وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Cloud Security Policy

Version: 1.3

Author: Cyber Security Policy and Standards

Document Classification: Public

Published Date: June 2018

Document History:

Version	Description	Date
1.0	Published V1.0 Document	March 2013
1.1	Branding Changed (ICTQATAR to MoTC)	April 2016
1.2	Mandatory questions identified	June 2017
1.3	Format Changed + MoTC Logo changed	June 2018

CONTENTS

1. Legal Mandate(s)

Emiri decision No. (8) for the year 2016 sets the mandate for the Ministry of Transport and Communication (hereinafter referred to as "MOTC") provides that MOTC has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter "ICT") in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual's life and community and build knowledge-based society and digital economy.

Article (22) of Emiri Decision No. 8 of 2016 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

This guideline has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

2. Introduction

Cloud computing offers a lot of potential benefits to public and government bodies, including scalability, elasticity, high performance, less administration headaches together with cost efficiency, agility, flexibility, faster time to market and new innovation opportunities.

Understanding, managing and controlling the risks mainly affecting confidentiality, security and resiliency related to the adoption is what this document trying to achieve.

Traditionally, managing security and resilience in traditional IT environments is very challenging for government agencies. Cloud computing presents some additional challenges.

For example:

- Lack of clear definitions pertaining cloud and its associated services and different architectures
- Lack of cloud security certification and standards and incomplete compatibility with currently adopted security standards
- Lack of a clear procurement language and methodology for choosing the most appropriate cloud service.
- Lack of a clear understanding on the implications introduced by cloud computing pertaining data cross-border movement
- Ensuring compliance with national laws and regulations.

And most importantly how we can digest the shift in the balance of responsibility and accountability for key functions such as governance and control over data and IT operations, and, in some instances, the quality and the availability of internet connectivity which is crucial for the service.

The purpose of this policy is to provide an overview of cloud computing and the security and privacy challenges involved. The document discusses the threats, technology risks, and safeguards for cloud environments, and aspires to provide the insight needed to make ICT decision makers take informed decisions by providing tools such as a detailed questionnaire that can be used to assess and evaluate the cloud service provider (CSP) offerings.

3. Definitions

- **Agencies**: Include government ministries, agencies and other public sector organizations in Qatar
- **Advanced Virtualization**: when the virtual ICT infrastructure has automated management capabilities
- **Application as a Service (AaaS):** see SaaS
- **Cloud:** a term used for global networks, originally used to reference the telephone network now commonly used as a reference to the internet
- **Cloud Broker:** an entity that creates and maintains relationships with multiple cloud service providers. It acts as a liaison between cloud service providers and cloud service customers. A cloud broker has not cloud resources of its own
- **Cloud Bursting**: is a technique used by Hybrid Clouds (See Hybrid Clouds) to provide additional resources to private clouds if needed. If the workload exceeds the private cloud's capacity a hybrid cloud automatically allocated additional resources through this technique
- **Cloud computer services:** see section 4.2
- **Cloud operating system**: an operating system that is specially designed to run in a cloud infrastructure and delivered to the user over the network.
- **Cloud Oriented Architecture**: An IT architecture that is fully compatible with cloud based components
- **Cloud Portability**: the ability to move applications and data from one cloud provider to another (Related to Vendor-lock in)
- **Cloud Service Provider**: (CSP) An entity (Private of Public) that provides cloud based platforms, infrastructure, application, security or storage services another entity/organization. Usually for a fee.
- **Cloud Services:** see 4.2
- **Cloud Service Architecture (CSA)**: an architecture in which applications act as services on the internet
- **Cloud Storage:** a service that allows the customers to save data by transferring it over the internet/WAN to another storage system managed by a third party
- **Cloud sourcing**: using a cloud service instead of a traditional IT service such as outsourcing storage
- **Cloud networking**: connecting multiple clouds computing environments
- **Cloud-ware**: software that enables creating, deploying, running or managing applications in the cloud

- **Community cloud:** see 4.3
- **Customer self-service**: a feature that allows the cloud customers to deploy, manage and terminate services themselves without involving the service provider
- **Classification labels:**
    - **Unclassified, Public or no Label:** Public Information
    - **Internal**: for State Agency internal use; material whose disclosure would cause light to moderate damage to the affected party
    - **Limited Access**: access for defined users, roles or user groups; material whose disclosure would cause serious damage to the affected party
    - **Restricted**: Confidential information with access limited to a very small set if persons; materials whose disclosure would cause severe damage to the affected party
- **Federation**: the act of combining data or identities across multiple platforms, federation can be managed by a cloud service provider or by a cloud broker
- **Governance**: the controls and practices and processes that make sure policies are enforced
- **Grid Computing**: is applying the resources if many computers in a network to a single problem at the same time
- **G.C.C:** Gulf Cooperation Council is a political and economic union of the Arab states bordering the Arabian gulf and located on or near the Arabian Peninsula, namely Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and United Arab Emirates.
- **Hardware or Infrastructure as a Service (Iaas):** see IaaS
- **Hosted Application**: an internet based or web based application that runs remotely
- **Internal Cloud**: a type of private cloud who services are provided by an IT department to those in its own organization
- **Location independent resource pooling:** Resource pooling that allows a cloud provider to assign resources (physical and Virtual) to a customer, those resources are location independent
- **Middle ware:** software that sits between applications and operating systems, usually consisting of services that enable and support operating in distributed architecture, as an example, the data on one database can be accessed through another data base on a different platform
- **MoTC:** Ministry of Transport and Communications
- **NIAP:** National Information Assurance Policy is a complete set of security controls issued by CS/QCERT the security division of MoTC.

- **Platform as a service (PaaS):** see 4.3
- **Qatar Computer Emergency Response Team (Q-CERT):** is an MoTC initiative that is concerned with the issues of cyber security
- **RACI (Responsible, Accountable, Consulted, and Informed) Matrix:** A common model used to define roles and responsibilities for members of cross-functional initiatives. The matrix allows members to easily understand which groups are responsible and accountable for activities and which must be consulted or informed.
- **Software as a Service (SaaS):** see 4.3
- **Cloud Service Provider**: an entity that provides cloud services
- **Service Level Agreement (SLA):** a contractual agreement between a service provider and a consumer (A state Agency), where the consumer requirements are specified and the service provider states the level of service responsibilities and guarantees regarding availability, performance and support levels.
- **Vendor Lock-in**: dependency on a particular vendor (cloud service provider) and the difficulty moving from one cloud service provider to another.
- **Virtual Machine (VM):** a file typically (called an Image) that when executed appears to the user as an actual machine. The VM can be started or stopped as needed, changes made to the VM while it is running can be stored to disk to make them persistent (definition source: *NIST*)
- **Virtualization:** the simulation of the software and or hardware upon which other software can run.
- **Virtual Private Cloud (VPC):** a private cloud that exists within a shared or public cloud

4. What Is Cloud Computing

Cloud Computing: is an ICT sourcing and delivery model for enabling 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.

Cloud Computing is composed of five essential characteristics, three service models, and four deployment models.

Cloud Infrastructure: is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, the abstraction layer consists of the software deployed across the physical layer.

4.1. Cloud Computing Characteristics:

- *On-demand self-service.* The consumer can provision multiple computing capabilities as needed. The provisioning can be entirely online.
- *Broad network access.* The services are available over the network and access is supported through multiple platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Resource pooling*. The cloud service provider computing resources are pooled to serve multiple consumers at the same time, the consumers can be from anywhere in the world. Examples of resources include storage, processing, memory, and network bandwidth.
- *Scalability*. Cloud resources can be easily provisioned and released. To the consumer, the resources available for provisioning may appear to be unlimited and can be appropriated in any quantity at any time.
- *Measured service*. Cloud systems automatically control and optimize resource use. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer.

4.2. Cloud Computing Service Models

- *Software as a Service (SaaS).* This model offers the state agency the facility to use the Cloud service provider's applications running on a cloud infrastructure. The software applications are accessible online via a web interface or via desktop application. The consumer has no control over the underlying hardware configuration.

- *Platform as a Service (PaaS).* This model offers the state agency the facility to deploy or install onto the cloud infrastructure a state agency-created or acquired application with the condition that the application is created using programming languages, libraries, services, and tools supported by the cloud service provider. The consumer has no control over the underlying hardware configuration, storage, network, operating system or management layers.

- *Infrastructure as a Service (IaaS).* This model offers the state agency the facility to utilize processing, storage, networks, and other computing resources where the consumer is able to install and run any software, which may include operating systems and applications. The state agency does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications.

4.3. Deployment Models:

- *Private cloud.* The cloud infrastructure is commissioned for exclusive use by a single organization/state agency comprising multiple consumers (e.g., different departments). 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. Also may exist in or outside the country.

- *Community cloud.* The cloud infrastructure is commissioned for exclusive use by a specific community/sector of consumers from organizations that have shared nature of work and obligations (e.g., same mission, ICT security requirements, legal, and sector specific compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. Also may exist in or outside the country. (e.g., Qatari Government Network).

- *Public cloud.* The cloud infrastructure is commissioned for open use by any organization. It may be owned, managed, and operated by a private or public organizations or a combination of them. It exists on the premises of the cloud service provider.

- *Hybrid cloud.* The cloud infrastructure is a composition of two or more different cloud infrastructures (private, community, or public) that remain separate entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., load balancing between clouds).

The following table summarizes the key concepts of sections 4.2 and 4.3

	Infrastructure Managed* by	Infrastructure Owned by	Infrastructure Location	Accessible and consumed by
Public	3rd party provider	3rd party provider	Off-site	Anyone
Private/Community	Organization or 3rd party provider	Organization or 3rd party provider	On-site or Off-site	Trusted**
Hybrid	Organization AND 3rd party provider	Organization AND 3rd party provider	Both on-site and off-site	Trusted and Untrusted

*Management Includes: governance, operations, security, compliance…etc.

**Trusted consumers: are those considered part of the organization legally

4.4. Why a Qatari Cloud Security Policy is required

Over the years the ICT organizations and ICT professionals in Qatar became well aware of the risks, governance practices and legal requirements that came with traditional IT desktop based environments. But due to the unique architecture and cross border locality nature of cloud services the privacy and security requirements for personal information (Qatar's information privacy and protection draft Law) and security requirements for government data (National Information Assurance Policies), transactions and communication must be addressed with a different perspective.

5. Potential Risks in Cloud Computing

Depending upon the cloud model of choice, an understanding and mitigation of the following risks will be required:

Issue	Explanation
Application Design	• Lesser customization, this may lead to increased complexities when integrating with existing legacy systems. • Some applications that require real time data access (Like some Data base applications) might need to be revisited to accommodate network latency in order to avoid I/O errors. • Some software licensing models may need revisiting to accommodate cloud deployments.
Architecture	• Before taking the decision to move to a cloud environment, the state agency must assess the impact on business processes to avoid any technical barriers.
Business Continuity	• Applications/services that did not previously require network access to function properly will be impacted by a loss of internet and/or WAN Business Continuity and disaster recovery plans must be thoroughly revisited and documented to accommodate the new architecture.
Data Location	• Due to the dynamic nature of the cloud, the state agency might not be fully aware about where its information actually resides at any given point in time.
Funding	• Due to the payment model of some cloud services, the ICT capital budgeting might need to be re-planned as operating expenses (OPEX) instead of capital expenses (CAPEX).

	• Some software licensing models may need revisiting to accommodate cloud deployments.
Legal and Regulatory	• State agency must have the capability/assurance to find and access its information at any time. • State agencies must be aware of all the Qatari legislations and regulatory requirements including but not limited to the NIAP, the Telecom Law (34) of 2006 and the Data protection and Privacy Law
SLAs	• State agencies need to ensure that the agreed service levels are achieved. State agencies should ensure that written SLAs are in place with CSPs.
Privacy and Reputation	• State agencies must be aware of the risks associated with any possible compromise to government or personal information through 3rd party accessing the information. • State agencies must be aware that if a data breach occurred this shall negatively affect the organization's reputation and may even extend the damage to the government as a whole.
Human Capital	• Moving to cloud architecture will mean less demand for hardware support and product specific systems administrators and a higher demand for system architects, program managers, security and privacy officers, data analysts, app designers and developers.
Security	• State agencies should be aware that they remain responsible for the security of the information even while residing with a cloud service provider. • State agencies should consider the portability of data in case of cloud service provider failure. Financial viability of the CSP should be a

	consideration to reduce the changes of CSP's financial failure. • State agencies should ensure that they have contracts in place with the CSP describing security controls.
Standards	• State agencies must thoroughly investigate the cloud service provider compliance certifications with special attention to the scope and validity of the certification.

6. Agency responsibility vis-à-vis the different cloud models

Depending on the cloud model of choice an Agency subscribing to an IaaS service may retain complete control of, and therefore be responsible for, the on-going security and maintenance of all operating systems, applications, virtual configurations (including the hypervisor and virtual security appliances), and data. In this scenario, the **CSP** would be responsible for maintaining the underlying physical network and computing hardware.

The following diagram illustrates how an Agency's responsibility may vary according to the cloud model

Example of how scope and responsibility may differ* by type of cloud service:

Cloud customer responsibility	
Cloud service provider responsibility	

	Type of Cloud Service		
Area of Responsibility	IAAS	PAAS	SAAS
Data			
Software, user applications			
Operating systems, databases			
Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc)			
Computer and network hardware (processor, memory, storage, cabling, etc.)			
Data center (physical facility)			

Source: PCI-DSS Virtualization guidelines, 2011

7. Key adoption drivers

Cloud computing introduces a lot of appealing features and capabilities that can be considered as adoption drivers for State Agencies

Driver	Benefit
Value for Money	• Reduces duplication and cost through consolidation, resources pooling and sharing • Allow for "controlled" payment available through the model "pay as you go" • Energy Saving and environment preservation • Less ICT management headaches allowing the State Agency to focus on core objectives and process improvements
Flexibility	• Fast service provisioning and deployment and on demand scalability
Operational Support	• High availability and around the clock professional Support
Security	• A cloud is a more uniform and homogeneous platform that allows automation of security management (such as vulnerability testing, audits, update management) and consistent enforcement of best practices. • Cloud platforms are designed and run for availability. • Use of enterprise grade cloud systems can also enhance security. Large, mature and enterprise grade cloud vendors have invested in sophisticated systems, process and people resources that can provide world class security. • The scale of operation enhances security and reduces costs to build and manage

	in the Cloud compared to agency implementation on an individual basis. • Because of their size and scale, large and mature CSPs can afford to hire specialized staff that might be uneconomical for individual agencies.
Agility	• Because of the scale and the resources that are pooled and shared in the Cloud, as provided by the CSP (be it a partner or an agency), new innovation scenarios are possible at a fraction of the cost of individual disparate implementations.

8. Scope and Application

This document applies to all State Agencies in the Qatari government that use or are planning to use cloud-computing services. This document can also be considered as a security *guide* to the entire ICT sector in the state of Qatar.

9. Policy Statements

9.1.

The Qatari Government state agencies may choose a local or a **G.C.C** based cloud services IF they demonstrate compliance with the security requirements stated in this document. Qatari Government state agencies SHALL not use a CSP that lies outside the legal jurisdiction or geographical boundaries of the state of Qatar and the **G.C.C**. unless the service entitlements comply with the information privacy and protection laws, NIAP (specifically with the data classification policy) and other applicable governing laws and regulations.

10. Cloud Security POLICY

10.1. Policy Objective

The objective of this policy is to make sure that the provisioning of a cloud service is in accordance with the business and security requirements and relevant laws and regulations.

10.2. Policy & Baseline Controls

10.2.1. Cloud computing security policy document	Each Agency's cloud computing security policy document SHALL be approved by senior management, and published and communicated to all employees and relevant external parties either as part of the organization's information security policy or as a separate policy. The policy should set the goals and objectives governing the cloud computing service.
10.2.2. Security program leadership	The senior management responsible for the cloud computing security policy SHALL be identified by name, title, business phone, business address and date of designation. Changes to the senior management MUST be documented within thirty (30) calendar days of the effective date of the change.
10.2.3. Review of the security policy	The security policy SHALL be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. For example: Architectural changes, service model changes, service upgrades or changing the CSP.
10.2.4. Completion and Submission of the Cloud Security Controls Questionnaire	The State Agency SHALL not sign an agreement with a CSP prior to the completion and passing of all the *mandatory* controls in the (**CSP Assessment Questionnaire**) (See Appendix A)
10.2.5. CSP Vetting	The state agency SHALL ensure that the CSP has passed all the necessary security requirements as assessed by an independent auditor.

11. Agile Delivery

11.1. Policy objective

One of the foundations and main features of cloud computing is agile delivery; it refers to the rapid and fast improvements and upgrades and changes that can be applied to cloud products and services. This reduced/shorter delivery time means less time to complete a proper risk evaluation and assessment of security implications.

11.2. Policy & Baseline Controls

11.2.1. Updates and releases	The State Agency SHALL agree appropriate update and release cycles affecting the security features with the CSP that the State Agency teams (Such as: Security, Continuity, legal and governance…etc.)
11.2.2. CSP agile risk Management practices	The State Agency SHALL request and assess the detailed information on how the CSP ensures and applies agile and rapid yet comprehensive risk management prior to contracting the CSP.
11.2.3. Risk Management Optimization	The State Agency SHALL optimize its risk management processes and tools to accommodate iterative and agile cloud deployments
11.2.4. CSP controls checking methodology	The State Agency SHALL ask and validate the CSP's risk control checking methodology or ensure that information security policy conforms with international best practices

12. Virtualization

12.1. Policy objective

In cloud computing, the majority of logical separation controls are not physical (i.e., separate servers). Instead, separation is enforced through logical system and application controls designed to help ensure data segmentation and integrity across the platform. One common mechanism for providing this separation of data and services is "virtualization."

12.2. Policy & Baseline Controls

12.2.1. CSP Hardening guides and policies	The State Agency SHALL assess the CSP virtualization hardening guides and policies and evaluate the 3rd party gap assessment against virtualization security standards like **NIST SP800-125.** This includes but not limited to: • Disable or remove all unnecessary interfaces, ports, devices and services; • Securely configure all virtual network interfaces and storage areas; • Establish limits on VM resource usage; • Ensure all operating systems and applications running inside the virtual machine are also hardened; • Validate the integrity of the cryptographic key-management operations; • Harden individual VM virtual hardware and containers;
12.2.2. Snap-Shots Security	The State Agency SHALL ensure that the CSP has the controls in place to guarantee that only authorized snapshots are taken, and that these snapshots' level of classification and storage location and encryption is compatible in strength with the production virtualization environment. (*Additional references on data classification is available in the NIA policies*)

12.2.3. Hypervisor Security	The State Agency SHALL ensure the following controls are applied: • State Agency has access to the Hypervisor administrative access logs; • Hypervisor complete Logging is enabled.
12.2.4. Client Image Support	The State Agency SHALL ensure that the CSP supports the use of trusted VMs provided by the State Agency, those VMs were made in compliance with the hardening guidelines in the NIAP
12.2.5. CSP vendor list	CSP shall provide the State Agency with its complete vendor list that will l have access to the State Agency data; at any point throughout the duration of the agreement. The CSP should also update the agency with any change in the vendor list.

13. Identity and Log Management

13.1. Policy objective

A seamless and secure identity management is an essential component of cloud computing, from a business, usability and security perspective.

While Log management (who has access to the logs?), is another management issue that must be addressed and agreed upon in advance.

13.2. Policy & Baseline Controls

13.2.1. Federated Identity	The State Agency SHOULD adopt identity federated standards such as SAML or openID and use that for users CSP authentication
13.2.2. Active Directory Authentication	The State Agency SHALL NOT grant the CSP permissions to directly use/access the organization authentication environment such as the organization's main directory
13.2.3. Multi-Factor Authentication	The State Agency SHALL ensure that the CSP support Several Multi-Factor authentication mechanisms, such as tokens, OTA one time passwords , biometrics…etc.
13.2.4. CSP Identity Management	The State Agency SHALL choose a CSP that allows State Agency control in managing its own identities, (including Staff Identity creation and deletion/termination)
13.2.5. Identity Regulatory Requirements	The State Agency SHALL ensure that the CSPs authentication process, access control, accountability and logging (Format, retention and Access) meet the Agency regulatory and legal requirements
13.2.6. Log Monitoring	State Agencies SHALL train their IT staff on accessing and using the CSP log services
13.2.7. Logging level and retention	State Agencies SHALL ensure logging is enabled for all security events (covering sessions and transaction information) for a period not less than 90 days

14. Web Application Security

14.1. Policy objective

Application security is absolutely critical in cloud computing. The Cloud is typically an open environment, and CSPs are exposing an increasing number of web interfaces and APIs to the Internet — far more than traditional closed on premises solutions, significantly increasing the application attack exposure.

14.2. Policy & Baseline Controls

14.2.1. CSP security team	The State Agency SHALL have the following information at hand: i. The location and time of access of the CSP security team
14.2.2. Application security	The State Agency SHALL ensure that the CSP Applies: i. Application layer firewalls ii. Secure code reviews are executed (if possible)prior to provisioning any application release iii. Secure web development best practices like OWASP secure development guides iv. OS and Applications security hardening best practices v. Periodic Penetration testing and that a remediation program is defined, and it includes fixing the vulnerabilities based on priority. All vulnerabilities should be prioritized and must be fixed and patched within SLAs agreed upon by the State Agency and the CSP. vi. A proper software development life cycle (SDLC) and that security is an integrated part in at least the following phases: • Planning and requirements gathering • Architecture and functional Design phase

	• Coding • Testing • Maintenance

15. Disaster Recovery

15.1. Policy objective

Data protection controls need to be maintained to ensure high availability and resilience of the data

15.2. Policy & Baseline Controls

15.2.1. Change management and Incident response	The State Agency SHALL ensure that the CSP adopt and is in compliance with change management and incident response procedures as specified in (ITIL)
15.2.2. DRP	The State Agency SHALL review the CSP DR plan and ensure it matches the state agency requirements, such as: i. Has the ability to retrieve and restore data following data loss incidents ii. CSP to provide the Agency at least annually with the DR testing reports the reports should be comprehensive, covering from the exercise scope till the final outcome and recommendations iii. Ensure the DR solution is capable of maintaining the same levels of security measures and controls utilized in the normal operation mode iv. Ensure that the DR solution is also owned and managed entirely by the Contracted CSP
15.2.3. Compliance	CSPs who are certified BS25999 or ISO 22301 are RECOMMENDED

16. E-discovery and Forensics

16.1. Policy objective

State Agencies may be requested to extract specific data to share it with a third party as part of a legal action or to support an on-going investigation, this is already a challenging task for data stored in-house and certainly poses a greater challenge when the data is stored by a CSP.

16.2. Policy & Baseline Controls

16.2.1. Data Originality	The State Agency SHALL determine if its obliged to provide "the original on the original hard disk/tape" or a copy would be sufficient i. If the "Original" copy is legally required then this should be communicated and stated in the contract with the CSP ii. If a "copy" with acceptable chain of custody is accepted, the chain of custody "pre-requisites" should be communicated an stated in the contract with the CSP
16.2.2. E-Discovery SLAs	The State Agency SHALL ensure that e-discovery costs and forensics requirements including cost and response times are detailed in the contract

17. Multi-tenant Platforms

17.1. Policy objective

Cloud computing challenges the traditional concepts on data segmentation and separation, the objective of this policy is to make sure that this is incorporated into the risk, security and audit programs.

17.2. Policy & Baseline Controls

17.2.1. Data segmentation	The State Agency SHALL document and regularly update/review the data-segmentation and separation controls at each of the four main layers at the CSP: (1) Network, (2) physical, (3) system and (4) application.
17.2.2. Assessing the data segmentation controls	The State Agency SHALL evaluate each of the Data segmentation controls at each layer, as well as the number and type of controls at each layer every 6 month and after major system changes and upgrades. Note: cloud data separation controls are typically weaker at the physical layer (as there is often no physical separation), requiring controls on the other three layers to be far stronger.
17.2.3. Data Labelling	The State Agency SHALL ensure that the CSP can meet the data labelling requirements of the NIAP.
17.2.4. Data Encryption	The State Agency SHALL ensure that data is encrypted at storage and in transit and in full compliance (at any given point in time) with NIAP and NIAP **Appendix B** for the government approved cryptographic algorithms and protocols.
17.2.5. Service Provider Supplied Encryption Keys	The State Agency SHALL ensure that they are using a unique set of encryption key(s). The unique encryption keys help protect data from being accessible in the event that it is inadvertently leaked from one CSP customer to another.

17.2.6. Software versus Hardware encryption keys	The State Agency SHOULD opt for Hardware encryption keys (Compliant with FIPS 140 2-3 and above) whenever supported.
17.2.7. Client Data Tagging	It is recommended that the State Agency ensure that the cloud service provider supports and can successfully demonstrate client data Meta-Tagging that is important for data segmentation and e-discovery.

18. Cloud Management

18.1. Policy objective

Moving data assets into the cloud may require significant realignment of client support departments. Roles and responsibilities often shift significantly when an organization begins using cloud services. For this reason, organizations must clearly define roles for managing cloud vendor relationships and service delivery.

18.2. Policy & Baseline Controls

18.2.1. Training and Awareness	The State Agency SHALL train its responsible staff on vendor management and cloud technologies.
18.2.2. Roles and Responsibilities	The State Agency SHALL define and document the different roles and responsibilities for the staff responsible for managing the cloud service. Example: legal, procurement, change management committee, business owners, security and risk.
18.2.3. RACI Matrix	The State Agency SHOULD create a RACI (Responsible, Accountable, Consulted, and Informed) matrix that includes the State Agency and the CSP to define accountability and obligations.
18.2.4. Escalation Tree	The State Agency SHALL develop a CSP escalation tree and disseminate it with the responsible team.

19. CSP Contractual requirements

19.1. Policy objective

Before moving a service out of an organization to any third party, a rigorous legal analysis and evaluation should be conducted.

19.2. Policy & Baseline Controls

19.2.1. Non-Disclosure Agreement	The State Agency SHALL sign an NDA (Appendix B) with the CSP before provisioning any service.
19.2.2. Data Ownership	The State Agency SHALL ensure that it retains the "Exclusive" right to data ownership throughout the duration of the agreement. The ownership includes all copies of data available with the CSP including backup media copies if any. State agencies should require that CSPs are not permitted to use state agencies' data for advertising or any other non-authorized secondary purpose.
19.2.3. Data Location	The State Agency SHALL "specify" in the contract the country(s) where it is acceptable for the data to be stored.
19.2.4. Legal Prevalence	The State Agency SHALL ensure that the CSP's own data privacy policy complies with the applicable laws in Qatar.
19.2.5. Data High Availability	• The State Agency SHALL ensure that SLAs reflect he applications and data high availability requirements (as per the State Agency's BIA or Business requirements) in the event of planned or unplanned disruptions or outages, with business continuity and disaster recovery planning and backup and redundancy mechanisms reviewed by the State Agency • SLAs should define financial remedies in the event of a business disruption.
19.2.6. Data Breach Notification	• The State Agency SHALL contractually ensures that they are "immediately" notified of any confirmed breach without any undue delay.

	• The State Agency SHALL contractually ensure that they are notified within 4 hours of any "Suspected" breach. From the time of breach discovery
19.2.7. Data Breach Penalty	The State Agency SHALL contractually state that the CSP will be responsible for any financial losses or penalties (up to the agreed Cap) that may occur due to a CSP breach
19.2.8. Right to be forgotten	The State Agency SHALL contractually state that the CSP will completely delete/eliminate any trace of Data/information at the end of the Agreement as agreed in the agreement.
19.2.9. Media destruction	State Agency SHALL contractually state and ensure that the CSP will comply with the data and media destruction and sanitization controls in the **NIAP**
19.2.10. Data Mobility	The State Agency SHALL ensure that the CSP supports the return of data to the State Agency. There should be no Vendor-lock In by the CSP.

20. General Recommendations to State Agencies

- State Agencies SHALL develop a roadmap to adopting and integrating cloud computing because of the complexity of the cloud environment that introduces a number of unknown variables for which government and public services will need to build new approaches to assess and manage the associated risks.
- It's RECOMMENDED not to assume that a successful deployment of an application in a cloud environment is automatically a positive indication for proceeding with many other deployments; the security and resilience requirements of each application should be examined carefully and individually.
- It's RECOMMENDED that State Agencies should always keep and maintain the capability of backtracking from the adoption of a cloud solution.

21. References:

1. National Information Assurance Policy (MoTC, April 2014)
2. Government Data Classification Policy (MoTC, April 2014)
3. Benefits, risks and recommendations for Cloud Computing information security (ENISA, November 2009)
4. Guidelines on security and privacy in public cloud computing (NIST, SP-800-144)
5. Security guidance for critical areas of focus in cloud computing (CSA V3.0)
6. Draft cloud computing synopsis and recommendations (NIST, SP-800-146)
7. FedRAMP security controls preface (DHS , 2012)
8. Cloud computing strategic direction paper (Australian Government , April 2011)
9. Hype Cycle for Cloud security (GARTNER, 2011)
10. The Enterprise Cloud (Shared Assessments, October 2010)
11. Security and Resilience in Government Clouds (ENISA, January 2011)
12. The NIST definitions of Cloud Computing (NIST, SP-800-145)

22. Appendix A (Contracted CSP Assessment QUeSTIONNAIRE)

The purpose of the assessment questionnaire is to act as a "guide" listing areas of concern and operational procedures that should be understood, evaluated during the CSP evaluation phase.

	Control Domain	CID	CSP Assessment Questions	Answer (Yes/No)	Reference
	(*) marks mandatory controls				
	Independent Audits	CO.01	*Do you allow customers to view your third party audit reports?		
		CO.02	*Do you conduct network penetration tests of your cloud service infrastructure regularly? If yes please elaborate on your test and remediation process		
		CO.03	*Do you conduct regular application penetration tests of your cloud infrastructure according to the industry best practices? If yes please elaborate on your test and remediation process.		
		CO.04	*Do you conduct internal audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.		
		CO.05	*Do you conduct external audits regularly according to the industry best practices? If yes please elaborate on your test and remediation process.		

		CO.06	Are the results of the network penetration tests available to customers at their request?		
		CO.07	*Are the results of internal and external audits available to customers at their request?		
	Third Party Audits	CO.08	Do you permit customers to perform independent vulnerability assessments?		
	Contact / Authority Maintenance	CO.9	Do you maintain updated liaisons and points of contact with local authorities? If yes then how frequently you validate the contacts?		
	Information System Regulatory Mapping	CO.10	*Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single customer only, without inadvertently accessing another customer's data?		
		CO.11	*Do you have capability to logically segment, isolate and recover data for a specific customer in the case of a failure or data loss?		
	Intellectual Property	CO.12	*Do you have policies and procedures in place describing what controls you have in place to protect customer's data marked as intellectual property?		
		CO.13	If utilization of customers services housed in the cloud is mined for cloud provider benefit, are the customers' defined IP rights preserved?		
		CO.14	If utilization of customers services housed in the cloud is mined for cloud provider benefit, do you provide		

			customers the ability to opt-out?		
INFORMATION GOVERNANCE	Ownership	IG.01	*Do you follow or support a structured data-labelling standard (ex. ISO 15489, Oasis XML Catalogue Specification, CSA data type guidance)? If yes please specify		
	Classification	IG.02	Do you provide a capability to identify virtual machines via policy tags/metadata?		
		IG.03	Do you provide a capability to identify hardware via policy tags/metadata/hardware tags?		
		IG.04	Do you have a capability to use system geographic location as an authentication factor?		
		IG.05	*Can you provide the physical location/geography of storage of a customer's data upon request?		
		IG.06	*Do you allow customers to define acceptable geographical locations for data routing or resource instantiation?		
	Handling / Labelling / Security Policy	IG.07	Do you consider all customer data to be "highly sensitive "and provide the same protection and controls across the board or you apply the controls according to the data specific classification or label?		
		IG.08	*Are mechanisms for label inheritance implemented for objects that act as aggregate containers for data?		

	Retention Policy	IG.09	*Do you have technical control capabilities to enforce customer data retention policies?		
		IG.10	*Do you have a documented procedure for responding to requests for customer data from governments or third parties?		
	Secure Disposal	IG.11	*Do you support secure deletion (ex. degaussing / cryptographic wiping) of archived data as determined by the customer?		
		IG.12	*Can you provide a published procedure for exiting the service arrangement, including assurance to sanitize all computing resources of customer data once a customer has exited your environment or has vacated a resource?		
	Nonproduction Data	IG.13	*Do you have procedures in place to ensure production data shall not be replicated or used in your test environments?		
	Information Leakage	IG.14	*Do you have controls in place to prevent data leakage or intentional/accidental compromise between customers in a multi-customer environment?		
		IG.15	Do you have a Data Loss Prevention (DLP) or extrusion prevention solution in place for all systems which interface with your cloud service offering?		

PHYSICAL ACCESS	Policy	PA.01	*Can you provide evidence that policies and procedures have been established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas?		
	User Access	PA.02	*Pursuant to local laws, regulations, ethics and contractual constraints are all employment candidates, contractors and third parties subject to background checks?		
	Controlled Access Points	PA.03	*Are physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) implemented?		
	Secure Area Authorization	PA.04	*Do you allow customers to specify which of your geographic locations their data is allowed to traverse into/out of (to address legal jurisdictional considerations based on where data is stored vs. accessed)?		
	Unauthorized Persons Entry	PA.05	*Are ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises monitored, controlled and isolated from data storage and process?		
	Offsite Authorization	PA.06	Do you provide customers with documentation that describes scenarios where data may be moved from one physical location to another? (ex. Offsite backups, business		

			continuity failovers, replication)		
	Offsite equipment	PA.07	Do you provide customers with documentation describing your policies and procedures governing asset management and repurposing of equipment?		
	Asset Management	PA.08	*Do you maintain a complete inventory of all of your critical assets?		
HR	Employment Agreements	HR.01	*Do you specifically train your employees regarding their role vs. the customer's role in providing information security controls?		
		HR.02	Do you document employee acknowledgment of training they have completed?		
	Employment Termination	HR.03	*Are Roles and responsibilities for following performing employment termination or change in employment procedures assigned, documented and communicated?		
INFORMATION SECURITY	Management Program	IS.01	*Do you provide customers with documentation describing your Information Security Management System (ISMS)?		
	Management Support / Involvement	IS.02	*Are policies in place to ensure executive and line management take formal action to support information security through clear		

			documented direction, commitment, explicit assignment and verification of assignment execution?		
	Policy	IS.03	Do your information security and privacy policies align with particular standards (ISO-27001, NIA, CoBIT, etc.)?		
		IS.04	Do you have agreements which ensure your providers adhere to your information security and privacy policies?		
		IS.05	*Can you provide evidence of due diligence mapping of your controls, architecture and processes to regulations and/or standards?		
	Baseline Requirements	IS.06	*Do you have documented information security baselines for every component of your infrastructure (ex. Hypervisors, operating systems, routers, DNS servers, etc.)?		
		IS.07	Do you have a capability to continuously monitor and report the compliance of your infrastructure against your information security baselines?		
		IS.08	*Do you allow your clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards?		
	Policy Reviews	IS.09	Do you notify your customers when you make material changes to your information security and/or privacy policies?		
		IS.10	*Is a formal disciplinary or sanction policy established for employees who have violated		

	Policy Enforcement		security policies and procedures?		
		IS.11	*Are employees made aware of what action might be taken in the event of a violation and stated as such in the policies and procedures?		
	User Access Policy	IS.12	*Do you have controls in place ensuring timely removal of access rights and permissions which is no longer required?		
		IS.13	*Do you provide metrics which track the speed with which you are able to remove access rights following a request from us?		
	User Access Restriction / Authorization	IS.14	*Do you document how you grant and approve access to customer data?		
		IS.15	Do you have a method of aligning provider and customer data classification methodologies for access control purposes?		
	User Access Revocation	IS.16	*Is timely de-provisioning, revocation or modification of user access to the organizations systems, information assets and data implemented upon any change in status of employees, contractors, customers, business partners or third parties?		
	User Access Reviews	IS.17	*Do you require at least annual certification of entitlements for all system users and administrators (exclusive of users maintained by your customers)?		

		IS.18	*If users are found to have inappropriate entitlements, are all remediation and certification actions recorded?		
		IS.19	Will you share user entitlement remediation and certification reports with your customers, if inappropriate access may have been allowed to customer data?		
	Training / Awareness	IS.20	*Do you provide or make available a formal security awareness training program for cloud-related access and data management issues (i.e., multi-tenancy, nationality, cloud delivery model segregation of duties implications, and conflicts of interest) for all persons with access to customer data?		
		IS.21	*Are administrators properly educated on their legal responsibilities with regard to security and data integrity?		
	Industry Knowledge / Benchmarking	IS.22	Do you participate in industry groups and professional associations related to information security?		
		IS.23	*Do you benchmark your security controls against industry standards?		
	Roles / Responsibilities	IS.24	Do you provide customers with a role definition document clarifying your administrative responsibilities vs. those of the customer?		
	Management Oversight	IS.25	Are Managers responsible for maintaining awareness of and complying with security policies, procedures and		

			standards that are relevant to their area of responsibility?		
	Segregation of Duties	IS.26	Do you provide customers with documentation on how you maintain segregation of duties within your cloud service offering?		
	User Responsibility	IS.27	*Is your staff made aware of their responsibilities for maintaining awareness and compliance with our published security policies, procedures, standards and applicable regulatory requirements?		
		IS.28	Are users made aware of their responsibilities for maintaining a safe and secure working environment?		
		IS.29	Are users made aware of their responsibilities for leaving unattended equipment in a secure manner?		
	Workspace	IS.30	*Do your data management policies and procedures address customer and service level security requirements?		
		IS.31	Do your data management policies and procedures include a tamper audit or software integrity function for unauthorized access to customer data?		
		IS.32	*Does the virtual machine management infrastructure include a tamper audit or software integrity function to detect changes to the build/configuration of the virtual machine?		

	Encryption	IS.33	*Do you have a capability to allow creation of unique encryption keys per customer?		
		IS.34	Do you support customer generated encryption keys or permit customers to encrypt data to an identity without access to a public key certificate. (e.g. Identity based encryption)?		
	Encryption Key Management	IS.35	*Do you encrypt customer data at rest (on disk/storage) within your environment?		
		IS.36	*Do you leverage encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances?		
		IS.37	Do you have a capability to manage encryption keys on behalf of customers?		
		IS.38	Do you maintain key management procedures?		
	Vulnerability / Patch Management	IS.39	*Do you conduct network-layer vulnerability scans regularly?		
		IS.40	*Do you conduct application-layer vulnerability scans regularly?		
		IS.41	*Do you conduct local operating system-layer vulnerability scans regularly?		
		IS.42	*Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?		

		IS.43	Will you provide your risk-based systems patching timeframes to your customers upon request?		
	Antivirus / Malicious Software	IS.44	Do you deploy multi anti-malware engines in your infrastructure?		
		IS.45	Do you ensure that security threat detection systems which use signatures, lists, or behavioural patterns are updated across all infrastructure components within industry accepted timeframes?		
	Incident Management	IS.46	*Do you have a documented security incident response plan?		
		IS.47	Do you integrate customized customer requirements into your security incident response plans?		
		IS.48	Do you have a CERT function (Computer Emergency Response Team)?		
		IS.49	Do you publish a roles and responsibilities document specifying what you vs. your customers are responsible for during security incidents?		
	Incident Reporting	IS.50	Does your security information and event management (SIEM) system merge data sources (app logs, firewall logs, IDS logs, physical access logs, etc.) for granular analysis and alerting?		
		IS.51	Does your logging and monitoring framework allow isolation of an incident to specific customers?		

	Incident Response Legal Preparation	IS.52	*Does your incident response plan comply with industry standards for legally admissible chain-of-custody management processes & controls?		
		IS.53	*Does your incident response capability include the use of legally admissible forensic data collection and analysis techniques?		
		IS.54	*Are you capable of supporting litigation holds (freeze of data from a specific point in time) for a specific customer without freezing other customer data?		
		IS.55	Do you enforce and attest to customer data separation when producing data in response to legal subpoenas?		
	Incident Response Metrics	IS.56	Do you monitor and quantify the types, volumes, and impacts on all information security incidents?		
		IS.57	Will you share statistical information security incident data with your customers upon request?		
	Acceptable Use	IS.58	Do you provide documentation regarding how you may utilize or access customer data and/or metadata?		
		IS.59	Do you collect or create metadata about customer data usage through the use of inspection technologies (search engines, etc.)?		
		IS.60	Do you allow customers to opt-out of having their		

			data/metadata accessed via inspection technologies?		
	Asset Returns	IS.61	*Are systems in place to monitor for privacy breaches and notify customers expeditiously if a privacy event may have impacted their data?		
		IS.62	*Is your Privacy Policy aligned with industry standards and Qatar's Law		
	e-Commerce Transactions	IS.63	Do you provide standard encryption methodologies (3DES, AES, etc.) to customers in order for them to protect their data if it is required to traverse public networks? (ex. the Internet)		
		IS.64	*Do you utilize standard encryption methodologies any time your infrastructure components need to communicate to each other over public networks (ex. Internet-based replication of data from one environment to another)?		
	Audit Tools Access	IS.65	Do you restrict, log, and monitor access to your information security management systems? (Ex. Hypervisors, firewalls, vulnerability scanners, network sniffers, APIs, etc.)		
	Diagnostic / Configuration Ports Access	IS.66	*Do you ensure hardening of admin workstations and Role Based Access Control to enforce the 'least privilege' principle		
	Network / Infrastructure Services	IS.67	Do you collect capacity and utilization data for all relevant components of your cloud service offering?		

		IS.68	Do you provide customers with capacity planning and utilization reports?		
	Portable / Mobile Devices	IS.69	*Do you allow mobile devises in your facility for administration purposes (e.g., tablets,)?		
	Source Code Access Restriction	IS.70	*Are controls in place to prevent unauthorized access to your application, program or object source code, and assure it is restricted to authorized personnel only?		
		IS.71	*Are controls in place to prevent unauthorized access to customer application, program or object source code, and assure it is restricted to authorized personnel only?		
	Utility Programs Access	IS.72	*Are utilities that can significantly manage virtualized partitions (ex. shutdown, clone, etc.) appropriately restricted and monitored?		
		IS.73	Do you have a capability to detect attacks which target the virtual infrastructure directly (ex. shimming, Blue Pill, Hyper jumping, etc.)?		
		IS.74	*Are attacks which target the virtual infrastructure prevented with technical controls?		
LEGAL	Nondisclosure Agreements	LG.01	*Are requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details identified,		

			documented and reviewed at planned intervals?		
	Third Party Agreements	LG.02	*Can you provide a list of current 3rd party organization that will have access to the customer's (My) data?		
OPERATIONS MANAGEMENT	Policy	OM.01	Are policies and procedures established and made available for all personnel to adequately support services operations roles?		
	Documentation	OM.02	Are Information system documentation (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure Configuring, installing, and operating the information system?		
	Capacity / Resource Planning	OM.03	Do you provide documentation regarding what levels of system (network, storage, memory, I/O, etc.) oversubscription you maintain and under what circumstances/scenarios?		
		OM.04	*Do you restrict use of the memory oversubscription capabilities present in the hypervisor?		

	Equipment Maintenance	OM.05	If using virtual infrastructure, does your cloud solution include hardware independent restore and recovery capabilities including offsite storage of backups?		
		OM.06	*If using virtual infrastructure, do you provide customers with a capability to restore a Virtual Machine to a previous state in time?		
		OM.07	*If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?		
		OM.08	*If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?		
		OM.09	Do you share reports on your backup/recovery exercise results?		
		OM.10	Does your cloud solution include software / provider independent restore and recovery capabilities?		
RISK MANAGEMENT	Program	RM.01	Is your organization insured by a 3rd party for losses?		
		RM.02	*Do your organization's service level agreements provide customer remuneration for losses they may incur due to outages or losses experienced within your infrastructure?		

	Assessments	RM.03	*Are formal risk assessments aligned with the enterprise-wide framework and performed at least annually, or at planned intervals, determining the likelihood and impact of all identified risks, using qualitative and quantitative methods?		
		RM.04	Is the likelihood and impact associated with inherent and residual risk determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance)?		
	Mitigation / Acceptance	RM.05	*Are risks mitigated to acceptable levels based on company-established criteria in accordance with reasonable resolution time frames?		
		RM.06	*Is remediation conducted at acceptable levels based on company-established criteria in accordance with reasonable time frames?		
	Business / Policy Change Impacts	RM.07	*Do risk assessment results include updates to security policies, procedures, standards and controls to ensure they remain relevant and effective?		
	Third Party Access				
		RM.08	Do you monitor service continuity with upstream internet providers in the event of provider failure?		
		RM.09	Do you have more than one provider for each service you depend on?		

		RM.10	Do you provide access to operational redundancy and continuity summaries which include the services on which you depend?		
		RM.11	Do you provide the customer the ability to declare a disaster?		
		RM.12	Do you provide a customer triggered failover option?		
		RM.13	*Do you share your business continuity and redundancy plans with your customers?		
SW DEPLOYMENT	New Development / Acquisition	SD.01	*Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?		
	Production Changes	SD.02	*Do you provide customers with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?		
	Quality Testing	SD.03	Do you provide your customers with documentation which describes your quality assurance process?		
	Outsourced Development	SD.04	*Do you have controls in place to ensure that standards of quality are being met for all software development?		
		SD.05	*Do you have controls in place to detect source code security defects for any outsourced		

			software development activities?		
	Unauthorized Software Installations	SD.06	*Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?		
	Impact Analysis	DR.01	Do you provide customers with on-going visibility and reporting into your operational Service Level Agreement (SLA) performance?		
		DR.02	Do you provide customers with on-going visibility and reporting into your SLA performance?		
	Business Continuity Planning	DR.03	Are you BS25999 or ISO 22301 certified?		
		DR.04	Do you provide customers with geographically resilient hosting options?		
	Business Continuity Testing	DR.05	*Are business continuity plans subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?		
	Environmental Risks	DR.06	*Is physical protection against damage from natural causes and disasters as well as deliberate attacks anticipated, designed and countermeasures applied?		
	Equipment Power Failures	DR.07	*Are Security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power		▪

			failures, network disruptions, etc.)?		
	Power / Telecommunications	DR.08	Do you provide customers with documentation showing the transport route of their data between your systems?		
		DR.09	Can customers define how their data is transported and through which legal jurisdiction?		
ARCHITECTURE	Customer Access Requirements	AR.01	Are all identified security, contractual and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets and information systems?		
		AR.02	Do you use open standards to delegate authentication capabilities to your customers?		
		AR.03	*Do you support identity federation standards (SAML, SPML, WS-Federation, etc.) as a means of authenticating/authorizing users?		
		AR.04	Do you have a Policy Enforcement Point capability (ex. XACML) to enforce regional legal and policy constraints on user access?		
		AR.05	Do you have an identity management system in place which enables both role-based and context-based entitlement to data (enables classification of data for a customer) if requested?		

		AR.06	*Do you provide customers with strong (multifactor) authentication options (digital certs, tokens, biometric, etc...) for user access?		
		AR.07	Do you allow customers to use third party identity assurance services?		
		AR.08	Do you utilize an automated source-code analysis tool to detect code security defects prior to production?		
		AR.09	*Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?		
	Data Integrity	AR.10	*Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?		
	Production / Nonproduction Environments	AR.11	*For your PaaS offering, do you provide customers with separate environments for production and test processes?		
		AR.12	For your IaaS offering, do you provide customers with guidance on how to create suitable production and test environments?		
	Remote User Multifactor Authentication	AR.13	*Is multi-factor authentication required for all remote user access?		

	Network Security	AR.14	For your IaaS offering, do you provide customers with guidance on how to create a layered security architecture equivalence using your virtualized solution?		
	Wireless Security	AR.15	*Are policies and procedures established and mechanisms implemented to protect network environment perimeter and configured to restrict unauthorized traffic?		
		AR.16	*Are policies and procedures established and mechanisms implemented to ensure proper security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings? (e.g., encryption keys, passwords, SNMP community strings, etc.)		
		AR.17	*Are policies and procedures established and mechanisms implemented to protect network environments and detect the presence of unauthorized (rogue) network devices for a timely disconnect from the network?		
	Shared Networks	AR.18	*Is access to systems with shared network infrastructure restricted to authorized personnel in accordance with security policies, procedures and standards. Networks shared with external entities shall have a documented plan detailing the compensating controls used to separate network traffic between organizations?		

	Clock Synchronization	AR.19	*Do you utilize a synchronized time-service protocol (ex. NTP) to ensure all systems have a common time reference?		
	Equipment Identification	AR.20	Is automated equipment identification used as a method of connection authentication to validate connection authentication integrity based on known equipment location?		
	Audit Logging / Intrusion Detection	AR.21	*Are file integrity (host) and network intrusion detection (IDS) tools implemented to help facilitate timely detection, investigation by root cause analysis and response to incidents?		
		AR.22	*Is Physical and logical user access to audit logs restricted to authorized personnel?		
		AR.23	*Can you provide evidence that due diligence mapping of currently applicable regulations and standards to your controls/architecture/processes has been done?		
	Mobile Code	AR.24	*Is mobile code tested (in terms of security) before its installation and use and the code configuration checked to ensure that the authorized mobile code operates according to a clearly defined security policy?		
		AR.25	*Is all unauthorized mobile code prevented from executing?		
The above questionnaire is primarily based on the CAI questions issued by the CSA. www.cloudsecurityalliance.org					

23. APPENDIX B (Non-Disclosure Agreement (NDA)) - Template

Note: The template below is valid in case of contracting a 3rd party Cloud service provider.

This Agreement dated XXX between YYY (hereinafter called "the **Owner**") and the Cloud service Provider (ZZZ) (hereinafter called "the **CSP**").

WHEREAS the Owner is in ownership and possession of certain confidential information (hereinafter called "the **Confidential Information**").

AND WHEREAS the Owner wishes to engage the CSP to provide cloud computing services or undertake cloud computing projects (hereinafter called "the **Purpose**") which may include disclosure of Confidential Information by Owner to the CSP in addition to other legal obligations.

NOW THEREFORE THIS AGREEMENT WITNESSETH that in consideration of the Owner disclosing the Confidential Information to the CSP and the mutual agreements and other good, valuable or nominal consideration, the receipt and sufficiency of which is hereby acknowledged, the CSP hereto undertakes and agrees with the Owner as follows:

1. DEFINITION

Agreement

Any reference herein to an Agreement means this Agreement which represents the entire understanding between the parties and supersedes all other agreements expresses or implied between the parties regarding disclosure of the Confidential Information.

The Confidential Information

In this Agreement, "the Confidential Information" means

Any information (whether written, oral, in electronic form or in any other media) that is disclosed in connection with the Purpose by or on behalf of the Owner to the CSP on or after the date of this Agreement; and/or the existence of the Purpose or any discussions or documents in relation to it (including the terms of this Agreement)"

Confidential Information does not include information which:

at the time of disclosure was in the public domain or subsequently enters into the public domain other than as the direct or indirect result of a breach of this Agreement by the CSP; or

the CSP can prove:

has been received by the CSP at any time from a third party who did not acquire it in confidence and who is free to make it available to the CSP without limitation; or

was independently developed by the Recipient without any breach of this Agreement.

2. THIRD PARTIES

The CSP shall not disclose the Confidential Information to third parties except that the CSP may disclose Confidential Information:

- to those of its officers, directors, employees, consultants, sub-contractors and professional advisers (the "CSP Parties") that reasonable require access to that Confidential Information in order for the Purpose to be fulfilled. The CSP will take reasonable steps to procure that each CSP Party will not do or omit to do anything which if done or omitted to be done by the CSP would constitute a breach of this Agreement. The CSP will be liable for the acts and omissions of its CSP Parties as if they were acts or omissions of the CSP;
- to the extent required by law or a court of competent jurisdiction or the rules of any applicable listing authority, securities exchange or governmental or regulatory body. Where reasonably practicable and lawful the CSP will notify the Owner in writing in advance of such disclosure, will consult with the Owner as to the content, purpose and means of disclosure and will seek to make such disclosure subject to obligations of confidence consistent, so far as possible, with the terms of this Agreement; or
- if the Owner has authorised disclosure in writing.

3. ACKNOWLEDGEMENT OF OWNERSHIP AND CONFIDENTIALITY

The CSP acknowledges and agrees that the Confidential Information disclosed to it by the Owner, or that it requires, sees, or learns of as a direct or indirect consequence of the discussions contemplated herein are the exclusive property of the Owner, and the CSP will keep that information strictly confidential.

4. NO TRANSFER OF RIGHTS

The CSP acknowledges and agrees that it shall not acquire any right or interest in the Confidential Information and that the Owner shall remain the sole owner of the Confidential Information, including but not limited to all patent, copyright, trademark, trade secret, trade name and other property rights pertaining thereto, anywhere in the world. The CSP shall not manufacture, use, sell, or distribute the Confidential Information without the written permission of the Owner.

5. NO OFFER FOR SALE

The parties acknowledge and agree that the disclosure of the Confidential Information by the Owner to the CSP does not constitute an offer by the Owner for the sale, license or other transfer of the Confidential Information. Any offer for sale, license, or other transfer of the Confidential Information shall be made pursuant to a separate agreement.

6. REMEDIES

Each party agrees that in the event of any such breach of this Agreement by it, that, in addition to all other remedies available to the other party by the Qatari law, the other party shall be entitled as a matter of right to apply to a court of competent jurisdiction for such relief by way of restraining order compliant with the provisions of this Agreement.

7. MODIFICATION

The parties can modify any term or condition of this Agreement only by mutual consent and by reducing such modifications to writing, signed by both parties.

8. SUCCESSORS

This Agreement shall be binding upon and inure to the benefit of both parties and their respective heirs, successors, assigns and representatives.

9. WAIVER

No waiver, delay, indulgence or failure to act by either party regarding any particular default or omission by the other party shall affect or impair any rights or remedies regarding that or any subsequent default or omission that are expressly waived in writing.

10. GOVERNING LAW

This Agreement shall be construed and interpreted in accordance with the laws of the State of Qatar. Disputes arising out of non-compliance with any of the terms in this Agreement shall be subject to the jurisdiction of the Courts of the State of Qatar.

11. COMMENCING PROCEEDINGS

The parties to this Agreement agree that the process of any suit, action, or proceeding before any court sitting in the State of Qatar, may be commenced by service delivered personally to the opposing party to this Agreement or to an appropriate agent for service.

12. CONTINUING OBLIGATION

Any rights and obligations under this Agreement that by their nature extend beyond the terms of this Agreement shall survive any expiration or termination of this Agreement and shall remain in effect for a period of two (2) years following such expiration or termination. However, either party may require a longer confidentiality term for specific information that should be marked and identified to the other party.

13. ATTORNEY FEES

If any litigation arises out of this Agreement, the prevailing party shall be entitled to reasonable attorney's fees, costs and expenses in addition to any other relief to which that party may be entitled

14. CAPTIONS

All indexes, titles, subject headings, section titles, and similar terms are provided for the purpose of reference and convenience and are not intended to be inclusive, definitive or to affect the meaning or scope of this agreement.

15. EXECUTION AUTHORITY

The persons whose signatures appear below certify that they are authorized to enter into this agreement on behalf of the party for whom they sign.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement.

OWNER		**CSP**, (xyz)	
Signed:		**Signed:**	
Name:		**Name:**	
Title:		**Title:**	
Date:		**Date:**	