Booklet 1 – Standards (Draft)

Preface

The emergence of the Internet as a universal network and the continued advancements and maturity of Web technology have served as catalysts for a well-designed data centers. Government agencies across the region have data centers that are burdened by aging IT environments that consume an increasing amount of the annual operating budget and may, in turn, lead to technological obsolescence. In many cases, these organizations recognize the need for a truly transformative modernization of IT systems and processes. Thailand government agencies data centers are also in the same situation with most of the agencies data centers scattered all around the country. Electronic government agency (EGA) of Thailand has been given the responsibility of leading the digitization initiatives in Thailand. EGA soon realized that there is an urgent need for the modernization of all the agency data centers. As part of the modernization initiative, EGA also realized that data centers across the agencies need to adopt industry specific standards.

Adoption of standards is quite essential in the whole modernization initiative, as it provides agencies a level of assurance that the service they are providing meets a proscribed level of measurement for performance, safe operations, etc. Apart from that, standards also provide cost savings in terms of energy and cooling, better security features, augmented services levels, better design and location and better service level agreements. By providing a common method of comparison, agencies can choose the level of standards they adopt based on their individual priorities.

As part of data center modernization strategy, Frost & Sullivan in conjunction with EGA conducted a focus group discussion to understand the current adoption levels of data center standards among government agencies. With the knowledge of current adoption levels of agency data centers, Frost & Sullivan was able to develop future adoption level of for all the government agencies of Thailand.

Globally different government bodies have adopted data center standards in their respective regions. Uptime and TIA 942, most popular data center standards are being recommended by the Japanese and Malaysian government. Australia, Malaysia and USA have defined the PUE specific standards for its government agencies. Likewise various governments have defined the standards for different function areas of the data center.

The standards booklet contains information about the importance and need of standards, examples of adoption of standards, five core elements of standards, relevance and challenges among standards, maturity model for nineteen sub parameters of standards, benefit realization of standards, adoption scenarios of standards and finally service level agreements (SLA) for colocation and cloud computing.

Contents

1. Executive Summary

Governments across the world utilises various standards for reliable, cost effective and higher utilization of their data infrastructure assets. The standards enable various important purposes for the government viz. securing sensitive IT assets, securing record and data of public sector agencies, energy efficiency, consumption based and higher competency infrastructure. Data center industry is more than 20 years old and there are sizable international bodies that have been developing standards for it. The standards have been developed for different components of the data center and also for a particular outcome. The whole data center industry is quite complex to run and these standard guidelines help the industry to run the data centers smoothly and efficiently. But these standards are not easy to follow and they are quite challenging.

The technology savings approach cover everything from facility lighting to cooling system design, and have proven useful in helping some companies curb the trend of rising data center energy consumption. Most organizations still lack a cohesive, holistic approach for reducing data center energy use. Today's data centers are subject to more rigorous compliance standards than ever before. Expectations from customers regarding uptime, environmental impact, quality, operations, security and safety are encouraging best practices from colocation providers and operators. Various government acencies across the globe are on a constant series of change with respect to their Data Center Strategy. Many of them are either revamping and modernising their data centers or are into a consolidation phase or are simply into the growth phase of the data center journey of the agencies. These strategies are bolstered by the standards that they will use for the overall strategy to come into effect and for future investments.
There are many examples of international standards available including Uptime and TIA 942. Both standards provide tiers for service availability for data centers. The standards for energy and power are energy star, NABERS and ASHARE. The standards related to services is the PT DCI standard and HIPPA. LEED and BISCI are design standards for data centers. These standards are being adopted my government globally.

Standards adoption is at nascent stage in Thailand data center market and adoption is quite low compared to other south Asian economies

It is challenging for the data centers to have knowledge about which standards to adopt and which not to adopt. As a part of GDCM Strategy, a standards framework has been designed for the government agencies in Thailand with five core areas (energy and power, design and structure, server storage and utilization, location and site and SLA's).The five core areas have been further divided into nineteen core sub-parameters and each of nineteen sub-parameters have five levels of adoption. The future adoption levels developed are the minimum level that each of the agencies should adopt and if required they can further go up in the chain. We also highlighted the adoption scenarios for the each of the nineteen sub parameters for four types of future agency data centers.

In some cases the government agencies would be using the services of third party colocation provider and cloud computing players. Frost & Sullivan have developed detailed components of service level agreements for both colocation and cloud computing, as this would help Thailand government agencies developing their own SLA's.

2. Need for the Standards

Rapidly-increasing traffic is driving the data storage for governmanet agencies as well as enterprises , which is resulting in continuous expansion of the data center. The number of web and mobile applications being developed and used is on the rise thereby driving demand for web space. The advent of newer technologies such as data analytics, big data, Internet-of-Things, etc. is increasing the amount of data that is collected and stored. Fuelled by these factors among others, the global data centers industry is expected to grow across the world. Data centers are essential to the functioning of modern economy and are found nearly in every sector of the economy: government institutions ,financial services, high-tech universities, media, telecommunication, , and retail.

The overall data center workloads are expected to double from 2013 to and the approximately five exabytes of data online in 2002 rose to 750 EB in 2009; by 2021 it is expected to cross the 35 zettabytes level. The growth of data centers is also driven by the evolution of cloud-based services and smart cities. By 2018, more than 78% of workloads will be processed by cloud data centers and almost 22% will be processed by traditional data centers,

Some of the world's biggest technology organizations (e.g., Microsoft, Google, IBM, and Cisco) have taken on the development of smart cities for which the data centers will provide the infrastructure support. For example, data centers will be storing and processing the data received through sensors to detect excessive air pollution, integrated traffic controls, and education systems. Overall, the number of data centers is expected to increase dramatically in the near future. Considering the growth expected in data center industry, interest is growing to reduce the energy consumption and make data centers more energy efficient.

Since data centers operate 24/7 and are highly energy intensive, the energy intensity of a data center may be 10 to 100 times of a typical commercial building. Rising energy prices are also increasing the operating cost of data centers and it has been reported that global data center carbon emissions will grow 7% year-on-year through 2020.

It is estimated that achieving just half of the technologically feasible savings through adopting best practices could cut electric use by 40% in data centers. The technology savings approach cover everything from facility lighting to cooling system design, and have proven useful in helping some companies curb the trend of rising data center energy consumption. Most organizations still lack a cohesive, holistic approach for reducing data center energy use. It is not considered sufficient to simply recognize the need to save energy and improve efficiency; one need to quantify key benefits associated with energy efficient practices and prioritizes actions to achieve them. To assist organizations measure the savings from adopting best practices, associations such as The Green Grid have developed metrics such as Power Usage Effectiveness (PUE) and Data Center Infrastructure Efficiency. Historically, mainframes had their own unique requirements, given the separate physical space and room utilities with limited movement post installation However, today data center environment is no longer static and characterized by the need for greater integration, outsourcing to third party environments and need for changes in environment to accommodate new technologies.

To enable effective management and provisioning of services in the dynamic environment, standards play a role in recommending practices and performance requirements and thereby provide a framework for best practices

Today's data centers are subject to more rigorous compliance standards than ever before. Expectations from customers regarding uptime, environmental impact, quality, operations, security and safety are encouraging best practices from colocation providers and operators. Certifications such as ISO, Uptime, Leed and SSAE16 are just some of the standards proving of significant importance to those in the market for colocation data centers. To help differentiate data centers, service providers and data center operators publish certifications for the following regulatory and standards organisations:

Various government acencies across the globe are on a constant series of change with respect to their Data Center Strategy. Many of them are either revamping and modernising their data centers or are into a consolidation phase or are simply into the growth phase of the data center journey of the agencies. These strategies are bolstered by the standards that they will use for the overall strategy to come into effect and for future investments.
Effectively as a result the standards have evolved over time and will continue to be in that mode based on:

- ✓ Experience of other players and agencies
- ✓ Geographical nuances, technology needs, behaviour of agencies, data types, weather conditions
- ✓ Technology used, robustness required
- ✓ Budgets
- ✓ Global best practices

Over the past 20 years as and when the data centers started gaining prominence, data centers were historically designed in the absence of established standards or best practices. This had many network administrators faced with the challenge of choosing technologies and deciphering how to properly implement them into an often-undersized space that is responsible for securely and reliably providing all the existing and future services to an enterprise. Not just the technological components but areas like security, design and construction were ad-hoc as similar to developing a commercial real-estate.
Over time, various standards started coming to shape- some developed by international bodies on specific areas of data center whilst some standard practices started gaining prominence as an outcome of lessons learnt across various implementations.

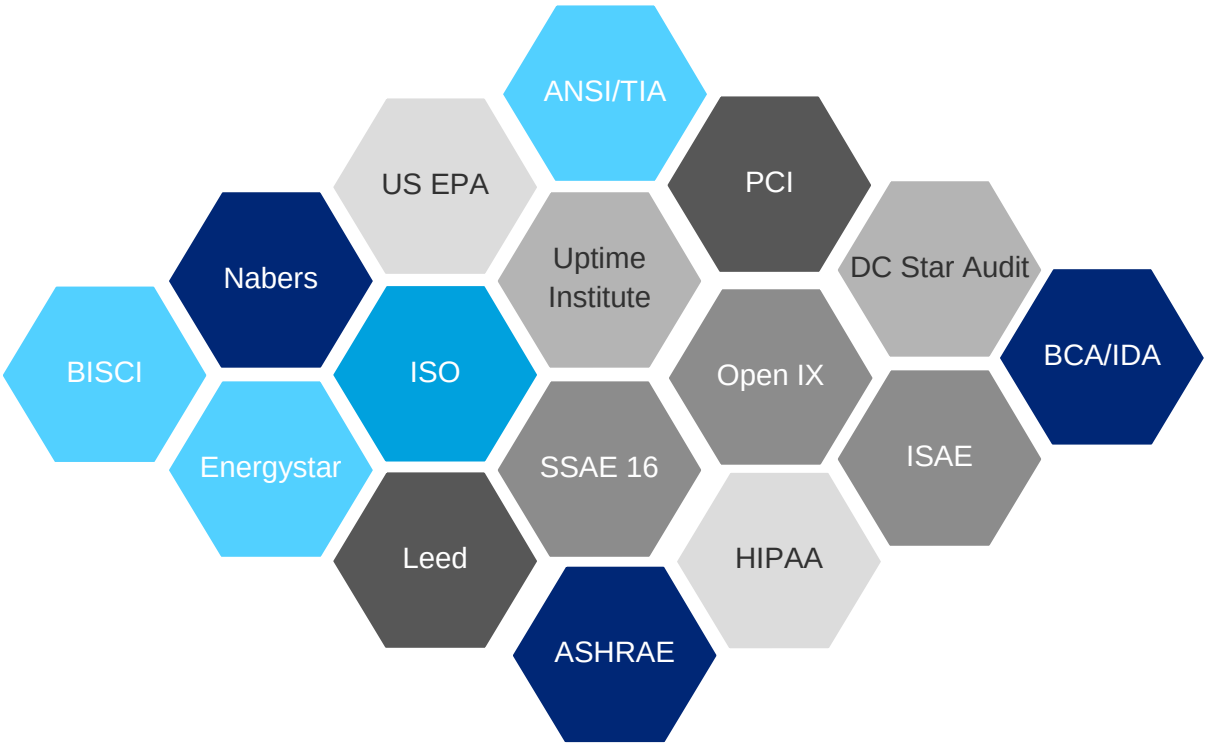


Fig 1: Various International Standards in the market

These standards have been developed with years of research and experience across fixed set of areas. For example, TIA has TIA-942 Telecommunications Infrastructure Standards for Data Centers, the first standard to specifically address data center infrastructure. Intended for use by data center designers early in the building development process, and covers the following:

> Site space and layout; > Cabling infrastructure > Tiered reliability > Environmental considerations.

These standards use international best practices and offer great results, compliance and certifications in many cases which are often treated as gold standards by various agencies and companies.

However, various companies and agencies do not prescribe to such standards alone as usually meeting the stringent guidelines come at a significant cost which to many organisations do not seem to be worthwhile proposition. A lot of technology or service provider companies also develop compliance to these standards hence as a result, if agencies follow a particular standard, it may mean that they would get restricted to utilising the services of select few companies thus not able to make specific choices. Which is why, various agencies practice their own standards and publish their own standard guidelines to the providers to enable an ecosystem of growth, revolution as well as best cost. However, many government agencies follow best practices approach and the standard fulfilment for few select areas while publish their own guidelines at their discretion on what works right for them.

3. Importance/Relevance of data center standards

Efficient data centers	Data centers has been in the market for more than 20 years now and the overall dynamics of data center industry has changed a lot since then. In the last decade, data center has become huge, complex and challenging to operate. The cost of data center downtime has increased significantly for companies in the last couple of years. The study of US data centers quantifies the average cost of an unplanned data center outage at slightly more than US$7,900 per minute and this is a 41% increase from the $5,600 it was in 2010. Data center cannot afford downtime or inefficiency, as it leads to increased cost and unhappy customers. Data center operators in the last couple of year have improved the availability and efficiency of data centers by adopting globally recognized data center standards.
Comparative analysis	Data center standards play an important role when it comes down to help choose which data center service to use. Data center customers rely on standards as a method of performing comparative analysis on competing suppliers. By providing a common method of comparison, standards help insulate customers from the need to make their decisions on solely on the basis of the claims of a provider. A prime example is found with the Tier system originally developed by the Uptime Institute. Comprised of four escalating Tiers that prescribed the physical componentry required to deliver specific levels of reliability the system became recognized as the de facto standard for reliable data center design.
Cost savings	As the data centers are becoming complex, rising energy costs are increasing the operating costs of running a data center. Data Centres consume an immense amount of power to perform functions reliably and effectively. The electrical costs in data centres typically accounts for 40-60% of the total operating costs. Improving energy efficiency of a data centre is extremely beneficial as it reduces the costs of operation of data center. Data center operators can use below mentioned three methods to reduce costs 1. Using industry recognised industry recognized internal design standards for data center components, so they consume less power in doing their job. This helps in reducing overall cost. 2. Follow the industry standards for matching the sizing of data center components more closely to the actual IT load so that the components operate at a higher efficiency. This eventually would lead to cost savings. 3. Adopt industry standards recognized technologies to reduce the need for electric power to supply data center support functions. This would also help in reducing the overall costs. All the three methods are using data center industry standards as a mean of reducing overall costs.

Environmental Impact	According to the Natural Resources Defence Council (NRDC), in US data centers in total used 91 billion kilowatt-hours (kWh) of electrical energy in 2013, and they will use 139 billion kWh by 2020. Data centers consume up to 3 percent of all global electricity production while producing 200 million metric tons of carbon dioxide. The data centers are producing huge impact on environment and lot of environmental groups are putting pressure on data center operators to use green data center practises to reduce environmental impact of the data centers. By adopting the data center industry best practises, the companies are able to reduce the impact on the environmental. Below are some of the steps that can be taken to reduce the impact on environment. 1. Use of renewable energy: This is one of the most important steps towards reducing the environmental impact of data centers. By using renewable energy companies are able to reduce their carbon foot print, which would lower the impact on the environment. 2. Use of efficient data centers: Another best way to reduce data centres' impact on the environment is to make them more efficient by implementing best practices in their design and operations.

4. Data Center Standards current situation in Thailand

Standards adoption is at nascent stage in Thailand data center market and adoption is quite low compared to other south Asian economies. There are very few government data centers that have complied with international standards concerning quality of service. In Thailand, EGA and PTT public company are the only players that have data center certified from uptime institute. Economies like Indonesia have large number of uptime certified data centers and in comparison Thailand number is quite small. With respect to TIA, not a single data center has got the certification from the respective governing body. The situation is expected to change in coming years, as the expectations of data center customers are expected to increase in coming years and demand for highly available data center would be a necessity.

Data Center standards challenges in Thailand

Standards are expensive to adopt
One of the biggest challenges faced by the data center operators is that the standards are expensive to adopt. The standards offer guidelines for operating and maintaining the data center efficiently. Uptime institute has developed tier system for data center availability and has defined the down time for each of tiers. Tier 1 is bare minimum and tier 4 is the best with respect to Uptime. To reach tier 4 certification data center operators need to have 2N+2 data center redundancy, which means data center need to have double power and mechanical components and also add two more to that. Power and cooling standards prescribe to install best in class power and cooling equipment, which increases the efficiency of the data center. To make data center physically safe, data center operators need to install high end cameras, wedge barriers, layered access control etc. Installing and maintain all these equipment increases the cost exponentially for data center operators. The adoption of standards is quite high in emerging economies, as these economies has low purchasing power capacity and most of the data center operators in the region are quite hesitant about heavy capital expenditure.

Long List of data center standards to choose from

Over the years, the number of standards for data centers have increased at very fast pace globally. It is challenging for data center operators to choose between which standards to use and which not to use. Data center standard has been developed for different components of the data center and has also been developed for the specific output of data centers. Uptime and TIA have been developed for availability, ASHARE and NABERS have been developed for power and cooling, PTDCI and HIPPA for data center security related standards, LEED and BISCI for data center design standards, ISO for operational standards, SSAE and ISAE for auditing the data center standards. Choosing the rights standards is very important for data center operators due to the below mentioned reasons:

a. Every data center has unique needs and it is not essential for the data center to adopt best in class standards. The data center operator might not be hosting the very critical information and can follow some essential standards and left out some non-essential standards.

b. Data center operator might be hosting banking data and there are specific data center security certifications that need to obtain before hosting any banking data. The security certification provides the guidelines that need to be followed to make the data center more secure.

Lack of people with complete understanding of standards

As the list of standards is quite long, there is lack of people with skills that have complete understanding of data center standards. There is a long list of standards that are available for data center operators to adopt, but there are few people available that have the skill set to understand all the standards available. There are people available that have knowledge of particular standard, but do not have the knowledge about other standards. This is a huge challenge, as data center operators do not adopt multiple standards and not knowing which one they should adopt is a big disadvantage. This kind of situation is more prevalent in emerging economies, as there is huge shortage of skilled people in the general workforce.

Budget is big issue for standards adoption

This challenge is quite specific to the data center operators in government sector. Most of the government agencies have fixed budges and these budgets are not much flexible to cover the standards expenses. Many agencies have the intent to adopt the data center standards, but due to budget woes, they are not able to move forward. This relevance of this challenge is expected to go down as the government is going to modernize the agency data centers and more emphasis would be put on the efficiency and environmental effects of data centers.

Data center operators are not experienced enough

Data center operators are not mature enough to understand value behind the adoption of data center standards. Most of the data center operators in Thailand are still in their early stages of the development and adopting industry best practises is not their priority for them. One more thing that is hindering the development of standards is that data center operators are not able to clearly see the ROI behind the investment, an issues which is related to the how mature the market is. This trend can be seen in government as well in private sector. Government sector has shown some maturity in terms of understanding of data centers standards, but due lot of bureaucratic hurdles things don't move further than that.

Lack of understanding at a bureaucratic level on the importance of adopting standards

This challenge is again quite specific to the government and its agencies. In most of the government offices, the approval process for purchasing any service or product is time consuming. In case of standards, there are large numbers of steps that need to be followed to completely adopt the standards, and it is challenging and time consuming to make budget committee members understand the value and importance of standards. Another issue that has creates a hurdle for the standard adoption is that everything has to be approved at ministry level. If there is no policy at the ministry level, which says that standards should be adopted, it would be quite difficult for the individual agency to convince ministry to approve budgets for standards adoption. The best scenario in this case would be if the ministry mandates the adoption of standards in every agency under its jurisdiction.

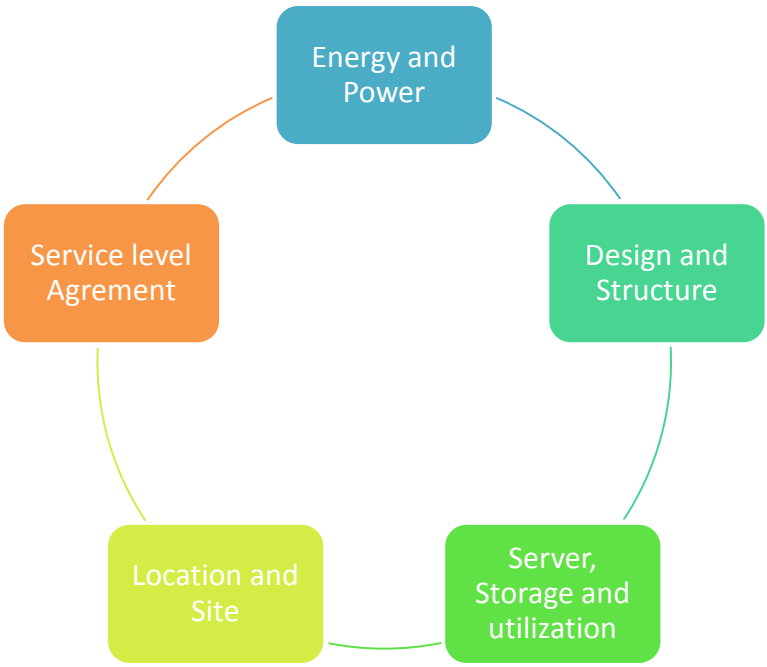
Lack of people who have full understanding of various standards and their implications

Once the data center standards are adopted, another challenge that comes into place is maintaining the standards. There is lack of people who have full understanding of standards and how to maintain the data center standards. Adoption of standards is one thing, but confronting to standards is all together new challenge. As the company or any government agency does not adopt any single standard, it is challenging to find people that have understanding of how to adhere to all the standards that has been adopted. Even if the company or agency finds such people with the required skill set, they are extremely expensive to hire and retain.

Many data center operators are still using legacy infrastructure

Most the data center operators in Thailand are running their data center on legacy infrastructure and legacy buildings. This issue can be seen more prevalent in government agencies than in enterprise sector, as most of the government data centers are situated in large government buildings. To adhere to data center standards, the agency has to remove old IT infrastructure and put in the new infrastructure, which would be very capital intensive for government agency. The legacy buildings structure is a challenge, as these building don't have any space for new equipment which is required if they follow any standards. A data center standard also dictates that data center should be located in place where it can be easily accessible, but it is a challenge for government agencies as it would be highly capital intensive to move the data center to new location.

5. Data Center Standards by Functional Areas



1. Energy and Power

Energy is one of the most important components in data centers. Data Centers consume an immense amount of power to perform functions reliably and effectively. The electrical costs in Data Centers typically accounts for 40-60% of the total operating costs.

Improving energy efficiency of a Data Center is extremely beneficial - it reduces the costs of operation and at the same time, lowers the environmental impact of the facility.

Meters: Meters provide data that offers insight into the operation of the data center infrastructure (i.e. power and cooling systems) within a data center. Specific types of meters exist for various reasons, from tracking the use of electricity to analysing the power quality in a facility and reporting problems such as transients and harmonics. Within a data center, meters would be in place that measure power (kW), energy (kWh), voltage & amperage, harmonics, power factor, flow rates, temperature & humidity, and more.

PUE: PUE is the ratio of energy coming into the data center, compared to how much power is actually consumed by IT equipment like servers. This measurement is expressed by a ratio, making 1.0 an ideal, yet almost impossible standard to achieve. The power usage effectiveness (PUE) rating has become the de facto standard measurement of efficiency in the data center industry.

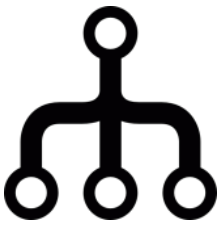
Redundancy: By redundancy we mean the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe. In data centers, the need for redundancy focuses on how much extra or spare power the data center can offer its customers as a back-up during a power outage. Unexpected power outages are the overwhelming usual cause for data center downtime.

Lighting: Lighting is important part of the data center that has often been ignored by the data center operators. An industry standard recommends using LED fixtures in data centers for three reasons: they consume less electricity, they generate less heat and they are nearly 100% dimmable. Sensor based lighting is also used in data center to reduce the energy costs.

UPS: Data center operators, when faced with the likelihood of downtime, and data processing errors caused by utility power, implement an uninterruptible power supply (UPS) system between the public power distribution system and their mission critical loads. The UPS system design configuration chosen for the application directly impacts the availability of the critical equipment it supports.

Cooling: Data center cooling or heat removal is one of the most essential yet least understood of all critical IT environment processes. As the latest computing equipment becomes smaller and uses the same or even more electricity than the equipment it replaced, more heat is being generated in data centers. Using the latest cooling technologies help the data center operator to reduce the cooling in data center and at the same time increase its efficiency.

2. Design and Structure



The data center infrastructure is central to the IT architecture, from which all content is sourced or passes through. Proper planning of the data center infrastructure design is critical, and performance, resiliency, and scalability need to be carefully considered. Another important aspect of the data center design is flexibility in quickly deploying and supporting new services. Designing a flexible architecture that has the ability to support new applications in a short time frame can result in a significant competitive advantage.

Cabling: In data center, the various entities make up the system work to together to protect and to manage both current and future equipment's and the thousands of connections exists between servers and switches and the outlying areas of the network. All of these entities are interrelated and connected by the cabling system, which designers and end-users are striving to design for better scalability, flexibility, manageability, availability and lower total cost of ownership

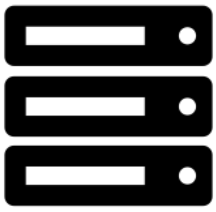
Physical Security: Data center has various physical threats and physical threats to IT equipment include such things as power and cooling problems, human error or malice, fire, leaks, and air quality. The data center operators need to protect the data center by installing proper lighting, installing normal CCTV and thermal cameras, wedge barriers at the data center gates and sensors around the data center perimeter. Extra security should be provided to the server room.

Building Design: The data center buildings are designed in a very specific manner and it is very essential that specific design is being followed to follow industry standards. One of the important features of the building the data center is to design it into zone. The zonal architecture helps in the overall data center security. For building design most of the data centers follow BISCI and TIA. TIA is much more popular among data center players. Many data center players use LEED industry standard for architectural design of data centers

Monitoring: Monitoring plays a very important role in today's complex data center environment. It helps the data center operators to monitor different components of data center through GUI interface. Initially data center operators were using simple building management systems for data centers and eventually they installed advanced building management systems. In today's complex environment the data center operators are using DCIM tools to monitor the data center.

Fire detection: A comprehensive fire detection and suppression system is required to ensure that life and property are protected. Fire and life safety protection systems (e.g., fire alarms, heat/smoke detectors, carbon monoxide detection, automated fire suppression, extinguishers, and emergency exit routes) should be professionally designed, installed and maintained. In a security zone or high security zone with a raised floor, heat and smoke detection devices must be installed both above and below the floor surface.

3. Server, Storage and utilization



The data centers are equipped to host / co-locate systems (e.g. Web Servers, Application Servers, Database Servers, SAN, and NAS etc.) to host applications at the data center to use the centralized computing power. Data centers have high availability, centralized authenticating system to authenticate the users to access their respective systems depending on the authentication matrix. The entire infrastructure in the data center would require monitoring tools and security tools for efficient operation.

Utilization and Virtualization: The utilization rate is defined as the overall extent to which data center different components are being used and is usually recorded as a percentage total input. The utilization rates can be calculated for server, network and storage. Understanding the utilization rates help the data center operators to understand the capacity utilization and plan for the future in case the utilization is quite high. Virtualization means the breaking the physical server in small servers and increased virtualization indicates better efficiency.

Monitoring: Monitoring tools effectively manage the computing environment of the, including various applications running in there. A typical data center would include network & security elements, servers, databases, applications etc. Many management software tools would help the data centers to establish and sustain an optimized, on-demand infrastructure, by continuously assessing and self-managing the systems, applications and databases.

Helpdesk: Helpdesk for data center provide seamless integration to log incident automatically via system and network management. It also allows detailed multiple levels/ tiers of categorization on the type of incident being logged. Helpdesk can provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels. Helpdesk must be able to log and escalate user interactions and requests.

Backup: Data center backup is extremely important, as it helps to recover the critical data in case of any major incident. The backup solution should be available for all the available operating systems and should also be capable SAN and NAS based backups. The backup solution would have a GUI platform to ensure smooth administration. The proposed backup solution should be able to write from multiple data streams.

Security: Data center security is very important for data center vendors and most of the vendor use advanced level of security measure to protect their IT infrastructure. Most of the vendors use enterprise level firewall, antivirus and vulnerability scans to protect their data centers. Transmission of data securely is also important for data center operators. Data center use advanced encryption technologies to transfer their data from one data center to another.

4. Location and Site

Determining the location of a data center is one of the crucial decisions for a company as it is based on strategy and goals of a company or government. Site selection plays an important role for the same as it will have direct impact on cost and TCO. There are many factors which affect site selection. All these factors should be looked from strategic perspective as nowadays an industry changes its focus and business direction in 5 to 7 years.

Location and Site: Data center should be easily accessible from multiple highways and should also have the option to expand in case of increased demand. Data center should location is readily accessible to authorized employees and fire and also emergency services are able to respond quickly to incidents. Easy access to electrical power is available from diverse sources and future expansion is possible if increased capacity is required for the data centers.

5. Service level Agreement

End-to-end service availability of the data center and its independent monitoring is the prime requirement to have reliable, seamless, smooth delivery of the services to the citizens. It is, therefore, necessary that appropriate Service Level Agreements (SLAs) be worked out between government and the Implementing Agency and that an independent Agency would be appointed to monitor the performance with reference to the SLA and related aspects

Disaster recovery: Disaster recovery focuses on the information or technology systems that support business functions. It is a subset of business continuity, which involves planning to keep all aspects of a business functioning in the midst of disruptive events. From a digital government perspective, controls and protections can be broadly grouped under the term Disaster Recovery (DR). Data center operators can have a single DR site or multiple DR sites.

Tier: Tier 1 to 4 data center is nothing but a standardized methodology used to define uptime of data center. Tier 4 data center considered as most robust and less prone to failures. Tier 4 is designed to host mission critical servers and computer systems, with fully redundant subsystems (cooling, power, network links, storage etc.) and compartmentalized security zones controlled by biometric access controls methods. Naturally, the simplest is a Tier 1 data center used by small business or shops.

6. Refined Maturity Model for Data centers

Data Center Level explanations

1	Level 1 Definition: Data center that are following level one standard, would be the data centers that can provide very basic form of service. Processes are usually ad hoc and the organization usually does not provide a stable environment. In spite of this ad hoc and chaotic environment, maturity level 1 organizations are able to provide services effectively.
2	Level 2 Definition: Data center that are following level two standards would realize that data center infrastructure and operations are critical to the business. The data center would start taking actions with respect to equipment, processes and people to further gain operational control and visibility.
3	Level 3 Definition: At level three maturity data centers wold be gaining efficiencies and service quality through standardization, policy development, governance, and implementing proactive/cross-departmental processes. This could help the data center become more standardized and work towards becoming more efficient.
4	Level 4 Definition: At level four maturity data centers wold be managing data center like any other business. The data center operator would adopt standards that would help to make the data center more customers focused in the long run. More sophisticated technologies become part of the data center, as data center tries to achieve higher efficiencies.
5	Level 5 Definition: At level five maturity data centers would be adopting standards that would help data centers to become nimble, adaptable and innovative. The organization's ability to rapidly respond to changes and opportunities is enhanced through adoption of best in class standards.

We have developed the five maturity levels for standards for government agencies. We have already identified the current level of readiness for standards among different government agencies. The below table defines the minimum level of standard that each of the four type of data centers should follow. If an agency feels that due to sensitive of data that it handles, it should be at higher level then should definitely move to upper levels.

Parameter	Sub Parameter's	Level 1	Level 2	Level 3	Level 4	Level 5
Energy & Power	Energy consumption	No Meters installed	Building level metres installed	Switch board metering installed	Circuit Level metering installed	End User level metering installed
	Power usage effectiveness	PUE not measured	Started measuring PUE. Total annualized kWh consumption. Measured at output Ideal PUE 2-2.5	Started measuring PUE. Total annualized kWh consumption. Measured at output 1.6-1.99	PUE measured, Total annualized kWh consumption. Measured at output Ideal PUE 1.4-1.59	PUE measured, Total annualized kWh consumption. Measured at output Ideal PUE <1.39
	Redundancy	Our components are not redundant (N)	We have one redundancy component (N+1)	We have redundancy component plus two more components (N+2)	We have double redundancy components(2N)	We have double redundancy components(2N+1)
	Lighting	We are using only fluorescent lights	Optimize lighting - Use of more efficient fluorescent lights	Use LED lights in all parts of DC	Using intelligent lighting system in data center	Daylighting and/or light pipes/tubes used to augment and reduce dependency on electrical lighting systems
	UPS	We do not use UPS for power interruptions and rely only on generator UPS System efficiency- not measured	We use a standby/of fine UPS for power interruptions UPS System efficiency measured- 50%-60%	We use a line interactive UPS System efficiency- measured- 61%-80%	We use a double conversion UPS System efficiency - 81%-90%	Efficient UPS - Use of double conversion eco mode UPS System efficiency - >90%
	Cooling	We use air cooled self-contained system and do not measure cooling output	We using chilled water system for cooling and Cooling System Efficiency- >1.5 kw/ton	We are using DX systems in data centers and do not measure cooling metrics Cooling System Efficiency- 1 kw/ton 1.49 kw/ton	We use direct fresh air evaporative cooling system and start tracking cooling metrics Cooling System Efficiency- .99kw/ton .5 kw/ton	We use indirect free air evaporative cooling system and keep an target for cooling metrics Cooling System Efficiency- <.5 kw/ton
Design & Structure	Colour Coding & Naming	We do not use any color coding or naming in DC	We use color coding and naming in server room only	We use color coding and naming convention using TIA standard guidelines in all parts of data center	We use color coding and naming convention for the whole DC using TIA standard guideline in all data centers in an area	We use color coding and naming convention using TIA standards in multiple data center sites in different parts of the country
	Security Assessment	Basic security with simple CCTV	Biometric access, CCTV on infra, lighting on perimeter	Sensor for perimeter, high resolution cameras	Wedge barrier, access control attached with CCTV in grey spaces	Thermal cameras in server room, Threat assessment conducted

	Building design	Building don't have zones, building designed not per any standards	Data center has been divided into different zones	Data center has been designed using basic level standards of TIA or BISCI or both	Data center would follow complete guide lines of TIA or BISCI or both.	Data center has been designed as per LEED standard
	Monitoring	No automated or centralized monitoring system for mechanical, electrical, and facility systems.	Use of Building Management system. Use IP-enabled meters that supply data to a building management system	Automated and centralized monitoring system inclusive of key critical mechanical, electrical, and facility systems	Automated and centralized monitoring system inclusive of key critical mechanical, electrical, facility, and key IT systems	Automated and centralized monitoring system inclusive of key critical mechanical, electrical, facility and key IT systems. Analytical and real-time data management capability such as integrated dashboards, and DCIM solutions.
Server, Storage and Utilization	Utilization & Virtualization	Utilization not measured	Tracking average monthly and peak utilization across the data center Storage 40%-60% utilization Network utilization greater than 40% in the data center Virtualized 10%-30%	Average monthly CPU utilization is greater than 20% in the data center Storage 61%-70% utilization Network utilization greater than 60% in the data center Virtualized 31%-50%	Average monthly CPU utilization is greater than 35% in the data center Storage 71%-90% utilization Network utilization greater than 70% in the data center Virtualized 51%-80%	Average monthly CPU utilization is greater than 50% in the data center Storage 91% + utilization Network utilization greater than 80% in the data center Virtualized >81%
	Monitoring IT infrastructure and software	We do not monitor IT infrastructure in our data center	We plan to use server and database monitoring tools	We plan to use web server monitoring tools in data center	Monitoring tool to be integrated with enterprise management system	Reporting from monitoring tools would enhance service efficiency
	Help desk	We do not have any helpdesk	We use helpdesk for data center that requires minimal support 8 hours operations 5 days a week	We use helpdesk that requires 24 hours support 5 days a week with L1 support facility	We use helpdesk that requires 24hr support; 7 days a week with L1 and L2 support	We use helpdesk that requires 24 hr. support, 7 days a week with L1, L2, L3 support
	Backup	No backup solution available	Back up their data and send these backups to an off-site storage facility	Weekly backup their data and send it to offsite storage facility	Daily backup their data and send it to offsite storage facility	Mission critical data is electronically vaulted

	Security for IT infrastructure and data	We do not use any network security and encryption technologies	We use basic firewalls that have high latency and low traffic handling capacity. We also use simple encryption technologies	We use enterprise firewall with high performance and concurrent connection capability. We use simple encryption technologies	We use enterprise firewall with high performance and concurrent connections capability. Encryption technologies are SLL or better	We use next generation firewalls that can secure discrete application layer transactions and includes intrusion prevention and application layer gateway. Use advanced Encryption technologies.
Location & Site	Accessible and expansion	Data center is not easily accessible and expansion not possible	Move data center to a more accessible location in the same area	Data center to be located at new location where it can be accessed from multiple roadways	Data center is expandable in single phase	Data center can be expanded in multiple phases
	Power and network availability	Data center has only 1 source for power and network.	Data center has single sources for power and two sources for network.	Data center two sources for power and 2 sources for network	Data center must use alternative energy sources for power in data centers and 2 sources for network	Data center must set a target for the usage renewable energy for power and 2 sources for network
SLA	Disaster recovery	Data center does not have any disaster recovery plan	Data center has start using shared DR site for recovery	Has developed a DR plan and are using multiple shared DR sites.	Has developed the DR plan and implemented the DR plan with single Disaster recovery site.	Has developed the DR plan and implemented the DR plan with multiple disaster recovery sites.
	Tier and Response time	Data center does not have any measure downtime/uptime.	Data center is tiered and have a downtime of >29 hrs./year but less than 50 hrs./yr.	Data center is tiered and has a downtime of 15-29 hrs./year	Data center is tired and has a downtime of 2 to 15 hrs.	Data center is tired and has a downtime of <2 hours/year

7. Benefit Realization –Standards

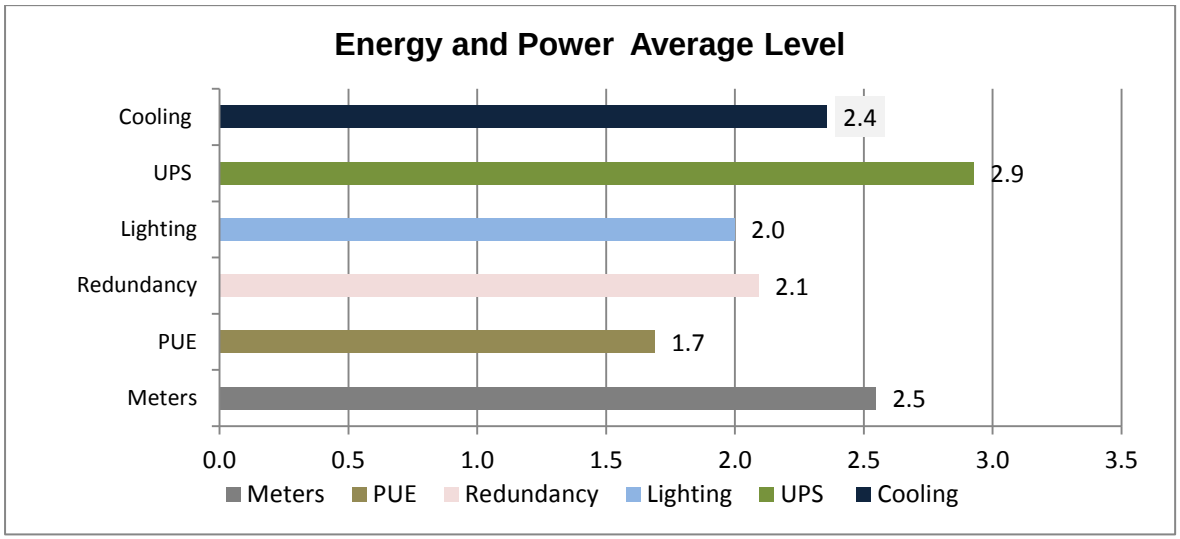
Improved Energy Measurement Capabilities	Adopting standards would help the data center in improving energy measurement capabilities. As the data center would install modern meters in their data centers, they would be able to measure the energy consumed accurately. This would enable data centers to measure energy consumed over a period of time and identify components that consume most of the energy.
Achieving high levels of PUE	PUE is industry defined metric to measure the usage of all the power equipment's in the data center. To achieve higher PUE levels data center would have to concentrate on using its equipment's efficiently. As the data center would achieve higher PUE, efficiency levels would also increase and that would ultimately lead to cost savings.
Better Redundancy	Redundancy plays an important role in case of any failure of any mechanical equipment. Moving to higher levels would make the data centers resistant to any equipment failure, as it would have spare for each of the equipment's. This would help data center to continue providing services, in case of any large equipment failure.
Optimized lighting	Data centers are usually using fluorescent lights, which are not efficient at all and consume lot of energy. LED lights consume less energy and can run for much longer time, compared to fluorescent lights. Intelligent lighting system would help the data center to reduce energy costs, as lights would be used only when needed. This would help the data centers to reduce energy costs.
Efficient UPS	Data centers are using UPS systems which are okay for some data centers, but as the usability of data centers would increase, need for more efficient data center is required. Efficient UPS would help in reducing the time to move to UPS power, in case of any failure. This plays an important role, when we are using data centers that are require to have high availability all the time.

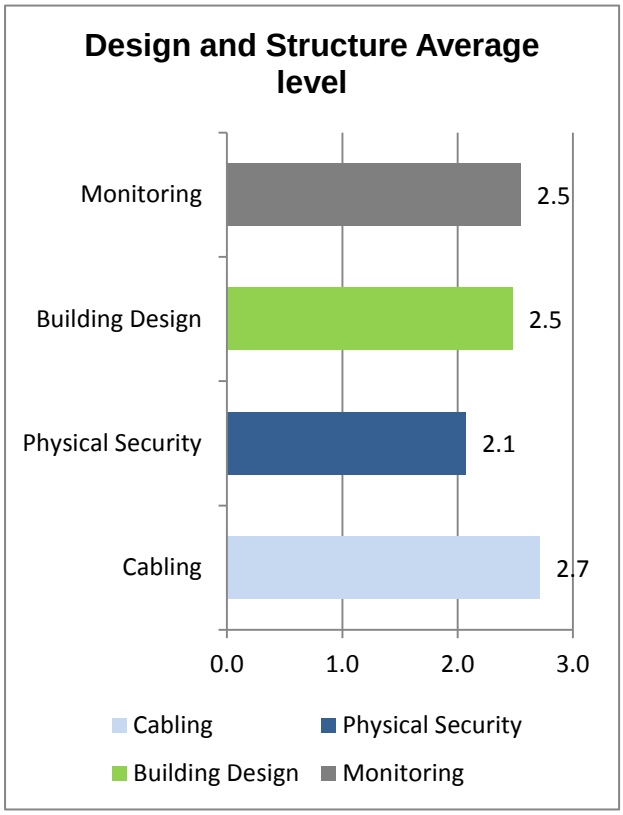
Better Cooling Systems	Cooling is an important component of data center and it consumes large amount of energy. Data center need to use cooling systems that are appropriate for it to work properly. Improved cooling systems would not be completely dependent on power to provide cooling, but would use outside air to provide cooling to data center. This would help in reducing the costs and improving the efficiency of data center.
Colour Coding and naming	Colour coding and naming would not help data center in saving any costs directly, but would provide the ability to resolve issues quickly. Using colour coding and naming would help the data centers to locate any problem in any data center quickly. This would help in improving the efficiency of data centers.
Improved Physical Security and better design	Data Centers keeps lot of sensitive information and having good physical security is important. This would also help the data centers to detect any physical threat before it can cause any damage. Better design would help the data center to improve its security by dividing its data center into different zones.
Physical and IT Infrastructure monitoring	Monitoring systems for the building would help in monitoring all the mechanical and IT equipment. This would help understanding the usage and health of equipment in the data center. Modern tools would help in asset identification and future capacity estimation. IT monitoring tool would help in the keeping a check on servers, data bases and web servers. This would also help in detecting any issue early on, thus resulting in preventing large failure
Better Utilization and Virtualization levels	Measuring Utilizing for IT components are important as it helps the data center operates to know how efficiently server, storage and network are being used. More utilization would provide good ROI for the capex spend. Improved virtualization levels would provide ideas of how many severs are being virtualized, as low virtualization would mean low efficiency.
Helpdesk with better advanced capabilities	Most of the data centers do not have capability to handle technical problems related to data centers operations. Establishing Help desk with advanced capabilities would help data center to resolve many issues quickly and also help in saving costs, as most of the trouble shooting would be done internally.

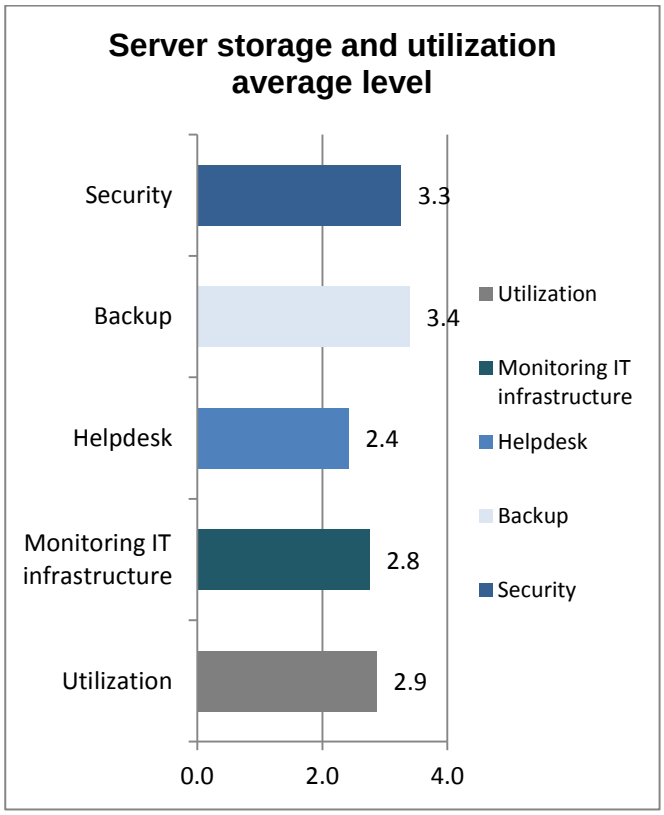
Improved backup capabilities	Backup is one of the important elements for any agency. Instead of taking backups on ad-hoc basis, if taking regularly would help in retrieving information in case of any technical issue. Weekly and daily backups are essential, as there is lot of sensitive information being kept in centralized data centers.
Security of IT infrastructure	This is one of the most important standards for data centers in the region. Data security breaches are quite widespread and the costs related to that are humongous. Having best in class of security for IT infrastructure would help the data centers avoid any unwanted intrusions, which would help them save lot of costs in the long run.
More accessible and expandable	Accessibility is important for a data center, as in case of any disaster it would be important for emergency services to reach there on time to save the infrastructure that is present in data center. As the demand for data centers would increase, it would be necessary for data center operators to plan for expansion initially, as this would help in reducing overall future costs.
Multiple sources of power	Having multiple sources of power and network would help the data centers in switching to alternative sources in case of any emergency. This would help in reducing the downtime and thus saving lot of costs for data centers.
Disaster recovery sites	Having disaster recovery site and well defined plan is important for data center operators. In case of any event which is leads to closing all the services in the data center, disaster recovery sites would help in running the data center services for its customers. This disaster recovery plays an important role in business continuity for data centers.
Tier and response time	Tier corresponds to the downtime that any particular type of data center is having. Lesser the downtime and response time, more would be availability of service for its customers, which would lead more satisfied customers.

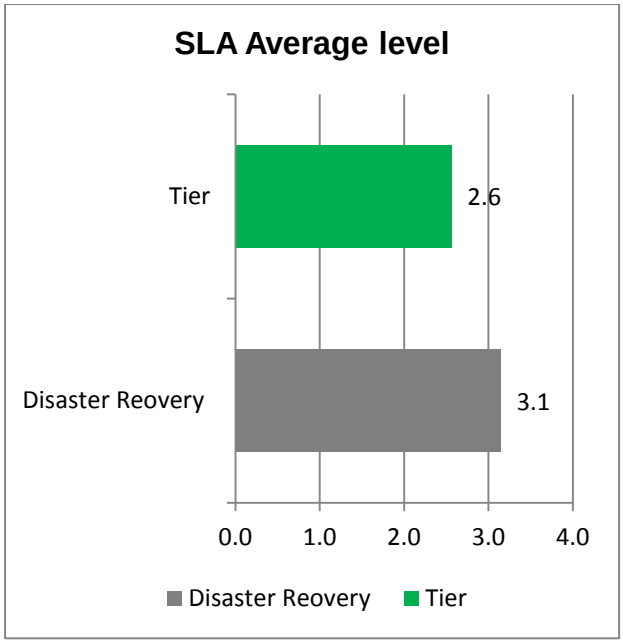
8. Current State of Agency data center in Thailand

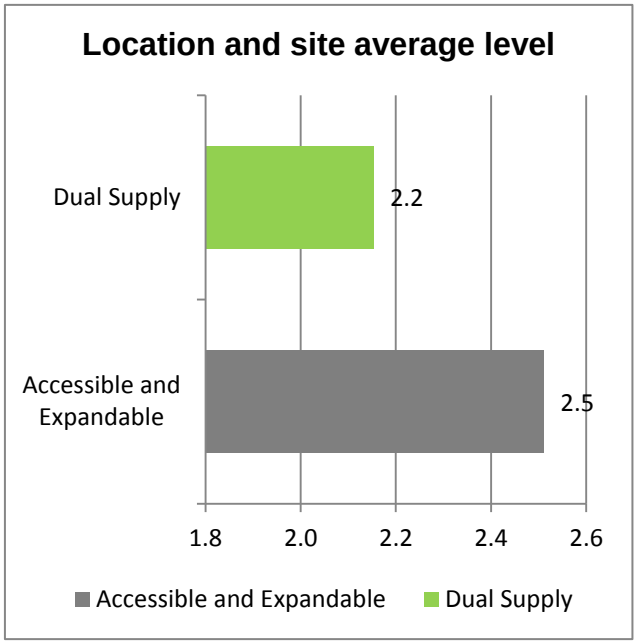
The focus group discussion was conducted in the March 2017 and people from government agencies attended the event. Questionnaires were designed to get answers for questions related to strategy and standards. The standards questions were divided into five levels and in below mentioned bar charts and average of responses has been taken for analysis purpose.








SLA Average level
Tier
2.6
Disaster Reovery
3.1
0.0
1.0
2.0
3.0
4.0
Disaster Reovery
Tier


Location and site average level
Dual Supply
2.2
Accessible and Expandable
2.5
1.8
2.0
2.2
2.4
2.6
Accessible and Expandable
Dual Supply

9. Frost & Sullivan Analysis of Future State for Standards for Data Centers

(Levels) Five Four Three Two One	Frost & Sullivan Future Recommended Level			
Standards	Our Analysis Agency DC Level	Our Analysis Ministry DC Level	Our Analysis Cross DC Level	Our Analysis G services Level
Energy consumption				
Power usage effectiveness				
Redundancy				
Lighting				
UPS				
Cooling				
Color Coding				
Security Assessment				
Building design				
Monitoring				
Utilization & Virtualization				
Monitoring IT infrastructure and software				
Help desk				
Backup				
Security for IT infrastructure and data				
Accessible and expansion				
Power and network availability				
Disaster recovery				
Tier and Response time				

The above diagram gives us an overview of the levels for the four data center models from our analysis. We have five primary areas for the standards namely energy and power, design and structure, server storage and utilization, location and site and finally SLA's. We had developed nineteen parameters form five main parameter from our analysis. The nineteen parameters are considered to be most important and the same nineteen sub parameters were also use in the focus group discussion. The levels for some of the sub parameters for four models would be same as what we have got in focus group discussion and for some the levels would be different. We will discuss the five main areas of standards, their sub parameters and what are the reasons behind our analysis for keeping them on different or same levels when compared to results that we got from the FGD.

10. Service Level Agreements- Colocation

Service level Agreement Definition	This Service Level Agreement ("SLA") defines the performance parameters and quality level of the Colocation Services provided by Vendor to the Agency (Government) under the Agreement. This document clarifies both Parties' responsibilities and procedures to ensure the Agency needs are met in a timely manner. This SLA and the Agreement shall be interpreted and applied together as a single instrument. In the event of any inconsistency between the SLA and the Agreement, the provisions of the Agreement shall prevail.

Service Description

Power	All electrical circuits would order with one (1) primary and one (1) redundant circuit for failover per cabinet. Aggregate draw may not exceed the thresholds defined herein. If Agency's actual power requirement exceeds the listed threshold, Agency may consider procurement of additional contiguous space to accommodate power consumption and heat dissipation.
Network	The network equipment would connect co-located servers to the outside network, providing seamless bandwidth and Internet connectivity. Network connectivity is provided from A and B sources to every server for redundancy. Top of rack switches will be connected via A and B sides. The redundant network connection allows properly configured servers to retain network connectivity during most regularly scheduled maintenance and unplanned events. Maintenance will be performed on only one side of the network at a time when possible.
Cooling	Conditioned Space Computer Room Air Conditioning ("CRAC") units are strategically placed in each Data Center to ensure that the appropriate ambient temperature and humidity thresholds are met.
Fire Detection	Data Centers are equipped with both water-based and non-water-based fire suppression systems, depending on location and local fire codes. In addition to these fire suppression systems, hand-held fire extinguishers are also placed strategically throughout the Data Center. Fire suppression systems are tested annually to ensure functionality.

Service Reporting	Service Reporting Service availability, usage and capacity reports, if applicable, are generated on a monthly basis using various Monitoring and Management tools. Service availability, usage and capacity reports are available to Agency upon request.
Physical Security	Facility Access and Physical Security includes controlled access and egress doors; controlled access permissions and access request methods; and managed key, access card and/or biometric systems for access control. CCTV/IP Video is used to monitor access, egress and infrastructure. Data center vendor reserves the right to access (or to allow third parties to access) any part of the Data Center or facility at any time for safety and security reasons, including Agency cage space or Agency cabinets.
Racks	Agencies can opt for lockable cabinet rack space. Cabinets are four-post racks with combination lockable doors and side panels. Agency authorized contacts will have a unique PIN to access their rack space. Full Rack – dedicated 42U rack Half Rack - dedicated 21U rack Third of a Rack – dedicated 14U rack"
Floor Space	For Agency's that require floor space without a rack (i.e., full rack SAN, etc.), Data center vendor offers leased floor space options based on the total square feet required.
Caged Space	Caged space is an option available to Agency's who are managing the Agency equipment installed at a Data Center in whole or in part. Caged space is comprised of a mesh wall around Agency's racks/cabinets with dedicated connectivity infrastructure. This connectivity is built on an Agency-by-Agency basis and no pre-wired cabling is provided
Remote Hands	Remote Hands is provided to Agency's for an additional charge, and it involves the most basic activities of an on-site technician performing as the "eyes, ears, and fingers" on the Agency's behalf.

Service Level Metrics

Power SLA	Service Availability goal for power in the data centers is 99.99%. This equates to 4.32 minutes of downtime monthly based on a 30-day month. Data Center vendor guarantees to keep at least one channel of power in service in order to reach our Service Availability goal for power. Agencies should use both channels of power that are available in the data center for their equipment if possible
Cooling SLA	Data center vendor to provide average temperatures of 65-78 degrees Fahrenheit over a 24 hour period within the cold aisles of the data center. Temperature fluctuations may temporarily occur in the 64-80 degree Fahrenheit range. Data center vendor reserves the right to modify the upper and lower limits in accordance with ASHRAE recommendations for data center operations of equipment.
Network SLA	Data center vendor should provide a 99.999% network uptime guarantee providing uninterrupted transit to the internet. Interrupted transit is defined as 100% packet loss to the internet and data center vendor guarantees Zero packet loss internal to DC's network.

Availability SLA	
Cumulative Service Unavailability	Agency Credit
<60 min	0
>60 min and < 2hours	1
>2 Hours and <3 hours	2
>3 Hours and <4 hours	3
15 hours	15

Response Time	Response Time	Solution
The loss of one or more critical components of a system resulting in a major impact on the Agency's business. The problem would have a high visibility to the Agency and their business operations, with no work around possible.	15 minutes	80% in 4 hours
The loss of one or more critical components of a system resulting in serious degradation of services to Agency's business. Priority 2 incidents are usually characterized by: · The Agency cannot work as normal but a bypass is available · The Agency is not yet experiencing serious disruptions, however, there is a potential to do so if the request is not solved.	1 hour	80% in 1 WD
Minor impact on service delivery. A non-critical part of an application, Operating system or server is affected by the problem. The problem has a moderate visibility to the Agency and a low impact on their business operations. Normal fault calls fall into this category. This is the default priority level assigned to faults. Note: All calls logged by fax or email automatically become Priority 3 or lower.	4 hours	80% in 4 WD
Fault has little or no operational impact. Included in this area are requests for information.	1 NWD	80% in 11 WD

Maintenance

Overall Maintenance	Data center vendor will notify Agency's about both scheduled and unscheduled maintenance. Services may not be available during the maintenance periods.
Infrastructure maintenance	Data Center infrastructure work can require extended outages for all services in the data center. Examples of such work include changes to our electrical, mechanical, network or firewall infrastructure.
Scheduled maintenance	Scheduled Maintenance will mean any maintenance where (a) Agency is notified 72 hours in advance, and (b) that is performed during a standard maintenance window of 10 PM to 6 AM local time. Information regarding Scheduled Maintenance will be provided to Agency's designated point of contact. Data center vendor reserves the right to perform maintenance outside of Scheduled Maintenance during an emergency
Unscheduled maintenance	Unscheduled maintenance tasks that require service downtime will be announced as soon as possible to the Agency
Change notification	Data Center will maintain a mailing list of Agency contacts who will be notified of planned maintenance and unplanned events. Agencies must notify data center vendor of any changes to contact information as part of providing escalation path information. Contact lists will be reviewed periodically.
Climate Control	Maintenance of the data center chilled water and environmental systems. Monitoring and control of climate conditions in all the data centers is required. Responding to climate-related alerts resulting from variations from climate conditions that exceed system thresholds (for example, excessive temperatures, hot spots, etc.).
Fire Detection and Suppression	Early warning detection system Individually zoned, double-interlocked, pre-action fire suppression system. Dry pipe with water suppression in the event of a fire Maintenance of all sensors and alarms Maintenance of the fire suppression system Monitoring of, and response to, all related alerts and alarms Compliance with relevant certification and fire code requirements
Power	Maintenance of the uninterruptible power supply system. Maintenance of the back-up generators and related systems Connection to the electrical source

Agency Responsibilities

Agency Support Agents	Agency agrees to designate Primary and Secondary Agency Support Representatives (CSR). The Primary CSR will serve as the primary liaison with OPS for the delivery and conduct of support services. The Secondary CSR will be fully authorized to assume this role in the absence of the Primary CSR. The CSR facilitates the delivery of support services with OPS by establishing priorities, refining requirements, coordinating scheduling, handling procurements, and disseminating information among appropriate staff. CSR may appoint technical contacts and will provide and maintain as current a list of personnel authorized to access their designated rack space.
Access	Agency will check in with the Operator on duty for access to the secure area where servers are located. Agencies will be issued a specific combination for access to their rack space. OPS will retain a master key that allows access to all rack spaces in order to execute emergency or planned maintenance work that has been coordinated with Agency. An emergency in this case is defined as any unforeseen circumstance that requires immediate action regardless of the impact to services provide on the Agency's servers. The emergency shall be determined to exist by OPS.
Ordering	Agency is responsible for the purchase, license and maintenance costs of all hardware, software, and network components directly associated with their specified SLA. Agency will work through OPS to obtain and install all network cables, KVM connectors and cables. Agency is required to consult with OPS on all hardware and network related procurements to be housed in the Co-location area prior to placing orders to ensure the products and/or services best meet Agency needs and are certified for standard 19" racks and related power, HVAC, etc. requirements.
Licensing Compliance	All software provided by the Agency for use on the Agency's computers/servers shall be properly licensed in sufficient quantities to cover actual usage.
Rack Utilization	Agency agrees to use rack space only for server and related hardware. Agency agrees to consult with OPS prior to placing additional hardware in their rack space and understands that such additions may impact on one or several elements of their SLA. Agency agrees to coordinate with OPS prior to any equipment relocation within the rack space that involves KVM or network connectivity.
Security System	Agency is responsible for the administration and security of their systems and explicitly agrees to adhere to existing security and use policies and procedures. Consistent with policy and practices, Data center vendor reserves the right to disconnect any server from the network that poses a threat or which may be directly tied to the assessment of a perceived threat to the environment because of security exposures or any condition that puts the surrounding area to threat, including potential violations of existing laws or policies.
Systems Management	Agency is responsible for the administration of their servers. As an option, Data Center vendor offers this service under a different service level agreement. While operating system version and patch level is left to the discretion of the Agency, data center vendor reserves the right to disconnect any server from the network that poses a threat to the environment because of back levelled software or patches.

Restore and Backup	Agency is responsible for backups and restores to their servers. As an option, data center vendor can offers this service under a different service level agreement (contact OPS for details).
Equipment Relocation/ Storage	In general, the Agency is responsible for moving, shipping, storing, and delivery of its property. Operation will work with the Agency to facilitate changes, movement and addition of servers and network-related equipment.
Business Continuance	Agency is responsible for development and implementation of their own business continuance plan. OPS will provide information on the ITS Business Continuance Plan upon request, but replacement of equipment and business continuity remains the responsibility of the Agency. If Agency wants to have a hot spare in the rack, it will be treated as just another piece of equipment at no additional charge. However, if it needs KVM or network ports, the Agency will be assessed an additional charge for that service.

Terms

Effective Term	This Service Agreement is in effect beginning XYZ data at 8:00 a.m. through XYZ data at 5:00 p.m., unless renewed or terminated as described below.
Billing	All Service Agreements are due and payable no later than XYZ date. If a signed agreement has not been received by that date, defined services will be discontinued until a signed agreement is received
Termination	One party may terminate this Service Agreement upon the failure of the other party to substantially perform the duties specified in this Agreement. This Service Agreement is terminated 30 days after written notification of this failure, unless the failing party corrects the failure to the satisfaction of the terminating party. On termination, the Agency is only liable for payment for services performed in accordance with the provisions of this Service Agreement prior to the effective date of the termination. Agency will coordinate with OPS for the removal of their equipment. Vendor will process appropriate refunds upon termination.
Amendments	Changes to this Service Agreement can take place when both parties agree in writing.
Renewal	The Agency will be given an opportunity to extend the term of this Service Agreement at least 60 days prior to the expiration date. In the event that either party wishes to re-negotiate any terms or conditions of this Service Agreement, they shall notify the other party of the proposed changes and, if required, a meeting will be held to discuss and agree upon revisions to the Service Agreement.

11. Service Level Agreements- Third party Cloud

Definitions

Agreement	The Cloud Computing services agreement between agency and Vendor, inclusive of all schedules, exhibits, attachments and other documents incorporated by reference
P1 (Priority 1)	The service is unavailable for all users; or an issue prevents payroll or tax processing and/or financials quarter-end or year-end close processing.
P2 (Priority 2)	The service contains a bug that prevents Agency from executing one or more critical business processes with a significant impact and no workaround exists.
P3 (Priority 3)	The service contains a bug that prevents Agency from executing one or more important business processes. A workaround exists but is not optimal
P4 (Priority 4)	The service contains an issue that may disrupt business processes where a workaround is available or functionality is not imperative to Agency's business operations.
Confidential Information	This means any information that a disclosing party treats in a confidential manner and that is marked “Confidential Information” prior to disclosure to the other party.
Data	This means all information, whether in oral or written (including electronic) form, created by or in any way originating with agency and end users, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with agency and End Users, in the course of using and configuring the Services provided under this agreement, and includes agency Data, End User Data, and Protected Information.
Downtime	This means any period of time of any duration that the Services are not made available by vendor to agency for any reason, including scheduled maintenance or Enhancements.

End User	This means the individuals (including, but not limited to employees, authorized agents, Third Party consultants, auditors and other independent contractors performing services for agency; any governmental, accrediting or regulatory bodies lawfully requesting or requiring access to any Services; Agencies of agency provided services; and any external users collaborating with agency) authorized by agency to access and use the Services provided by Vendor under this Agreement.
End User Data	Includes end user account credentials and information, and all records sent, received, or created by or for end users, including email content, headers, and attachments, and any Protected Information of any end User or third Party contained therein or in any logs or other records of Vendor reflecting End User's use of Vendor Services.
Services	This means vendor's computing solutions, provided over the Internet to agency pursuant to this agreement, that provide the functionality and/or produce the results described in the Documentation, including without limitation all Enhancements thereto and all interfaces.
Third Party	This means persons, corporations and entities other than vendor, agency or any of their employees, contractors or agents.
Agency data	This includes credentials issued to agency by vendor and all records relating to agency's use of Vendor Services and administration of End User accounts, including any protected Information of agency personnel that does not otherwise constitute Protected Information of an End User.

Service Details

IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

Cloud Deployment Model

Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It would be owned, managed, and operated by the government organization and it exists on premises.
Public Cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid Cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third-party, or some combination of them, and it may exist on or off premises.

Service Levels

Vendor represents and warrants that the Services will be performed in a professional manner consistent with industry standards reasonably applicable to such services.
Vendor represents and warrants that the Services will be operational at least 99.99% of the time in any given month during the term of this Agreement, meaning that the outage or Downtime percentage will be not more than .01%.

If the Services availability falls below 99.99% in any month, vendor shall provide agency with a credit of that month's bill for Services according to the table below.

Availability	Percentage of Credit
99.60% to 99.69%	10%
99.50% to 99.59%	20%
99.00% to 99.49%	30%
97.00% to 99.00%	50%
Below 97.00%	75%

Service	Availability
Cloud Server availability	99.99%
Cloud Network availability	99.99%
Cloud Storage availability	99.99%

Vendor shall provide agency with monthly reports documenting its compliance with the service levels detailed herein. Reports shall include, but not be limited to, providing the following information:
a) Monthly Services availability by percent time, dates and minutes that Services were not available, and identification of months in which agreed upon service levels were not achieved;
b) Average transaction processing time per week, the fastest and slowest individual transaction processing time per week, the percent of transactions processed that meet the service levels stated herein, and identification of weeks in which agreed upon service levels are not met.

Data Privacy

Vendor will use agency Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for agency and its End User's sole benefit, and will not share such data with or disclose it to any Third Party without the prior written consent of agency or as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such data for Vendor's own benefit and, in particular, will not engage in "data mining" of Agency or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by agency

Vendor will provide access to agency and End User Data only to those Vendor employees, contractors and subcontractors ("Vendor Staff") who need to access the data to fulfil Vendor's obligations under this Agreement. Vendor will ensure that, prior to being granted access to the data, Vendor Staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

Data Security and integrity

All facilities that store and process agency data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such data from unauthorized access, destruction, modification, or disclosure. Such measures will be no less protective than those used to secure vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved.

Vendor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Services to agency in a manner that is, at all times during the term of this Agreement, at a level equal to or more stringent than anywhere else

Without limiting the foregoing, vendor warrants that all agency data will be encrypted in transmission (including via web interface) and in storage at a level equivalent to or stronger than 128-bit level encryption.

Vendor shall at all times use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to anti-virus and anti-malware protections and intrusion detection and reporting methods

Vendor will configure the Services to filter spam while permitting communications from Third Party Internet Protocol addresses identified by agency as legitimate.

Physical and Environmental Security -Controls that provide reasonable assurance that access to physical servers at the production data center is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes.

Monitoring the network and production systems, including error logs on servers, disks and security events fur any potential problems.

Such monitoring includes:

a) Reviewing changes affecting systems handling authentication, authorization, and auditing;

b) Reviewing privileged access to Workday production systems; and

c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

Data Compromise Response

Vendor shall report, either orally or in writing, to agency any data compromise involving agency or end user data, or circumstances that could have resulted in unauthorized access to or disclosure or use of agency or end user data, not authorized by this agreement or in writing by agency, including any reasonable belief that an unauthorized individual has accessed agency or end user data. Vendor shall make the report to agency immediately upon discovery of the unauthorized disclosure, but in no event more than 48 hours after vendor reasonably believes there has been such unauthorized use or disclosure. Oral reports by vendor regarding data compromises will be reduced to writing and supplied to agency as soon as reasonably practicable, but in no event more than 48 hours after oral report.

Immediately upon becoming aware of any such Data Compromise, vendor shall fully investigate the circumstances, extent and causes of the data compromise, and report the results to agency and continue to keep agency informed on a daily basis of the progress of its investigation until the issue has been effectively resolved.

Vendor's report discussed herein shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the agency or End User Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure (if known), (iv) what vendor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action vendor has taken or shall take to prevent future similar unauthorized use or disclosure.

Data retention and disposal

Vendor will retain data in an end User's account, including attachments, until the end user deletes them or for the time period mutually agreed to by the parties

Using appropriate and reliable storage media, Vendor will regularly backup agency and end user data and retain such backup copies for a minimum of 12 months.

Vendor will retain logs associated with end user activity for a minimum of 12 months.

Data transfer upon termination or expiration

Upon termination or expiration of this agreement, vendor will ensure that all agency and end user data are securely transferred to agency, or a third Party designated by agency, within 30 days. Vendor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of agency, and that agency will have access to agency and end user data during the transition. In the event that it is not possible to transfer the aforementioned data to agency in a format that does not require proprietary software to access the data, Vendor shall provide agency with an unlimited use, perpetual license

Vendor will provide agency with no less than 90 calendar days' notice of impending cessation of its business or that of any Vendor subcontractor and any contingency plans in the event of notice of such cessation. This includes immediate transfer of any previously escrowed assets and data and providing agency access to vendor's facilities to remove and destroy agency-owned assets and data.

Vendor will provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to agency.

Vendor shall implement its contingency and/or exit plans and take all necessary actions to provide for an effective and efficient transition of service with minimal disruption to agency. Vendor will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal downtime and effect on agency, all such work to be coordinated and performed no less than 90 calendar days in advance of the formal, final transition date

Data Location

Vendor guarantees that the location of the data would be in Thailand only and in no case would vendor move the data to other countries. If the cloud vendor plans to move the data from one location to another within Thailand, vendor needs to obtain permission from the agency for such movement. Vendor should also provide X days of notice to agency for the movement.

Interruptions in service; suspension and termination of service; changes to service

Vendor shall be responsible for providing disaster recovery Services if vendor experiences or suffers a disaster. Vendor shall take all necessary steps to ensure that Agency shall not be denied access to the Services for more than five 10 hours in the event there is a disaster impacting any vendor infrastructure necessary to provide the Services. Vendor shall maintain the capability to resume provisions of the Services from an alternative location and via an alternative telecommunications route in the event of a disaster that renders the Vendor's primary infrastructure unusable or unavailable

Vendor warrants that the minimum technical requirements for access to and operation of the Services If future enhancements to the Services require use of newer versions of these web browsers, vendor will provide a minimum of X days written notice to agency prior to implementing such enhancements.

From time to time it may be necessary or desirable for either the agency or vendor to propose changes in the Services provided. Such changes shall be made pursuant to the Change Control Procedure. Automatic enhancements to any software used by vendor to provide the Services that simply improve the speed, efficiency, reliability, or availability of existing Services and do not alter or add functionality, are not considered “changes to the Services” and such enhancements will be implemented by vendor on a schedule no less favourable than provided by vendor to any other Agency receiving comparable levels of Services.

Vendor will provide agency with X calendar day’s prior notice of any times that the Services will be unavailable due to non-emergency maintenance or enhancements. In the event of unscheduled and unforeseen times that the Services will for any reason, except as otherwise prohibited by law, Vendor will immediately notify agency and cooperate with agency’s reasonable requests for information regarding the services being unavailable (including causes, effect on Services, and estimated duration).

Vendor may suspend access to services by an end user immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of vendor’s Services or the network(s) or facilities used to provide the Services. Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The suspension will be lifted immediately once the breach is cured.

Technical support

During the term of this agreement vendor will provide agency with ongoing technical support for the Services at no less than the levels and in the manner(s) specified.

Vendor may not withdraw technical support for any Service without X months advance written notice to agency, and then only if vendor would be allowed to withdraw the technical support.

Agency shall receive at its option the general help desk technical support offered by vendor to its other customers. Irrespective of vendor's general technical support offerings, vendor shall provide agency option with the following technical support

Vendor shall provide technical support to agency for the purpose of answering questions relating to the Services, including (a) clarification of functions and features of the Services; (b) clarification of the documentation; (c) guidance in the operation of the Services; and (d) error verification, analysis, and correction, including the failure to produce results in accordance with the documentation

Such assistance shall be provided by vendor twenty-four (24) hours a day, seven (7) days a week via a toll-free telephone number and live, online chat staffed by help desk technicians sufficiently trained and experienced to identify and resolve most support issues and who shall respond to all agency requests for support within fifteen (15) minutes after receiving a request for assistance.

Correction of Services errors

Priority	Description	Target Response Time	Target Update Time	Target Fix Time
P1	Production software unusable/Production cloud servers inaccessible	1 hour, Providers executive notified of issue	1hr	Immediate - work commences and continues until issue resolved or workaround deployed
P2	Partial software functionality unusable/Partial service unavailable	4 hours	1 Day	2 days, subject to available maintenance slot
P3	Cosmetic issue	1 working day	1 working day	Next software release/service update
P4	Information request	2 working days	2 working day	n/a

Training

Vendor shall provide agency with training for the purposes of understanding and using the Services ("Training Services"). Training Services will be provided by vendor as detailed below at no additional cost to agency. Training Services will be provided by vendor at agency at mutually agreeable dates and times, but no later than one hundred eighty (180) calendar days following the Effective Date of this Agreement

Transition Assistance

Vendor will develop, provide and implement the transition assistance to support Agency's successful and uninterrupted transition from its current solution, or other solution in this area, to vendor's services. Transition Assistance will be provided by vendor detailed below at no additional cost to agency. Transition assistance will be provided by vendor at agency location at mutually agreeable dates and times, but no later than ten X calendar days following the Effective Date of this Agreement.

Within no more than ten X calendar days after the effective date of this agreement, vendor shall, at its own expense, provide qualified individuals to (a) uninstall existing solution, (b) implement the Services, and (c) assist in testing of the Services to ensure that they are functioning in accordance with the terms of this Agreement.

Fees, invoicing, payment and pricing

Agency agrees to pay all net undisputed amounts due to vendor in accordance with the Services fee schedule set forth below. Such fees will be payable after access to the Services is provided to agency and within thirty X calendar days of agency's receipt of Vendor's invoice or the invoice due date, whichever is later. Agency shall not be subject to late payment fees.

Agency need to specify services fee details here including a description of the service being acquired, list price and agency cost per unit of each service being acquired, quantity of units initially being acquired, the term for each service being acquired, and any other pertinent considerations or limitations applicable to the services being acquired.

Agency will have the option to acquire additional Services throughout the duration of the Agreement

Agency will have the option to acquire additional Services for a monthly prorated portion of per unit cost in order that all Services acquired maintain the same term.

Services acquired during the initial purchase shall be provided by vendor to agency for an initial one (1) year term (the "Initial Services Term") commencing on the "Services Commencement Date" (as hereafter defined). The Initial Services Term shall be renewable for successive one (1) year terms ("Extension Terms", and collectively with the Initial Services Term, the "Services Term") upon written notice from agency to vendor. For the purposes of this agreement, the term "Services Commencement "shall refer to the first day of the month following the month in which the Services were initially provided to agency.

After the first anniversary of the Initial Services Term, the Services shall be renewable for successive one (1) year terms ("Extension Terms") upon written notice from agency to Vendor.

Vendor should include pricing changes notice X days before the change (requirement to give notice prior to pricing changes) Vendor should mention number of pricing changes time frame limitation (limitation on how many pricing changes can occur within set time frame) Demand Pricing (requirement to match lower pricing offered to other similar entities when quantities, services, etc., are comparable) Costs for Special Services/Additional Quantities/Etc. (costs related to items not specifically included in the original contract scope)

Terms and Termination

Agency may terminate this agreement upon X calendar days written notice.

Vendor shall provide written notification regarding upcoming annual Agreement term expiration dates no less than X calendar days prior to expiration dates.

Agency may terminate this Agreement immediately upon Vendor's any substantive breach of the terms of this Agreement.

Warranties, representations and covenants

Agencies shall have the right to discontinue use of the Services for any reason, and shall receive a full refund of all payments, for a period of X calendar days after the Services Commencement Date (the “Warranty Period”).

Services Warranty: Vendor represents and warrants that the Services provided to agency under this agreement shall conform to, be performed, function, and produce results substantially in accordance with the Documentation. Vendor shall offer agency warranty coverage equal to or greater than that offered by vendor to any of its customers.

Disabling Code Warranty: Vendor represents, warrants and agrees that the services do not contain and agency will not receive from vendor any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any agency system or Data (a "Disabling Code").

Intellectual Property Warranty: Vendor represents, warrants and agrees that vendor has all Intellectual Property Rights necessary to provide the services to agency in accordance with the terms of this agreement; vendor is the sole owner or is a valid licensee of all software, text, pictures, audio, video, logos and copy that provides the foundation for provision of the Services, and has secured all necessary licenses, consents, and authorizations with respect to the use of these underlying elements; the Services do not and shall not infringe upon any patent, copyright, trademark or other proprietary right or violate any trade secret or other contractual right of any Third Party; and there is currently no actual or threatened suit against vendor by any Third Party based on an alleged violation of such right. This warranty shall survive the expiration or termination of this Agreement.

Date/Time Change Warranty. Vendor represents and warrants to agency that the Services provided will accurately process date and time-based calculations under circumstances of change including, but not limited to: century changes and daylight saving time changes. Vendor must repair any date/time change defects at vendor’s own expense.

Compliance with Laws Warranty: Vendor represents and warrants to agency that it will comply with all applicable laws, including its tax responsibilities, pertaining to the Agreement and its provision of the Services to agency.

Audit

Vendor is responsible for keeping accurate records related to its performance and obligations under this Agreement. In particular, records will be kept documenting any price, cost or budget computations required under the Agreement.

Vendor agrees that agency or its authorized representative has the right to audit any directly pertinent books, documents, papers and records related to transactions and/or performance of the terms and conditions of the Agreement. Vendor shall make available to agency or its representative all such records and documents for audit on vendor's premises during regular business hours within X business days of a written request for availability. Vendor agrees to either: (a) allow agency to make and retain copies of those documents useful for documenting the audit activity and results; or (b) sequester the original or copies of those documents which agency identifies for later access by agency.

The right to audit shall include periodic examinations of records throughout the term of the Agreement and for a period of X years after its termination.