WP 1 – Review and analyze best EU and global practices in cloud computing

DEV 1.4 – Regulatory Compliance with international experience

**Authors:**

**Prof.dr Dragan Đurić, IMTM**

**Igor Ognjanović, IMTM**

Table of Contents

[1. Introduction 3](#_Toc468092454)

[2. Cloud Computing standards for interoperability and portability 4](#_Toc468092455)

[3. Cloud computing standards for security 5](#_Toc468092456)

[4. Filling Cloud computing standards gaps… 6](#_Toc468092457)

[5. Conclusion 7](#_Toc468092458)

# Introduction

# Information systems are a strategic element in the proper functioning and stability of the banking and insurance sectors. The field of IT is also constantly evolving as technologies and solutions are constantly being renewed.

# Cloud computing is a relatively new term used to describe a variety of established business strategies, technologies, and processing methodologies. Although the term cloud computing is gaining in usage, there is no widely-accepted definition, 1 and numerous business strategies, technologies, and architectures are represented as cloud computing. In general, cloud computing is a migration from owned resources to shared resources in which client users receive information technology services, on demand, from third-party service providers via the Internet “cloud.”

# Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. These models include: a private cloud, which is operated solely for an organization; a community cloud, which is shared by several organizations; a public cloud, which is available to any paying customer; and a hybrid cloud, which is a composition of two or more clouds (private, community, or public).

#  Outsourcing to a cloud service provider can be advantageous to financial institutions because of potential benefits such as cost reduction, flexibility, scalability, improved load balancing, and speed. Before approving any outsourcing of significant functions, it is important to ensure such actions are consistent with the institution’s strategic plans and corporate objectives approved by the board of directors and senior management.

# Cloud Computing standards for 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.

# The migration path to cloud computing should preserve existing investments in technologies which are appropriate to the cloud system, and that enables the coexistence and interoperability of on-premises software and cloud services. Additionally, the migration to a cloud system should enable various multiple cloud platforms seamless access between and among various cloud services, to optimize the cloud consumer expectations and experience.

# 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

# Cloud Standards for Interoperability

# Interoperability may be assessed at the IaaS, PaaS, and SaaS levels. Each of these levels, which may be combined in any particular cloud service or product in practice, presents special considerations, and as a result, the standards landscape is intrinsically unique and specific to each level. At the IaaS level, two published standard sets exist that are applicable, the Open Cloud Computing Interface (OCCI) specification set and the Cloud Infrastructure Management Interface (CIMI) set. OCCI, published in early 2011, is slightly more general in formulation and presents a generic boundary level protocol for achieving restful control of a target infrastructure within the given boundary. It has been applied to virtual machine instantiation and control, provision and discovery of network features and other internal features, and has an extensible, self-describing feature set. CIMI, more recently developed and published in late 2012, has a tightly described calling sequence. Each of these standard sets has seen significant uptake, and several available cloud system products either already implement or plan to be implement at least one of them.

# In PaaS applications, an extensive ecosystem of vendor-specific products that are not interchangeable has emerged. A recent effort to produce a PaaS-specific standard22 has been started by the OASIS Cloud Application Management Protocol (CAMP) technical committee, with support from several industry participants, and is making rapid progress towards producing a workable specification.

# In the case where a SaaS application is consumed through a web browser, there may be many standards that are used to achieve interoperability between what is essentially a web server and the user’s browser, such as IP (v4, v6), TCP, HTTP, SSL/TLS, HTML, XML, REST, Atom, AtomPub, RSS, and JavaScript/JSON. None of these web standards are cloud-specific, and these same standards are being used in many web browser-based management interfaces.

# Where data is acted on by multiple services, cloud or otherwise, there are various standards that enable interoperability. Also important are interoperability standards for distributed applications such as SOAP, WS and ebXML. Other standards that can be used for interoperability between cloud services include OpenID, Odata, CDMI, AMQP, and XMPP. Most important for interoperability are canonical data content formats, typically today expressed using XML standards. Such standard canonical formats include “nouns,” i.e., the data objects being acted on, but also (implicitly or explicitly) the “verbs,” i.e., the actions that a receiving service may or should take on such a data object (e.g., Sync, Process, Get, Show, etc.). While “verbs” may be somewhat generic, such canonical formats are in general specific to a particular domain.

# Various standards exist corresponding to different application domains (e.g., OAGi BODs for business documents or ODF and OOXML for office productivity documents). Also important is the stack of interoperability standards for interfaces, packaging, and transport such as SOAP, WS-\* and ebXML. Since the SaaS area is so wide-ranging, cloud-based SaaS products are likely to continue to exercise and to explore the full range of Internet protocols for their communication and interfaces. It is more likely that data formats and metadata-based interchange methods will be standardized in cloud system products rather than having SaaS interfaces themselves converge. Examples of such data format description standardization include the Data Format Description Language (DFDL) from OGF and the Cloud Data Management Interface (CDMI) data-container metadata model of the Storage Networking Industry Association (SNIA). As the cloud computing landscape is currently heavily populated by vendor-specific formats, such general-purpose standardization efforts may be crucial to achieving interoperability at the SaaS level.

#  Cloud standards for portability

# Over the last year, much progress has been made on new standards in this area. Open Virtualization Format (OVF) from the Distributed Management Task Force (DMTF), for example, was developed to address portability concerns between various virtualization platforms. It consists of metadata about a virtual machine image or groups of images that can be deployed as a unit. It provides a mechanism to package and deploy services as either a virtual appliance or used within an enterprise to prepackage known configurations of a virtual machine image or images. It may contain information regarding the number of CPUs, memory required to run effectively, and network configuration information. It also can contain digital signatures to ensure the integrity of the machine images being deployed along with licensing information in the form of a machine-readable EULA (End User License Agreement) so that it can be understood before the image(s) is deployed.

# Significant progress has also been made in the creation of new standards focused on portability concerns at higher levels of abstraction such as the cloud service and application. Topology and Orchestration Services for Applications (TOSCA) from OASIS, for example, was developed to address portability concerns between services and applications that may be required to be deployed on different cloud providers and platforms due to reasons such as regulatory concerns, changing business and market factors, or evolving technical requirements. TOSCA provides a machinereadable language to describe the relationships between components, requirements, and capabilities. The intent is to facilitate service and life cycle management of services and applications in IaaS, PaaS, and SaaS environments while enabling the specification of life cycle operations at that level of abstraction, e.g., deploy, patch, shutdown, in a cloud platform and provider independent fashion. As of February 2013, the TOSCA specification had completed a 30-day public review. A primer, which includes a chapter on the relationship between OVF and TOSCA is under development.

# A future direction of workloads data and metadata standardization is to help improve the automation of inter-cloud system workload deployment. Concepts such as standardized SLAs, sophisticated inter-virtual machine network configuration and switching information, and software license information regarding all of the various components that make up the workload are possibilities.

# Another aspect of portability in the cloud system is that of storage and data (including metadata) portability between cloud systems, for example, between storage cloud services and between compatible application services in SaaS and PaaS layers.

# Cloud storage services may be seen as a special class of application service, where the storage metadata (as distinct from the stored data content) is the application data that a receiving cloud system must be able to process. For cloud storage services, as much of the actual data movement needs to be done in bulk moves of massive numbers of objects, retaining the data organization (into containers, for example) and retaining the associated metadata are main portability requirements.

#  Data portability between cloud application services requires standard formats and protocols. The canonical data formats commonly involved in portability scenarios may be focused on widely used application categories, for example, email or office productivity, or on specific formats used by particular domains of use, for example, science or medical domains. Popular methods for interchange of data in cloud systems generally leverage representations in either JSON or XML formats, and are often customized to particular fields of use through standards.

# Standards are key to achieving portability. Building on existing standards and specifications that are known to work and are in widespread use and documenting how the standards are implemented, allows developers to continue to use their chosen development languages and tools as they build for cloud systems. This keeps migration costs and risks low by enabling organizations to leverage their IT staff’s current skills, and by providing a secure migration path that preserves existing investments. Examples of languages, tools, and standards that are common in the cloud system include programming languages such as Java, C#, PHP, Python and Ruby; Internet protocols for service access such as REST, SOAP, and XML; federated identity standards for service authentication such as SAML and OAuth; and standards for managing virtualized environments.

# Standards continue to rapidly evolve in step with technology. Hence, cloud standards may be at different stages of maturity and levels of acceptance. OVF, for example, is an open standard for packaging and distributing virtual appliances. Originally offered as a proprietary format to the DMTF, OVF was first published in March 2009, and subsequently adopted in August 2010 as a national standard by the American National Standards Institute (ANSI).

# 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.

# Summary

# Substantial progress has been made by SDOs to develop standards that meet specific cloud computing requirements and use cases. There are now existing standards that support cloud service interoperability and data portability but gaps remain in the standards, specifically in the PaaS area, and current development efforts still need to mature.

# As cloud standards evolve, they will need to describe how services interoperate and how data can be readily ported between cloud offerings. As cloud standards and IT standards that support cloud implementations change and evolve, the issues of governance and orchestration of cloud architectures will become more prevalent and simultaneously, how to ‘standardize’ a governance model will need to be updated. Governance of the cloud is analogous to the governance of Internet but rather than standardizing on packets of data, it is standardizing on how data and services are shared. Cloud standards will need to describe how services and data can be readily ported or interoperate between cloud offerings as seamless, efficient access to data and services across cloud providers will become the demand signal from customers. The SAJACC group has received and has begun analyzing input from several SDOs and from federal agencies with regard to this topic, including the area of service agreements and SLAs that is explored further in Section 6.6, “Cloud Standards for Performance”.

# Cloud computing standards for 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 secureby-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.

# Cloud computing standards for security

# There are numerous reasons why cloud computing standards for performance are needed in today’s market. Consumers need to be able to objectively determine the costs and benefits of moving to cloud services; to validate claims of performance by cloud providers; and to objectively compare services from multiple providers in order to better meet a specific need.

# Determining performance involves establishing a set of metrics that will provide a clear picture of how a given cloud service performs. This is complex due to the fact that specific metrics and standards will be needed for not only specific categories of services, but also due to the domains in which they are needed. For example, dealing with private healthcare data will need performance standards relating to both privacy and security. Standards might be needed for attributes that are associated with the service such as network performance. Additionally, standards are needed that measure attributes specific to cloud service such as virtual machine performance.

# While not an exhaustive list, other potential performance aspects relevant to the cloud include:

# Management performance

# Benchmark performance

# Cloud service life cycle elements:

# Negotiation performance

#  Instantiation performance o

# Termination performance

# Performance testing

# Monitoring

# Auditing

# In the end, these performance standards will be of interest to many of the stakeholders involved in cloud computing. Cloud consumers and providers will use these standards and metrics as a basis for creating measurable and enforceable service level agreement contracts. Auditors will be able to measure performance for their customers. Cloud brokers will need these standards to ensure that their customer’s specific needs are met. Cloud providers will be performing self-evaluations on their own offerings.

# 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.

# Agencies using cloud services should be careful to include suitable performance, monitoring, and emergency metrics and conditions into the cloud service master agreement and associated SLA. These elements, reflecting the agencies given mission and goals, will help to ensure that each agency will pay only for needed services.

# Cloud services are particularly well suited to deployment of automated terms and conditions for the delivery of these services. While the basic parameters, legal, and cost controls for cloud services require agency approval and human-mediated review, automated tools should be deployed where appropriate to ensure conditions such as failover in the event of cloud service component failure or compromise, and scaling to meet emergent needs or to grow or shrink service delivery according to cost and/or demand, and other relevant features.

# Wherever possible, standards-based methods for monitoring, measuring, and scaling delivery of the resources to meet agency missions should be pursued.

# Cloud computing standards for service agreements

# 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.

# Examples of these methods can be seen in several open source products based on the WSAgreement and WS-Agreement-Negotiation specifications from OGF. Recent work from an interSDO joint task force led by TM Forum has also produced a white paper describing the considerations for end-to-end service agreement management specifically oriented towards management of multiple cloud service SLAs. The possibility of “TOSCA service template extension to support SLA management and possible mapping to SID information framework,” is also discussed.

# The TM Forum has developed a set of standards to help in the implementation and management of services that span multiple partners in a “multi-cloud” system. Organized as "packs", these standards focus on managing service level agreements between partners, and ensure consistency in the management of information across aggregated services with particular emphasis where these services cross multi-company boundaries. There are Business, Technical, and Accelerator Packs that have been published; these documents augment the Cloud Service Level Agreement Handbook (GB917) that was published by the TM Forum in April 2012. The TM Forum has also developed a series of documents working primarily with large-scale enterprises and ensuring that their best practice needs are met in the delivery of cloud services.

1. **Filling Cloud computing standards gaps**

# Cloud computing is the result of evolutions of distributed computing technologies, enabled by advances in fast and low-cost networks, commoditized faster hardware, practical high-performance virtualization technologies, and maturing interactive web technologies. Cloud computing continues to leverage the maturity of these underlying technologies, including many standard-based technologies and system architecture components. As the previous sections of the cloud computing standards survey show, the majority of cloud system relevant standards are from these pre-cloud era technologies.

# In the meantime, there are emerging challenges in some areas in cloud computing that have been addressed by technology vendors and service providers’ unique innovations. New service model interactions and the distributed nature in resource control and ownership in cloud computing have resulted in new standards gaps. Some of these gaps are introduced by new service model interactions and the distributed nature of resource control and ownership in cloud computing and some are pre-cloud computing era technology standardization gaps that are now brought to the forefront.

# In this section, first, we use the cloud computing conceptual model from NIST Cloud Computing Reference Architecture and Taxonomy Working Group as described in Chapter 3 as the framework of reference to identify these gaps in need of standardization. Secondly, we use a broad set of USG business use cases as described in previous sections and from the NIST Cloud Computing Target Business Use Case Working Group, to identify priorities of standardization that will maximize the benefits and meet the more urgent needs of federal government consumers.

# Areas of Standardization Gaps

# As the cloud computing conceptual model indicates, cloud computing consumers do not have direct visibility into the physical computing resources. Instead, consumers interact with service providers through three service model interfaces, IaaS, PaaS, and SaaS, to gain a view of the abstracted computing resource they are using. As described in Chapter 5, Cloud Computing Standards, these interaction interfaces can be categorized into two types: (1) functional interfaces that expose the primary function of the service, and (2) management interfaces that let the consumers manage the rented computing resources. The following areas of standardization gaps are observed through the standards inventory

#  SAAS Functional Interfaces

# The varieties of the SaaS applications determine what can be consumed by the SaaS consumer. There are varying degrees of functional standardization. SaaS applications are mainly available by using a web browser, and some are consumed as a web service using other application clients, such as standalone desktop applications and mobile applications. Even as most SaaS applications are using web and web service standards to deliver these application capabilities, application-specific data and metadata standards remain standardization gaps in portability and interoperability. For example, email and office productivity application data format standards and interfaces are required to achieve interoperability and portability for migrating from existing systems to cloud systems.

# Another important area for standardization is the metadata format and interfaces, in particular, to support compliance needs. For example, standard metadata format and APIs to describe and generate e-discovery metadata for emails, document management systems, financial account systems, etc., will help government consumers to leverage commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software products to meet e-discovery requirements. This is especially important when email messaging systems, content management systems, or Enterprise Resource Planning (ERP) financial systems migrate to a SaaS model.

#  SaaS Self-service Management Interfaces

# Due to the diverse domain and functional differences among SaaS offerings, the management interfaces used for the consumers to administer and customize the application functionalities are also very diverse. However, certain management functionalities are common, such as those related to user account and credential management. These common management functionalities represent candidates for interoperability standardization.

# PaaS Functional Interfaces

# PaaS functional interfaces encompass the runtime environment with supporting libraries and system components for developers to develop and deploy SaaS applications. Standard-based APIs are often part of a PaaS offering such that the PaaS provider can enable existing development for a cloudbased hosting system. However, data format for backup and migration of application workload, including database serialization/de-serialization, need further standardization to support portability.

# Security

# As cloud systems are typically external components in a consumer organization’s overall IT system, especially in the outsourced (off-site) deployment models, the need to have seamless security integration calls for interoperable standard interfaces for authentication, authorization, and communication protections. The challenges of identity and access management across different network and administration domains are more prominent in the cloud system as the implementation of these capabilities within the cloud systems are often not the same organization as consumer organization where the identity information originates. Standardization in areas such as identity provisioning, management, secure and efficient replication across different systems, and identity federation will greatly help to improve the identity management capabilities in cloud systems. A related area with specifically wide government usage that can benefit from standardization is single sign-on interface and protocols that support strong authentication.

#  Government IT systems have strong auditing and compliance needs. In many cases, these requirements must be in place before a system can be approved for operation. The standardization gap in this area exacerbates as the consumer organizations typically do not own or control the underlying system resources that implement the system capabilities. Standardization in policies, processes, and technical controls that support the security auditing requirements, regulations, and law compliance needs to consider the collaboration process between the cloud consumers and providers, their roles, and the sharing of the responsibilities in implementing the system capabilities.

#  Accessibility

# A standardized “framework” for exchanging an individual’s accessibility requirements does not presently exist. A standardized method for automatic recognition of a user’s requirements for accessibility would automatically identify the need for having an accessibility requirement known after the first request, for example, captioning for all subsequent video. (Note: Such automatic recognition features can trigger privacy issues depending how the information is used.)

# Standardization priorities based on Cloud Computing Adoption Priorities

# As described in the Federal Cloud Computing Strategy, some cloud computing business use cases have higher priorities than others. The requirements expressed in these high-priority target business use cases can be used to prioritize the standardization gaps. For example, various USG groups have identified data center consolidation using virtualization technologies as one of the primary goals in the next few years. Migrating collaboration applications, including email messaging (email, contacts, and calendars) and online office productivity application, to the cloud system is also quoted as an early target of government cloud operation.

# By analyzing the USG cloud computing target business use cases with their specific technical requirements, one can point out the following basic drivers that can be used to prioritize cloud computing standard gaps:

# The focus on supporting migration of system workload, including data, metadata and processing logic of existing in-house IT systems, to cloud-based systems to ensure continuous operation; this focus is centered on portability standards.

# The need to have interoperability between existing in-house IT systems and cloud-based systems, as cloud-deployed systems will be only a part of the overall enterprise system; this need is centered on interoperability standards, including security standards.

# The need to help government consumers to choose and buy the most cost-effective solutions. If a cloud solution is not as economical as an in-house traditional IT system, there is no financial incentive to move the system to the cloud system.

# Based on these understandings, the following areas of standardization gaps in cloud computing are of higher priority:

#  Security Auditing and Compliance

# Data format standards for auditing, compliance data and metadata are needed. Standard interfaces to retrieve and manage these data and metadata assets are also required to be integrated with existing tools and processes. In addition, policy, process and technical control standards are needed to support more manageable assessment and accreditation processes, which are often a prerequisite before a system is put in operation.

# Identity and Access Management

# As described earlier, security integration of a cloud system into existing enterprise security infrastructure is a must for the majority of government systems with moderate and greater impact. Existing practices of external cloud-based components in identity and access management is often based on proprietary and custom integration solutions. Constant and standard ways of provisioning identity data, managing identity data, and replicating to-and-from cloud system components, are needed to ensure that consumer organizations’ short-term and long-terms needs are met.

# Many government systems are required to have strong authentication, such as two-factor authentication implemented in an Internet-deployed system. Standards in supporting single sign-on and strong authentication are a must for these types of systems.

# SaaS Application Specific Data and Metadata

# To support the urgent need to migrate certain applications to the cloud system, application-specific data and metadata format standards are required. This is an area where a lot of SaaS providers currently help consumer organizations to migrate their existing system by offering custom conversion and migration support. However, without standards in data and metadata format for these applications, the potential danger exists of creating non-interoperable islands of cloud solutions and vendor lock-in. For example, some SaaS email solutions may not be fully interoperable with in-house email and calendaring solutions. There are specific email working groups25 in the federal cloud computing initiative that are looking into putting forward specific metadata standardization requirements for email security, privacy, and record management. Other SaaS functional areas, such as document management and financial systems, are also among the high-priority areas where standards in data and metadata are needed.

# Resource Description and Discovery

# Description and discovery of computing resources needs are usually the first steps for consumers to take to start using cloud computing. Standard methods to describe resources will facilitate programmatically interoperable cloud applications to discover and use cloud computing resources such as computing resources, storage resources, or application resources. To establish private or community cloud computing as a way to implement data center consolidation, standards for these areas are important to avoid the implementation of vendor-specific interfaces, and also helps to increase the dynamic provisioning capabilities of the solution and utility of the computing resources.

# The following table summarizes the areas of standardization gaps and standardization priorities based on cloud computing adoption requirements.

# Conclusion

# The fundamentals of risk and risk management defined here apply to cloud computing as they do to other forms of outsourcing. Cloud computing may require more robust controls due to the nature of the service. When evaluating the feasibility of outsourcing to a cloud-computing service provider, it is important to look beyond potential benefits and to perform a thorough due diligence and risk assessment of elements specific to that service. Vendor management, information security, audits, legal and regulatory compliance, and business continuity planning are key elements of sound risk management and risk mitigation controls for cloud computing. As with other service provider offerings, cloud computing may not be appropriate for all financial institutions.