

amazon web services
institute

Cloud First Playbook for Asia Pacific (APAC)



Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Notices.....	2
Contents.....	3
Leave behind	5
Backbone Document.....	9
Why Cloud Computing is Different.....	10
Defining Cloud Computing.....	11
Benefits of Cloud Computing	13
Journey to Cloud: What is a Cloud First Policy?	15
Journey to Cloud: What is a Cloud Native Policy?	15
Module 1: Security	16
Shared Security Responsibility Model.....	17
Cloud Certifications and Compliance.....	18
Data Privacy and Control.....	19
What Next?	19
Module 2: Data Classification	20
Value of Data Classification	21
Creating a Data Classification Policy.....	21
Data Residency	23
Appendix 1: Data Classification Example	24
Module 3: Starting your Cloud Journey.....	31
Starting your Cloud Journey	32
Module 4: CSP Accreditation.....	36
Creating an Accreditation Guideline.....	37
<i>Appendix 1: Sample Cloud Accreditation.....</i>	<i>38</i>
Module 5: Cloud Procurement	39
Cloud Procurement.....	40
Sample Cloud First Policy	47
Sample Cloud First Policy.....	48
Section 1: General Policy.....	48
<i>Goal.....</i>	<i>48</i>
<i>Cloud First Policy.....</i>	<i>48</i>
<i>Agency Implementation</i>	<i>48</i>
<i>Cloud Computing Benefits</i>	<i>49</i>

Section 2: Definition of Terms.....	50
<i>What is Cloud Computing?</i>	50
<i>Essential Characteristics</i>	50
Section 3: Data Classifications.....	51
Section 4: Security.....	53
<i>Shared Responsibility Security Framework</i>	53
<i>Data Residency</i>	55
Section 6: Migration Policy.....	56
1. <i>Take stock</i>	57
2. <i>Plan</i>	57
3. <i>Migrate and Manage</i>	57
Section 7: Data Ownership, Retrieval, and Interoperability	58
<i>Data Ownership</i>	58
<i>Ownership</i>	58
<i>Access</i>	58
<i>Interoperability</i>	58
<i>Open Data</i>	58
Section 8: Accreditation Process for CSPs.....	59
<i>Baseline Security Controls</i>	59
<i>Technical and Sector-Specific Certifications</i>	59
Conclusion	60

Leave Behind



Why Cloud First?

Executive Summary

The world's leading digital governments rely on the cloud's flexibility, innovation, and scale to empower officials with the insight they need to deliver top-tier public services. Amazon Web Services (AWS) helps governments become digital organizations, which enables them to focus on their core mission: serving citizens. Modern governments work on the front lines of service delivery and face a challenging fiscal environment. With no room for administrative waste, governments increasingly need rapid access to technologies that simplify their processes, deliver massive reductions in administrative costs, and enable innovation to create efficient and effective citizen services.

Commercial cloud computing has become the default pathway for governments to transform themselves into innovative citizen-centric service delivery organizations—just as it has become the default for innovation in the banking, insurance and professional services market. Cloud Service Providers (CSPs) such as AWS offer a range of on-demand services from compute, storage, networking, database, to powerful analytics including artificial intelligence and machine learning functions that make service delivery more accurate and more effective. Throughout the service sector, the cloud has become the industry standard as organizations recognize the cost-savings potential relative to on-premises data centers, the cloud's embedded high level of security, and its data science capabilities (in addition to a myriad of other benefits the cloud offers).

Cloud First

A Cloud First policy directs or requires government agencies to use commercial cloud services as the primary enabler for IT modernization. CSPs now make it easy for government customers to move away from the capital expenditure (CapEx) model of buying and owning physical IT assets that depreciate. Instead, agencies can allocate their IT budgets toward operating expenditures (OpEx) to cover only the services they use, while also avoiding traditional CapEx-related 'tech debt' through having on-demand access to leading-edge IT products and services. A well-crafted Cloud First policy can lead to cost savings, provides greater security than on-premises solutions, allows the flexibility for government entities to adjust usage, and augments efforts for workforce development and transparency.

Key Policy Considerations

Federal governments from Argentina to Australia, Bahrain, Canada, Chile, the Philippines, Singapore, the United Kingdom, and the United States have adopted smart cloud policies to modernize their IT infrastructure. Drawing on these experiences, AWS has identified a set of best practices to support a transition to cloud-first environment.

- **Promoting Cloud First policies:** Governments issue a policy statement with an actionable directive – including timetables—that creates a framework for the implementation of cloud technologies, clarifies the roles and responsibilities of government entities and CSPs, and establishes a procurement vehicle that is designed to gain the full benefits of cloud technologies. Once governments have established cloud first policies and procurement vehicle, their IT professionals can engineer 'born in the cloud' or 'cloud native' solutions.

- **Cloud Accreditation, Compliance, and Security:** Governments use existing domestic and international cloud-centric accreditation systems to evaluate CSPs (rather than create their own unique certification programs) and leverage the shared responsibility model for cloud security.
- **Data Classification:** Governments categorize their data based on its level of sensitivity, and then manage each segment in a manner congruent with its level of sensitivity.
- **Data Privacy and Control:** Governments establish and/or adopt complementary security, data processing and privacy policies to support a successful transition to the cloud.
- **Cloud Contracting and Procurement:** Governments design and institute a cloud contracting vehicle that agencies can use to gain the full benefits of cloud, with cloud-centric terms and conditions, pricing, governance, security, etc. Contract vehicles and procurement guidelines recognize the pay-as-you-go model of commercial cloud computing, and the role of CSP partners and resellers in the cloud delivery model.

As governments transition to Cloud First policies, CSPs have identified a few potential policy pitfalls. To optimize the cloud journey, government leaders need to (1) fully commit to the cloud, (2) formalize the budgeting and procurement processes, (3) establish timelines for cloud migration, (4) take steps to avoid traditional hardware and licensing-based vendor lock-in, and (5) take the time to build and then follow a cloud migration roadmap.

The full AWS team is at the disposal of government leaders to help develop and implement smart cloud-first policies.

Case Study: The United Kingdom's Cloud Journey

The UK Government is a global leader in commercial cloud adoption. The UK Government first released a cloud strategy as part of its Government ICT Strategy in March 2011. The first cloud strategy fit right into the UK Government Digital Strategy's objective at the time of transforming the government and become 'digital by default.' The initial cloud strategy articulated a need for a cloud contract vehicle (G-Cloud) that would include pay-as-you-go with flexibility for agencies to scale-up and down as needed, and avoid vendor lock-in. By May 2013, the UK Minister for the Cabinet announced a Cloud First policy that applied to all public sector IT procurements and emphasized the need for faster adoption across government agencies to take advantage of cost savings. In the years since, the Cabinet Office established a three-tiered data classification system for government contractors (2014), the National Cyber Security Center published cloud implementing security principles (2016), and announced a shift from cloud-first to cloud native (2017). More recently, the National Health System issued guidance on best practices to secure patient data and other digital health initiatives (2018).

UK federal employees access the G-cloud program through the digital marketplace. After completing an internal approvals process, government officials can log on, select the options that best fits their needs—be it Infrastructure-as-a-service, Platform-as-a-service, or Software-as-a-service. Examples of UK agencies that rely on AWS include the UK Ministry of Justice, Data Service, and Driver and Vehicle Licensing Agency - all using the AWS Cloud. In the years to come, UK government agencies are well positioned to develop programs in a cloud native environment.

Backbone Document

Defines cloud computing and a Cloud First Policy, and introduces the cloud value proposition.

Why Cloud Computing is Different

The primary difference between cloud computing and traditional “computing” or IT, is that in a cloud model you are not buying physical assets. Before cloud computing, if you wanted compute, storage and other IT services you first needed to buy physical servers, network equipment, racks, and cabling. Then in a secure, air conditioned and climate controlled room, you would take your IT equipment and unpack it, install it, connect it, configure it, assign it, manage it, and monitor it. You paid the bills to power all of this infrastructure and every few years you had to replace your servers and infrastructure, along with occasionally purchasing additional servers and infrastructure to meet projected increases in demand.

Cloud computing – a hyper-scale, distributed, and highly secure IT infrastructure – stands in contrast. Through cloud computing, government entities have access to powerful compute, storage, and other IT services, and pay to tap into these services in a utility-style model – only paying for the resources used. Cloud Services Providers (CSPs) offer cloud services at massive scale, in the same way to all customers, with customers tapping into these standardized services on-demand—only paying for what they use.

Understanding the fundamental differences between the standardized delivery model of cloud computing compared to traditional on-premises IT, which has a high degree of customization, helps set expectations regarding CSP and government customer responsibilities in a cloud model. As cloud customers do not purchase physical assets from CSPs, it follows that governments should not approach cloud policy and procurement as if they are purchasing physical assets. Cloud policy should take into account how standardized utility-style services are budgeted for, procured, secured, and used, and build a Cloud First strategy that is intentionally different from traditional IT—designed to harness the benefits of the cloud delivery model.

Defining Cloud Computing

Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the Internet with pay-as-you-go pricing. Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet. A cloud services platform owns and maintains the network-connected hardware required for these application services, while the user provisions and uses what is needed via a web application.

This cloud model is composed of five essential characteristics and deployment models.¹

Essential Characteristics

1. **On-demand self-service.** Government agencies can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2. **Broad network access.** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).
3. **Resource pooling.** The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to agency demand. There is a sense of location independence in that the government agency generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.
4. **Rapid elasticity.** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward to commensurate with demand. To the agency, the capabilities available for provisioning often appear to be unlimited and can be utilized in any quantity at any time.
5. **Measured service.** Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer (i.e., the government agency) of the utilized service.

¹ The NIST Definition of Cloud Computing, Special Publication 800-145, Sep 2011, Definition of Cloud Computing
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Deployment Models

1. **Private.** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. government agencies). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
2. **Virtual Private.** The cloud infrastructure is provisioned for exclusive use by a single organization based on enhanced global security and compliance standards. It provides a virtual private cloud environment off premise with strong isolation and may provide dedicated infrastructure for exclusive use by an organization.
3. **Community.** The cloud infrastructure is provisioned for exclusive use by a specific community of users from agencies (or organizations) that have shared concerns (e.g. mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the agencies in the community, a third party, or some combination of them, and it may exist on or off premises.
4. **Public.** The cloud infrastructure is provisioned for open use. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
5. **Hybrid.** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds).

Benefits of Cloud Computing

Cloud computing has brought forth a new and more efficient means of managing government information technology resources, and opens up avenues for modernization, innovation, and cost savings. The main benefits of cloud computing for government entities are listed below.

1. **Cost savings** – Cloud computing grants government customers access to significant cost savings as they move from a forecast-procurement model to a consumption model and benefit from economies of scale. For example, according to a 2018 International Data Corporation (IDC) White Paper, commissioned by AWS,² “on average, organizations will lower 5-year cost of operations by 51%” by moving to the AWS Cloud.”
2. **Greater budget control** – A utility-based ‘pay for what you use’ model means that government agencies can purchase as much or as little resource as they need, as they need it. Cloud scalability results in systems usage being dialed up or down throughout the year as it is required. The cloud also makes it easier to identify the cost of a system and attribute IT costs to individual business owners, resulting in greater transparency.
3. **Spur innovation** – Cloud computing provides industry-shaping technology quickly, at an affordable cost, no matter what the scale. Governments simply cannot effectively keep pace with private sector innovation through continuing to refresh on-premises infrastructure every three or five years. Cloud computing is in a state of exponential technological advance compared to on-premises IT, and can drive innovation throughout government and public sector agencies.
4. **Leapfrog ahead in development** – In the past, it took decades for emerging markets to acquire the technical resources and infrastructure to stay ahead of the pack. With the advent of cloud computing, governments have instant access to world-leading technologies, are able to deploy IT projects at scale immediately.
5. **Inter-agency collaboration for greater efficiency and better citizen services** – Cloud computing enables more effective collaboration as agencies more easily share resources across institutions, allowing for greater efficiency, entrepreneurship, and creativity in delivering public services.
6. **Faster deployment of services** – Reducing the amount of ICT infrastructure required to be built and owned by government agencies reduces overall deployment times, and shifts the focus from management of infrastructure to delivery of services. Public ICT facilities and services can be tested and deployed quicker, and maintained more cost effectively, than if government agencies own and run unique computing facilities themselves.

²

https://pages.awscloud.com/Global_IDC_Enterprise_White_paper.html

7. **New security models** – Governments can obtain greater security in the cloud than is available in traditional data centers. The cloud enables customers to formalize account design, automate security and governance controls, and streamline auditing.
8. **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.
9. **Decreased spending on legacy infrastructure** – Deploying government services in cloud infrastructure results in immediate reductions of large capital outlays for ICT infrastructure and maintenance costs, and also allows government customs to optimize future spend.
10. **Efficiency and sustainability** – Cloud computing helps governments meet and exceed efficiency and carbon reduction targets. For example, a typical large-scale cloud provider achieves approximately 65% server utilization rates versus 15% on-premises, which means when companies move to the cloud, they typically provision fewer than 1/4 of the servers than they would on-premises.³

³ NRDC 2014 "[Data Center Efficiency Assessment](#)" report

Journey to Cloud: What is a Cloud First Policy?

A Cloud First Policy directs government entities to use public cloud services as the default, and in preference to traditional IT systems. In light of the benefits the public cloud brings, a Cloud First policy is aimed at accelerating cloud adoption within government. A smart Cloud First Policy will dictate the following:

In order to increase cloud adoption, all government agencies shall:

1. Include cloud as part of their strategic ICT plans and budgets
2. Utilize cloud for all new projects and workloads
3. Consider cloud first while migrating or upgrading existing applications or infrastructure

It is important to state that Cloud First means *Public* Cloud First. The importance of scale cannot be underestimated when it comes to realizing the benefits of cloud computing, and a private or community cloud cannot come close to matching the massive scale (and associated benefits of scale) of the public cloud. Only a commercial public cloud provider operating at a truly massive scale, with millions of customers worldwide, can create a model that can then pass on the value and benefits of operating at scale to customers.

Journey to Cloud: What is a Cloud Native Policy?

A Cloud Native policy focuses on utilizing “born in the cloud” solutions, rather than simply directing government agencies to lift and shift their current IT operations to the cloud. In a typical cloud journey, a public sector entity starts by using cloud computing for basic infrastructure needs, such as compute and storage, and then makes a step towards Cloud Native by picking “born in the cloud” solutions. In the final ideal end state of a government with a Cloud Native Policy, government and public sector entities will be opting for standalone “born in the cloud” solutions.

Journey to Cloud

A cloud first policy can be seen as the first step in a longer-term strategy to move to a truly “cloud native” solution.



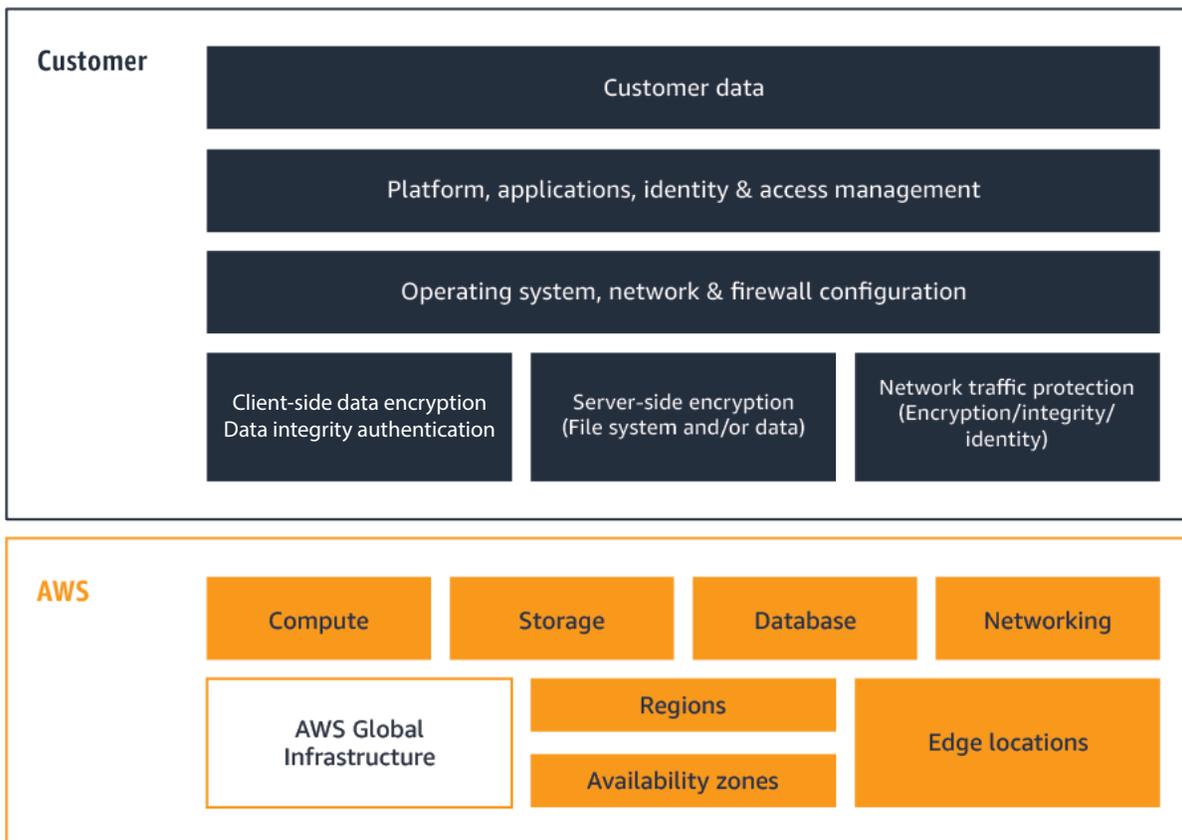
Module 1: Security

Introduces the Shared Responsibility Model, compliance programs, and how data control works in the cloud.

Shared Security Responsibility Model

Security and Compliance is a shared responsibility between a cloud service provider (CSP) like AWS and the customer. While each CSP has a different model and terminology, the key elements of the shared responsibility can be understood by looking at the AWS Shared Responsibility Model. The AWS Shared Responsibility Model can help relieve customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS-provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is referred to as Security "of" the Cloud versus Security "in" the Cloud.

AWS Shared Responsibility Model



AWS responsibility "Security of the Cloud" - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility “Security in the Cloud” – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Virtual Private Cloud (Amazon VPC), and Amazon S3 are categorized as Infrastructure as a Service (IaaS) and, as such, require the customer to perform all of the necessary security configuration and management tasks. If a customer deploys an Amazon EC2 instance, they are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance.

A clear understanding of the shared responsibility model is central to a solid cloud security strategy, and should be clearly communicated in policy.

Cloud Certifications and Compliance

Third party certifications provide government organizations with assurance that cloud providers have effective physical and logical security controls in place. When government customers leverage these certifications they avoid subjecting themselves to duplicative, overly burdensome processes or approval workflows that may not be required for a cloud environment. Using such accreditations also enables government customers to build a more efficient and fast compliance process.

The following figure displays just some of the many certifications that AWS has achieved and secured for its customers over the last decade.



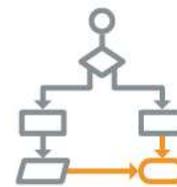
Certifications/Attestation

- DoD SRG - FedRAMP - FIPS - IRAP - ISO 9001 - ISO 27001
- ISO 27017 - ISO 27018 - MTCS - PCI DSS Level 1 - SEC Rule
- 17-a-4(f) - SOC 1 - SOC 2 - SOC 3



Laws, Regulations, and Privacy

- CS Mark (Japan) - EAR - EU Model Clauses - FERPA - GLBA
- HIPAA - HITECH - IRS 1075 - ITAR - My Number Act (Japan) - U.K. DPA 1988 - VPAT/Section 508 - EU Data Protection Directive
- Privacy Act (Australia) - PDPA - 2010 (Malaysia) - PDPA - 2012 (Singapore)



Alignments/Frameworks

- CJIS - CLIA - CMS EDGE - CMSR - CSA - FDA - FedRAMP TIC
- FISC - FISMA - G-Cloud - GxP (FDA CFR 21 Part 11)
- IT Grundschutz - MITA 3.0 - MPAA - NERC - NIST - PHR
- UK Cyber Essential

Data Privacy and Control

Cloud policy should require that CSPs provide governance-focused, audit-friendly services that are built with global data privacy and data protection best practices in mind. For example, validation by an independent third party attesting that a CSP aligns with ISO 27018, the first international code of practice to focus on protection of personal data in the cloud. This validation demonstrates that a CSP has a system of controls in place specifically to address the privacy protection of their content.

Cloud policy should also be clear that customers retain full control and ownership over their data, and have the ability to choose the geographic location(s) in which to store their data. Cloud providers should also provide identity and access controls enabling customers to restrict access to customer infrastructure and data. There are five important basic concepts regarding data ownership and management in the cloud shared responsibility model:

1. Customers continue to own their data.
2. Customers choose the geographic location(s) in which to store their data—it does not move unless the customer decides to move it.
3. Customers can download or delete their data whenever they like.
4. Customers can “crypto-delete” their data by deleting the master encryption keys that are required to decrypt the data keys, which are, in turn, required to decrypt the data.
5. Customers should consider the sensitivity of their data and decide whether and how to encrypt the data while it is in transit and at rest.

Government customers should ensure that CSPs provide documentation detailing how customers can use cloud services to meet specific compliance and data privacy/protection requirements, based on international standards.

What Next?

- Consider picking a test agency to run a proof-of-concept (POC) to identify and address security concerns
- Once the initial POC has been conducted, create a template and scale to other government agencies
- Establish a Cloud Center of Excellence (CCOE) comprised of key decision-makers involved in the journey to cloud to oversee and drive additional efforts
- Consider allocating resources for cloud training for government employees

Module 2: Data Classification

Introduces the value of data classification and best practices for creating a data classification policy.

Value of Data Classification

Data classification has been used for decades to help organizations safeguard sensitive or critical data with appropriate levels of protection. Regardless of whether data is processed or stored in traditional on-premises systems or the cloud, data classification is a starting point for maintaining the confidentiality (and potentially the integrity and availability) of data based on the data's risk impact level.

Data classification allows organizations to think about data based on sensitivity and operational impact, which then helps the organization assess risks associated with different types of data. Reputable standards organizations, such as the International Standards Organization (ISO) and the National Institute of Standards and Technology (NIST), recommend data classification schemes so that information can be more effectively managed and secured according to its relative risk and criticality, advising against practices that treat all data equally. Each data classification level should be associated with a baseline set of security controls that provide appropriate protection against vulnerabilities, threats, and risks which commensurate with the designated protection level.

By classifying information based on risk, an organization can focus its security efforts on appropriately protecting information that is sensitive. The result is better security exactly where security is needed.

Creating a Data Classification Policy

Governments are best positioned to develop their own classification schemes based on organizational and risk management needs. Government agencies should select the appropriate cloud deployment model according to their specific needs, the type of data they handle, and assessed risk (refer to table below). Depending on the classification of the data, agencies will need to apply the relevant security controls (e.g., encryption) within their cloud environment. In most cases, a three-tier data classification approach (Table 1) works well for governments, government organizations, and commercial customers.

Table 1 — Example Three-tier classification scheme

Data Classification	System Security Categorization	Cloud Deployment Model Options
Unclassified	Low to High	Accredited public cloud
Official	Moderate to High	Accredited public cloud
Secret and above	Moderate to High	Accredited public cloud/hybrid/community cloud/tightly-controlled public cloud

To create a data classification policy, governments should keep in mind the three-tier classification scheme, and note the following key high-level principles:

- There is typically no need to provide a carve-out for sector-specific data, such as healthcare, defense, or financial services data. In public cloud, all customers benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.
- Most government data will fall into the unclassified or official categories.
- Avoid over classification. Over-classification of data into more discrete categories than required increases the complexity of storing, processing and transmission of data, and can result in an overall weakening of security by spreading an organization's defenses over a much broader set of systems and data than is necessary. Over-classification may also incur additional costs when implementing controls and limit availability of data and capability opportunities.
- Where possible, data classification policies themselves should not be classified as "secret and above". It will be difficult for CSPs to help enable customers to comply with a data classification policy that cannot be reviewed because the policy itself is classified.

Government agencies ready to embark on classifying their own data can refer to the following roadmap:

Phase I — Inventory. The very first step is to conduct an inventory of the various data types that exist in the organization. It doesn't need to be minutely detailed, but enough to gain a broad understanding of what type of data exists, where within the organization it exists, how is it used, and if any of it is governed by a compliance regulation or policy. Once the inventory is complete, group the data types into one of the data classification tiers the organization has adopted. For example, general business correspondence may be assigned to Tier 1 for Unclassified data, sensitive contract information and privacy information may be assigned to Tier 2 for Official data, and national security or intellectual property may be assigned to Tier 3 for Secret data.

Phase II — Risk Assessment and Classify. We recommend that organizations conduct a risk assessment for each broad data type and assign a level of potential risk (Low, Moderate, or High) to each security objective - confidentiality, integrity and availability - with an associated risk matrix. The organization can then assign overall risk to the data (and supporting information systems) based on the high-watermark level across the three factors. Once classified, security controls should align with the risk to the type of information, ensuring to include any required compliance requirements for the specified data (e.g., PCI). This is where data labeling and handling guidance and procedures are developed and implemented as part of the administrative and technical controls. It is important to keep the classification system as simple as possible and to not over-classify data as a risk avoidance technique as it may incur additional costs when implementing controls and limit availability of data and capability opportunities.

Phase III — Security Assessment and System Authorization. A quality assurance process to assess the implementation of security controls is needed to ensure that the proper controls were selected and implemented for the specified system and data, that the controls work as designed, and that any compliance requirements are met. We recommend that a senior IT leader (CIO or CISO) or organizational business leader, who is responsible for the system and data, review the security assessment and formally authorize the system for use in the organization.

Phase IV — Continuous Monitoring. In addition to ever-present external threats, normal system operations, updates, and changes to the environment can potentially affect security controls. It is critical that automated and manual means of monitoring the security of systems are included in the system's development and operations to ensure that changes don't adversely affect the security of a system and take it out of compliance.

See **Appendix 1** for a detailed example of an outcome of the above process.

Data Residency

Data residency requirements do not improve the overall security posture of an organization. Governments should assess their data classification approach and hone in on which data needs to stay within their country or region, and why. By doing so, governments may find that their data, potentially even official or secret data, may be stored and/or replicated elsewhere if there is no particular legal or policy geographical requirement. This can further reduce risk of data loss in the event of a disaster and provide access to technologies and capabilities that may not be available in the government's area.

Moreover, in today's climate, risk management is an even more formidable task when considering mobile technology and the interrelationships between external and internal entities. Any system connected to the internet, directly or indirectly, presents a credible attack vector, without regard for the physical location of the infrastructure or system. As technology continues to advance and change customer threat vulnerabilities and vectors, governments must re-evaluate how they are modelling their data management and privacy strategies and risk tolerance. Three fundamental realities have disrupted the traditional 'full stack control' model of data management:

1. **Most Threats are Exploited Remotely.** The physical location of data has little to no impact on threats propagated over the Internet.
2. **Manual Processes Present Risk of Human Error.** Human process failure plays a role in root cause failure (if not the entire cause) of most cybersecurity.
3. **Insider Threats Prevail as a Significant Risk.** The vast majority of major data compromises have occurred either through unintentional errors or intentional malicious behavior by individuals using authorized accounts that had the right to access the data.

Physical location of data has no bearing on any of the above listed realities. Breaches do not require physical access to a server but instead exploit a lack of effectively implemented logical security controls. The best mechanisms to protect, detect, respond, and recover is to use the transformational security a hyperscale CSP offers through modernization and automation.

Appendix 1: Data Classification Example

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
Unclassified	Low to High	Accredited public cloud	<p><i>(Potential User: All government agencies)</i></p> <ul style="list-style-type: none"> • Most day-to-day government 'business' activities data including administrative management (e.g., email, procurement, account data, executed contracts, receipts, inter-office memoranda, Intranet web pages) except that for which there is for specific reason to classify as Tier 2 or Tier 3. • Disaster preparedness, national security, military, government benefits, regulatory oversight, critical infrastructure and key assets management and other information where the information is not of the type not classified as Tier 2 or Tier 3. • Training materials • Marketing or promotional information (prior to authorized release) • Information related to other general government administrative or program activities (e.g. government asset sales information, government customer service information, legislative relations, and central personnel management or government property management information) that are not otherwise classified by a government unit with a national defence, intelligence or information security mission or a major program where unauthorized disclosure of the information could result in the loss of life or serious threat of injury, requiring a higher level of restrictiveness (Tier 2 or 3). • Intra-agency workplace policy development and management information (e.g., dress codes, time reporting requirements, etc.)

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
			<ul style="list-style-type: none"> • Accounting Information, description: related to assets, liabilities, fund balances, revenues and expenses associated with government funds and expenditures (e.g., payments, disbursements, salaries and expenses, operation and maintenance, procurement, working capital, trust funds) • Open data • Published government documents (e.g., marketing or promotional information, annual reports, published research, transcripts of public meetings, hearings, legislative testimony, legislative sessions, legislative records, administrative orders, speeches) • Published program or product descriptions • Public cryptographic keys • Internet web pages • Catalogues • Job vacancy notices

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
Official	Moderate to High	Accredited public cloud	<p><i>(Potential User: All government agencies)</i></p> <ul style="list-style-type: none"> • Personally identifying information about individuals (e.g., email address, name (first and last), phone number, street address, real-time geo-location, fax number, IP address social security numbers or other government issued identifiers, government financial identifiers). • Human Resources Management (e.g., HR strategy, staff acquisition management, organization and position management, compensation, benefits, employee performance, employee relations, labor relations, and separation management, HR development) except that which is for specific reasons classified as Tier 3. • Personal profile information (i.e., user name and password pairs, facial recognition and biometric markers, complete geo-location tracking data). • Aggregated financial or market data • Organizational and operational support, with not limited to: <ul style="list-style-type: none"> ○ Passwords and PIN codes, private cryptographic keys, VPN tokens ○ Credit and debit card numbers ○ Vendor bank account numbers and payment instructions ○ Employee HR Records ○ Internal telephone directories ○ Shared calendars and other such collaborative software solutions ○ Draft request proposals ○ Employee disciplinary reports ○ Government benefits 'entitlement event' information ○ Service level agreements

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
			<ul style="list-style-type: none"> • Law-, regulation- and policy-making information, deliberative information prior to authorized publication is typically classified as Tier 2 (such as unedited internal commentary or discussion) as premature disclosure carries risks of disruption to the law- or policy-making process (e.g., inappropriate influence of special interests, loss of confidence in the process). Once law or policy information is published for public comment or the law, regulation or policy is promulgated, the information that is made public would be classified as Public. So too, the deliberative information may be reclassified. • Protected legal or health information (i.e. attorney-client privileged, doctor-patient privileged medical records, genetic information). • Trade secret and confidential material business information (e.g., pricing, merger/acquisition information, marketing plan, proprietary processes, marketing plans, new product designs, proprietary processes), where the public disclosure of which would not be expected to cause severe or catastrophic legal, financial or reputational damage. • Intellectual property information (e.g., enforcement of copyright, patent, trademark and trade secret). Certain intellectual property assets may be related to weapons or weapon systems and would be classified with national security information.

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
Secret and above	Moderate to High	Accredited public cloud/hybrid/cloud/tightly-controlled public cloud	<ul style="list-style-type: none"> • National security and defense information (e.g. information describing technological countermeasures to chemical, biological, radiological and nuclear threats, terrorist threats, laboratory testing on new and promising devices and basic and applied science that can lead to new countermeasure). <i>Potential user: Coordinating Minister of Politics, Law and Security; Defense Ministry; Military; Police.</i> • Government intelligence information (<i>potential user: Coordinating Minister of Politics, Law and Security; Intelligence Agency; Military Intelligence; Police Intelligence</i>) • Law enforcement information related to an ongoing criminal or terrorist investigation (<i>potential user: Coordinating Minister of Politics, Law and Security; Police; Anti-terrorism task force</i>) • Government program monitoring or oversight investigations information, description: <ul style="list-style-type: none"> ○ Where public confidence consequences may potentially be severe or catastrophic, such as in the case of a ministry that has a national defense, intelligence or information security mission, and integrity, confidentiality or accessibility is of high sensitivity. ○ Where an oversight investigation of a major program related to human safety is at issue and there is a risk to human life or loss of major assets • Security management information related to the physical protection of an organization's personnel, assets and facilities, including security clearance management, with conditions:

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
			<ul style="list-style-type: none"> ○ Where there is a reasonable expectation of threat to life such as government aircraft, key government facilities and critical infrastructure (e.g., legislative and government executive offices, law enforcement facilities, nuclear power plants, dams where there is a risk of potential physical threat such as a bomb or assassination opportunity); ○ Where criminals could use information associated with physical security to gain access to government facilities to perpetrate a major crime (e.g., extraction of inmates from detention facilities, theft of commodities market projections, theft of blank licensing materials, access to currency printing facilities). <p><i>(Potential User: Coordinating Minister of Politics, Law and Security; Defense Minister; Military; Police; Secret Service)</i></p> <ul style="list-style-type: none"> ● Foreign policy and diplomatic relations information including the operation of embassies, consulates and ongoing membership in international organizations, the development of treaties and agreements and conflict resolution stemming from inter- and intra-state disagreements <i>(Potential User: Coordinating Minister of Politics, Law and Security; Foreign Affairs Minister,)</i> ● Global Trade Information including activities associated with the importing and exporting of goods to and from the country; e.g., export promotion, tariffs, legal enforcement, with conditions: <ul style="list-style-type: none"> ○ Unauthorized disclosure of export promotion processes may have an adverse result on the success of the process, posing a severe or catastrophic threat to an agency's mission capability.

Data Classification	System Security Categorization	Cloud Deployment Model Options	Examples of Governments Related Work
			<ul style="list-style-type: none"> ○ Similarly, information that supports tariffs/quotas monitoring process might include intelligence information with regard to a dumping situation. Further, the requirement for adequate means to detect corruption is high; therefore the integrity impact level for such information is high. ○ Unauthorized disclosure, modification or destruction of merchandise inspection information can be expected to have a severe or catastrophic impact on the ability of the agency to determine, report and record the discovered illegal status of imported or exported merchandise. ● Highly sensitive trade secret, intellectual property rights and material confidential business information e.g., government’s responsibility to keep, protect or store private sectors’; certain pricing, merger/acquisition information, marketing plan, proprietary processes, marketing plans, new product designs, inventions prior to a patent application or held as trade secret; the public disclosure of which could be expected to cause severe or catastrophic legal, financial or reputational damage to the business (<i>Potential User: Coordinating Minister of Economic Affairs; Investment Coordinating Board; Trade Minister; Minister of Law and Human Rights</i>) ● Government payment and benefits information where payment activities are a part of an agency’s service mission (e.g. payment of benefits) and integrity compromise or failure of payment could be life-threatening (<i>Potential User: Coordinating Minister of Economic Affairs; Finance Minister; State Apparatus Minister</i>) ● Taxation management information for which the unauthorized disclosure could impede anti-terrorism or other national security activities or endanger the lives of government agents or informants (<i>potential user: Coordinating Minister of Economic Affairs; Finance Minister</i>)

Module 3:

Starting your Cloud Journey

Introduces key principles for government agencies to keep in mind when starting their cloud journey.

Starting your Cloud Journey

Many government organizations want to move to the cloud, but understandably struggle when it comes to *how* to move to the cloud. A core benefit of cloud computing is the broad range of standardized services that can be used to build a unique IT environment. But with such a broad feature set to choose from, and many new concepts and roles and responsibilities to understand, it can be confusing to know which cloud migration path to take. Therefore, high-level policy guidance in the form of a cloud migration roadmap can help government organizations get started on the right path to cloud adoption.

There is no one-size-fits-all way to move to the cloud. However, an overall cloud strategy providing direction on important considerations around migration goals, hybrid vs all cloud architecture, connectivity, multi-cloud vs single cloud, criteria for prioritization of applications or workloads for migration and how to adopt key features of the cloud business model (pay-as-you-go for example) could be provided at the policy level to drive clarity on cloud adoption. The overall cloud strategy could further be supported by a cloud migration roadmap or plan, to help ensure agency or departmental cloud plans are aligned to key migration operational activities.⁴ Cloud migration roadmap patterns that have become apparent in the last decade include:

1. Look to **development and test** workloads as a learning path to cloud adoption.
2. Use cloud for **entirely new applications**. Building new applications on the cloud provides all of the advantages of cloud right from the get-go. There are no legacy concerns or hindrances, and no need for migration plans.
3. As cloud skills and maturity develops, look to **moving websites** and digital properties, analytics, and mobile applications to the cloud.
4. Move **business-critical applications** to the cloud, and ensure that the cloud is leveraged for its enhanced Disaster Recovery capabilities.
5. **Migrate entire data centers** to the cloud and go **'all-in.'** Thinking long term, cloud adoption plans should consider whether there will be a need for a data centers that are coming up for lease in 6/12/18 months, or others that will require a significant technology refresh. Can these workloads be moved to, or built on, the cloud instead? And can all future development and workloads be Cloud-Native?

⁴ For example, see AWS Migration Whitepaper, March 2018 <https://d1.awsstatic.com/whitepapers/Migration/aws-migration-whitepaper.pdf> and Migrating to AWS: Best Practices and Strategies <https://d1.awsstatic.com/Migration/migrating-to-aws-ebook.pdf>

Cloud migration roadmaps can also provide a checklist of operational activities when moving to the cloud. Examples of which include business strategy, governance and identity, process changes, architecture considerations, organizational maturity (from IT professionals to contracting/legal/finance), cultural changes, and new roles and responsibilities, to name just a few. Some policy-level migration roadmap considerations include:

1. **Get cloud migration buy-in from key departmental stakeholders.** A key element of a successful cloud strategy is the education and involvement of all key stakeholders (procurement, legal, budget/finance, security, IT, and business leadership) at an early stage. This ensures that there is a clear understanding and support of how cloud adoption will influence existing practices.
2. **Clearly define the scope and business case for cloud migration.** The business case should detail tangible benefits of moving to the cloud, so that leadership and IT staff understand how they can optimize value from the investments made in cloud computing. Communicate how new approaches to IT procurement and management can get the full benefits of adopting the scalability, lower costs, and innovative nature of cloud technology. Use financial and strategic analysis techniques to define the expected results of each state of the cloud migration, and the capabilities of the target cloud platform—in-line with current readiness and strategic goals. Determine how existing applications and environments will evolve for cloud adoption and whether existing technology systems and services will be leveraged in a hybrid environment, or instead replaced.
3. **Plan for cultural change.** Build understanding of the positive cultural changes and new skill-sets that come with cloud computing. Review and update operations and employee skills to accommodate the change in practices that come with a cloud migration. This includes ensuring that a government organization (or a partner) has the experience necessary to move workloads and applications to the cloud, and training/certifying staff en masse for the required cloud skills.
4. **Evaluate and audit the current environment and applications.** Understand your on-premises environment, determine what physical and virtual servers exist, and what applications are running on those servers—to help develop a strategic approach for each group of applications. This action provides the required data for project planning and cost estimation. Manually performing such discovery can take weeks or months to perform, so we recommend taking advantage of automated discovery tools. Also, capture information on the existing governance, risk management, and security/compliance processes to determine how much change is needed across the organization.

5. **Cloud cost analysis and Total Cost of Ownership (TCO) review:** Calculate and compare the projected costs of upcoming IT initiatives as both CapEx (on-premises) and OpEx (cloud) options. Compare the projected costs of both planned and new IT initiatives over 1, 3, 5 years (or whichever timeframe is appropriate for the initiative). Take into account the costs that come with initial migration efforts (such as SI or managed services engagements) and how overall IT costs will normalize in the longer term. Also factor-in cloud optimization options, such as utilizing serverless options.
6. **Migration planning.** The primary objective of the migration plan is to lead the overall migration effort. This includes how to manage the scope, schedule, resource plan, issues and risks, coordination, and communication to all stakeholders. Working on the plan early can organize the project as multiple teams migrate multiple applications. The migration plan considers critical factors such as the migration order for workloads, when resources may be needed, cost, and tracking the overall progress of the migration.
7. **Technical planning.** Planning a migration goes beyond cost, schedule, and scope. It includes taking the application and data analysis from auditing existing environments and workloads (see step 4 above), and building an initial plan of prioritized applications and workloads to move to the cloud. Use the cloud for dev and test to become familiar with the features available, and develop future architectures and Proof of Concepts (POCs) to aid the execution of a streamlined migration.
8. **Security planning.** Develop strategies for building a secure landing zone for all applications that are ready to move to the cloud, taking into account; network security (VPC), identity and access management, logging and monitoring, infrastructure security, data protection, incident response, resilience, compliance validation, secure continuous integration/continuous deployment (CI/CD), configuration and vulnerability analysis, and security big data analytics.
9. **Standardize and Share Reference Architectures and Templates.** Build a library of standard architectures and use cases that can be shared among multiple applications within an organization (or even between agencies). This provides efficiency and faster compliance with standards, and reduces the time and effort spent in designing architectures for new applications on the cloud. This can include building standardized security and account models to help enforce account governance. Also, look to promote automation throughout.
10. **Create Cloud Service Metrics.** Define suitable metrics to track the progress of cloud adoption and capture the effectiveness of migration processes and activities. Monitor cloud assets to ensure that a desired level of usage, spend, and performance is being reached. Gain an understanding of CSP tools available to track and predict usage and spend at a granular level, and how to use usage/spend alerts to help enforce budgetary governance.

11. **Establishing a Cloud Centre of Excellence (CCoE) or Cloud Program Office (CPO)** is often an effective way to address the different considerations discussed above. A cross-functional cloud focused team spanning representatives from policy, legal, audit, security, procurement, finance, human resources and technology can help bring focus, establish an overall strategy, engage experts, drive consensus decisions, and help

institutionalize best practices. The same team could also be the catalyst for culture change across government, and could run early POCs to validate and convince skeptics on common concerns. The CCoE can start out small with a 5-6 core empowered members focused on policy issues and the overall cloud strategy, and can scale / evolve as the discussion moves to operational issues.

Module 4: CSP Accreditation

Introduces the best practices for creating a cloud services provider (CSP) accreditation guideline.



Creating an Accreditation Guideline

Governments should use existing domestic and international cloud-centric accreditation systems to evaluate CSPs (rather than create their own unique certification programs). The accreditation process should include baseline security assurance requirements to ensure basic levels of service reliability from CSPs, and to assure that they have secure and controlled platforms providing the necessary array of security features which government agencies can use.

An example of baseline security assurance requirements is included in the table below:

Requirements	Baseline Certification and/or Protocol Required	Description
Security Assurance Requirements	<ul style="list-style-type: none">• ISO/IEC 27001 - Information Security Management• Payment Card Industry (PCI) Data Security Standard (DSS)• <i>Optional: Service Organization Control (SOC) 1 and 2</i>• <i>Optional: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</i>	These Security Assurance Requirements ensure that Cloud Service Providers have the necessary security certifications to host government workloads.

Where government customers find the need to add requirements to existing security baselines, they should ensure that the requirements:

- Clearly articulate the risk analysis that justifies modification of the requirements baseline and existing requirements do not provide similar protection.
- Accept alternative measures or compensating controls that demonstrate security equivalency.
- Focus on security capabilities and outcomes instead of specific implementations that will be outdated or ineffective with advancements in cloud technology.

Individual sectors may also have specific certifications required. These should be considered in tandem with the baseline certifications required, depending on the government agency's requirements. For example, US Health departments require compliance to the US Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH).

Appendix 1: Sample Cloud Accreditation



Government
Ministry "Owner"
Typically
overseeing ICT

Step 1

Cloud Service Provider (CSP) applies to government ministry overseeing information, communications, and technology for accreditation, providing relevant documentary proof of baseline security and encryption certifications.

Step 2

Upon successful verification of baseline certifications, the ICT ministry (or relevant government agency) awards accreditation (valid for 2 years) to the CSP



Accreditation

Baseline security requirements:

1. ISO/IEC27001 – Information Security Management
2. Payment Card Industry (PCI) Data Security Standards (DSS)
3. All data at rest or in transit should be encrypted.*

*Accepted encryption algorithms include:

- AES (128 bits and higher)
- TDES (minimum double-length keys)
- RSA (1024 bits or higher)
- ECC (160 bits or higher)

Module 5: Cloud Procurement

Explains the differences between traditional IT procurement and cloud procurement.



Cloud Procurement

Cloud procurement is unlike traditional technology purchasing. Entities in the public sector are accustomed to buying IT infrastructure using procurement approaches and policies designed for purchase of technology products such as hardware and software, and human services such as consulting and maintenance services. However, such traditional procurement and contracting approaches inhibit customer ability to adopt cloud services. Cloud procurement presents an opportunity to re-evaluate existing procurement strategies – including procurement policies – in order to create a flexible procurement process that enables public sector organizations to extract the full benefits of the cloud.

Hyperscale cloud services providers are able to provide massive economies of scale, which generate efficiencies and cost-savings. This allows CSPs to invest in industry-leading security and technology at a scale and cost than any individual customer could. Services are highly scalable and provided on a one to many basis, which means the services operate the same way for all customers. As a result, services and products cannot be customized for individual customers. Importantly, CSP terms and conditions are designed to reflect these unique characteristics of the cloud computing model. Therefore, it's imperative that a CSP's terms and conditions are incorporated and utilized to the fullest extent practicable.

To create a flexible procurement process suitable for cloud procurement, policy makers should consider a) the key differences between traditional IT procurement and cloud procurement, and the implications for procurement policy; b) leverage industry best practices to provide direction to buying agencies; and c) evaluate and select the procurement model that works best in their local context.

Key Differences between Traditional IT Procurement and Cloud Procurement

There are five key factors that differentiate Cloud Procurement from Traditional IT procurement emanating from the fundamental characteristics of the commercial cloud business model.

Table 1: Key Differences between Traditional IT Procurement and Cloud Procurement

Differentiating Factor	Traditional IT Procurement	Cloud Procurement
Requirements	Highly prescriptive requirements, sourcing end-to-end solution.	Performance-based requirements, sourcing building blocks, rapid innovation.
Budget/ price	Known capacity, fixed price or fixed catalog, fixed term contract.	On-demand, consumption-based, pay-as-you-go.
Contract Terms & Conditions	Terms & Conditions focused on hardware/software.	Cloud service-provider Terms & Conditions. Standard SLAs.
Governance	Process-heavy approval/intake process, centralized control.	Self-service, distributed control with governance.
Security & Audit	Security Assurance and Audit	Shared Responsibility and third-party certifications/attestations.

Leverage Industry Best Practices to Provide Direction to Buying Agencies

1. **Performance Based Requirements:**

Customers should focus on performance-based solutions, SLAs, and terms and conditions that prioritize workloads and outcomes, as opposed to traditional “prescriptive” procurement requirements that specify what the underlying infrastructure stack should consist of (and traditionally focus on contractual means to mitigate risk, rather than looking to technical means).

2. **Embrace Pay-as-You-Go Pricing:** Realizing the benefits of cloud computing requires thinking beyond the commonly accepted approach of fixed-price contracting and product line items. Instead, we advise a focus on building a dynamic spending model for the on-demand, utility-style, pay-as-you-go nature of cloud computing. To contract for the cloud in a manner that accounts for fluctuating demand, government customers need a contract that lets them pay for services as they are consumed. CSP pricing should be:

- Offered via a pay-as-you-go utility model, where at the end of each month customers simply pay for their usage.
- Allowed the flexibility to fluctuate based on market pricing so that customers can take advantage of the dynamic and competitive nature of cloud pricing.
- Offered with capabilities to help monitor and control spend, with CSP reporting, monitoring, and forecasting tools that allow customers to (1) monitor usage and spend at both summary and granular levels, (2) set up

alerts to be notified when usage and spend hit custom thresholds, and (3) estimate usage and spend in order to plan future cloud budgets.

Also, CSPs should be allowed to offer different pricing models as this enables government customers to evaluate each pricing model against the requirements of their solicitations (eg. scenario based pricing), as opposed to an arbitrary “apples to apples” pricing comparison through compute or storage units since these may not be the same across CSPs. CSPs should provide transparent, publicly available, up-to-date pricing, and tools that allow customers to evaluate their pricing.

3. **Incorporate CSP Contract Terms and Conditions:**

A CSP’s unique terms and conditions are integral to realizing the benefits of the cloud, as utility-type cloud services have value in operating at a massive scale, driving innovation and cost efficiencies. Government customers should allow for evolving terms and conditions in order to benefit from dynamic service enhancements that are prevalent to cloud technology. Unnecessary restrictions or change consent requirements can limit the ability to both scale and take advantage of frequent innovative service changes. Ultimately, creating terms that are static or specific to a singular type of technology will not allow for flexibility or scalability in such a restrictive procurement environment. Cloud is a dynamic and fast moving technology, and contracts that lock down future cloud services will need to be renegotiated/recreated on a regular basis.

4. **Leverage Industry Best Practices for Security & Assurance/ Audit:** There are two key areas in procurement that need to be considered when it comes to security:

- Leveraging industry best practices regarding security, privacy, and auditing provides assurance that effective physical and logical security controls are in place, preventing overly burdensome processes or approval workflows that may not be justified by real risk and compliance needs.
- As cloud computing customers are building systems on top of cloud infrastructure, the security and compliance responsibilities are shared between service providers and cloud consumers. In the cloud computing shared responsibility model, customers control how they architect and secure their applications and data put on the infrastructure, while CSPs are responsible for providing services on a highly secure and controlled infrastructure and for providing a wide array of additional security features. Procurement policies and the approach to solicitations need to take this into consideration.

5. **Agile Governance:** There are four elements to consider when it comes to cloud governance: 1) cloud customers should retain full control and ownership over their data; 2) they should have the ability to choose the geographic location(s) in which to store their data; 3) they should be able to utilize CSP identity and access controls available to restrict access to customer infrastructure and data; and 4) cloud customers should build a governance model for managing and using cloud within their agency.

As an example regarding this final point of cloud governance, buying cloud off a traditional product list can reduce the benefits of cloud. Cloud is typically used in an agile DevOps type model where the end user is constantly changing and streamlining the architecture. This means giving end users the ability to access all services, while also building controls using CSP provided Identity and Access Management (IAM) and other tools so that end users comply with internal security and spending practices.

6. **Shared Responsibility:** The shared responsibility model is mostly used when discussing security and compliance in the cloud, but this delineation of responsibilities applies to all aspects of cloud computing. A Cloud First policy can help inform as to what is within a CSP's remit in a cloud environment, and what will remain a customer responsibility. From this, government organizations can further understand how a CSP's partner network of consulting and technology companies can help the customer utilize the cloud and manage their responsibilities. Simply put, the responsibilities in the cloud model are:

- A CSP Provides Cloud Services
- A Government Customer Utilizes Cloud Services
- Partners (if needed) Help the Government Customer Access and Utilize Cloud Services

Governments should understand the models of how CSPs provide their offerings and recognize that partners providing consulting, managed services, reselling and much more are critical to the process. Procurements should be built to take these partners into account.

7. **CSP Evaluation:** Evaluating CSPs and writing evaluation criteria can often be challenging for customers, especially while trying to ensure that 'true' cloud providers qualify. To ensure CSPs are not inappropriately excluded by evaluation criteria: Pre-qualification should be aligned with compliance requirements based on global industry standards; technical

evaluation should be on the basis of depth & breadth of services, architectural support available, self-service, availability of tools for billing, monitoring, cost optimization etc; and commercial evaluation should be on the basis of scenario pricing or total cost of ownership over the usable life of the service.

Evaluate and select the procurement model & contract vehicle that works best in their local context

Policy makers can consider one of the following three cloud procurement models:

1. Buy cloud services directly from the CSP using terms designed for a commercially available service and purchased as a commercial item service offered without labor hours.
2. Buy indirectly from CSP partner or reseller negotiating a customized agreement with that organization.
3. Buy cloud services directly from the CSP but have a CSP partner provide billing and manage the cloud services.

When evaluating which model to employ, policy makers (and buying agencies) need to consider the cloud skills they have available within the government sector (or the specific agency) and to what extent they would want to develop them in the future; whether the users would buy cloud services -or will they buy solutions; are they able to consume pay-as-you-go; and if there is flexibility in accepting the CSP's commercial and legal terms.

Once the policy makers have selected the procurement model that works best within the context of their environment, there are usually a few contract vehicle types to choose from, which could be direct or indirect:

1. **Issue a Solution/ Project Procurement:** This is the closest to procuring traditional IT solutions, except that requirements are written for cloud.
2. **Leverage Existing Contract Vehicles:** As the adoption rate of cloud computing grows, many public sector entities have established approved publicly awarded contract vehicles to purchase cloud services. Taking advantage of existing contracts will help accelerate deployment. Alternatively, CSP partners could potentially have existing contract vehicles or customer relationships. Reseller programs enable qualified partners to resell cloud services to both commercial and public sector end customers, through these contracts.
3. **Create 'Whole-of-Government' Procurement Frameworks:** One of the best opportunities for effective public sector procurement of cloud services is through Whole-of-Government procurement frameworks that enable a multi-organizational award of cloud contracts, from which eligible purchasers affiliated with the purchasing organization can efficiently acquire cloud solutions that meet their needs. A well-designed cloud ready framework should adopt the best practices described in the section above and can benefit both the participating organizations and vendors through standardization, better alignment to XaaS models, simplification of the buying process, and reduced costs through efficiency gains and volume aggregation.

Such frameworks can take many forms and may be known as Schedules; Term Contracts; Government-Wide Acquisition Contracts (GWACs); Information and Communication Technologies (ICT) schemes; and Indefinite Delivery/Indefinite Quantity (ID/IQ) vehicles among others. It should be noted however that these frameworks, if not designed specifically or adapted for cloud, can prevent customers from taking full advantage of the benefits from cloud. Alternatively, in the simplest form the framework can also be a direct purchase from CSPs basis of their standard contracts.

While addressing the procurement topic and developing a procurement approach that works best for the local context can look daunting, developing an in-depth understanding of cloud business models and procurement best practices is the important starting point. The understanding and learnings can be operationalized by a Cloud Centre of Excellence (CCoE) or a Cloud Program Office comprising of a cross-functional team including representatives from policy, legal, procurement, finance, audit, business and technology.

Sample Cloud First Policy

A template for creating Cloud First Policy based on global best practices.



Sample Cloud First Policy

The Highlighted Terms in brackets refer to the following:

[Country] refers to the country in which the policy is being issued

[Quasi-Governmental Entities] refers to additional quasi-governmental institutions to be included such as government-owned corporations, state-owned enterprises, etc.

[Government Agency] refers to the government agency issuing the Cloud First Policy

Section 1: General Policy

Goal

The **[Country]** Government is committed to reducing the cost of government information and communication technologies (ICT) by eliminating duplication and fragmentation, and will lead by example in using cloud computing services to reduce costs, increase productivity, and develop excellent citizen services.

Cloud First Policy

In light of the benefits the cloud brings, this cloud first policy is aimed at accelerating cloud adoption within government. In order to increase cloud adoption, all government agencies shall:

1. Include cloud a part of their strategic ICT plans and budgets
2. Utilize cloud for all new projects and workloads
3. Consider cloud first while migrating/upgrading existing applications/infrastructure

Agency Implementation

All Departments, National Government Agencies and **[Quasi-Governmental Entities]**, including State Universities and Colleges (SUCs), should adopt cloud computing as the preferred ICT deployment strategy for their own administrative use and delivery of government services in accordance with the above, except

1. when it can be shown that an alternative ICT deployment strategy meets special requirements of a government agency and
2. when it can be shown that an alternative ICT deployment strategy is more cost effective from a Total Cost of Ownership (TCO) perspective,⁵ and demonstrates at least the same level of security assurance that a cloud computing deployment offers.

⁵ **Total cost of ownership (TCO)** is a comprehensive assessment of information technology (IT) or other costs across the organization over time. For IT, TCO includes hardware and software acquisition, management and support, communications, end-user expenses and the opportunity cost of downtime, training and other productivity losses. See also Annex B.

Cloud Computing Benefits

1. **Spur innovation** – Cloud computing allows government customers to access industry-shaping technology quickly, at an affordable cost, no matter what the scale. A successful Cloud First policy results in leading-edge IT environments that spur invention and innovation.
2. **Inter-agency collaboration for greater efficiency and better citizen services** – Cloud enables more effective collaboration as agencies more easily share resources across institutions, allowing for greater efficiency, entrepreneurship, and creativity in delivering public services.
3. **Faster deployment of services** – reducing the amounts of ICT infrastructure required to be built and owned by government agencies reduces overall deployment times, and shifts the focus from management of infrastructure to delivery of services. Public ICT facilities and services can be tested and deployed quicker, and maintained more cost effectively, than if government agencies own and run unique computing facilities themselves.
4. **New security models** – Governments can obtain greater security in the cloud than is available in traditional data centers. The cloud enables customers to formalize account design, automate security and governance controls, and streamline auditing.
5. **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.
6. **Greater budget control** – A utility-based 'pay for what you use' model means that government agencies can purchase as much or as little resource as they need, as they need it. Cloud scalability results in systems usage being dialed up or down throughout the year as it is required. Transparency of the utility-based pricing structure means that spending caps and alerts can be implemented to further assist in budget control.
7. **Decreased spending on legacy infrastructure** – Deploying government services in cloud infrastructure results in immediate reductions of large capital outlays for ICT infrastructure and maintenance costs. Best of class services are made available to government agencies through cloud provisioning.
8. **Efficiency and sustainability** – Cloud computing helps governments meet and exceed efficiency and carbon reduction targets. The cloud allows for the avoidance of over-provisioning workloads, thereby reducing resource consumption because these workloads resize to the demand load.

Section 2: Definition of Terms

This section covers a number of key concepts associated with cloud computing.

What is Cloud Computing?

Cloud computing is 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. This cloud model is composed of five essential characteristics, five deployment models, and certain assurances.

Essential Characteristics⁶

On-demand self-service. Government agencies can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g. mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to agency demand. There is a sense of location independence in that the government agency generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g. country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the agency, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer (i.e., the government agency) of the utilized service.

⁶ Based upon US Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication 800-145, Sep 2011, Definition of Cloud Computing <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

Section 3: Data Classifications

Classifying data into discrete categories enables the [Country] Government to better protect government information and make better-informed decisions with regard to access, storing and transmission of Government data. Data classifications achieve stronger outcomes for government agencies by clarifying the safeguards required for protecting different types of data, thereby reducing uncertainty, standardizing access, and reducing costs. It also enables business and other public sector agencies to be able to better use and manage appropriately classified data.

Data can be broadly divided into three tiers of Public Sector Data Classification:

- **Tier 1: Unclassified data**, which can be stored on accredited public cloud
- **Tier 2: Official data**, which can be stored on accredited public cloud with encryption requirements;
- **Tier 3: Secret and above**, which may require private (on premise) cloud deployment with specific encryption requirements.

Government agencies are recommended to select the appropriate cloud deployment model according to an agency's specific needs, and the type of data it handles according to the Public Sector Data Classification, as illustrated in the table below. Depending on the classification of the agency's data, there will be a requirement to apply certain controls. Agencies may find that these controls are addressed by a public cloud provider or that they may only be serviced by a private cloud delivered on-premise.

Public Sector Data Classification	Suggested Cloud Deployment Model	Data Examples	MC78 Correspondence
Tier 1: Unclassified	Can be stored on accredited public cloud.	Open Data, publicly available information including informational websites, terminology systems, standards, practitioner registries	<ul style="list-style-type: none"> • Non-sensitive Matters
Tier 2: Official	Can be stored on accredited public cloud or Virtual Private Cloud and meets a higher set of security standards and encryption protocols than compared with Tier 1 data, at agency discretion. Must have encryption to deal with restricted data.	Restricted matters, business data, email, and CRM systems. Examples include financial records and medical records such as personally identifiable education records, personally identifiable financial information (PIFI), protected health information	<ul style="list-style-type: none"> • Restricted Matters
Tier 3: Secret and above	Confidential data may be stored on VPC, community cloud or require a private cloud deployment to achieve the compliance required for sensitive data, at agency discretion. Must have encryption.	Political documents dealing with matters of international negotiations, technical matters of military value, major governmental projects such as proposals to adjust the nation's economy (before official publication) internal audit data, trade secrets, technical data supporting technology transfer agreements	<ul style="list-style-type: none"> • Confidential Matters, • Secret Matters, • Top Secret Matters

This work has been further developed in a specific Data Classification paper and agencies should refer to that paper for further detail.

Section 4: Security

The benefit of migrating government workloads and data onto to public cloud is the ability to enhance overall data security. Accredited CSPs will meet international security standards, will be certified appropriately, and will abide by all relevant [Country] laws and industry standards.

Government agencies will be expected to develop a security framework applying a risk management approach towards their own data control requirements (see **Data Classification**), and align this with internationally recognized standards and certifications, as well as [Country] industry standards. The precise baseline level of security requirements for contracted cloud services is laid out in the Security Framework section below. Stipulated security controls can include any one or more of the following:

- Personnel security
- Physical and environmental security
- Business continuity management and incidence response
- Inventory and configuration management
- Data encryption
- Access controls, monitoring and logging
- Network security and monitoring
- System security and integrity.

Shared Responsibility Security Framework

Managing the security of contracted cloud services is a responsibility that is shared between the contracting agency and the cloud service provider, with the contracting agency responsible for selecting and implementing security controls for any workloads that it operates in the cloud, while the cloud service provider is responsible for ensuring that the services used by the contracting agency are highly secure and resilient so they are available to use on demand.

Data security of the public cloud depends upon:

1. Meeting security requirements for each data classification level; and
2. Employing standardized tools and procedures for audit.

Data that can be migrated to the public cloud will need to meet security requirements for accreditation, and be verified by internationally recognized security assurance frameworks. Accepted international security assurance controls include ISO 27001, Service Organization Controls Report (SOC) 1 and 2, and the Payment Card Industry Data Security Standard (PCI DSS). Data will be encrypted using industry-tested and accepted standards and algorithms, such as AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits or higher), ECC (160 bits or higher), and ElGamal (1024 bits or higher).

The table below outlines the baseline (i.e. required) and optional (i.e. agency discretion applied) security controls that to be applied to classified government data, and which accredited CSPs must have met to be permitted to host classified government data.

Security Controls	Baseline Certification and/or Protocol Required	Description
Security Assurance Requirements	<ul style="list-style-type: none"> • ISO/IEC 27001 - Information Security Management • Payment Card Industry (PCI) Data Security Standard (DSS) • <i>Optional: Service Organization Control (SOC) 1 and 2</i> • <i>Optional: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</i> 	<p>These are the baseline and <i>optional</i> Security Assurance Requirements for Cloud Service Providers to be accredited.</p> <p>These Security Assurance Requirements ensure that Cloud Service Providers have the necessary security certifications to host government workloads.</p>
Encryption Requirements	<ul style="list-style-type: none"> • AES (128 bits and higher) • TDES (minimum double-length keys) • RSA (1024 bits or higher) • ECC (160 bits or higher) 	<p>These are the baseline Encryption Requirements for Government Workloads before being deployed on an accredited. Note that while Cloud Service Providers can provide services with such Encryption technologies built in, these technologies can also be deployed by Government Agencies on such Workloads.</p> <p>These Encryption Requirements ensure that workloads on any of the accredited Providers is encrypted with the minimum baseline required by Philippine Government.</p>

In addition to the above outlined baseline and optional security controls, Government cloud service providers should provide logical security audit on data access, including logs and audit trails to ensure the prescribed security and privacy requirements are met. Government agencies should rely on logical audits and continuous security monitoring to ensure cloud services meet the agreed-upon data confidentiality and integrity, that there have been no data breaches, and that data and workloads are continuously available.

Data Residency

The benefits of cloud are best realized when there are no data residency restrictions placed on data. Data residency restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure. Nevertheless, where agencies have concerns with extraterritorial access to Tier 3 Secret and Above are involved, then the appropriate security standards and controls should be employed or the agency should work with [Government Agency] to consider deploying a private, on-premise cloud solution.

Section 6: Migration Policy

Migrating data and workloads to the cloud enhances the availability and functionality of services, and improves interoperability with a wider range of other government data and workloads. Migration to cloud also enables greater automation of certain processes, increasing the availability and agility of computing resources for processes that have variable processing demands.

Migration can be seen as a three-step process:



1. Take stock

- Define objectives
- Identify resources and value drivers
- Determine data classifications
- Map security considerations



2. Plan

- Define responsibilities and reporting lines
- Identify skills gaps
- Determine data sharing and permissions
- Choose suitable cloud environment
- Create roadmap



3. Migrate and manage

- Migrate data and test workloads
- Track, document and analyze performance against objectives
- Iterate on cloud strategy

1. Take Stock

Identify how IT resources are aligned to objectives, and how costs are optimized. Take stock of entity data classifications and the corresponding security considerations. Non-sensitive workloads and those that pose low security concerns should be prioritized for migration first. Government websites, public archives, development and testing environments, are more readily moved to the cloud.

The value of moving workloads to the cloud is determined by the technology lifecycle and the increased functionality that cloud can bring. Moving workloads from IT resources that are near the end of their current technology lifecycle can avoid costly investments in new IT resources.

2. Plan

Create a roadmap for migrating service to the cloud, including defining responsibilities and reporting lines. Migrating workloads to the cloud can change the skills needed within the organization, for example by requiring more developers and engineers, and fewer people concerned with managing IT infrastructure. This means working with cloud providers to understand the staff skills, training and education needed in the migration and post-migration workloads.

- Identify data that can be shared, and would benefit from being shared, and requirements on security and access permissions for such data.
- Identify the suitable cloud environment, such as virtualization of legacy IT, performance and functionality requirements, costs, and compatibility with legacy IT.
- Determine whether replacing existing applications with new ones or to redesign service delivery architecture from the bottom-up is preferred.

Contracted cloud services should be able to integrate with existing services and should be interoperable with locally provisioned IT. They should be contracted on an aggregated basis to meet planned data and workload migration needs.

3. Migrate and Manage

Track, document and analyze progress of the plan in an iterative manner. Monitor performance and service delivery against objectives, and compare costs against the migration plan.

Following migration, adequate testing of the cloud environment needs to be performed before existing solutions are decommissioned. Testing should be performed on the basis of both typical/normal usage scenarios and extraordinary utilization/demand scenarios.

Ensure that staff are trained in the contracting and management of cloud services through service level agreements (SLAs) with cloud vendors and possess the requisite skills to manage the migrated workloads.

Section 7: Data Ownership, Retrieval, and Interoperability

Data Ownership

Government institutions will retain full control and ownership over their data, with CSP identity and access controls available to restrict access to customer infrastructure and data. CSPs should provide customers with a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity.

Ownership

Service contracts related to provisioning of cloud services for Government agencies shall clearly provide that any data migrated to the cloud remains the property of the contracting Government entity, regardless of who owns, manages or operates the cloud. The contracting agency will retain rights of data access, retrieval, modification and deletion regardless of the physical location of the cloud services, including the right to approve, deny and revoke access by third parties.

Access

Access, retrieval, modification and deletion of data remains the right of the contracting Government agency and will be reflected in the relevant service contracts. The policies and processes pertaining to data access will be defined according to the needs of the contracting entity and specified in the agreement between the Government agency and the cloud provider.

Interoperability

A major benefit of cloud computing as compared to traditional IT infrastructure is that customers have the flexibility to avoid traditional vendor lock-in, and CSPs should allow customers to move data on and off their cloud platforms as needed.

A cloud system's components may come from different sources including public and private cloud implementations. These components should be replaceable by new or different components from different providers and continue to work, to facilitate the exchange of data between systems. CSPs are required to provide interoperability, ensuring government agencies may be able to change CSPs easily without a lengthy procurement and implementation cycle.

Open Data

Globally, governments are increasingly making their non-restricted data available for the public to discover, access, and use. These open data initiatives facilitate the development of public services, fuel entrepreneurship, accelerate research and scientific discovery, and create efficiencies across multiple sectors.

Government entities should endorse the open data principle and, where technically feasible and economically reasonable, make non-restricted data available to other Government agencies and the public through the cloud. In keeping with this principle and Policy, Government agencies should likewise manage their data assets to promote openness and use for the public good.

Section 8: Accreditation Process for CSPs

Baseline Security Controls

In order to provide a higher degree of assurance to agencies looking to deploy on public cloud, [Government Agency] provides a list of baseline certifications required to be accredited. Agencies should look to selecting a CSP with these baseline Security Assurances which match their functional requirements.

Requirements	Baseline Certification and/or Protocol Required	Description
Security Assurance Requirements	<ul style="list-style-type: none">• ISO/IEC 27001 - Information Security Management• Payment Card Industry (PCI) Data Security Standard (DSS)• <i>Optional: Service Organization Control (SOC) 1 and 2</i>• <i>Optional: ISO/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors</i>	These baseline and <i>optional</i> Security Assurance Requirements ensure that Cloud Service Providers have the necessary security certifications to host government workloads.

Further information on these baseline Security Assurances will be provided by DICT.

Technical and Sector-Specific Certifications

Individual sectors may also have specific certifications required. These should be considered in tandem with the baseline certifications required, depending on the government agency's requirements. For example, US Health departments require compliance to the US Health Insurance Portability and Accountability Act (HIPAA), and the Health Information Technology for Economic and Clinical Health (HITECH). Refer to the Annex for a sample list of sectoral and technical accreditations.

Conclusion

The [Country] Government recognizes [Country] citizens expect government services to be available, effective, and responsive to its communities, when and where required. Key to realizing such a vision is the effective use of ICT by government, and in today's environment that means both embracing and leading with the adoption of cloud computing services. The availability of cloud services provides an opportunity for government to deliver services more broadly, more efficiently, and more cost effectively, as well as providing services that are more responsive to business and community needs.

This policy document has been developed to help drive a greater take up of cloud services by government agencies through promoting a 'cloud first' approach. The paper has provided the approaches and the tools necessary for government agencies to be able to confidently get started on the cloud, identifying what to look for, what steps to take in which order, and the resources available.

