



เอกสารประกอบการประชุมรับฟังความคิดเห็น
ต่อ (ร่าง) ยุทธศาสตร์การพัฒนาศูนย์ข้อมูลภาครัฐ
(Government Data Center Modernization)

และ (ร่าง) มาตรฐานบริการศูนย์ข้อมูลภาครัฐ

วันพุธที่ 26 เมษายน 2560 เวลา 13.00 – 16:30 น.

ณ ห้องประชุมออดิทอเรียม อาคารทรงกลม ศูนย์ประชุมวายุภักษ์
โรงแรมเซ็นทาราศูนย์ราชการและคอนเวนชันเซ็นเตอร์ แจ้งวัฒนะ

การพัฒนาศูนย์ข้อมูลภาครัฐ

(Government Data Center Modernization)

Contents

1. Data Center Modernization-Country Benchmarking	3
2. Thailand Government Data Center Modernization.....	5
3. Government Data Center Modernization Strategy	11
4. Data center Standards	20

1. Data Center Modernization-Country Benchmarking Government Datacenter Modernization

Multiple forces have driven government agencies across the world to focus on Datacentre Modernization in the last decade. From a technology standpoint, today’s Datacentres must support provisioning on demand, scalability, virtualization and the flexibility to respond to fast changing requirements and operational situations.

Malaysia Data Center Modernization

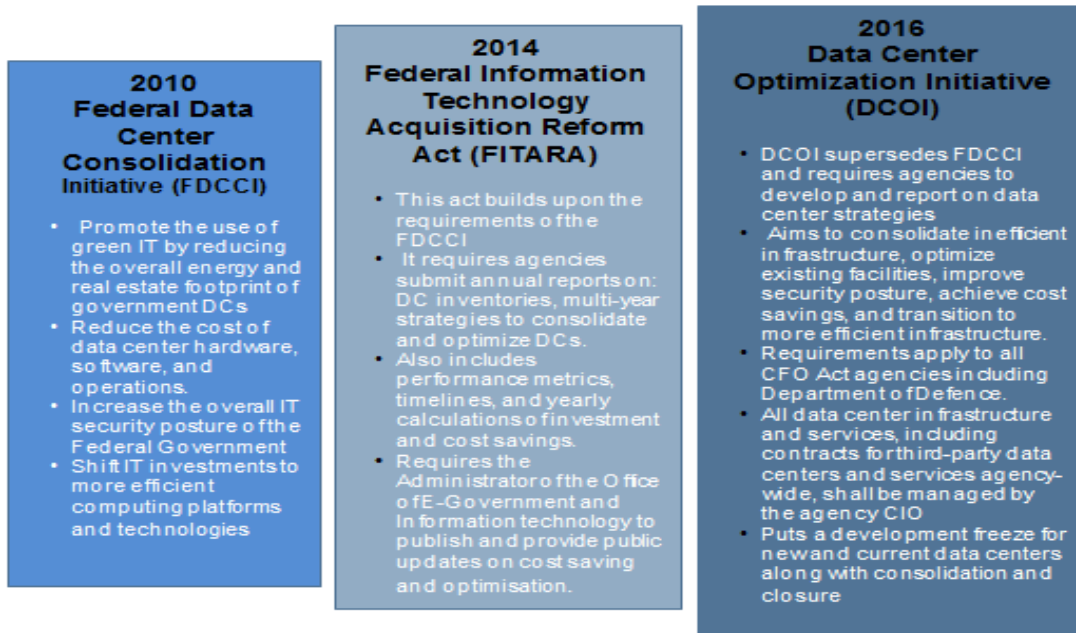
Time Period	1990-2010	2011-2015	2016-2020
Digital Roadmap	<p>Focus on developing Malaysia as Knowledge hub</p> <p>Focusing on Improving public sector service delivery for citizens</p> <p>Articulation of Vision 2020</p>	<p>Development of the ICT roadmap for public sector(2011-2015)</p> <p>Development of the government led infrastructure initiatives</p> <p>Further articulation of Vision 2020.</p>	<p>Development of the ICT roadmap for public sector(2016-2020)</p> <p>Focus on developing digital government</p> <p>Strengthening of the government infrastructure</p>
Government data center Strategy	Development of shared services model	Development of government data centers	Development of public data center model

In 1990s, a focus on knowledge-based industries was viewed by the government as the way for Malaysia to realize its aspiration to become a high-income country. A focus on ICT and knowledge creation as the path to sustained growth was first introduced in the Seventh Malaysian Economic Plan (1996–2000). From 2011 to 2015, Malaysia government focused on developing a strong and challenging roadmap for public sector. This roadmap focused on centralized infrastructure and development of one network for the government. From 2016-2020, Government plans to focus on alignment of the use of technology with the business direction of the Public Sector, alignment of the ICT implementation with ICT agenda of the Public Sector and lastly ensures return of investment through exploitation of technology and a structured and well planned ICT implementation.

As part of the developing the public sector in the Malaysia, Government started focusing on the data center modernization process and this was included in the ICT plan for 2011 to 2015. The central government agency MAMPU was given the responsibility of modernizing the data center in Malaysia. By 2015, Mampu has established two government data centers which was being used by more than eighty government agencies. As per the ICT plan for 2016 to 2020, Mampu plans to open six government data centers and start offering full-fledged cloud computing and colocation services through these data centers. Government expects more than ninety percent agencies would use either cloud or colocation service from MAMPU by 2020, and this would help in the reduction of own data center usage.

United States Data Center Modernization

The Office of Management and Budget (OMB) is the largest office within the Executive Office of the President of the United States and many government agencies comes under this office. Under the OMB, The Office of E-Government and Information Technology (E-Gov), headed by the Federal Government's Chief Information Officer, have developed the plan for federal data center consolidation plan in 2010.



United States government launched the Federal Data Center Consolidation initiative to promote the use of green IT. FDCCI provided guidelines on reducing the overall energy and real estate footprint of data centers and cutting the cost of data center hardware, software and operations -- while increasing the overall IT security posture of the federal government.

To date, government agencies have closed 4,300 of nearly 11,000 data centers and achieved some \$2.8 billion in cost savings and avoidances through fiscal 2015. US government estimates indicate at least \$5 billion more in savings is still achievable and it is possibly more than that.

The latest initiative DCOI, which supersedes FDCCI, mandates that agencies should fill the below conditions by 2018.

- Agencies should install advanced energy metering must be installed and energy usage accurately reported to the Office of Management and Budget.
- Existing data centers must operate at a power usage effectiveness (PUE) rate of 1.5 or below or potentially be shuttered by the deadline.
- Manual reporting is no longer acceptable, and data center infrastructure management (DCIM) tools must be implemented for automated monitoring and operations.

2. Thailand Government Data Center Modernization

Data centers are ever-evolving and integrate with a widely interconnected and increasingly virtual IT infrastructure. The modern data center is powering this innovation and creativity at levels of scale that have broad impact across business, education and government.

These are three areas of immediate opportunities for Modernization

- Modernizing the IT infrastructure for utilizing opportunities cloud deployments
- Optimizing applications and current legacy data centers
- Ensuring and safeguarding the information and data

Today's government agencies struggle to maintain the delicate balance between the growing demand for technology services and tightening budget restraints. Government agencies are increasingly facing challenges, such as complex IT environments, use of manual processes, lack of visibility across systems and insufficient budget and personnel resources.

Key Challenges faced by the Thai government agencies



- Security includes: data security, security handling at the agency, handing of high risk and mission critical data.
- Data handling includes data integration and classification, agency responsibility, data cleansing, accuracy and quality.
- Human resources include: lack of human resources at the agency, lack of skills and overall lack of availability of skilled resources
- Budget and Cost include the allocated budgets for expenses and increasing costs of operations as well as upgradation.
- Agency policies and management include shared utilization, planning, focus on DR and backup, citizen centricity etc.
- Data Center Setup include server, storage, cabling, cooling set, power setup, floor architecture, racks, building design etc.

Current State of Government data center Infrastructure in Thailand

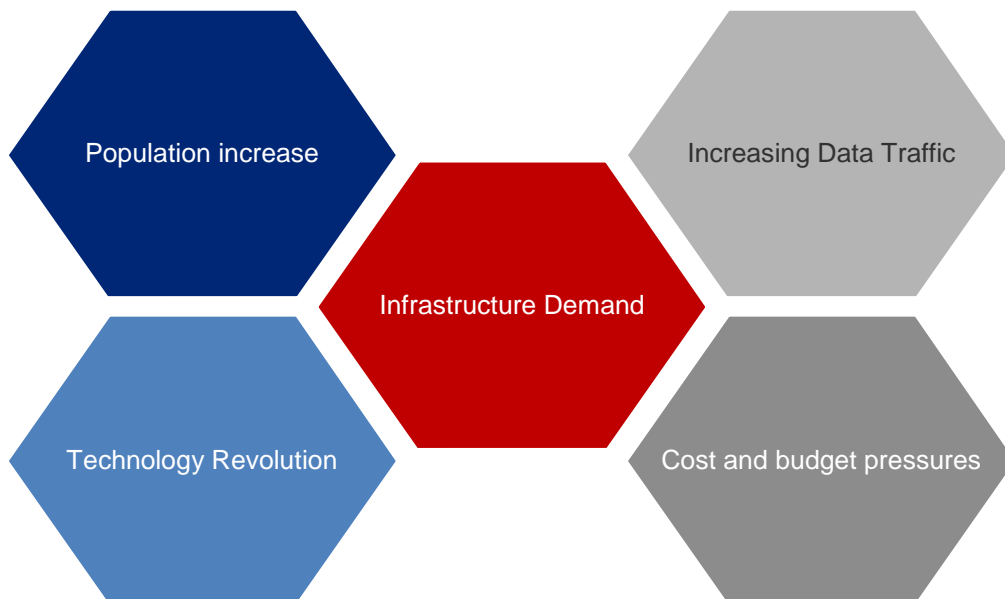
Our analysis on discussions with agencies reveals that agencies recognise the importance of improvement of their data center operations and clearly identify the need for change. Various agencies identified the need for a national program and a blueprint to bring all the agencies on a common platform to drive change and to ensure improvement of services, productivity, and knowledge and operations excellence.

The top 4 areas that were identified based on agency feedback to be the most important areas where Thailand needs to improve in their DC services are:



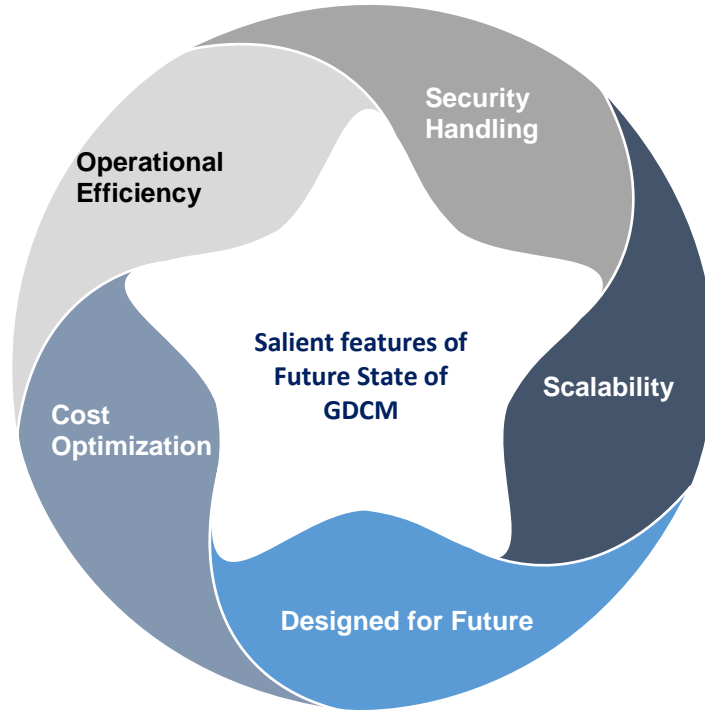
Future Data Center Infrastructure of Thailand

With the ever changing and developing macro-economic environment and government's focus on Digital Economy, Thailand's agency infrastructure needs a shift for better. A number of themes hold the keys to form as building blocks for future state of Thailand Government Data Infrastructure.



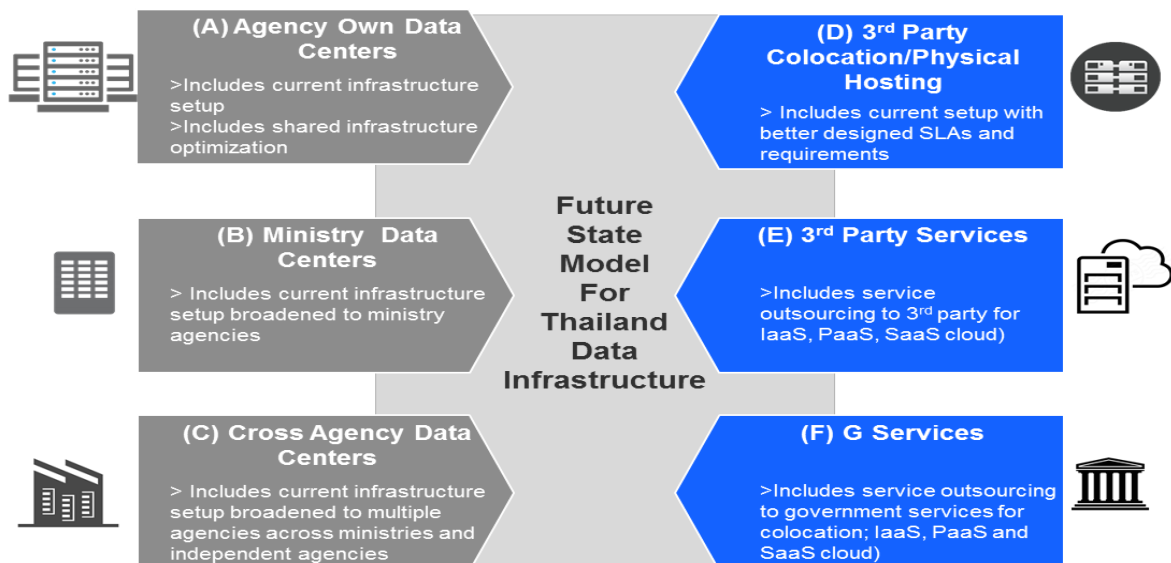
Building Blocks of Future Strategy

Future State for Thailand’s Data Infrastructure Initiative called Government Data Center Modernization (GDCM) will have 6 salient features that differentiate it, from the current infrastructure and will be the building blocks for the future strategy.



Future Operating model of Thailand Government Data Center Infrastructure

Thailand Government’s Data Infrastructure in future will be managed under Thailand Government Data Center Management (GDCM) Initiative that will oversee the implementation of GDCM Strategy over next 5 years (2017-2022).



(A) Agency Own Data Centers

Agency Own Data Centers is the current agency set-up, with government investments spent in establishment of the facility that will offer data hosting capability to the particular agency only at higher service levels, security and utilization.

(B) Ministry Data Centers

Ministry Data Centers are large data centers currently served as current agency set-up, that in future will be transformed for pan ministry operations to enable hosting of data, services and applications across ministry agencies

(C) Cross-Agency Data Centers

Cross-Agency Data Centers originates from the current agency set-up but enables a multiple agency integrated government infrastructure with reduced government spending, greater efficiency and better service delivery offering services to host data of agencies across multiple ministries as well as independent agencies.

(D) 3rd party Colocation/Physical Hosting

Colocation/3rd party hosting is an ongoing service area that enables outsourcing the management and supporting infrastructure to host agency servers to enable a better environment to ensure better connectivity, security, stability, predictability, reduced need for capex on building improvements and opex on management and business support, Colocation enables a much better service provision for mission critical data and other elements that require better support and availability.

(E) 3rd party services (IaaS, PaaS and SaaS cloud)

3rd party services include IaaS, PaaS and SaaS cloud service provision by private companies and enterprises where agencies can outsource their entire data management to 3rd party cloud facilities without holding physical infrastructure or need for maintaining data. Entire responsibility and the physical assets like servers, storage and environment is the responsibility of 3rd party to provide lower cost, optimized, flexible and energy efficient services.

(F) G-Services (Colocation, IaaS, PaaS and SaaS cloud)

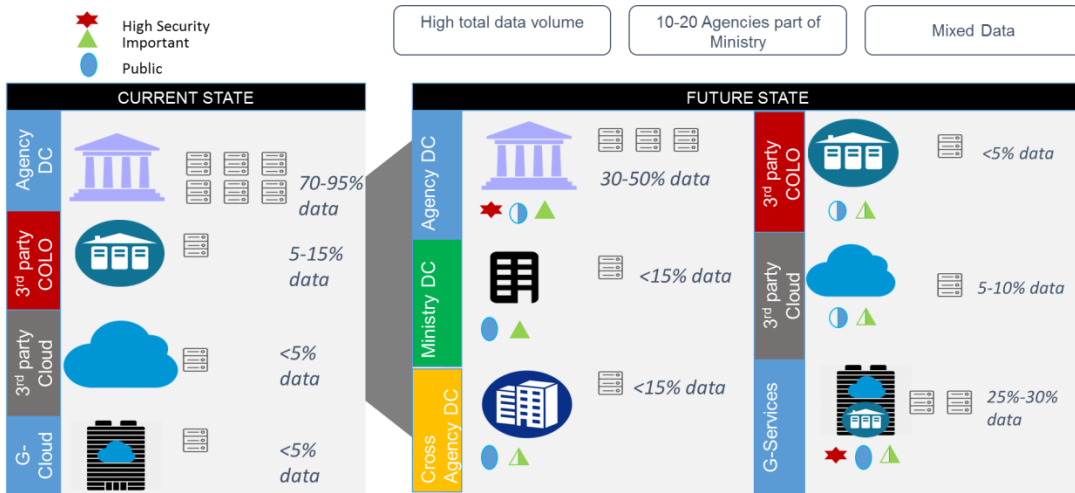
G- services include service provision by the government for colocation, IaaS, PaaS and SaaS cloud to provide data management, computing and hosting solutions to the government agencies in an outsourcing model. The service quality will be almost at par with 3rd party servicing with added benefit of higher security handling. Entire responsibility and the physical assets like servers, storage and environment will be the responsibility of G-services in case of G-Cloud to provide secured, lower cost, optimized, flexible and energy efficient services.

Bringing everything together: Minimum Recommendations for an Optimized Infrastructure

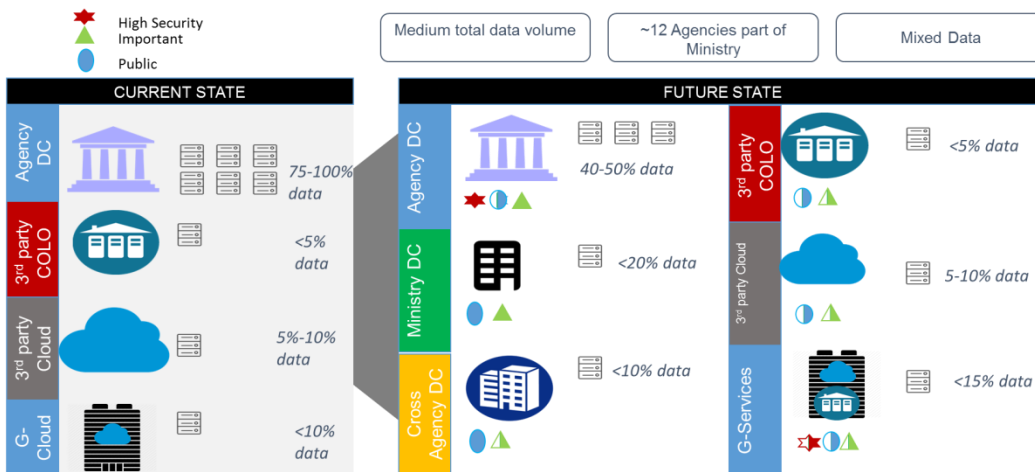
	Future State Model improvement over current state					
	(A) Agency Own Data Center	(B) Ministry Data Center	(C) Cross Agency Data Center	(D) 3 rd party Colocati on	(E) 3 rd party Services	(F) G- Services
<i>Handling of high security data</i>						
<i>Handling of public data</i>						
<i>Handling of important and mission critical data</i>						
<i>Improvement in standard adoption</i>						
<i>Support in data integration</i>						
<i>Cost efficiencies</i>						
<i>Solves issues of procurement lead times and OPEX budget</i>						
<i>Solves human resource availability and quality issues</i>						
<i>Better utilization of resources and infrastructure</i>						
<i>Reduces reliance on government budgets</i>						
<i>Reduces overall cost spent by government</i>						
<i>Ensures high scalability</i>						
<i>Ensures high resilience, availability and reliability</i>						
<i>Effectively balances and manages technology advancements</i>						
<i>Ability to manage future growth of data analytics and other complex computing needs.</i>						
<i>Optimal use of government resources</i>						

** Please note that the above future state model guidelines are minimum recommended guidelines. Agencies with high security data need to conduct detailed assessment in iDiscovery sessions on their minimum requirements*

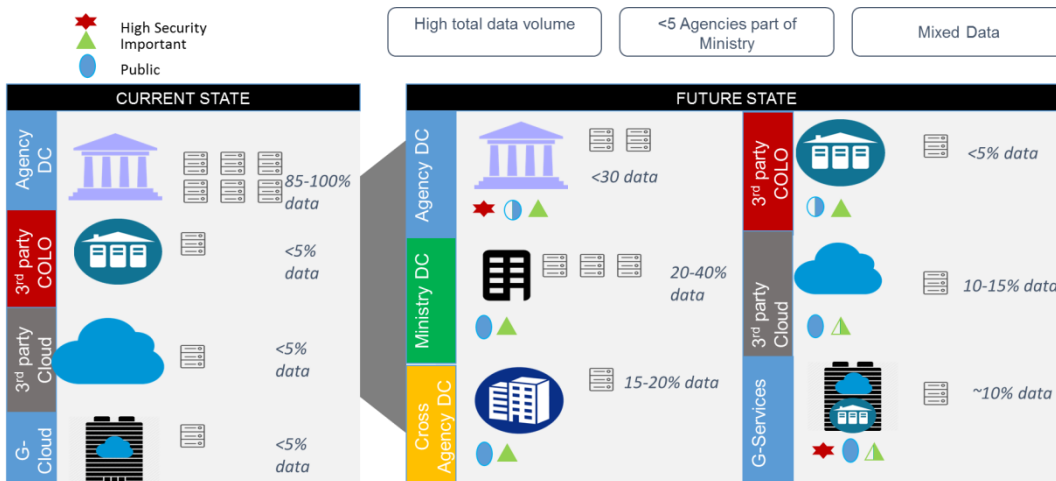
Example of how ministries and agencies will operate in future from data perspective: Large Ministry: e.g. Science and Tech



Example of how ministries and agencies will operate in future from data perspective: Medium Ministry: e.g. Commerce



Example of how ministries and agencies will operate in future from data perspective: Small Ministry: e.g. Tourism & Sports



3. Government Data Center Modernization Strategy



GDCM plan is based on comprehensive understanding and analysis of Thailand's data infrastructure including hard infrastructure, applications, data center establishments, views from the agency officials as well as international best practices. The detailed analysis enabled understanding of trends and needs in Thailand, expectations of agencies, issues and problems faced by agencies and citizens and the resulting issues. GDCM initiative will plan to yield a number of key benefits including enablement and strengthening of government data security, provision of efficient and cost effective servicing, transferring part of the efforts from agencies to other entities that enable an optimized functioning, addressing human resource challenges and improving the technology footprint of Thailand government's data infrastructure

The initiative aims at mitigating and resolving the following issues and challenges faced by the agencies:

Reduce cost of operations including maintenance

As covered in previous sections, one of the core concerns of the agencies is the increase in cost and insufficient government budgets to meet the service delivery needs. GDCM plans to reduce the effort that agencies would need to spend on their data infrastructure support services thus reducing their overall need.

Reduce overall government spending

As a part of digital economy, one of the important aims for GDCM initiative is to enable government to perform the key function effectively at reduced government spending by utilizing new technology, concepts and frameworks.

Improving efficiency of data center infrastructure

Establishing standards, which upon realization will enable an efficient data center ecosystem. At the same time, establishing shared facilities that will improve the overall utilization of the infrastructure.

Be future ready

Enable the government to plan for future and be able to embrace the new challenges of data and complexity expansion as well as rising citizen needs. As a building block to larger goals of citizen centricity, integrated operations as well as utilization of cloud and other technologies enable the use of latest systems that offer efficient, real-time computing capabilities that are the needs for today and tomorrow.

Enable multiple options for agencies to choose

Establishing highly matured options that can be taken up by agencies to improve their reliance on data center and to enable usage of other areas to solve their issues

Objective of Government Data Center Modernization (GDCM) Initiative



The key objective of the Strategy is to develop a data infrastructure approach to protect Thailand's high security data and to achieve operational excellence in service delivery. In achieving these, there are several other objectives including: business sustainability over long term, cost efficiency, technology innovation and preparedness for data revolution

Vision of Government Data Center Modernization (GDCM) Initiative



"To be an effective government data infrastructure that enables public service delivery through efficient, secured, cost effective and optimized operations"

Government data center modernization will support in the following key goals:

Realigning government data based on security characteristics of the data to enable higher security to national security data and appropriate handling of important data

Shifting IT infrastructure needs to more efficient technologies and service delivery options

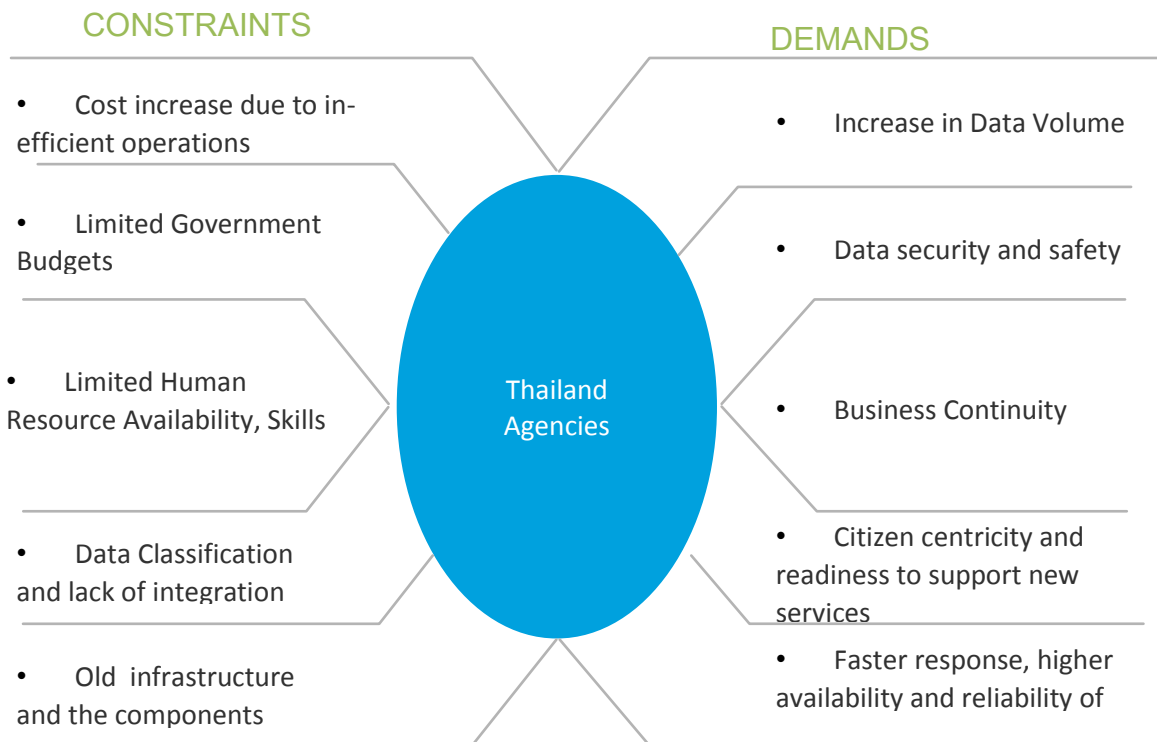
Reduce the cost of IT infrastructure viz, servers, storage, software and maintenance.

Implement shared operations at agency level, ministry level and government level.

Realigning the need for IT human resources at agency level

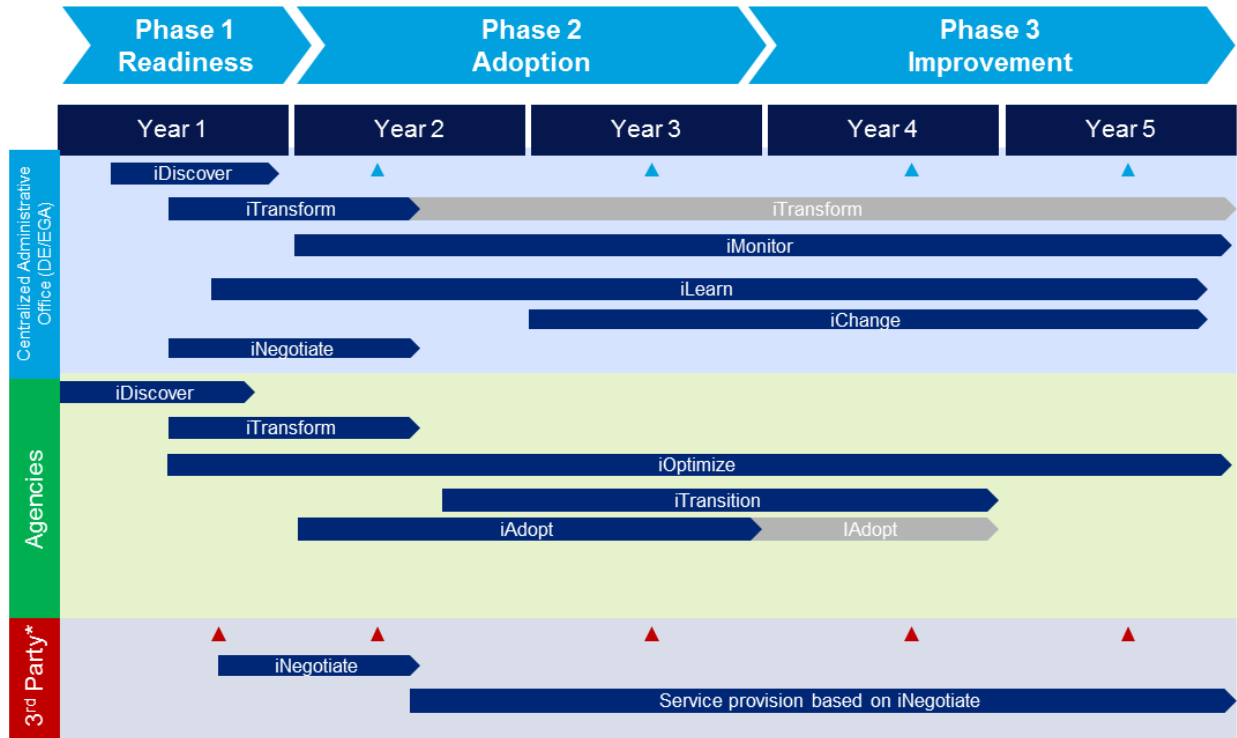
Data Center Developmental Plan

Government Agencies constrains and demands



Implementation Plan

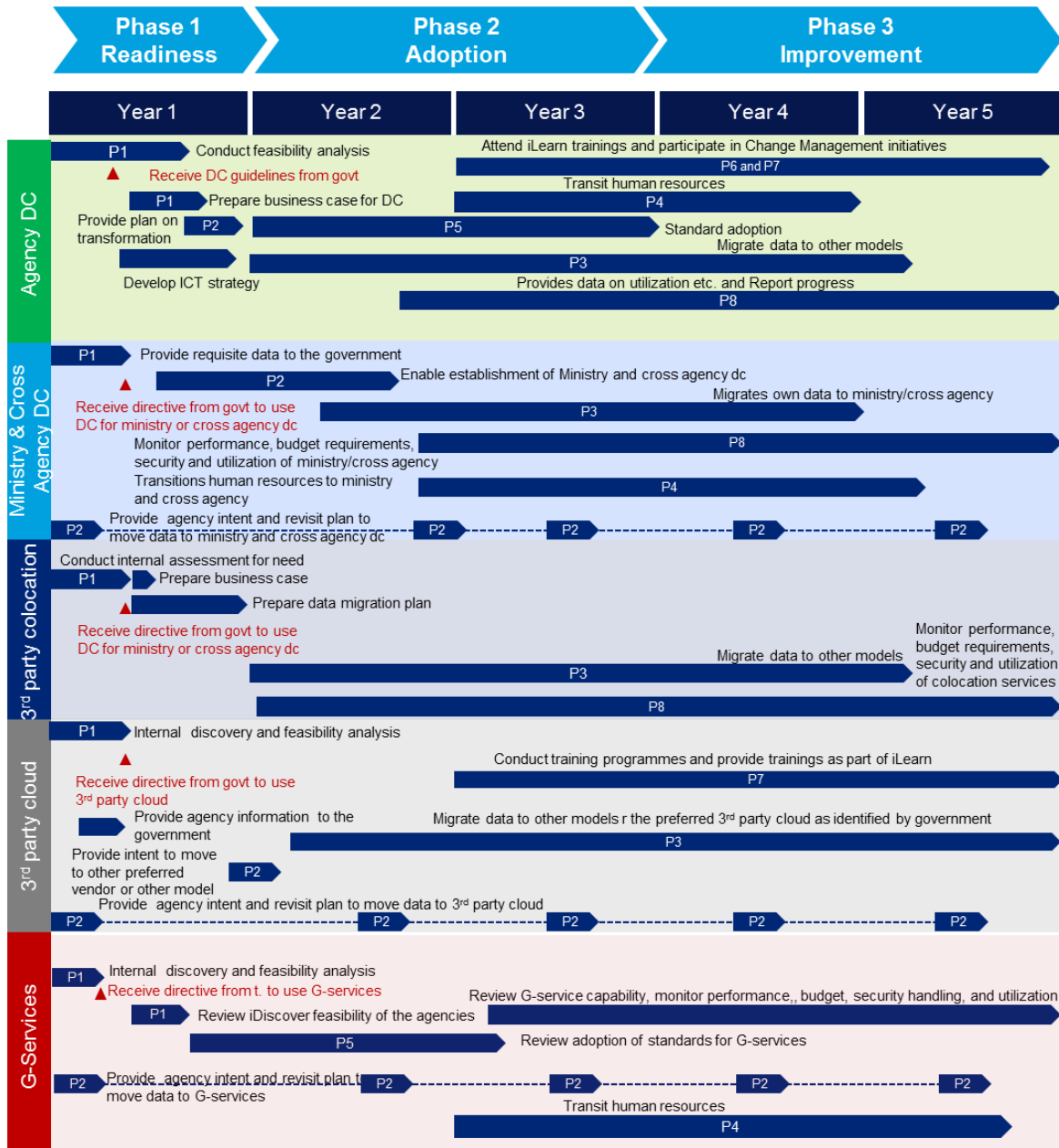
The implementation plan below highlights the key expectations and coverage across 5 years' timeline.



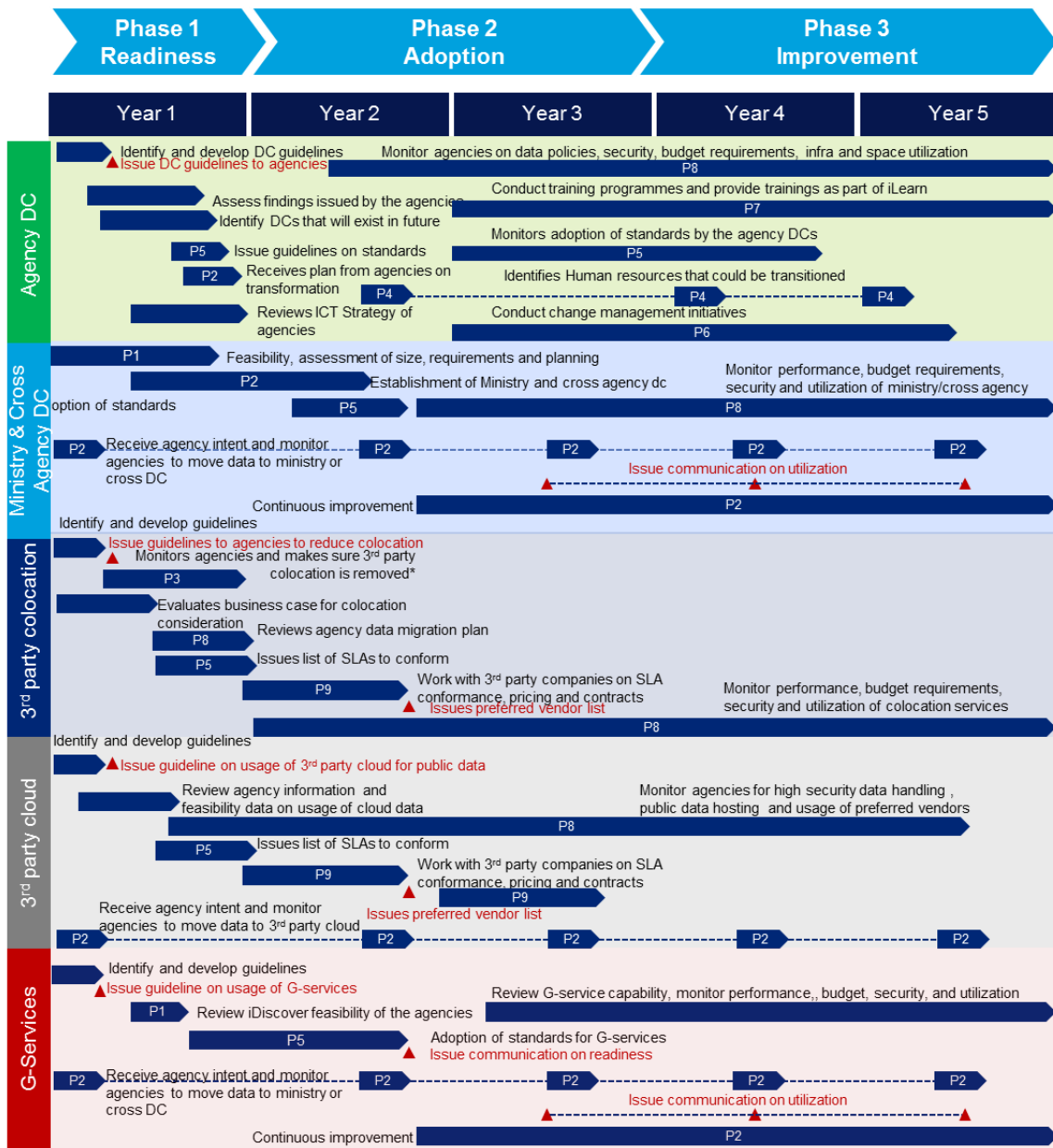
*Only involved in D and E areas

Legend	
	Project activities including planning, executing, monitoring and closing
	Review, checking for updates
	Government checkpoints on updates
	Checkpoint on SLA adherence, quality and service





Implementation Plan for Government Agencies








Implementation Plan for the Government (GDCM Administration Office)



GDCM Strategy Implementation Projects

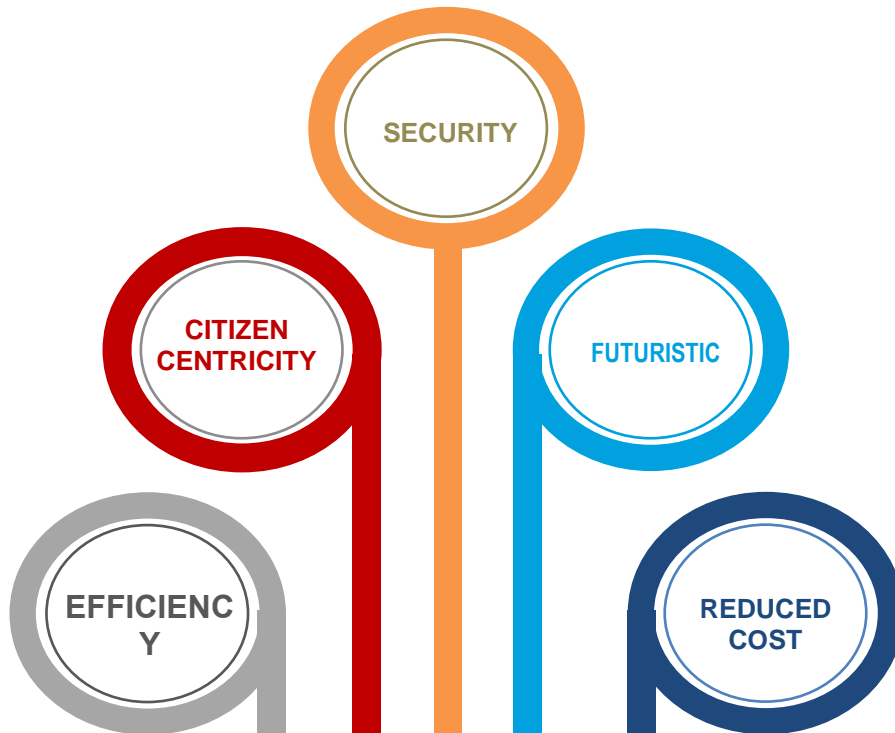
Type	Project Name and Aim	Description of Project
(P1) Project 1	 <p>iDISCOVER <i>Discovery study to understand feasibility of the model and requirements for alternate hosting</i></p>	<ul style="list-style-type: none"> ▪ This project covers conducting feasibility study and analysis by the agencies to discover their real needs and implementation readiness ▪ The study will entail agencies to provide details to the government on their current data classification, security handling, feasibility readiness for future models, applications, specifications etc. ▪ Government also conducts iDiscover study to identify readiness and feasibility of Ministry DC, cross agency DC and G-Services. ▪ The iDiscover project will enable coverage for agencies to identify the right future models to focus on.
(P2) Project 2	 <p>iTRANSFORM <i>Project to transform agency data centers into ministry and cross agency DCs</i></p>	<ul style="list-style-type: none"> ▪ This project identifies the criteria for selection of ministry and cross agency data centers. ▪ This is followed by identification of key requirements for establishing the ministry and cross agency data centers. The requirements range from standards, dc size, infrastructure requirements, quality assurance and other infrastructure elements necessary. ▪ Following the discovery of business requirements, the DCs will be converted to ministry and cross agency DCs ▪ This is followed by running communication plan, monitoring the progress, utilization of the transformed data centers.
(P3) Project 3	 <p>iOPTIMIZE <i>Project to migrate data from one model to other</i></p>	<ul style="list-style-type: none"> ▪ This project entails the data transition across the model after feasibility study and planning exercise is complete. ▪ This project entails movement of data from the agency own data center primarily to other areas like G-services, ministry. Cross agency data centers and 3rd party cloud. It also entails security based data transfer. ▪ This project also entails end state achievement for various models: data center closure, switch from 3rd party colocation, reduction in usage of own data center etc.
(P4) Project 4	 <p>iTRANSITION <i>Project to deploy human resources across agencies and models as required</i></p>	<p>This project focuses on human resource transition across various models.</p> <p>With rapid movement of data under migration, end state would result in human resources that would get freed from the data centers to be able to be deployed at other agencies or ministry Dc or cross agency DC or G-services.</p> <p>These resources will go through a process of transition based on their job roles</p>


<p>(P5) Project 5</p>	 <p>iADOPT <i>Project to adopt the identified standards</i></p>	<ul style="list-style-type: none"> ▪ This project enables adoption of the standards across the agencies as well as G-services. ▪ This project will start with feasibility analysis for standard adoption and identify guidelines for agencies to adopt based on “waves” developed in Phase 1. ▪ Agencies will have to adopt the standards across next 5 years based on the wave they are a part of and meet the adoption guidelines ▪ Government will monitor the adoption of the agencies and will provide reporting. ▪ Government will ensure that the ministry DCs cross agency DCs and the G-services comply to set standards.
<p>(P6) Project 6</p>	 <p>iCHANGE <i>Project to management change implementation and management</i></p>	<ul style="list-style-type: none"> ▪ This project revolved around change management process which starts from change readiness assessment. Government will conduct change readiness assessment for the agencies going through transformation from data migration, data center closure, data center conversion to ministry/cross agency dc, human resource transition etc. ▪ Government will plan change management events as well as analysis of the degree of change and identify gaps that needs to be filled. ▪ Government will identify sub initiatives to bridge the caps and will identify change agents who will make the change easier for the agencies to adopt ▪ Government will monitor the change and will use communication plan, culture dissemination and transition plan to seamless settling the change.
<p>(P7) Project 7</p>	 <p>iLEARN Project to provide training to human resources</p>	<ul style="list-style-type: none"> ▪ The project involves identifying training needs of the agency staff that needs to be provided as a part of transformation programme. ▪ These training courses would be across multiple areas: technology transformation, cloud, data center effectiveness, PUE, improving utilisation, standards, change management, job roles and responsibilities, leadership effectiveness, monitoring and reporting, project management as well as specific data center areas of operations. ▪ These trainings will be developed by the government representative or 3rd party as and needed. ▪ Government will develop and provide a calendar of event to conduct these trainings. ▪ Government will impart the trainings and measure its effectiveness.
<p>(P8) Project 8</p>	 <p>iMONITOR Project to monitor and report progress</p>	<ul style="list-style-type: none"> ▪ This project involves monitoring the progress of data migration and take up of the 6 areas. ▪ Government will periodically monitor and report the progress to the agencies and will promote the progress and setup of the new areas


<p>(P9) Project 9</p>	 <p>iNEGOTIATE Progress to negotiate better rates, services, SLAs with 3rd. party</p>	<ul style="list-style-type: none"> This short project involves government to identify the 3rd party vendors for colocation and cloud services and negotiate the SLAs, human resource requirements, servicing, quality and pricing for the overall agencies.
---------------------------	--	--

Benefit Realization Government data center modernization Initiative

Government Data Center Modernization will yield not only a modern infrastructure contributed by establishment and realization of identified standards but also utilise effective utilization of 6 key areas of future operations of data center infrastructure: With the effective utilization of all these components together, the government will be able to realise the following benefits.



- 

EFFICIENCY
Resulting from economies of scale, agile infrastructure, flexible, easier operations, efficient delivery, resource efficiency, better infrastructure and higher utilization.
- 

CITIZEN CENTRICITY
Through integrated service delivery, improvement of availability, better preparedness for new service provision, increasing customer experience with better accessibility and reliability of data.

- **SECURITY**
 To comply to government data security policies and standards and adapt to new policies

- **FUTURISTIC**
 To develop a flexible and agile ecosystem with futuristic and emerging technologies that are sustainable and upgradable

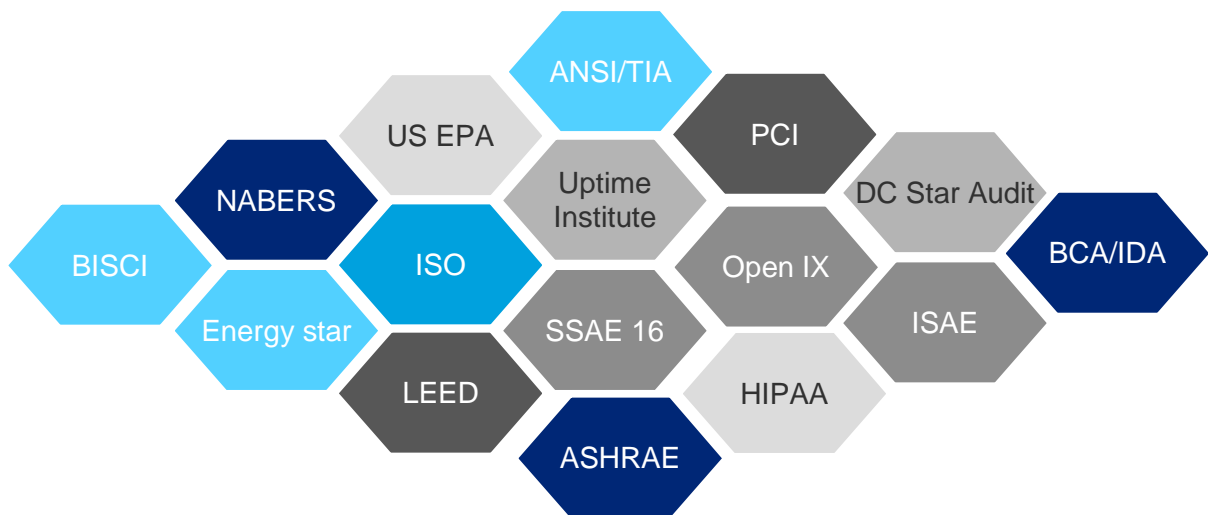
- **REDUCED COST**
 To enable overall reduction of future capital expenditure and operating expenses resulting from better utilization of infrastructure and usage of alternative models

4. Data center Standards

Data Center Standards

Standards typically in business parlance are universally or widely accepted, agreed upon, or established means of determining what a product, service, facility or a concept is required to be or is required to behave.

Standards by International Bodies



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. The figure above shows some of the standards developed with respect to data centers over a period of time.

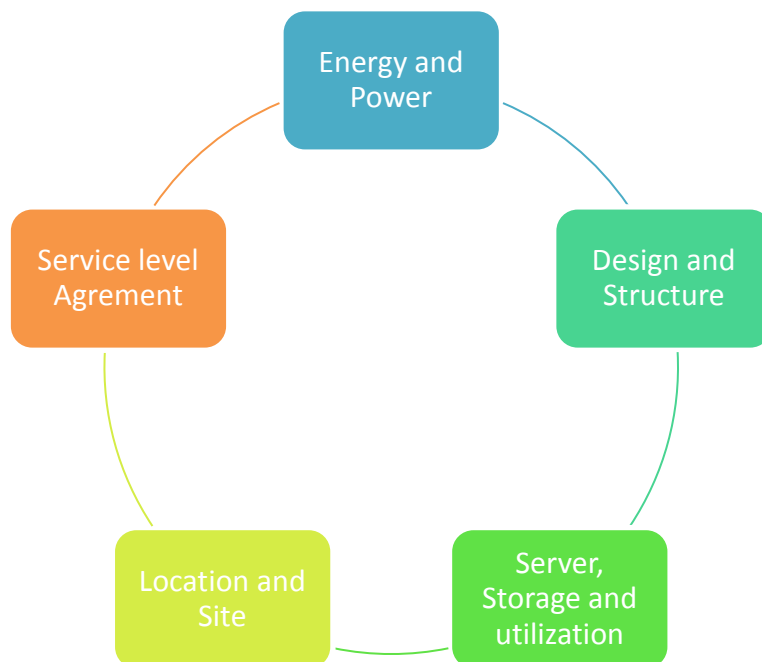
Standards in this document are hence viewed from 2 varied dimensions. The first dimension is based on the fact that certain international bodies and associations have prescribed

guidelines, certifications and specifications for select functional areas or structural elements that are used as global standards to follow.

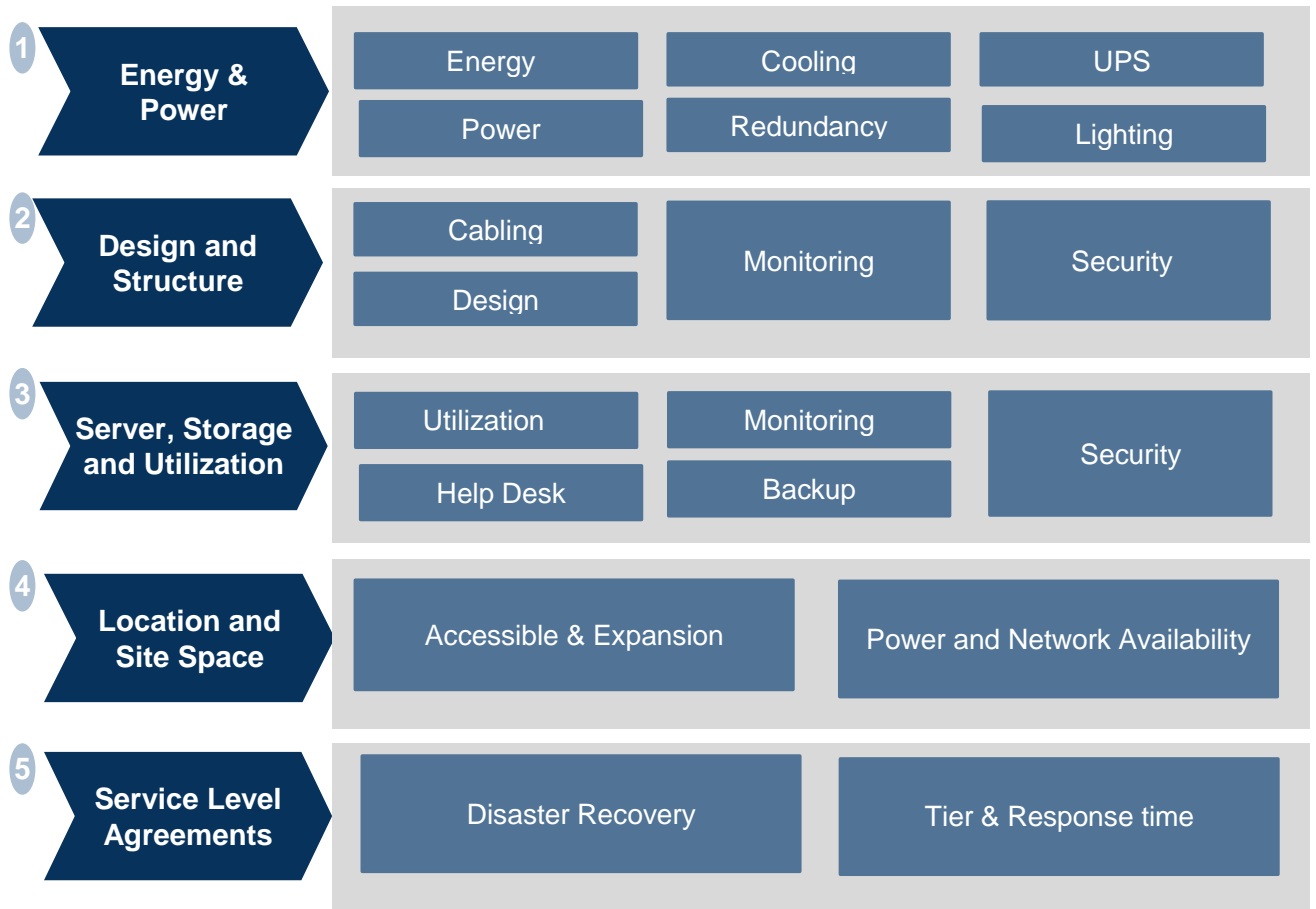
Standards Framework by Functional Areas

The data center standards framework is a comprehensive methodology that empowers coverage of the entire ecosystem of a data center across 5 broad functional areas. These functional areas include the core elements as well as non-core elements of the data center on which the concept, installation, enablement, maintenance and operations of a data-center is governed.

The second dimension is how the Standards are viewed based on functional areas as governed by the Agency itself. Which means, that each agency develop and prescribe their own set of guidelines and specifications that suit their needs. Certain group of agencies like government agencies work at tandem to align to a unified standard specification as prescribed by a party like EGA. In the diagram below, it



Based on these functional areas, 19 DC elements are articulated as below that together form the Modern Data Center Architecture.



Data Center Standards Importance & Challenges

Importance

- Adopting standards would help the data center become more efficient.
- Comparative analysis would help the customers to make the right decision when choosing any data center provider.
- Adopting Data center would decrease the cost of operating the data center in long run.
- Data center adopting industry standards would help reduce the environmental impact.

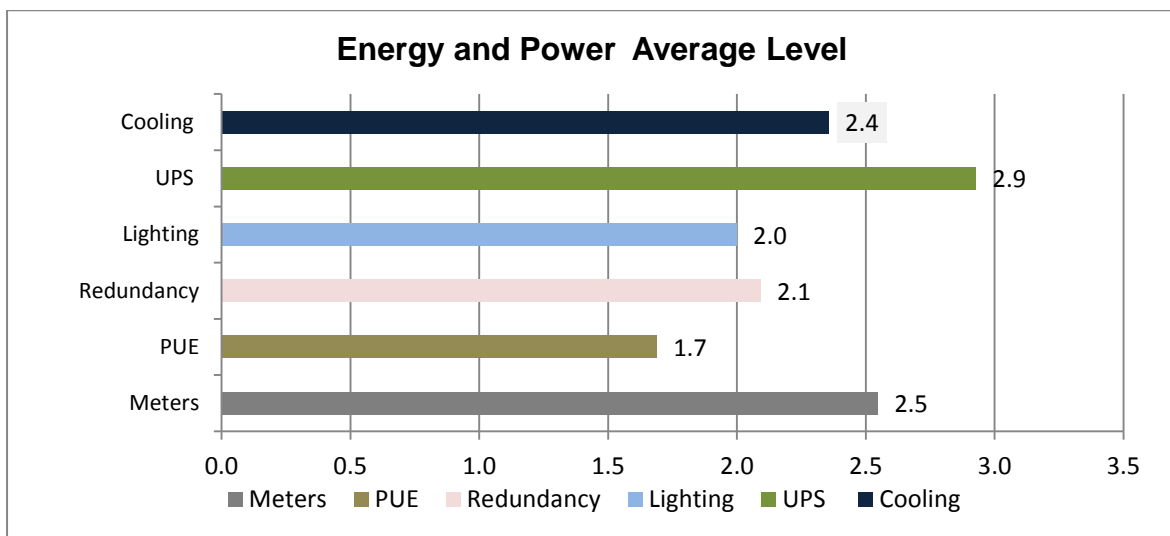
Challenges

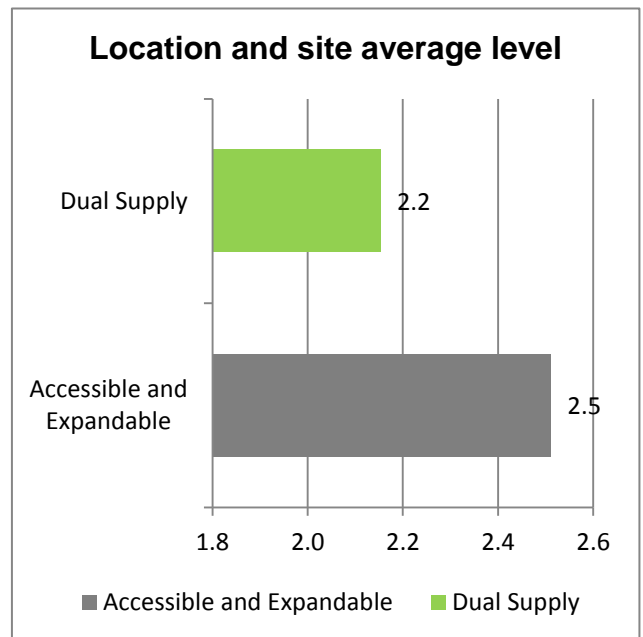
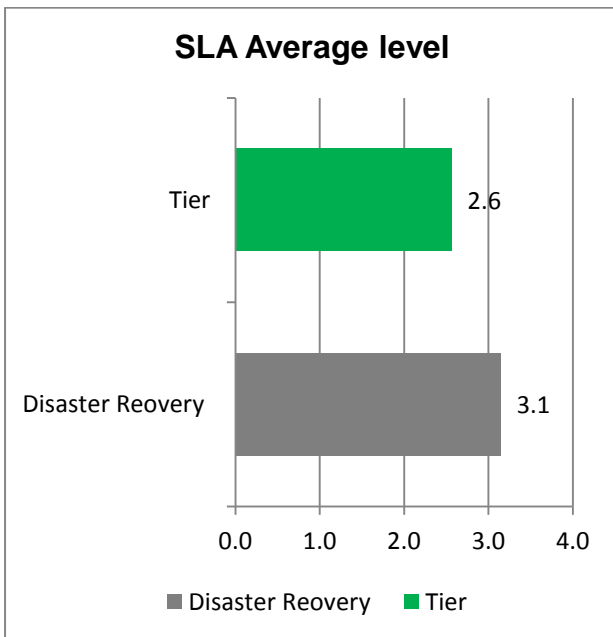
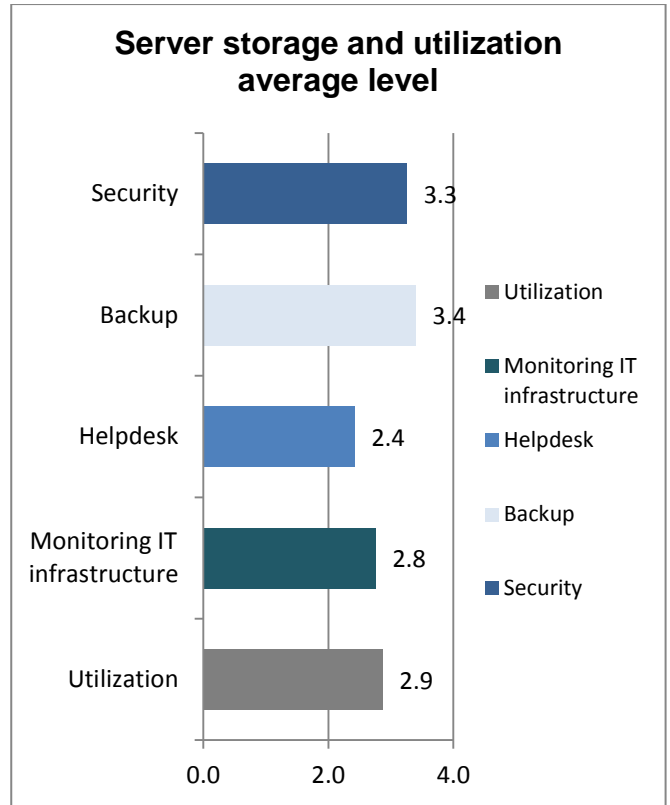
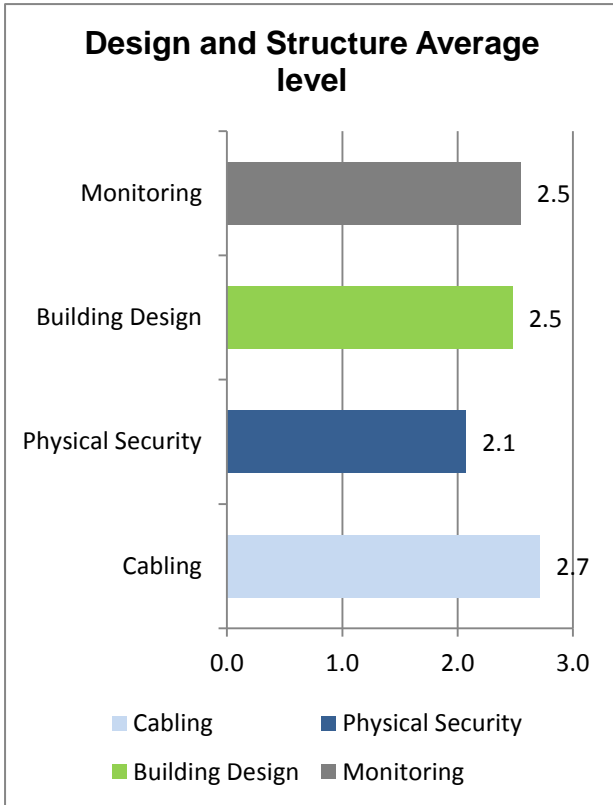
- Adopting standards is a cost intensive and effort intensive process.
- Long List of data center standards to choose from.
- Lack of people with complete understanding of standards
- Budget is big issue for standards adoption
- Data center operators are not experienced enough

- Lack of knowledge at a bureaucratic level on the importance of adopting standards
- Lack of people who have full understanding of various standards and their implications
- Many data center operators are still using legacy infrastructure

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.





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:	1 hour	80% in 1 WD
<ul style="list-style-type: none"> · 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. 		

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.	4 hours	80% in 4 WD
This is the default priority level assigned to faults. Note: All calls logged by fax or email automatically become Priority 3 or lower.		
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	<ul style="list-style-type: none"> 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

<p>Power</p>	<p>Maintenance of the uninterruptible power supply system. Maintenance of the back-up generators and related systems Connection to the electrical source</p>
---------------------	--

Agency Responsibilities

<p>Agency Support Agents</p>	<p>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.</p>
-------------------------------------	--

<p>Access</p>	<p>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.</p>
----------------------	---

<p>Ordering</p>	<p>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.</p>
------------------------	--

<p>Licensing Compliance</p>	<p>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.</p>
------------------------------------	---

<p>Rack Utilization</p>	<p>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.</p>
--------------------------------	---

FGA

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 date at 8:00 a.m. through XYZ date 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.

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%

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 for 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 X 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 X 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 X months.

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

Data center Standard adoption levels – Frost & Sullivan recommendations for Agency Data centers

Data Center Level

<p style="font-size: 48pt; text-align: center;">1</p>	<p>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.</p>
<p style="font-size: 48pt; text-align: center;">2</p>	<p>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.</p>
<p style="font-size: 48pt; text-align: center;">3</p>	<p>Level 3 Definition: At level three maturity data centers would 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.</p>
<p style="font-size: 48pt; text-align: center;">4</p>	<p>Level 4 Definition: At level four maturity data centers would 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.</p>
<p style="font-size: 48pt; text-align: center;">5</p>	<p>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.</p>

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.

Standards	Frost & Sullivan Future Recommended Level			
	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 chart that has been designed for the future standard adoption for government agencies. These are minimum standards that any agency should adopt and any agency having high security data should higher level of standards.

Appendix

Description for Average Level – Maturity Model for Data Centers

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	Thermal cameras in server room, Threat assessment conducted

				spaces	
--	--	--	--	--------	--

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 BISC1 or both	Data center would follow complete guide lines of TIA or BISC1 or both.	Data center has been designed as per LEED standard	
	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.	
Monitoring						
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	Data center must set a target for the usage renewable energy for power and make data center more connected
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