apr. 2018].

Secretariat-policies.info.yorku.ca. (2015). Network Security and Management (Guidelines and Procedures) | Secretariat Policies. [online] Available at: http://secretariat-policies.info.yorku.ca/policies/network-security-and-management-guidelines-and-procedures/ [Accessed 23 Apr. 2018].

Cisco.com. (2017). Cisco ASA 5585-X. [online] Available at: https://www.cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generation-firewalls/datasheet-c78-730903.pdf [Accessed 23 Apr. 2018].

Fortinet. (2016). Enterprise Firewall - DCIPS. [online] Available at: https://www.fortinet.com/solutions/enterprise-midsize-business/data-center-security-sdn/dcips.html [Accessed 23 Apr. 2018].

Keystone NAP. (2017). Advanced Security - Keystone NAP. [online] Available at: http://www.keystonenap.com/advanced-security/ [Accessed 23 Apr. 2018].