Cloud and Hosting Services Standard

V-1.0

Ministry of Technology and Communications

VALIDATION & DISTRIBUTION:

	Name	Email	Issue date
Issued by	Governance & Compliance Division	IT.accreditation@mtc.gov.om	2019
Verified by			
Approved by	Steering Committee		

Distribution List	
1.	MTC
2.	IT Service Providers
3.	Online Publishing

DOCUMENT REVISION HISTORY:

Version	Date	Author	Remarks
1.0	2019	Governance & Compliance Division	Creation of document

Contents

1 Introduction

As government agencies transition their applications and data to use cloud computing, it is critically important that the level of security provided in the cloud environment be equal to or better than the security provided by their non-cloud IT environment. Failure to ensure appropriate security protection could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing.

Standards are already available in support of many of the functions and requirements for cloud computing. While many of these standards were developed in support of pre-cloud computing technologies, such as those designed for web services and the Internet, they also support the functions and requirements of cloud computing. Refer to OeGAF-Technical Reference Model (TRM) for the standards catalogue.

While there are only a few cloud computing specific standards (such as virtualization, infrastructure management, service level agreements (SLAs), audits and cloud-specific data handling) at present, there is a fast-changing landscape of cloud computing-relevant standardization under way in a number of Standards Developing Organizations (SDO). In the context of putting recommendations for the Cloud Computing Standards for Oman government entities, every effort has been made to gather input from SDOs active in this area. This is an intermediate result which simply lists standards relevant for cloud computing customers. The overview of standards was produced in collaboration with different government stakeholders including TRA.

1.1 Target audience

This document is aimed at CIO's, architects in government organizations who are procuring cloud services. It may be of interest also for cloud service providers.

1.2 Scope

This document analyses a range of different cloud standards from a security and resilience perspective, for government agencies adopting or using cloud computing services. Standards we discuss in this document include security standards, cloud computing standards, interoperability standards etc. This is not an exhaustive or complete list – there are hundreds of standards that could be (or become) relevant. Especially in the area of information security governance and risk management there is a flurry of initiatives aiming to customize existing information security management standards (like ISO270001) to fit better the situation of cloud computing service providers.

We skip technical standards on and below the transport layer (i.e. Ethernet, TCP/IP, TLS/SSL, HTTP, SMTP etc.), because these layers are very generic and also highly standardized. For the sake of brevity, we also skip a range of cryptographic standards, which are used for encrypting or authenticating messages or stored data (i.e. SHA-1, SHA-256, Blowfish, RSA, ECC, etc.).

2 Introduction to Cloud Computing

Cloud computing is a 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. This cloud model is composed of *five essential characteristics*, *three service models*, and *four deployment models* as discussed in detail below.

2.1 Essential Characteristics

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's 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 consumer demand. There is a sense of location independence in that the customer 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 rapidly and elastically provisioned, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, 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 of the utilized service.

2.2 Service Models

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.[2] The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider.[3] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

There are some emerging cloud service models like Security as a Service. These service models are out of the scope of this document

2.3 Deployment Models

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). 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.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

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

Throughout this document, any general use of the term "cloud" or "cloud system" should be assumed to apply to each of the four deployment models. Care is taken to specify a specific deployment model when a statement is not applicable to all four models.

To add clarity, this document uses the following terms consistently:

cloud consumer or **customer**: a person or organization that is a customer of a cloud; note that a cloud customer may itself be a cloud and that clouds may offer services to one another;

client: a machine or software application that accesses a cloud over a network connection, perhaps on behalf of a consumer; and

cloud provider or **provider**: an organization that provides cloud services.

3 Cloud and Hosting/Computing Requirements

(Contractual Obligations)

Cloud Service Provider (CSP) offering cloud services to government agencies must meet following requirements.

For all currently implemented cloud services and those services currently in the acquisition process prior to release of this standard [release date] must meet all requirements by [date – 2 years from the release date of standard].

3.1 Security Requirements:

The CSP offering cloud services to government agencies shall apply the appropriate set of controls to ensure compliance to security standards including but not limited to:

- ISO/IEC 27001,
- ISO/IEC 27017,
- ISO/IEC 27018,
- Cloud Security Alliance (CSA) – Control Matrix.
- PCI-DSS Compliance - for hosting Online Payment Solutions.

3.2 Privacy Requirements:

CSP shall be responsible for the following privacy and security safeguards:

1. To the extent required to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the Government access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.
2. If new or unanticipated threats or hazards are discovered by either the Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
3. The CSP shall also comply with any additional privacy requirements required by the government.
4. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the CSPs' IT environment being used to provide or facilitate services for the Government. CSP shall be responsible for the following privacy and security safeguards:
    a. The CSP shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the CSP under this contract or otherwise provided by the Government.

b. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the CSP shall afford the Government access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to:
   i. Authenticated and unauthenticated operating system/network vulnerability scans
   ii. Authenticated and unauthenticated web application vulnerability scans
   iii. Authenticated and unauthenticated database application vulnerability scans
   iv. Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

If the CSP chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.

3.3 Sensitive Information Storage And Processing

Government data and/or information must only be hosted/transacted/processed with in the geo boundaries of Sultanate of Oman. This includes the primary storage as well as the backup or disaster recovery arrangements.

Sensitive information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The CSP shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following agreed Media Sanitization methods.

The CSP shall develop and maintain plan for disengagement and transition of services - in case agency is transitioning to a new CSP or alternatively bringing the services back in-house.

Agreement for retrieval/return of all data (including the primary storage as well as the backup or disaster recovery arrangements), in case of disengagement, in formats approved by the agency.

3.4 Protection Of Information

The CSP shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The CSP shall also protect all Government data, equipment, etc. by treating the information as sensitive. It is anticipated that this information will be gathered, created, and stored within the primary work location. If CSP personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets.

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The CSP shall ensure that the facilities that house the network infrastructure are physically secure.

The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The CSP shall provide requested data at no additional cost to the government.

No data shall be released by the CSP without the consent of the Government in writing. All requests for release must be submitted in writing to the agency representative.

3.5 Confidentiality And Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the CSP in the performance of this contract, are the property of the Government of Oman and must be submitted to the contracting agency at the conclusion of the contract. The Government of Oman has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the Government of Oman and cannot be reproduced, or retained by the CSP. All appropriate project documentation will be given to the agency during and at the end of this contract. The CSP shall not release any information without the written consent of the Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the CSP by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the CSP assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its sub-contractor shall be under the supervision of the CSP or the CSP's responsible employees. Each officer or employee of the CSP or any of its sub-contractor to whom any Government record may be made available or disclosed shall be notified in writing by the CSP that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by [mention applicable/relevant law clauses here].

4 Accreditation of CSPs

MTC requires cloud service providers to utilize a Third-Party Assessment Organization to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.

The MTC security staff will be available for consultation during the process. MTC will review the results before issuing Accreditation decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Accreditation decision.

CSPs must comply with all of the requirements within this standard. They should keep records of all customer engagement`s activities and document the delivered service and associated processes as well for assurance purposes.

Accreditation of the CSPs will be valid as long as they maintain their ISMS Certification, Security Clearance for Assessing highly classified information and Systems, and the required level of team`s skills and competencies.

4.1 Assessment of the System:

1. The CSP shall comply with the requirements as stated in this standard, including making available any documentation, physical access, and logical access needed to support this requirement. The CSP shall create, maintain and update the following documentation:
   - Security Assessment Report
   - System Security Plan
   - IT System Contingency Plan
   - IT System Contingency Plan Test Results
   - Plan of Action and Milestones
   - Continuous Monitoring Plan
   - Control Implementation Summary Table
   - Results of Penetration Testing
   - Software Code Review (for SaaS, Software as a service)
   - Interconnection Agreements/Service Level Agreements/Memorandum of Agreements
2. Information systems must be assessed by Third-Party Assessment Organization whenever there is a significant change to the system's security posture in accordance with the Continuous Monitoring Plan.

3. The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the CSP shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with the requirements. Review activities include but are not limited to scanning operating systems , web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.
4. Identified gaps between required Security Controls including Continuous Monitoring controls and the CSP's implementation as documented in the Security Assessment Report shall be tracked by the CSP for mitigation in a *Mitigation Action Plan* document. Depending on the severity of the gaps, the Government may require them to be remediated before Accreditation is issued.
5. The CSP is responsible for mitigating all security risks found during assessment and continuous monitoring activities. All vulnerabilities must be mitigated within **30 days** from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

4.2 Reporting and Continuous Monitoring:

Maintenance of the CSP Accreditation will be through continuous monitoring and periodic audit of the operational controls within a CSP’s system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment.

Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the MTC as required by Requirements stated in this document. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the MTC to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Accredited CSPs will be required to submit monitoring reports to MTC on regular basis.

5 References

The CSA's guidance noted that application security must be "represented as a clearly articulated set of actions and guarantees within the SLA. This can include providing documentation of security measures taken by the vendor, as well as allowing for reasonable security testing related to ongoing activities such as logging, audit reports and periodic validation of security controls."

CSA STAR Attestation – CSA STAR Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. STAR Attestation provides for rigorous third party independent assessments of cloud providers.
https://cloudsecurityalliance.org/star/attestation/

Data sovereignty is the concept that information which has been converted and stored in binary digital form is subject to the laws of the country in which it is located.

Annexure A - Cloud Computing Standards

This document focuses primarily on most challenging concerns for cloud computing, and prescribes requirements for government agencies to mitigate risk associated with public cloud deployment. The concerns are:

- **Security**
- **Interoperability and Portability**
- **Performance**
- **Accessibility**

5.1 Security

The term cloud computing encompasses a variety of systems and technologies as well as service and deployment models, and business models. Cloud computing's unique attributes such as elasticity, rapid provisioning and releasing, resource pooling, multi-tenancy, broad-network accessibility, and ubiquity bring many benefits to cloud adopters, but also entails specific security risks associated with the type of adopted cloud and deployment mode. To accelerate the adoption of cloud computing, and to advance the deployment of cloud services, solutions coping with cloud security threats need to be addressed.

Many of the threats that cloud providers and consumers face can be dealt with through traditional security processes and mechanisms such as security policies, cryptography, identity management, intrusion detection/prevention systems, and supply chain vulnerability analysis. However, risk management activities must be undertaken to determine how to mitigate the threats specific to different cloud models and to analyze existing standards for gaps that need to be addressed.

Securing the information systems and ensuring the confidentiality, integrity, and availability of information and information being processed, stored, and transmitted are particularly relevant as these are the high-priority concerns and present a higher risk of being compromised in a cloud computing system. Cloud computing implementations are subject to local physical threats as well as remote, external threats.

Consistent with other applications of IT, the threat sources include accidents, natural disasters that induce external loss of service, hostile governments, criminal organizations, terrorist groups, and malicious or unintentional vulnerabilities exploited through internal, external, authorized, or unauthorized access to the system. The complexity of the cloud computing architecture supporting three service types and four deployment models, and the cloud characteristics, specifically multi-tenancy, heighten the need to consider data and systems protection in the context of logical, physical boundaries and data flow separation.

Possible types of security challenges for cloud computing services include the following:

- Compromises to the confidentiality and integrity of data in transit to and from a cloud provider and at rest;
- Attacks which take advantage of the homogeneity and power of cloud computing systems to rapidly scale and increase the magnitude of the attack;
- A consumer’s unauthorized access (through improper authentication or authorization, or exploit of vulnerabilities introduced maliciously or unintentionally) to software, data, and resources provisioned to, and owned by another authorized cloud consumer;
- Increased levels of network-based attacks that exploit software not designed for an Internet-based model and vulnerabilities existing in resources formerly accessed through private networks;
- Limited ability to encrypt data at rest in a multi-tenancy environment;
- Portability constraints resulting from the lack of standardization of cloud services application programming interfaces (APIs) that preclude cloud consumers to easily migrate to a new cloud service provider when availability requirements are not met;
- Attacks that exploit the physical abstraction of cloud resources and exploit a lack of transparency in audit procedures or records;
- Attacks that take advantage of known, older vulnerabilities in virtual machines that have not been properly updated and patched;
- Attacks that exploit inconsistencies in global privacy policies and regulations;

- Attacks that exploit cloud computing supply chain vulnerabilities to include those that occur while cloud computing components are in transit from the supplier to the cloud service provider;
- Insider abuse of their privileges, especially cloud provider's personnel in high risk roles (e.g. system administrators; and
- Interception of data in transit (man-in-the-middle attacks).

Some of the main security objectives for a cloud computing implementer should include:

- Protect consumers' data from unauthorized access, disclosure, modification or monitoring. This includes supporting identity management and access control policies for authorized users accessing cloud services. This includes the ability of a customer to make access to its data selectively available to other users.
- Prevent unauthorized access to cloud computing infrastructure resources. This includes implementing security domains that have logical separation between computing resources (e.g. logical separation of customer workloads running on the same physical server by VM monitors [hypervisors] in a multi-tenant environment) and using secure-by-default configurations.
- Deploy in the cloud web applications designed and implemented for an Internet threat model.
- Challenges to prevent Internet browsers using cloud computing from attacks to mitigate end-user security vulnerabilities. This includes taking measures to protect internet-connected personal computing devices by applying security software, personal firewalls, and patch maintenance.
- Include access control and intrusion detection and prevention solutions in cloud computing implementations and conduct an independent assessment to verify that the solutions are installed and functional. This includes traditional perimeter security measures in combination with the domain security model. Traditional perimeter security includes restricting physical access to network and devices; protecting individual components from exploitation through security patch deployment; setting as default most secure configurations; disabling all unused

ports and services; using role-based access control; monitoring audit trails; minimizing privileges to minimum necessary; using antivirus software; and encrypting communications.

- Define trust boundaries between cloud provider(s) and consumers to ensure that the responsibilities to implement security controls are clearly identified.
- Implement standardized APIs for interoperability and portability to support easy migration of consumers' data to other cloud providers when necessary.

The following tables map security standards to various security categories. Some of the listed standards apply to more than one category and are therefore listed more than once.

Authentication & Authorization

Standards	**SDO**
ISO/IEC 9594-8 | X.509 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	ISO/IEC & ITU-T
ISO/IEC 29115 **|** X.1254 Information technology -- Security techniques -- Entity authentication assurance framework	ISO/IEC & ITU-T
RFC 5246 Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	IETF
RFC 3820: X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile	IETF
RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	IETF
RFC 5849 OAuth (Open Authorization Protocol)	IETF
OpenID Authentication	OpenID
eXtensible Access Control Markup Language (XACML)	OASIS
Security Assertion Markup Language (SAML)	OASIS

Confidentiality

Standards	SDO
RFC 5246 Secure Sockets Layer (SSL)/ Transport Layer Security (TLS)	IETF
Key Management Interoperability Protocol (KMIP)	OASIS
XML Encryption Syntax and Processing	W3C

Integrity

Standards	SDO
XML signature (XMLDSig)	W3C

Identity Management

Standards	SDO
X.1253 : Security guidelines for identity management systems	ITU-T
Service Provisioning Markup Language (SPML)	OASIS
Web Services Federation Language (WS-Federation) Version 1.2	OASIS
WS-Trust 1.3	OASIS
Security Assertion Markup Language (SAML)	OASIS
OpenID Authentication 1.1	OpenID Foundation

Security Monitoring & Incident Response

Standards	**SDO**
ISO/IEC 27035-1 Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management	ISO/IEC
ISO/IEC 27035-3 Information technology -- Security techniques -- Information security incident management -- Part 3: Guidelines for CSIRT operations	ISO/IEC
ISO/IEC 27039; Information technology -- Security techniques -- Selection, deployment and operations of intrusion detection systems	ISO/IEC
ISO/IEC 18180 Information technology - Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2 (NIST IR 7275)	ISO/IEC
X.1500 Cybersecurity information exchange techniques	ITU-T
X.1520: Common vulnerabilities and exposures	ITU-T
X.1521 Common Vulnerability Scoring System	ITU-T
PCI Data Security Standard	PCI

Security Controls

Standards	**SDO**
Cloud Controls Matrix Version 1.3	CSA
ISO/IEC 27001:2005 Information Technology – Security Techniques Information Security Management Systems Requirements	ISO/IEC

ISO/IEC 27017 Information technology -- Security techniques -- Information security management - Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002	ISO/IEC
ISO/IEC 27018 Code of Practice for Data Protection Controls for Public Cloud Computing Services	ISO/IEC
ISO/IEC 27036-4 Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services	ISO/IEC

Security Policy Management

Standards	**SDO**
ATIS-02000008 Trusted Information Exchange (TIE)	ATIS
ISO/IEC 27002 Code of practice for information security management	ISO/IEC
eXtensible Access Control Markup Language (XACML)	OASIS

Availability

Standards	**SDO**
ATIS-02000009 Cloud Services Lifecycle Checklist	ATIS
ISO 22301 Societal security — Business continuity management systems --- Requirements	ISO
ISO/IEC 27031	ISO

Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity	

5.2 Interoperability And Portability

Cloud platforms should make it possible to securely and efficiently move data in, out, and among cloud providers and to make it possible to port applications from one cloud platform to another. Data may be transient or persistent, structured or unstructured and may be stored in a file system, cache, relational or non-relational database. Cloud interoperability means that data can be processed by different services on different cloud systems through common specifications. Cloud portability means that data can be moved from one cloud system to another and that applications can be ported and run on different cloud systems at an acceptable cost.

Cloud interoperability allows seamless exchange and use of data and services among various cloud infrastructure offerings and to use the data and services exchanged to enable them to operate effectively together.

Cloud portability allows two or more kinds of cloud infrastructures to seamlessly use data and services from one cloud system and be used for other cloud systems.

For example, a financial application might use a petabyte of data, but that data might be securely housed in a single cloud database, making it relatively easy to port. On the other hand, a customer relationship management (CRM) application running in the cloud system might process only a terabyte of data but which is shared among thousands of users; moving the CRM application – and all its distributed data – from one cloud system to another would be more challenging. Overall, functionality of cloud interoperability is preferable.

5.2.1 Cloud Standards For Interoperability

The interoperability of cloud services can be categorized by the management and functional interfaces of the cloud services. Many existing IT standards contribute to the interoperability between cloud consumer applications and cloud services, and between cloud services themselves. There are standardization efforts that are specifically initiated to address the interoperability issues in the cloud system. These cloud specific standards are listed in table below – Interoperability Standards.

Service Interoperability

Standards	**SDO**
ISO/IEC 17826 Information technology — Cloud Data Management Interface (CDMI)	ISO
Cloud Infrastructure Management Interface (CIMI)	DMTF
Y.3520 Cloud computing framework for end to end resource management.	ITU-T
Open Cloud Computing Interface (OCCI)	OGF
Data Format Description Language (DFDL)	OGF
Topology and Orchestration Specification or Cloud Applications (TOSCA),Version 1.0	OASIS

5.2.2 Cloud Computing Standards For Portability

Portability issues in the cloud system include workload and data portability. While some of the cloud computing workload portability issues are new, many of existing data and metadata standards were developed before the cloud computing era. The following table focuses on cloud-specific portability standards.

Data Portability

Standards	**SDO**
ISO/IEC 17826 Information technology — Cloud Data Management Interface (CDMI)	ISO

Cloud Data Management Interface (CDMI)	SNIA

System Portability

Standards	**SDO**
ISO/IEC 17203 Information technology -- Open Virtualization Format (OVF) specification	ISO
Open Virtualization Format (OVF), OVF 2.0	DMTF
Topology and Orchestration Specification for Cloud Applications (TOSCA),Version 1.0	OASIS

5.3 Performance

The topic of performance includes considerations related to monitoring, reporting, measuring, scaling, and right-sizing cloud resources to meet the expected or experienced demand. This area deserves careful consideration, as it relates directly to the factors that control the potential cost savings to the government from the use of cloud computing.

Performance can potentially be scaled to meet conditions of anticipated or real-world demand, within the parameters of a cloud service agreement. It is therefore crucial that such agreements contain all necessary parameters that relate to the conditions for delivery of the associated cloud service or product. Only by careful measurement and by proper anticipation of peak workload conditions, backed by appropriate service remedies, credits, or penalties and appropriate fallback arrangements, can true cost savings be realized with proper delivery of services.

Wherever possible, standards-based methods for monitoring, measuring, and scaling delivery of the resources to meet agency missions should be pursued. At the moment, most cloud service agreements are expressed in human-readable terms for review by legal staff and management. Tools are increasingly available, however, for expression of service agreement conditions, remedies, and provisions that can be expressed in machine-readable terms and that can even serve as the basis for service templates that can be provisioned automatically, directly from the service agreement template. Table below provides a list of relevant standards.

Service Agreements

Standards	**SDO**
Topology and Orchestration Specification for Cloud Applications (TOSCA),Version 1.0	OASIS
TR178 Enabling End-to-End Cloud SLA Management, Version 0.4	TM Forum
TR194 Multi-Cloud Service Management Accelerator Pack - Introduction, Release 1.0	TM Forum
TR195 Multi-Cloud Service Management Pack - Business Guide, Release 1.0	TM Forum
TR196 Multi-Cloud Service Management Pack - Technical Guide, Release 1.0	TM Forum
TR197 Multi-Cloud Service Management Pack – SLA Business Blueprint	TM Forum
TR198 Multi-Cloud Service Management Pack – Developer Primer	TM Forum

5.4 Accessibility

Accessibility is relevant to cloud computing services at the application level where a human interacts with an application. This is where accessibility is measured. Therefore, many of the existing accessibility standards for ICT applications are relevant to cloud computing applications.

The following table lists accessibility standards relevant for cloud computing applications.

Accessibility

Standards	**SDO**
W3C Web Content Accessibility Guidelines (WCAG) 2.0	W3C
ISO 9241-20, Ergonomics of human-system interaction -- Part 20: Accessibility guidelines for information/communication technology (ICT) equipment and services	ISO/IEC
ISO 9241-171, Ergonomics of human-system interaction -- Part 171: Guidance on software accessibility	ISO/IEC
ISO/IEC 24751-1, Information technology -- Individualized adaptability and accessibility in e-learning, education and training -- Part 1: Framework and reference model	ISO/IEC

ANSI/HFES 200 Human Factors Engineering of Software User Interfaces (Parts 1, 2, and 3)	ANSI

Endnote:

Standards continue to rapidly evolve in step with technology. Hence, cloud standards may be at different stages of maturity and levels of acceptance. When a provider claims conformance with any other standard, it should cite the specific version and publish implementation, errata, and testing notes. This will provide the transparency necessary for informed consumer choice, as well as ensure reasonably seamless technical interoperability between on-premises and cloud virtualized systems.