# Booklet 2 – Strategy (Draft)

# Contents

## 1. Executive Summary

Governments across the world perform complex functions to manage the country, state, city and society at large by driving internal operations, public facing services, policy establishment and decision making. Data infrastructure is a crucial pillar for success of any government as it forms the backbone of proper functioning of the government. Government data infrastructure includes the government assets include data that consists of public data that includes usage of personal data as well as data from the people and for the people; important data that helps govern the government services and highly important or secretive data that's important internal data for the country. The data infrastructure also includes elements that hold the data and handles them effectively for management of government services and functioning that includes government data centers as well as private infrastructure set ups.

Many government agencies have been working towards developing a Data Center strategy that supports the larger Digital Roadmaps for the country. They have embarked on programs that seek ways to modernize the existing Data Centers and develop IT facilities that are optimized in the digital age. Across the world including some of the most developed to under-developed nations, data center modernization has become a priority initiative to enable a stronger, flexible, long lasting, secured and cost optimised infrastructure. Today's government agencies struggle to maintain the delicate balance between the growing demand for technology services and tightening budget restraints.

Thailand is moving ahead in transforming itself into a digital leader aims to transform Thailand and to digitalize areas such as infrastructure, manufacturing, government services, businesses as well as several other sectors.Thai 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. The rising volume of electronic data, the growth in cloud opportunities and the need for secure and affordable large-scale data storage contribute to the increasing reliance on data centers at Thailand. Thailand will go through a massive need for data center infrastructure in years to come due to increase in data, population and economic growth.

Future state for Thailand Government's Data Infrastructure is defined as the new infrastructure setup that will be realized by realignment of government's vision and goal, it's data infrastructure strategy; hopes and needs of people and agencies; issues, risks and challenges that government will witness now and in times to come as well as current infrastructure setup. Thailand data infrastructure needs a modernization strategy to make it agile, secured, cost effective and efficient ecosystem. Future State for Thailand's Data Infrastructure Initiative called Government Data Center Modernization (GDCM) will have 5 salient features that differentiate it, from the current infrastructure and will be the building blocks for the future strategy- Security Handling, Scalability, Futuristic, Cost Optimisation and Operational Efficiency. Thailand Government's Data Infrastructure in future will be managed under Thailand Government Data Center Modernization (GDCM) Initiative that will oversee the implementation of GDCM Strategy over next initial 5 years (2017-2022). The Future Operating Model consists of 6 key areas of future operation for the data infrastructure: Agency Own Data Centers, Ministry Level Data Centers, Cross Agency Data Centers, 3rd Party Colocation/Hosting, 3rd Party Services and G-Services. Each Operating Model area will be operational based on current operating conditions and will be available to be embraced by the agencies based on their needs. Establishment of 6 models based on standards as well as strategy will ensure improved performance for agencies and reduced overall spending.

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. GDCM plan also includes implementation and utilization of identified standards across 5 domains namely: Energy & Power; Design and Structure; Server, Storage and Utilization; Location and Site Space. The standards and SLAs across these 5 areas (19 identified elements) will enable adoption of highly standardised infrastructure.

Over the course of next 5 years, it will be expected for most of the agencies to have considered adoption of ways and means to improve their data infrastructure and to have met the set objectives and goals by the government.The performance indicators for GDCM strategy implementation would include: asset and capacity utilization; HR utilization; Shared services; Cost Optimisation; Security and Strategic Framework. GDCM Strategy Implementation will underpin accountability, growth of Thailand, improved capability, innovation and collaboration.

With 5 year of total implementation of the strategy, the implementation is divided over 3 phases:

- Phase 1-Readiness to cover across 1 year and focus on readiness of government and agencies for the transformation
- Phase 2-Adoption to cover 2 years of effort on adoption of GDCM plan
- Phase 3-Improvement to cover across 2 years of effort on rapid adoption after the base is set and monitoring and improving the implementation.

As a part of GDCM strategy implementation 9 projects are identified to enable management as well as swift implementation of GDCM, namely: iDiscover, iTransform, iOptimize, iTransition, iAdopt, iChange, iLearn, iMonitor and iNegotiate.

With the implementation of GDCM strategy, Thailand data infrastructure will emerge as a strong, standardized, cost optimized, agile, secured and efficient ecosystem that is designed for future.

## 2. Background

Multiple forces have driven government agencies across the world to focus on Data Center Modernization in the last decade. From a technology standpoint, today's Data Centers must support provisioning on demand, scalability, virtualization and the flexibility to respond to fast changing requirements and operational situations. From an environmental perspective, they face pressure to optimize power consumption and reduce carbon footprint. Further, from an economic standpoint, there has been an enhanced focus on maximizing returns from existing assets. As more efficient use of IT assets becomes a priority, the need to align the data center's facilities and IT processes becomes greater to maintain uptime, coordinate complex integrated systems and deploy shared resources

Many government agencies have been working towards developing a Data Center strategy that supports the larger Digital Roadmaps for the country. They have embarked on programs that seek ways to modernize the existing Data Centers and develop IT facilities that are optimized in the digital age While the primary objectives of Data Center programs vary, rom driving significant improvements in reliability, efficiency, operational effectiveness to cost savings, or that of augmenting new layers of security, intelligence and automation – Data Center stakeholders realize that such initiatives will be critical to supporting the larger objectives of the government.

Data center Modernization is emerging as a key need among government agencies globally. Some of biggest drivers for the modernization are the cost saving and overall improvement of efficiency in the government delivering services to its citizens.

**South Korea:** The South Korea was one of the first countries which saw the inefficiency early on and formed a government agency that would develop central data centers for the government agencies. Country formed two central data centers between 2005 and 2007. The consolidation continued till 2011.

**United States of America:** United States started its consolidating its data centers in 2010, under FDCCI ((federal data center consolidation initiative). The initiative was estimated to drive a cost saving of more than $2 billion dollars through datacenter consolidation between 2010-2015. Government replaced the FDCCI with DCOI (data center optimization initiative) in 2016.

**UK:** The UK government has launched the initiative to consolidate disparate government IT storage and data center technology into a single managed provision solution. The whole exercise would help UK government to save around 105 million pounds.

**Australia**: The government of Australia hopes to save up to $1 billion by centralizing all its data center services, a project that will extend through 2025. Phase one of the consolidation plan includes aggregating demand for data center space and defining the standards to be used in procuring equipment and floor space. The second phase will see government departments sharing solutions and technology and the third phase will show adoption of new opportunities in technology, processes or policy.

**Singapore:** Singapore government has been a private cloud user since 2012 and the company has been hosting its entire infrastructure in third party data centers. Singapore government uses Singtel data centers to hosts the private cloud and it is also managed by the SingTel only.

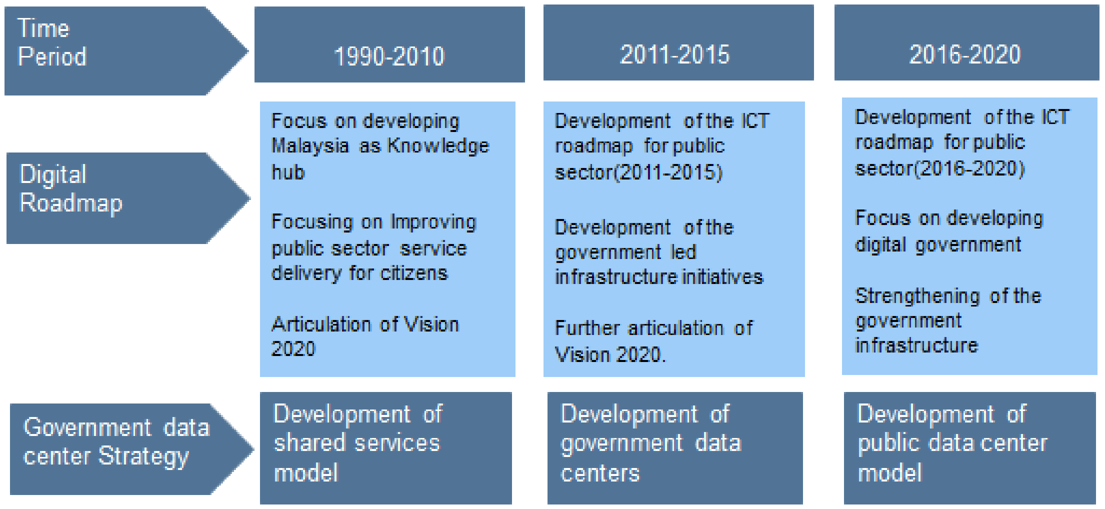
**Canada:** SSC (Shared Service Center) will consolidate 485 government data centers into seven. These modern and efficient facilities will be designed to evolve to meet the ever-changing needs of citizens, government and technology. This consolidation will reduce the government's data center footprint from 600,000 square feet to 180,000 square feet. From 23,000 servers to 14,000 severs.

**Hong Kong**: The Hong Kong Government have early on realized the value of data centers and the economic value that it adds to the economy. The country has developed several economic zones, where data center can be easily opened. Government in initiated he blueprint for data center consolidation.

**Malaysia**: Malaysia plans to move towards making public sector completely digital by 2020. Malaysia envisaged consolidating the data centers in 2011, as per their ICT plan 2011-2015. Government opened three government data center by 2015 and multiple agencies were provided the required data center services from it. By 2020, Malaysia expects to move all the agencies to the centralized data center environments

## 3. Data Center Modernization-Country Benchmarking

**Malaysia Data Center Modernization**



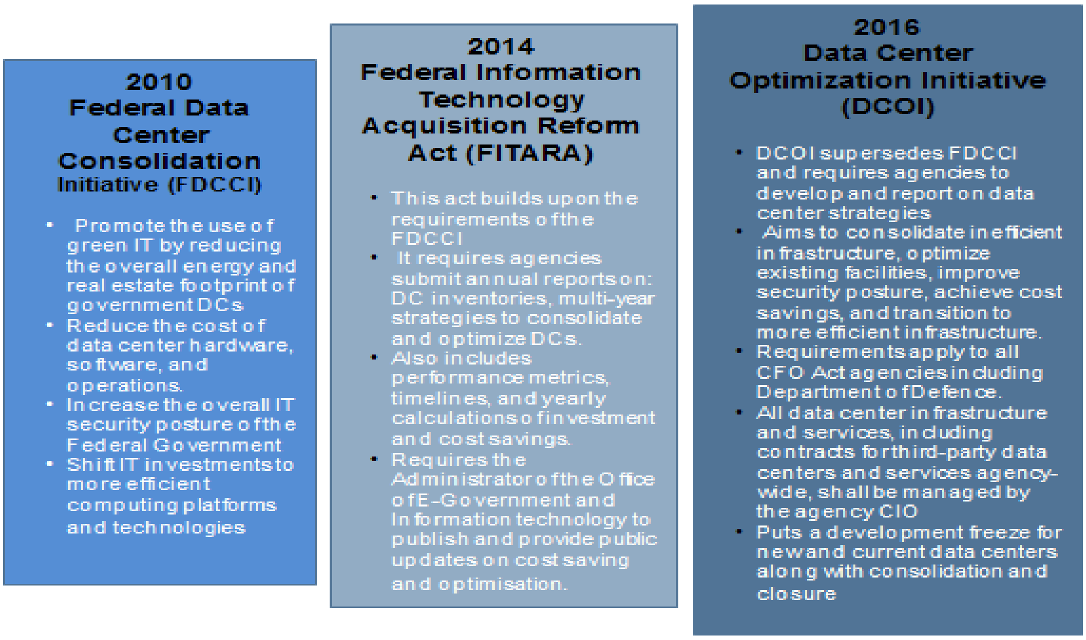
| Time Period | 1990-2010 | 2011-2015 | 2016-2020 |
|---|---|---|---|
| Digital Roadmap | Focus on developing Malaysia as Knowledge hub<br>Focusing on Improving public sector service delivery for citizens<br>Articulation of Vision 2020 | Development of the ICT roadmap for public sector(2011-2015)<br>Development of the government led infrastructure initiatives<br>Further articulation of Vision 2020. | Development of the ICT roadmap for public sector(2016-2020)<br>Focus on developing digital government<br>Strengthening of the government infrastructure |
| 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.



**2010 Federal Data Center Consolidation Initiative (FDCCI)**

- Promote the use of green IT by reducing the overall energy and real estate footprint of government DCs
- Reduce the cost of data center hardware, software, and operations.
- Increase the overall IT security posture of the Federal Government
- Shift IT investments to more efficient computing platforms and technologies

**2014 Federal Information Technology Acquisition Reform Act (FITARA)**

- This act builds upon the requirements of the FDCCI
- It requires agencies submit annual reports on: DC inventories, multi-year strategies to consolidate and optimize DCs.
- Also includes performance metrics, timelines, and yearly calculations of investment and cost savings.
- Requires the Administrator of the Office of E-Government and Information technology to publish and provide public updates on cost saving and optimisation.

**2016 Data Center Optimization Initiative (DCOI)**

- DCOI supersedes FDCCI and requires agencies to develop and report on data center strategies
- Aims to consolidate inefficient infrastructure, optimize existing facilities, improve security posture, achieve cost savings, and transition to more efficient infrastructure.
- Requirements apply to all CFO Act agencies including Department of Defence.
- All data center infrastructure and services, including contracts for third-party data centers and services agency-wide, shall be managed by the agency CIO
- Puts a development freeze for new and current data centers along with consolidation and closure

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.

Data centers are ever-evolving and integrate with a widely interconnected and increasingly virtual IT infrastructure. Data and data storage continue to be optimized in the digital age. Government agencies are lightning their data loads within data centers to make information more accessible through the cloud as well as using data centers for off-site security. The digital economy is creating large volumes of data thanks to large number of connected devices, smart machines and cloud-powered services. Intelligence and insights gathered from this data are being used to fuel innovation and creativity in new ways. The modern data center is powering this innovation and creativity at levels of scale that have broad impact across business, education and government. Modernizing data centers establishes the backbone for business transformation.

These are three areas of immediate opportunities for Modernization

1) Modernizing the IT infrastructure for utilizing opportunities cloud deployments
2) Optimizing applications and current legacy data centers
3) Ensuring and safeguarding the information and data

As more efficient use of IT assets becomes a clear and pressing priority for IT organizations, the need to align the data centers' facilities and IT processes becomes greater to maintain uptime, coordinate complex integrated systems and deploy shared resources reliably. In particular, some of the key mechanical, electrical and plumbing (MEP) components that data centers rely on, are not designed to last that long. In addition, rapidly changing data processing requirements demand that data remain flexible and support greater rack densities. Organizations with a data centers that are 10 years of age or older have several options: building a new data center, putting applications in the public cloud, leasing space in a colocation facility or modernizing the existing data center.

Many government agencies continue to cycle through a gradual transition away from distributed data center architectures to even more centralized sites—and, in some cases, those that are gradually more localized. In part, this means IT strategies are moving out beyond consolidation plans to focus instead on improving and updating facilities where assets have already been centralized.

Modernization efforts go a long way in supporting the needs of mission-critical IT assets as the risk of downtime becomes more stringently unthinkable. Many agencies are looking to make the most of previous investments also choose to modernize their existing facilities, as it can often be done more cost-effectively than the other options and usually yields significant improvements in reliability, efficiency and operational effectiveness. Retrofitting can also help provide powerful new layers of security, intelligence and automation.

As any governmental agency will confirm, maintaining legacy IT has a series of pros and cons — but mostly cons that can result in expenses resulting from high operating costs to inefficiencies and security vulnerabilities. These expenses could be attributed to the government working with systems that are aging and incompatible with modern security solutions.

**Business leaders of government agencies face the difficult challenges of delivering more IT infrastructure and services with critically limited staffing and budget resources.**

Agencies across the board compete for additional compute power to run more and larger workloads. Users in every discipline appeal for greater storage capacity to handle increasingly massive datasets. Security requirements place added burden on systems and administrators.

# 4. Strategic Approach

## Government Data Center Modernisation

Data Center Modernisation is an objective approach, to develop the data handling capability of the government to enable fulfilling the government set objectives by the aid of better IT infrastructure and support.

Across the world, each country has a strong data center backbone that supports the government machinery in running it smoothly. In today's digital economy, governments and their agencies can stay updated by accelerating application and IT service delivery. A modern data center infrastructure brings the right balance of compute, to help them thrive, than just survive. Some of the technologies driving data center modernization include cloud computing, flash storage, virtualization and software-defined networking. IT departments are under more pressure than ever to deliver increasing value back to the business. In addition to responding to day-to-day operational challenges, IT is being asked to define an efficient path to new deployment paradigms, including server virtualization, cloud computing, and ultimately, a software-defined infrastructure. Data Center Modernization enables IT decision-makers to better meet business needs for greater performance, security, networking, storage, and software efficiency advantages—all while lowering operating expenses. Governments consider the benefits of IT modernization through the lens of infrastructure modernization technology benefits, including better performance, efficiency, and security.

**Definition**

Data center modernization is the organizational decision to restructure how data is captured and stored within a company based on organizational needs, economic trends and new technologies available.

## Government Data Center Modernization (GDCM): Global Approach

Today's government agencies struggle to maintain the delicate balance between the growing demand for technology services and tightening budget restraints. Whether the challenge is in the area of digital forensics, online services, disaster recovery or more, the data and demands keep growing and becoming more complex by the day. The legacy IT investments are becoming increasingly obsolete due to maintenance of outdated software and hardware. Not only are these legacy systems costly to maintain by government agencies, but they are also increasingly vulnerable to cyber threats.

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. Many of these challenges can be directly correlated to outdated IT systems, and the results are leaving state and local organizations unable to innovate, limiting the citizen service delivery and opening the door to potential cybersecurity threats. The use of often duplicative legacy systems not only wastes scarce resources, but it also increases IT complexity for agencies. Government organizations are moving away from the culture enabled by legacy systems' traditional, limited operations and begin sharing information.

## 5. Thailand: ICT Plans

Today, information and communications technology (ICT) is increasingly a part of daily life and a driver of inclusive economic growth, social stability, and sustainable development. Thailand is moving ahead in transforming itself into a digital leader. In order to accelerate the transformation, new digital trends such as big data, the internet of things, social media, mobile advertising and cloud computing are reshaping the way people interact with each other and transforming the business landscape. Thailand Government is focusing on the Digital Thailand vision to enhance competitiveness of various industries in the country and position Thailand as the digital leader in ASEAN.

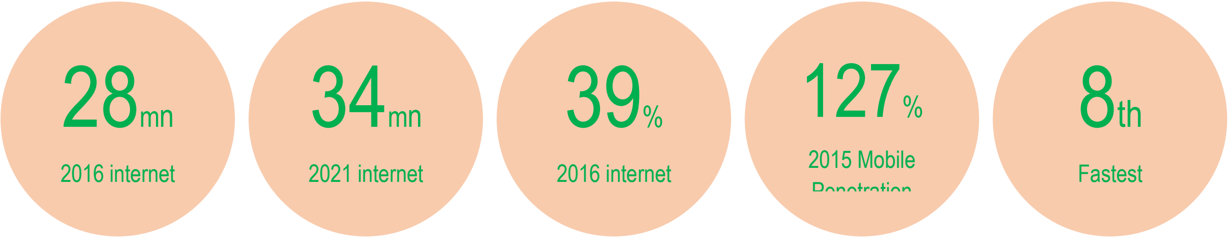
Digital Thailand is defined as a transformed Thailand that maximizes the use of digital technologies in all socio-economic activities to develop infrastructure, innovation, data, human capital and other digital resources that will drive the country towards wealth, stability and sustainability

According to the United Nations E-Government Survey 2016, Thailand ranks 77th out of 193 countries and territories in the e-government development index, up 25 places compared to 2014. In ASEAN, Thailand’s e-government development index is ranked fourth.

*Thailand’s overall information and communication technology (ICT) spending was estimated to reach $21 to 20.5 billion in 2015, accounting for 7% of the country’s GDP.*

Growth in the ICT sector will be stimulated by the government’s plans to create a digital economy. The Ministry of Information and Communication technology (MICT) also plans to build a regional internet gateway by adding more submarine cable lines to accommodate growing usage and also become an internet connectivity hub in ASEAN by 2020. Investing in the country’s submarine cable lines connecting from India to Thailand and to Hong Kong, will attract more internet traffic from the Great Mekong sub region which is currently servicing 270 million people. The Government has a plan to embrace the adoption of digital technology for economic and social development. The transformation into the digital economy is seen as an important step in the modernization of the Thai economy by allowing the use of ICT technology to manage businesses and provide services. The Government is also improving ways to provide services and transactions electronically.

In Thailand, there were around 40 million smartphone subscriptions in 2015. The number of smartphone subscriptions in Thailand is expected to double by 2021. The increase in smartphone subscriptions will fuel the growth of mobile broadband in Thailand. Smartphone subscriptions were close to 60% in 2016 and by 2021, it is projected to reach 80% of the total mobile subscriptions.



*Sources: Stastica, Worldbank, Bangkokpost, NBTC*

As of 2015, Thailand and Singapore were the only two countries in South East Asia with over 100% mobile broadband subscription. Mobile broadband subscriptions penetration reached around 120% in Thailand in 2015 and is expected to reach around 160% by 2021. The Ministry of Information and Communication Technology has come up with a digital landscape, covering the next 20 years, with a view to developing the country into a fully digital Thailand.

## National Digital Economy Master Plan (2016-2020)

The Thai Government's objective of building a Digital Economy and Society for Thailand is one of the most ambitious and important short- and long-term initiatives for shaping the future of the country. The emergence of Digital Thailand will have direct benefits in the areas of GDP growth and broad-based socioeconomic prosperity and inclusion; labour productivity and employment; and competitiveness within the ASEAN Economic Community and beyond. To drive further digital innovation and create new business opportunities, the Master Plan lays out a long-term strategy that involves the development of infrastructure, workforce and other resources to serve rapidly evolving public and business needs.

*The six areas highlighted in the plan include Hard Infrastructure, Soft Infrastructure, Service Infrastructure, Digital Economy Acceleration, Digital Society and a Digital Workforce.*

The government plans to work in cooperation with the private sector to improve Thailand's hard infrastructure, so that it is capable of supporting a digital economy. The Digital Thailand plan will also create new opportunities for other types of businesses, including Start-ups and SMEs, which will get support from the establishment of incubation centers and e-commerce knowledge sharing programs. Moreover, business related to e-commerce platforms or logistics will stand to gain from the rise in demand for the delivery of goods that will result from a fast growing e-commerce market.

## Thailand Digital Government Plan 2017-2021

The plan aims to develop digital capabilities within all sectors, including agriculture, tourism, education, the medical profession, investment, disaster prevention, and public administration, in order to drive economic and social progress. To achieve this objective, digital technologies need to be incorporated into public services.

There are 5 focus areas of Thailand Digital Government Development Plan 2017-2021

1  Enhancing citizen quality of life
2 Raising business competitiveness
3 Strengthening citizen security and safety
4 Enhancing government efficiency
5 Integrating and fostering Digital Government Infrastructure

The Vision of Thiland Digital Government plan is to "Drive Thailand's government towards becoming Digital Government with Integration among agencies, Smart Operations, Citizen-Centric Services and Driven Transformation"

In Thailand Digital Government Development Plan 2017-2021, Strategy 4- Government Efficiency Enhancement aims to integrate and enhance the efficiency of government operations through cross-agency connectivity in order to boost government digital capabilities in management, finance and spending, procurement, assets management, human resource and payroll, resulting in providing the government operations with convenience, speed, transparency as well as building blocks towards becoming complete Digital Government.

Strategy 5 - Integration and Enhancement of Government Digital Infrastructure aims to consolidate government services through cross-agency connectivity and developing government electronics services infrastructure together with fostering digital skills for government employees at all levels and agencies, as a result establishing a foundation for gearing government agencies towards being complete Digital Government."

Government Data Center Modernization (GDCM) will be a strong pillar in enabling Strategy 4 and Strategy 5 on enhancing government efficiency and Intergrating digital government infrastructure. GDCM will enable better utilisation of government infrastructure and resources, increase in data center infrastructure efficiency, modernise the infrastructure to meet the demand for future and foster a long term sustainable environment of digital government infrastructure.

### Thailand Smart Cities

As part of the government's digital economy policy, Phuket will be transformed into a 'Smart City' this year, with Chiang Mai slated to be the same in 2017. The move is expected to attract technology start-ups to these cities, enhance digital-related investment, improve the standard of living for residents, and boost the tourist industries in the 2 cities. The government has allocated

THB 97 Million to turn Phuket into a smart city; this is part of the broader 'Smart Thailand initiative that seeks to transform the country into an ASEAN digital hub. Developing Smart Cities in Thailand is a key point in the government’s plan to adapt towards a digital economy. Eventually, the goal is to develop smart cities across Thailand, but do so in a way that allows provinces to adapt its development according to its economic needs.

## 6. Thailand: Ministries and Agency Overview

The Government of Thailand consists of ministries, bureaus, and departments. Each of the ministries and bureaus is led by a minister who is a member of the Council of Ministers A bureau may be an independent agency with the same status as a ministry or may be subject to a ministry. The ministries and bureaus are divided into departments; each department is led by a director general. There is a central government agency called Office of the Prime Minister, led by the prime minister and bears ministerial status

There are also independent central government agencies. These agencies are not under any ministry, bureau, or department, but are directly subject to the prime minister. They are:

- Bureau of the Royal Household
- National Research Council of Thailand
- Office of His Majesty's Principal Private Secretary
- Office of National Buddhism
- Office of the Royal Development Projects Boards

- Royal Institute of Thailand
- Southern Border Provinces Administration Center

The Cabinet Ministries of Thailand are the government agencies comprising the executive branch of the Government of Thailand. Each ministry is headed by a Minister of State and eventually, several Deputy Ministers. The present structure of the Royal Thai Government has been the same since the Administrative Reorganisation Act, BE 2545.
The cabinet includes 19 ministries plus the Office of the Prime Minister (OPM). The ministries, OPM, various ministry agencies managed by the ministries and other independent agencies form the management backbone for Thailand government machinery.

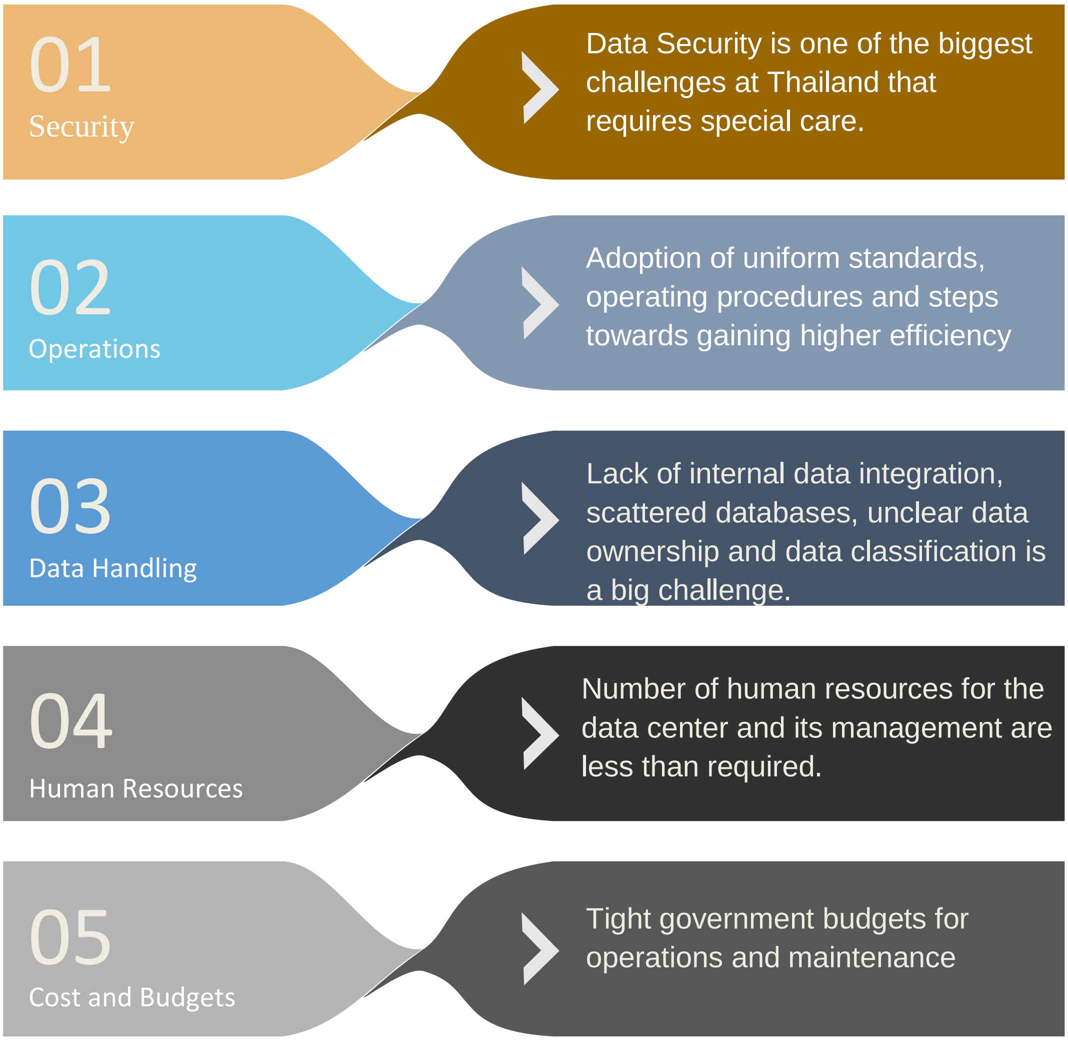
| | | | |
|---|---|---|---|
| Office of the Prime Minister | Ministry of Defence | Ministry of Finance | Ministry of Foreign Affairs |
| Ministry of Tourism & Sports | Ministry of Social Development and Human Security | Ministry of Agriculture and Cooperatives | Ministry of Transport |
| Ministry of Natural Resources and Environment | Ministry of Digital Economy and Society | Ministry of Energy | Ministry of Commerce |
| Ministry of Interior | Ministry of Justice | Ministry of Labour | Ministry of Culture |
| Ministry of Science & Technology | Ministry of Education | Ministry of Public Health | Ministry of Industry |

*Fig 1: Thailand Government Ministries*

## 7. Key Issues and Challenges

The rising volume of electronic data, the growth in cloud opportunities and the need for secure and affordable large-scale data storage contribute to the increasing reliance on data centers at Thailand. In the past, managing a data center was easier process while agencies planned for the foreseeable future. But due to the inexorable trend of processing more and more data, the management of these facilities grew in complexity. Complicating the situation, operational decisions at the data center include data integration, data quality, sharing, utilization, power, cooling, rack space, storage utilization etc. This is in addition to other complex issues for standard adoption and facility improvement.
Thai agencies face many of the same basic challenges across the spectrum, including security concerns, compliance standards and increase in size of data. By virtue of being government organizations, these agencies need to be extra careful in planning and executing their strategy as well as budgeting

Our analysis reveals the top 5 challenges that the Thai agencies are facing in the current operating environment.



01 Security

Data Security is one of the biggest challenges at Thailand that requires special care.

02 Operations

Adoption of uniform standards, operating procedures and steps towards gaining higher efficiency

03 Data Handling

Lack of internal data integration, scattered databases, unclear data ownership and data classification is a big challenge.

04 Human Resources

Number of human resources for the data center and its management are less than required.

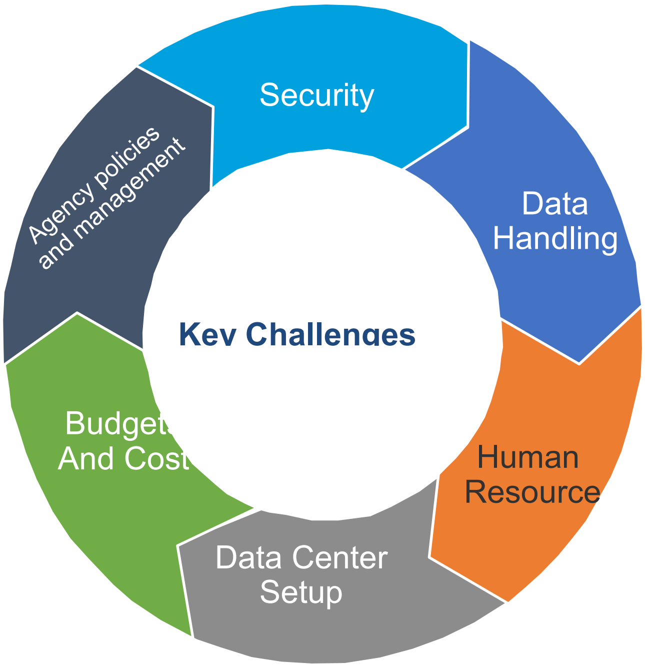
05 Cost and Budgets

Tight government budgets for operations and maintenance

*Fig 2: Challenges faced by Thailand agencies*

In current times, the ICT teams of the agencies are increasingly under pressure to solve their critical data storage challenges, avoiding hardware issue and continue to deliver services in a cost-effective way to end-users.

The below analysis buckets the key challenges that are faced by Thai agencies into 6 core areas:



- 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.
- Data Center Setup include: server, storage, cabling, cooling setup, power setup, floor architecture, racks, building design etc.
- 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.

### Security

- Handling secured data and maintaining security based practices and to ensure that mission critical data is handled effectively was identified as one of the most important challenges that agencies are facing collectively.
- 30% agencies identified security handling as an important challenge that they are facing currently.
- Agencies identified that as the size of data is increasing, there is increasing pressure on managing security which makes it hard to balance. With the increase in cyber warfare, external attacks and risks of handling classified data, security handling has become a large challenge.

### Data Handling

- 54% agencies recognised data handling as one of the big challenge across the agency infrastructure.
- The integration of data between the agencies and ministries, non-alignment on the ownership of data, scattered databases, requirement for data cleansing, non-electronic data, poor classification, accuracy and integrity of data etc were found as the key issues in data handling.
- Agencies identified that the data and information is scattered across various divisions with ICT as admin for information lying in the same agency as an important area of concern.

## Human Resources

- 28% agencies identified that Human Resource issues as an important challenge that deters in their current operations.
- Agencies identified that the human resources in their data center are limited or are in short supply, primarily because the hiring decisions were taken few years back after which the data and the size of infrastructure increased considerably.
- With limited budgets, increasing the size of human resources is not always possible which creates burden on existing resourcing.
- Availability of new skilled staff due to shortage of trained workers is another challenge that's hindering the quality of support.
- Many agencies identified that the limitation of human resources is partly due to personnel structure limitations, high churning of the IT professional and lower compensation in government jobs as compared to private companies

## Data Center Setup

- 26% agency respondents feel that the key data center elements including the servers, systems, storage and other elements of infrastructure pose a burden on their agencies due to various factors.
- The most important challenge in data center setup includes standards usage and steps towards efficiency that are often required and communicated but lack of standardisation hinders the adoption.
- The misalignment between the agencies, ministries and cross ministries on standard adoption creates a challenge for the agencies.
- Data center setup challenges also include: aged IT systems that require higher maintenance and result into higher cost of operations, increased requirement of size/servers and other improvement works required to host increase in data, improper electrical, cooling and other architectural issues, lack of space, migration issues etc contribute towards key challenges.

## Budgets and Cost

- 18% agency respondents think that budgets and cost is one of the important challenges that their agencies are facing.
- Tight government budgets in line with the increasing requirements create issues like quality and service level adherence is an increasing challenge.
- Increase in cost due to increase in maintaining staff, electricity charges, maintenance of security, skilling the staff, handling higher quantity of data, increasing user demands, wastage and lower utilisation of IT resources causes further issues in running the agency operations effectively.

## Agency Policies and Management

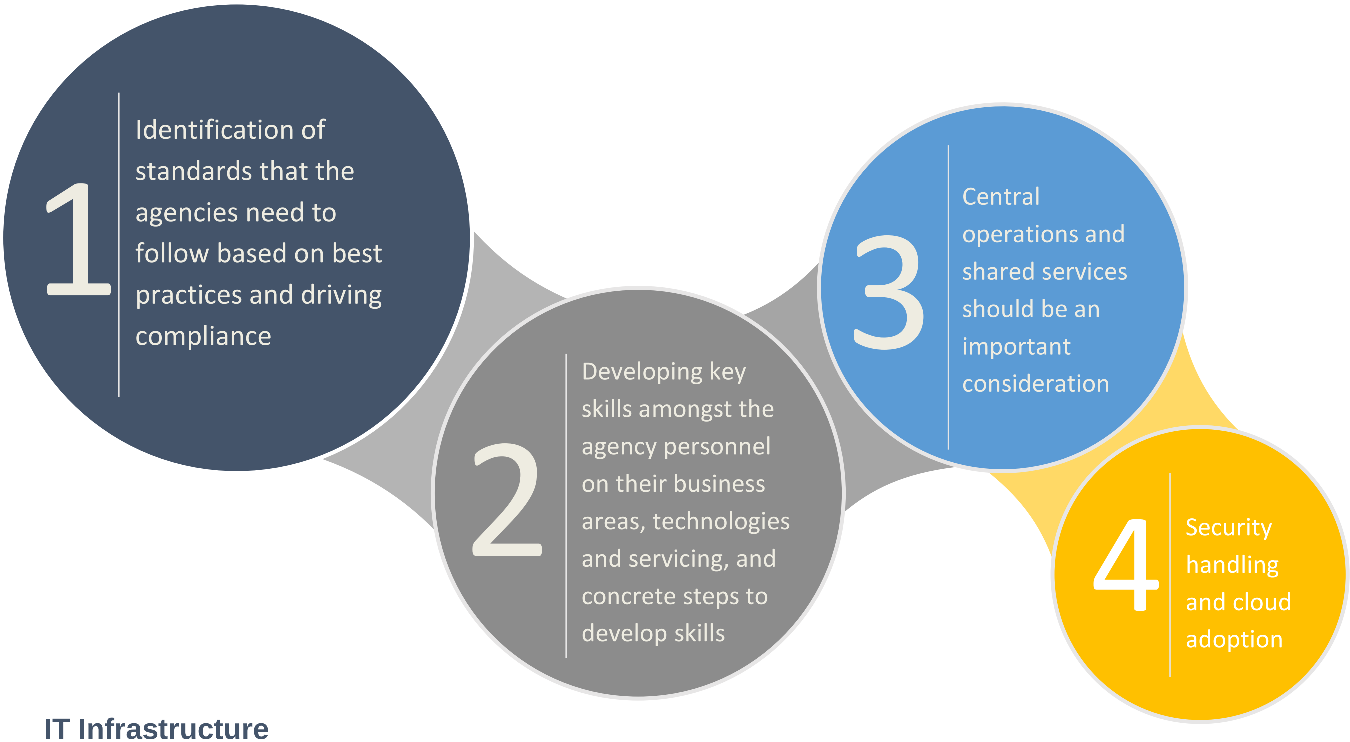
- 25% agency respondents think that agency policies and management play an important role in effective management of the data center
- Major concerns include: non comprehensive backup and DR, non-sharing of their resources to increase the utilization and agency policies.
- Lack of citizen centric approach and inability to serve the users better due to high volumes of data and lack of planning is a growing challenge faced by the agencies.
- Network issues and buildings that require improvement and are working with older infrastructure are other key challenges as noted by agencies.

## 8. Current State of Government Infrastructure in Thailand

### Current Infrastructure

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:



1 Identification of standards that the agencies need to follow based on best practices and driving compliance

2 Developing key skills amongst the agency personnel on their business areas, technologies and servicing, and concrete steps to develop skills

3 Central operations and shared services should be an important consideration

4 Security handling and cloud adoption

### IT Infrastructure

Agency IT resources including the servers, storage, other peripheral devices, software etc are expensive and important preposition. IT infrastructure including network infrastructure is estimated to account for  65% of the total cost spent as capex (excluding  the cost of site purchase) With high expenses, it's important to utilise the last drop of the infrastructure to enable an effective performance as well as best utilisation of resources. It is crucial for agencies to implement strategies to convert inefficient infrastructure into efficient services and to optimize existing facilities by improving security handling, and achieve cost savings. One way to do this is to transition to more efficient infrastructure, such as cloud services and inter-agency shared services.  Agencies can use alternative arrangements where possible when planning new applications or support applications or moving existing applications by taking into consideration the cost, elasticity, and resiliency benefits of provisioned environments.

Thai agencies DCs are reported to work on low utilisation rates and 51% agency representatives believe that their agencies are not working at optimised utilisation levels.

Agencies identified various reasons for poor utilisation:

- Inability of IT teams to utilise the infrastructure properly
- Low budget that’s utilised on usage and maintenance for day to day operations
- Unutilised applications and data, lack of measurement systems and processes
- Lack of planning to support future demand
- Poor procurement planning without feasibility analysis
- Fulfilment of allocated and remaining budgets
- Shorter lifecycle of equipments

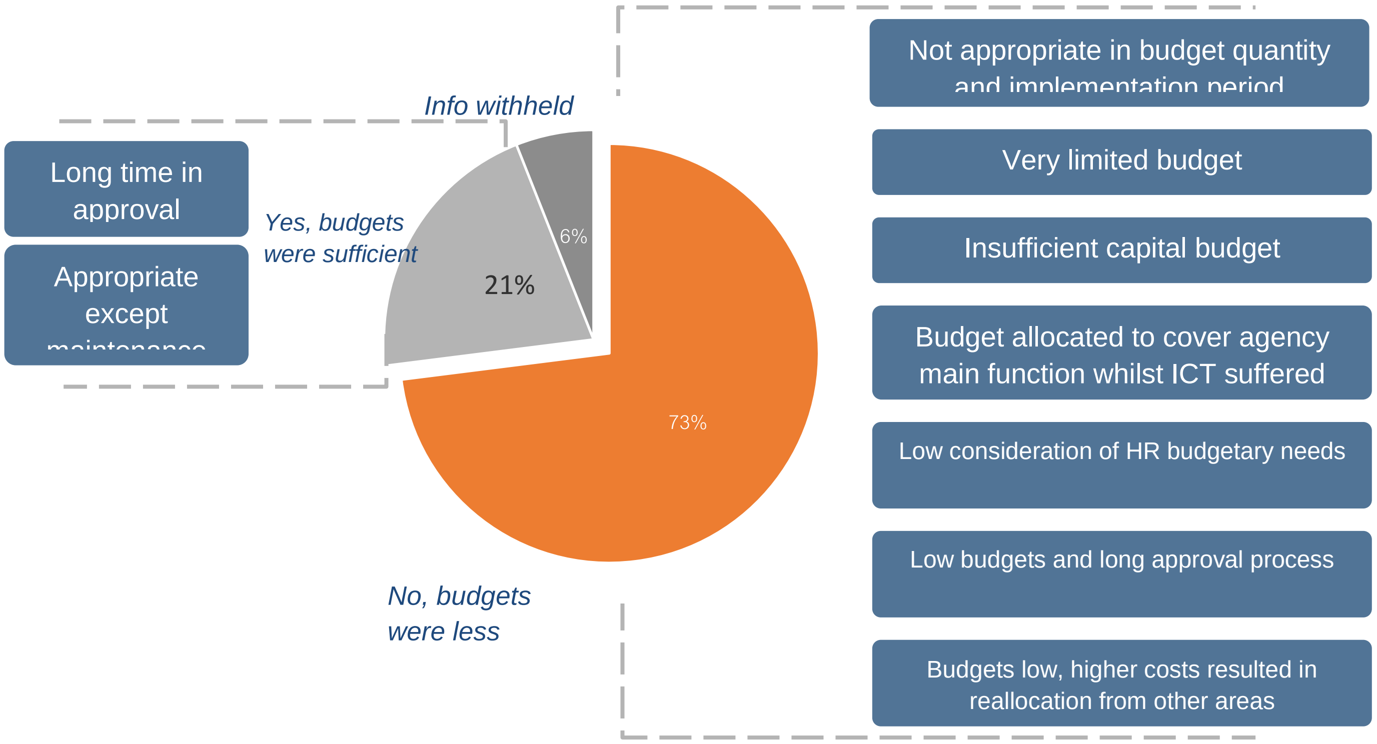
### Key Takeaways

- Currently, a lot of agencies are operating with lower utilisation of their IT resources due to various factors including: lack of proper planning, lack of measurement, unutilised applications and data, lack of training etc.
- A modern infrastructure at a government level, must ensure high levels of utilisation of national assets, by all means to ensure available infrastructure to all agencies as required and to be able to allocate capital budgets and operating expenses sufficiently.
- Key takeaways for the future operating model should be to take steps to improve DC utilisation, cross-share the infrastructure, utilise other models to host data and improve agency level/server level utilisation.
- A standardised approach to achieve higher utilisation will ensure cost savings, better allocation of resources and informed planning for future needs.

### Budgets

Agencies identified availability of government budgets as an important deterrent in their operations.

Governments all over the world are spearheading initiatives to either reduce government budgets or to consolidate data center operations. With reduced budgets the operations of government IT infrastructure takes a toll and need to be relooked in order to operate effectively and efficiently.



### Key Takeaways

- Government budgets have been aggressive in past few years and apart from the need to handle budgeting exercise appropriately (that is out of scope of this initiative); there is a need to better manage the budget at an agency level.
- New ways to solve business issues and to conduct agency operations effectively needs to be considered and followed.
- A standardised approach that results in cost savings as well as better management of infrastructure is advised for future model.

## Human Resourcing

35 % of the agencies identified lack of capability and training as major issues for HR management followed by high churn rate of IT workers at 12%. Other reasons cited by the agencies for the low human resource capability are less attractive compensation provided by the government as compared to private companies, insufficient resources for 24X7 operations, staff insourcing risks and insufficient personnel for hardware, software and other IT roles.

## Key Takeaways

- Human resource challenges pose a serious risk to the operations of the government agencies specially the IT personnel for proper functioning of the IT operations.
- In line with lower Government budgets, and lack of availability of right skilled workers, lower salaries and high attrition, agencies need to consider various options to strengthen their business continuity.
- Agencies need to consider alternate arrangements for colocation, 3rd party services and government services to enable seamless operations for future model.

## Data Security

Data Security and data handling are identified as the key issues that need to be addressed well in order to maintain quality services as well as a harmonious government infrastructure at Thailand.

In an era where cyber warfare is the most widely preferred method of engagement, government data centers face significant threats not just from domestic but also foreign hackers. When it comes to security, government agencies are held to the highest standards as it is arguably the top priority - and that makes it major budget expense across the world. There are various challenges in keeping data secure, from the office workstation to the enterprise data center to the mobile devices that the employees have. Other challenges include current security solutions, including integration challenges, long provisioning cycles, performance shortcomings, fragmented solutions, and lack of security for their virtual machines. Security for the data center and cloud computing has to ensure not only the protection of north-south communications (those to and from the data center) but also east-west communications (those between virtual machines). Over the least five years, government networks have become magnets for breaches and attacks ranging from malware loaded onto host servers to network viruses.

Our analysis reveals that about 73% agency respondents feel that their agencies do have some or the other minor security issues that they face currently while 15% feel that their agencies do not handle high security data effectively. Security is recognised as the most important concern across the world while the government agencies across the world is battling against the myriad issues. Cyber security in general has been identified as a major concern though; there are increasing concerns over cloud adoption by the Thai agencies. Handling critical data appropriately under secured environment is an important issue for a few government agencies.

15%

*Agency respondents feel that their agency does not handle high security applications appropriately*

**Key Takeaways**

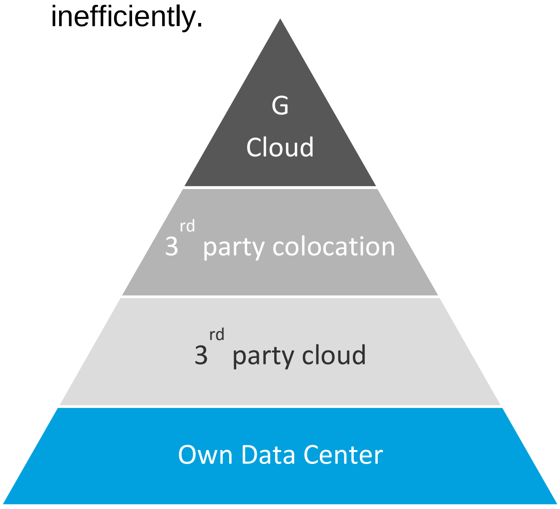
- Security is one of the major challenges for any government agency including Thailand.
- High security risks poses a risk on infrastructure security and classified data for the country
- Thailand GDCM should enable an infrastructure that is designed keeping in mind the security aspirations and need to operate in a secured environment
- The physical infrastructure must be supported by better security features, compliance and processes that should be standardised for future state.
- Data must also be kept by utilising various options based on appropriate security need for the national agencies.

## Agency Infrastructure and Data Handling

The agencies recognise the need to move towards a more efficient infrastructure. The current agency infrastructure comprise of Own Data Center, G-cloud, 3rd party colocation and 3rd party cloud. Out of the 42 surveyed agencies, 90% agencies claimed to be using their own data centers to store and process their data while 20% claimed to be using 3rd party colocation and G-cloud each and only 7% on 3rd party cloud.

Agency infrastructure is a very important element for proper functioning of government machinery. Apart from other infrastructure like data carriage services, VPN, communication network and other telecommunication services, the agency infrastructure includes data centers and the server it owns.

Thai agencies currently are managed via the 4 key data infrastructure elements, albeit inefficiently.



- The 4 pronged model currently supports the DC and data infrastructure of Thailand
- Own Data Centers are most widely used infrastructure area as the data stays within the agency from ownership perspective and security
- 3rd party cloud is an important area about 64 applications hosted on 3rd party cloud (2014).
- 3rd party colocation is also an important choice that agencies take for outsourcing the maintenance and operations while maintaining security with 300+servers colocated
- 109 reported apps are on G-Cloud (as of 2014)

### Own Data Center

The current agency infrastructure is highly skewed towards own data centers for the government agencies. Based on the data analysis from the data received from the agencies, nearly 92% agencies operated through their own data centers. Agencies feel that having an own data center provides them the agility in the business whilst maintains the security as well. Some of the agencies that provide financial data and have confidential contents, maintain their own DC. Agencies also feel that keeping data on the own dc helps them by not relying on other agencies for space sharing. Certain applications also cannot be supported by G-Cloud.

**Key Takeaways**

- Even though agency data centers are the most important element of agency infrastructure setup, agencies need to think on alternative ways to host their data.
- Own Agency Data center increases the security handling capability of agencies but also poses a risk on budget allocation, maintenance, failure, availability and reliability of the services.
- To meet the standardised guidelines, agency DCs need to spend significant cost to be able to witness the ROI of business improvements.
- The dated agency dc setup and aged servers and infrastructure poses a security risk as well as higher cost than required that is spent through government budgets.
- Any new investments to revamp the agency setup would mean a high capital expenditure.
- In nutshell, future state of the agency infrastructure should strongly consider opportunities from other areas especially where data criticality and security is not at stake.

## 3rd Party Cloud

The current agency infrastructure does utilise 3rd party cloud services with services from various Thailand based companies to support their applications.

**Key Takeaways**

- It's important to focus resources where there is a potential of maximum return (such as the value delivered to the stakeholders)
- It is essential that agencies look for scalable enterprise solutions, capable of accommodating increased user traffic and content through highly secure data-hosting operations
- 3rd party cloud does have higher concerns on security handling capability but are improving day by day in their services, technologies and security solutions.
- The benefits of virtualization—cutting costs, increasing flexibility, and saving energy are a stepping stone to cloud adoption.
- 3rd party cloud will enable the agencies to solve issues like: disaster recovery, software updates and purchase, scalability, capital expenditure, document control and security handling.
- Even though security may be a barrier for critical and national security data, a lot of non-secured data can still be moved to hosted solutions including cloud that can be handled at lower costs, highly available and reliable systems.
- Big advantage of 3rd party cloud is reduced focus on human resources and day to day operations which are a major concern for Thai agencies today.

## 3rd Party Colocation

Thailand agencies have various servers that are hosted at 3rd party players as co-located servers. 324 servers (2014) are collocated with various organizations. Colocation is considered as a very important and practiced area for Thai agencies. Many agencies clearly prefer 3rd party colocation as it provides facilities of both worlds: Higher security as well as limited effort requirements for operational management and human resources.

### Key Takeaways

- 3rd party colocation is a preferred option for various agencies to host their data.
- It is essential that agencies take a rational look in identifying which applications and servers can and should be hosted on 3rd party.
- Agencies also need to be well aware of SLAs that the 3rd party colocation companies are working on.
- 3rd party colocation does have some concerns on data security handling capability but it's lesser than the concerns that agencies have on 3rd party cloud.
- Colocation is a good option for agencies which have small server rooms or smaller infrastructure with a rapid requirement for a larger infrastructure or infra that requires higher handling of secured data or critical applications.

## G-Cloud

G-cloud is offered by EGA as an IT infrastructure area that can run remotely over network and ensures higher security and lesser costs of admin and human resources.

### Key Takeaways

- G-Cloud is emerging as an important area for Agencies to consider moving their applications.
- Data Security, reliability, availability are important challenges that G-cloud would need to address.
- G-Cloud will be an important area going forward as agencies feel that it will be a good option to reduce their maintenance costs, equipment procurement and that the agencies will be able to rely on the service quality promised.
- G-Cloud should also keep in mind the data classification and data integration.
- G-Cloud should have an evolutionary approach where they adopt standardised services to enable hosting of public data and move to higher standards of data in long term.
- G-cloud should also maintain long term sustainability, availability 24X7, customer support and all the features that are provided by 3rd party cloud at higher security handling capabilities and lower costs.

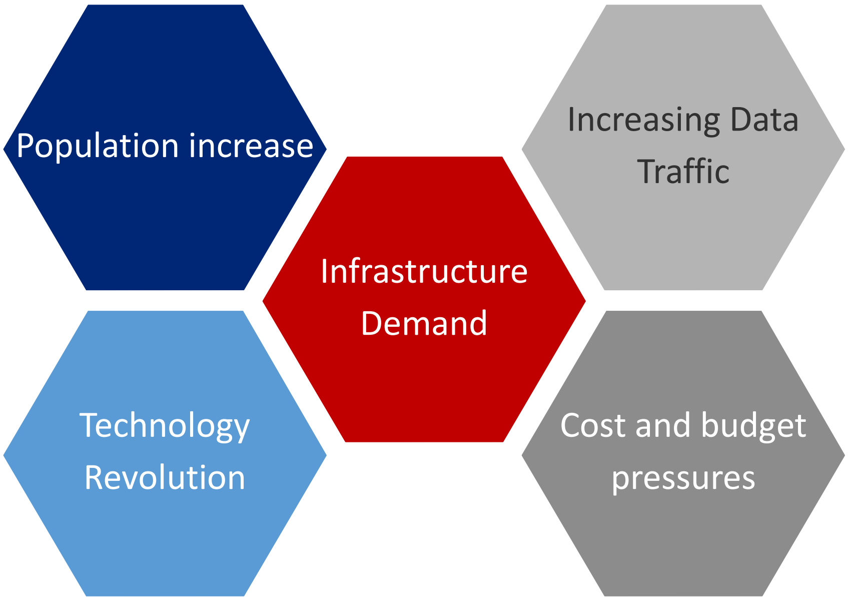
## 9. Future Data Infrastructure of Thailand

The Future State of any government enterprise, economy, and country or technology state is reflective of the path that the country has been set on and the growing trends and challenges that are witnessed in the market.

Thailand is at the cusp of revolution. With a stagnant GDP growth but continuous efforts to grow Thailand is a key indicator on the seriousness of the country to make it big on the world map. The improvement in Thailand's world competitiveness ranking as a good sign, reflecting the country's success in building the national economy and linking with the local economy. In 2016, Thailand ranks 28th among 61 economies. Its ranking in 2013 was 27th and dropped to 29th in 2014 and 30th in 2015. The country' total score for 2016 is 74.681, against 69.786 in 2015. Among the five ASEAN countries, namely Singapore, Malaysia, Thailand, the Philippines, and Indonesia, Thailand is the only ASEAN member that ranks better than its ranking last year. Thailand is accelerating large infrastructure development projects in terms of technology, public health, and the environment. Emphasis is placed on innovation and "green industry. Thailand has long been included with a group of economies in East and Southeast Asia, who, because of their outstanding growth performance, have been at the center of the research and discussion of the determinants of economic growth. Thailand's economic growth is lagging peers in South-East Asia, with the International Monetary Fund forecasting expansion of 3.3% this year.

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.



**Population increase**

Population growth at Thailand as like other countries will see higher demand for better digital infrastructure services, increased data analytics and expectations from the government This will intensify the efforts, cost as well as the investments required to manage and maintain the mammoth data center infrastructure. Choices need to be made around how to accommodate Thailand’s growth.

**Technology revolution**

Technology is accelerating faster than ever before, and will help shape demand for infrastructure as well as the choices for infrastructure provision. Future technological advances can assist us in combatting the challenges we face by helping us to both make better use of information (for example through smart devices, Internet of Things and sensors, and smart meters), better use of the infrastructure that we already have, while also potentially opening up new possibilities for infrastructure provision

**Cost and budget pressures**

With the growing cost of services right from electricity to human resources, the infrastructure service provision is growing expensive day by day. Growing cost of service provision is a global phenomenon that every country is grappling today. With budget pressures and delay in budget approvals as well as stringent purse, agencies will find it increasingly difficult to cope up in current circumstances.

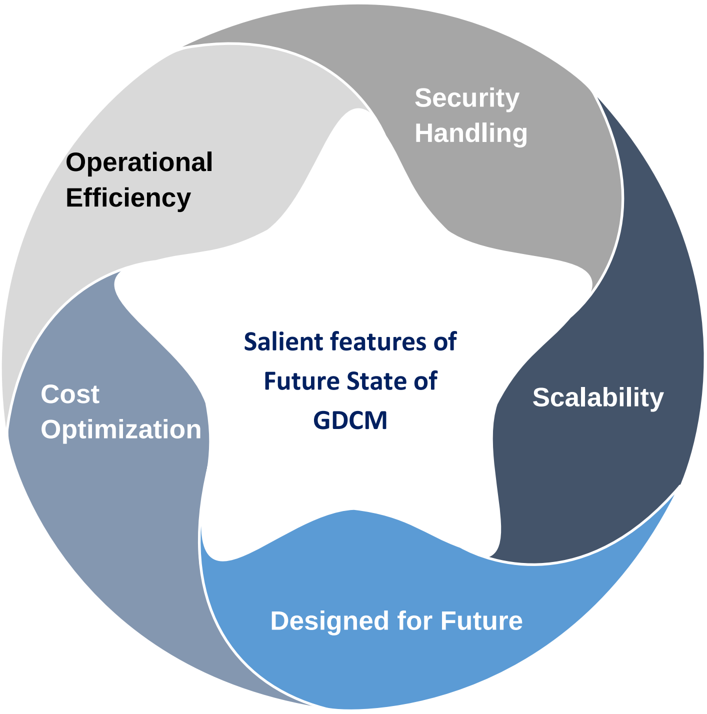
**Increasing data traffic**

Data is increasing multifold every year. Not just with increase in population but the sheer volume of data due to better digital infrastructure, connected devices, online applications and services, financial and business transactions, information exchange services and need of services and analytics is driving massive growth in data and the required infrastructure required to support it. With the current models of operation, it will become highly inefficient and costly affair to operate the government of the future.

### Maturity Parameters of future infrastructure

Future state for Thailand Government’s Data Infrastructure is defined as the new infrastructure setup that will be realized by realignment of government’s vision and goal, it’s data infrastructure strategy; hopes and needs of people and agencies; issues, risks and challenges that government will witness now and in times to come as well as current infrastructure setup.

Future State for Thailand's Data Infrastructure Initiative called Government Data Center Modernization (GDCM) will have 5 salient features that differentiate it, from the current infrastructure and will be the building blocks for the future strategy.



### Security Handling

One of the most powerful feature and a key requirement for future model, Security Handling is crucial for the future state of Thailand Government's Data Infrastructure.

Security Handling covers high security protection and usage of national security data, use of encryption and other secured technologies for data transfer, security coverage to mission critical data and important customer data and effective management of general data.

### Key Features in Future State

The future state infrastructure should follow the security standards as highlighted in the standards document that cover data security, cyber security and physical security.

Each future infrastructure area will be differentiated based on security handling capacity and capability.

The data needs to be classified and governed appropriately by the government agencies to take informed decisions on their future state of operations.

The future operations would spread across infrastructure that's highly updated, utilized secured data handling capabilities and operates with reduced risk

## Scalability

Data is everywhere. Data is big and it's getting bigger. Thailand's current state of data infrastructure recognizes the need for scalability. In last few years, the applications have grown as much as the infrastructure investments and data center setups. Currently, the data centers are operating at low utilization levels-space wise as well as system utilization. The key reasons for keeping higher capacity is scalability.

Scalability covers ability of the government ministries and agencies to be nimble by having options that can range across scalability parameters to host their applications on scalable options as required. Scalability offers reliability of service offerings in case the application complexity increases, new data points are identified and new service provisions are identified that need higher storage and computing facilities. A high scalable infrastructure will have capability to expand as required and be able to provide solutions that need not go through long procurement cycles, installation and setup. Scalability offers quick options to plug, play, use and pay as you go.

### Key Features in Future State

The future state infrastructure should identify various scalable options that can be utilized as need be.

Each future infrastructure area will be differentiated based on scalability for the agencies and ministries to make informed decisions.

Scalability will ensure higher utilization of data center infrastructure and CAPEX/OPEX investments by the governments in future. The agencies needing scalability would be advised to move to scalable options than investing large capex on infrastructure development capabilities and depreciating assets.

The data needs to be cleansed and classified to ensure economies of scale and optimum utilization of space.

## Designed For Future

The future state of Thailand Government's Data Infrastructure should be sustainable and enable open innovation, usage and adoption of new technologies and above all be standardized. From an enterprise architecture perspective, the important consideration is the way data moves. Current applications are talking to each other; there are endpoints that need to collaborate, and work together; and there is a much higher degree of virtualization that is taking place. This combination causes the network flow to spill out in all directions at the same time, creating more north-south traffic and a huge rise in east-west traffic.

In the past, the timescales allowed for this application to complete were in the seconds. The modern application will need to do the job in milliseconds and even faster in times to come. For citizen centric applications and those that require financial transactions, this becomes increasingly complex. Increasing new traffic will come from a combination of areas from data analytics applications, big data application and from the Internet of Things (IoT).

Designed for future covers capabilities that will enable the data infrastructure to be future proof offering faster delivery and service to its recipients including the citizens. The future capabilities include increasing reliance on cloud technologies and upgradation of applications and data elements in years to come. The new class of application – built using technologies like virtualization, containers and micro-services and accessing multiple external services – presents a radically different workflow to the standard application.

### Key Features in Future State

The future state infrastructure should follow the identified standards for energy, power, location, design and optimization. These standards are carefully developed considering the current state, ROI, costs and long term strategy.

Future proof infrastructure should enable new technology innovations and new applications.

The infrastructure should be developed considering the complexities arising from data analytics, data feed coming from IoT devices and other complex data sources.

The future infrastructure should be ready with support staff and human resources who understand these systems are able to grasp the changes faster. The agencies should be able to move between the infrastructures options to make themselves future proof.

The infrastructure should consider location based Data center location (for new considerations) including the location of multi-agency data centers should go through feasibility study and analysis before design.

### Cost Optimization

With alarming increase in data, cost of providing services, technologies including hardware and software, leasing of facilities etc, there is an increased pressure on the agencies to reduce their spending. The rising cost of data center space (or the opportunity cost), energy, human resources, redundancies in current infrastructure, sub-optimal utilization, economic sluggishness and the ongoing digital economy initiative are the key drivers that point towards one direction- cost optimization. Cost optimization does not mean clampdown of infrastructure as practiced in many geographies.

Cost Optimization covers effective utilization of government resources by using operating budgets effectively, maintaining infrastructure as much as needed, utilizing other available infrastructure options that result in cost savings for the government, relying on low capex technologies and options that reduces the burden of depreciating infrastructure and a long term perspective that takes into account the massive growth of data and need to be prudent- cost wise.

Cost optimization enables exploration of in-house alternatives on using shared infrastructure, colocation and virtualization to achieve lower costs and improve quality of service. Outsourcing and cloud computing are rapidly becoming valid alternatives to “in-house” implementation without impacting service levels or goals.

### Key Features in Future State

The future state infrastructure should operate as cost effective government machinery with reduced capex requirements from hardware, software and operations.

The applications and data should be shifted to a balance of cost effective and efficient platforms and technologies.

The security led approach must be followed to ensure the utilization of other lower cost and flexible solutions for low risk data.

The operating expenses must also be minimized considering the utilization of alternative areas for service provision.

The utilization of the infrastructure must be improved over time by increasing shared capacity usage.

## Operational efficiency

Data center efficiency and its utilization are important aspects of effective management of government infrastructure.  Optimizing data center power use is a high priority for data center managers, but they continue to face challenges as power becomes a larger percentage of ongoing data center costs. From space utilization perspective, Data centers built before the advent of server virtualization may be overbuilt for today's equipment needs, enabling further reduction of the necessary space for IT equipment and less IT power. Higher operational efficiency for the data centers result in better staff efficiency, greater flexibility to support changing business needs, higher scalability resulting from efficiencies achieved and lower costs of operations.

Operational Efficiency covers the optimization of servers, storage, network and facilities assets to maximize capacity and availability. It also includes design of flexibility to support changing business needs. Specific areas include improving the SLA performance of the infrastructure, usage of virtualization and cloud computing, storage management technologies, backup, archiving, business continuity and cost investments.

### Key Features in Future State

The future state infrastructure should follow the standards that are designed for each infrastructure area that govern the best practices to increase operational efficiency

Each future infrastructure area will be differentiated based on operational efficiency capabilities. The agencies will be able to move across the areas in order to attain higher operational efficiency.

Efficient infrastructure should enable a flexible servicing and reduce operating costs. The infrastructure will have an ability  to better serve the needs of the core business and respond to shifts in market demand

The agencies will be able to better forecast the capacity and availability to meet the business needs

## 10. Future Operating Model of Thailand Government's Data Infrastructure

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

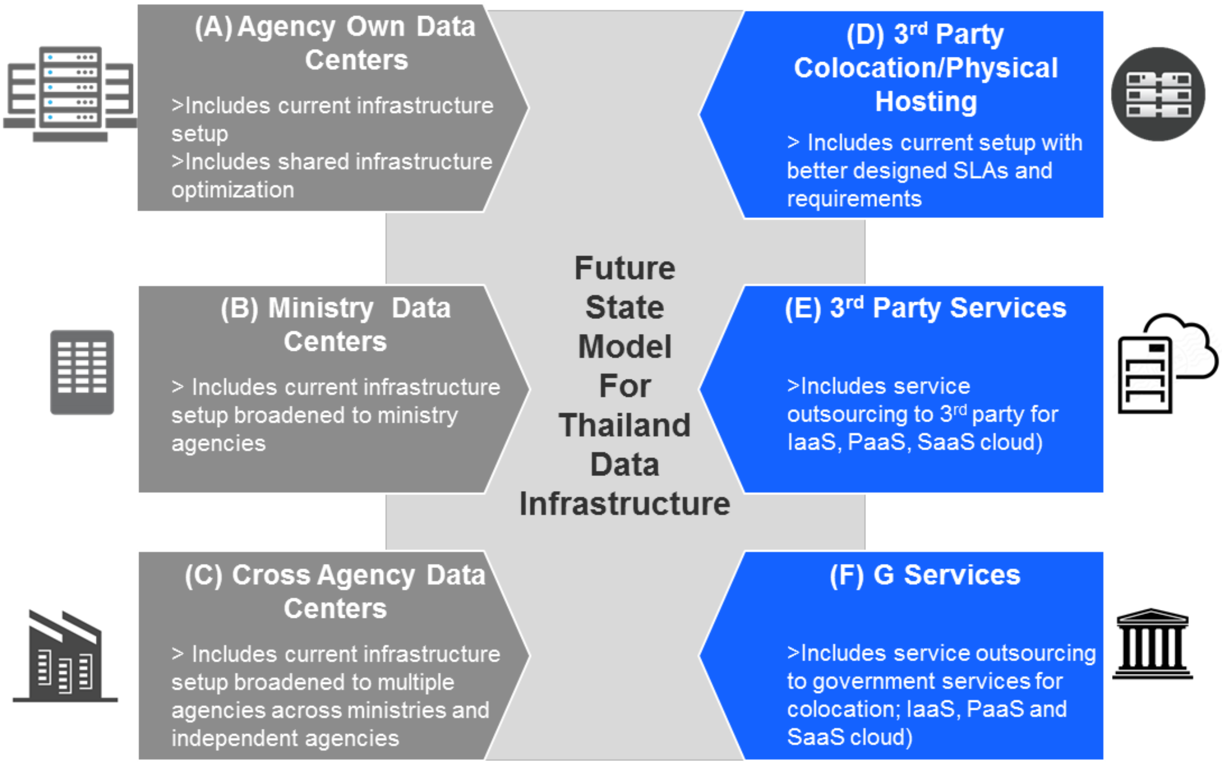
The Future State Operations will need to ensure that Thailand achieves the objectives of Digital Economy and aligns the infrastructure to long term integrated operations.

The future state operations must enable various option areas that the ministries and agencies should be able to choose from and operate in future. The government will also drive the achievement of goals that it will set forth, to revolutionize the overall infrastructure.

The Future Operating Model consists of 6 key areas of future operation for the data infrastructure:

(A) Agency Own Data Centers
(B) Ministry Level Data Centers
(C) Cross Agency Data Centers
(D) 3rd Party Colocation/Hosting
(E) 3rd Party Services
(F) G-Services

Each Operating Model area will be operational based on current operating conditions and will be available to be embraced by the agencies based on their needs.



(A) Agency Own Data Centers

>Includes current infrastructure setup
>Includes shared infrastructure optimization

(D) 3rd Party Colocation/Physical Hosting

> Includes current setup with better designed SLAs and requirements

Future State Model For Thailand Data Infrastructure

(B) Ministry Data Centers

> Includes current infrastructure setup broadened to ministry agencies

(E) 3rd Party Services

>Includes service outsourcing to 3rd party for IaaS, PaaS, SaaS cloud)

(C) Cross Agency Data Centers

> Includes current infrastructure setup broadened to multiple agencies across ministries and independent agencies

(F) G Services

>Includes service outsourcing to government services for colocation; IaaS, PaaS and SaaS cloud)

### (A) Agency Own Data Centers

The future operating model will continue the legacy of agency's own data centers that are far ahead in terms of operations, efficiency and usage requirements. Agency data centers will need to radically change for a futuristic model that houses high security and important data for the agencies. In the wake of budget limitations, growth of data, other available options for hosting and business efficiency requirements, the own data centers need to transform into highly utilized infrastructure used for specific purposes. Agencies would be required to provide utilization as well as security based information to the government and the rationale for using own data center to host data centers.

Definition

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.

The Agency Own Data Centers will need to be upgraded meeting the standards guidelines covered in the standards section. In the current state, the existing data centers have been used primarily by the agencies to host their data, that's beset with various issues and challenges. The future operating model of Agency Own Data Centers will operate at relatively much higher maturity levels of operations.

The Agency Own Data Center of the future will focus on solving 4 key aspects of the data infrastructure.

Handling High Security Data and Computing

Increasing availability and reliability of data

Reducing Operational Cost in current operations

Improving Human Resource availability and capability

**Operational Management in Future State**

- The overall management of the Agency Own Data Center will be governed by the agency data center team as it is currently.
- The agency would need to provide reporting on key aspects of data center efficiency as outlined in the implementation guidelines section.
- Operations and maintenance will be the responsibility of existing teams. Government would provide support in training teams based on their areas of expertise.

### (B) Ministry  Data Centers

Ministry Data Centers are the larger data centers that will form a vital part of ministry infrastructure. It should be ensured that the infrastructure is robust, reliable and responsive to current and future needs. Ministry Data Centers are needed for the much needed scalability that will be needed in years to come. These data centers will be high security facilities, intended to support information system needs and requirements of the agencies falling in a particular ministry.  The ministry data centers will be highly efficient and optimized data center that will enable ministry to provide citizen centric, integrated, accessible and cost effective services

Definition

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

Ministry Data Centers are new mode of service provision that utilizes existing infrastructure that is set-up for various agencies. The large data centers will be converted into Ministry Data Centers based on DC Size, agency data, location and current infrastructure readiness. The data centers will need to be upgraded, to meet the standards guidelines covered in the standards section. In the current state, the existing data centers have been used by individual agencies with limited shared capacity. In the future state, few existing data centers would be converted into ministry data centers to be able to host data across multiple agencies of the same ministry. The key advantage of this set-up would be to use economies of scale, be able to utilize the higher unused capacity, be able to setup better standardized infrastructure across multiple agencies, ensure security with information staying within the ministry premises. Location selection would be a critical element for this data center as it needs to be ensured that the agencies are physically placed in the nearby vicinity. These data centers would be able to host various common data that are utilized by same ministry agencies as well as important but not national security data.

The Agency Own Data Center of the future will focus on 4 key aspects of the data infrastructure.

Handling High Volume Data and Computing needs

Economies of scale resulting into better utilization

Reducing Operational Cost in current operations

Standardized services with better classified data within the ministry

**Operational Management in Future State**

- The overall management of the Ministry Data Center will be governed by the Ministry level team at the data center.
- The ministry level team will comprise of the existing team of the agency as well as other members from other agencies to form a larger team.
- The operations and maintenance will be performed by existing team. The team will be broadened based on need.
- The DC would indirectly report into government and provide reporting on key aspects of data center efficiency, utilization, cost management and resourcing.

### (C) Cross-Agency Data Centers

Various ministry agencies as well as independent agencies see a need for an integrated data center that can house vast amounts of data in secured operations to utilize economies of scale. Cross Agency Data Centers are very large facilities of data centers that already exist in terms of DC space. These data centers would be converted from currently existing data centers that are operated by specific agencies to become self-sufficient, large infrastructure service provider to enable the government to work in a GDC (government data center model). The Cross-Agency Data Centers addresses the need of building the physical infrastructure to interconnect government agencies and be able to support in data integration.

Definition:

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.

A number of agencies operate their own data centers or outsource their data center needs. The current need is not only to cut back on costs, but to optimize ICT resources and operations, and address data security concerns. The Cross Agency DC will enable a faster data exchange and collaboration among government agencies. It provides centralized servers and colocation and storage facilities. These data centers will be operated 24/7 and will be fully equipped with the necessary network equipment and connectivity, data storage facilities, as well as with cooling, security, power, monitoring, and fire-protection systems. Data center services for participating government agencies comprise of physical hosting or collocation, backups, and security.

The Cross-Agency Data Center of the future will focus on 4 key aspects of the data infrastructure.

Overall increase in IT service provision

Better disaster recovery

Use of efficient computing platforms and technologies

Reduced government spending

The new data center will evolve from the current DC setup involving large DC space and infrastructure. The new structure will need to be upgraded to meet the requisite needs and be able to offer high quality services, availability, technology usage, scalability and performance.

### Operational Management in Future State

- The overall management of the Cross-Agency Data Center will be governed by a central team that will be formed to manage the data center.
- Few members from the agency data center team will be a part of the central team.
- The agency would need to provide reporting on key aspects of data center efficiency, operations and management to the central body.
- Operations and maintenance will be the responsibility of existing teams that will be extended to support the functioning of the data center effectively. Government would provide support in training teams based on their areas of expertise.

## (D) 3rd party Colocation/Physical Hosting

Various agencies believe that 3rd party colocation services are important for the overall service provision as it helps reduce the reliance on government budgets to some extent and the human resource requirements. 3rd party colocation is important elements of data infrastructure ecosystem and the future state does see a need for such a service provision area. Colocation of data and services is not a recent phenomenon. Government agencies including Thailand have been practicing it successfully. Colocation or 'colo' enables the agency to rent space for their servers and computing hardware with provision of other infrastructure elements at the rented space itself- building, power, cooling, bandwidth, and physical security while the agency provides server, storage and maintenance in some cases.

In Future State the functionality of Colocation would not change significantly from the present state apart from the clear drawn SLAs which will be driven to identify the right colocation party and to follow the SLAs to ensure that the set policies are been met. The second element that will change is the choice of data that will be colocated. Colocation of data will be strictly reserved to public and low importance data. Even though the information is stored on agency servers, still to contain the risks, there will be limited data elements that will be able to be colocated.

Definition:

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.

A number of agencies currently colocate their data center needs partly or fully. Colocation companies provide deep expertise, 24X7 monitoring, meets government guidelines and supports crucial data and IT needs. The data is housed in fully redundant and highly secured data centers that ensure high scalability due to their ability to expand. The agencies IT systems, websites and other applications are hosted on high connectivity infrastructure, secured with advanced physical security systems. It also alleviates the overhead burden and cost of hiring security staff as well as other human resources required for management of the data center. The 3rd party colocation/hosting of the future will focus on s 4 key aspects of the data infrastructure.

Increase in scalability with availability of support infrastructure

Better connectivity and redundancy for network connections

24X7 monitoring and support

Reduced government spending for small DC needs

The colocation services will evolve from the current setup by identifying SLAs that the agencies would need the colocation companies to adhere to. The agencies would select the right colocation partner which provides the right service provision as covered in standards section for 3rd party colocation. Agencies would need to be picky in selecting the right data that is just right to be colocated.

**Operational Management in Future State**

- The overall management of the relationship, maintenance and data management will be performed by the agency that is colocating their needs.
- Government to work on pricing, SLA and vendor guidance that will be made available to the agencies.
- 3rd party to provide services as covered in the contract.

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

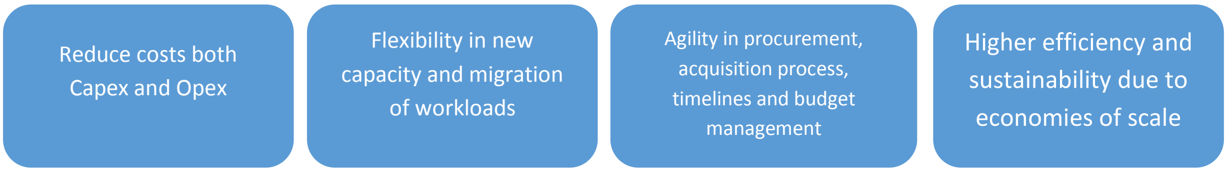
The future operating model of 3rd party services will continue to serve agencies on need based services. 3rd party cloud has emerged to be a very important and growing area that saves infrastructure cost and outsources the operations and capability requirements to a 3rd party. Many agencies believe that movement to cloud will save huge costs for procurement of servers and operational costs of maintenance and human resource requirements. 3rd party services would provide higher stability, transparency and initiatives to manage and maintain the SLA requirements. Cloud embracement will help agencies achieve massive carbon footprint reductions, gain in productivity and efficiency, as well as reducing risks and costs. From business processes perspective, cloud offers ways for agencies to better align business processes to meet the needs of citizens, gain greater business agility, and acquire the requisite flexibility to meet the changing market. In the future state operations, the 3rd party services would be able to host large scale public data or data that requires high availability.

Definition:

3rd party services include IaaS, PaaS and SaaS cloud service provision by private companies and enterprises where agencies can outsource their entire data management too 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.

3rd party Cloud outsourcing will significantly changes the way information and services are consumed and provided and will help the government in Improving workforce productivity, lower costs by using energy and resources more efficiently, enhance agility, growth, and simplicity and help ensure resilient and trusted collaboration. Instead of both owning and managing IT services for themselves, or using an outsourcing approach built around dedicated hardware, software, and support services, agencies can use cloud computing to meet their IT requirements using a flexible, on-demand, and rapidly scalable model that requires neither ownership on their part, nor provision of dedicated resources.

The 3rd party services of the future will focus on s 4 key aspects of the data infrastructure.



Reduce costs both Capex and Opex

Flexibility in new capacity and migration of workloads

Agility in procurement, acquisition process, timelines and budget management

Higher efficiency and sustainability due to economies of scale

The 3rd party services will increasingly be embraced with time and will evolve from the current setup by making the services available at cheaper cost and embrace better technologies in time to come. The future state will need the 3rd party services to adhere to government (agency) provided standards. Government will support the agencies with the set of SLA requirements and advisory on selection of right partner. The agencies will also need to make sure to identify the right data that can be hosted on 3rd party cloud.

**Operational Management in Future State**

- The overall management of the relationship and data provision will be performed by the agency that is outsourcing their needs.
- Government to work on pricing, SLA and vendor guidance that will be made available to the agencies.
- 3rd party to provide services as covered in the contract.

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

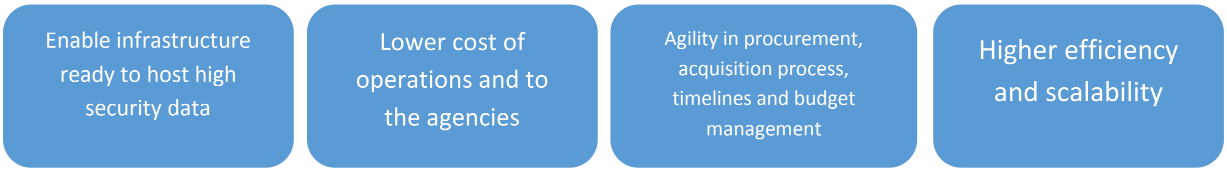
The future operating model of Government Services will include provision of services like Co-location, IaaS, PaaS and SaaS cloud that will be significantly improved from current state. Agencies identify G-Services as one of the most promising future operating area that will enable them to operate efficiently under high security service provisions, managed by the government. Agencies believe that G-Services will be the future of government data center modernization and assign it as a no. 1 priority, as it will allow integrated operations management by the government. G-services will enable usage of shared resources, standardized operations, reduce capital and operating expenses for the agencies, reduce operational and maintenance burden, be able to handle important and high security data and reduce the overall burden of the government. Many agencies believe that movement to G-services will save huge costs for procurement of servers and operational costs of maintenance that they are facing today. The human resource capability will be uniformly addressed and be handled by government which reduces their individual risk of maintenance. The services will be provided with expert guidance and management that offloads the risks from the agencies to the G-services team.

However agencies argue the applicability of G-services to be limited to public data like e-document systems, emails and published data which will be appropriately management by G-services. For the intended benefits, G-services will need to up the game by being able to provide the infrastructure that is highly scalable and advanced in terms of technology adoption and offer secured facilities. The clear advantage of G-services over 3rd party cloud and colocation is higher security management and containment of data within government managed premises thus reducing the risk of data loss or cyber security issues, significantly. However the operational teams need to make sure that the SLAs are adhered to, provide 24X7 support like 3rd party services, be able to ramp up the infrastructure based on needs and be highly standardized.

Definition: 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.

G-Services will significantly address the increasing needs of agencies to support increasing data and capital requirements to address the growth, data security and ownership, data integration and support, data center agility, resilience and scalability challenges, high standard adoption, challenges faced by agencies in budget allocation and reliance on budgets including longer lead times and availability of ready infrastructure with high technology components and efficiency. The future state of G-service will include all the capabilities of 3rd party outsourcing from the standard adoption perspective as well as ability to support higher security data.

G-Services of the future will focus on 4 key aspects of the data infrastructure.



Enable infrastructure ready to host high security data

Lower cost of operations and to the agencies

Agility in procurement, acquisition process, timelines and budget management

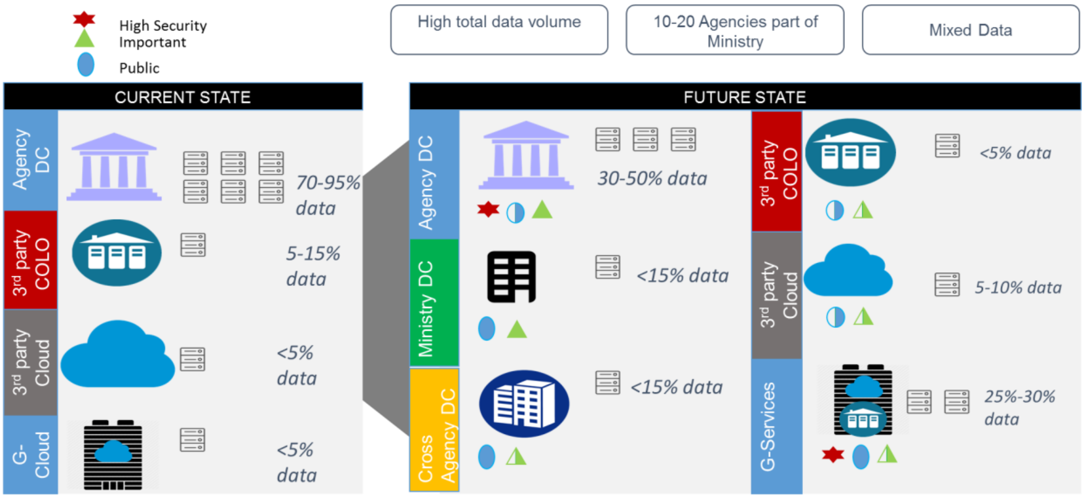
Higher efficiency and scalability

G-Services will increasingly be utilized by agencies as they see huge merit in services offered by the government. Key important areas that the government would need to focus would be to focus on data integration/classification for the hosted data, provision of 24X7 servicing to provide issue resolution, high resilience and scalability to ramp up, standardized operations at reduced overall cost to the agencies.

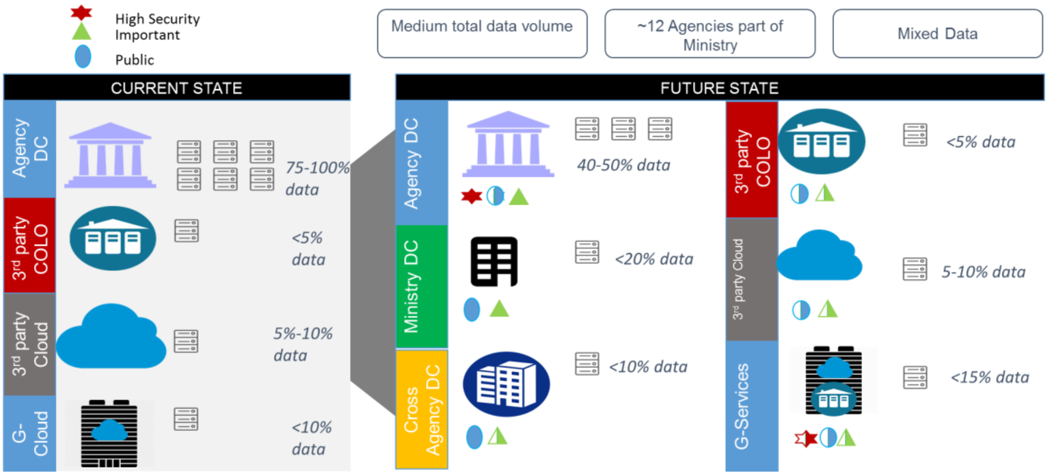
**Operational Management in Future State**

- The overall management of G-services will be done by specific teams that are operating currently with better servicing capabilities with additional human resources as required.
- The agency teams will be able to maintain the relationship between G-services and the agency as customer-vendor relationship and will be able to seek service quality information, and standards fulfilments etc.
- Government to work on pricing and make services available to all agencies.

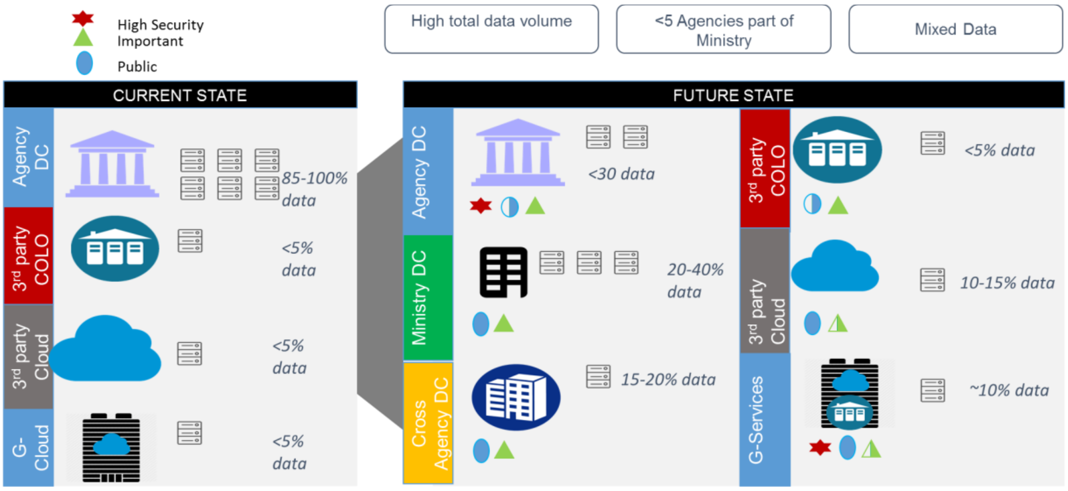
## Example of how ministries and agencies will operate in future from data perspective: Large Ministry: e.g. Science and Tech



## 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



# 11. 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:

### Optimize cost of operations including maintenance

As covered in previous sections, one of the core concerns of the agencies is the increase in cost and inadequate 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.

### Optimize 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 including Cloud to choose from

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 GDCM Strategy is to improve data infrastructure per the Digital Development Policy to enable 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
- Enabling infrastructure with standardised approach and service delivery
- Optimize the cost and investment for the infrastructure
- Implement shared operations at agency level, ministry level and government level
- Improve agency efficiency

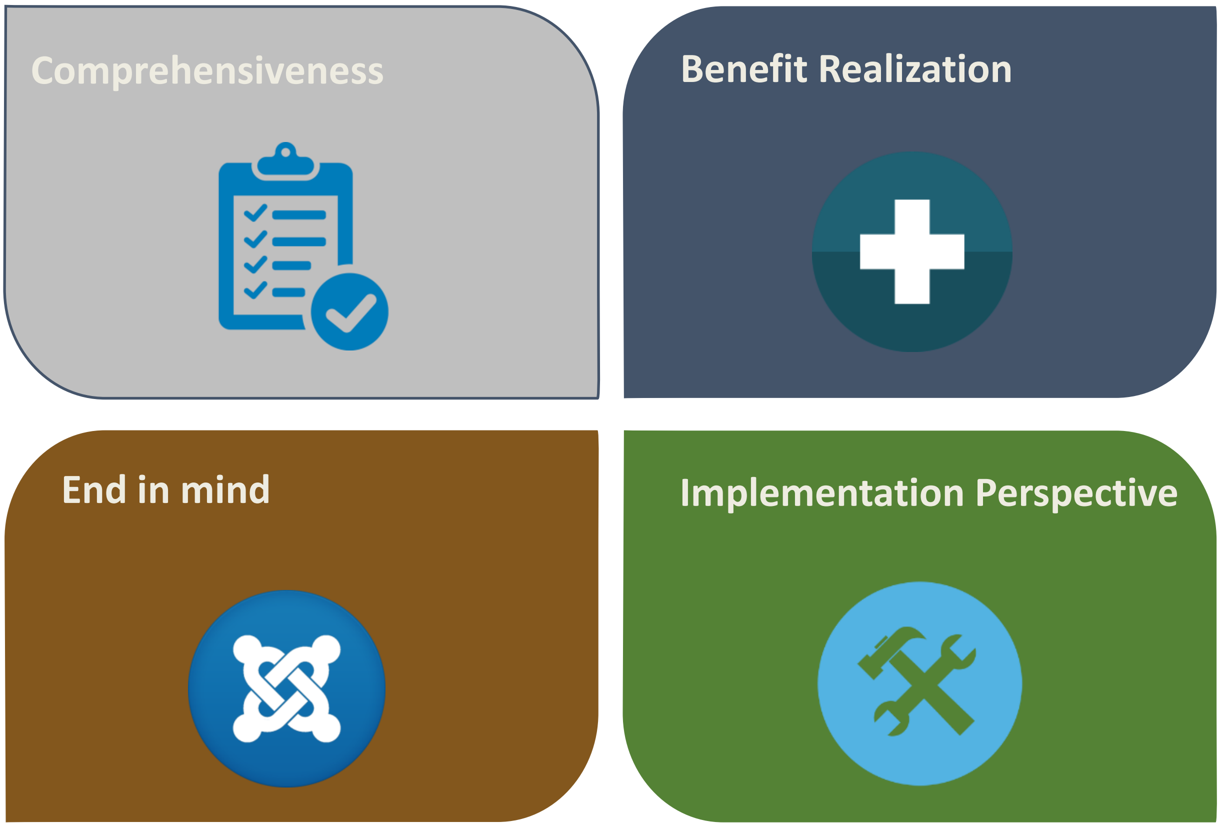
### Guiding Principles for Strategy Formulation

Government Data Center Modernization (GDCM) initiative is planned to adopt modern technologies and practices that improve the security posture of Thailand government and at the same time, enable an efficient use of government ICT infrastructure. The strategy will enable Government of Thailand as well as the agencies to adopt best practices to realize and reap multiple benefits that will grow the infrastructure of the nation and enable long term sustenance. The following guiding principles have guided the formulation of strategy and the business imperative:

1. Alignment with Digital Economy and Prime Minister’s vision for Government Infrastructure and Modernization
2. Strategy based on data security, criticality of applications, current operations perspective and inclusive growth
3. Utilizes the key improvements in technology via standards and SLA adoption for identified models to enable a successful realization of benefits
4. Consideration of skillsets, people development, human capital availability, and technology transfer
5. Accountability of agencies and ministries through granular steps to realize overall objectives.

### Key Attributes of Thailand Government Data Center Modernization Strategy

Data center modernization and consolidation is the continuous optimization and enhancement of existing data center infrastructure, enabling better support for mission-critical or high security applications. Thailand Government Data Center Modernisation is a long term initiative that aims at utilising new opportunities and improvements to increase efficiency, efficacy and to enable an overall infrastructure to be more reliable, available, dependable and secured. The key aspects that enable a successful government data center modernization strategy (GDCM) are:



Comprehensiveness

Benefit Realization

End in mind

Implementation Perspective

| | |
|---|---|
| **A.**<br>**Comprehensiveness** | • Strategy should have checkpoints to identify the value generated and perform root-cause-analysis for any issues |
| | • Key risks and dependencies must be identified and highlighted from the start of the programme to the end of the programme. |
| | • The strategy must ensure that the various applications are not affected in terms of downtime for any strategic move for a significant time. |
| | • The strategy must also align to provide access to multiple options for ministries and agencies to access to offer seamless service. |

| | |
|---|---|
| **B.**<br>**Benefits Realisation** | • The strategy must enhance the overall objectives of the initiative. |
| | • The strategy must not harm existing mission critical workloads that form the lifeline to the operations. |
| | • The strategy must keep in mind the business environment growth in line with growth in digital market, increase in technology adoption and data creation. |

| | |
|---|---|
| **C.**<br>**End in Mind** | • The strategy must enable a higher level of citizen centricity |
| | • The strategy must ensure that it uses and utilises most optimum model to ensure better servicing as well as cost, output, utilisation and scale. |
| | • The strategy must complement the standards that should be developed for the future model. |

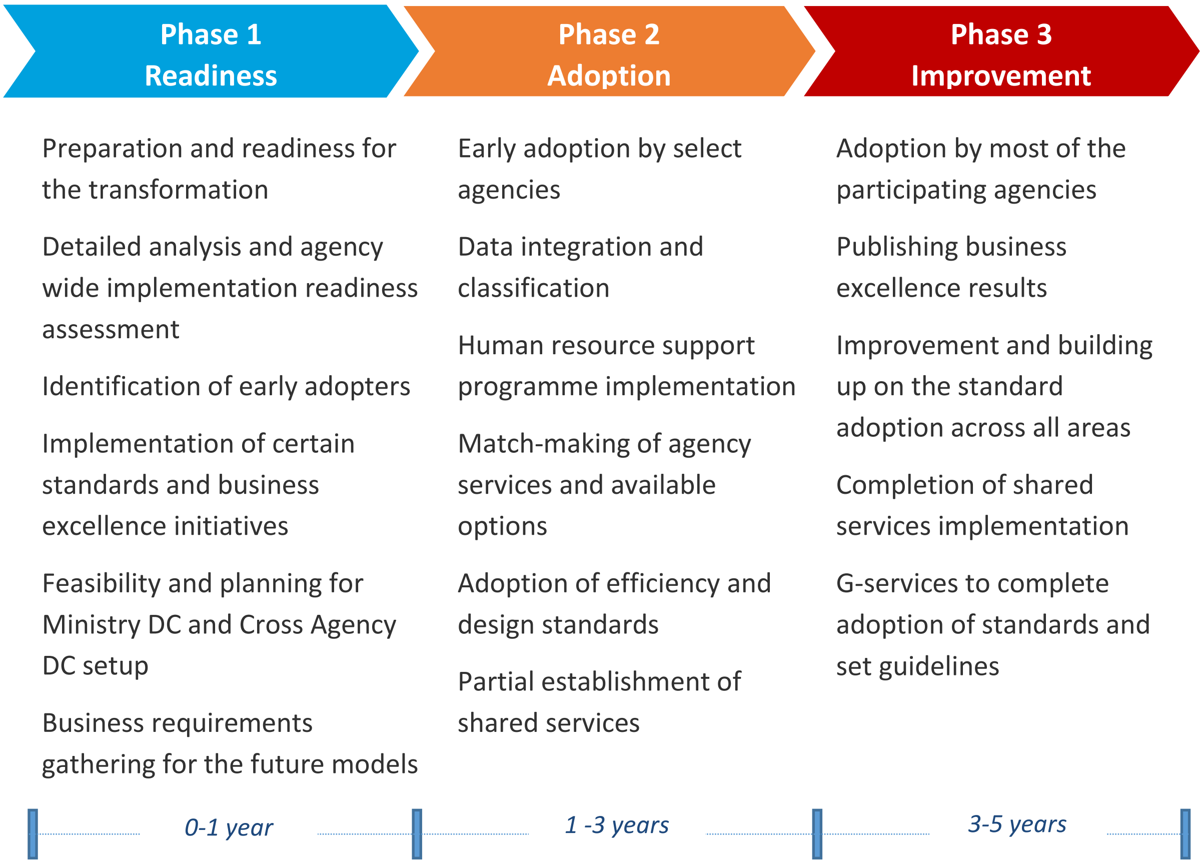
| | |
|---|---|
| **D.**<br>**Implementation Perspective** | • Identified strategy must have a mission and a vision that must be followed across all levels of parties involved solutions for the strategy and the initiatives must keep the implementation duration in sight and must be planned well to support and complement other initiatives. |
| | • Strategy should be implemented keeping end in mind being mindful of the implementation issues, migratory issues and problems that multiple parties must face. |
| | • The strategy must focus on pain-points and implement realistic and practical approach to data center modernisation. |
| | • The strategy must identify how to offer better service based on optimised model and how incrementally these models can be developed and enhanced. |

## 12. Implementation

The implementation of the GDCM Initiative will be conducted in a phased approach over a period of 5 years (2017-2022). With a rapidly evolving business dynamics, agencies are continuously growing at various rates with new applications, services and requirements. External market on the other hand, is growing at a far more rapid pace with technology innovations as well as technology obsoleteness. Hence it is not prudent for all agencies to go through the transformation together. With varied business needs, human resourcing issues need for new capex, application launch, data integration and classification issues; agencies face numerous issues and complexities that need to be considered while developing an implementation approach.

Over the course of next 5 years, it will be expected for most of the agencies to have considered adoption of ways and means to improve their data infrastructure and to have met the set objectives and goals by the government.

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



**Phase 1**
**Readiness**

Preparation and readiness for the transformation

Detailed analysis and agency wide implementation readiness assessment

Identification of early adopters

Implementation of certain standards and business excellence initiatives

Feasibility and planning for Ministry DC and Cross Agency DC setup

Business requirements gathering for the future models

*0-1 year*

**Phase 2**
**Adoption**

Early adoption by select agencies

Data integration and classification

Human resource support programme implementation

Match-making of agency services and available options

Adoption of efficiency and design standards

Partial establishment of shared services

*1 -3 years*

**Phase 3**
**Improvement**

Adoption by most of the participating agencies

Publishing business excellence results

Improvement and building up on the standard adoption across all areas

Completion of shared services implementation

G-services to complete adoption of standards and set guidelines

*3-5 years*

## 13. Project Worthiness and Benefits

Government Data Center Modernization (GDCM) Initiative will deliver a number of benefits that include: improvement in current infrastructure in terms of utilization, availability, efficiency, use of latest technology elements, better security, design and improved facilities, better sustainability and resilience, better disaster recovery and business continuity, data security for national data, resource availability and creation of new options for service provision. The initiative will also enable cost optimisation for the government as well as for the agencies and save capex investments in the purchase of new IT infrastructure significantly as well as operating costs in the areas of human resources, day to day maintenance, operations, energy consumption and network usage.

The following are the key areas of improvement and the benefits that this engagement will enable:

### Adoption of Standards

The new delivery model will enable better adoption of chosen standards based on developed guidelines for agency data-centers. Even though, the data centers would differ across the adoption cycle of the standards, incremental benefits will be realised by aligning the agencies on new standard adoption right from increasing the utilization to energy efficiency. New areas like Ministry Data Centers and Cross Agency Data Centers will be established with higher set of standards and quality of infrastructure. This will enable development of infrastructure for future to enable ling term sustenance.

### No compromise on Security

The new delivery model will enable strong effort to manage security posture of the government and adopting a security centric approach. High security data will be handled with care and efforts and investments will be made to establish higher security standards. On the same lines, low security data will be handled appropriately to use economies of scale.

### Capacity Improvement

With the rapid need of capacity, scalability is a pre-requisite that will be addressed with the future state of infrastructure and implementation of GDCM. With new standard adoption and alternative approach to usage of shared services, 3rd party cloud and government services, the capacity will be further enhanced to capture the future growth.

### Utilisation of Government Infrastructure

The current government data infrastructure is not utilised efficiently. GDCM will enable a high utilisation of the current infrastructure by the virtue of shared services. A higher return on government investment will enable government to focus their expenditure in growth of alternative areas which helps the national cause for Thailand.

### Cost Reduction

With the new model, the agencies will be able to save significant budgets of maintaining their own infrastructure by exploring other areas. With economies of scale, various cost elements like IT infrastructure, energy, human resource requirements, hardware elements, software will reduce by the shifting of capabilities into cost effective opportunities.

### Focus on core activities

New models will result in agencies being able to focus on their core business and be able to be more citizens focussed. Maintenance and management of IT infrastructure will shift to other areas that are more efficient and economically prudent.

### Location based aggregation

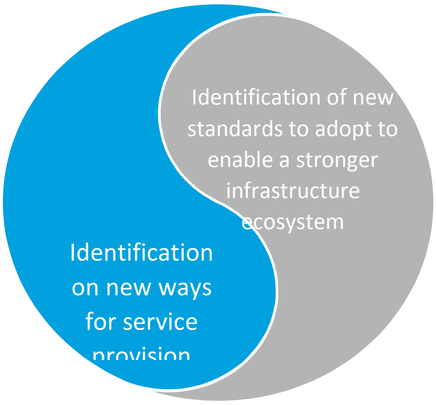
Ministry data centers and Cross Agency data centers will be developed and enhanced from current infrastructure based on locational proximity and achievable benefits of economies of scale. With aggregation, the government will be able to focus on data integration and integrate mission critical applications.

As covered in the previous document on GDCM Strategy, the aim for the Government Data Center Modernization is to improve the efficiency and security; reduce cost of operations and government spending and to enable the government infrastructure to be future ready to embrace the challenges of data explosion, growing citizen needs, and data complexity as well as rising costs.

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

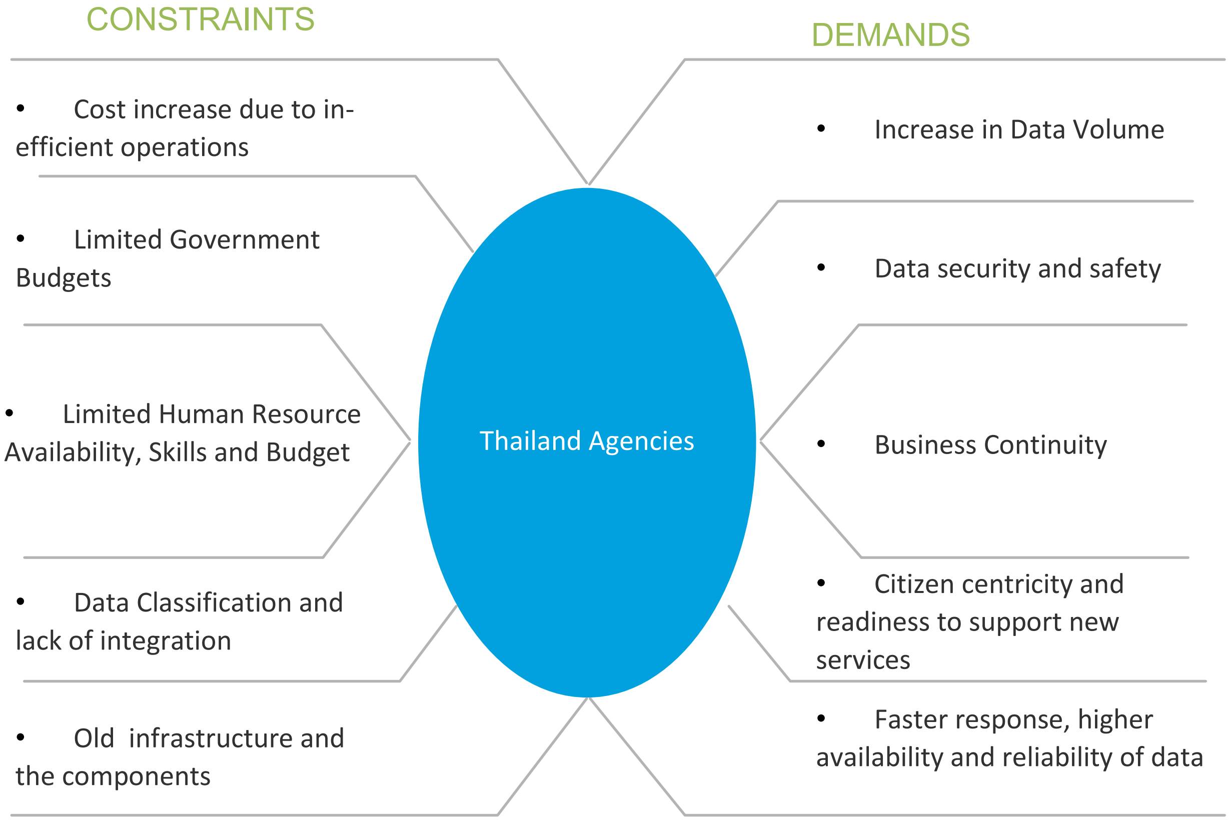
Most agencies have one or more data centres, of varying effectiveness and efficiency levels that are supported by internal human resource teams who provide this support as part of wider roles. Each agency explores ways to meet their data provision needs by the use of their current infrastructure at the cost of running in-efficient operations depending on the budgets and support provided by the government. The result is that, the agencies are not able to utilise the established data centre services provision in an optimal way that may further results in compromising data security, inefficient operations and data center provision earmarked for scalability, wastage of government resources and overall ineffective utilisation of the setup. While, with advanced technologies and infrastructure availability, already practiced across the world, Thai agencies are currently operating in environment that breeds long term unsustainability, wastage of resources and infrastructure that gives rise to further issues like manpower shortage, security concerns and sudden increase in overall cost of operations. External drivers such as increasing power costs and concerns about availability, difficulty in securing budgets from the government in alignment with tighter government budgets, maintenance of security, skilling the staff, handling higher quantity of data, increasing user demands, wastage and lower utilisation of IT resources causes further issues in running the agency operations effectively. Agencies are increasingly concerned about facility availability and current condition of the data centers that need a modernization strategy. Many agencies are worried about reliability, resilience and business continuity that pose as a challenge. At the same time data usage (and storage) is increasing significantly with an estimated growth of 25% year on year. There is a need to answer the fundamental issue of how the agency DCs needs to focus on the core activity of the agency. This ultimately need to the need for Government Data Center Modernization Strategy to enable a comprehensive, integrated as well as sustainable plan to enable the government data infrastructure to operate optimally.

The Government Data Center Modernization Strategy answers the identified core issues, concerns, demands and constraints that Thailand agencies are facing today. The strategy not only covers the provision of services through alternative ways and approaches but also enables the use of technologically armed standards to enable an ecosystem of agility, responsiveness, integration, sustenance, future proofing, security and management.


Identification of new standards to adopt to enable a stronger infrastructure ecosystem
Identification on new ways for service provision

The Thailand Government Data Center Modernisation Strategy Plan rests on the understanding of government data infrastructure that includes agency data centers, cloud hosting, colocation services and the use of government cloud that are presently being utilised in current condition by the agencies. These current provisions support the entire government data needs for the government and related services for the citizens. With the changing times both from the data growth and complexity perspective and the demand for services as well as from the business constraints that pose bottlenecks for the agencies, it is vital to enable and establish an infrastructure that transforms the capability of government in alignment with Digital Economy.

**Government Agencies constrains and demands**



CONSTRAINTS

- Cost increase due to in-efficient operations
- Limited Government Budgets
- Limited Human Resource Availability, Skills and Budget
- Data Classification and lack of integration
- Old infrastructure and the components

Thailand Agencies

DEMANDS

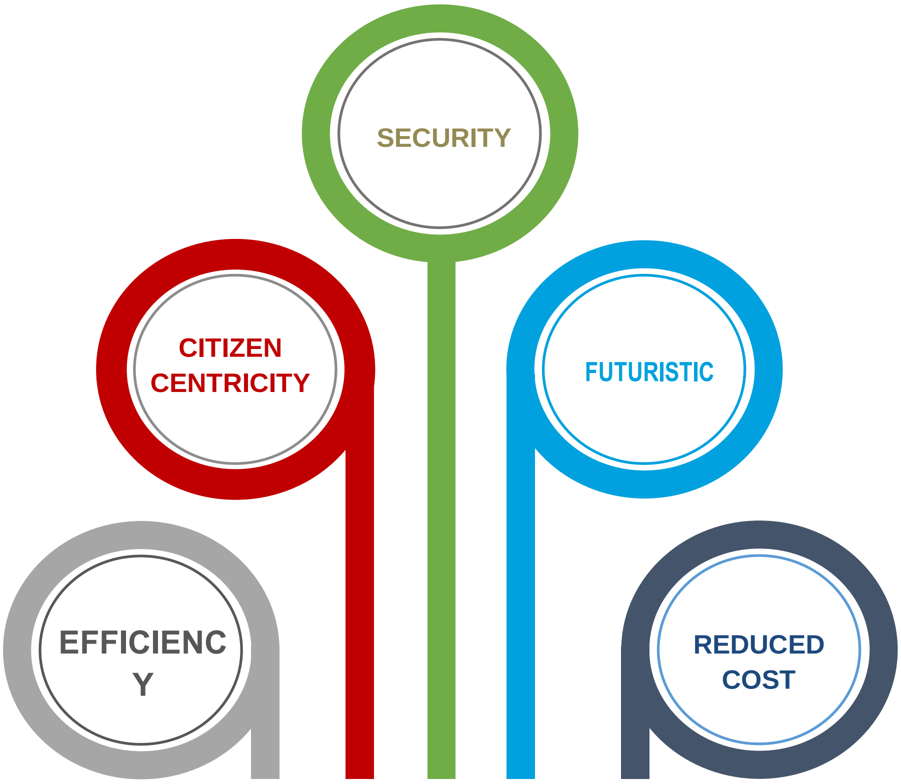
- Increase in Data Volume
- Data security and safety
- Business Continuity
- Citizen centricity and readiness to support new services
- Faster response, higher availability and reliability of data

Across the world, governments have recognised the need for embracing new technologies, innovation as well as usage of shared services to prove as drivers for Digital Economy and enable sustainable living for the citizens.

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:

(G) Agency Own Data Centers
(H) Ministry Level Data Centers
(I) Cross Agency Data Centers
(J) 3rd Party Colocation/Hosting
(K) 3rd Party Services
(L) G-Services

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

# 14. GDCM Development Plan

GDCM Development Plan for Thailand entails a well-coordinated, documented, planned and well executed strategy for data center service provision as well as standard adoption. The development plan will impact the agencies and ministries differently and there may be individual trends, constraints and issues that they are facing. The plan at an aggregate level. Provides the business case for the transformation and establishes the hypothesis for Government Data Center Modernization Strategy.

Future service provision entails how the current data should be handled in future and where this data should reside in future. With security led transformation, it is critical that the future operations are well documented and identified for each agency, in terms of future provisions they would operate out of. There are two main aspects this strategy seeks to address, the types of provision that can be provided, and the mechanism for delivering that provision and associated cost savings and service improvements. The Thailand Agencies have significant existing data centres that belong to the agencies themselves, and this infrastructure can be leveraged more effectively.

Thus one aim is to seek to optimize the use and reuse of existing data centres. However, existing provision (data centers) are limited in terms of size, capacity as well as data storage requirements by classification on data security.

The existing provision needs to be clearly identified in terms of capacity, utilization, maximum capacity, further enhancements possible, future plan of investments and strategic intent.

As a result, the future state is proposed to be built around 6 areas of operations. These 6 areas will form **Thailand Government Data Center Ecosystem.** The new ecosystem will house multiple opportunities are areas for agencies to host their current and future data. From service provision perspective, the role of agencies and the government is articulated below that provides service provision guidelines on the service provision.

## Usage of Agency Data Centers

There are significant existing infrastructure elements that are established by the government agencies at Thailand in the form of government data centers.

The current agency infrastructure comprise of Own Data Center, G-cloud, 3rd party colocation and 3rd party cloud. Out of the 42 surveyed agencies, 90% agencies claimed to be using their own data centers to store and process their data while 20% claimed to be using 3rd party colocation and G-cloud each and only 7% on 3rd party cloud.

The future state operations of the Thailand Government Infrastructure would aim at using the established resources that can be more fully utilized within the agency, but are currently not utilised efficiently. The key barriers to the efficient utilisation of existing data centers are variability in facilities standards bot, network connectivity, lack of common standards, data classification issues, data security handling and unpredictability of future use. Agencies are individually virtualising services, and there are opportunities through virtualisation to establish a common platform in the form of Ministry Data Centers and Cross Agency Data Centers. These data centers would enable the migration of services to service the needs of agencies and to be scaled for ministry wide or cross agency scopes. This will be key to be optimal use of government resource. This platform will need, at minimum common standards and interoperability, however national procurement for a virtualisation systems might bring additional significant benefits, compared with individual procurements.

The key strategic guidelines to agencies and agency data centers are:

- Agency data centers to follow strict guidelines for service provision, data classification, maintenance, standard establishment, human resource handling and operational efficiency.
- Certain identified agency data centers will develop further into Ministry Data Centers and Cross-Agency Data Centers on meeting criteria set by the government as a part of initiative called **“iTransform.”**
- Agencies that do not meet the guidelines and criteria set by the government would need to close and the agency data would need to be hosted through alternate modes.
- Agencies to follow the further agency wise plans for the transformation based on government directives.
- Agencies would need to carry out discovery study in the year 1 to identify data classification needs, prepare a business case for their data center and conduct feasibility study for data migration based on applications and requirements to other alternative areas. The initiative will be called as **“iDiscover.”**
- Agency to carry out feasibility plan for standard adoption based on identified adoption cycle. Post planning, agencies will have to meet the guidelines and criteria set by the government. The initiative will be called as “**iAdopt**.”
- Agency must identify the human resource needs and identify resources that can be shared with other provision areas. The study will be a part of larger initiative called “**iTransition.**”
- Agencies must utilise own data centers to host the data, as per the data classification plan identified.
- Agencies must identify judiciously ways to offload public data to G-services, Ministry DCs and Cross Agency DCs or 3rd party cloud as a part of initiative called “**iOptimize**.”

## Development of Ministry and Cross Agency Data Centers

Even an agency with only a single data center is likely to own servers with average utilization below 5 percent and server racks with spare capacity. Thailand Agency Data Centers on the whole faces a large issue of utilisation, spare capacity as well as provision for scalability. Data centers represent clear, short-term opportunities to capture value by better using existing resources and forgoing future IT purchases.

The development of shared service for Thailand stems from the fact that large data centers need to justify the government spending as well as set up as an example of shared pool of infrastructure and resources.

The shared infrastructure in the form of Ministry and Cross Agency Data Centers will have large dedicated hosting space (500 m2+) and meets the  standard guidelines as provided in appendix.

Shared Services will provide various benefits to the Thai government including:

- ✓ *Ensure compliance to established standards for standardized use.*
- ✓ *Quick onboarding of Government agency data.*
- ✓ *High availability to ensure non-stop operations (24 by 7)*

- ✓ *High Speed Connectivity to Government Network.*
- ✓ *Physical Security and backup to ensure trouble free operations*
- ✓ *Service Delivery reported against defined Service level agreement*
- ✓ *Lower total cost of ownership.*
- ✓ *Better utilization of resources (human resource as well as technology resources like hardware and software).*
- ✓ *Handling high volume data and computing needs*
- ✓ *Higher utilization of government resource*

The key strategic guidelines to agencies and the government are:

- Government representative to conduct feasibility to analyse and identify the data centers ready to be converted to Ministry or Cross Agency DC. The initiative will be called as "**iDiscover**".
- Agencies must comply with government directive to establish the agency DC into Ministry or Cross Agency DC.
- Agency must be able to use the shared service data center (cross agency/ministry agency) to store their own data
- Agency must provide their resources, infrastructure and teams as a part of the infrastructure.
- Governance team for ministry/cross-agency data center must ensure that the shared service operations meet the set guidelines and standards as identified in the standards section.
- Governance team to ensure that they set the governance criteria and mechanism to measure the performance of the data center with identified SLAs
- Governance team to ensure that the data centers are converted into ministry and cross agency data centers in the prescribed timeframe as provided in the implementation plan as per "**iAdopt**" initiative
- Agencies within the same ministry with a ministry data center must ensure that they utilise the ministry data center effectively and host atleast 10% of their data on ministry data center.
- Governance team to identify the "radius" of coverage of cross-agency data center and which agencies (independent or ministry) would come under their purview.
- Agencies that fall under the radius of cross-agency data center, must ensure that they host atleast 10% of their data onto the cross –agency data center as a part of "**iOptimize**" initiative

- Governance team to ensure that the ministry and cross-agency data centers are established, up and running and utilised based on the timelines as provided in the implementation plan.

## Reduction of use of Colocation Services

Third party colocation is a practice utilised by multiple government agencies. Based on the records from the survey, about 20% agencies use 3rd party colocation services in some or the other capacity. With data center colocation, smaller agencies (with low data) can benefit from the same technological advancements as their larger counterparts without the added burden of in-house storage and maintenance of equipment. However, most of the agencies that use colocation, incidentally maintain their own data centers too.

3rd party colocation provides a host of benefits including:

- ✓ *Greater focus on day to day operations*
- ✓ *Human resourcing needs for data maintenance is outsourced*
- ✓ *Fast and reliable infrastructure that reduces the need and reliance for onsite-IT support, communication and resource sharing.*
- ✓ *Provides scalability options to expand the resources*
- ✓ *Mitigates risk*
- ✓ *Improved cost savings.*

However, in Thailand's context, Colocation services are widely used despite of the cost heavy IT infrastructure spent in data centers. With multiple facilities like standardised agency data centers with better security and reliability; ministry data centers and cross agency data centers that will be established as best in class service provisions; 3rd party cloud and well as G-Services that include colocation services, the agencies are spoilt for choice.

Agencies have multiple options to choose from – that provide as good or better services and advantages as colocation.

Hence from a strategic perspective, in retrospect of the cost of operations as well as availability of other suitable options, 3rd party colocation services is recommended to be significantly reduced as a part of GDCM strategic plan.

The key strategic guidelines to agencies and the government are:

- Agencies must comply with government directive to reduce the reliance on 3rd party colocation and reduce their hosting on 3rd party colocation.
- No new agency unless that it doesn't' have its own data center, will be permitted to use colocation services provided by 3rd party. They will be able to use colocation services provided by the government as a part of G-Services.

- If an agency that does not have its own data center would want to use 3rd party colocation services, they would need to prepare a business case citing the reasons and specifications on the reasons for not using government services and other service provisions. The business case will be evaluated on case by case basis by the government body.
- Agencies with existing usage of 3rd party colocation will not be able to renew their contract unless there is a specific business need. Such agencies would need to prepare a business case citing the reasons and specifications on the reasons for not using government services and other service provisions. The business case will be evaluated on case by case basis by the government body.
- Each agency with data on 3rd party colocation must prepare a data migration plan and risk mitigation plan for uninterrupted services.
- Government team must ensure provision of colocation services as a part of G-services with standard SLA adoption as specified in the standards document.
- Government team must ensure provision of ministry and cross agency data centers with standard adoption as specified in the standards document as part of "**iAdopt**" initiative
- Government team must ensure provision of cloud services as a part of G-Services with standard adoption as specified in the standards document.
- Agencies must utilise the other identified areas to migrate their data storage and computing needs seamlessly as a part of "**iOptimize**" initiative

## Gaining prominence of Cloud

Governments across the world are slowly migrating towards the adoption of cloud services to capitalise on the economies of scale and lower costs. Cloud computing is growing exponentially, but many agencies still having reservations about using the cloud for their data management and data storage. Many government agencies fear that the cloud is unsecure and expensive. Governments across the world are investing huge money on establishing their own cloud mechanisms. Cloud computing is transforming operations of agencies and creating a paradigm shift by delivering hosted services through the internet with unabated cost benefits and strategic innovation. With growing financial constraints of the past few years, agencies must identify options to seek optimized business models while measuring their performance and service deliveries more closely. While cloud deployments are mainly considered to contain costs by sharing services and infrastructures, government agencies have also devised innovative means of ensuring compliance across the enterprise. The federal government doesn't only rely on the same cloud computing model that hosts consumer applications. The private cloud environments they operate in definitely leverage some of the characteristics of elasticity in those public clouds but they need to be more reliable to handle mission critical workloads. Increasingly, Government organizations are redefining their businesses to deliver improved citizen services.

At Thailand, many agencies must support their mission-critical operations with agile and innovative cloud deployments that incorporate mobile, social and analytics technologies.

However, they also have to take stringent compliance and security measures to not compromise on national security from inside and outside threats.

At Thailand, currently, only 10% agencies utilize 3rd party cloud facilities with services from multiple cloud operators. It is further estimated that only 2.6% of government data is currently hosted on 3rd party cloud.

These figures are starling as the cloud proliferation has multiple benefits to realize that improves the overall efficiency of data handling, reduces cost and increases security.

- ✓ *Provides flexibility of resources that allows allow creation of new operational systems, both for internal and external use*
- ✓ *Increases security and secured handling of data as the enterprise grade cloud is found to be more secured than other data storage options. With technologies like data encryption, the data can be encrypted into various levels of clearance steps.*
- ✓ *Consolidating data into a cloud storage options gives an opportunity to classify data better and organize them to become efficient and useful.*
- ✓ *Reduces cost significantly with operating expense needs that's significantly lesser than maintaining own data centers.*
- ✓ *Usage of latest technology*
- ✓ *Teams are better utilised and focus on core activities.*

The key strategic guidelines to agencies are:

- Agencies must comply with government directive to increase hosting of their public data on 3rd party cloud.
- Agencies must need to conduct an internal discovery and feasibility study as a part of "**iDiscover**" initiative to identify which data they can host on cloud and identify the timelines, plan etc and provide the details to the government as per the set plan.
- Agencies must need to conduct a feasibility study for hosting any new data or application on cloud and ultimately host the data on cloud. Agency must submit a feasibility report and result to the government as per the set plan as a part of **iDiscover.**
- Government must identify 3rd party cloud operators who comply to the set standards and SLAs provided by the government
- Government must identify a preferred list of vendors for 3rd party cloud operators who comply to set standards with negotiated rate (cost) and support services.
- Agencies must choose the preferred list of 3rd party cloud operators only to outsource their data needs for any new service.
- Agencies may be permitted to utilise the contract with existing 3rd party cloud service operator and setup to meet their needs for existing data and services.
- Agencies must host any new public data and migrate the feasible data onto 3rd party cloud as a result of feasibility study, as a part of initiative "**iOptimize**"

## Government Services as a new paradigm

Government organizations are redefining their businesses to deliver improved citizen services. Governments, agencies, and ministries around the world are transitioning to secure cloud computing and realizing tangible operational and financial benefits The Government Services for hosting e-government services for use by agencies, aims at more agile and cost-effective delivery of common e-government infrastructure.

The Thailand Government has taken a leap in adoption of the Government Services model to meet rising public demands and community expectations on e-government services and reap the benefits of emerging technologies. G-Services include Government Cloud environment that comprises three service layers:

- **Software as a Service (SaaS):** Shared services for a portfolio of applications/services, including electronic information management, human resources management, electronic procurement etc.
- **Platform as a Service (PaaS):** e-Government Infrastructure Service platform to enhance efficiency and cost-effectiveness in providing public services.
- **Infrastructure as a Service (IaaS):** Government Cloud Platform that provides scalable and flexible computing resources for hosting e-government services.
- Other than the cloud layers, government also provides **Colo cation services** as a part of G-Services

At Thailand, currently, only 16% agencies utilize G-Services with 9% of the total government data hosted on G-Services.

Benefits of Government Services (G-Services) include:

- ✓ *Cost saving through economy of scale and resource sharing;*
- ✓ *Time saving through streamlined procurement and system implementation, and on-demand service provision;*
- ✓ *Enhanced agility in meeting dynamic demand of agencies on IT resources and services; and*
- ✓ *Generate demands for various types of IT professional works and services, and foster development of local IT industry in strengthening the related professional skills and business models in cloud computing.*
- ✓ *Standardised environment with matured cloud environment and government support.*
- ✓ *Higher security due to following best market standards and government facility provision.*

The key strategic guidelines to agencies are:

- Agencies must comply with government directive to increase hosting of their national security, important and public data on G-Services.
- Agencies must need to conduct an internal discovery and feasibility study as a part of "**iDiscover**" initiative to identify which data they can host on G-Services and identify the timelines, plan etc and provide the details to the government as per the set plan.
- Agencies must need to conduct a feasibility study for hosting any new data or application on G-Services and ultimately host the data on G-Services. Agency must submit a feasibility report and result to the government as per the set plan as a part of **iDiscover.**
- Government must conduct feasibility study to identify the growth and requirements from G-services perspective to prepare the next plan of action. The feasibility plan will be covered as a part of "**iDiscover**" initiative.
- Government must enable meeting the set standards for G-Services as outlined in the standards document as a part of **iAdopt** initiative.
- Government must be prepared for the size of data, scalability and handling large data sets from infrastructure perspective. Such readiness for G-Services will be a part of "**iTransform**" plan.
- Agencies must choose G-services over 3rd party cloud or colocation to host their data. Agencies must submit reasoning for not selecting G-services over 3rd party cloud/colocation as a part of "**iOptimize**" initiative.

- Agencies may be permitted to utilise the contract with existing 3rd party cloud service operator and setup to meet their needs for existing data and services.
- Agencies must host any new public data and migrate the feasible data onto “G-Services” as a result of feasibility study, as a part of initiative “**iOptimize**”

## 15. GDCM Technical Guidelines

The Government Data Center Modernization Strategy entails technical requirements for agencies to follow to maintain their own agency data centers. Agency Data Centers. The technical guidelines cover technology enabled operations to manage and maintain the agency data centers from guidelines and best practices perspective.

**Server Management:** Server management means monitoring of critical resources of the operating system. Agencies must monitor various operating system parameters such as processors, memory, files, and processes, file systems, etc. where applicable, using agents on the servers to be monitored. This would also involve defining warning threshold, integrating with enterprises management systems and also provide a common look and feel across all platforms.

**Database Management:** Database management would involve monitoring critical resources and parameters of databases. Specifically data base management would involve installing tools that proactively monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc. where applicable, using agents on the servers to be monitored. This would also involve integration with enterprise management system, automatics discovery of data bases and enforcement of sophisticated policies.

**Help Desk:** This would involve providing centralized helpdesk for data centers. The help desk should provide flexibility of logging incident manually via windows GUI and web interface**.** The helpdesk would be able to provide seamless integration and classification and categorization of incidents. Help desk would also be able to tracking, escalation and audits for all the incidents.

**Web Management:** This would involve the monitoring of critical web servers. The Web Servers would be proactively monitored for the availability, health and performance of Web servers**.** The web management would include web response monitor and web traffic analyzer, which would help in providing accessibility and performance of the websites.

**Network Security:** This would involve the minimal deployment of the following baseline controls on all network devices. This would involve using access control lists, strong authentication mechanism, intrusion detection and digital certificate verification.

**Anti-Virus:** This would involve maintaining the anti-virus measures in data centers. The anti-virus can be host or web based and would provide inbound and outbound monitoring of all data transfer mechanism and all email systems.

**Host Server Security:** This would involve the deployment of baseline controls on all host servers including detail description of operating/file system controls used to secure servers and access controls (authentication & authorization) on servers, platforms and databases.

This would also involve reviewing access controls rights, admin rights, warning mode for policy implementation and advanced security features.

**Identification, Authentication and Authorization:** This would involve restricting the electronic access to the Web site or application beyond user level access to only authorized persons. In this the users should be uniquely identified and authenticated by the systems. The use of any form of generic or shared user identifier is expressly prohibited.

**Management of Passwords:** This deals with the management of passwords for user. This would involve providing guidelines like changing of passwords in set number of days, encryption of password file, auditing of accounts, using strong passwords etc.

**Data Transmission Security:** This would involve safeguard the confidentiality and integrity of all data being transmitted over any form of data network. This guideline would advise using strong, industry standard encryption for the data identified as 'sensitive' or 'confidential' as per data classification.

**Firewall Services:** This would involve using the firewall tools and services in accordance with the Data Center requirements, policies and procedures, including general maintenance and monitoring of firewalls and implementation of firewall rule set changes.

**Intrusion Detection and prevention Services**: This would involve using the intrusion detection/prevention tools to detect unauthorized access to or unauthorized activity on the networks, computer systems and network devices associated with the State Data Center.

**Security Monitoring:** This would involve providing security monitoring services to its data centers. Specifically this would involve real time monitoring of all systems and network devices/systems to detect potential security violations.

**Incident Response:** This would involve the reporting of any and all security incidents. Specifically this would involve agencies retaining the logs of all security-related systems, to include but not limited to firewalls, intrusion detection systems, access control measures (both electronic and physical) and file integrity checker logs for forensic or evidentiary purposes.

**Backup:** This would involve providing centralized online backup for mission critical applications. The backup solution should be available on various OS platforms such as Windows and UNIX platforms and be capable of supporting SAN based backup / restore from various platforms.

**Storage Resource Management:** This would involve managing and monitoring the storage resources effectives distributed on SAN/ NAS. This would involve discovery of infrastructure and file systems, configuration management, event management and reporting, policy management etc.

## 16. GDCM Data Policy Guidelines

This policy describes Government's administrative system for the secure, timely and efficient sharing of information/data. All information that government needs to collect, store, process, generates or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection. Security classifications indicate the sensitivity of information (in terms of the likely impact resulting from compromise, loss or misuse) and the need to defend against a broad profile of applicable threats. There are three levels of classification:

### Public Data

All routine public sector business, operations and services data should be treated as official - many departments and agencies will operate exclusively at this level.
This includes a wide range of information, of differing value and sensitivity, which needs to be defended against the any threat, and to comply with legal, regulatory and international obligations. This includes:

- ✓ The day to day business of government, service delivery and public finances.
- ✓ Routine international relations and diplomatic activities.
- ✓ Public safety, criminal justice and enforcement activities.
- ✓ Commercial interests, including information provided in confidence and intellectual
- ✓ Personal information that is required to be protected

### Important Data

Sensitive data that requires protection against the highly capable threat profile, and where the effect of accidental or deliberate compromise would be likely to result in any of the following:

- ✓ Directly threaten a liberty or safety of citizens
- ✓ Cause damage to the operational effectiveness of country
- ✓ Cause damage to the operational effectiveness of intelligence operations.
- ✓ Cause major impairment to the ability to investigate or prosecute serious organised crime.

### National Security Data

Exceptionally sensitive information assets that directly support (or threaten) the national security of the particular country or allies and require extremely high assurance of protection from all threats. This includes where the effect of accidental or deliberate compromise would be likely to result in any of the following:

- ✓ Lead directly to widespread loss of life.
- ✓ Threaten directly the internal stability of that particular country.
- ✓ Raise international tension.
- ✓ Cause exceptionally grave damage to the effectiveness or security of that particular country.
- ✓ Cause exceptionally grave damage to relations with friendly nations.
- ✓ Cause exceptionally grave damage to the continuing effectiveness of extremely valuable security or intelligence operations.
- ✓ Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.

Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. As a minimum, all information must be handled with care to comply with legal and regulatory obligations and reduce the risk of loss or inappropriate access. Agencies may need to apply controls above (or below) the baseline on a risk managed basis appropriate to local circumstances and in line with government risk appetite tolerances.  The classification scheme applies to information (or other specific assets). Major ICT infrastructure (e.g. large aggregated data sets, payments systems, etc.) may require enhanced controls to effectively manage associated confidentiality, integrity and availability risks – determined on a case by case basis following a robust risk assessment.

## 17. GDCM Policy Guidelines

### Data Center Behavioral guidelines

This guide line would involve behaviors of people who are using data center as well as the visitors of the data centers. Specifically this would involve about the not damaging the infrastructure, proper attire, not bringing combustible substances and not bringing in any skateboards. This would also involving obeying the instruction of data center staff in terms of inspection, evacuation and addressing the violation of any data center rules.

### Pictures or Video

This would involve the guidelines related to picture and videos in the data centers. Any visitor or any employee is prohibited of using any photographic equipment, audio monitoring and audio capturing devices in data centers.

### Physical Security

This would involve proving the guidelines for the physical security of data center. This guideline dictates that data centers should restricted access, should have 24*7 security staff presence in data center, should have security cameras and should have restricted access to sensitive areas.

### Data Center Ingress and Egress

This guideline deals with visitors must only allowed entering the data center, if it has valid government issued ID and have authorization to access the facility.

### Access List Management

This guideline dictates that ministries and agencies are responsible for maintaining and updating the access list in the data centers.

### Common Areas

This guideline dictates usage of common areas in the data centers. It dictates that people must use common area in proper manner.

### Cage/Cabinet and Cabling Requirements

This guideline would involve around handling of cabinets within data centers. The guideline would detail about the cleanness of cabinets, security of cabinets, and removal of refuse material. This guideline would prohibit creating of office space near cabinet, bringing any combustible material near cabinet, using cabinet's tops for storage, making any alteration to cabinet space and putting operating equipment outside cabinets.

### Rack/Cabinet Doors

These guidelines talks about cabinet doors. This guideline dictates that no one should be allowed to remove or replace cabinet doors and if it needs to done then proper permission should be taken.

### Floor Tiles

These guidelines talks about floor tiles. This guideline dictates that no one should be allowed to lift or move the floor tiles and permission should be given to authorized person only.

### Data Center Equipment

These guidelines talks about loan of equipment to customers. This guideline dictates that agencies are responsible for the loaned equipment.

### Receiving

This guideline talks about receiving the equipment in data centers. All the equipment in data center should be received through receiving dock and it should also bear the agency name on it.

### Removal of Equipment at End of Term

These guidelines talks Removal of Equipment at End of Term, where it dictates that agencies will have all their hardware removed from the Data Center no later than the Effective Cancellation Date.

### Customer Provided Power Strips

This guideline talks about the power strips, where it dictates that agencies are prohibited from plugging their own power strips into Data Center.

### Customer Provided Additional Security Devices

This guideline talks about adding the security devices, where it dictates that agencies are not allowed to add security devices that would hinder agency from accessing their cabinet

## 18. GDCM Financial Guidelines

One of the major aims of Government Data Center Modernization Strategy is to rationalize and optimize the cost it takes for the lifetime of the data infrastructure. The cost optimisation accrued over the life of the Strategy will principally consist of:

| |
|---|
| Increased efficiency in use of data center infrastructure; |
| Reduced data center floor space and associated costs; |
| Increased efficiency of data center ICT assets; |
| Improved matching of data center ICT facilities to business need |
| Standardised ICT infrastructure architectures and earlier use of new technologies |
| Identification and migration to the cost efficient ways of storing and using data. |

Modernization of data center facilities has emerged as a competitiveness critical success factor and, if properly executed, a critical piece of an ongoing strategy to better service citizens. However, modernization comes at a cost and risks and rewards need to be balanced with available budgets. The scale of risk depends not only on the state of the equipment but also the human resources in place to support that equipment. The data center has to be modified in order to accommodate an organization’ s evolving business goals. In an aging data center facility, common issues that need to be resolved include lack of space, inefficient/costly cooling, or a power infrastructure that is not flexible enough to accommodate rapid growth. In addition, infrastructure systems need to be evaluated to determine if maintenance costs are too high or if antiquated systems are threatening the reliability of data center operations.

There are clear financial gains to be achieved in a data center consolidation process, and gains can be measured in different ways:

- Reducing physical locations can reduce overhead and operational costs associated with multiple data center locations or reduce data center energy costs.
- Consolidating software onto fewer hardware platforms can reduce hardware maintenance costs and software licencing fees.
- Modernization can reduce the number of server, storage and network (hardware) units to be purchased, leading to lower acquisition and finance costs.
- Optimizing core business applications such as order processing, inventory management, invoicing or management reports makes support and upgrades easier. So rather than having multiple email or database platforms for various departments, pick one and make it serve the entire organisation.
- Modernization can simplify and reduce errors in system processes such as data protection services, security, network services, system discovery and management.
- Modernization should also examine the business processes themselves and redefine roles and procedures to best utilise computing resources and IT staffing talent.

Thailand Data Center Modernisation is a unique transformation project as it entails large machinery of government infrastructure in the form of agency data centers, which the government has been carefully investing in for last few years.

As articulated earlier, the benefits of Thailand GDCM are varied and cover measurable as well as intangible benefits that will be realized over time.

Key listed benefits include

| | Financial Investment | Financial Benefit |
|---|---|---|
| Adoption of Standards | High investments from adoption perspective.<br>Each agency to comply to identified standards.<br>With reduced reliance on agency DCs, the compliance requirement for standards is reduced. | With high standardized systems, redundancy, data loss is reduced and accuracy of data is achieved. The time to service increases and overall performance of the system, agency and government improves. This translates into financial benefits, in terms of lesser time to operate, lesser computing and data storage required, which adds upto the savings. Adoption to standards also saves various costs like electricity, human resources, service and maintenance. |
| Security Compliance | Based on security requirements, data needs to be migrated to other model. The cost of migration is to be borne in order to increase data security. | The financial loss that would be generated if secured data is lost or infiltrated. The opportunity cost of compliance to security is significant. |
| Capacity Improvement | Rationalization and adoption of efficient ways of working results in capacity improvement. | With capacity improvement, the need to purchase new hardware or operational cost to host data is significantly reduced. |
| Higher Utilization of Government Resources | GDCM will result in higher utilization of government resources. The higher utilization would be achieved by higher migration, reduced or closed Data centers and optimization of delivery.<br>Outsourcing to 3rd party cloud or G-services would be other options. All these options would need financial investments from the government. | Higher utilization will result in lower cost of operations as well as lower need for capital expenses. The operational expenses in turn would generate higher return of investment, this increasing the asset capitalization for Thailand. |
| Cost Optimization | With alternatives ways to host data, newer ways of providing shared services using G-servicing, and ministry, cross agency data will be practiced. This will reduce the reliance on capital budgets but increase the operational expense requirements. | The return on investment will be significant as the agencies will have to maintain fewer assets and focus on getting services at cheaper negotiated costs. |
| Focus on Core Activities | Agencies that will outsource their data needs will be spending higher operational costs but the cost will be spent in an optimized way. | With focus on core activities, agencies will be able to perform their duties better and be able to generate higher ROI on the minimum investments they make |
| Human Resource Transition | With new options for delivery, human resources that already are a limited asset for Thai agencies, will be cross deployed and be used with other services. | The overall cost of hiring and salaries etc will reduce as the current human resource ecosystem will be able to facilitate the transformed ecosystem. |

## 19. GDCM Implementation Plan

Government Data Center Modernization Strategy (GDCM) will be conducted in a phased approach over a period of 5 years (2017-2022). As agencies are constantly changing and evolving their information systems and technology with new data, challenges and issues, it's very important to have a unified strategy and implementation focus to make GDCM successful. There are a number of trigger points such as outsourcing contracts with 3rd party, human resource hiring, asset refreshment cycles, maintenance lease, end of life for data center or asset, expanding data center capacity, capital budgeting exercises etc, which need to be performed and hence it's crucial that the agencies and ministries are on the same page from implementation perspective.

Government Data Center Modernization Implementation Plan outlines the high level plan across next 5 years (2017-2022) for the government and the agencies. Agencies will be required to include actions and outcomes in their individual strategic plans that they will need to develop in year 1 as coordinated with, and conform to the GDCM Strategy.In the first five years, the GDCM Strategy will aim at meeting the following objectives

- ✓ Aggregate the total data center demand and establish feasibility studies to the realization of GDCM Strategy
- ✓ Identify and develop business requirements for the future model
- ✓ Assist early adopters to move to shared resource solutions;
- ✓ Adopt the standards to be used in data center equipment and operations so that maximum efficiencies can be achieved;
- ✓ Established shared service models
- ✓ Adoption by the identified agencies
- ✓ Publish the improvement and progress of the 5 year initiative.

## Drivers for GDCM Strategy Implementation

| Performance Indicators | Strategic Drivers |
|---|---|
| Asset and Capacity Utilization | ▪ Flexibility and openness  for increasing the utilization with clear accountability around defining the appropriate future models as well as internal assessment by the agencies<br>▪ Investment in terms of time and effort to increasing key capabilities of the data center to increase the utilization and identifying steps to improve asset value as well as performance via standard adoption. |
| HR Utilization | ▪ Establish HR training plans by the government to improve the quality and performance of human resources.<br>▪ Agency's openness and focus on enabling employees with government training programmes in terms of enrolment as well as facilitation of training course completion.<br>▪ Agency's approach for HR rationalisation to enable usage of existing human resources efficiently and be able to be utilised across other models like G-Services, Ministry and Cross Agency DCs. |
| Shared Services | ▪ Establish a governance team that monitors the take up on shared services with accountability to the agencies on usage of shared services as per the outlined plan.<br>▪ Develop capabilities, quality, standards, scalability and setup for the shared service options as provided.<br>▪ Proper feasibility study from the agency's perspective to rationally identify data that can be hosted across shared services. |
| Cost Optimization | ▪ Clear accountability of optimising cost by channelizing their data requirements across 6 models appropriately by the agencies<br>▪ Align processes and plan to allow reduce the reliance on government for capital budgets and operational expenses<br>▪ Run budget assessment exercise in year 1 to identify and validate the overall budget that can be saved with the GDCM model |
| Security | ▪ Establish clarity around how to improve security position of the agencies based on ongoing projects, applications and current data hosting.<br>▪ Conducting feasibility analysis by the agencies to identify their security position, risks and identify mitigation plan to meet the security guidelines. |
| Strategic Framework | ▪ Clarity around GDCM strategy, outcomes, key targets and government policy to be developed in year 1.<br>▪ Establish organisation structure to focus on implementation of the strategy as well as monitoring the progress. |

## Design Principles for GDCM Strategy Implementation

The design principles for GDCM Strategy Implementation are developed to guide and support the design and implementation right from Phase 1 of the Implementation plan. It will enable how the Whole of government (WOG) as well as individual agencies and their ministries will transition from As-Is to To-Be.

| Design Principle | | Organisation Design Implications |
|---|---|---|
| **Accountability** | Drive clear ownership and accountability across the ecosystem and within end-to-end processes | ▪ Accountability for end-to-end ecosystem may sit entirely within government or individual agency.<br>▪ Clear accountability must be established at agency, people responsibility, government responsibility or administration responsibility<br>▪ Clear accountability will drive performance success of individuals and teams |
| **Country Growth** | Capable of supporting and driving the growth of Thailand in terms of people, data, quality, technology advancement and digital economy | ▪ Developing capabilities at Thailand to enable and support the countries growth<br>▪ Give authority to agencies to select the best suitable option to select out of 6 service models based on issued guidelines<br>▪ Train and get people ready for transformation.<br>▪ Aim to develop country into a technology enabled hotspot from the perspective of data growth readiness. |
| **Capability** | Focus on strengths and build capabilities across the ecosystem to realise the benefits | ▪ Centers of excellence may be created to focus on training and learning.<br>▪ Government to identify early adopters for new future state models who can become role models for the change.<br>▪ Identify capability gaps and build the government infrastructure to support capability development<br>▪ Data integration and classification is an area of importance to realise the economies of scale, clear roles and responsibilities, saving space and replication of data as well as effort. |
| **Innovation** | Facilitate innovation as well as take up on better technology solutions that enable growth | ▪ Protect current strength and core competences of agencies, systems, applications etc. if the current infrastructure is absolutely essential and the new infrastructure does not have ability to provide.<br>▪ Establishment of shared services from the agencies-ministry as well as cross agency with utilization of multiple standard elements to improve and expand the infrastructure.<br>▪ Development of G-services as well as enabling take up of cloud services (G-services as well as 3rd party) to grow<br>▪ Encourage an innovation culture which provides the right environment to take informed risks |

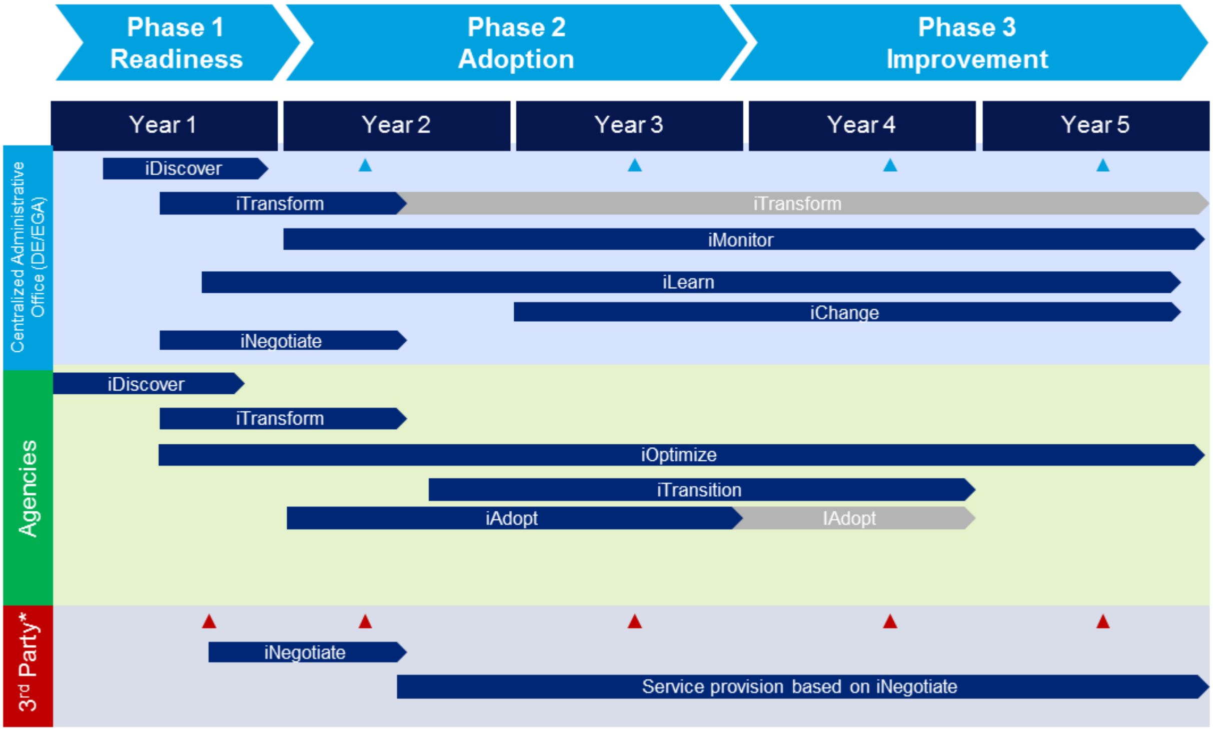
| Design Principle | | Organisation Design Implications |
|---|---|---|
| **Collaboration** | Create a structure which encourages cross-functional collaboration and effectiveness | Leverage collaborative culture to increase effectiveness by clarifying interfaces and accountabilities<br>Develop strategic frameworks to facilitate collaboration and decision making |

## GDCM Strategy Implementation Plan Basis

| Area | Implementation Plan basis |
|---|---|
| **Accountability** | The plan is based on accountability defined for government as having control for governance, developing the policy, framework, running various projects and initiatives, driving strategy for cost optimisation, training & data transition.<br>The plan is based on accountability defined for agencies as having control over their decision making for choosing the way they would like to operate in future, right to conduct feasibility study, benefits realisation and in effect, movement to alternative mechanism. |
| **Activity Sequencing** | The sequencing of activities in the implementation plan is based on prioritising activities that enable the transition and that will enable the achievement of project drivers and benefits. |
| **Business as Usual** | The plan is based on ensuring that capabilities being developed will be developed and maintained through a central body and will be launched with minimum impact to the agencies. The data transition also will be conducted to enable BAU. |
| **Governance / Strategy** | The plan is based on establishing critical governance and strategies GDCM strategy |
| **IT Infrastructure** | The plan is based on establishing appropriate IT infrastructure and identifying 6 options for agencies to consider. |
| **Engagement** | The plan is based on putting administrative team in place before establishing. Internal agency transitioning teams will closely be engaged in the decision making as well as the transition in future. |
| **Constraints** | The plan does not reflect potential constraints there may be around budgeting and resourcing, nor integration with other programmes and projects |
| **Implementation** | The plan includes a number of key activities required to be undertaken prior to the start of implementation to allow for a running start to implementation and to both mitigate risk and manage the change.<br>The implementation period of 5 years is developed in such a way that it gives 1 year for readiness and assessment. |

# GDCM Implementation Plan (Short version)

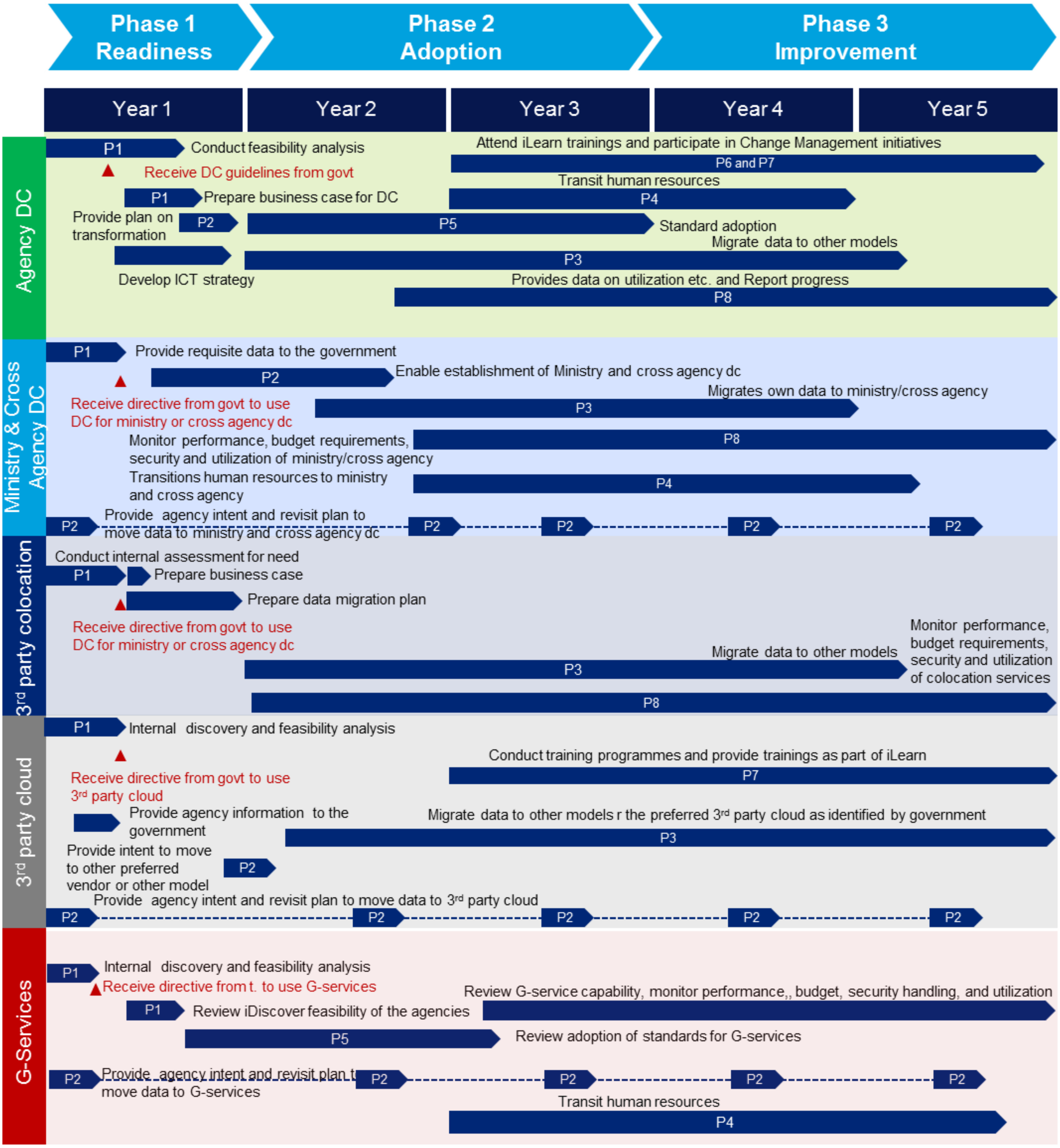
The implementation plan below highlights the key expectations and coverage across 5 years' timeline.



*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 |

# GDCM Implementation Plan for the Government Agencies



Phase 1 Readiness

Phase 2 Adoption

Phase 3 Improvement

Year 1

Year 2

Year 3

Year 4

Year 5

Agency DC

P1 Conduct feasibility analysis

Receive DC guidelines from govt

P1 Prepare business case for DC

Provide plan on transformation P2

Develop ICT strategy

P5

Attend iLearn trainings and participate in Change Management initiatives

P6 and P7

Transit human resources

P4

Standard adoption

Migrate data to other models

P3

Provides data on utilization etc. and Report progress

P8

Ministry & Cross Agency DC

P1 Provide requisite data to the government

P2 Enable establishment of Ministry and cross agency dc

Receive directive from govt to use DC for ministry or cross agency dc

Migrates own data to ministry/cross agency

P3

Monitor performance, budget requirements, security and utilization of ministry/cross agency

P8

Transitions human resources to ministry and cross agency

P4

P2 Provide agency intent and revisit plan to move data to ministry and cross agency dc P2 P2 P2 P2

3rd party colocation

Conduct internal assessment for need

P1 Prepare business case

Prepare data migration plan

Receive directive from govt to use DC for ministry or cross agency dc

Migrate data to other models

P3

Monitor performance, budget requirements, security and utilization of colocation services

P8

3rd party cloud

P1 Internal discovery and feasibility analysis

Receive directive from govt to use 3rd party cloud

Conduct training programmes and provide trainings as part of iLearn

P7

Provide agency information to the government

Migrate data to other models r the preferred 3rd party cloud as identified by government

P3

Provide intent to move to other preferred vendor or other model P2

Provide agency intent and revisit plan to move data to 3rd party cloud

P2 P2 P2 P2 P2

G-Services

P1 Internal discovery and feasibility analysis

Receive directive from t. to use G-services

P1 Review iDiscover feasibility of the agencies

Review G-service capability, monitor performance,, budget, security handling, and utilization

P5

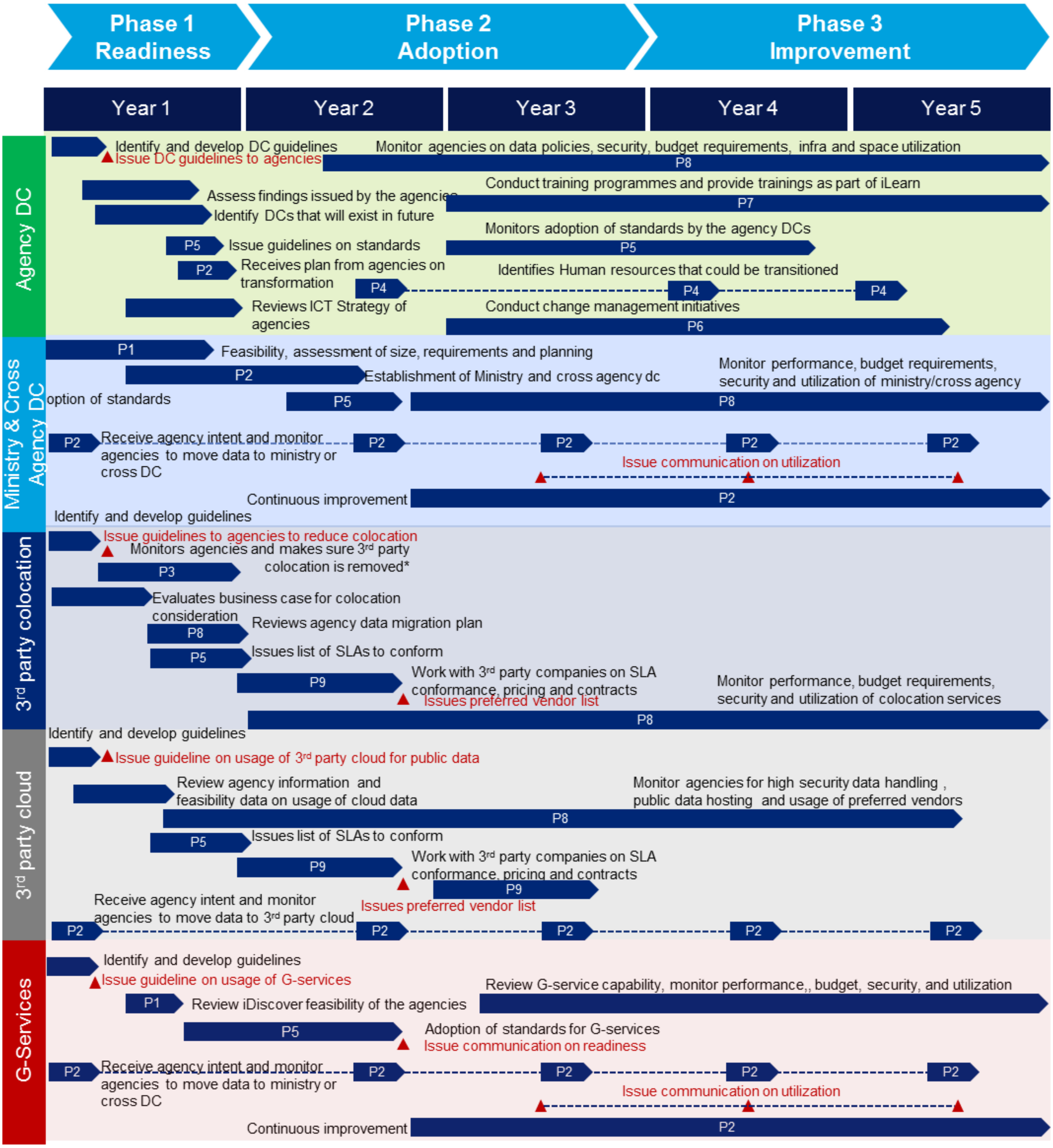
Review adoption of standards for G-services

P2 Provide agency intent and revisit plan to move data to G-services P2 P2 P2 P2

Transit human resources

P4

# Implementation Plan for the Government (GDCM Administrative Office)



Phase 1 Readiness

Phase 2 Adoption

Phase 3 Improvement

Year 1

Year 2

Year 3

Year 4

Year 5

**Agency DC**

Identify and develop DC guidelines

▲ Issue DC guidelines to agencies

Monitor agencies on data policies, security, budget requirements, infra and space utilization

P8

Assess findings issued by the agencies

Identify DCs that will exist in future

Conduct training programmes and provide trainings as part of iLearn

P7

P5 Issue guidelines on standards

Monitors adoption of standards by the agency DCs

P5

P2 Receives plan from agencies on transformation

Identifies Human resources that could be transitioned

P4

P4

P4

Reviews ICT Strategy of agencies

Conduct change management initiatives

P6

**Ministry & Cross Agency DC**

P1 Feasibility, assessment of size, requirements and planning

P2 Establishment of Ministry and cross agency dc

option of standards

P5

Monitor performance, budget requirements, security and utilization of ministry/cross agency

P8

P2 Receive agency intent and monitor agencies to move data to ministry or cross DC

P2

P2

P2

P2

Issue communication on utilization

▲ ▲ ▲

Continuous improvement

P2

Identify and develop guidelines

**3rd party colocation**

Issue guidelines to agencies to reduce colocation

▲ Monitors agencies and makes sure 3rd party colocation is removed*

P3

Evaluates business case for colocation consideration

Reviews agency data migration plan

P8

P5

Issues list of SLAs to conform

P9

Work with 3rd party companies on SLA conformance, pricing and contracts

▲ Issues preferred vendor list

Monitor performance, budget requirements, security and utilization of colocation services

P8

Identify and develop guidelines

**3rd party cloud**

▲ Issue guideline on usage of 3rd party cloud for public data

Review agency information and feasibility data on usage of cloud data

Monitor agencies for high security data handling , public data hosting and usage of preferred vendors

P8

P5

Issues list of SLAs to conform

P9

Work with 3rd party companies on SLA conformance, pricing and contracts

▲

P9

Receive agency intent and monitor agencies to move data to 3rd party cloud

Issues preferred vendor list

P2

P2

P2

P2

P2

**G-Services**

Identify and develop guidelines

▲ Issue guideline on usage of G-services

Review G-service capability, monitor performance,, budget, security, and utilization

P1 Review iDiscover feasibility of the agencies

P5

Adoption of standards for G-services

▲ Issue communication on readiness

P2 Receive agency intent and monitor agencies to move data to ministry or cross DC

P2

P2

P2

P2

Issue communication on utilization

▲ ▲ ▲

Continuous improvement

P2

# GDCM Strategy Implementation Projects

9 Projects are identified as a part of Implementation Strategy to enable the management as well as swift implementation of GDCM.

| Type | Project Name and Aim | Description of Project |
|---|---|---|
| (P1)<br>Project 1 | **iDISCOVER**<br>*Discovery study to understand feasibility of the model and requirements for alternate hosting* | ▪ This project covers conducting feasibility study and analysis by the agencies to discover their real needs and implementation readiness<br>▪ 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.<br>▪ Government also conducts iDiscover study to identify readiness and feasibility of Ministry DC, cross agency DC and G-Services.<br>▪ The iDiscover project will enable coverage for agencies to identify the right future models to focus on. |
| (P2)<br>Project 2 | **iTRANSFORM**<br>*Project to transform agency data centers into ministry and cross agency DCs* | ▪ This project identifies the criteria for selection of ministry and cross agency data centers.<br>▪ 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.<br>▪ Following the discovery of business requirements, the DCs will be converted to ministry and cross agency DCs<br>▪ This is followed by running communication plan, monitoring the progress, utilization of the transformed data centers. |
| (P3)<br>Project 3 | **iOPTIMIZE**<br>*Project to migrate data from one model to other* | ▪ This project entails the data transition across the model after feasibility study and planning exercise is complete.<br>▪ 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.<br>▪ 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)<br>Project 4 | **iTRANSITION**<br>*Project to deploy human resources* | This project focuses on human resource transition across various models.<br>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.<br>These resources will go through a process of transition based on their job roles |

| | | |
|---|---|---|
| | *across agencies and models as required* | |

| | | |
|---|---|---|
| **(P5)**<br>**Project 5** | **iADOPT**<br>*Project to adopt the identified standards* | ▪ This project enables adoption of the standards across the agencies as well as Gservices.<br>▪ This project will start with feasibility analysis for standard adoption and identify guidelines for agencies to adopt based on “waves” developed in Phase 1.<br>▪ 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<br>▪ Government will monitor the adoption of the agencies and will provide reporting.<br>▪ Government will ensure that the ministry DCs cross agency DCs and the G-services comply to set standards. |
| **(P6)**<br>**Project 6** | **iCHANGE**<br>*Project to management change implementation and management* | ▪ 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.<br>▪ Government will plan change management events as well as analysis of the degree of change and identify gaps that needs to be filled.<br>▪ 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<br>▪ Government will monitor the change and will use communication plan, culture dissemination and transition plan to seamless settling the change. |
| **(P7)**<br>**Project 7** | **iLEARN**<br>*Project to provide training to human resources* | ▪ The project involves identifying training needs of the agency staff that needs to be provided as a part of transformation programme.<br>▪ 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.<br>▪ These trainings will be developed by the government representative or 3rd party as and needed.<br>▪ Government will develop and provide a calendar of event to conduct these trainings.<br>▪ Government will impart the trainings and measure its effectiveness. |

| | | |
|---|---|---|
| (P8)<br>Project 8 | **iMONITOR**<br>*Project to monitor and report progress* | ▪ This project involves monitoring the progress of data migration and take up of the 6 areas.<br>▪ Government will periodically monitor and report the progress to the agencies and will promote the progress and setup of the new areas |
| (P9)<br>Project 9 | **iNEGOTIATE**<br>*Progress to negotiate better rates, services, SLAs with 3rd. party* | ▪ 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. |

## GDCM Strategy Implementation Assumptions

| Assumption | Description |
|---|---|
| **Accountability** | The plan assumes the definition of accountability identified in the Key Design Principles. Further sophistication accountability will be developed in Phase 1 of the implementation. |
| **Phase 1 readiness** | The plan assumes a start of pre-implementation activities before the start of phase 2 as a part of Phase 1. |
| **Resourcing** | The plan assumes that the appropriate level of resourcing both in terms of project personnel and input from the agencies will be provided in order to deliver the necessary changes. The Phase 1 incorporates various studies and analysis to identify the change. |
| **Change Management** | The plan assumes that in order for change to be successfully implemented culture and change activities will be undertaken to enable the transition. |
| **Stakeholders** | The plan assumes that external stakeholders will not delay or prevent implementation (e.g. agencies, political situation) |
| **Process and Policies** | The plan assumes that pragmatic processes and policies will be defined in line with transitioning accountability in Phase 1 |
| **Strategy** | The plan assumes that any transition work being currently undertaken will not significantly change the organisation structure or implementation plan. |
| **Resource Requirements** | The plan assumes that resource requirements needed for implementation and governance will be identified and on boarded seamlessly. |

# GDCM Strategy Implementation Critical Success Factors

| Critical Success Factors | Requirements |
|---|---|
| Support and commitment from the Government | ▪ Continuous engagement of the government including Department of Digital Economy and other technology departments to support the initiative and maintain the momentum |
| Availability of Human Resources | ▪ Identification of right human resources for the governance<br>▪ Identification of back up plans for human resource availability<br>▪ Providing continuous training and learning to the teams to support the transition and rapid performance improvement |
| Strategic Framework | ▪ Clearly defined strategy and the framework to support the enforcement. |
| Financial resourcing and planning | ▪ Recognition of GDCM as a priority area in the Government Agenda<br>▪ Identifying financial resourcing and earmarking budget for Ministry, Cross Agency set up, Feasibility Studies by the government and the agencies as well as development of G-Services and implementation of standards. |
| Commitment by all parties | ▪ Commitment by all parties including government, government representative agency to manage the transformation, technology partners, service providers, agencies and ministries<br>▪ Active coordination amongst key stakeholders to develop and enforce the GDCM strategy |
| Sustainable Infrastructure | ▪ Provide and make available, the infrastructure as identified and developed in GDCM strategy<br>▪ Enable network and information security as planned<br>▪ Provide infrastructure to support the transition. |
| Availability of research and studies | ▪ Conduct multiple studies to identify and elaborate on the strategy for the implementation in Phase 1.<br>▪ Identification of change agents<br>▪ Identification of early adopters |

## GDCM Strategy Implementation Risks

| Risk | Mitigation Actions |
|---|---|
| Business performance could suffer during transition | ▪ Ensure robust transition structures are in place to help manage the transition<br>▪ Identify areas of concern and monitor closely<br>▪ Allow sufficient time to build new capabilities |
| Losing human resources to transition | ▪ Develop a retention policy to incentivise key individuals<br>▪ Engage key individuals in the change<br>▪ Openly discuss future career prospects with those who might be concerned they are at risk<br>▪ Cross-train where possible<br>▪ Implement knowledge sharing practices |
| Not finding good resources to fit key roles if needed | ▪ Allow sufficient time for recruitment/selection<br>▪ Be realistic about what is available and be open to modifying roles slightly to accommodate candidates<br>▪ Create development plans for internal candidates |
| Failing to preserve what works well today | ▪ Clearly identify what data need to be preserved and identify data/applications that should go through transition.<br>▪ Monitor those areas during implementation |
| Not having right technology in place to support the change | ▪ Identify technology requirements required to support organisational changes<br>▪ Plan the organisational changes implementation to accommodate technology implementation or accelerate the technology implementation to accommodate the organisational changes implementation<br>▪ Define alternative established models like 3rd party cloud to support the changes |
| Resistance to change: Agencies not supporting desired ways of working | ▪ Identify the agency requirements required to support the change in phase 1<br>▪ Consider commencing a change management programme that addresses awareness, capability, reinforcing mechanisms and role modelling to support the new ways of working |
| Damaging agency relationships during transition | ▪ Communicate to agencies using a communication plan<br>▪ Create clear instructions for CAO on how to work with agencies during the transition |
| Governance Structure as well as infrastructure becoming overloaded with change | ▪ Run feasibility plan for the implementation readiness in Phase 1<br>▪ Develop implementation plan in accordance with other changes also going on<br>▪ Monitor change readiness and employee engagement throughout the transition |
| Technology Failure | ▪ Use business continuity plan for the agencies. Agencies develop BCP for the transition period<br>▪ Use disaster recovery plan |

| | |
|---|---|
| Privacy and Security Concerns | ▪ Implement security measures as outlined in the standard adoption<br>▪ Follow implementation readiness as outlined in phase 1 for security handling |

## 20. GDCM Strategy Guidelines

In the past, Thai agencies focused our data center investments on improving IT infrastructure as a means to deliver a foundation for the efficient growth of the agencies data center needs. But, in the current level of maturity as well as operational drivers and constraints, it's crucial for Thai agencies to focus on the elements like security; data center efficiency, infrastructure simplification, reduction of energy consumption and overall cost optimization; to enable a sustainable growth.

Our transformational strategy is to utilize a disciplined approach to change management and adopt the underline policy, directives and plans set along the implementation journey for the agencies.

In keeping pace with the change in infrastructure pattern, usage and the way data is handled, we will realize every key benefit that has been highlighted for the effective data center infrastructure. With a refreshed infrastructure, adopting new areas like G-Services, 3rd party cloud as well as shared services in the form of Ministry and Cross-Agency Datacenters, there will be a huge growth, not only in the capability development, but also ability to handle large and increasing data volumes, preparedness for future as well as long term sustenance.

The performance of the strategy can be measured over next few years through the following indicators which will be refined in year 1 of the strategy:

1. Effective Utilization of assets, capacity and resources
2. Cost efficiency
3. Enhanced security
4. Shared services
5. Strategic Framework

### 1. EFFECTIVE UTILIZATION OF ASSETS, CAPACITY AND RESOURCES

Our data center strategy represents how assets (government assets in the form of data centers, network and key enablers for DC setup, G-Services), capacity (in the form of DC space, bandwidth, servers/storage) as well as resources (including human resources) are effectively utilised. An effective utilization would mean that agency has just enough resources, assets and capacity to meet their needs (including the scalability for growing needs) with minimum wastage. The future model for Data Infrastructure is developed keeping in mind, the agility as well as the need for higher utilization of government assets. With a high focus on the utilization of assets, capacity and resources, government will be able to support the agencies and the nation with nimbleness.

### 2. SHARED SERVICES

As a part of digital economy and citizen centricity, one of the key elements for GDCM strategy is the ability to offer Shared Services and the strategy to grow the provision. Shared services can be viewed from various perspectives of increased availability, reliability, security, cost optimization, responsiveness to the citizens and compliance to set standards. The GDCM strategy highlights the usage of various shared service models ranging from increasing the agency capabilities to offer shared services to neighbouring agencies to increase their own utilization to utilizing government developed ministry and cross agency data center. Shared services also include utilising government services (G-Services) that include G-Cloud and government colocation services. Agencies may also choose the 3rd party cloud model to host their data. From a KPI perspective, it's vital to know how many agencies and at what level of transformation have been adopting the shared service capabilities developed by the government or covered in the GDCM strategy.

## 3. COST EFFICIENCY

Our data center strategy represents a large shift in how the cost efficiency was being treated with the rapid growth in the data center requirements in the past. With focus on cost efficiency, the key requirements for the government would be to reduce the reliance on new capital investments via the use of latest technologies using the shared services model. The efficacy of shared services in the form of Ministry and cross-agency data centers has been highlighted earlier to enable an integrated infrastructure to support the ministries and multiple agencies together. These shared service models are created to enable secured, integrated, cost effective and highly scalable options to the agencies to enable seamless servicing. The other models including G-Services as well as 3rd party cloud also represent a massive shift in the way agencies view data centers as the only option to meet their data requirements. With our new data center strategy, agencies will be able to focus on their core activities with reduced need for human resources as well as data center support by utilizing cloud based services. G-services in particular, will be a scalable infrastructure supported by the government to enable a secured cloud based servicing to the agencies. The government will in turn be responsible to ensure that the SLAs, security and the standard guidelines for G-services are established and maintained. From operational expenses perspective, the goal of the government is not to reduce the spending in particular but to ensure that each Thai-baht spent as operational expense is utilized effectively and gets a higher return on government investment.

## 4. ENHANCED SECURITY

The GDCM strategy highlights security as one of the crucial drivers for developing the modernization strategy as in today's time, it's become increasingly important to maintain and manage the security of the national data. Every bite of government data is an important element and the GDCM strategy recognises the need to save-guard it's asset.

With the new strategy, agencies are urged to utilise the 6 future models judiciously, to maintain and enhance their security position of the data. As following steps, government will conduct multiple studies to identify the security positioning of the agencies which will be assessed during various phases of the transformation. With right security handling of the national data, it will improve the security handling capability as well as future data handling mechanism for years to come.

## 5. STRATEGIC FRAMEWORK

GDCM Strategy identifies the strategic motive, aim, mission as well as key initiatives that the government plans to implement a modernization strategy. A very important indicator for the success of the Strategy is to check the efficacy of the strategy formulation, ratification, enforcement and implementation. KPIs can be set for the government as well as the agencies to enable a seamless functioning of the strategy and follow through of the activities in year 1 of strategy establishment.

Following is a list of some of the identified Key Performance Indicators (KPIs') that can be used as a part of Strategy.

| *Area* | *KPIs* |
|---|---|
| 1a. Utilization of Assets and Capacity | • % of Data Centers Closed<br>• % of Data Center requirements significantly reduced<br>• % Increase of Data Center capacity utilization<br>• % of Increase of Server Utilization |
| 1b. HR Utilization | • % of Human Resources Trained on Data Center process<br>• % of Human Resources cross deployed and transitioned<br>• Number of Training Sessions conducted<br>• % of senior IT staff trained on agency process and linkage with DC<br>• % of IT staff trained in DC area expertise |
| 2. Shared Services | • Number of Ministry/Cross Agency DC established<br>• Number of agencies moving their data<br>• % of data hosted on Ministry/Cross Agency, 3rd party Cloud and G-Services<br>• Number of 3rd party vendors with negotiated rates and priority list prepared by government<br>• % of services conducted independently through G-Services<br>• % of services conducted independently through Ministry and Cross Agency DC<br>• % of services conducted independently through 3rdparty cloud. |
| 3. Cost Optimization | • % of capital budget requirement increase/decrease because of optimisation<br>• % of operational cost requirement increase/decrease because of optimisation<br>• % overall reduction in budget allocation |
| 4. Security | • % of agencies that migrated data based on the plan |
| 5. Strategic Framework | • GDCM Strategy Organisation Structure<br>• Government Policy and Framework<br>• Feasibility Analysis Report Submission by Agencies<br>• ICT Strategy of Ministries and Agencies<br>• ICT Implementation Plan of Ministries and Agencies |

## 21. GDCM Human Resource Guideline

Human resources are most important asset of any government infrastructure. In today’s world, data centers are critical in supporting the development and operations of nearly every sector of the economy. With growing complexity of the data infrastructure, getting right talent and in adequate numbers has become a big challenge for agencies and the government. The data center industry is experiencing a shortage of personnel. his trend reflects, in part, an aging global demographic but also increasing demand for data center personnel

Drivers of the data center market are similar to those that drive overall internet growth and include increasing broadband penetration, e-commerce, video delivery, gaming, social networking, VOIP, cloud computing and web applications that make the internet and data networking a key enabler of business and consumer activity. More qualified personnel are required to respond to this accelerated growth.

Thailand agencies believe that human resource capability is one of the most important challenge that the agency data centers are facing today.

The following is the guideline on the level of jobs and the expertise required in a data center. These skills are similar across all future forms –Outsourced Service Providers as well as internal data centers.

| | |
|---|---|
| Data Center Test Engineer | Tasked with setting up environments in order to test PC and network solutions within the data center, while also exposing any issues and identifying major contributing factors. |
| Data Center Environmental and Safety Technician | Offering support and monitoring the various environmental, health and safety activities within the data centers, it’s your responsibility to investigate any safety issues while conducting environmental training. |
| Infrastructure Architects | Responsible for the design of the data center, infrastructure architects typically take care of any supporting services such as cooling and power – while project managers ensure any major installations are well maintained. |
| Data Center Manager | Overseeing the general running of the facilities, it’s imperative that data center managers have a wide range of knowledge of all things data center-related – from understanding about network and operating systems to knowing the correct protocols and processes. |
| Electrical Engineer, Data Center R&D | Working in a team that helps design and build the software, hardware and networking technologies, your role as a hardware engineer sees you develop small scale projects right through to high volume manufacturing. |

| | |
|---|---|
| Data Center Maintenance Planner/Scheduler | As a data center maintenance planner/scheduler, this involves communicating both internally as well as maintaining regular contact with clients. Planning requirements for customers and managing entire project lifecycles, you ensure efficient execution of the various planning and scheduling processes – additionally, providing equipment-related knowledge and technical expertise on improving preventive maintenance tasks. |
| Data Center Control Systems Staff Engineer | This role usually entails at least 10 years' experience as well as a relevant degree, with experience in critical infrastructure such as industrial automation, SCADA systems and PLCs. Providing technical support to the engineering and operations teams, your responsibilities encompass resolving any critical electrical controls related matters along with handling any procurement and vendor management issues. |
| Network & Security Engineer | Owning all aspects of the ICT strategy, including the overall system architecture and road-map through to detailed design and implementation through to operations.<br>Architect all IT systems and data center management systems<br>Manage and organise the data center operations network |

Many of these job roles are high priority roles across the agencies. With limited government budget, the brighter talent likes to work for corporates than working for government agencies. A huge amount of talent also migrates to other parts of the world to look out for better opportunities. The result is that the local markets are in dearth of right talent.

Thailand GDCM initiative aims at:

- Nurturing the current talent and safeguarding their jobs and roles for the future. Government wil enable identification of transition roles across agencies and other government supported models like Ministry Data Cen ter, Cross Agency Data Center, G-Services etc.
- Provide trainings, skilling and re-skilling current human resources to face the market realities and learn the latest information to enable better performance.
- Establish HR training plans by the government to improve the quality and performance of human resources.
- Agency's openness and focus on enabling employees with government training programmes in terms of enrolment as well as facilitation of training course completion.
- Agency's approach for HR rationalisation to enable usage of existing human resources efficiently and be able to be utilised across other models like G-Services, Ministry and Cross Agency DCs.

Human resources outsourcing continues to flourish as a key element in an organization’s broader strategic approach to growth. A 2013 survey conducted by the Society for Human Resources Management pinpointed the six most common reasons why businesses increasingly rely on this resource:

- Save costs
- Focus on strategy
- Improve compliance
- Improve accuracy
- Gain access to HRO expertise
- Take advantage of technology

Human resources outsourcing is increasingly seen as a critical option for government agencies with the following benefits:

- Greater productivity – Rather than handling routine administrative tasks, employees can focus on more strategic functions.
- Access to advanced technology – The use of state-of-the-art equipment without having to own it.
- Expert help with compliance information – Allowing a trusted provider to stay up to date on changing laws related to hiring, insurance claims management, and benefits regulations.

Human resources outsourcing can enable agencies to grow without making it necessary to hire additional personnel, and by assisting with compliance issues, can help minimize the threat of financial consequences due to a failure to comply with state and federal employment regulations.

## Current and Future Trends

- Moving to the Cloud. Transferring company HR data off of servers and into the cloud is becoming the standard approach across many government agencies Human resources outsourcing providers point to the cloud's more efficient data security processes and its value in enabling businesses to maintain operational continuity. Cloud-based Human Resources Outsourcing aids in advanced reporting and analytics, as well as integrated employee support and related HR functions.
- Process Automation. Building on the use of cloud-based HR platforms, smart process automation can improve productivity, simplify employee benefits management, and can significantly reduce manual back-office functions.
- Selective Outsourcing. Another continuing trend is selective outsourcing, in which companies outsource specific employee administration functions requiring specialized knowledge while retaining other functions in-house. Selective outsourcing can be an effective approach for candidate recruitment, compliance with the creation of an employee handbook, and non-harassment training.
- Social Media Recruiting. Many HR outsourcing providers are expanding their social media recruitment and selection efforts, hoping to capitalize on the growth and diversity of business-focused platforms.

# Appendix A: GDCM Data Policy Guidelines

## Security

- Everyone who works with government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.
- Accidental or deliberate compromise, loss or misuse of government information may lead to damage and can constitute a criminal offence. Individuals are personally responsible for protecting any government information or other assets in their care, and must be provided with guidance about security requirements and how legislation relates to their role, including the potential sanctions (criminal or disciplinary) that may result from inappropriate behaviours.
- Agencies/government must have a breach management system in place to aid the detection and reporting of inappropriate behaviours, enable disciplinary procedures to be enforced and assist with any criminal proceedings.

## Sensitive Information

- Access to sensitive information must only be granted on the basis of a genuine „need to know‟ and an appropriate personnel security control.
- Information needs to be trusted and available to the right people at the right time. The failure to share and exploit information can impede effective government business and can have severe consequences (e.g. medical records or case management files). The principles of openness, transparency, open Data and information reuse require individuals to consider the proactive publishing of public sector information and data sets. However, this must always be a reasoned judgement, taking data protection and confidentiality into account.
- The compromise, loss or misuse of sensitive information may have a significant impact on an individual, an organisation, or on government business more generally. Access to sensitive information must be no wider than necessary for the efficient conduct of an organisation's business and limited to those with a business need and the appropriate personnel security control. This „need to know‟ principle applies wherever sensitive information is collected, stored, processed or shared within government and when dealing with external public and private sector organisations, and international partners.
- The more sensitive the material, the more important it is to fully understand (and ensure compliance with) the relevant security requirements. In extremis, there may be a need to share sensitive material to those without the necessary personnel security control, for example when immediate action is required to protect life or to stop a serious crime. In such circumstances a common sense approach should be adopted - if time permits, alternatives should be considered and steps taken to protect the source of information. If there is any doubt about providing access to sensitive assets, individuals should consult their managers or security staff before doing so and when time permits record the reasons for their actions.

## Asset Protection

- Assets received from or exchanged with external partners must be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.
- The policy applies equally to assets entrusted to government by others, such as foreign governments, international organisations, NGOs and private individuals.
- Where specific reciprocal security agreements / arrangements are in place with foreign governments or international organisations, equivalent protections and markings must be recognised and any information received must be handled with at least the same degree of protection as if it were Thailand information of equivalent classification.
- Where no relevant security agreements / arrangements are in place, information or other assets received from a foreign country, international organisation or a Thailand NGO must at a minimum be protected to an equivalent standard as that afforded to government official assets, although higher classifications may be appropriate.
- Data Owners are responsible for identifying any sensitive information within this category and for putting in place appropriate business processes to ensure that it is securely handled, reflecting the potential impact from compromise or loss and in line with any specific statutory requirements. Individuals should be encouraged to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate.
- To support specific business requirements and compartmentalise information, agencies may apply an optional descriptor, alongside the official sensitive classification marking, to distinguish particular types of information and indicate the need for additional common sense precautions to limit access.
- Organisations may apply a descriptor to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes. Descriptors should be used in conjunction with a security classification and applied in the format: „public-sensitive [descriptor]'
- Government can maintain the following list of core descriptors to ensure a consistent approach is adopted across all departments:
- Descriptors must not be applied to information that is sent to overseas partners (unless formally agreed in advance) as they are not recognised under any international agreements and are likely to cause confusion.

## Codewords

Code words provide security cover for a particular asset or event. A Codeword is a single word expressed in capital letters and is placed immediately after the classification marking. They are usually only applied to sensitive and secret data points.

## Working with Security Classifications

- Security classifications can be applied to any data point that has value to the business. This includes information in whatever form (but not the IT systems used to store or process classified information), items of equipment, hardware and other valuables. Classification markings should be clear and conspicuous, including any special handling instructions. Where it is impractical to apply a marking (e.g. on equipment), staff must be made aware of the protection and procedures required. Where an asset has inherent transferable value or the nature of the item dictates the need for special handling (e.g. firearms, toxic / atomic materials etc.), organisations must ensure that appropriate (in some cases, statutory) controls are in place to protect against compromise, loss or damage.
- When working with information assets, the following points need to be considered:
- There is no requirement to explicitly mark routine public assets.
- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise.
- When working with documents, classifications must be in capitals at the top and bottom of each page. More sensitive information should be separated into appendices, so the main body can be distributed widely with fewer restrictions.
- Sensitive material published on intranet sites must also be clearly marked.
- It is good practice to reference the classification in the subject line and / or text of email communications. Where practicable systems should compel users to select a classification before sending, e.g. via a drop-down menu.
- Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Every effort should be made to consult the originating organisation before a sensitive asset is considered for disclosure
- A file, or group of sensitive documents or assets, must carry the highest marking contained within it. For example, a paper file or an e-mail string containing and secret material must be covered by the higher marking (i.e. secret).
- E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an e-mail „string‟ before they add to it and forward it on.
- In certain circumstances there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitised digest or pre-agreed form of words at a lower classification in anticipation of such a requirement.
- Where practicable, time-expiry limits should be considered so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g. official statistics.

## Valuing technology assets: Confidentiality, Integrity and Availability

- ICT systems need to keep information confidential, but also maintain the integrity and availability of information and / or services. The degree of impact on the business from a loss of availability or integrity may vary and should be considered as part of a comprehensive risk assessment process that takes into account threat, vulnerability, likelihood and mitigations.
- In certain contexts, the loss or compromise of integrity or availability may be so catastrophic that enhanced controls to mitigate these risks will be required even if the likelihood seems slight. Moreover, there are statutory security requirements that must be upheld in number of specialist fields, such as atomic materials, air safety, firearms, and witness protection.
- The compromise of a significant volume of data (e.g. personal data) is likely to have a higher impact than the loss of individual information assets, and may merit more restrictive handling controls. Likewise, the inter-connectivity of different data sets may allow more sensitive connections to be made by association. Aggregation, accumulation and association of data (within ICT systems and on removable media) must be carefully considered as part of the risk management process as additional protective controls may or may not be appropriate.

## Physical Security: Risk Assessment Methodologies

- Physical security controls for the protection of government assets should be applied according to layering principles. A risk assessment is required to determine applicable threats and risks.
- Once the threat(s) to the information is/are understood, and prior to purchasing or deploying a new security system or product, an Operational Requirement (OR - a structured methodology for determining security requirements) should be undertaken.
- Where assets require protection from surreptitious attack, the „Security Assessment for Protectively Marked Assets‟ (SAPMA) risk assessment methodology should be completed to determine suitable additional security controls to prevent or detect compromise.

## Information Security Principles

- Information at any level of classification should receive broadly consistent levels of protection across the Public Sector. This consistency is essential to establish trust between organisations and promote greater interoperability.
- The broad risk appetite for information types will be overseen by the appropriate pan-government governance body. For the public, sensitive and secret tiers government need to set up a governing body to access the security risk.
- Public Sector organisations continue to own and manage their own information risk, within the bounds of the top level government risk appetite set by the governing body. Within this framework there remains an enduring requirement for organisations to assess their own information risks and make appropriate accreditation decisions which balance risk with realising business opportunities.

## Confidentiality, Integrity and Availability Considerations

- The Classification Policy relates to confidentiality requirements. However, Public Sector information and services often have significant Integrity and/or availability requirements too. There exist many scenarios where the consequences of a loss of integrity or availability can be significantly more severe than a loss of confidentiality.
- A high Integrity or Availability requirement does not lead to a high classification. A holistic risk assessment must be conducted, which includes the consideration of risks to confidentiality, integrity and availability respectively. Treatment of significant Integrity or availability requirements may require robust technical controls and a high level of assurance, over and above that indicated by the (confidentiality driven) classification.

## Sensitive Information

- Some particularly sensitive information will attract a Caveat (e.g. official-sensitive) or special handling instructions (e.g. codewords or National Caveats) to denote the need for further controls, particularly in respect of sharing. The impact of compromise of this information may be higher, but this does not imply that it will necessarily be subject to the threat model applicable to higher tiers.
- Such information can be managed at the same classification level, but with a more prescriptive information handling model, potentially supported by extra procedural or technical controls to reinforce the need to know. The aim of additional technical controls is to manage the information characteristics that attract the additional marking (for example enforcing access control, or technically limiting the number of records a user can view). These controls will be data and system dependent.

## Aggregation

- As government employs greater sharing and reuse of commoditised ICT solutions as well as shifting public services delivery to online channels, there is potential for large volumes of data objects to be concentrated in a small number of systems or services, or for a single system to provide a large number of government services.
- Aggregation of data or services may result in the following conditions being realised:

- The impact to the business from the loss, compromise or misuse of an aggregated data set is likely to be higher than the impact of compromise of a single object. The increase in impact can, under some circumstances, be severe (such as very large sets of citizen data);

- Existing Threat Sources will remain relevant but these threats may be more motivated to mount an attack as the benefit to them of compromising a large number of data objects is more appealing;

- Threat Sources may be attracted to attack the aggregated data set or service because the return on investment may be sufficiently increased. This is especially relevant when considering aggregation of value bearing transactions. These Threat Sources may therefore deem it worthwhile to deploy an increased technical capability.

- Aggregated data sets should be considered to be within the same classification level; however where the impact of compromise or loss has increased as a result of aggregation, these aggregated data sets must be carefully and tightly controlled.

## Assessing the impact on the Business

- Aggregation of data at rest on end user devices, or the aggregated presentation of data to end user devices must be avoided as far the business requirement allows. This minimises the impact of compromise of the device or of inappropriate action from the user (accidental or malicious). This may include technical controls to physically limit the data or services being accessed, as well as transactional monitoring approaches to detect and respond to anomalous data or service access.
- A risk assessment must be undertaken to determine the specific technical controls needed to protect the aggregated data set – this will include an understanding of how aggregation affects threat. Technical controls to protect an aggregated data set should be robust and risk owners may decide that they require a higher level of assurance or additional technical capability (such as fault tolerance). The risk assessment for the given aggregated service or data set should determine the specific technical controls within an appropriate architecture.
- Organisations are required to assess the potential impact to the business in the event that specific information risks are realised. This assessment should form part of a comprehensive risk assessment which also considers threat, vulnerability and likelihood. This risk assessment process considers Confidentiality, Integrity and Availability of information independently.
- Within each tier there will be a range of information with varying degrees of business impact should the risks be realised – this is particularly true when considering the public tier.
- The existing Business Impact Level (BIL) structure should continue to be used in the course of an information risk assessment process. BIL‟s should not on their own be used to „label‟ information systems or indicate a level of accreditation. In due course the BIL policy will be revised to provide a qualitative assessment process that supports the genuine business priorities. There is no direct mapping between existing BILs and any given classification.

## Security Enforcing Functionality

Where any security functionality or security product is relied upon, there must be confidence that those products or functions are effective and are providing the protection that is expected of them. All such products must therefore have an appropriate level of independent validation or assurance, proportionate to the classification of the information they are used to protect.

## Data Handling Requirements

All users are responsible for following the controls based on classification of the data. The table below lists the controls for the data based on classification of data.

Category

| | Public | Important | National Security |
|---|---|---|---|
| Access Controls | Viewing - No restriction Modifications - Authorization by Data Owner or designee required | Viewing and modification - Restricted to authorized individuals as needed for business-related roles; Data Owner or designee grants permission for access, plus approval from supervisor • Authentication and authorization required for access | • Viewing and modification - Restricted to authorized individuals as needed for business-related roles; Data Owner or designee grants permission for access, plus approval from supervisor<br>• Authentication and authorization required for access<br>• Confidentiality agreement required |
| Copying/Printing | • No restrictions | • Data should only be printed when there is a legitimate need<br>• Copies must be limited to individuals with a need to know<br>• Data should not be left unattended on a printer/fax<br>• May be sent via Campus Mail | • Data should only be printed when there is a legitimate need • Copies must be limited to individuals authorized to access the data and have signed a confidentiality agreement • Data should not be left unattended on a printer/fax • Copies must be labeled “Confidential”; must be sent via Confidential envelope |
| Network Security | • May reside on a public network; Protection with a firewall recommended • Protection only with router ACLs acceptable | • Protection with a network firewall required • Protection with router ACLs acceptable<br>• Servers hosting the data should not be visible to entire Internet, nor to unprotected subnets like guest wireless networks • May be in a shared network server subnet with a common firewall ruleset for the set of servers | • Protection with a network firewall using "default deny" ruleset required • Protection with router ACLs required • Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like guest wireless networks • Must have a firewall ruleset dedicated to the system • The firewall ruleset should be reviewed periodically |

| | | | |
|---|---|---|---|
| System Security | • Must follow general best practices for system management and security • Host-based software firewall recommended | • Must follow OS-specific best practices for system management and security • Host-based software firewall required. • Host-based software IDS/IPS recommended | • Must follow OS-specific best practices for system management and security • Host-based software firewall required; Hostbased software IDS/IPS recommended |
| Virtual Environments | May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines | • May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines • Should not share the same virtual host environment with guest virtual servers of other security classifications | May be hosted in a virtual server environment • All other security controls apply to both the host and the guest virtual machines • Cannot share the same virtual host environment with guest virtual servers of other security classifications |
| Physical Security | System must be locked or logged out when unattended | System must be locked or logged out when unattended • Hosted in a secure location required; a Secure Data Center is recommended | • System must be locked or logged out when unattended • Hosted in a Secure Data Center required • Physical access must be monitored, logged, and limited to authorized individuals 24x7 |
| Remote Access to systems hosting the data | No restrictions | • Access restricted to local network or VPN • Remote access by third party for technical support limited to authenticated, Temporary access via secure protocols over the Internet | • Restricted to local network or secure VPN group • Unsupervised remote access by third party for technical support not allowed • Two-factor authentication recommended |
| Data Storage | • Storage on a secure server recommended • Storage in a secure Data Center recommended | • Storage on a secure server recommended • Storage in a secure Data Center recommended • Should not store on an individual's workstation or a mobile device | • Storage on a secure server required • Storage in Secure Data Center required • Should not store on an individual workstation or mobile device (e.g., a laptop computer); if stored on a workstation or mobile device, must use whole-disk encryption • Encryption on backup media required • Paper/hard copy: do not leave unattended where others may see it otherwise, it must be stored in a secure location |

| | | | |
|---|---|---|---|
| Transmission | • No restrictions | • Information will only be shared with defined users on appropriate and accredited recipient ICT systems | Encryption required (for example, via SSL or secure file transfer protocols) • Cannot transmit via e-mail unless encrypted and secured with a digital signature |
| Backup/Disaster Recovery | Backups required; daily backups recommended | Daily backups required • Off-site storage recommended | • Daily backups required • Off-site storage in a secure location required |
| Media Sanitization and Disposal (hard drives, CDs, DVDs, tapes, paper, etc.) | • No restrictions | • Recycle Reports. • Wipe/erase media | • Shred reports • Destruction of electronic media |
| Training | • General security awareness training recommended | General security awareness training required • Data security training required | • General security awareness training required • Data security training required Applicable policy and regulation training required |
| Auditing | Not needed | Logins | Logins, access and changes |
| Mobile Devices | Password protection recommended • Locked when not in use recommended | • Password protection required • Locked when not in use required | Password protection required. • Locked when not in use required • Encryption required |
| Disposal / Destruction | Dispose of with care using approved commercial disposal products to make reconstitution unlikely | Verify document is complete before destruction<br>Use approved equipment and or service providers | Control measures to witness / record destruction |

# Appendix B: GDCM Policy Guidelines

## Data Center Behavioural guidelines

- All people visiting data center must conduct them in a courteous professional manner while visiting the Data Center. Agencies shall refrain from using any profanity or offensive language.
- No one should be allowed to tamper with, or in any manner adversely affect, security, infrastructure monitoring, and/or safety systems within the Data Center.
- Alcohol, controlled substances, firearms and explosives are not permitted on data center property. Smoking, drinking, and eating are strictly prohibited within the Data Center raised floor space. Smoking is expressly prohibited in all data center buildings.
- Persons under 18 years of age or requiring adult supervision are not permitted within the Data Center without the express written permission of Data center operator.
- All visitors to the Data Center should wear appropriate footwear and attire.
- Unless otherwise expressly permitted by Data Center operator in writing, storage of combustible materials (e.g. wood, cardboard and corrugated paper, plastic or foam packing materials, flammable liquids or solvents) are prohibited within the Data Center. All the people are expected to be familiar with and adhere to all standards associated with work in a computer room environment
- Use of cell phones inside the Data Center is allowed. Two-way radios are not permitted the Data Center. Cell phones with camera capabilities may not be used for picture or video capture.
- Skateboards, skates, scooters, bicycles or other types of vehicles are prohibited in the Data Center.
- Sharing proprietary information, without the express written permission of agency is strictly prohibited.
- All hand-carry containers, boxes, bags, laptops, purses, backpacks, or equipment carried into or out of the Data Center are subject to inspection by data center staff and/or Security.
- Data center operator would not accept Mail/Post on behalf of agency o at the Data Center. All Mail/Post should be directed to agency's business address.
- People must cooperate and obey all reasonable requests of Data Center personnel while within the Data Center, including immediately addressing any violations of rules when brought to Agency's attention.
- Upon activation of a smoke detector or emergency alarm, all agencies personal must be prepared to evacuate the building and to receive further instructions from the data center staff.

## Pictures or Video

- Any use of cameras, video, and other photographic equipment along with but not limited to audio monitoring and audio capture devices are prohibited within the Data Center without the express written permission of  Agency or Ministry. No person, other than data center staff, shall be permitted to take photo or videotape records within the Data Center.
- No one is permitted to take pictures or videos of the Data Center. Site pictures or videos must be arranged in advance and according to data center security regulations.
- If pictures or video are required for insurance or marketing purposes, contact data center operator for assistance.
- All types of cameras, unless otherwise provided in this Service Guide, are prohibited in the Data Center.

## Physical Security

- Data Centers are secured facilities. Access to the data center and other areas of the facility are restricted to authorized persons.
- General agency personal access is restricted to authorized areas only.
- Security controls include 24 x 7 staff presence, sign-in procedures for all ingresses and egresses, managed key and access card plans, managed access permissions, and access request methods.
- Security cameras are used to monitor some areas of the facility including lobbies, common areas, Data Center floor space, and admin areas. All cameras are monitored and images are retained. Violations noted by camera will be addressed promptly.
- Tampering with, or in any manner adversely affecting, security and/or safety systems within the Data Center is strictly prohibited.
- Exterior Data Center doors may not be propped open. These access doors are monitored and alarmed.
- Data Center operator reserves the right to access any part of the data center at any time for safety and security reasons.

## Data Center Ingress and Egress

- All Customers entering the Data Center must:
- Possess a valid government-issued photo ID.
- Have authorization to access the facility.
- Sign in and out as required by the facility.
- Display their temporary “T” security badge at all times while in the facility.
- Surrender their security badge and Data Center owned tools prior to exiting the facility.
- Agencies personal are expected to be familiar with and adhere to all standards associated with work in a computer room environment.

## Access List Management

- Ministry and Agencies are responsible for maintaining and updating their access list. Data center manager should ask for a written submission for additions and deletions to the Customer’s access permissions list. Individuals identified on this list will be granted access to the cabinets. Agencies may grant temporary access to their Cabinet for an employee, vendor or technician by submitting an e-mail to x@xx.com
- Data center operator (Ministry or Agency) remains responsible for the activities of these individuals as with any other authorized agencies employees, contractors, or vendors.

## Common Areas

- The common areas are lobbies and hallways.
- People using the common areas must throw away their trash in the appropriate receptacles.
- A staging area is not available for general people visiting data center.
- Data centers operator's reserves the right to deny access to those people who abuse the common areas and the rights of other Customers.

## Cage/Cabinet and Cabling Requirements

- The cabinet shall, at all times, be clean, neat, and orderly. Cabinet space shall not pose any danger or hazard to employees (including subcontractors) that may be requested or required to enter the cabinet to perform a service or to any other customers of the Data Center.
- Data center operator must take all necessary precautions to ensure the physical security of property contained within their data center location(s). Cabinet doors must be secured at all times.
- Data center operators must remove all refuse materials. These materials include, but are not limited to boxes, crates, corrugated paper, plastic, foam packing materials, and any other materials which are non-essential to the operation of the equipment. Materials must be placed in designated disposal area at the loading dock.
- The creation of "office space" within the server area on the data center floor is prohibited. The server area is reserved strictly for cabinet(s) and the contents thereof.
- "Un-racked" equipment, i.e. operating equipment outside of cabinets or racks, is strictly prohibited.
- No combustible material, e.g. cardboard, foam, or paper, shall be stored in the cabinet.
- Data center should not hang or mount anything on the walls, cabinets, fire suppression equipment or network gear unless authorized by the Computer Operations staff.
- The tops of cabinets or ladder racks may not be used for physical storage.
- Unsecured cabling across aisles or on the floor is strictly prohibited. All devices must be installed in racks or cabinets. Ladder racking must support all cabling between rows.
- Cable wrapping, wire management, zip ties and/or Velcro, must be used to organize cabling in a rack or cabinet.
- All racking and de-racking of equipment will be done solely by data center operator.
- Data center operator reserves the right to decline the implementation of a Change Order if it determines the cabinet or cabling is not in compliance. Vendor in violation will be notified by data center operator in writing and vendor must remedy the situation immediately.
- Agencies who do not comply with cabinet and cabling requirements will be notified and requested to promptly remedy the situation. If the agencies fail to remedy the situation, EGA will make the agencies cabinet or cabling compliant and charge the Customer the time and material fees this action has incurred.
- No one should climb onto cabinet and or scale walls. One must request data center staff assistance if they need to access cabinet /rack tops.
- One should not make any physical alternations or modifications to the space, without prior written permission from data center operator.

# Rack/Cabinet Doors

- No one should are not allowed to remove or replace the doors of their assigned cabinets. Door replacement request must be submitted to proper authorities and once approved; the appropriate computer Operations staff will remove or replace the cabinet doors.
- If agencies cabinets are equipped with doors, the doors must be closed when the agency is finished working on devices.
- Should the locks or doors not function properly, data center operator should contact the authorized locksmith for assistance. Do not pry, bend, or force the doors open.

# Floor Tiles

- Data center personal are prohibited from lifting or moving floor tiles. The sub-floor area is a restricted area, accessible by authorized staff only. The perforated tiles are strategically placed for HVAC cooling patterns. If there are temperature problems, the data center operator should notify cooling vendors to rectify the problem.

# Data Center Equipment

- Data Center equipment such as tools, dollies, carts, server lifts, monitor and keyboards will be available to agencies. Agencies are responsible for all loaned equipment while they are checked out and shall return the equipment immediately after use.
- Modification of equipment on loan from the Data Center is not permitted without prior written approval from agencies.

# Receiving

- Large amounts of equipment, shipments, or large devices must enter the Data Center through the shipping/receiving dock.
- Hand-carried equipment brought into the Data Center that need to be installed may require technician assistance to help calculate the additional power draw of any new equipment being added to a rack. This assistance is to help ensure SLAs are not jeopardized.
- All equipment brought to the Data Center must have the Agencies name on it. Unidentified equipment is a security risk. Any unidentified equipment delivered to agency will be refused for security reasons.
- Data Center operator staff will not move unpack or uncarted any agency owned equipment (cabinets, servers, etc). Agencies are responsible for unpacking, uncarting, and movement of heavy equipment to the Data Center floor, including all associated costs. Assistance for equipment more than 100 pounds may be offered to the Customer at the discretion of agencies
- Proper protection plans must be implemented to prevent damage to data center infrastructure.

# Removal of Equipment at End of Term

- Unless otherwise agreed to in writing, agencies will have all their hardware removed from the Data Center no later than the Effective Cancellation Date.
- Agencies shall refer to the Service Guide for Cancellation guidance.

## Customer Provided Power Strips

- Agencies are prohibited from plugging their own power strips into Data Center. This is in violation of electrical and safety codes and agencies reserve the right to demand their removal from the Data Center. Any violations of this policy must be rectified within one business day. Failure to correct this violation after one business day is a material breach of the terms of the customer's contract.

## Customer Provided Additional Security Devices

- Agencies are not allowed to add security devices that would hinder agency from accessing their cabinet. This is for security and safety reasons. Agency must have access to all areas of the Data Center at all times.