GUIDELINE FOR PRIVACY AND SECURITY IN CLOUD FIRST POLICY ENVIRONMENT

Normaziah Abdul Aziz | Hafizah Mansor
Mohamed Ridza Wahiddin | Rizal Mohd Nor | Najwa Abu Bakar

Table of Contents

EXECUTIVE SUMMARY

PART 1: Cloud First Strategies and Policies of Several Countries

PART 2: Privacy and Security of Cloud Computing Platform

PART 3: Embracing Cloud First Policy- the Malaysian Context

EXECUTIVE SUMMARY

Cloud computing and Cloud First Policy can come hand-in-hand. The latter is a policy with strategies to realise cloud computing technology. Some organisations have adopted Cloud computing with encouraging and successful outcome, while others are still evaluating or undecided. This document aims to provide a guideline for Cloud adopters to leverage on Cloud's benefit while managing to avoid possible risks that may be encountered.

This guideline gives a background by reviewing adoption of Cloud First Policy implementation in several countries worldwide and highlighting initiatives and adoption in our neighbouring ASEAN countries. The discussion of privacy and security in Cloud computing platform which includes data classification, security and privacy governance, guideline implementation and security cases brings a thorough understanding on Cloud and its policy.

As some organisations in Malaysia are keen on using Cloud computing in its services, this guideline is to help them make informed decision regarding Cloud adoption. It elaborates on benefits of implementing Cloud which are - improved efficiency, increased speed and agility, access to greater service breadth and depth, cost reduction, pace of innovation, operational continuity and business recovery and focus on core competencies. Discussion on data classification in the Malaysian context uncovers different official data types which is a useful knowledge for Cloud adoption in government sectors. The discussion includes risks and challenges including security and privacy, data ownership and legal issues related to data classification.

To determine a suitable Cloud deployment model, whether private, hybrid, or public Cloud, certain factors are to be considered. Among others are criticality of cloud services, type of workload, migration costs, elasticity, security threats, multi-tenancy, compliance, environment portability and disaster recovery or failover. Four options to acquire a new Cloud service --- in-house development and deployment; Cloud provider development, deployment and support; independent cloud service development provider; and off-the-shelf purchase of a cloud application Software as a Service. The selection of option depends on the human resource skills, startup consideration, updates to services and testing, deployment and support.

To implement Cloud computing in Malaysia, organisations may refer to steps provided in this guideline. First, it is useful to have a proper organisation's data classification, next is to assemble a team for Cloud adoption planning and operational, then develop a business case and cloud strategy for the organisation. The team then needs to select a suitable cloud deployment model and cloud service model, and determine skills needed for the Cloud services. Next, they need to develop governance policies and service agreements, assess and resolve privacy, security and data residency issues. It is important to integrate with the existing enterprise systems and develop a proof-of-concept before moving to the production stage.

Researcher and Writer Team Members

Dr. Normaziah Abdul Aziz, Associate Professor

Dr. Hafizah Mansor, Assistant Professor

Dr. Mohamed Ridza Wahiddin, Professor

Dr. Rizal Mohd Nor, Assistant Professor

Dr. Najwa Abu Bakar, Post Doctorate Researcher

Cyber Security Center of Excellence,
Kulliyyah of Information and Communication Technology,
International Islamic University Malaysia
2018

Acknowledgements

We would like to thank Microsoft Malaysia for supporting the research work in developing this guideline. Thank you also to Muhammad Qayyum Mahamad Yazid who kindly designed the report cover for us.

PART 1

Cloud First Strategies and Policies of Several Countries

1.1 Introduction

Cloud Computing technology has been conveniently available for more than a decade. Researchers and system developers have been using it for various types of purposes from testing to running fully functioning systems. National Institute for Standards and Technology (NIST) from USA defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[1] Another almost similar definition of cloud computing is as a "paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand".[2] The adoption of Cloud for storage and processing has been shown to give many benefits as compared to traditional infrastructure or on-premise platform. The economies of scale from very large Cloud infrastructure that the industry refers to as Hyper-Scale Cloud or Warehouse Scale Computing drive high impact improvement towards the advancement of Cloud technology as compared to traditional data centers. The benefits include scalability, flexibility, cost-effective, energy efficiency, better security and data protection, increased innovation and improved collaboration. [3]

Part 1 of this report studies Cloud National Strategies of several countries. It provides the compare and contrast analysis as well as the major challenges of Cloud First implementation. This is an initial study as part of the process to develop a guideline for government or non-government agencies in implementing the Cloud First policy in Malaysia. In this report, the word "agencies" refers to different types of for-profit and non-profit government or state agencies while the word "organizations" refers to for-profit or non-profit companies such as corporations and small businesses, as well as professional and charity organizations.

1.1.1 Cloud First Strategies

Cloud First policy was first issued by federal government of United State intended to accelerate the realization of Cloud Computing in which agencies were required to consider safe and secure Cloud Computing before making investments. The policy includes the efforts of government to achieve efficient operations by taking advantage of the benefits of Cloud Computing. Cloud First strategy means that organizations need to consider cloud deployment over traditional architecture every time they want to

[1] Cloud Computing Strategy for Norway (2016). Norwegian Ministry of Local Government and Modernisation, https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

[2] ISO/IEC 17788:2014 (2014), http://standards.iso.org/ittf/PubliclyAvailableStandards/c060544_ISO_IEC_17788_2014.zip

[3] Hyperscale (2018). Hyperscale – In Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Hyperscale

bring new applications and services online. Federal government of United State have suggested agencies to consider: 1) learning about what federal, state and local agencies are doing; 2) developing Cloud Computing strategy with deliverables and milestone for government and deciding what should go into public, private or hybrid cloud; and 3) building partnership and finding help from private sector companies, other governments and associations.[4]

Many Cloud Computing experts and consultants have shared explained the concept of "cloud-first" versus "cloud-only". The concept of "cloud-first" is a consideration and not a mandate. "Cloud-only", on the other hand, is making Cloud adoption a top priority despite fit issues of workloads.[5] Not every workload can move to cloud or should move to the cloud. Fit issues include several categories such as security, compliance, governance, performance, and suitability for using services or platforms in the public cloud as well as availability of the Cloud services or platforms. Cloud-first philosophy is an option to be considered and proceed to adopt the Cloud solutions if they are better in every way especially full and absolute control of security and after considering all the fit issues. [6] Basic requirements of adopting Cloud Services include sourcing, architecture, information security, data protection and procurement where some of the actions include[7]:

a) Determining data security, governance and compliance requirements

b) Identifying and evaluating current workloads and data sets for migration

c) Examining cloud cost factors for compute, data storage and data movement

d) Ensuring appropriate data protection and disaster recovery services are in place

e) Ensuring data protection and disaster recovery strategy provides copies of data to be stored off-site and preferably offline

Figure 1.1 shows NIST generic cloud computing reference architecture that is intended to facilitate the understanding of Cloud Computing requirements, uses, characteristics and standards. It presents the major actors, their activities and functions in Cloud Computing.

[4] Federal Cloud Computing Strategy, https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

[5] Linthicum, David (2017). Don't be a lemming: Cloud-first doesn't mean cloud-only, https://www.infoworld.com/article/3166055/cloud-computing/dont-be-a-lemming-cloud-first-doesnt-mean-cloud-only.html

[6] Dykstra, Jarin (2016). Cloud-first vs Cloud-only, https://www.linkedin.com/pulse/cloud-first-vs-cloud-only-jarin-dykstra

[7] Ortiz, Joseph (2016). What are the Requirements of a Cloud First Strategy?, https://storageswiss.com/2016/06/14/requirements-of-a-cloud-first-strategy/

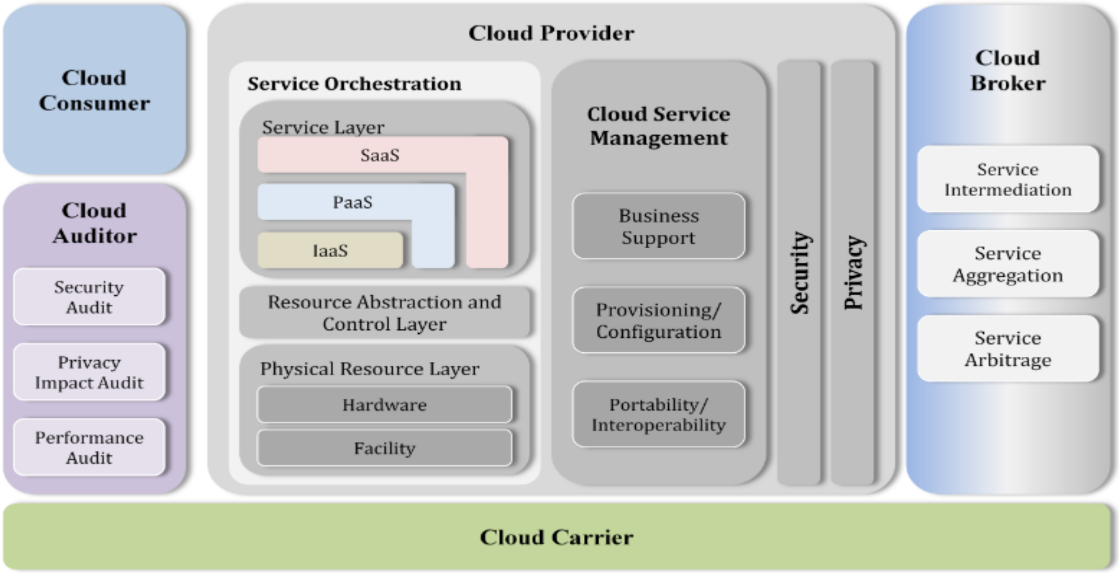


Figure 1.1: NIST Cloud Computing Reference Architecture[8]

1.2 Reviews of Cloud Implementation

Studies of cloud implementation in many countries have been published in many literatures. This section reviews the existing published documents related to the implementation of Cloud in other countries. The documents published as strategy and implementation guidelines from USA, New Zealand, Australia, European Union, Japan, Singapore, Bahrain and Norway have been studied. Countries implementing Cloud have presented strategies as guidelines to plan the transformation of existing IT infrastructure into more efficient, agile and innovative Cloud environment. Section 2.1 summarizes the cloud implementation information extracted from the documents. The general information and guidelines about the reported cloud implementation, main objectives, risks or challenges, goals or actions, and strategy and policy have been presented.

1.2.1 Cloud Implementation Worldwide

The Cloud First Policy in United States released by The White House in 2011, is a policy intended to accelerate the pace at which the Federal Government realizes the value of Cloud Computing by requiring agencies to evaluate safe and secure Cloud Computing options before making any new investments. The objective is to achieve operational efficiencies by adopting "light" technology and shared services. For United State, in the published documented strategy, a structured framework called Decision Framework for Cloud Migration is presented. The framework contains three major migration steps to be considered by agencies during cloud migration planning that include 1) Selecting services to move to the cloud by identifying sources of value (efficiency, agility, innovation) and determining cloud readiness, 2)

[8] Liu et al. (2012). NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292), http://bigdatawg.nist.gov/_uploadfiles/M0008_v1_7256814129.pdf

Provisioning cloud services effectively, and 3) Managing services rather than assets. The framework is flexible and adjustable according to the needs of agencies. [9]

Japan's Smart Cloud Services aims to realize full utilization of ICT through development and diffusion of next-generation cloud services (smart cloud services) that can reach beyond corporate and industrial frameworks to share vast volumes of information and knowledge among all social systems. Japan delayed the utilization of ICT in government; medical care; education; agricultural, forestry, and fisheries; etc., thus Japan needs full utilization of ICT through diffusion of cloud services. In Japan's Smart Cloud Strategy presented in 2010, there are three Smart Cloud strategies for Japan that are 1) Utilization Strategy, 2) Technology Strategy, and 3) International Strategy. First, for its Utilization Strategy, Japan has promoted full utilization of ICT, performed environmental arrangements for diffusion of cloud services, assisted in creation of new cloud services and expanded cloud services globally. Full utilization of ICT includes the implementation of Cloud in medical, education and agriculture. Social infrastructure has been advanced with the development of Smart grid, Green ITS (Intelligent Transportation System) and management of roads and bridges through IPv6 based sensor networks. SMEs and venture companies have been vitalized by establishing cross-regional cooperation between SMEs and improving Supply Chain Management through cloud services. Second, for its Technology Strategy, Japan has promoted research and development of next generation cloud technology. The technologies include the a) technology for collection, extraction, accumulation and modeling of a vast majority of real-time streaming data and its optimization at times when conditions change, b) technology that enhances security and reliability, and c) technology that promotes “Green ICT”. Japan also has promoted standardization that is user-centric and focusing on SLA (Service Level Agreement), Security Level and Interoperability for hybrid cloud services. Finally, for its International Strategy, issues to be discussed at international level include jurisdiction over databases stored in other countries such as privacy protection act, dispute settlement mechanism, countermeasures against "harmful" information, and possibility of government intervention with respect to private-sector data and ownership of IPRs regarding data stored on a cloud data center in other countries. A consensus to cooperate between public and private sectors, to formulate international rules using international vehicles such as APEC, OECD and ITU, and to have bilateral consultations has been composed. Dialogues on policies under the cooperation of industries, universities, and the government have been held.[10] Furthermore, after the tsunami, earthquake and nuclear disaster in March 2011, IT managers in Japan started to realize the importance of Cloud for national disaster recovery. Cloud has been considered as best practice during IT decision making and infrastructure rebuilding to ensure disaster recovery and business continuity will be handled with the highest priority.[11]

The European Cloud Strategy is a policy strategy document that contains the key actions that EC policy makers have identified to support the uptake of Cloud computing in Europe. The European Cloud Strategy has two main objectives that are 1) Making Europe Cloud-friendly and Cloud-active, and 2) Connecting digital agenda initiatives. The challenges include trust, security, dependability, governance, control, interoperability, standards, privacy and legal issues. Therefore, EU has listed three strategies for implementing Cloud that are 1) Standards and Certification, 2) Safe and Fair Contract Terms, and 3) European Cloud Partnership. First, for establishing Standards and Certification, ETSI (European Telecoms

[9] Federal Cloud Computing Strategy, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/1151/downloads/2012/09/Vivek-Kundra-Federal-Cloud-Computing-Strategy-02142011.pdf

[10] Cloud Services in Japan (2011). Retrieved from http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/111102_1.pdf

[11] Phil (2013). Fukushima sends Japanese IT to the Cloud, https://www.theregister.co.uk/2013/09/03/japan_fukushima_earthquake_it_rebuild_dr/

Standards Institute) has to coordinate stakeholders, identify necessary standards (e.g. for security and interoperability), and recognize ICT technical specifications for data protection. The European Union Agency for Network and Information Security (ENISA) and other agencies need to assist development of EU-wide voluntary certification schemes and agree with industry harmonised metrics for energy consumption and carbon emissions of cloud services. Second, to achieve Safe and Fair Contract Terms, terms for cloud computing service level agreements for professional cloud users model need to be developed with stakeholders. EU also modeled contract terms and conditions pursuant to Common European Sales Law. Standard contractual clauses and binding corporate rules for international data transfers by cloud providers were reviewed. EU has been working with industries towards producing code of conduct for cloud providers.[12]

For Australia, the main objective of The National Cloud Computing Strategy[13] is to create and use world-class cloud services to boost innovation and productivity across the digital economy. Some of the challenges are the lack of quality information, the issues of data ownership, privacy and security, the vendor lock-in and interoperability, unequal bargaining power and loss of Internet connectivity and availability of a quality connection. Australia's Cloud strategies include 1) Maximizing the value of Cloud Computing in Government, 2) Promoting Cloud Computing to small businesses, not-for-profits and consumers, and 3) Supporting a vibrant cloud services sector. Australia helps government agencies adopt cloud services and value first through cloud services. For small businesses, not-to-profits and consumers, a comprehensive suite of tools and online resources, consumer protection and effective law and enhancement of existing successes have been laid out. To support a vibrant cloud services sector, ICT skills and capacity are improved, competition, growth and foreign investment are promoted, and research and development are supported National.

New Zealand reaffirmed its Cloud First policy across the public sector and retained the Cloud Computing Risk and Assurance Framework developed and to be implemented to assess and adopt cloud services in 2015. The Government ICT Strategy and Action Plan to 2017 guideline seeks to improve service delivery and deliver substantial savings across government, with cloud computing as a key enabler. The Cloud First policy enables agencies to better take advantage of emerging technologies to drive innovation and deliver greater value. Key benefits of cloud services for the Government are cost-effective, increased agility, greater choice, improved security and resiliency. Guidelines for adopting Cloud have been prepared in New Zealand Government's ICT website including the Cloud development and implementation plan, resources for Cloud architecture, risks assessment, security controls for cloud services, cloud services purchasing guideline, Cloud adopters showcase and briefing notes for accelerating public Cloud services.[14]

In Cloud First Policy for Bahrain[15], the presented objectives are 1) to reduce the cost of government ICT by eliminating duplication of solutions and fragmentation in the technology environment, and leveraging the efficiencies of on-demand provisioning of ICT services; 2) to increase security by using accredited platforms; and 3) to increase productivity and agility, and thus improving citizen services. ICT

[12] The European Cloud Strategy (2012), https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy
[13] The National Cloud Computing Strategy (2013), https://www.communications.gov.au/sites/g/files/net301/f/National_Cloud_Computing_Strategy.PDF
[14] Guidance and Resources: Using Cloud Services (2018), https://www.ict.govt.nz/guidance-and-resources/using-cloud-services
[15] Cloud First Policy (2017), http://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf

at entity level must focus on functional excellence and delivering higher business value. ICT Infrastructure is one key candidate for national level consolidation and optimization. Standardized infrastructure management facilitates changes in government business processes in an easier and quicker way. Cost optimization and risk reduction across government are enabled through leveraging common platform and information systems for cross-government service delivery.

Norway has published their Cloud Computing Strategy.[16] Although Norway does not plan to mandate Cloud First policy, cloud services will always be considered when public agencies need to procure ICT systems.

Interestingly, Cloud strategy for a small republic called Estonia has been considered as an extreme case where the entire infrastructure of the country is migrated to the cloud for the purpose of national security and data sovereignty. This strategy allows Estonian government to be in control of normal state operations digitally during unexpected situations such as the invasion of physical territory by foreign force[17].

1.2.2 Cloud Implementation in ASEAN Countries

Association of Southeast Asian Nations (ASEAN) member countries, excluding Singapore, are considered as the late adopter of cloud computing technology. A report on Cloud Computing in ASEAN countries for developing ICT framework and policy recommendation initiative has been published by Electronic Government Agency.[18] Standard Cloud Computing models, major vendors' architecture and government cloud initiatives are listed. Cloud Computing trend, ASEAN Cloud Computing readiness, benchmarking and comparative analysis of Cloud Computing in ASEAN and the policy and legal infrastructure have been studied. The report also presented the Cloud Computing country profiles for Brunei, Indonesia, Malaysia, Philippines, Singapore, Thailand and Vietnam. Finally, the Trusted ASEAN Cloud Framework and policy were recommended.

Another noteworthy report by the Lee Kuan Yew School of Public Policy and Microsoft highlighted the current development of Cloud Computing initiatives in ASEAN countries as a preparation for facing the age of Fourth Industrial Revolution.[19] The report emphasized that Cloud Computing offers considerable benefits for government and businesses in ASEAN. Some of the benefits pointed out:

a) Enables organizations to accelerate digital transformation through public, private, and hybrid cloud services;

b) Provides efficient and integrated public sector for delivering front-line services;

c) Allows various government agencies to work together with a whole-of-government approach instead of in the typical government silos;

[16] Cloud Computing Strategy for Norway (2016). Norwegian Ministry of Local Government and Modernisation, https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

[17] TheDataVault (2014). Estonia Uploads It's Entire Government To the Cloud, https://thedatavault.com/estonia-government-cloud-computing/

[18] Electronic Government Agency (EGA) (2017), http://mdes.go.th/assets/portals/14/files/590621%20Study%20on%20Cloud%20Computing%20on%20ASEAN%20FINAL.pdf

[19] National University of Singapore and Microsoft (2017). A Cloud for Doing Good: A Technology Revolution for All in ASEAN, https://ncmedia.azureedge.net/ncmedia/2017/10/A-Cloud-for-Doing-Good-FINAL.pdf

d) Offers cost-effective large-scale national social protection programs such as a biometric identification system for cash transfer;

e) Improves city services and citizen participation in government decisions affecting their lives such as smart city transformation;

f) Improves facilities such as financial and health services and increase revenues of rural areas by leveraging the cloud and big data analytics for agriculture;

g) Creates competitive SMEs by freeing up capital investments for information technology (IT) and by increasing productivity through automation;

h) Reduces manufacturing costs, improves production quality and productivity, provides flexibility and efficiency, shortens response times to customer requests and demands, and opens up new and innovative business opportunities by adopting cloud-based, open Internet of Things operating systems;

i) Minimises costs and improves access to banking facilities such as mobile banking and digital payment systems;

j) Reduces costs and increases more connected healthcare services by allowing the implementation of data analytics, tele-medicine in rural areas, diagnostic support, disaster recovery and backup services.

Besides benefits, there are several identified challenges of Cloud Computing implementation in the region. One of the main challenges is the lack of awareness, knowledge and understanding about Cloud Computing technology. It refrained both government and business organizations from pursuing any service contract in order to avoid operational complexity and addition of costs. There are also issues of data localization requirements where there is a need to identify specific rules and regulations for each country. Cost and quality of broadband infrastructure also becomes the barrier of Cloud Computing adoption in ASEAN region. Other challenges include privacy and cybersecurity concerns, lack of common cloud standards across countries, and requirements for government and cloud service providers to comply with international standards such as ISO 22301 for business continuity management, ISO/IEC 27001 for information security management, and ISO/IEC 27018 for data privacy in the Cloud. These challenges faced by many ASEAN countries such as Philippines, Vietnam and Myanmar. [20]

Singapore, however, is an early adopter of Cloud, after United State, Japan and EU. In Singapore, G-Cloud is the next generation whole-of-government infrastructure established since 2010. It provides efficient, scalable and resilient Cloud Computing resources and designed to meet different levels of security and governance requirements that cannot be fulfilled by public cloud. Singapore is a lead adopter of cloud computing due to five key drivers: (1) Public demand for and satisfaction with e-government services; (2) Focus on whole-of-government policies and practices; (3) Restructuring of technology agencies to integrate strategy and implementation; (4) Building the Smart Nation Platform; and (5) Purpose-driven cloud applications, especially in healthcare. To further aggregate the whole-of-government demand to maximise cost savings to the Government, the Government will identify and provide Software-as-a-Service offerings, such as business analytics, customer relationship management and web content management. G-Cloud enables standardisation, and sharing of computing resources and

[20] National University of Singapore and Microsoft (2017). A Cloud for Doing Good: A Technology Revolution for All in ASEAN, https://ncmedia.azureedge.net/ncmedia/2017/10/A-Cloud-for-Doing-Good-FINAL.pdf

applications at the whole-of-government level, thereby generating cost savings to the Government. The Infocomm Development Authority (IDA) of Singapore is the authority that promotes and regulates Cloud Computing in Singapore. Singapore's Cloud objective is to sharpen the overall economic competitiveness through adoption of Cloud Computing and enhance the vibrancy and growth of the information and communication sector through the development of a Cloud ecosystem. To achieve these objectives, IDA has identified six key strategies 1) supporting flagship users of cloud services, (2) attracting cloud players, (3) developing manpower competency for industry (4) forging R&D relationships and building knowledge capital assets, (5) providing enabling infrastructure, and (6) building a trusted environment through policy and legislations.[21]

The projects introduced by government for supporting flagship users include: a) iSPRINT Scheme to increase SME productivity, promote packaged and customized solutions prequalified by IDA, and harness cloud technology to enhance business operations; b) SaaS Enablement Program (SEP) to provide funding for SaaS enablement in specific industry verticals; c) Cloud Innovation Centre (CIC) to boost the adoption of cloud services among small or newly established businesses and encourage businesses to use a private cloud; d) Productivity and Innovation Credit (PIC) scheme to grant businesses in order to 400% tax deductions for five years against the acquisition of IT equipment, acquisition and licensing of intellectual property rights, staff training, research and development, registration of patents and trademarks, and design projects; and e) Initiatives to promote adoption such as the Call for Cloud Computing Proposals and the seminar series for public education on cloud computing. Cloud computing development is also strongly supported by Singapore human resource development strategy called the Competency Development for Industry and Manpower. The actions to realize the strategy include several projects that are: a) Infocomm Manpower Development Roadmap v2.0 for capacity development and equipping students with Cloud Computing knowledge and skills; b) Development of competency standards for identifying job roles related to Cloud Computing; c) Training programs by giving short training courses for IT personnel develop Cloud Computing skills; and d) Building a talent pipeline project where IDA works with IT schools to offer both diploma and degree courses to provide education and practical training relevant to Cloud Computing. ASEAN countries should learn from the Cloud Computing best practice implemented by developing countries and Singapore. Mainly, there are four areas of Cloud Computing adoption that are the infrastructure, the development strategy, the Cloud promotion and demand boost, and finally, research and human resource development (EGA, 2017). Cloud Computing infrastructure consists of physical infrastructure such as complete universal broadband service and legal infrastructure covering rules and regulations for data protection, data localization, data security, IPR and cyber-crime acts. Following the development of infrastructure, the strategy for development, promotion, research and human resources need to be properly planned to match the existing government short term and long-term ICT agenda.[22]

1.3 Summary of Part 1

Part 1 of this report has reviewed the implementation of Cloud Computing in countries that are considered as early adopters. The Cloud Computing and Cloud First have been implemented by government and non-government agencies in United States, Japan, Australia, New Zealand, EU, Singapore, Estonia, Bahrain and Norway. Although not all countries claimed that they are adopting Cloud First strategy, they have prepared detail guidelines and policy as well as appointed credible agencies that

[21] Cloud Computing for Singapore Government Fact Sheet (2013), https://www.imda.gov.sg/-/media/imda/files/inner/about-us/newsroom/speeches/2013/1505_cloudasia2013/gcloudfactsheet.pdf?la=en

[22] Electronic Government Agency (EGA) (2017), http://mdes.go.th/assets/portals/14/files/590621%20Study%20on%20Cloud%20Computing%20on%20ASEAN%20FINAL.pdf

manage, conduct training and consultations to government and non-government organisations that plan to adopt Cloud Computing strategies. Appendix A provides summary of Cloud First or Cloud Computing implementation in these countries including the objectives, risks, goals, strategies and policies. Privacy and security are among the major risks and concerns for most adopters of Cloud computing and services. Part 2 of this report discusses these issues and presents comparisons of the implementation worldwide.

PART 2

Privacy and Security of Cloud Computing Platform

2.1 Introduction

Cloud First policy, as mentioned in Part 1 is the consideration to adopt Cloud computing provided that the technology and services fulfill the information technology requirements of the organizations, as well as organizations' security and privacy objectives. Cloud computing is a form of outsourcing information technology services, functions and data storage online over the Internet. Migrating government and industries' workloads and data to Cloud environment can improve security controls of physical location and network security. However, the main challenge of Cloud computing is the protection of sensitive data from various attacks.[23] Security and privacy are the fundamental factors that determine the success of Cloud computing strategy. Failure to implement proper security measures and privacy protection causes reputational harm, higher costs and potential loss of business. Every decision to adopt Cloud services must be followed by clear understanding of its potential security benefits, the associated risks, security requirements and responsibilities, as well as the realistic expectations set between organizations and service providers.[24]

Organizations and Cloud providers are responsible to ensure availability of safe and secure Cloud solutions to provide imminent IT services. The basic security needs for Cloud implementation are: [25]

- Data controls and access policies to determine where to store data and who can access physical locations
- Data characteristics to assess suitable fundamental protections required by certain information
- Governance to ensure Cloud service providers are transparent, have proper security and management controls, and provide necessary information for agency to audit the efficacy of those controls
- Compliance to laws, regulations and agency requirements.
- Privacy and confidentiality to protect sensitive data from accidental and unauthorized access
- Integrity to ensure authorized, complete and accurate data

As Cloud adoptions become the norms in any organizations, more sensitive information is stored in Cloud for convenience. Thus, raised security concerns among security professionals include:

[23] Shackleford, Dave (2017). Cloud Security: Defense in Detail if Not in Depth. A SANS Survey, 2017 SANS Institute. https://www.sans.org/summit-archives/file/summit-archive-1519076280.pdf

[24] CSCC (2017). Security for Cloud Computing Ten Steps to Ensure Success Version 3, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

[25] Jansen and Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

- Unauthorized access of sensitive data by outsiders such as other cloud tenants
- Limitations on access to collect incident response data and evidence for forensic analysis
- Insecure, unmanaged devices accessing sensitive data from the cloud
- Incidents involving downtime/inaccessibility, poor configurations, and account or credential hijacking
- Inability to audit
- Breach of sensitive data by cloud personnel
- Lack of visibility, auditability, and effective controls to monitor activity in public clouds
- Loss of governance ownership because of limitations in service agreements with cloud provider leaving gaps in security defence
- Responsibility ambiguity over security and privacy aspects causing vital parts of defence to be left unguarded
- Authentication and authorization to determine the identity of the user for accessing sensitive data from anywhere
- Isolation failure due to multi-tenancy and shared resources such as storage, memory and routing
- Legal risks when organizations compliance to certification and standards may be lost if service provider cannot provide evidence of their own compliance
- Security incidents are handled by Cloud service provider
- Management interface vulnerability and increased risk, especially when combined with remote access and web browser vulnerabilities
- Application and data protection
- Personal data regulation
- Malicious behaviour of insiders
- Business failure of the provider
- Service unavailability
- Vendor lock-in
- Insecure and incomplete data deletion

Typical security controls utilized for cloud environment including secure access using VPN, log management, vulnerability management and encryption, as well as the use of security-as-a-service (SecaaS) solutions to fulfill security and compliance requirements.[26] However, recent development of Cloud implementations has caused Cloud security to evolve. There are changes in worldwide privacy regulations, standards to different aspects of Cloud security such as logging and monitoring, formal information governance framework, cryptographic key management services, identity and access management in microservices environment.[27] There is also a need for of a unified system to protect the confidentiality and privacy of the Cloud users. Cloud technology is an evolving paradigm, it is critical to have experts involved at every turn to stay current with the changing needs of the government and cybersecurity communities. Uniformity or similarity of concepts, definitions, policies, standards, frameworks and enforcements are critical for a cohesive and trans-border cloud strategy.[28]

[26] Jansen and Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[27] CSCC (2017). Security for Cloud Computing Ten Steps to Ensure Success Version 3, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

[28] Greiman, Virginia (2015). National Strategies for Cloud Innovation and Security. ICCSM2015-3rd International Conference on Cloud Security and Management. University of Washington, USA 22-23 October 2015.

2.2 Cloud Computing Privacy and Security Strategy

To fulfill the Cloud computing security and privacy needs, there are suggestions and recommendations on how to implement Cloud. Some of the identified Cloud security strategies include strengthening privacy laws, increasing law enforcement, helping users make informed choices, transparency among cloud providers' security practices, and promoting user confidence through common approaches to jurisdiction. The organizations and the Cloud computing providers equally share the privacy and security responsibilities. Although the Cloud service providers are responsible for the security of the Cloud, the owners of the data are responsible to control and protect the data. The level of responsibilities depends on the deployment model type and should be understood by each party.[29] There is also a potential for certain parts of security defense to be left unguarded if the privacy and security responsibilities are not defined clearly between organizations and service providers.

2.2.1 Cloud Data Classification

Data classification is a very critical process to establish risk management and data security. Proper Cloud data classification policy is the top priority to ensure data that is the most valuable asset stored in Cloud is protected.[30] Data classification is "*the process of organizing data by relevant categories so that it may be used and protected more efficiently*".[31] It is a method to grade, mark, label or tag information based on the identified damage that could happen resulting from unauthorised disclosure in order to specify the needed protective measures.[32] An organized data classification framework is needed as the main reference for organizations, employees and service providers involved in the process of handling the data. It is also to ensure appropriate data protection and compliance with security policies.[33] Data classification operational framework includes the process of:

- Defining the data classification objectives
- Determining the categories and criteria to be used to classify the data e.g. classification based on sensitivity levels such as restricted, private, and public
- Tagging, labelling or marking the data according to classification categories
- Outlining the roles and responsibilities of employees in maintaining proper data classification protocols
- Implementing security standards that correspond with data categories and tags
- Defining data protection requirements for each data type
- Defining policies and procedures by considering security and confidentiality of each data type
- Defining the potential risks when the security policies for data types are breached or compromised
- Specifying the security and privacy response, measures and rules that should be placed during data handling e.g. retrieving, transmitting, storing or copying
- Specifying the data protection tools for each data type e.g. encryption and tokenization

United Kingdom, Australia and New Zealand are some of the countries that have come out with a government security classification system to help organizations to identify protection requirements for

[29] Federal Cloud Computing Strategy, https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

[30] Mudd, Michael (2016). HKCSView: Security is not the issue - its data classification, https://www.cw.com.hk/security/hkcsview-security-not-issue-its-data-classification

[31] Lord, Nate (2017). What is Data Classification? A Data Classification Definition. Digital Guardian. Retrieved from https://digitalguardian.com/blog/what-data-classification-data-classification-definition

[32] New Zealand GCSB (2002). Security in Government Sector, https://www.gcsb.govt.nz/assets/GCSB-Documents/Security-in-the-Government-Sector-2002.pdf

[33] Higashi, Michael (2015). Cloud Data Protection 101: Data Classification. CipherCloud. Retrieved from https://ciphercloud.com/cloud-data-protection-101-data-classification/

official information and to fulfil the protection requirements. For New Zealand, official information that need special protection from unauthorised or accidental access are identified and marked based on risk-assessment of the damage levels caused when the specific contents are disclosed. There are two types of information specified by security classification that specifies how the information must be protected: 1) policy and privacy information, and 2) national security information. Public interest and personal privacy information are materials that should be protected and marked as IN CONFIDENCE and SENSITIVE. National security information materials should be protected and marked as RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET. Other official information that are not categorized under security classification are marked as UNCLASSIFIED.[34] These types of security classification and protective markings should also be applied towards official information handled by within IT and Cloud environments.

Government organizations and industries with critical information such as banking and healthcare should implement data classification to protect different types of data and to focus their resources and investment towards security controls of the most sensitive information.[35] To determine which data needs protection and at what level, data privacy regulations or industry best practices for specific data should be focused. For example, HIPAA and HITECH are the standards for healthcare services and Gramm-leach-Bliley Act (GLBA) is the regulation for financial services.[36]

Data classification categories should be carefully determined to avoid unnecessary cost and the marking and classification should be automated. Organizations should avoid under-classification and over-classification of data. The under-classification of data causes official information stored in Cloud service does not have appropriate security controls and adequate level of protection. On the other hand, over-classification causes unnecessary controls being specified leading to excessive costs resulting in suitable cloud services being rejected. Therefore, it is critical that an agency accurately assesses the value, criticality and sensitivity of its data, and correctly classifies it to ensure that it is appropriately protected. For typical Platform as a Service (PaaS) and Software as a Service (SaaS) deployment types, the data classification is handled in general and by configuration options provided by PaaS and SaaS services. Nevertheless, organizations need to define and be aware of how sensitive data is handled by the utilized services.[37]

2.2.2 Security and Privacy Governance in the Cloud

Cloud security and privacy governance is the ability of organizations to effectively control, monitor and manage Cloud security and privacy policies, procedures, and standards. To address Cloud governance, the risks and complexity of each Cloud deployment models (public, private or hybrid) should be considered. Some of the typical security and privacy issues that need to be governed by an organization throughout the system lifecycle are:

- Who owns, accesses, deletes, and replicates data
- How data is stored, protected, and used
- How to verify policy enforcement
- How to measure and validate service performance
- What are the suitable audit mechanisms and tools to ensure privacy and security practices are followed

[34] NZ PSR (2018). New Zealand Government Security Classification System. Protective Security Requirements (PSR). Retrieved from https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

[35] Cloud First Policy (2017). General Directorate of Governance and Operations Version 1.0. Retrieved from http://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf

[36] Higashi, Michael (2015). Cloud Data Protection 101: Data Classification. CipherCloud. Retrieved from https://ciphercloud.com/cloud-data-protection-101-data-classification/

[37] CSCC (2017). Security for Cloud Computing Ten Steps to Ensure Success Version 3, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Privacy and data protection governance framework outlined by Forrester Research in 2012 include five steps that can be taken to be proactive in protecting sensitive data and preventing privacy infringements.[38] The steps are listed below:

1. **Define data privacy scope**; The first step to know the compliance requirements for the Cloud system, the extent of the geographic location needs to be identified. For every country where the system will be located, data privacy for all individual states, countries and federal laws must be considered. Second, the various definitions of personal data types and classification needs to be clearly understood so that it can be appropriately protected.
2. **Determine organizational roles and responsibilities**; Privacy, data protection and compliance activities should be handled by privacy professional or chief privacy officer across the organization.
3. **Map laws and regulations into business requirements**; Implementing an online privacy tool and process map for business processes by examining relevant legal requirements allows requirements to be self-determined.
4. **Embed privacy compliance in organizational culture**; Privacy policies and procedures need to be persistently implemented to fulfil identified compliance gaps in organizations.
5. **Continuously monitor requirements**; Security requirements are parts of the evolving privacy and data protection laws that need to be monitored.

2.2.3 Cloud Security and Privacy Implementation Framework and Guidelines

Guidelines on security and privacy have been prepared by National Institute of Standards and Technology (NIST).[39] The guidelines list suggestions of privacy and security that need to be implemented by government agencies as follows:

1. **Proper planning of security and privacy of Cloud solutions prior to adoption;** Due to sensitivity of data and to fully benefit from the IT investment, security objectives and planning prior to Cloud adoption are documented to ensure security and privacy that are in compliance to organizational policies. Security objectives of organizations determine every decision made for outsourcing IT services and transitioning organizational data, applications and resources to public cloud. Risk-based approach should be taken for analysing available security and privacy options and in deciding the placement of organizational functions in Cloud.
2. **Understand the public Cloud environment offered by the cloud provider;** Organizations adopting Cloud technology are responsible to understand the policies, procedures, technical controls, technology and system architecture used by cloud provider and its implications for security and privacy. Next, verification of security and privacy assurance, claims, certification and compliance to certain entity should be made whenever possible through independent assessment by organizations. The complete understanding of Cloud implementation can be used to analyse, to formulate protection, to perform assessment, risk management and risk mitigation, and to continuously monitor the security and privacy state of the organization.
3. **Ensure that a Cloud solution satisfies organizational security and privacy;** Although it is a norm for public Cloud providers to offer wide range of services with default non-negotiable service agreements, negotiated service agreements are also possible especially for critical data and

[38] Budge and Shey (2012). Privacy and data protection governance in five steps. Essential Guide. Search CIO, TechTarget. Retrieved from http://searchcio.techtarget.com/tip/Privacy-and-data-protection-governance-in-five-steps

[39] Jansen and Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

applications. Negotiated agreements can consider organization's security and privacy needs to suit the context of organization's operation and can be adjusted, configured, deployed and managed to meet organization's requirements. The vetting of employees, data ownership and exit rights, breach notification, isolation of tenant applications, data encryption and segregation, tracking and reporting service effectiveness, compliance with laws and regulations, and the use of validated products meeting federal or national standards are examples of the security and privacy details concerned by organizations. Assurance also should be documented to corroborate that the Cloud provider should perform the negotiated agreement. Alternatively, compensating controls to work around the shortcomings of public cloud service or more suitable deployment model such as internal private cloud with better security and privacy authority for organizations can be considered.

4. **Ensure that the client-side computing environment meets organizational security and privacy requirements for cloud computing;** Cloud services are expected from different Cloud providers; cloud-based applications may be developed by the organizations themselves; Cloud services may be accessed using web browsers, or mobile devices, or social media and public sites; and there may be unknown services running malware which can affect client-side Cloud services. Client-side Cloud security and privacy need to be tested and necessary security measures need to be employed.
5. **Maintain accountability over the privacy and security of data and applications implemented and deployed in public cloud computing environments;** Strong and correctly implemented security and privacy management practices and control that operate as intended and fulfil organizational requirements are essential for operating and maintaining a secure Cloud solution. It includes assets monitoring and the assessment of security policies, standards, procedures, controls, and guidelines used to preserve security. Besides continuous monitoring of security and privacy management practices and control, risk assessment and management for each organization levels, that are governance level, mission or business process level and information system level, are crucial. Data about the state of the system that are the ongoing privacy and security controls, vulnerabilities and threats are collected and analysed to support risk management decisions and to respond by accepting, avoiding or mitigating risk as situations change. In Cloud computing systems, risk assessment and management are challenging as the environment is under the control of cloud provider. Risk analysis should consider both qualitative and quantitative factors and carefully balanced between the possibility to implement security measures (technical, management and operational) and the necessary steps to reduce risks to acceptable level. Security of Cloud depends on security and complexity of many individual components those are for general computing and management backplane such as for self-service, resource metering, quota management, data replication and recovery, service level monitoring, and workload management.

Table 2.1 presents the summary of the security and privacy issues and the recommendations by NIST and Cloud Standards Customer Council. NIST identified the security and privacy areas and provide the basic recommendations while CSCC provides steps for evaluation and management of security and privacy aiming to mitigate risk and deliver adequate level of support by considering recently analysed Cloud computing landscape.

Table 2.1: Security and Privacy Issues and Recommendations by NIST [40] and CSCC [41]

No	Areas	Recommendations by NIST	Recommendations by CSCC
1	**Governance**	• Follow the policies, procedures, and standards used for: ✓ Application development and service provisioning ✓ Design, implementation, testing, use, and monitoring of deployed services. • Prepare audit mechanisms and tools	• Implement formal information governance framework ✓ Define people tasks to manage information and establish measurement, policy and control mechanisms ✓ Describe the roles, responsibilities, communication, rules and policies regarding content production. ✓ Require specificity and transparency on the legal and regulatory obligations and business value of information. ✓ Follow ISO/IEC 38500 standard describing guiding principles for governing IT in organizations
2	**Compliance**	• Understand laws and regulations ✓ Data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.	• Implement compliance framework ✓ Understanding the internal control environment of a cloud service provider, including risks, controls, and other governance issues when that environment touches the provision of cloud services. ✓ Access to the corporate audit trail, including workflow and authorization, when the audit trail spans cloud services. ✓ Assurance of the facilities for management and control of cloud services and how such facilities are secured.

[40] Jansen and Grance (2011). Guidelines on Security and Privacy in Public Cloud Computing, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

[41] CSCC (2017). Security for Cloud Computing Ten Steps to Ensure Success Version 3, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

No	Areas	Recommendations by NIST (cont.)	Recommendations by CSCC (cont.)
3	**Trust**	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.	• Assess the security provisions for cloud applications • Analyse the impact of deployment model on application security ✓ Infrastructure as a Service (IaaS) ✓ Platform as a Service (PaaS) ✓ Software as a Service (SaaS)
4	**Architecture, Networks, Connections and Isolation**	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components. • Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.	• Ensure cloud networks and connections are secure • Identifying external network requirements ✓ Traffic screening ✓ Denial-of-service protection ✓ Intrusion detection and prevention ✓ Logging and notification • Identifying internal network requirements ✓ Provide tools to protect customers from one another ✓ Provide tools to allow customers to implement network segmentation ✓ Protect the provider's network ✓ Monitor for intrusion attempts
5	**Identity and Access Management**	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.	✓ Manage people, roles and identities ✓ Cloud service provider support for people, roles and identities

No	Areas	Recommendations by NIST (cont.)	Recommendations by CSCC (cont.)
6	**Physical Infrastructure and Facilities**		- Evaluate security controls on physical infrastructure and facilities - Follow standards such as ISO/IEC 27002 - Implement security controls of physical infrastructure
7	**Data Protection and Availability**	- Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. - Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. - Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider. - Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. - Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.	- Ensure proper protection of data - Controls for securing data in cloud computing ✓ Create a data asset catalog ✓ Consider all forms of data ✓ Consider privacy requirements ✓ Apply confidentiality, integrity and availability procedures ✓ Enable security logging and monitoring ✓ Data activity monitoring - Enforce privacy policies
8	**Incident Response**	- Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. - Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. - Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.	- Manage security terms in the Cloud Service Agreement (CSA) ✓ Specify security responsibilities of providers and customers ✓ The security terms must also be passed down to any peer cloud service providers ✓ Identify the security metrics for measuring performance effectiveness of security management - Explicitly document procedures for notification and handling of security incidents
9	**Exit Process**		✓ Understand the security requirements of the exit process Ensure that the exit process is documented as part of the CSA ✓ Ensure complete deletion of data ✓ Ensure data is protected against loss or breach during exit process

2.3 Security Cases on Cloud Platforms

This section shares some security cases on Cloud. It is not to discourage readers of this report, but rather to learn from such incidents and make effort to harden our own Cloud systems. The following lists Cloud security and operational issues in 2017 reported by surveys where the respondents were from organizations in United States, Europe, Canada, Australia and Asia [42] [43]:

- Data theft is the top security threats in Australian organizations
- Amazon had a major outage in its S3 storage environment due to operator error
- Microsoft Azure also fell prey to a cooling systems outage that affected cloud services hosted in Japan
- In Asia, virus/malware outbreak is the top incident type reported on a weekly basis.
- Phishing email attacks are selected as the second highest amongst Asian organisations surveyed, except for Singapore who ranked phishing emails as the highest weekly occurring security incidents impacting their businesses.
- Weekly attacks are reported as impacting Asian organisations more regularly than Australian organisations.
- Respondents from both Australia and Asia highlight that external hackers followed by criminal syndicates and then employees are the greatest potential threat to their organisations in the future.
- Cloud data and application breach due to more attackers focusing on the cloud, particularly on poorly configured cloud applications and management interfaces.
- Account and credential hijacking in 50% of attacks in 2016, and slightly fewer, 42%, experienced such attacks in 2017.
- Hypervisors misconfiguration or vulnerability showing up in 45% of attacks compared to just 25% in 2016.
- In early 2017, within Microsoft Azure, private keys for the cloud provider's orchestration tools were left embedded in provider-supplied images and discovered by a customer.
- More than two-thirds of incoming attacks on Azure services in 1Q17 came from IP addresses in China and the United States, at 35.1 percent and 32.5 percent, respectively. Korea was third at 3.1 percent, followed by 116 other countries and regions.
- Compromised virtual machines often communicate with command-and-control (C&C) servers at known malicious IP addresses to receive instructions. More than 89 percent of the malicious IP addresses contacted by compromised Azure virtual machines in 1Q17 were located in China, followed by the United States at 4.2 percent.
- Outbound attacks detected by Azure Security Center, 1Q17 include Communication with malicious IP 51.0%**,** RDP brute force 23.0%**,** Spam 19.0%**,** Port scanning/port sweeping 3.7%**,** SSH brute force 1.7 %
- Sony play stations DDoS attacked. The cloud server was damaged and lost mailing list data by five thousand due to the defectiveness updated program, illegal access attacked net banking users ID and passwords, which led to illegal wire transfer.

[42] Telstraglobal.com (2017). Telstra Cyber Security Report 2017. Retrieved from https://www.telstraglobal.com/images/assets/insights/resources/Telstra_Cyber_Security_Report_2017_-_Whitepaper.pdf

[43] Shackleford, Dave (2017). Cloud Security: Defense in Detail if Not in Depth. A SANS Survey, 2017 SANS Institute. https://www.sans.org/summit-archives/file/summit-archive-1519076280.pdf

Table 2.2 presents the reported workloads and applications located in private, public and hybrid Clouds, and sensitive data stored in the Cloud.

Table 2.2: Reported workloads, applications and sensitive data in the Clouds [44]

Workloads and Applications in the Clouds (Private, Public, or Both)	Sensitive Data in the Cloud
• Business applications and data • Workforce applications (Dropbox, etc) • Backups and disaster recovery • Storage and archiving of data • Managed services • Server virtualization • Security services • Hosted network services • Desktop virtualization	• Employee records • Business intelligence • Business records (finance and accounting) • Customer personally identifiable information • Intellectual property • Customer financial information • Health records • Customer payment card information • National security or law enforcement data • Student records

Table 2.3 presents the actual security incidents and the used Cloud attack methods reported in 2016 and 2017.

Table 2.3: Reported actual incidents and cloud attack methods in the Clouds [44]

Actual Incidents (2016-2017)	Cloud Attack Methods (2016-2017)
• Access to sensitive information by insecure, unmanaged devices • Unauthorized access to sensitive data by other cloud tenants • Inability to respond to incidents traversing our cloud apps and data • Inability to encrypt data within the environment • Misuse by insiders from your organization • Poor data hygiene or inability to delete data from the environment • Breach of sensitive data by cloud provider personnel • Not knowing with certainty where sensitive data is geographically located • Lack of visibility into what data is being processed in the public cloud and where • Lack of ability to audit • Malware intrusion from other cloud tenants • Inability to meet compliance requirements • Misconfiguration or vulnerability of hypervisors and other virtualization managers • Unauthorized access by outsiders • Inability of the cloud provider to meet service level or SLAs • Poor configuration and security of quickly spun-up application components (e.g., containers) • Downtime or unavailability of applications when needed	• Denial of service attacks • Misconfiguration or vulnerability of hypervisors and other virtualization managers • Account or credential hijacking • Exploit against hosting provider vulnerability • Exploit against virtual server OS/application vulnerability • Sensitive data exfiltration directly from cloud app • Privileged user abuse • Crossover from other hosted cloud applications • Adversary pivoting from cloud to internal systems

[44] Shackleford, Dave (2017). Cloud Security: Defense in Detail if Not in Depth. A SANS Survey, 2017 SANS Institute. https://www.sans.org/summit-archives/file/summit-archive-1519076280.pdf

2.4 Cloud Computing Privacy and Security Implementation Worldwide

It is important to note that privacy and security have distinct concerns and impacts. Security concerns the technical parts of Cloud computing implementation such as system integrity, prevention from unauthorized access and service availability. Privacy, on the other hand, focuses on the legal or regulatory parts of Cloud computing such as unauthorized access to personally identifiable information and tampering or deletion of personal information. The potential impacts of security include destruction of data or systems, loss of business and reputation damage while privacy causes violation of regulations, laws and a person's rights. Thus, security and privacy also use different measures and tools. Security uses intrusion detection, perimeter hardening, defense in depth and information security policy to fulfill security requirements. Privacy approaches include the implementation of data encryption, personnel vetting, identity and access management, split-and-spread, and privacy policy. Security and privacy measures, strategies, laws and regulations vary and change rapidly. Thus, Cloud computing users need to periodically review every aspect covered by privacy regulations.[45]

Privacy and security measures, framework, strategies, assessment, benchmarking, risk management, laws and regulations, cloud partnership (international and across public-private sectors) collaboration agreement and cloud actors (across jurisdictions, responsibilities and liabilities) are some of the prepared government documents to be referred by organizations that adopt Cloud computing services in many countries. Privacy regulations covers the scope of the protection, entities to which the regulations apply, protected data transmission to other countries, "safe harbor" status, available data protection agency of the government, government special rights and available overriding protection in government's constitution. [45] Table 2.4 presents security and privacy implementation worldwide.

[45] CSCC (2017). Security for Cloud Computing Ten Steps to Ensure Success Version 3, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

Table 2.4: Security and Privacy Implementation [46] [47]

Region	Security Implementation	Privacy Implementation
Worldwide	• Most countries have security requirements and implemented cybersecurity frameworks, laws and policies	• Payment Card Industry (PCI) Data Security Standards (DSS)
United State	• Security requirements of Federal Government IT programs. • Federal Information Security Management Act (FISMA) requires every decision to apply Cloud computing model ✓ to comply with Federal Information Processing Standards agency specific policies; ✓ to fulfill Authorization to Operate requirements; and ✓ to perform vulnerability and security event monitoring, logging, and reporting. • NIST Risk Management Framework is prepared to ensure secure and trustworthy Cloud environment. To form a solid governance foundation, the following bodies have been specified certain roles and responsibilities (NIST, 2011): ✓ National Institute of Standards and Technology (NIST) with Federal, State, and local government agencies, private sectors, and international bodies identify and prioritize cloud computing standards and guidance ✓ General Service Administration (GSA) develops government Cloud-based application solutions where needed ✓ Department of Homeland Security (DHS) monitors Cloud operational security issues ✓ Organizations are responsible to evaluate strategies to consider Cloud computing solutions ✓ Federal CIO Council drives Cloud adoption among government agencies, identify next-generation cloud technologies, and share best practices and reusable example analyses and templates ✓ The Office of Management and Budget (OMB) coordinates activities across governance bodies, set overall cloud-related priorities, and provides guidance to agencies	• No privacy laws • Privacy obligations in specific circumstances imposed by range of government agency and industry sector laws • Lots of gaps and overlaps in coverage • Examples of industry sector privacy laws ✓ Federal Trade Commission Act ✓ Electronic Communications Privacy Act ✓ Health Insurance Portability and Accountability Act ✓ Fair Credit Reporting Act ✓ Gramm-Leach-Bliley Act

[46] CSCC (2017). Security for Cloud Computing Ten Steps to Ensure Success Version 3, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

[47] Cloudscorecard.bsa.org (2016). 2016 BSA Global Cloud Computing Scorecard. Retrieved from http://cloudscorecard.bsa.org/2016/

Region	Security Implementation (cont.)	Privacy Implementation (cont.)
Japan	• Japan has a comprehensive suite of modern laws that support and facilitate the digital economy and cloud computing. • Japan's intellectual property laws cover the full range of protections relevant to cloud computing. • Japan is very active in the development of international standards.	• Japan has comprehensive privacy legislation, which it plans to strengthen by introducing a new central regulator, complemented by stronger enforcement provisions that will come into force in 2017. • Personal Information Protection Act; protects personal data
EU	Security Framework for Governmental Clouds implement Plan, Do, Check, Action (PDCA) Cycle. Based on input collected during the desk research and some preliminary interviews, a logic model for a security framework for governmental clouds was sketched including the specific activities and steps. In addition to that, a description of the different roles of the involved parties (cloud customer, cloud provider, citizens, so on) is included and their responsibilities/involvement to each of the phases of the lifecycle is defined. Risk Management also has been included in Security Framework for Governmental Clouds.	• General Data Protection Regulation (GDPR) • Different local laws and regulations • Stricter rules in Benelux countries, the Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Iceland, Portugal, Slovakia, and Slovenia
New Zealand	• Risks of using Cloud services are assessed based on value, criticality and sensitivity. • Official information is classified following documented guidelines Security in Government Sector (SIGS, 2002) and official information are protected following New Zealand Information Security Manual (NZISM).	• For New Zealand, the Government Chief Privacy Officer has issued core expectations that represent good practice for privacy management and governance in the State services. • A Privacy Maturity Assessment Framework has also been developed to help agencies assess their existing capability and implement appropriate improvements. • The expectations and the Privacy Maturity Assessment Framework were developed and tested in collaboration with privacy practitioners from across government. Risk Management has been included in the Privacy Maturity Assessment Framework. • The Government Chief Information Officer (GCIO) guides agencies to obtain social licenses for public cloud services. The guidance is based on research performed by the Data Futures Partnership and Stats NZ. In public cloud services, jurisdictional risks or data sovereignty occur where data is subject to the laws of the country where cloud services providers store, process, or transmit data. • GCIO has also developed frameworks for assessing jurisdictional risks in relation to both jurisdictions and cloud services providers. Agencies are encouraged to use these frameworks to inform their risk assessments of public cloud services (ICT.govt.nz, 2018).

Region	Security Implementation	Privacy Implementation
Australia	• The government will clarify obligations on agencies in relation to risk management, data security, privacy and the storage and processing of data offshore. The government also publishes guidance targeted towards industry and users on how existing privacy legislation fits with cloud computing. • R&D are initiated for the areas of privacy, security interoperability, portability and the use of cloud services for data analysis. • The Protective Security Policy Framework (PSPF) establishes the risk management framework that agencies must use in addressing risks to Australian Government information holdings. • The PSPF directs agencies to apply sound security risk management practices and is complemented by the Information Security Manual (ISM). • The National Standing Committee for Cloud Computing (NSCCC) is a collaboration between industry, consumer groups and government. Chaired by DBCDE, and co-chaired by Global Access Partners. • The NSCCC has been an invaluable way for government and industry to consider the issues impacting on cloud computing in Australia. • Australian government set up a CloudStore to provide a marketplace of qualified cloud offerings on public clouds or G-Cloud from the industry for government agencies to procure.	• Cloud service providers are obliged to follow Australian Economy wide Privacy Act 1988 to appropriately protect personal information (including where data is stored and processed in jurisdictions outside of Australia). • Consumer protection and effective law promotes adequate privacy protection. • Austrade will work in partnership with industry to promote Australia as a trusted hub for data storage and processing and will encourage foreign investment and participation. • Government's privacy responsibilities under the Privacy Act 1988, the Freedom of Information Act 1982, the Archives Act 1983, and other legislation.
Singapore	• Singapore has legislation that enables Singapore's law enforcement and government security bodies to seek access to information. • Foreign law enforcement bodies may also work with the local law enforcement and government security bodies to obtain access to information in Singapore. • Security and privacy issues are considered as key factors to consider for migration, and at the same time are the main barriers for adoption. • The Multi-Tier Cloud Security (MTCS) Singapore Standard (SS584) is the world's first cloud security standard that covers multiple tiers of cloud security. It can be applied by Cloud Service Providers (CSPs) to meet differing cloud user needs for data sensitivity and business criticality. It is a key part of building trust through transparency as cloud grows in importance. While the adoption of MTCS Singapore Standard (SS584) is voluntary for CSPs, SS584 is a requirement for CSPs participating in public cloud services bulk tenders for Government procurement of public cloud services. • For Singapore, MTCS has three levels of security, Level 1 being the base and Level 3 being the most stringent: ✓ Level 1; Designed for non-business critical data and system, with baseline security controls to address security risks and threats in potentially low impact information systems using cloud services (e.g. Web site hosting public information) ✓ Level 2; Designed to address the need of most organisations running business critical data and systems through a set of more stringent security controls to address security risks and threats in potentially moderate impact information systems using cloud services to protect business and personal information (e.g. Confidential business data, email, CRM – customer relation management systems) ✓ Level 3; Designed for regulated organisations with specific requirements and more stringent security requirements. Industry specific regulations may be applied in addition to these controls to supplement and address security risks and threats in high impact information systems using cloud services (e.g. Highly confidential business data, financial records, medical records)	• Singapore has the most stringent privacy regulations of ASEAN region. Personal Data Commission established in 2013 enforces Personal Data Protection Act 2012. • ISO/IEC 27018:2014 establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

Region	Security Implementation (cont.)	Privacy Implementation (cont.)
Asia Pacific region, and others		• Some countries have data protection laws based on Privacy and Security Guidelines of the Organization for Economic Cooperation and Development (OECD) and Asia Pacific Economic Cooperation's (APEC) Privacy Framework • Malaysia and India have limited protections • Besides Singapore, South Korea also has stringent privacy regulations of the region.

2.5 Summary of Part 2

Security and privacy are the most critical fit issues that need to be carefully considered before adopting Cloud in agencies and organizations. This part of the report has discussed in detail the Cloud security and privacy issues, cases and implementation guidelines. The comparison of the existing implementation for both security and privacy in other countries has also been presented. Part 3 explains why Cloud First is recommended to be implemented in Malaysia, the proposed data classification for Malaysian context and the steps by steps implementation guideline.

PART 3

Embracing Cloud First Policy- the Malaysian Context

3.1 Why Cloud First Policy is recommended?

Cloud First policy can be one of the strategy for Malaysia to wisely adopt for digital transformation of public and private sectors in the country. Cloud technology enables rapid delivery of public sector services with reduction in cost. Through this policy, Malaysian government can also facilitate Cloud adoption among private sectors and encourage the publishing of progressive guidelines for companies in regulated industries such as banking and financial services.[48] Advantages for adopting Cloud by the public sectors among others are improved efficiency and productivity, increased speed and agility, access to greater services, reduced procurement and maintenance cost, create innovation opportunities, provide operational continuity and business recovery, allow focus on core activities. These facts are further explained in Appendix B.

Based on studies performed and presented in Part 1 and Part 2 of this document and 2018 Planning Guide for Cloud Computing by Gartner[49], the latest findings show that organizations worldwide adopt Cloud First strategy across multiple layers of Cloud services that are software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS). As discussed in Part 1 of this document, Cloud First strategy is an option only if the adoption of Cloud computing is suitable and provides more benefits to the organizations after considering security risks and constraints. Not all IT components are suitable to be migrated to Cloud infrastructure and platforms due to issues such as security, compliance, governance and performance that need to be carefully considered. Therefore, hybrid IT approach is also a norm in which Cloud computing is rapidly adopted while maintaining the on-premise IT infrastructure. The challenge is to maintain data privacy and securely manage integrations and interdependencies.

In Part 3 here, two important matters are discussed and recommended for organisations, particularly public sectors in Malaysia to be concerned on when adopting Cloud First policy:

a) Data classification for prioritization of data
b) Process and checklist for proper execution and management

The discussion also incorporates security and privacy checklists that should be considered in every critical step. This provides guideline on how to adopt Cloud computing by assuming that organizations have

[48] Cloud First strategy to be introduced to national agenda
http://english.astroawani.com/malaysia-news/cloud-first-strategy-be-introduced-national-agenda-158403
[49] 2018 Planning Guide for Cloud Computing, https://www.gartner.com/doc/3810365/-planning-guide-cloud-computing

equipped themselves with the latest knowledge of Cloud computing characteristics (i.e. on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service), service models (i.e. SaaS, IaaS and PaaS), and deployment models (i.e. public, private, community and hybrid).

3.2 Data classification

One major concern that public sectors have when adopting cloud is what can be on the cloud and what should not. In other words, a concern on security, privacy and data residency prior to adopting Cloud technology. A practical and well-documented data classification framework is an important starting point for public sector entities when considering incorporating cloud services. This helps decision makers and officers in charged to understand what types of data can be stored on which platform and systems.

Let's step back to understand and organize data accordingly so that one can strike a balance of reaping advantages of Cloud (as in Appendix B) while securing privacy and confidentiality of data. In Malaysia, the Official Secret Act (1972) known as OSA has 5 levels of data classifications as depicted in Figure 3.1 - Top Secret (Rahsia Besar), Secret (Rahsia), Confidential (Sulit), Restricted (Terhad) and Unclassified.

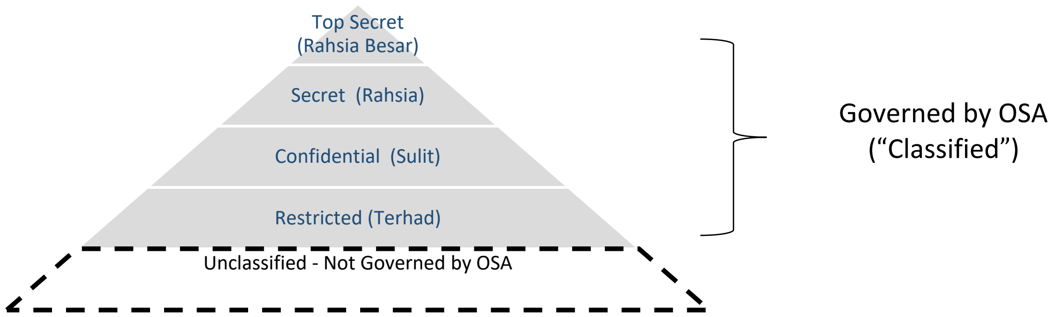


Figure 3.1: The existing data classification in Malaysia based on Official Secret Act (OSA)

Four of the data classes i.e. Top secret, Secret, Confidential and Restricted are governed by the OSA as Classified while the last one as Unclassified and not governed by the OSA.

The triangle in Figure 3.1 also represents that the amount of data increases from top secret to unclassified information. But nevertheless, the cost of overprotecting this massive volume of less sensitive data in the lower end of the pyramid can be staggering as indicated in Figure 3.2. Conservative calculations suggest at least a 10 times cost difference between systems required for very sensitive information, and the commercial systems suitable for the less sensitive information that a government holds. A key benefit of a robust data classification is thus the ability to better align costs with security.[50]

[50] Microsoft (2018). Malaysia Cloud Adoption 2018. Inclusive Cloud Adoption in Malaysia: From Procurement to Consumption.

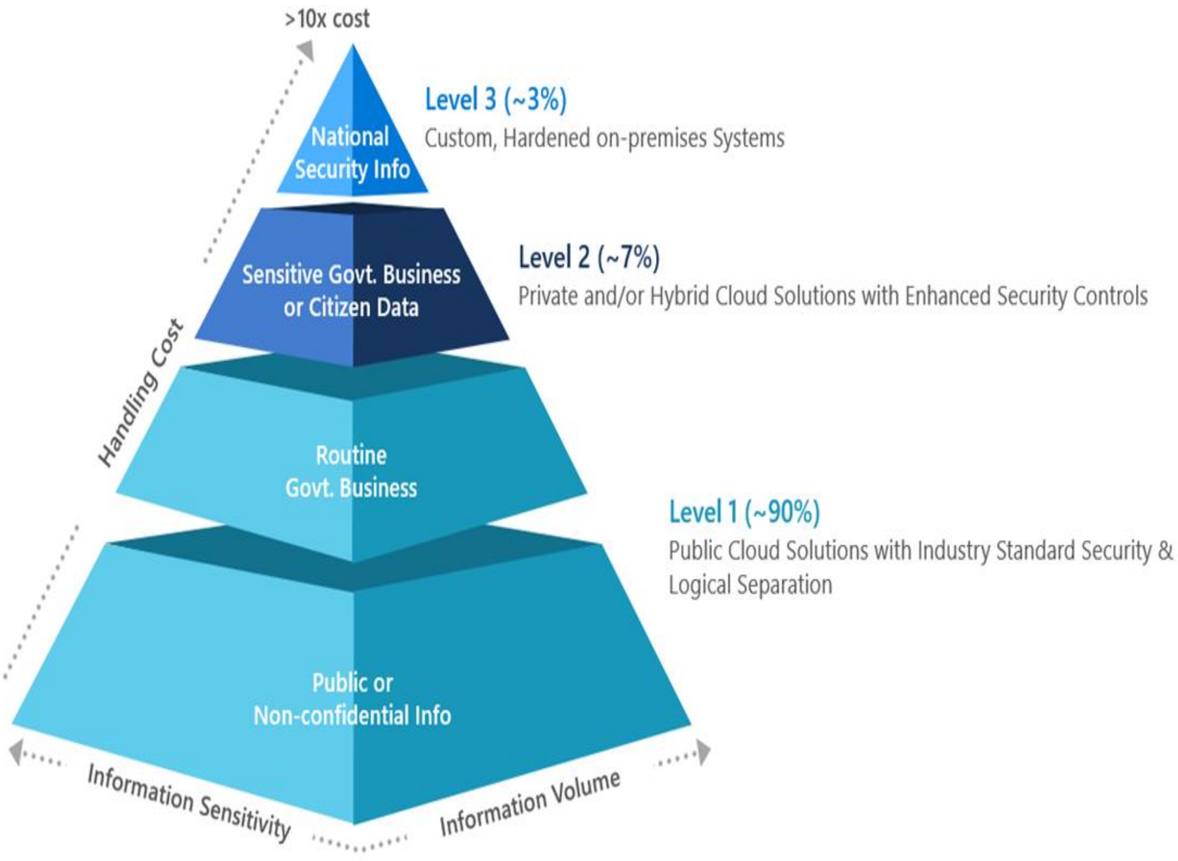

>10x cost
Level 3 (~3%)
Custom, Hardened on-premises Systems
National Security Info
Level 2 (~7%)
Private and/or Hybrid Cloud Solutions with Enhanced Security Controls
Sensitive Govt. Business or Citizen Data
Handling Cost
Routine Govt. Business
Level 1 (~90%)
Public Cloud Solutions with Industry Standard Security & Logical Separation
Public or Non-confidential Info
Information Sensitivity
Information Volume

Figure 3.2: Relationship between data sensitivity, data volumes and cost of security controls [51]

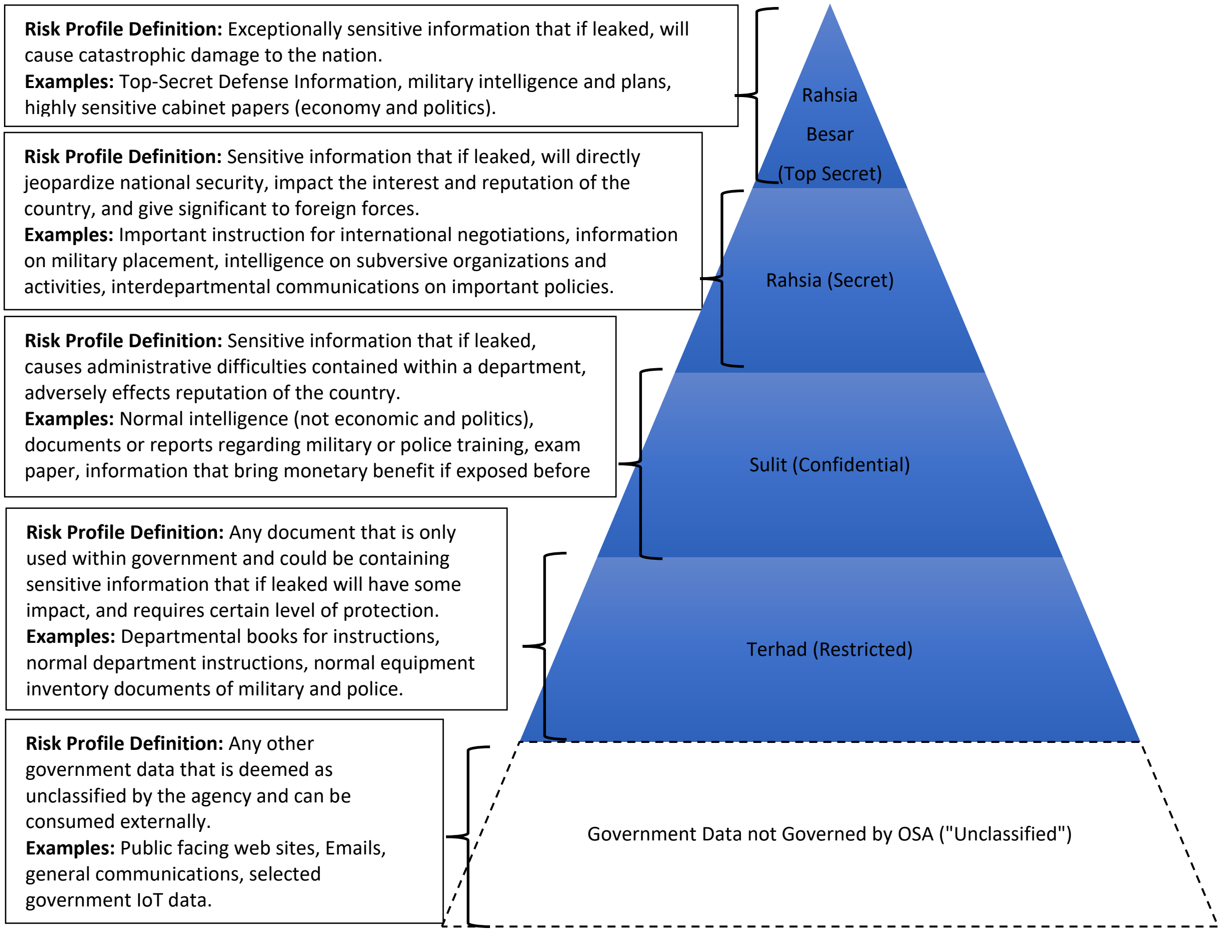
Classification of data comes with risk assessment. Based on the risk assessment particularly for confidentiality and integrity of official documents, decisions can be made on what and how official documents can be stored, transmitted or used. Figure 3.3 shows the OSA document classification with risk assessment framework for each data categories.

[51] Microsoft (2018). Malaysia Cloud Adoption 2018. Inclusive Cloud Adoption in Malaysia: From Procurement to Consumption.

Figure 3.3: Risk Assessment Framework to address confidentiality and integrity

OSA Document Classification Model

Proposed Risk Assessment Framework - to address confidentiality and integrity risks.



Risk Profile Definition: Exceptionally sensitive information that if leaked, will cause catastrophic damage to the nation.
Examples: Top-Secret Defense Information, military intelligence and plans, highly sensitive cabinet papers (economy and politics).

Risk Profile Definition: Sensitive information that if leaked, will directly jeopardize national security, impact the interest and reputation of the country, and give significant to foreign forces.
Examples: Important instruction for international negotiations, information on military placement, intelligence on subversive organizations and activities, interdepartmental communications on important policies.

Risk Profile Definition: Sensitive information that if leaked, causes administrative difficulties contained within a department, adversely effects reputation of the country.
Examples: Normal intelligence (not economic and politics), documents or reports regarding military or police training, exam paper, information that bring monetary benefit if exposed before

Risk Profile Definition: Any document that is only used within government and could be containing sensitive information that if leaked will have some impact, and requires certain level of protection.
Examples: Departmental books for instructions, normal department instructions, normal equipment inventory documents of military and police.

Risk Profile Definition: Any other government data that is deemed as unclassified by the agency and can be consumed externally.
Examples: Public facing web sites, Emails, general communications, selected government IoT data.

Rahsia Besar (Top Secret)
Rahsia (Secret)
Sulit (Confidential)
Terhad (Restricted)
Government Data not Governed by OSA ("Unclassified")

Note: Emails are not classified - but DLP checked and outbound email must contain attachments (except links to files).

As part of simplifying and preserving the present data classification in Malaysia, it is proposed to map the existing OSA data classifications into 4 tiers as in Figure 3.4. Top secret documents are grouped as Tier 1 category, Secret documents are classified as Tier 2, Confidential and Restricted Official documents are combined as Tier 3 and Unclassified documents as Tier 4.

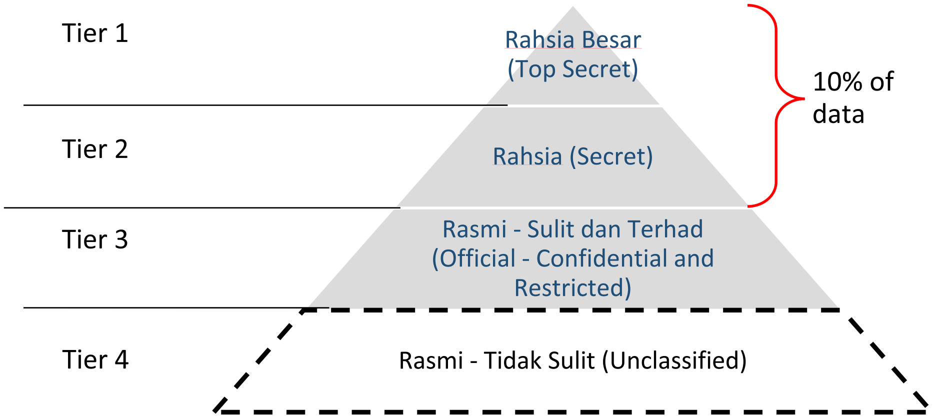

Tier 1
Tier 2
Tier 3
Tier 4
Rahsia Besar (Top Secret)
Rahsia (Secret)
Rasmi - Sulit dan Terhad (Official - Confidential and Restricted)
Rasmi - Tidak Sulit (Unclassified)
10% of data

Figure 3.4: Mapping the existing OSA classification into four tiers of data classifications

The proposed data classification for Malaysia is based on UK new data classification approach[52]. Description in terms of the implication of each tier's data leakage and example of each classification tiers are described in Table 3.1.

[52] Introducing the Government Security Classifications, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf

Table 3.1: Description and examples of a 4-tiered data classification

Classification	Description	Examples
Tier 1 **Top Secret Data (*Data Rahsia Besar*)**	This category is the most sensitive information that the highest levels of protection from the most serious threats are required. The exceptionally sensitive information that if leaked, will cause catastrophic damage to the nation.	Top secret defense information, military intelligence and plans, highly sensitive cabinet papers on economy and policies.
Tier 2 **Secret Data *(Data Rahsia)***	This category includes very sensitive information that requires high protective measures to defend against highly capable threat actors.	Secret military capabilities, international relations or investigation of serious crime.
Tier 3 **Confidential and Restricted Official Data (*Data Rasmi Sulit dan Terhad)***	Confidential and restricted official data are sensitive information that if leaked, causes administrative difficulties contained within a department and will adversely affect reputation of the country.	Normal intelligence (not economic or political), documents or reports regarding military or police training, national examination papers, information that bring monetary benefits if exposed before time.
Tier 4 **Unclassified Official Data (*Data Rasmi Tidak Sulit)***	This encompasses any other government data that is deemed as unclassified by the agency and can be consumed externally.	Public facing websites, official documents for public reference, emails without Tier 2 and Tier3 information, general communications, downloadable official forms.

To further understand the underlying of these four tiers, listing on controls of each tier is tabulated in Table 3.2.

Table 3.2: Security controls for each data classification of electronic documents

Public Sector Data Classification	Security Controls
Tier 1: **Top Secret Data** **(*Data Rahsia Besar*)**	• Clearance Level: Strictly for a very minimal number of authorized government personnel with official security clearance • Access: 2 factor authentication, Digital Rights Management (DRM), audited logs • Electronic Transmission: Strictly Prohibited, Air-Gapped Systems, Encrypted, In-country • Electronic Storage: Special Isolated PC/Printer, Air-Gapped Government DC/System, ISO27001, DRM, Encrypted, In-country • Electronic Disposal: NIST-80088 electronic data destruction
Tier 2: Secret Data (*Data Rahsia*)	• Clearance Level: Strictly for a minimal number of authorized government personnel with official security clearance • Access: 2 factor authentication, Digital Rights Management (DRM), audited logs • Electronic Transmission: Prohibited (Print only), Air-Gapped Systems, Encrypted, In-country • Electronic Storage: Special Isolated PC/Printer, Air-Gapped Government DC/System, ISO27001, DRM, Encrypted, In-country • Electronic Disposal: NIST-80088 electronic data destruction
Tier 3: Confidential and Restricted Official Data (*Data Rasmi Sulit & Terhad)*	• Clearance Level: Authorized Government Officials/Users • Access: 2 factor authentication, DRM, audited logs • Electronic Transmission: Encrypted, Rights Management System (RMS), Data Loss Prevention (DLP) protected, sharing via URLs • Electronic Storage: Any secured DC, ISO27001, Encrypted • Electronic Disposal: Delete accompanied by overwriting of storage space *(added overwriting to avoid data carving by irresponsible party).*
Tier 4: Unclassified Official Data (*Data Rasmi Tidak Sulit)*	• Clearance Level: Any authorized users • Access: Authentication, audited logs • Electronic Transmission: Encrypted, DLP protected *(conflicting with electronic disposal?)* • Electronic Storage: Any DC, ISO27001 • Electronic Disposal: Normal Delete

Referring to Table 3.2, all four tiers of data classifications have their own clearance level, access control and handling of the electronic transmission, storage and disposal.

As for Tier 1 - Top secret category, its clearance level is strictly for a very minimal number of authorized government personnel who has official security clearance; its access controls are with at least 2 factor authentication on different mediums, applies Digital Rights Management (DRM), and has its file logs audited periodically; strictly no digital or printed transmission of the document, apply air-gapped systems, electronic document versions are to be encrypted with strong algorithm and proper encryption key management and the document physically does not leave the dedicated storage; in terms of electronic storage, it has to be in an air-gapped government data center, applies ISO 27001:2013 (or latest version), apply DRM, file encryption and available in country only; for digital document disposal, apply NIST-80088 electronic data destruction.

For Tier 2 - Secret category, its clearance level is strictly for a minimal number of authorized government personnel who has official security clearance; its access controls are with at least 2 factor authentication on different mediums, applies Digital Rights Management (DRM), and has its file logs audited periodically; strictly no digital transmission of the document, transmit only in printed form, apply air-gapped systems, electronic document versions are to be encrypted with strong algorithm and proper encryption key management and the document physically does not leave the country; in terms of electronic storage, it has to be in an air-gapped government data center, applies ISO 27001:2013 (or latest version), apply DRM, file encryption and available in country only; for digital document disposal, apply NIST-80088 electronic data destruction.

In Tier 3 – Official Confidential and Restricted documents clearance level is for authorized government officials and users only, its access controls are with at least 2 factor authentication on different mediums, applies Digital Rights Management (DRM), and has its file logs audited periodically; electronic documents can be transmitted but MUST be encrypted, impose Rights Management System (RMS), apply Data Loss Prevention (DLP) controls, file sharing must be through URL to ease monitoring of data access and control of data not leaving internal server that hosts it; electronic storage can be at any secured data center with mandatory encrypted with strong algorithm encryption and proper management of the encryption key and apply ISO 27001:2013 (or latest version); disposal of the digital documents is through normal delete accompanied with over writing of its storage medium with appropriate tools such as *DataHapus* (newly developed by CyberSecurity Malaysia for MAMPU) or similar tools that does overwriting.

Lastly, Tier 4 level i.e. Unclassified Official documents have clearance level of any authorized users; access control via authentication without 2 factor authentication and with audited logs of the files; electronic transmission is allowed and encouraged to be encrypted if it involves personal data transmission, DLP protected when necessary; the digital documents can be stored in any data center and apply ISO 270001:2013 (or latest version); electronic disposal can be as normal file deletion.

By referring to controls for each tier in Table 3.2 enable decisions to be made on which data can be on Cloud and which are not to be on Cloud. Tier 4 data, which is unclassified and for public access, suits well to be on the Cloud platform. Proper controls can be made such as authorized user, audit logs and a few others if necessary. As for Tier 3, the confidential and restricted official data, a more stringent control need to be imposed. By having a 4-tiered data classification, it is proposed that the decision for implementation of Cloud computing for government data can be made. Table 3.3 summarizes the details of each classification group in those 4 tiers.

Table 3.3: Details of each data classification group

	Risk Profile (if leaked)	Create	Use	Transit	Storage	Disposal	Best Practice Controls
Top Secret	Nationwide disruption. Widespread loss of life. Affects all of government. Raises international tension.	Staff with top secret clearance. Marked "Top Secret". No device allowed.	Top secret clearance. Need basis. 2 Factor authentication and authorization. No device allowed. Logging use.	Physical transmission only.	Physical storage only.	NIST 800-88 Physical destruction.	Stand-alone system. Dedicated room. Government facilities.
Secret	Disruptions contained within a state of region. Small scale loss of life. Affects state government. Affect diplomatic relationship.	Staff with a minimum Secret clearance. Marked "Secret"	Minimum Secret clearance. Need basis. 2 Factor authentication and authorization. Logging use.	Approved encryption (national encryption if possible)	Approved encryption (national encryption if possible). DRM.	NIST 800-88. Physical destruction.	No connection to internet. ISO27001 compliance. Digital Rights Management. Government DC.
Confidential	Disruptions contained within a department. Adversely effects reputation of government /officers.	Authorized Staff. Created in the server. Marked "Confidential"	Gov-Staff authorized by creator/owner/department 2 Factor authentication and authorization. Logging use. DRM.	Approved encryption. DLP protected.	Approved encryption. DRM.	NIST 800-88. Physical destruction.	ISO27001 compliance. ISO 27018 if outsourced. Digital Rights Management.
Restricted	Privacy of an individual, entity, department or nation. Public or external information that is subsequently considered classified.	Uploaded and/or categorized by Data classification officer.	Users authorized by creator/owner. Valid owner/ originator of data. User authentication and authorization. Logging use. DRM.	Encrypted. DLP protected.	Approved encryption. DRM.	Delete function applied across all storage.	ISO27001 compliance. ISO 27018 if outsourced. Digital Rights Management.
Unclassified	No foreseen privacy risk if accidently leaked.	Any unclassified government official. Other data that are not inherently publicly available.	User authentication and authorization. Logging use.	Approved encryption. DLP protected.	Approved encryption.	Delete function applied.	ISO27001 compliance. ISO 27018 if outsourced. Digital Rights Management recommended.
Open	No risk when publicly used.	Government data explicitly made public. Any non-government entities.	No restriction to use data. Unauthorized changed not allowed.	Encryption recommended.	Encryption recommended.	Delete function applied	ISO27001 compliance. ISO 27018 if outsourced.

It is proposed that the owner of data at ministry, agencies and relevant committee classify their data prior to embarking to any cloud services. An effective approach to implement data classification is to use the PLAN, DO, CHECK, ACT (PDCA) model. Figure 3.5 charts the tasks that are required to successfully implement data classification in this model.

PLAN. Identify data assets, a data custodian to deploy the classification program, and develop protection profiles.

DO. After data classification policies are agreed upon, deploy the program and implement enforcement technologies as needed for confidential data.

CHECK. Check and validate reports to ensure that the tools and methods being used are effectively addressing the classification policies.

ACT. Review the status of data access and review files and data that require revision using a reclassification and revision methodology to adopt changes and to address new risks.

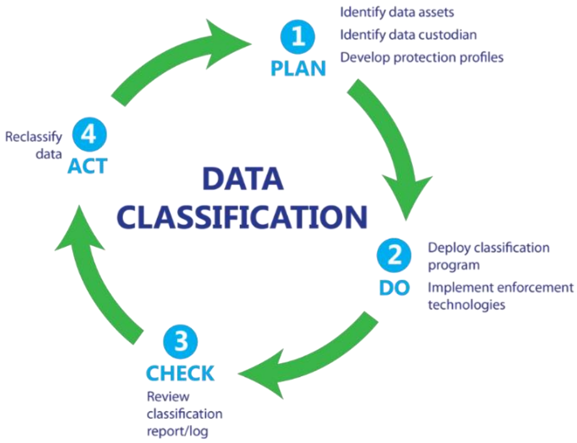

1
PLAN
Identify data assets
Identify data custodian
Develop protection profiles
DATA CLASSIFICATION
2
DO
Deploy classification program
Implement enforcement technologies
3
CHECK
Review classification report/log
4
ACT
Reclassify data

Figure 3.5: PDCA Framework for Data Classification

Upon having a correct and suitable data classification, government agencies shall or shall not embrace Cloud First policy with proper justifications.

3.3 Cloud Computing Guidelines

The roadmap for Cloud computing has been presented by Cloud Standards Customer Council (CSCC).[53] Figure 3.6 shows that there are 10 steps of Cloud computing guidelines that are presented in the following subsections.

[53] Practical Guide to Cloud Computing, http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Computing.pdf

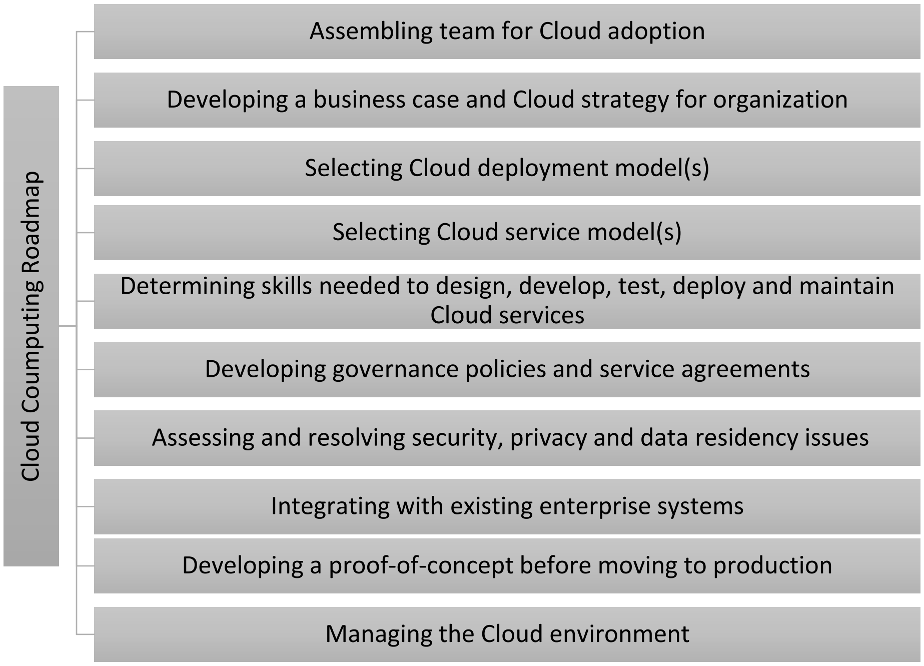

Cloud Coumputing Roadmap
Assembling team for Cloud adoption
Developing a business case and Cloud strategy for organization
Selecting Cloud deployment model(s)
Selecting Cloud service model(s)
Determining skills needed to design, develop, test, deploy and maintain Cloud services
Developing governance policies and service agreements
Assessing and resolving security, privacy and data residency issues
Integrating with existing enterprise systems
Developing a proof-of-concept before moving to production
Managing the Cloud environment

Figure 3.6: 10 steps of Cloud computing guidelines

3.3.1 Assembling team for Cloud adoption

To implement Cloud, a team should be defined to develop and approve Cloud business strategy and implementation plan for Cloud services as part of the whole IT environment. Adopting Cloud computing means the digitalization of business and is a strategic business decision in which decision making should be collaborative between IT and business leaders. Some of the C-Suites tasks look like the following:

CIO: Fulfill cost, performance, longevity, and feature/functionality guideline requirements

CEO: Focus on growing the business and innovate to differentiate through technology

CDO: Map digital capabilities to strategic priorities to improve costs and revenue generation such as re-engineering or automation of business processes, enable new functionality or efficiency, measure efficiencies and ROI by monitoring digital initiatives

CFO: Take care of financial growth while deliver efficiencies through technology adoption and ensure data privacy, security and maintenance of financial records.

CISO: Take care of integrated physical and logical standardization and security through information management, risk management, brand protection, third-party relationship management and other functions beyond traditional role.

CMO: Take care of customer experience, new customer touch points, new opportunities for engagement, and more integrated experiences by co-driving Digital Transformation.

The three phases of Cloud adoption are presented in Table 3.4.

Table 3.4: Three phases of Cloud adoption

No	Phases of Cloud Adoption	Leaders
A	Strategic Planning Phase Discussing vision, terms of reference, and guidelines	CEO and senior management team
(i)	Vision Task: Define the overall vision for Cloud adoption and strategy that address the future of business and the acquired differentiation, competitive advantage, and value proposition gained.	
(ii)	Terms of reference Task: Define purpose, goals, guiding principles, roles and responsibilities, rules of engagement of the teams	
(iii)	Procedures Task: Define broad guidelines including security and privacy, data maintenance and location policies for Cloud adoption in the form of business framework to fulfil high-level requirements	
B	Workload/tactical Planning Phase Performing business and a technical analysis are performed.	Led by the CIO or CTO
(i)	Business analysis Task: Review and communicate regulatory compliance and legal requirements Goal: To define business requirements and long-term strategy for Cloud transition as the foundation for categorizing and identifying applications or workloads to be migrated to the Cloud to deliver sufficient return on investment and value.	Senior business stakeholders such as the CMO, product or application owners, IT (including as necessary the CIO, CTO, CISO, lead architects and business continuity manager), and legal representatives
(ii)	Technical analysis Task: Develop Transformation Guideline that includes components such as Critical Success Factors, Service Management Capability Maturity Guideline, Organizational Functional Model, IT Architectures and Operations Models, Process and Capabilities, etc. as part of the organizations' Technology Guideline. On the Technology Guideline, the business requirement analysis results are mapped to the available Cloud services and deployment models to decide the procurement and provisioning of services.	IT (or digital) stakeholders including the CIO, CTO, CDO, CCO, CISO as well as lead architects, operations personnel, IT security, and senior business managers
C	Operations Planning Phase Identifying operational plan and process	Leaders from various operations groups
(i)	Procurement. Task: Identifying the suitable Cloud providers, discussing the assessment models or instruments	Procurement team, finance, legal, senior business managers, and IT including the CIO, CTO and lead architects to be engage
(ii)	Implementation. Task: Developing, customizing and configuring the solutions for deployment, identifying the required processes and high-level gap analysis to come out with risk mitigation and management.	Lead architects, developers and testers as well as operations personnel.
(iii)	Operations. Task: Inspecting the ongoing operations and management of Cloud services. Detail examination is performed to find the impact for any changes made to the Cloud implementation.	Business owners, operations personnel, customer support, and IT including developers and testers

3.3.2 Developing a business case and Cloud strategy for organization

At this stage, every problem addressed by Cloud computing are identified and specific quantified justification must show that Cloud computing is the right strategic alternative. The key elements of strategic planning are presented in Table 3.5. All team members from entire organizations such as IT, business, operations, legal and executives should be well educated by understanding the Cloud computing definition, terminology and process that adds value to existing IT environments.

Table 3.5: Elements of strategic planning for Cloud First implementation

No	Element of Strategic Planning
a	Educating the team
	- Understanding what Cloud computing is and what it is not
	- Understanding standardized Cloud computing definition and terminology
	- Understanding that Cloud computing is an iterative process that adds value to existing IT environments
b	Preparing short and long-term plans
	- Creating master blueprint and roadmap
	- Mapping Cloud computing benefits against business problems to identify potential solution areas
	- Anticipating disruptions that may occur both inside and outside IT such as service levels, security, legal, vendor management, etc
	- Long term planning considering interoperability, portability and ease of integration up front to reduce the risk of vendor lock in
c	Understanding required services and functionality
	- Determining business case and potential ROI and potential new revenue opportunities
d	Executing thorough cost analysis
	- Analysing overall cost of application migration to Cloud by including: On-going Cloud service costs Service management License management Application re-designs Application deployment and testing Application maintenance and administration Application integration Cost of developing Cloud computing skills Human resources and talent management implications Additional tools/services/processes
e	Assessing the impact to service levels
	- Considering application characteristics (for each migrated application): Application availability Application performance Application security Privacy Regulatory compliance Data residency
f	Identifying clear success goals and metrics to measure progress
	- Defining success factors in proposal
	- Agreeing to metrics
	- Defining baseline for existing service to measure the impact of new services
	- Identifying trigger points to be measured
g	Considering the existing IT environment
	- The developed Cloud adoption strategy must integrate existing technologies, standards and reusable services
h	Assessing the current operational support model
	- Validating the impact of integrated Cloud enabled operational support model

No	Element of Strategic Planning (cont.)
i	Understanding legal/regulatory requirements
	- Understanding legal/regulatory constraints and frameworks to be complied based on: Physical location of data Data breach Personal data privacy Destruction or transfer for unwanted data Intellectual property or information ownership Law enforcement access Service availability - Understanding Cloud service deployment standard and compliances required by various industries
j	Identifying required skills
	- Mapping required skills against available skills - Addressing potential gaps by enhancing internal skills or considering external skills
k	Tracking results for an extended time
	- Reinforcing the achievement of objectives - Identifying trends that can be used to improve the new service
l	Understanding the exit process
	- Ensuring that the exit clause is part of Cloud service agreement - Understanding the exit process and responsibilities of the service provider and customer - Ensuring business continuity during exit process - Specifying measurable metrics to ensure Cloud provider implements the specified procedures - Maintaining privacy of data

3.3.3 Selecting Cloud deployment model(s)

To fulfill organization's business requirements, the suitable Cloud deployment models need to be determined based on many factors as included in Appendix C.

Private Cloud resources are dedicated to one customer. Two forms of private Cloud:

1) On-premises private Cloud is a form where the Cloud environment is implemented in organizations' premises

2) Private hosted Cloud or dedicated Cloud is a form where the Cloud environment is located in provider's premises, but the dedicated resources are not shared with other customers.

Hybrid Cloud has many benefits by addressing the organization requirements to choose public cloud service during high demand and for non-sensitive applications and data such as new software development. Organizations use private Cloud deployment for more sensitive applications and data such as payroll information. Both public and private Cloud deployments are integrated with traditional non-cloud applications and data.

The level of IT maturity and the size of an organization are the factors that contribute to the decisions made towards the type of Cloud service deployment models. There are three types of organizations that are:

- Large organizations with mature IT environments normally choose private cloud deployments at first and later move some workloads to hybrid and public deployments.
- SMBs may choose hybrid deployment models by putting new applications in public Cloud to benefit from cost savings, larger capacity, lower skill requirements and better application functionalities.

3.3.4 Selecting Cloud service model(s)

The three most common Cloud service models are Software as a Service (SaaS), Platform as a Service (PaaS), and Information as a Service (IaaS); each has its potential benefits and issues.

a) Software as a Service (SaaS)

Adopting SaaS is like buying a complete packaged application or service running as a Cloud service. SaaS offers advantages that are:

- Accessibility over the public Internet
- Flexibility to provision and de-provision by choosing services to be consumed and business process to be executed based on usage-based pricing or pay-as-you-go concept
- Minimal configuration as it offers standard feature set
- Eliminating high start-up costs and reducing capital expenditure on the Software installation and licensing as SaaS services are based on subscription basis
- Shorter deployment
- Instantaneous upgrades and transparent testing performed by service providers
- Highly scalable and allows organizations to scale up in the future
- IT infrastructure and software are managed by service providers, allowing organizations to focus on features of services to achieve business objectives
- Security and privacy requirements are fulfilled by service providers
- Availability of the services, backing up data and maintenance of data recovery procedure are provided

There are two categories of SaaS

- Horizontal SaaS offerings. These offerings are typically applicable to organizations across various types of sectors such as email, customer relationship management (CRM), productivity, collaboration, human resources (HR), analytics, etc.
- Sector-specific offerings. Applications in these SaaS offerings are sector-specific such as logistics, supply chain management (SCM) and healthcare.

b) Platform as a Service (PaaS)

PaaS provides:

- Integrated development and runtime platform for creating, deploying and managing custom applications in a Cloud service.
- Integrated workload management, dynamic resource management, high availability and business priorities
- Standardization and automation of common set of topologies and software components
- Elasticity, efficiency and automated workload management
- Workload and infrastructure characteristics can be dynamically adjusted to fulfill priorities and SLAs
- Ready-developed software stack for development and deployment of custom applications
- Reduced resources for applications development and operation
- Quickly and inexpensively develop and deploy new applications

- Support Cloud native applications and technologies such as containers, "serverless" computing and microservices
- Facility for software developers and IT professionals to communicate, collaborate and integrate

c) Infrastructure as a Service (IaaS)

IaaS provides integrated service management, automation and rapid provisioning that give the following benefits:

- Reducing operating expenses and capital expenses by improving resource utilization and administrator-to-server ratio
- Increased efficiency and automation of standardized solutions
- Integrated management and real-time monitoring
- Improved visibility of business processes and system performance
- Scalable operations and resources to fulfill scalable organizations' requirements

Adoption of Cloud Service Model for Large Organizations and for SMBs

Each organization has unique characteristics and different business objectives and requirements. Basically, there are two types of organizations; they are large organizations and SMBs. Large organizations with mature IT systems and infrastructure have implemented in-house applications and have invested a lot in hardware, software, development and runtime platforms, as well as management and human resources. Therefore, these organizations may need time to determine the suitable adoption approach and transformation strategy. SMBs, on the other hand, do not have complex IT infrastructure, development and runtime platforms, lack of human resources and are more willing to adopt the subscription-based services provided by SaaS, PaaS and IaaS to reduce costs. The SaaS, PaaS, and IaaS adoption approach for large organizations and SMBs are included in Appendix C.

3.3.5 Determining skills needed to design, develop, test, deploy and maintain Cloud services

The skills needed for designing, developing, testing, deploying and maintaining Cloud services vary depending on the size of the organizations. Large organizations may reassign internal resources to accommodate and focus towards the new Cloud project. SMBs may use the available internal skills to support existing applications and consider outsourcing the IT deployment and management tasks from Cloud service providers or other independent developers. Appendix D presents the options that can be considered during the transformation and adoption of a new Cloud application services. Additional staff development and training are always needed to ensure that staffs are equipped with the needed Cloud computing skills.

3.3.6 Developing governance policies and service agreements

Organizations as Cloud service customers have the final responsibility for performing due diligence, understanding agreements and potential impact to the day-to-day operations. It is a must for the organizations to have the necessary internal strategy, governance, and processes to benefit from the Cloud computing services. Cloud Service Agreement (CSAs) is composed of three components; they are Customer Agreement, Acceptable Use Policy and Service Level Agreement. To evaluate the Cloud service agreements, the following should be considered:

- Policies. Organizations policies and processes, as well as obligations the organizations have with their customers and suppliers that may constrain Cloud service decisions and operations.
- Culture. Identifying cultural issues that can potentially be considered in agreements.
- Governance. Cloud service agreements should include good governance where appropriate decisions are made to fulfill the transparency and accountability requirements for improving trust and assurance.
- Objectives. Organizations' objectives and expectations determine the approaches taken.
- Metrics/Measures. The Service Level Agreements needs consistent measurement to validate service levels and determine appropriate actions to be taken.
- Terms and Conditions/Acceptable Use Policies. Cloud service agreements' terms, conditions, and use policies that need to be considered include exclusions, limitations, usage and disclaimers.
- Service Level Agreements. This document states the promised technical performance that should be delivered by Cloud providers, appropriate actions during failures, and how any future disagreements should be handled.
- Remediation and Compensation. In case of failures, the offered compensations and responsibilities of the parties involved, as well as the disaster recovery and business continuity plans are to be defined.

Organizations also have responsibilities to constantly monitor that the Cloud services are received as expected and to ensure that the services delivered to the users or clients of the organizations fulfill the objectives.

3.3.7 Assessing and resolving security, privacy and data residency issues

Figure 3.7 shows the process to resolve security, privacy and data residency issues adapted from CSCC.[54]

[54] Security for Cloud Computing Ten Steps to Ensure Success, http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

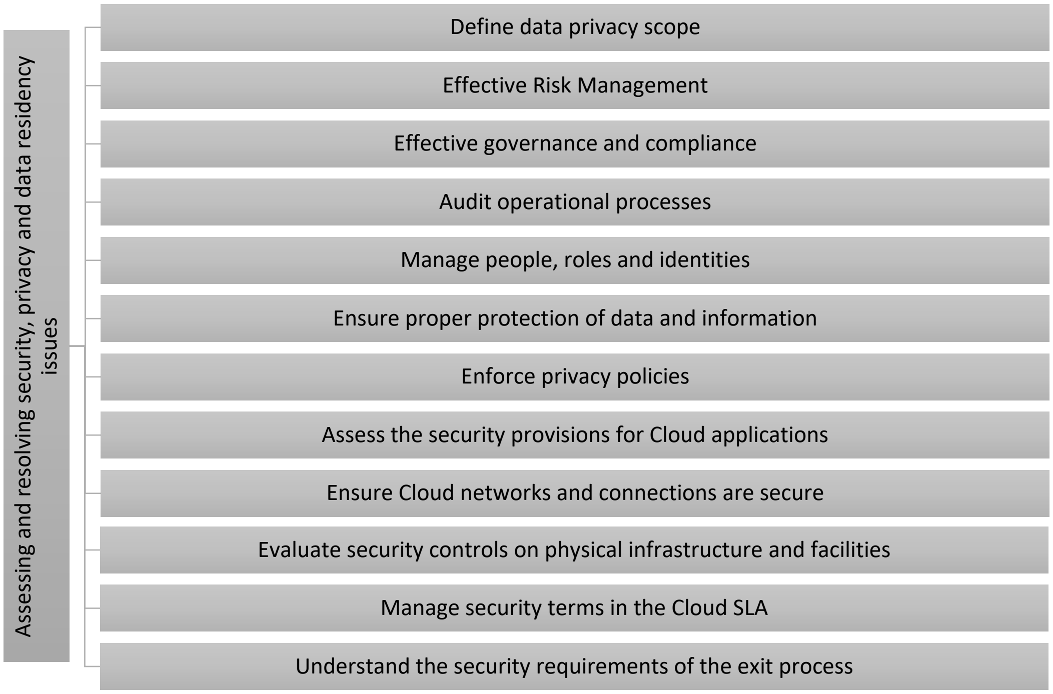

Assessing and resolving security, privacy and data residency issues
Define data privacy scope
Effective Risk Management
Effective governance and compliance
Audit operational processes
Manage people, roles and identities
Ensure proper protection of data and information
Enforce privacy policies
Assess the security provisions for Cloud applications
Ensure Cloud networks and connections are secure
Evaluate security controls on physical infrastructure and facilities
Manage security terms in the Cloud SLA
Understand the security requirements of the exit process

Figure 3.7: Process in resolving security, privacy and data residency

3.3.7.1 Define Data Privacy Scope

The definition of data privacy scope includes the following steps:

1) Identifying the compliance requirements for Cloud systems based on geographic location; For every country where the system will be located, data privacy for all individual states, countries and federal laws must be considered

2) Understanding the various definitions of personal data types and classification for implementing appropriate data protection.

3.3.7.2 Effective Risk Management

The general risk management framework includes risk assessment, risk treatment and risk control. Table 3.6 presents the risk management framework applied to Cloud Ecosystem from Cloud consumers perspective.

Table 3.6: Risk management framework for Cloud ecosystem

Risk management activities	**Steps**	**Risk Management Framework**
Risk assessment (analyse cloud Environment to identify potential vulnerabilities and shortcomings)	1. Categorize	Categorize the information system and the information processed, stored, and transmitted by that system based on a system impact analysis. Identify operational, performance, security, and privacy requirements.
	2. Select (includes Evaluate-Select-Negotiate)	Identify and select functional capabilities for the entire information system, Identify and select the associated baseline security controls based upon the system’s impact level, the privacy controls. Tailor and supplement the security controls by selecting enhancements and/or additional controls deemed necessary.
		Identify and select best-fitting cloud architecture for this information system.
		Evaluate/review cloud Providers that meet Consumer’s criteria (architecture, functional capabilities, and controls).
		Select cloud Provider(s) that best meet(s) the desired architecture and the security requirements (ideally should select the Provider that provides as many controls as possible to minimize the number of controls that will have to be tailored). Identify the controls that will be implemented by the Consumer, the controls implemented by the Provider as part of the offering, and the controls that need to be tailored (via compensating controls and/or parameter selection).
		Negotiate SLA, metrics, and sign SA as part of the procurement process. Document all the controls in the security plan. Review and approve the security plan.
Risk treatment (design mitigation policies and plans)	3. Implement	Implement security and privacy controls for which the cloud Consumer is responsible.
	4. Assess	Assess the cloud Provider's implementation of the tailored security and privacy controls.
		Assess the implementation of the security and privacy controls, and identify any inheritance and dependency relationships between the Provider's controls and Consumer’s controls
	5. Authorize	Authorize the cloud-based information system to operate.
Risk control (risk monitoring - surveying, reviewing events, identifying policy adjustments)	6. Monitor	Continuous monitoring of operations and effectiveness of the security and privacy controls under Consumer’s management.
		Continuous monitoring of cloud Provider's operations related to the cloud-based information system and assess the systems’ security posture.
		Reassess and reauthorize (periodic or ongoing) the cloud Provider’s service.

3.3.7.3 Effective governance and compliance

Organizations must understand the specific laws and regulations such as data retention, privacy, disclosure requirements and residency related to their operations, locations and industries where they belong. To achieve effective governance, the service level agreement (SLA) and associated documents must include the details of actions that should be taken by all the involved parties for every occurrence and incidents that may happen. Organizations should understand roles and responsibilities of providers and customers specified in the service agreements.[55] The actions taken during incidents include sending notification, resolving the incidents, restoring services, applying best practice forensics for investigating the incidents and making long-term changes to avoid future occurrence.

Data governance is also affected by data residency and data sovereignty. Steps of data residency [56] include:

1. **Establish a governance structure.** Each organization should establish a team with representatives from business lines, IT security, legal, compliance and personnel representing geographic locations of organizations' resources.
2. **Ensure proper metadata management.** Each organization should have a complete main enterprise "data landscape" or information model.
3. **Define all the policies and rules on sensitive data elements.** Policies determine the data storage location, data classifications and levels of anonymities and encryption of certain data.
4. **Establish reports to monitor the application of policies.** Organizations should monitor data residing in every countries and jurisdictions and identify deviation.
5. **Implement tools to track the provenance and pedigree of information.** Organizations should track data transformation and process when moving data across boundaries.

To ensure effective compliance to the laws and regulations, the steps may include:

1. **Mapping of laws and regulations into business requirements**; Implementing an online privacy tool and process map for business processes by examining relevant legal requirements allows requirements to be self-determined.
2. **Embedding privacy compliance in organizational culture**; Privacy policies and procedures need to be persistently implemented to fulfil identified compliance gaps in organizations.
3. **Continuously monitoring requirements**; Security requirements are parts of the evolving privacy and data protection laws that need to be monitored.

3.3.7.4 Audit operational processes

Organizations should obtain professional security audits of the Cloud service that are consistent with the followings:

- General international information security standards such as ISO 27001/27002
- Cloud specific standards such as ISO/IEC 27017
- Code of practice for protection of personally identifiable information (PII) in public clouds acting

[55] Public Cloud Service Agreements: What to Expect and What to Negotiate. Version 2.0.1, http://www.cloud-council.org/deliverables/CSCC-Public-Cloud-Service-Agreements-What-to-Expect-and-What-to-Negotiate.pdf
[56] Data Residency Challenges, http://www.cloud-council.org/deliverables/CSCC-Data-Residency-Challenges.pdf

as PII processors, ISO/IEC 27018

Organizations also can provide frameworks for evaluating security controls to be applied to Cloud service providers such as:

- Standards for Attestation Engagements (SSAE 16), a regulation for redefining and updating how service companies report on compliance controls.
- CoBIT 5, a business framework for the governance and management of enterprise IT.
- Cloud Assurance Assessor Program (CAAP) that provides assurance of the qualifications to validate Cloud providers.

There are also standards for specific services or industries include:

- Payment Card Industry (PCI) standard
- Data Security Standard (DSS)

Other guidance provided by Cloud Security Alliance (CSA) and example of codes of conduct include:

- Cloud Controls Matrix (CCM) for assessing the overall security risk of a cloud provider.
- Consensus Assessments Initiative Questionnaire (CAIQ) for cloud consumers and auditors to assess the security capabilities of a cloud provider as well as to become provider self-assessment program.
- Certificate of Cloud Security Knowledge (CCSK), a certification of cloud security knowledge for personnel
- Registry for cloud service providers to publish the self-assessment results (STAR) [9].
- EU Cloud Code of Conduct, codes of conduct to handle personal data in cloud services.

3.3.7.5 Manage people, roles and identities

Organizations should manage proper user identification, strong authentication, and role-based access control to resources. Organizations should consider its requirements and questions Cloud service provider capabilities to support for people, roles and identities that include:

- Federated Identity Management (FIM), External Identity Providers (EIP)
- Identity Provisioning and Delegation
- Single Sign-On (SSO), Single Sign-Off
- Identity and Access Audit
- Robust Authentication
- Role, Entitlement and Policy Management
- Service ID and API Keys

3.3.7.6 Ensure proper protection of data and information

Organizations should assign security classifications to all data including proprietary application code and system images that must be protected against theft and tampering. Organizations can ensure data security by implementing the following controls:

- Create a data asset catalog
- Consider all forms of data
- Consider privacy requirements
- Apply confidentiality, integrity and availability procedures
- Enable security logging and monitoring

- Data activity monitoring

3.3.7.7 Enforce privacy policies

Organizations should enforce policies for the acquisition, secure storage, access limitation, personnel responsibilities, monitoring and use of sensitive data such as Personal Identifiable Information (PII).

3.3.7.8 Assess the security provisions for Cloud applications

Every choice of deployment model (IaaS, PaaS, and SaaS) has different security responsibilities that need to be assessed.

3.3.7.9 Ensure Cloud networks and connections are secure

Cloud provider's internal network and the connection between the providers and customers must be protected and monitored against threats. Cloud providers are responsible to fulfill external network requirements that organizations should evaluate based on the following categories:

- Traffic screening
- Denial-of-service protection
- Intrusion detection and prevention
- Logging and notification

The internal network requirements include:

- Providing tools to protect customers from one another
- Providing tools to allow customers to implement network segmentation
- Protect the provider's network
- Monitoring for intrusion attempts

3.3.7.10 Evaluate security controls on physical infrastructure and facilities

The physical security of the equipment in the Cloud service providers should be protected against accidents and natural disasters, and have proper procedures for personnel screening and disposition of removal media.

3.3.7.11 Manage security terms in the Cloud SLA

The security terms in the Cloud SLA and Cloud Service Agreement (CSA) must be fully understood by all parties. CSA should explicitly document several elements including:

1. Security requirements that need to be fulfilled by providers and must be passed to any peer providers joining to supply any part of services.
2. CSA should document that during data breach incidents, the provider should:
    - Include detail and specific information in the notification
    - Stop the incidents immediately
    - Restore secure access to the service immediately
    - Investigate incidents using best-practice forensic
    - Plan for long-term modifications to infrastructure to avoid future incidents
    - Test the effectiveness of the modifications
    - Compensation that must be given if the breach was the fault of the provider
3. Metrics and standards for measuring performance and effectiveness of information security

management. Some of the resources for specific information on security metrics include:

- ISO/IEC 27004:2016, Information security management -- Monitoring, measurement, analysis and evaluation
- ISO/IEC 19086, Cloud computing -- Service level agreement (SLA) framework
- NIST Special Publication (SP) 800-55 Rev.1, Performance Measurement Guide for Information Security
- CIS Consensus Security Metrics v1.1.0

3.3.7.12 Understand the security requirements of the exit process

Organizations should understand the exit process during termination of the use of Cloud service such as complete removal of customer data from all tiers of storage and proper handling of cache or backup data.

3.3.8 Integrating with existing enterprise systems

Hybrid implementation is commonly implemented for large organizations where Cloud services are integrated with existing applications and systems. The integrated components include data, process integration, management capabilities and business capabilities. Some of the integration process includes:

- Allocate certain period to review and adapt internal policies and processes of the existing applications when they run in Cloud.
- Adopt open standards for data formats, communication protocols and API (or create an adapter component to translate) to achieve interoperability and portability between Cloud services and in-house applications and systems.
- Integrate organization's Identity and Access Management (IdAM) and support a common standard for the system
- Avoid costliest method of integrating new Cloud services into the organization by developing custom code for each new Cloud service.

3.3.9 Developing a proof-of-concept before moving to production

Upon completion of business case for Cloud computing with established business drivers and projected ROI, senior management need to review the proposal, projected costs, timeline, risks, resulting benefits and a rollback plan. If the senior management agrees to proceed, proof-of-concept (POC) team is established comprising resources from Information Technology and Functional Representation. The POC can be implemented either in-house or in public Cloud service using a representative data set rather than production data to ensure data security. Public Cloud service provides quick provisioning and scalability.

To implement POC, the success criteria for the new Cloud services are as follows:

- Costs
- Key performance indicator (KPI)
- User satisfaction
- Infrastructure prep and delivery
- Problem resolution
- Security
- Monitoring and reporting
- Disaster Recovery (DR)

Next, the success criteria for the Cloud implementation activities to be completed by the implementation team are as follows:

- It is verified that the Cloud services delivered required functionalities in a test environment
- It is verified that all processes work as intended
- It is verified that data recovery activities, formatting, migration, and ETL (extract, transform and load) capabilities function
- It is verified that the Cloud services are integrated with management and monitoring systems
- It is ensured that the help desk can address questions and problems quickly
- Back out plan is developed should there is an unexpected problem in the early stages of production so that it will not impact users
- Identity and access management are verified in the new Cloud environment
- Administrative staff have access to perform admin activities within the new Cloud service
- The time taken for data and system recovery activities to be completed in the current system and the new Cloud service are compared

After all the testing activities have been done, all the stakeholders need to sign off that their area is working properly. Next, to put the new Cloud service into full production, the following items should be completed:

- Business contracts are agreed
- Agreed Service Level Agreements (SLAs) are agreed
- Customer support (help desk) are trained
- Post implementation management or operations plan are prepared

3.3.10 Managing the Cloud environment

To ensure successful operation of Cloud service, responsibilities within customer organization are shared mainly between CIO and the manager of customer support as in Table 3.7.

Table 3.7: Responsibilities within customer organization

No	Cloud Environment Management Responsibilities	Team
1	Overall responsibility for the successful operation of Cloud services	CIO
2	Manages the day to day operational challenges	Customer support manager
3	Disaster recovery for a SaaS service - protecting organization and digital assets - initiating the disaster recovery process - completing recovery process - verifying safety of data	Cloud service provider, customer support manager, trained individuals
4	Disaster recovery for a IaaS service - protecting organization and digital assets - initiating the disaster recovery process - completing recovery process - verifying safety of data	Cloud service customer, customer support manager, trained individuals
5	Incident reporting documented in service agreement and service delivery process	Cloud service provider and Cloud service customer
6	Management of the Cloud environment and changes of business requirements	Cloud service customer
7	Management of vendor in multiple Cloud vendors environment	

3.4 Summary of Part 3

Two major issues are highlighted and recommended for organisations, particularly public sectors in Malaysia to be concerned when adopting Cloud First policy – a) Data classification for prioritization of data and b) Process and checklist for proper execution and management. When data are classified accordingly by the organization or data owner, it will ease for decision making on which data are to be in house and which are to be on the cloud for efficiency of services while preserving the privacy and security of data. By following recommended processes with their checklist described in this section, one can ensure proper operational, management and monitoring of cloud adoption can be in practice.

3.5 Conclusion

In conclusion, this guideline educates and proposes to organisations on Cloud Computing and understanding Cloud First policy for adoption.

Reviewing the implementation of Cloud First policy and adoption of Cloud computing in other countries, this guideline combines all important issues and proposes possible solutions to be adopted in Malaysia's context. It gives a clear step-by-step process for organisations and agencies in Malaysia to refer to when adopting Cloud technology, while ensuring privacy and security of organisations' data at rest, data in transit and data in process.

APPENDIX A

Table A.1: Summary of Cloud First or Cloud Computing Implementation in Other Countries

Country	Cloud Implementation and Objective
USA[57]	Objective: To achieve operational efficiencies by adopting "light" technology and shared services
New Zealand[58]	Objective: The Government ICT Strategy and Action Plan to 2017 seeks to improve service delivery and deliver substantial savings across government, with cloud computing as a key enabler.
Australia[59]	Objective: Create and use world-class cloud services to boost innovation and productivity across the digital economy
European Union[60]	Objectives: • Making Europe Cloud-friendly and Cloud-active. • Connecting digital agenda initiatives.
Japan[61]	Objective: Realizing full utilization of ICT through development and diffusion of next-generation cloud services (smart cloud services) that can reach beyond corporate and industrial frameworks to share vast volumes of information and knowledge among all social systems
Bahrain[62]	Objectives: •Reducing the cost of government ICT by eliminating duplication of solutions and fragmentation in the technology environment, and leveraging the efficiencies of on-demand provisioning of ICT services; • Increasing security by using accredited platforms; • Increasing productivity and agility, and thus improving citizen services.
Singapore[63]	Objective: G-Cloud is the next generation whole-of-government infrastructure. It will provide efficient, scalable and resilient cloud computing resources and will be designed to meet different levels of security and governance requirements

[57] The Cloud First Policy, https://www.doi.gov/cloud/strategy

[58] Guideline for Using Cloud Services, https://www.ict.govt.nz/guidance-and-resources/using-cloud-services/

[59] Australia National Cloud Computing Strategy, https://www.communications.gov.au/sites/g/files/net301/f/National_Cloud_Computing_Strategy.PDF

[60] European Cloud Strategy 2012, https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy

[61] Smart Cloud Strategy in Japan (2010), https://www.slideserve.com/inga/smart-cloud-strategy-in-japan

[62] Cloud First Policy, http://www.nea.gov.bh/Attachments/iGA_Cloud-First_Policy_V1.0.pdf

[63] Cloud Computing for Singapore Government Fact Sheet (2013), https://www.tech.gov.sg

Table A.2: Summary of Risks, Goals, Strategy and Policy of Cloud Implementation Worldwide

Country	Risks/Challenges	Goals/Actions	Strategy and Policy
USA		6 steps of the Decision Framework for Cloud Migration	•Selecting services to move to the cloud -Identify sources of value-efficiency, agility, innovation -Determine cloud readiness •Provisioning cloud services effectively •Managing services rather than assets
New Zealand	Security and Privacy	• Exploiting emerging technologies • Unlocking the value of information • Leveraging agency transformations • Partnerships with the private sector	• Exploiting emerging technologies The accelerated pace of disruptive change generated by cloud services presents an opportunity to change the way the public sector operates, exits costs, and delivers services to citizens and businesses • Unlocking the value of information Increased availability of government-held information and data analytics and predictive modelling have the potential to unlock the value of information to help solve complex problems and generate innovative ideas • Leveraging agency transformations Major agency transformation programmes have a critical role in delivering key components of an ICT ecosystem for the public sector that enables the integration of services across multiple agencies and their delivery partners • Partnerships with the private sector Partnerships with the private sector are increasingly being used to drive innovation and encourage greater risk-taking
Australia	• Lack of quality information • Data ownership, privacy and security • Vendor lock-in and interoperability • Unequal bargaining power • Loss of internet connectivity and availability of a quality connection	Maximising the value of cloud computing in Government	• Helping government agencies adopt cloud services • Value first through cloud services
		Promoting cloud computing to small businesses, not-for-profits and consumers	• A comprehensive suite of tools and online resources • Consumer protection and effective law • Enhancing existing successes
		Supporting a vibrant cloud services sector	• ICT skills and capacity • Promoting competition, growth and foreign investment • Supporting research and development
European Union	-Trust and Security, Dependability -Governance and Control -Interoperability and standards -Privacy and Legal	Standards and Certification	• ETSI (European Telecoms Standards Institute) to coordinate stakeholders & identify necessary standards (e.g. for security and interoperability) • Recognize ICT technical specifications for data protection • ENISA & others to assist development of EU-wide voluntary certification schemes • Agree with industry harmonised metrics for energy consumption & carbon emissions of cloud services
		Safe and Fair Contract Terms	• Develop with stakeholders model terms for cloud computing service level agreements for professional cloud users • European model contract terms and conditions pursuant to Common European Sales Law; expert group for cloud-related issues beyond the CSL • Review standard contractual clauses & binding corporate rules for international data transfers by cloud providers • Work with industry towards a code of conduct for cloud providers for Article 29 Working Party to endorse
		European Cloud Partnership	• What: ✓ Identify common requirements for public sector cloud use ✓ Towards common & joint public procurement of cloud services ✓ Shape the market to benefit private use • How : ✓ Steering Board: industry and MS ✓ Pre-Commercial Procurement Action with MS (FP7, EUR 10m call published), with industry input ✓ Umbrella for MS cloud activities

Country	Risks/Challenges	Goals/Actions	Strategy and Policy
Japan	Delay in utilization of ICT • Lagging behind in utilization of ICT in government; medical care; education; agricultural, forestry, and fisheries; etc. • Need for full utilization of ICT through diffusion of cloud services	Utilization Strategy	• Promotion of ICT Utilization ✓ Medical care cloud ✓ Education **cloud** ✓ Agriculture cloud • Advancing social infrastructure ✓ Smart grid ✓ Green ITS (Intelligent Transportation System) ✓ Management of roads & bridges through IPv6 based sensor networks • Vitalization of SMEs & venture companies ✓ Cross-regional cooperation between SMEs ✓ Improvement of Supply Chain Management through cloud services
		Technology Strategy	• R&D ✓ Technology for collection, extraction, accumulation and modeling of a vast ✓ Majority of real-time streaming data and its optimization at times when ✓ conditions change ✓ Technology that enhances security and reliability ✓ Technology that promotes “Green ICT” - Green by ICT : Green cloud data centers - Green of ICT • Standardization ✓ User-centric approach is required. ”Elimination of excessive lock-in” vs “Ensuring service & technology innovation” ✓ Focus should be put on: --- SLA --- Security level --- Interoperability for hybrid cloud services
		International Strategy	• With the widespread use of cloud services, case storing and processing of data overseas may increase. • Issues to be discussed at international fora （examples） ✓ Jurisdiction over databases stored in other countries (e.g. privacy protection act) ✓ Dispute settlement mechanism ✓ Countermeasures against “harmful” information ✓Possibility of government intervention with respect to private-sector data ✓ Ownership of IPRs regarding data stored on a cloud data center in other countries • Towards consensus building ✓ Cooperation between public and private sectors ✓ITU, OECD, APEC, and other international fora ✓ Bilateral consultations
Bahrain		• ICT at entity level must focus on functional excellence and delivering higher business value • ICT Infrastructure is one key candidate for national level consolidation and optimization • Standardized infrastructure management facilitate changes in government business processes in an easier and quicker way - Enable cost optimization and risk reduction across government through leveraging common platform and information systems for cross-	

		government service delivery	
Country	**Risks/Challenges**	**Goals/Actions**	**Strategy and Policy**
Singapore		• High Assurance Zone – a physically dedicated computing resource pool which will only be used by Government to serve its high assurance needs. • Medium Assurance Zone – a computing resource pool which will be shared with non-government cloud users to lower cost computing resources for Government with security controls in place; and • Basic Assurance Zone – a computing resource pool based on public cloud offerings.	To further aggregate the whole-of-government demand to maximise cost savings to the Government, the Government will identify and provide Software-as-a-Service offerings, such as business analytics, customer relationship management and web content management. G-Cloud enables standardisation, and sharing of computing resources and applications at the whole-of-government level, thereby generating cost savings to the Government.

APPENDIX B

Benefits of a Government Cloud First Policy[64]

Benefits	Benefits of Cloud to the Government
Improved efficiency and productivity	Government agencies are able to improve server utilization as well as the productivity in application development, management and network.
Increased speed and agility	In a cloud computing environment, new IT resources are only ever a click away, which means reduced time taken to make those resources available from weeks to just minutes. This results in a dramatic increase in agility for the government agencies, since the cost and time it takes to experiment and develop is significantly lower.
Access to greater service breadth and depth	Cloud computing allows governments to access industry-shaping technology quickly, at an affordable cost, irrespective of the scale.
Cost reduction	By using cloud computing, governments can achieve a lower variable cost because their usage is aggregated in the cloud, which translates into lower, “pay-as-you-go” prices.
Pace of innovation	Governments are able to quickly tap into innovation in the private sector and create more links with emerging technologies than before, encouraging an entrepreneurial culture within the government.
Operational continuity and business recovery	With centralized data storage, management, and backups, data retrieval and business recovery during times of crisis (e.g. natural disasters or other disruptive events) become faster, easier and more cost effective.
Focus on core competencies	The ultimate benefit of the cloud is that governments can spend less time on undifferentiated tasks and more time focusing on delivering services and adding value to the public.

[64] Microsoft (2018). Malaysia Cloud Adoption 2018. Inclusive Cloud Adoption in Malaysia: From Procurement to Consumption.

APPENDIX C

The consideration factors to determine the suitable Cloud deployment models[65]

Consideration Factors	Private	Hybrid	Public
Criticality of cloud services	Private clouds are appropriate for mission critical applications and compliance sensitive services necessary for business continuity. Critical data availability is key to deciding whether to keep the workload on-premise.	Hybrid deployments help take advantage of public cloud features for certain non-critical workloads, while retaining business critical data and applications on-premise.	Public clouds are more appropriate for services that are not mission critical and do not require access to sensitive information. They can also be more appropriate for organizations that do not have the resources to ensure high availability of on-premises systems.
Type of workload	Private on-premises may be preferable for applications that have very stringent latency requirements.	Cloud bursting of on-premises core business capabilities during seasonal surge is an example; replicating selected customer information to a lightweight cloud database for quicker access by mobile apps is another.	Public cloud is suitable for workloads that require access to high volume data (e.g., real-time analytics running against very large data stores), for workloads with highly variable load patterns, and for access to advanced services that may be difficult to implement on-premises.
Migration costs	With a Private deployment model, installing and managing cloud software may incur significant cloud software costs even if non-allocated hardware exists within a consumer organization. Expenses may be mitigated if the organization has adopted a service-oriented architecture environment and moves to an expense formula for internal departments.	Hybrid deployments, by definition, are transitory between private and public, and hence a point in migration to/from public cloud. Costs can be controlled based on need and maturity.	Public clouds have low upfront costs for the use of cloud services. The implications are similar to the outsourced private cloud scenario except that additional security precautions need to be taken into account.
Elasticity	With Private (On-premise), finite resources are available since computing and storage capacity is fixed and has been sized to correspond to anticipated workloads and cost restrictions. If an organization is large enough, it may be able to provide enough elasticity to clients within the consumer organization.	Hybrid deployments typically include a component of public cloud services; availability of resources is only limited by acceptable security limitations.	Public clouds can generally be considered unrestricted in their size. Additionally, they can generally use multi-tenancy without being limited by static security perimeters, which allows a potentially high degree of flexibility in the movement of customer workloads to available resources.

[65] Practical Guide to Cloud Computing, http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Computing.pdf

Consideration Factors (cont.)	Private	Hybrid	Public
Security threats	With Private (On-premise), consumers have the option of implementing appropriately strong security to protect resources against external threats to the same level of security as can be achieved for non-cloud resources.	Organizations utilizing Hybrid deployments can choose to limit the kind of data/services that are exposed to the public, thus helping mitigate threats.	With a Public model, customers have limited visibility and control over information regarding security. The details of provider system operation are usually considered proprietary and not available for examination by customers. Certification of cloud services may provide a level of assurance to customers.
Multi-tenancy	With Private, risks are mitigated by restricting the number of possible attackers: all of the clients would typically be members of the customer organization or authorized guests or partners.	Multi-tenancy on the public part of a Hybrid cloud can be limited to either periodic use (bursting) or by exposing limited information/services to the public cloud. Sensitive and mission critical areas can still reside on-premises to minimize risks.	With a typical Public model, a single physical machine may be shared by the workloads of any combination of customers. In practice, this means that a customer's workload may be co-resident with the workloads of competitors. This introduces potential reliability and security risks, though evolution of technology and practices have helped reduce both.
Compliance	Organizations using an on-premise model typically have more control but also more responsibility in ensuring compliance with various industry and government standards (HIPAA, GDPR, etc.) since they control the entirety of the infrastructure.	Hybrid deployments help organizations stay compliant by providing the customer with the ability to choose the environment most suitable for compliance requirements – on-premises or public cloud. Care needs to be taken however, to ensure compliance where solutions transition between the two.	Many public cloud services are explicitly certified for compliance with one or more standards and/or regulations. It is necessary to select cloud services with appropriate certifications - or cloud services which the customer can get certified appropriately.
Environment portability	For on-premise deployments, portability is unlikely to pose a significant challenge.	Portability is typically an issue with the public cloud part of a Hybrid deployment. In addition to avoiding potential vendor lock-in, organizations need to ensure access via API and a streamlined integration approach to all parts of the applications/infrastructure.	Organizations need to investigate portability and minimize risk of vendor lock-in before they proceed with deployment on public clouds.
Disaster Recovery/ Failover	Depending on the size and maturity of the organization and the nature of the application, DR and failover provisioning might involve significant costs and workload. It might require multiple physically separated data centers, for example.	Organizations might choose to leverage public cloud to act as a failover option for their internal applications, or for disaster recovery, but they need to ensure regular synchronization between on-premises and public cloud systems.	Many large cloud service providers have multiple data centers across the globe and provide DR and failover options with standardized and documented procedures.

APPENDIX D

The options for acquiring a new Cloud service [66]

Options	Skills	Startup considerations	Updates to services	Testing, deployment and support
In-house development and deployment	Dependent on internal skills, acquired training, and availability of in-house resources to develop and support new applications.	Should reduce the learning curve on how to link to legacy services.	The enterprise owns the cloud application and can incorporate future updates and maintenance based on their internal processes and schedule.	Offers potentially tighter controls and governance during the testing, deployment and support process. In-house test and operations managers can work closely with IT and business leaders to ensure thorough support is provided.
Cloud provider development, deployment and support	The cloud provider's area of expertise is cloud computing which should translate into a shorter development and deployment timeline especially with the first cloud service.	A cloud provider will have to be educated on the legacy services which will be linked to the cloud service (APIs, data formats, security, etc.).	If the cloud provider does the maintenance for new features, the enterprise needs to understand costs and the expected responsiveness to complete requested updates.	Requires coordination between the enterprise development and operations teams with the cloud provider development and test teams.
Independent cloud service development provider	Should have proven experience and expertise on the specific cloud application service under consideration, thereby reducing development, testing and deployment costs.	Will require education and production knowledge of the legacy services and infrastructure which will be linked to the cloud service.	Will require coordination and a structured engagement with the enterprise implementation team and also the cloud provider implementation team in order to test and deploy the cloud service.	Ongoing updates, testing, and governance could be more complex and costly as well as take longer given the need to coordinate three parties as opposed to two.
Off the shelf purchase of a cloud application Software as a Service (SaaS)	Ensure that the application meets all the business requirements for the enterprise and all the open standards and API requirements of the enterprise.	Validate the level of effort required to adjust business processes accordingly and map the off the shelf data formats to the enterprise's data formats.	Determine who will be responsible for the modification, testing deployment, and maintenance activities.	Ensure the total cost of ownership of the off the shelf service offsets the costs for modification. If the time to production-ready deployment is significantly shorter, then the off the shelf option should be considered.

[66] Practical Guide to Cloud Computing, http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Computing.pdf